



Cyber Security

System-relevant additional information	10
Introduction	11
Other information	12
Type of documentation	12
Security strategy	13
Motivation	13
Protection objectives	14
Golden rules for secure systems	15
Defense in Depth concept	19
Security management	22
Basics of security	23
IEC 62443 terms	23
Types of Components	23
Security Level	24
Security Vector	25
Communication Protocols	26
SSH (Secure Shell)	26
SFTP (SSH File Transfer Protocol)	27
HTTP (Hypertext Transfer Protocol)	28
HTTPS (Hypertext Transfer Protocol Secure)	29
NTP (Network Time Protocol)	30
PLC-Designer Gateway Search	30
PLC-Designer Gateway	31
PLC-Designer UDP Communication	33
OPC UA (OPC Unified Architecture)	36
EtherCAT Master Diagnosis	37
UI Designer	38
UI Designer Secure	39
GCI	40
EtherNET/IP Messaging	41
SysLog	42
Integrity	43
Validate integrity	43
Certificate handling	45
Formats and structures of certificates	45
Examples of use cases for certificates for the use case encryption	46
Difference between self-signed and PKI certificates	48
Generate self-signed certificate	49
Integrate a certificate in the Windows Certificate Store	50
Core Automation Platform	51
Overview	53
Zones and conduits	55
"Enterprise-Zone", "Plant-Zone" and "Production-Zone"	55
"CAP-Machine" Zone	55
"CAP-Field" zone	56
"CAP-Tools" zone	56
Roles	57
Authentication, identification and authorization	59

Content

Certificate handling	62
Integrity and Signing	65
Inventory and Events	66
Conduit IT/OT Gateway	67
Handling SysLog	67
Handling NTP	69
x5x0 IoT Gateway	70
Product description	70
Commissioning and hardening instructions	72
Security mechanisms	73
Security functions	75
x5x0.OPCUAClient.Authentication	75
Drives DataHub	77
Product description	77
Security mechanisms	79
Commissioning and hardening notes and organizational measures	79
Security functions	80
DataHub.UserAPI.Authentication	80
DataHub.Northbound.MQTT	81
DataHub.Southbound.GCI	81
Security data	81
DrivesDataHub.AccountManagementGuidelines	81
DrivesDataHub.AccountManagementGuidelines :: DrivesDataHub.UserManagement	81
DrivesDataHub.Ports	82
EASY System Designer	84
Description	84
Security mechanisms	86
Commissioning and hardening notes and organizational measures	86
Security functions	87
SystemDesigner.DownloadImportFile	87
Security data	88
SystemDesigner.DownloadImportFile:UserPasswordRequirements	88
PLC Designer	89
Product description	89
Security mechanisms	91
Commissioning, hardening and decommissioning notes and organizational measures	93
Security functions	94
PLCDesigner.InstallerInspectorDeploymentServer	94
PLCDesigner.Project.ImportFile	95
PLCDesigner.Project.UserManagement	98
PLCDesigner.PasswordManager	100
PLCDesigner.Project.Integrity	102
PLCDesigner.Project.Encryption.WithPassword	105
PLCDesigner.Project.Encryption.WithCertificate	110
PLCDesigner.Project.Signature.WithCertificate	115
Security data	117
PLCDesigner.AccountManagementGuidelines	117

PLCDesigner.PasswordManager	118
Controller.EncryptedCommunication.PLCDesigner	118
PLCDesigner.Installation	118
EASY UI Designer	119
Product description	119
Security mechanisms	121
Commissioning, hardening and decommissioning notes and organizational measures	123
Security functions	125
UIDesigner.OPCUAClient.Authentication	125
UIDesigner.OPCUAClient.Certificate	127
UIDesigner.ServerManagerUI.Authentication	131
UIDesigner.ServerManagerUI.Certificate	133
UIDesigner.ServerManagerUI.Authorization	136
UIDesigner.TargetDeviceManager.Authentication	137
UIDesigner.TargetDeviceManager.Certificate	141
UIDesigner.TargetDeviceManager.Authorization	142
UIDesigner.UserManagement	143
UIDesigner.SystemUseNotification	147
Security data	150
UIDesigner.AccountManagementGuidelines	150
Storing credentials for authentication	151
Controller	153
Controller 1.x	154
Product description	154
Security mechanisms	157
Commissioning and hardening notes and organizational measures	160
Security functions	163
Controller.SFTPServer	163
Controller.SSHServer	170
Controller.Firewall	173
Controller.UserManagement	185
Controller.EncryptedCommunication.PLCDesigner	199
Controller.Application.Signature	210
Controller.Application.Encryption	211
Controller.CertificateStore.viaPLCDesigner	222
Controller.CertificateStore.viaAdvancedVisu	226
Controller.CertificateStore.HAProxy	231
Replace Certificate for HA Proxy	235
Controller.WebDiagnosis	236
Controller.OPCUAServer.Authentication	240
Controller.OPCUAServer.Certificate	244
Controller.OPCUAServer.GDS	245
Controller.OPCUAServer.GDS.Provisioning	245
Controller.OPCUAClient.Authenticate	247
Controller.OPCUAClient.Certificate	250
Controller.SysLog	251
Controller.SecurityKeyService (SKS)	261
Controller.ComponentDirectory	263
Controller.NTP	266

Content

Controller.WebVisu.Activation	268
Controller.WebVisu.UserManagement	270
Controller.WebVisu.Certificate	272
Controller.USB-Interface	274
Security data	276
Controller.AccountManagementGuidelines	276
Controller.Firewall : PortList with deactivate firewall	278
Controller.Firewall : PortList with activated firewall and default parameter set	280
Controller.EncryptedCommunication.PLCDesigner : Certificate	282
Controller.CertificateStore.HAProxy : Certificate	282
Controller.CertificateStore.SysLogProxy : Certificate	282
Controller.SysLog : MonitoredFilesAndDirectories	283
FAST	285
Product description	285
Security mechanisms	287
Commissioning and hardening instructions	288
Security functions	289
FAST.Library.Signature	289
FAST.SysLog	295
Security data	298
FAST.AccountManagementGuidelines	298
v4x0 Web Panel	299
Product description	299
Security mechanisms	301
Commissioning, Hardening and Decommissioning Notes and Organizational Measures	302
Security functions	304
v4x0.FirmwareUpdate	304
v4x0.Authentication	309
v4x0.Authorization	315
v4x0.Certificate	317
v4x0.Session	319
v4x0.NTP	321
v4x0.Services	322
v4x0.WebBrowser	326
v4x0.Logging	326
v4x0.Security	327
v4x0.BackupAndRestore	327
Security data	328
v4x0.AccountManagementGuidelines	329
v4x0.PortList	329
EASY Starter Suite	331
EASY Starter	332
Product description	332
Security mechanisms	334
Commissioning, hardening and decommissioning notes	335
Security functions	336
EasyStarter.Authentication	336

EasyStarter.Certificate	338
Security data	344
EasyStarter.AccountManagementGuidelines	344
EasyStarter.Certificate	344
EASY Firmware Loader	345
Product description	345
Security mechanisms	346
Commissioning and hardening instructions	347
Security functions	349
FirmwareLoader.Authentication	349
FirmwareLoader.Certificate	351
Security data	351
FirmwareLoader.AccountManagementGuidelines	351
EASY Application Loader	352
Product description	352
Security mechanisms	353
Commissioning and hardening instructions	354
Security functions	356
ApplicationLoader.Authentication	356
ApplicationLoader.Certificate	359
Security data	359
ApplicationLoader.AccountManagementGuidelines	359
EASY Package Manager	360
Product description	360
Security mechanisms	361
Commissioning and hardening notes and organizational measures	362
Security functions	364
PackageManager.Tool.Integrity	364
PackageManager.Package.Integrity	365
Security data	366
PackageManager.AccountManagementGuidelines	366
PackageManager.FirmwarePackage.Integrity: Hash Function	366
PackageManager.Tools.Integrity: Hash Function	366
i9x0 servo inverters	367
Product description	367
Security mechanisms	370
Security mechanisms : Device Replacement	373
Device Replacement (i9x0-base) from Version V1.x to Version V2.x	373
Device Replacement (i9x0-para) from Version V1.x to Version 2.x	373
Device Replacement (i9x0-prog) from Version V1.x to Version V2.x	374
Device Replacement (i9x0-prog) from Version V2.x to Version V2.y	375
Security mechanisms : Nodename	377
Commissioning, Hardening and Decommissioning Notes and Organizational Measures	379
Security functions	381
i9x0.SFTPServer	381
i9x0.SSHServer	388
i9x0.MinimumAndDefaultSecurity	389
Identification of the secure default delivery status	390

Content

Set the secure configuration	390
Behavior with minimum security	391
Behavior with default security	392
i9x0.SecureFactoryReset	392
i9x0.Firewall	394
i9x0.UserManagement	401
i9x0.EncryptedCommunication.PLCDesigner	412
i9x0.CertificateStore.viaPLCDesigner	420
i9x0.OPCUAServer.Authentication	422
i9x0.OPCUAServer.Certificate	425
i9x0.Application.Encryption	427
i9x0.NTP	436
i9x0.SecureBoot	438
i9x0.FirmwareUpdate	438
i9x0.DeviceReplacement	439
i9x0.SysLog	440
i9x0.WebVisu.Activation	448
i9x0.WebVisu.UserManagement	449
i9x0.WebVisu.Certificate	452
Security data	455
i9x0.AccountManagementGuidelines	455
i9x0.Firewall : PortList with deactive firewall	456
i9x0.Firewall : PortList with activated firewall and default parameter set	457
i9x0.EncryptedCommunication.PLCDesigner : Certificate	459
i9x0.CertificateStore.SysLogProxy : Certificate	459
i9x0.SysLog : MonitoredFilesAndDirectories	459
o450 Motor Driven Roller	461
Product description	461
Security mechanisms	462
Commissioning and hardening notes and organizational measures	464
Security functions	464
MotorDrivenRoller.FirmwareUpdate	465
Security data	465
MotorDrivenRoller.AccountManagementGuidelines	465
m300 Lenze Smart Motor	466
Product description	466
Security mechanisms	468
Security mechanisms :: Decommissioning	469
Commissioning and hardening notes and organizational measures	469
Security functions	470
m300.FirmwareUpdate	470
m300.AccessProtection	471
m300.BackupAndRestore	472
Security data	472
m300.AccountManagementGuidelines	472

Version	Date
4.0	04/2026



Current sets of documentation and software updates with regard to Lenze products can be found in the Download area at:
www.lenze.com

Target group

This documentation is intended exclusively for qualified technical personnel.

System-relevant additional information

The following information can be found in this chapter

- Introduction
- Security strategy
The motivation is introduced and the protection objectives are discussed. In addition, the golden rule for secure systems, the defense in depth concept and a brief introduction to the topic of security management are introduced.
- Basics of security
The IEC 62443 standard, the communication protocols, some notes on integrity and certificate handling are described here.
- Core Automation Platform
This section contains a typical product constellation and a grouping into zones and conduits.

Introduction

For the main Lenze product lines, Lenze discusses selected technical topics from ongoing product development and support, without any guarantee of completeness or accuracy.

Our cyber security documentation provides information on:

- Functional enhancements
- Remedied functional limitations
- Functional limitations

Our cyber security documentation is intended exclusively for qualified technical personnel. Our cyber security documentation is carefully edited, but it contains only general information (self-help for users of the cyber security documentation). It is explicitly not a consulting offer for the respective concrete technical problem solution. If you need advice for a specific technical problem, please contact us directly.

Our cyber security documentation service therefore expressly does not include any assumption of liability by us, as you use our cyber security documentation at your own risk.

For clarification: Our other obligations within the scope of concluded customer contracts remain unaffected by this.

Before using our cyber security documentation, please note:



This cyber security documentation is intended only for qualified technical personnel of business users of Lenze products.

This cyber security documentation is a self-help tool that users may utilize exclusively at their own risk, excluding any liability on the part of Lenze.

Introduction

Other information

Other information

Lenze reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the security documentation and other Lenze publications such as catalogs, the content of the other documentation shall have precedence.

Type of documentation

The cyber security strategy first provides for a description of the status quo and, based on this, enables a step-by-step implementation of the requirements of IEC 62443. This documentation currently describes some of the implemented functions and is thus intended to provide clarity in the functions described here. This documentation is not yet full and therefore does not yet reflect the complete picture of the components.

Security strategy

The motivation is introduced and the protection objectives are discussed. In addition, the golden rule for secure systems, the defense in depth concept and a brief introduction to the topic are introduced.

Motivation

In order to introduce cyber security, the interaction between components, organization and people must be considered.

Three aspects of cyber security are important:

- Components considered for security
- Management systems for security
- Trained personnel for security

These three aspects are part of the cyber security consideration in the following standard. The IEC62443 standard focuses on three levels, the operator, the system integrator and the component supplier.

- IEC 62443-2-x: Operator
- IEC 62443-3-x: System Integrator
- IEC 62443-4-x: Component Supplier

IEC 62443-2-x overlaps with IEC 2700x, as this is where the aspects of information security and cyber security come together.

Information security focuses on the protection of business processes. The focus here is on minimizing business risk. This results in a prioritization of the protection objectives:

1. Confidentiality
2. Integrity
3. Availability

Cyber security focuses on the assets in the automation system (OT – Operational Technology). The focus here is on the protection of assets against unauthorized use and the associated modification with regard to disclosure of information. This results in the following protection objectives:

1. Availability
2. Integrity
3. Confidentiality

These objectives are achieved through a combination of security functions within the assets, as well as organizational measures and requirements for the asset environment. Only a comprehensive approach ensures the necessary protection objectives.

It is important to differentiate between functional safety and cyber security. Although these two considerations represent an interface, the focus is different and the observation can be done separately, except for a few repercussions. The focus differs as follows.



Focus of Functional Safety:
Protection of life and the environment.



Focus of cyber security:
Protection of equipment, facilities, including the necessary data.

Protection objectives

Availability

"We say that the system ensures availability when authenticated and authorized subjects cannot be interfered with in the exercise of their permissions without authorization." (Claudia Eckert)

Different parallel processes run in an IT system. These processes can have a certain degree of influence on the system. However, as long as these processes are executed within a designated time frame that does not adversely affect the system's promised availability, they are generally considered valid. Only when the retroactive effect affects the assigned availabilities are they interpreted as harmful. This can occur, for example, due to an excessive processor load.

Integrity

"We say that the system ensures data integrity when it is not possible for subjects to manipulate the data to be protected without authorization and unnoticed." (Claudia Eckert)

Integrity considerations require an existing authorization to define rights. On the basis of these rights, subjects are allowed to make changes to data. In contrast, other subjects are not allowed to make changes. Integrity ensures that no unauthorized changes have been made to the data. This can be done on the basis of data in motion (e.g. via Ethernet) or data at rest (e.g. stored files).

Integrity lies between a tamper protection, which is a mechanism that securely reliably prevents changes and a manipulation detection, which is a mechanism that reliably detects unauthorized changes.

Confidentiality

"We say that the system ensures information confidentiality if it does not allow unauthorized information gathering". (Claudia Eckert)

The basis of confidentiality is an authorization concept. it determines which subject is allowed to access which object. The goal is to prevent unauthorized subjects from accessing the objects.. Even with this protection goal, a distinction can be made between confidentiality of data in motion (e.g. over Ethernet) or data at rest (e.g. stored files).

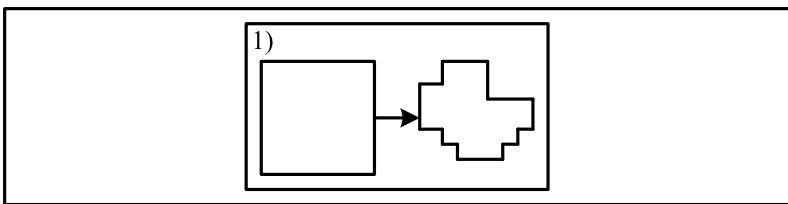
Golden rules for secure systems

The focus is on all cyber security requirements that have a preventive character. These can be summarized in the following 7 golden rules.

Based on these golden rules, the following requirements are necessary:

- Security know-how for the user of the components.
- Physical access control to the components.
- Loss of convenience in handling the components.
- Higher configuration and programming effort for the PLC programmer, the engineer and the service technician.

Minimize Attack Surface



Golden Rule: Minimize Attack Surface

Every area of a system used represents a potential attack surface. The goal is therefore to keep this attack surface as small as possible and thus minimize it. For this purpose, only the functions in the system that are necessary for essential operation should be usable. This applies not only to externally visible functions but also to the integrated internal functions.

The following points need to be optimized:

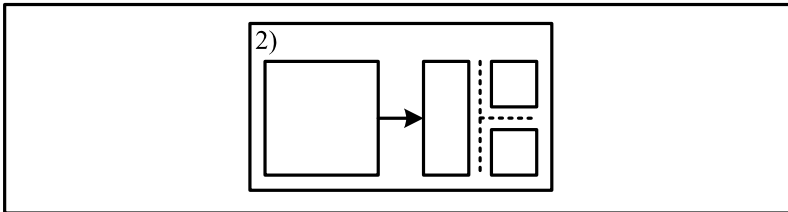
- Uninstall or deactivate software packages that are not necessary
- Disable unnecessary services or features
- Check factory settings and restrict them if necessary
- Restrict user privileges and access rights
- Limit network functions, e.g. ports, protocols, services
- etc.

All these measures fall within the scope of system or component hardening and are subject to the least privilege principle. The least privilege principle is a cyber security concept in which a user is only granted the minimum level of access or authorization required for his or her activity.

Security strategy

Golden rules for secure systems

Separate Systems



Golden Rule: Separate Systems

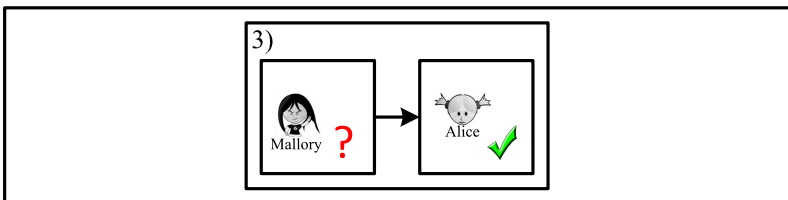
An effective mechanism for security resilience is the defense-in-depth concept. It describes a layered security structure with cascading protection mechanisms. Several layers act on different protective mechanisms.

The concept of defense-in-depth is underlined by the separation of essential functions. Here, the main functions should be logically separated. This makes it more difficult for an attacker to continue to hang on.

The following points need to be optimized:

- Separation of physical or logical networks
- Separation of preparation systems for development and verification to the main system for production
- Separation of different protection zones for assets with different protection needs
- etc.

Appropriate Authentication



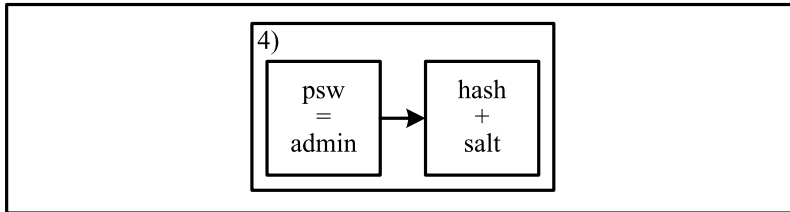
Golden Rule: Appropriate Authentication

As soon as a communication is confidential (at the latest when it crosses a security zone), it must be authenticated. This applies regardless of whether the communication is between humans, software processes, or devices.

The following points need to be optimized:

- The stronger authentication method is preferable to the weaker one
- Consideration of the transfer of authentication secrets
- Consideration of the storage of authentication secrets
- Establishment of a role-based access system and the need-to-know principle (knowledge only if necessary) to be used
- Consistent withdrawal of authorization without necessity
- etc.

Confidential encryption



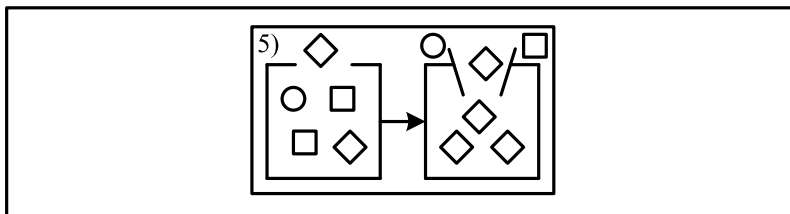
Golden Rule: Confidential encryption

The establishment of this requirement starts with the identification of the trustworthy information. This information must be encrypted due to its sensitive content. Here, the consideration refers to the transmitted information, as well as to the resting information.

The following points need to be optimized:

- Consideration of encryption methods with regard to their security
- Consideration of the handling of the necessary keys
- Consideration of auxiliary procedures, e.g. the key exchange
- etc.

Validate Inputs



Golden Rule: Validate Inputs

Any external input must be validated. It is irrelevant whether this input is from a human user, a software interface, or a device.

The content of the validation is the check for expected inputs. This is intended to exclude the exploitation of extended input up to the insertion of active code.

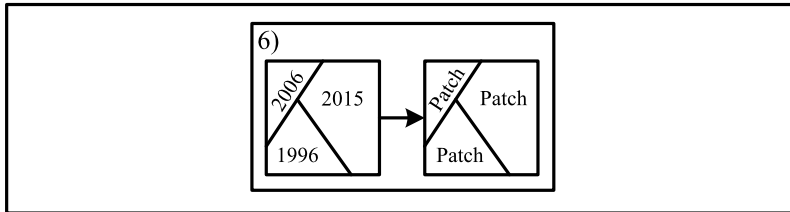
The following points need to be optimized:

- Checking the character set (e.g. checking whether unauthorized characters are present)
- Checking the length (minimum and maximum length)
- Checking the time input (e.g. the fast repetition on an interface for human users is conspicuous)
- Checking the content (e.g. February 31 is not a valid date)
- etc.

Security strategy

Golden rules for secure systems

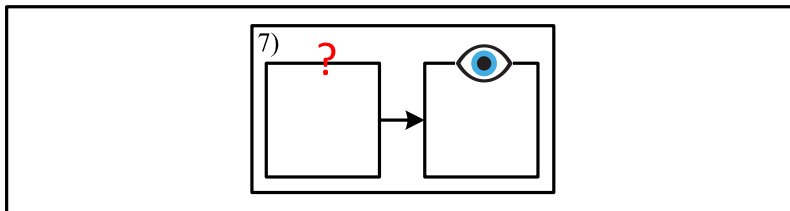
Update regularly



Golden Rule: Update regularly

Systems or components with outdated versions are vulnerable to attacks. Especially in the case of known security vulnerabilities, corresponding versions must be patched. It should be noted that patches can be introduced by the component vendor, but also corrective action can also take place in the component environment.

Continuously Verify Security



Golden Rule: Continuously Verify Security

The cyber security attack analysis is not static but constantly evolving. This affects the security level of the components or the system if it is not constantly improved.

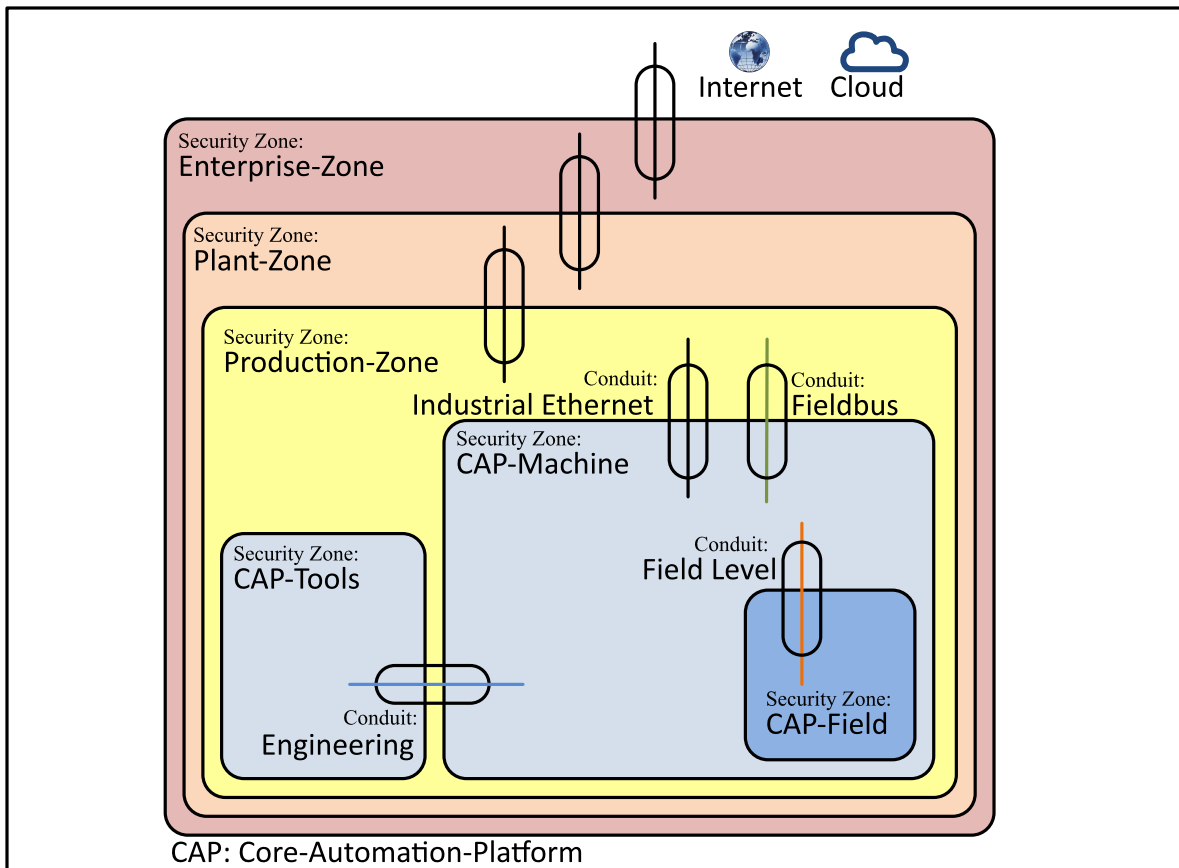
System monitoring must be used. These are advanced firewall systems IPS (Intrusion Prevention Systems) or IDS (Intrusion Detection Systems). As a result, the field of application is observed and measures can be derived directly from it.

This system monitoring is accompanied by verification at component level. Vulnerability and penetration tests should be mentioned here.

Finally, a process must be established to evaluate the relevant log files.

Defense in Depth concept

Due to the increasing networking of horizontal and vertical data streams, the need for cyber security in automation systems is increasing. IEC 62443 requires a protection concept "Defense in Depth". This requires multi-layer protection in automation at both system and component level. The following describes the Defense in Depth concept at the system level. The schematic structure Minimization of in the following picture.



Defense in Depth Concept

Here, the protection mechanisms for the operator of a plant fall on the enterprise, plant and production zones. A consideration according to IEC 62443-3-x is recommended.

The following properties are assumed and must be ensured by the operator:

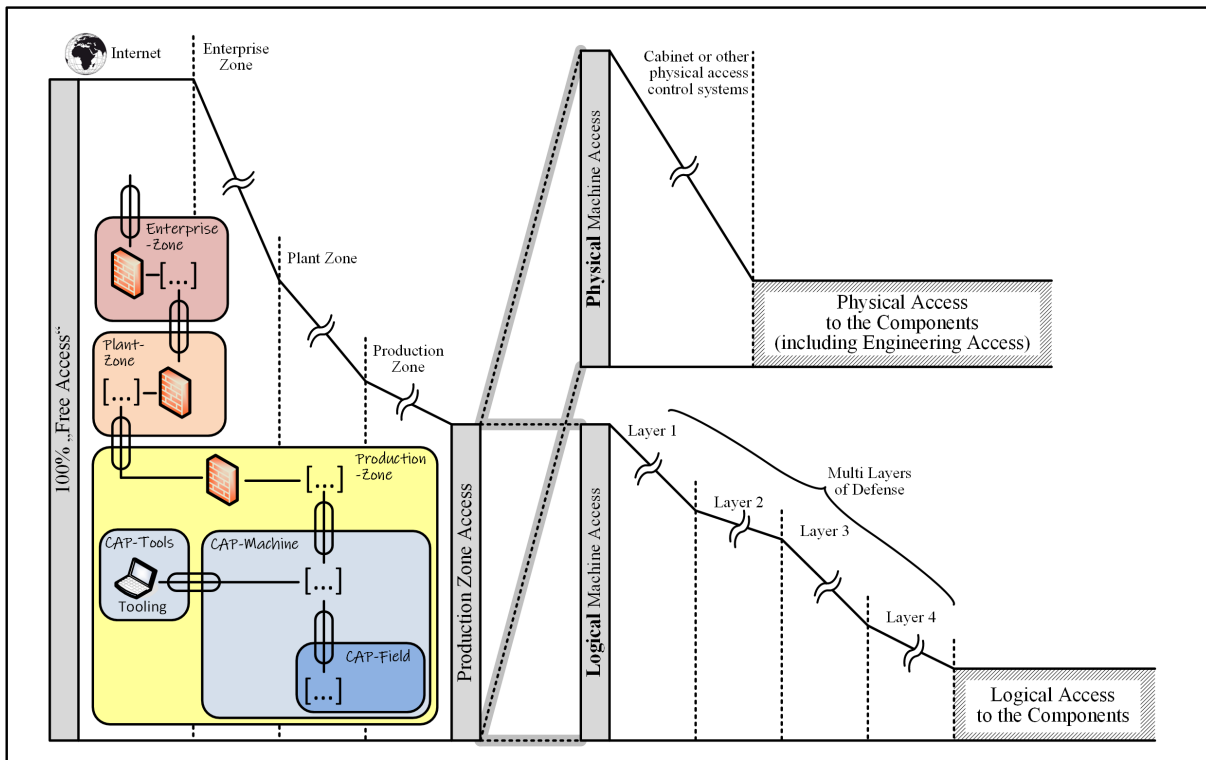
- Minimization of the physical access to the machine, e.g. locking the cabinets.
- Firewall Protection to minimize the Attack Surface.
- Virus Protection to scan all data in motion and at rest.
- Risk appropriate authentication methods.
- Organizational measures for protection, when handling with removable data carriers.

A security zone called "CAP Machine" is defined within the production zone. The components in this zone are permanently active and must have the same level of protection.

Additionally, a security zone called "CAP Tools" contains all commissioning and maintenance tools. These tools are not permanently active, but only when necessary. Within the "CAP Machine" security zone, there is a subordinate "CAP Field" security zone. The components in this zone are permanently active, but must be protected by organizational measures.

Security strategy

Defense in Depth concept



Multi Layers of Defense

Some examples of defences of depth are described below. They are not intended to be exhaustive, but merely examples that need to be defined and detailed through a risk assessment in the operation.

Multi Layers of Defense in the Enterprise-, Plant- and Production-Zone (in responsibility of the Operator):

- Administrative Controls: Policies & Procedures
e.g. Cyber Security Guidelines and Implementation of Organizational Activities
- Administrative Controls: User Training & Awareness
e.g. Education of cyber security best practices
- Administrative Controls: Access Control Policies
e.g. Definition of Rights, Groups and Users
- Administrative Controls: Monitoring or/and Auditing
e.g. Review of Policies & Procedures and Monitoring of Auditable Events
- Administrative Controls: Implement of Incident Response Team
e.g. Receiving, reviewing , assessing and addressing security-related issues and/or incidents.
- Physical Controls: Facility Access
e.g. Restrict access to Enterprise-, Plant- and Production Zone.
- Physical Controls: Visitor Access
e.g. Enforcing Visitor Protection
- Technical Controls: Firewalls
e.g. Minimize system surface via blocking networks, devices, ports
- Technical Controls: Network Monitoring
e.g. Intrusion Detection Systems and Intrusion Prevention Systems
- Technical Controls: Antivirus Detection
e.g. Protection of network virus detection and virus detection running on the host-systems

- Technical Controls: Encryptions
e.g. Use only encrypted protocols and encrypt relevant data

Multi Layers of Defense for Physical Machine Access:

- Physical Controls: Cabinet Access or Physical Barriers
e.g. Restrict access to Cabinets

Multi Layers of Defense for Logical Machine Access:

- Administrative Controls: Policies & Procedures
e.g. Implement measures of the Components (refer to Cyber Security Technical Documentation).
- Technical Controls: Firewalls
e.g. Restrict component surface via blocking ports, protocols (refer to Cyber Security Technical Documentation)
- Technical Controls: Encryption
e.g. Use encryption for protocols and relevant data (refer to Cyber Security Technical Documentation)
- Technical Controls: Access Control
e.g. Configuration of Rights, Groups and Users of the components (refer to Cyber Security Technical Documentation)
- Technical Controls: Backup and Restore
e.g. After first implementation generate a Backup and verify the Backup via Restore (refer to Cyber Security Technical Documentation)

Security strategy

Security management

Security management

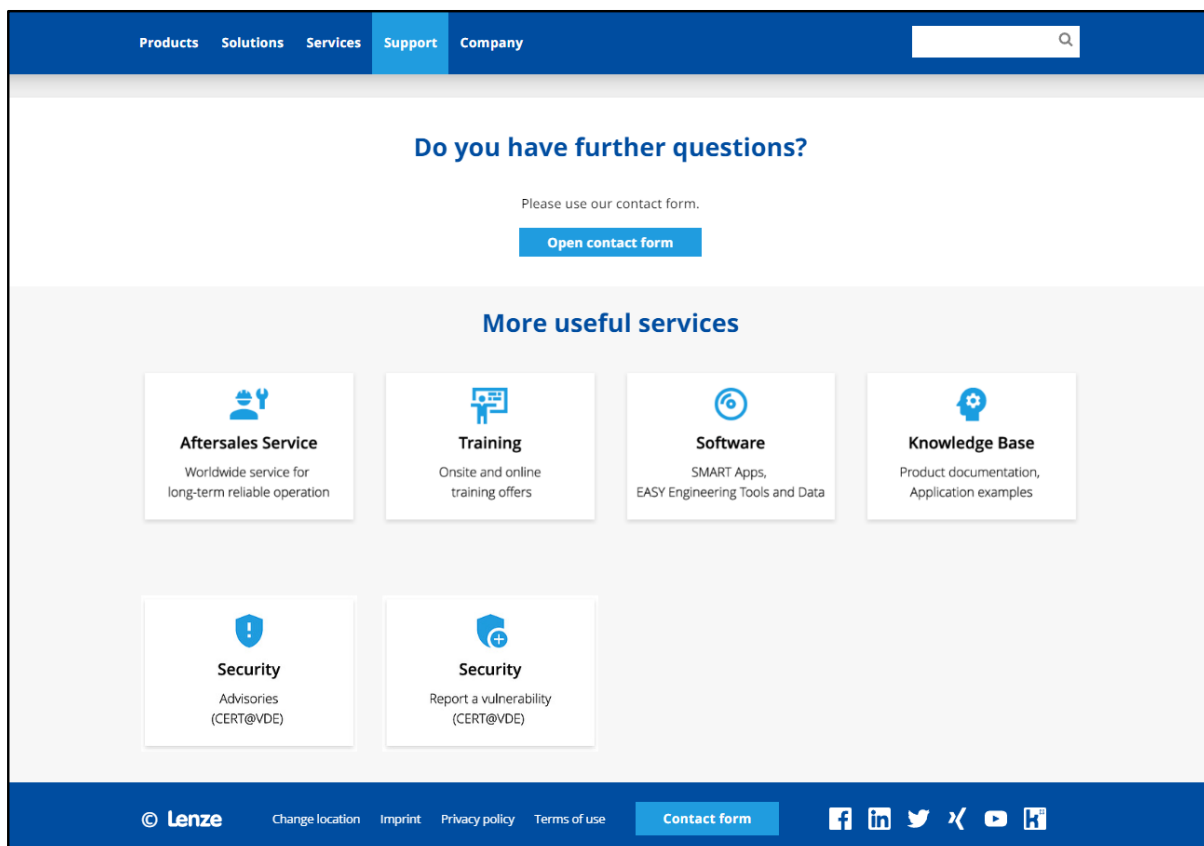
A Product Security Incident Response Team (PSIRT) is currently being established at Lenze SE. For this purpose, a communication channel has been established on the homepage. Contact us via postal address:

Lenze
Hans-Lenze-Straße 1
D-31855 Aerzen
Germany

or via

<https://www.lenze.com/>

and the "Support" tab.



Homepage for Support Security

This includes two links:

- Security advisories (link to the CERT@VDE)
<https://certvde.com/en/advisories/vendor/LENZE/>
The security advisories are published here.
- Report a vulnerability (link to the CERT@VDE)
<https://certvde.com/en/service/report-a-vulnerability/>
You can report a vulnerability here.

Basics of security

The IEC 62443 standard, the communication protocols, some notes on integrity and certificate handling are described here.

IEC 62443 terms

This chapter explains some of the terms used in the IEC 62443 standard.

Types of Components

IEC 62443-4-2 describes the security requirements for the components. These requirements are divided into foundational requirements (FRs). The FRs are then divided into component requirements (CRs) and requirement enhancements (REs). These requirements depend on four types of components.

Software application requirements (SAR)

Software that is either executed on one of the devices mentioned below or used as engineering software for diagnostics and commissioning.

Embedded device requirements (EDR)

A device with a specific purpose and software focus. Usually, firmware updates are possible here, but the user rarely has the chance to change the purpose of the device. This is the difference between EDR and HDR.

Host device requirements (HDR)

A device with a universal character. Usually, commercially available operating systems are used here and the user can adapt the device to the desired purpose.

Network device requirements (NDR)

A device that focuses on network traffic. Examples include are switches, routers and firewalls to NDRs often combine different network segments. Therefore, the focus here should be placed on physical and logical network separation.

Basics of security

IEC 62443 terms

Security Level

The Security Level (SL) is divided into five different levels (0, 1, 2, 3, 4) and cyber security increases with each level.

Security Level	Brief Description
SL 0	No special requirements or protective measures necessary
SL 1	Protection against occasional or accidental abuse Attackers: well-meaning employees or external threats e.g. through negligent application of the IT security guidelines
SL 2	Protection against intentional abuse with simple means, little effort, general skills, low motivation Attackers: no extensive knowledge, no detailed knowledge of IT security, no detailed knowledge of the specialist area, no detailed knowledge of the attacked system e.g. through the use of automated tools targeting a wide area rather than a specific system
SL 3	Protection against intentional abuse with sophisticated means, medium effort, IACS-specific skills, medium motivation (IACS: Industrial automation and control system) Attackers: excellent knowledge of IT security, excellent knowledge of the subject, excellent knowledge of the target system e.g. by using attack vectors specially tailored to the target system
SL 4	Protection against intentional misuse with sophisticated means, considerable effort, IACS-specific skills, high motivation (IACS: Industrial automation and control system) Attackers: excellent knowledge as in SL-3, but with higher motivation and more resources e.g. through the use of high-performance computers, a large number of computers, or a large amount of time

A distinction is made between three types of SL:

- SL-T (Target SL): Desired security level in the target application
- SL-A (Achieved SL): Currently achievable security level in the target application
- SL-C (Capability SL): Currently achievable security level regardless of the target application

Security Vector

The Security Vector was introduced to further specify the key figure of the security level. Here, the focus shifts from the component to the foundational requirements (FRs). Each FR is sorted into a Security Level (SL) and evaluated. This allows different details about the component to be displayed.

The Security Vector is specified as follows:

- $SL(Component) = \{FR1\ FR2\ FR3\ FR4\ FR5\ FR6\ FR7\}$

The component under consideration is referenced in parentheses, and the respective key figures are in curly brackets.

The information in the curly brackets refers to the core requirements from IEC 62443-4-2 and forms the FR (foundational requirements).

- FR1: (IAC) Identification and Authentication Control
- FR2: (UC) User Control
- FR3: (SI) System Integrity
- FR4: (DC) Data Confidentiality
- FR5: (RDF) Restricted Data Flow
- FR6: (TRE) Timely Response to Events
- FR7: (RA) Resource Availability

Basics of security

Communication Protocols

Communication Protocols

Secure communication protects data from unauthorized access and ensures confidential transmission. When digital communication between sender and receiver is encrypted, its content cannot be read by third parties.

SSH (Secure Shell)

Name of Protocol

Secure Shell (SSH)

Purpose

SSH is a cryptographic protocol that enables secure communication over unsecured networks. One common use is accessing remote command line. On this basis, other protocols can be set up, such as the SFTP (Secure File Transfer Protocol). SSH replaces TELNET and other remote logon schemes that provide no security.

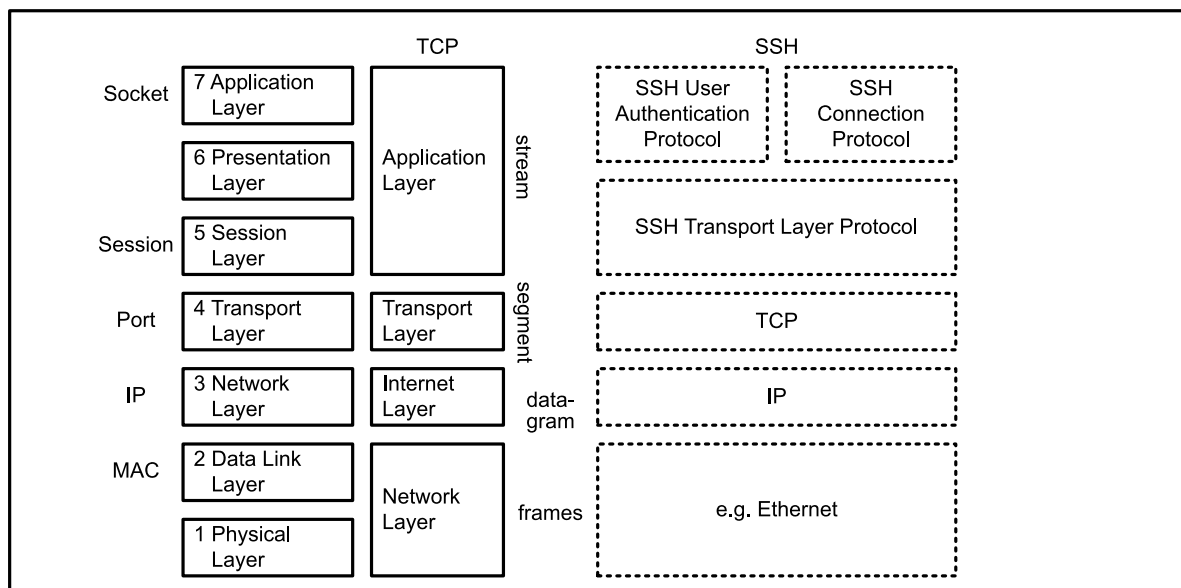
Ports

tcp/22

Architecture

SSH applications are based on a client-server architecture and can be used for network function, such as file transfer. The SSH User Authentication Protocol is used to authenticate the user to the server. SSH Connection Protocol provide logical channels. SSH Transport Layer Protocol is responsible for server authentication, confidentiality and integrity.

ISO/OSI Model



SSH in the ISO/OSI Model

SFTP (SSH File Transfer Protocol)

Name of Protocol

SSH File Transfer Protocol (SFTP)

Purpose

The SFTP is an extension of the Secure Shell Protocol (SSH). The SFTP provides secure file transfer capabilities. This protocol assumes that it is running over a secure channel, such as SSH. This is necessary because SFTP assumes, that there is already an authenticated client and server. It should not be confused with the outdated Simple File Transfer Protocol (SFTP). As auxiliary tools, please refer to PuTTY (<https://www.putty.org/>) and WinSCP (<https://winscp.net/>).

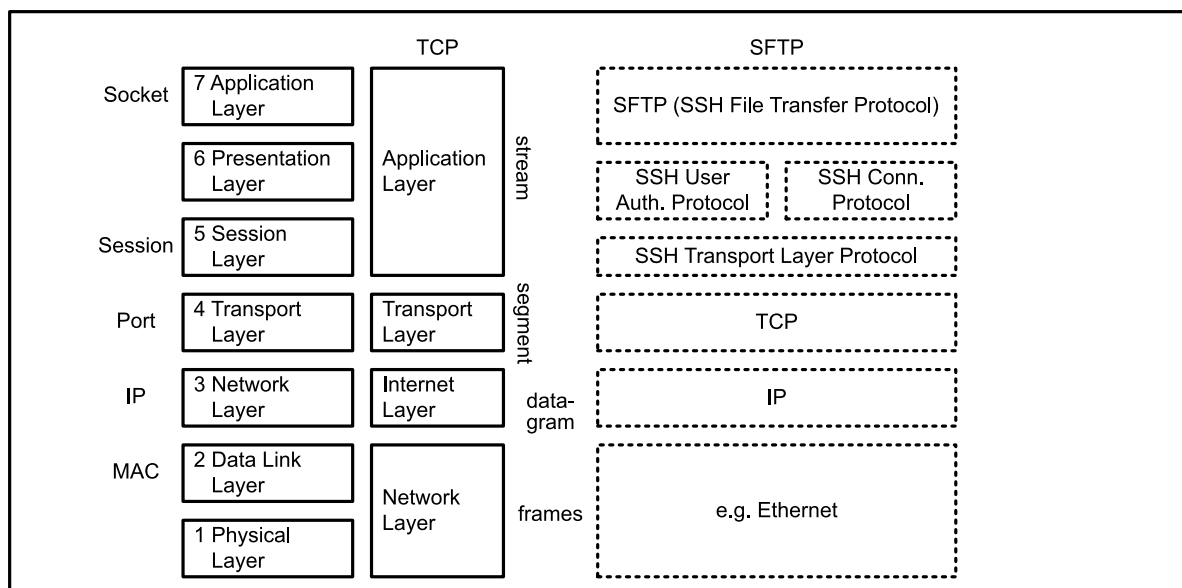
Ports

tcp/22, tcp/31855, tcp/47877

Architecture

SFTP uses the SSH protocol. With this protocol, encrypted data transmission with a connection between client and server and vice versa is possible.

ISO/OSI-Model



SFTP in the ISO/OSI Model

Basics of security

Communication Protocols

HTTP (Hypertext Transfer Protocol)

Name of Protocol

Hypertext Transfer Protocol (HTTP)

Purpose

HTTP is a stateless protocol for transmitting data. The focus here is on the transmission of websites. It is currently no longer recommended to use HTTP, but only the secured HTTPS protocol.

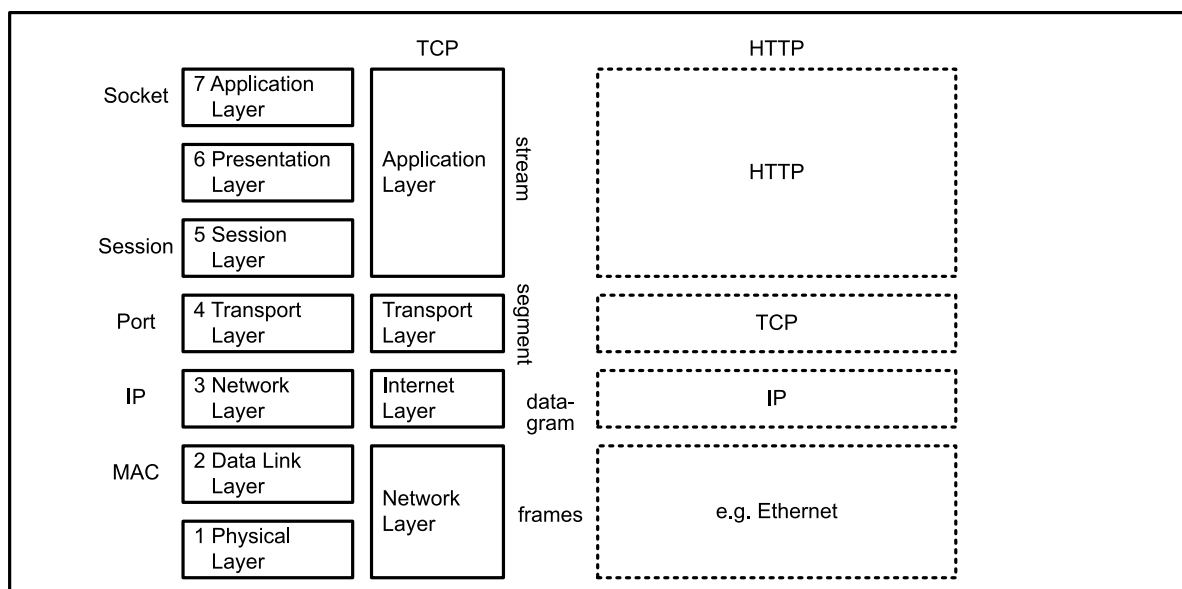
Ports

tcp/80

Architecture

HTTP is based on the TCP layer.

ISO/OSI-Model



HTTP in the ISO/OSI Model

HTTPS (Hypertext Transfer Protocol Secure)

Name of Protocol

Hypertext Transfer Protocol Secure (HTTPS)

Purpose

HTTPS is a communication protocol for that allows data to be transmitted in encrypted form, making it as secure as possible against eavesdropping and forgery. The protection goal is secure encryption and authentication. It is used in the connection between a web browser (client) and a web server (server).

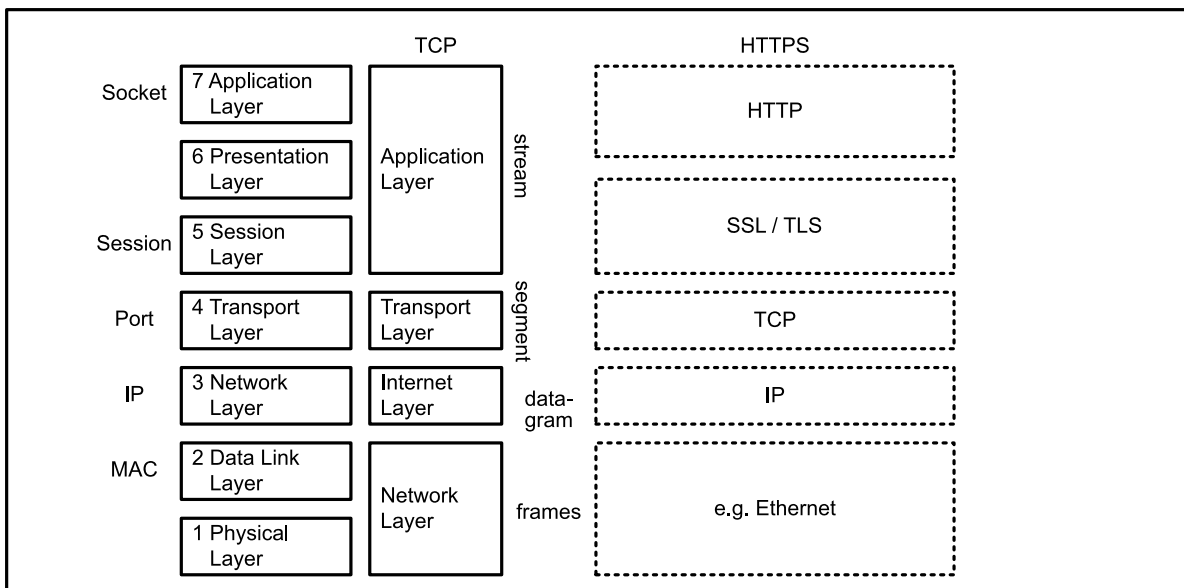
Ports

tcp/443

Architecture

HTTPS is structured similarly to HTTP. The additional protective measures are made possible by the subordinate SSL / TLS. Here, identification and authentication are ensured by the SSL handshake protocol and by a subsequent secure key exchange including encryption to maintain confidentiality.

ISO/OSI-Model



HTTPS in the ISO/OSI Model

Basics of security

Communication Protocols

NTP (Network Time Protocol)

Name of Protocol

Network Time Protocol (NTP)

Purpose

The NTP focuses on the synchronization of real-time clocks in systems. The connectionless UDP protocol is usually used, but the use of TCP is also possible.

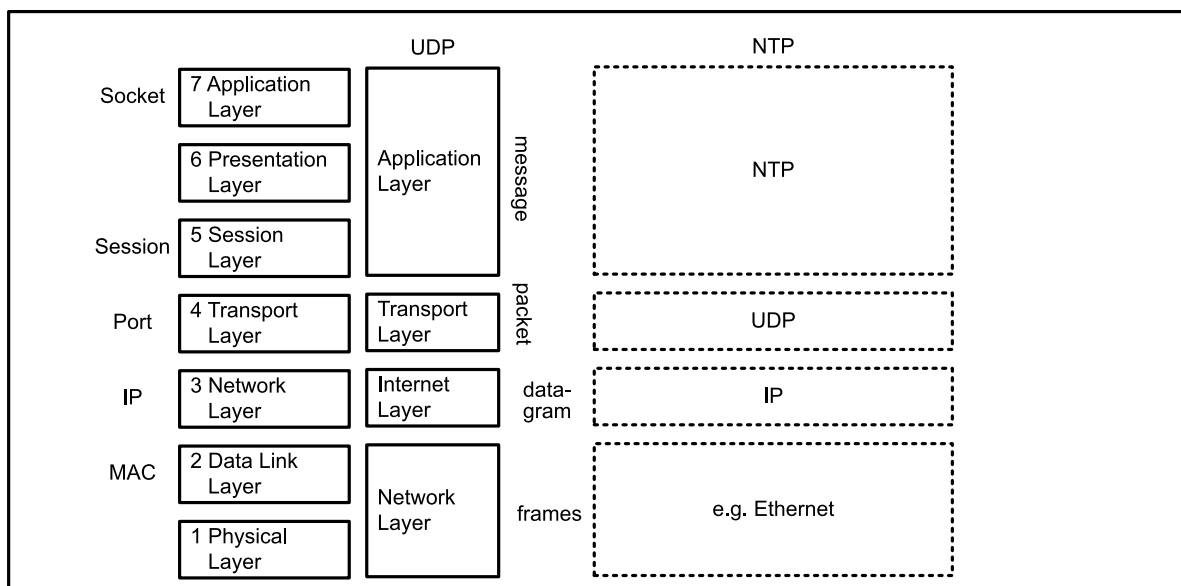
Ports

udp/123

Architecture:

The NTP protocol is usually based on the UDP packet.

ISO/OSI-Model



NTP in the ISO/OSI Model

PLC-Designer Gateway Search

Name of Protocol

PLC Designer Gateway

Purpose

This protocol is used to search for the Gateway via the PLC Designer.

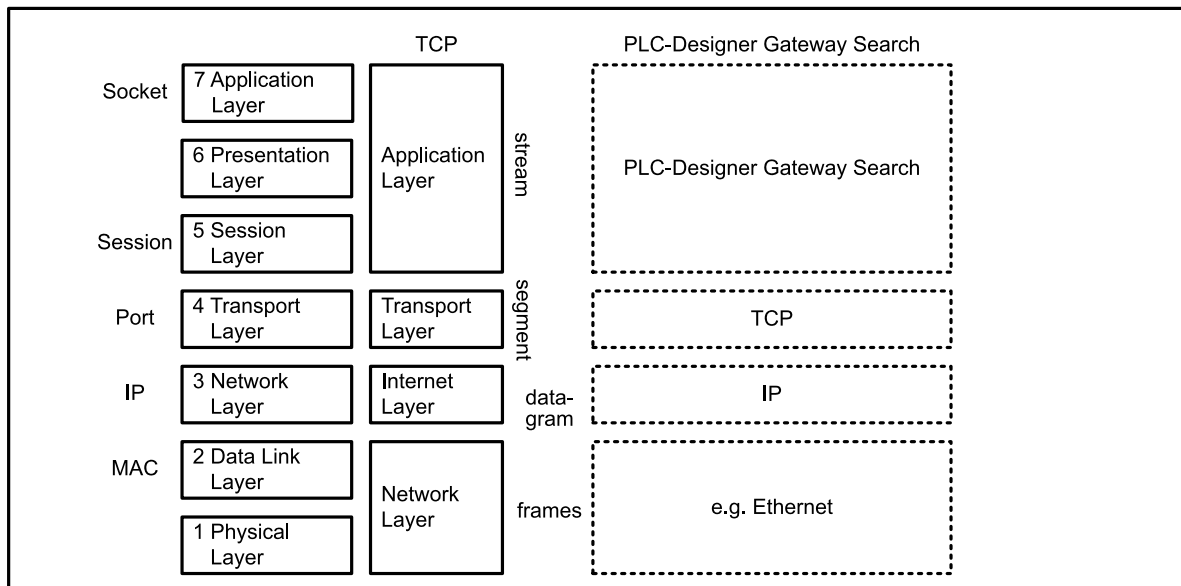
Ports

tcp/1217

Architecture

This communication is based on the TCP communication.

ISO/OSI-Model



PLC Designer Gateway Search in the ISO/OSI Model

PLC-Designer Gateway

Name of Protocol

PLC Designer Gateway

Purpose

This protocol is used for the PLC Designer Gateway.

Ports

tcp/11740

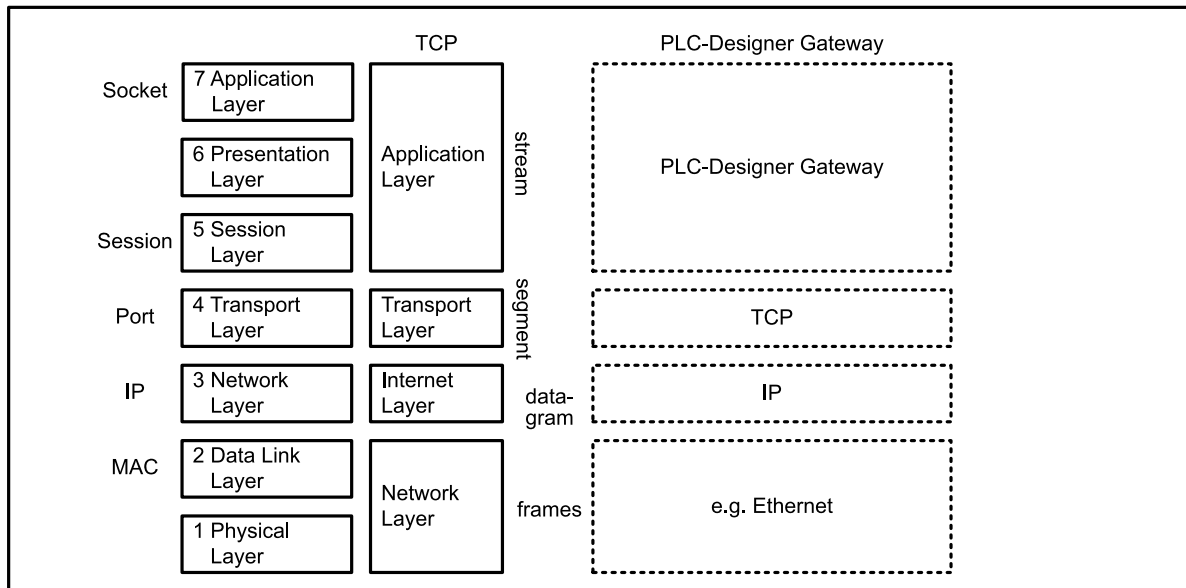
Architecture

These communication is based on the tcp-communication.

Basics of security

Communication Protocols

ISO/OSI-Model



PLC Designer Gateway in the ISO/OSI Model

PLC-Designer UDP Communication

Name of Protocol

PLC Designer UDP Communication

Purpose

This protocol is used to run the network scan and the communication between »PLC Designer« and Controller.

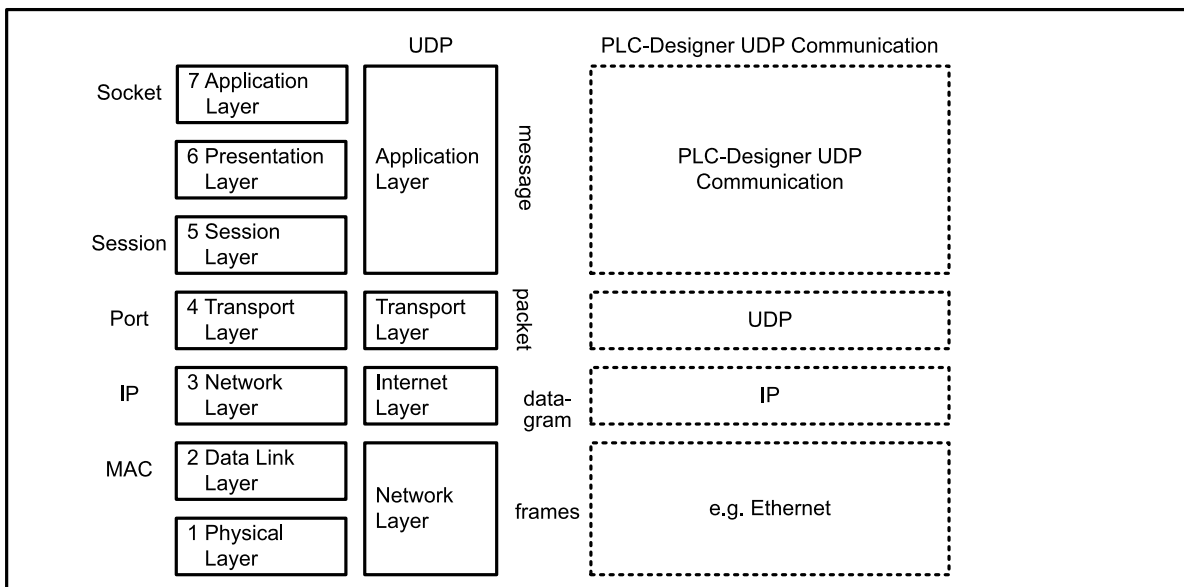
Ports

udp/1740 ... 1743

Architecture

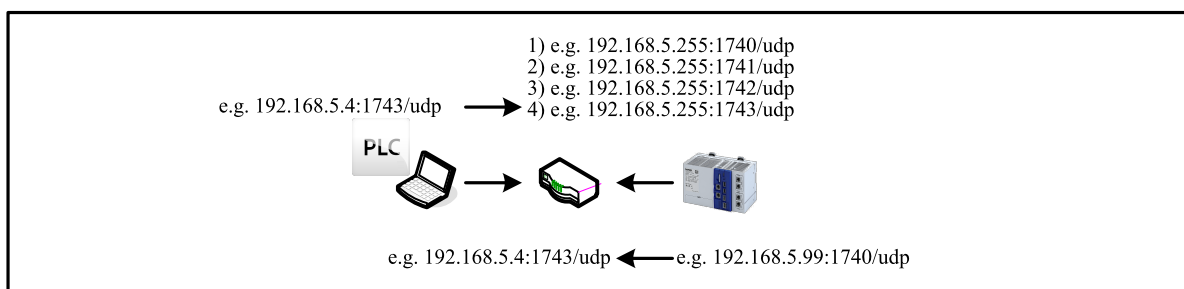
This communication is based on the UDP communication.

ISO/OSI Model



PLC Designer UDP Communication in the ISO/OSI Model

Scan Network



Scan Network

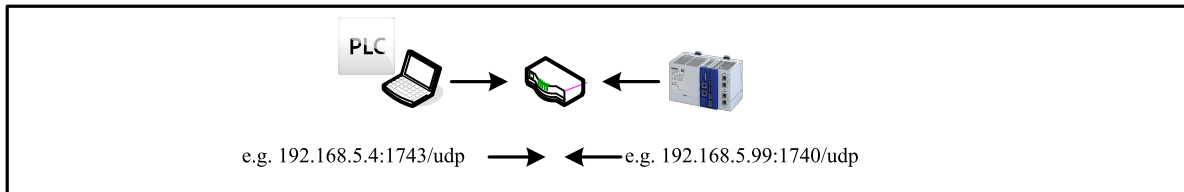
Basics of security

Communication Protocols

The »PLC Designer« is installed on a computer with an exemplary IP address of 192.168.5.4. This requests the network via UDP protocol on port 1743 and requests the broadcast IP address in the subnet on 192.168.5.255 on ports 1740, 1741, 1742, 1743 in sequence. Existing devices, in this example 192.168.5.99, will respond via port 1740 and thus expose themselves to the network scan.

Communication

After performing a network scan, you can access the controller online. Here we use the previously scanned UDP connection.



UDP Communication

Basics of security

Communication Protocols

OPC UA (OPC Unified Architecture)

Name of Protocol

OPC Unified Architecture (OPC-UA)

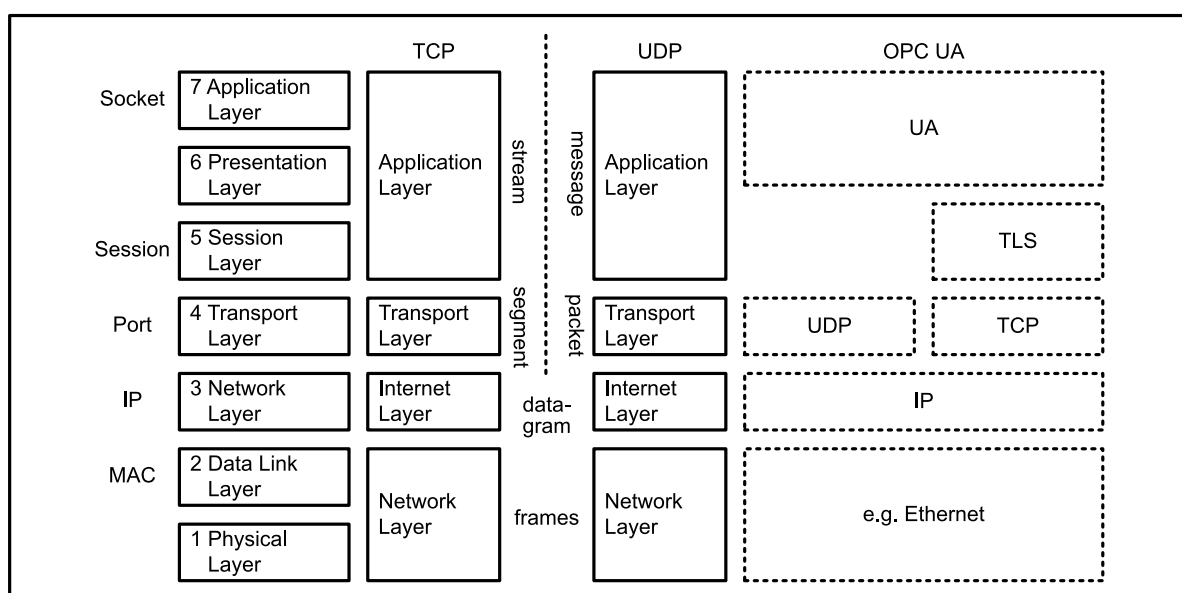
Purpose

The OPC UA protocol is a platform-independent architectural approach. It is primarily used for horizontal and vertical communication in automation systems.

Ports

tcp/4840, udp/4840

ISO/OSI-Model



OPC UA in the ISO/OSI Model

EtherCAT Master Diagnosis

Name of Protocol

X11

Purpose

After installing the »PLC Designer«, a diagnostic tool for the EtherCAT master is available in the »PLC Designer« directory in the LenzeECDiagnosis folder. This diagnostic tool can be used for diagnostics as well as for active access to the EtherCAT Master.

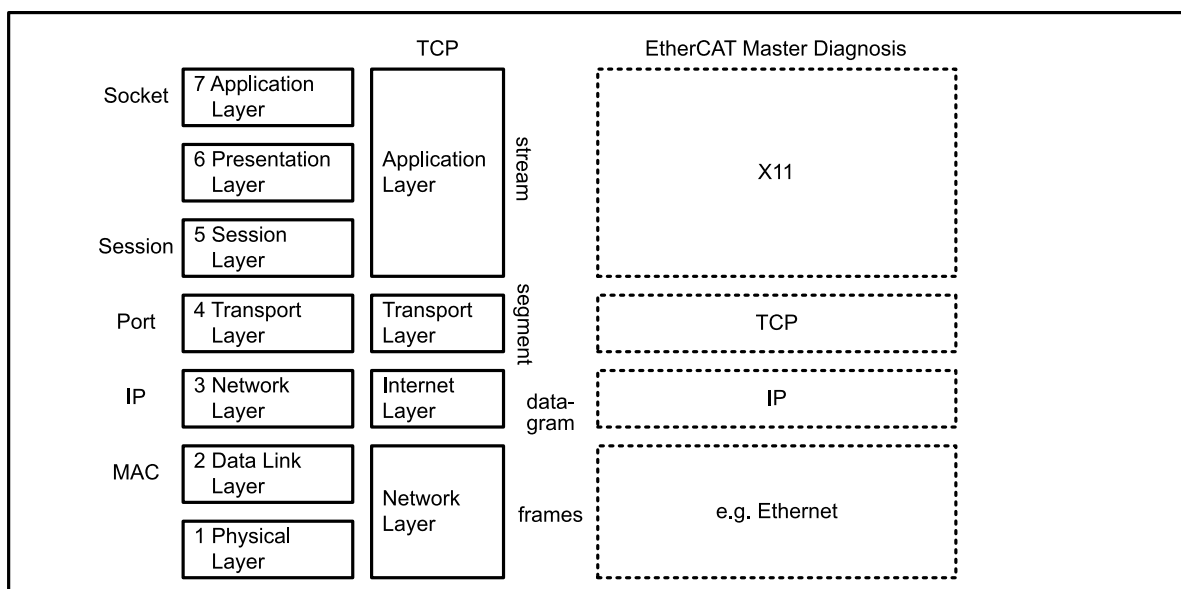
Ports

tcp/6000

Architecture

The protocol used here is based on TCP.

ISO/OSI-Model



EtherCAT Master Diagnosis in the ISO/OSI Model

Basics of security

Communication Protocols

UI Designer

Name of Protocol

UI Designer

Purpose

The »EASY UI Designer« uses the standard TCP IP communication via port 7100.

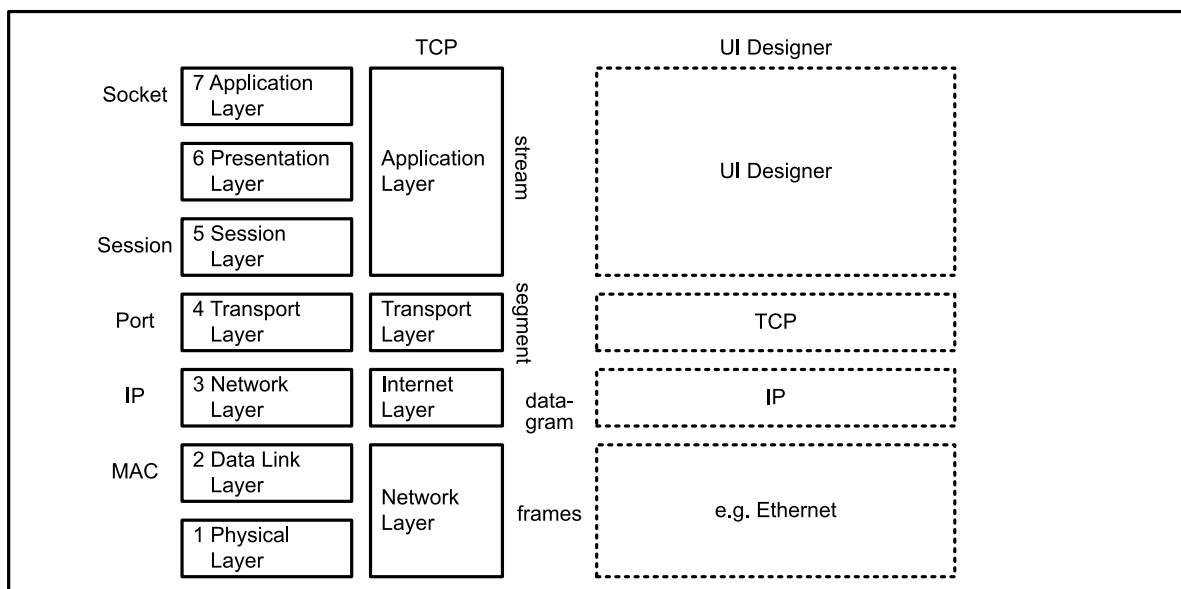
Ports

tcp/7100

Architecture

The protocol used here is based on TCP.

ISO/OSI-Model



UI Designer in the ISO/OSI Model

UI Designer Secure

Name of Protocol

UI Designer Secure

Purpose

The »EASY UI Designer« uses the standard TCP IP communication and the standard SSL/TLS encryption via port 7200.

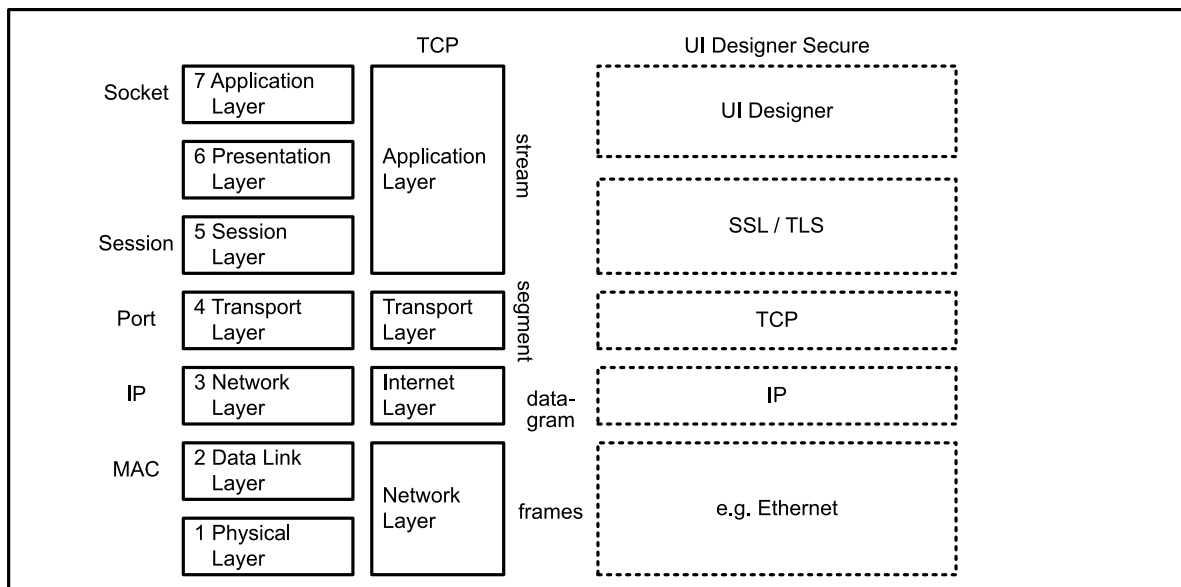
Ports

tcp/7200

Architecture

The protocol used here is based on TCP.

ISO/OSI-Model



UI Designer Secure in the ISO/OSI Model

Basics of security

Communication Protocols

GCI

Name of Protocol

GCI

Purpose

GCI is a proprietary protocol for communication between engineering tools and devices. It is designed to be embedded in various communication protocols. When a GCI is transmitted via an Ethernet protocol, port tcp/9410 is used. The standard TCP connection elements, such as the 3-way handshake, are used here. This is followed by proprietary communication via request and response protocols.

Various services are available via GCI, for example

- GCI parameter service
- GCI file service
- ...

In terms of cyber security, this protocol must be classified as insecure, since it does not include integrity, authentication or encryption.

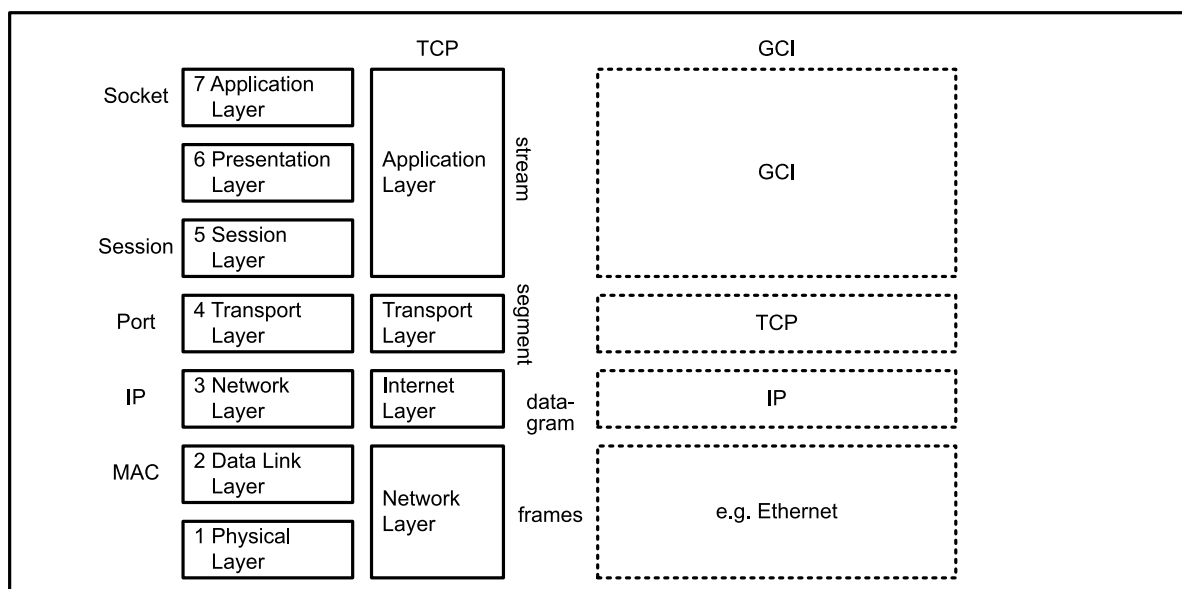
Ports

tcp/9410

Architecture

The protocol used here is based on TCP.

ISO/OSI-Model



GCI in the ISO/OSI Model

EtherNET/IP Messaging

Name of Protocol

EtherNET/IP

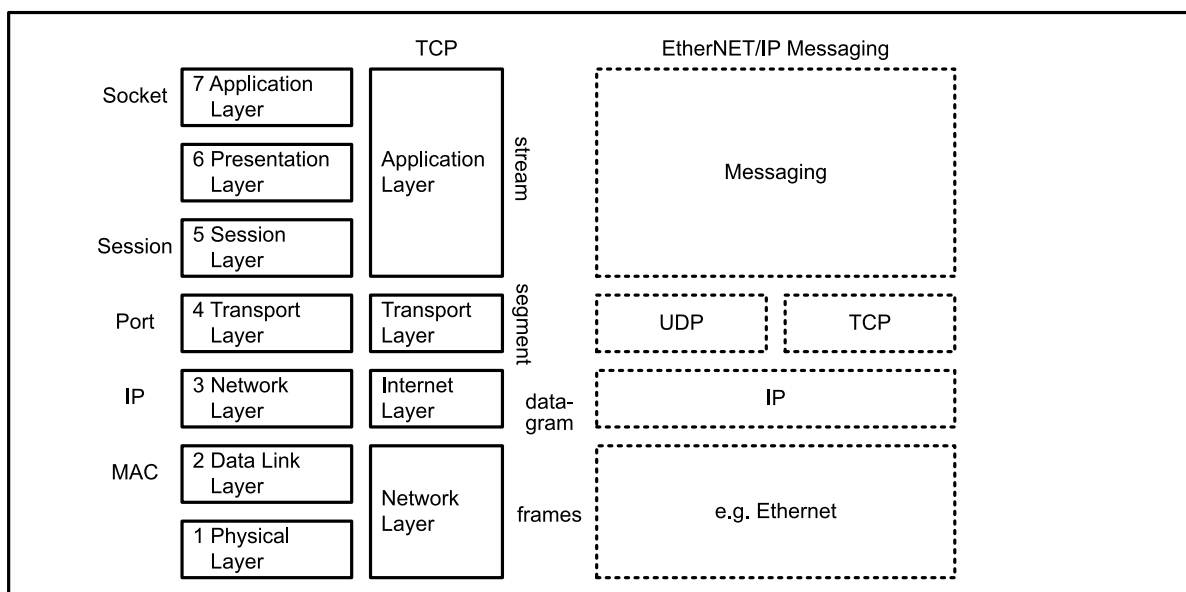
Purpose

The EtherNET/IP protocol via the port 44818 is used for messaging, data transfer, upload/download, peer messaging, etc.

Ports

tcp/44818

ISO/OSI Model



EtherNET/IP Messaging in the ISO/OSI Model

Basics of security

Communication Protocols

SysLog

Name of Protocol

SysLog

Purpose

The System Logging Protocol (SysLog) allows devices to send important activity to a central SysLog server via the SysLog protocol. This allows end users to monitor their infrastructure.

Ports

udp/514

tcp/514

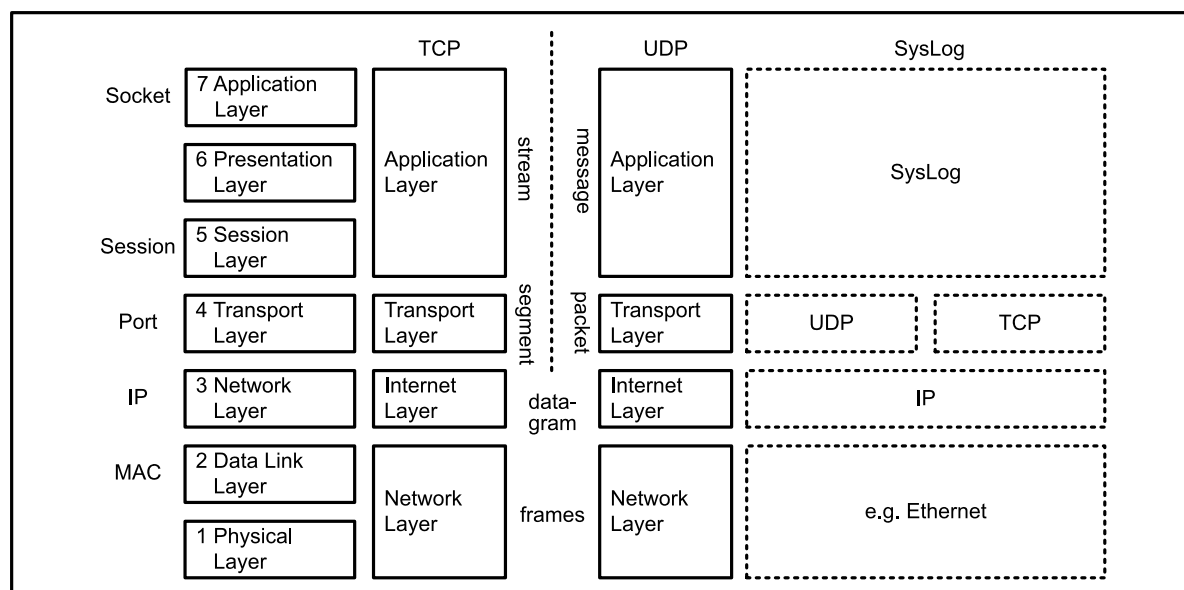


Since some Linux distributions do not allow TCP sockets in the range up to port 1000, the TCP port is often not left at 514, but moved to a higher port range.

Architecture:

The protocol used here is based on UDP or / and TCP.

ISO/OSI Model



SysLog in the ISO/OSI Model

Integrity

Integrity is intended to protect information from unauthorized modification. In most cases, it does not prevent the modification itself, but rather detects an unauthorized modification.

This is usually done using hash functions. These functions map input data to a hash value of a fixed size. This hash function is based on the one-way function requirement, which means that it should be possible to calculate a hash value from input data using simple means. However, it should not be possible to deduce information about the input data from the hash value. Even minor changes to the input data should be clearly visible in the hash value. Additionally, the function must be free of collisions, meaning it should be mathematically very difficult for two different input data to result in the same hash value.

Validate integrity

There are many ways to validate the integrity. In the following, a method using the Windows Command Line Interface (CLI) is presented.

Example Task

A file test.txt is downloaded from a website and additionally the hash value 024348b5-fe28136bbe798f095be5d121edea86dfea2067e1ab0a1c7b8fe79abf is specified on the website. In addition, there is a note that the hash procedure SHA256 was used.

Example Solution

The file test.txt is saved to the hard disk in "c:\temp\". The command line is called with the command "cmd". It is changed with "cd c:\temp\" to the desired directory. With the command "dir" the directory content can be displayed and the file "test.txt" appears. With the following syntax the integrity value can be calculated:

```
certutil -hashfile <file> {MD5 | SHA1 | SHA256 | SHA512}
```

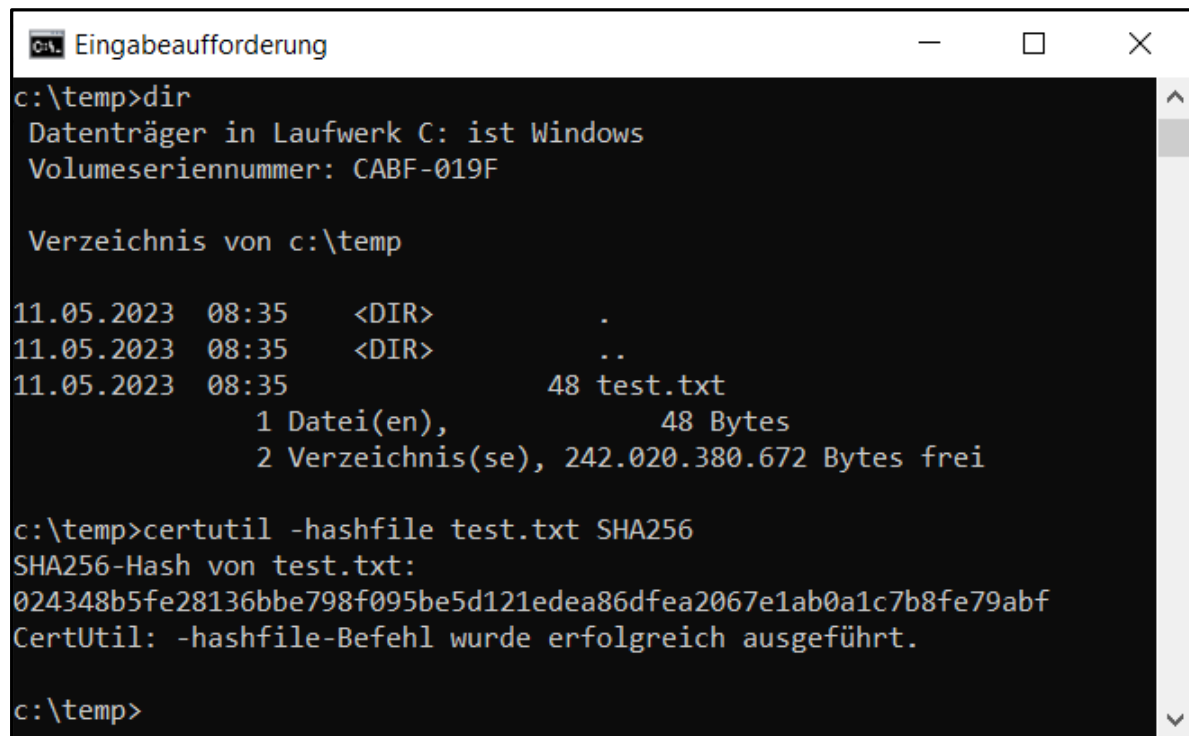
In this example, the command line as follows:

```
certutil -hashfile test.txt SHA256
```

Basics of security

Integrity

And the output looks like this:



```
C:\> c:\temp>dir
Datenträger in Laufwerk C: ist Windows
Volumeseriennummer: CABF-019F

Verzeichnis von c:\temp

11.05.2023  08:35    <DIR>          .
11.05.2023  08:35    <DIR>          ..
11.05.2023  08:35                48 test.txt
                1 Datei(en),               48 Bytes
                2 Verzeichnis(se), 242.020.380.672 Bytes frei

c:\temp>certutil -hashfile test.txt SHA256
SHA256-Hash von test.txt:
024348b5fe28136bbe798f095be5d121edea86dfea2067e1ab0a1c7b8fe79abf
CertUtil: -hashfile-Befehl wurde erfolgreich ausgeführt.

c:\temp>
```

Check hashvalue with certutil

Certificate handling

Certificates can be used in different ways. In most cases, they are used to verify identities or encrypt data.

Formats and structures of certificates

Certificates are based on the ISO/IEC 9594-8:2020 standard, the so-called X.509 standard.

Typical certificate file types:

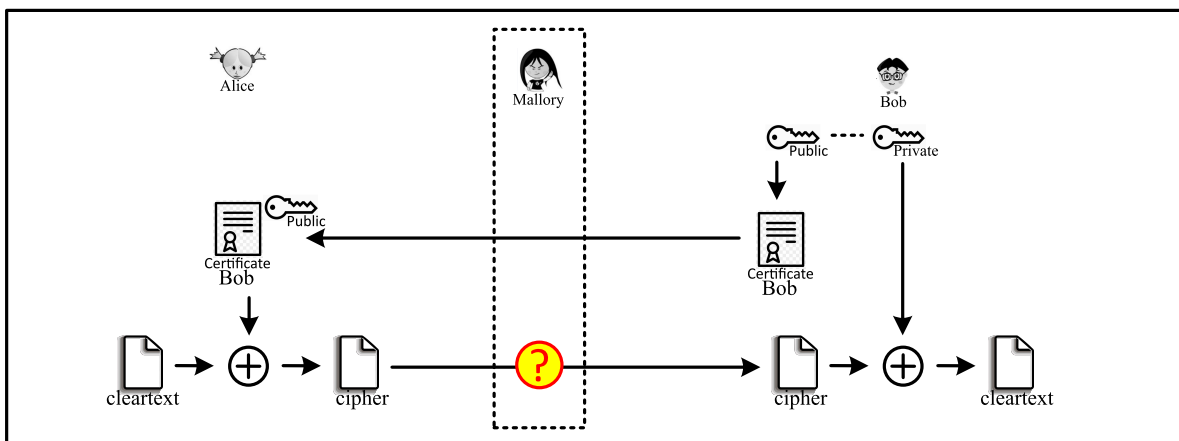
Format	File	Typically included keys	Notes
*.pem, *.cer, *.crt	Base64 encoded ASCII	Public key	Most common format
*.key	Base64 encoded ASCII	Private key	
*.der	Binary	Public and private key	
*.p7b, *.p7c	Base64 encoded ASCII	Public key, include intermediate certificates	
*.pfx	Binary	Private key, include intermediate certificates	

Basics of security

Certificate handling

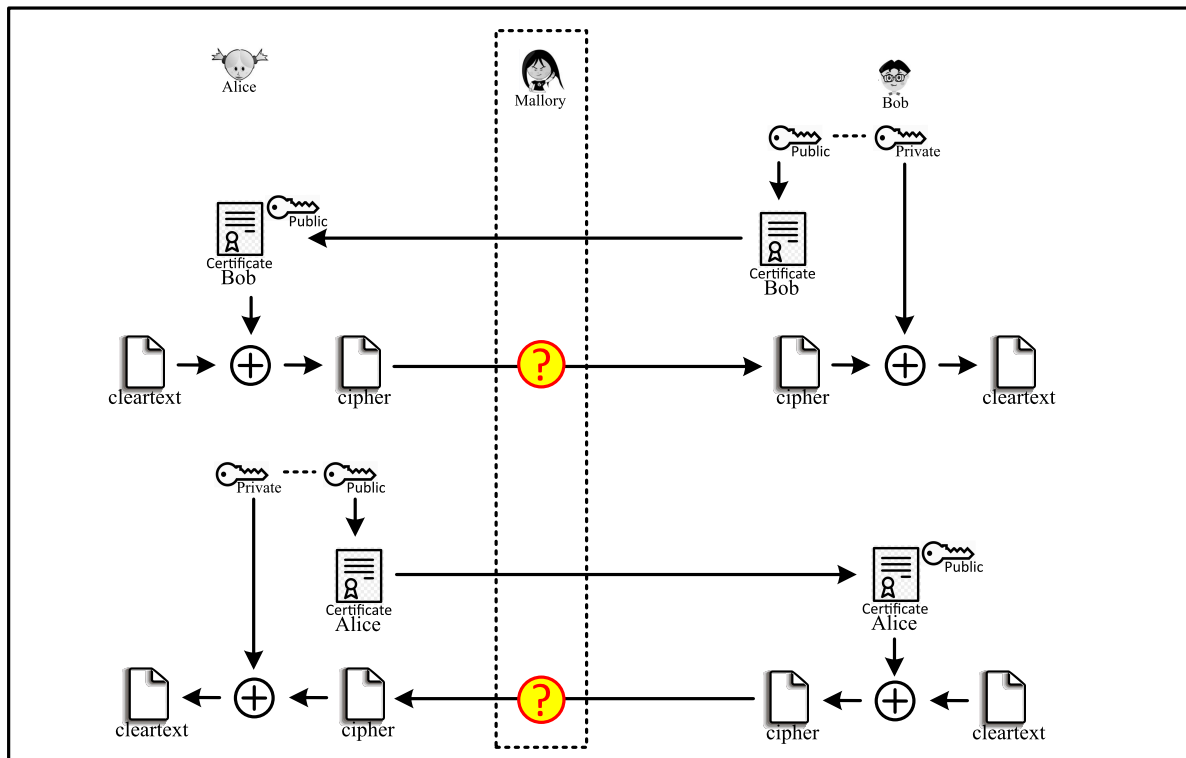
Examples of use cases for certificates for the use case encryption

A simple example of using certificates is outlined here to illustrate the principle. The task is for Alice to send a file to Bob in a way that prevents Mallory from reading it if she intercepts it. To do this, Bob creates a key pair consisting of a private and a public key. The private key remains with Bob and is kept secret. The public key is filed in a certificate and stored as a certificate file. Upon Alice's request, Bob sends the certificate to Alice. Mallory could intercept this and read it as well.



Example for encryption in one way (asymmetric encryption)

Alice takes Bob's public key from his certificate and uses it to encrypt the file to be transferred. If this file is transmitted to Bob and intercepted by Mallory, she cannot read it even if she knows Bob's public key. Bob, in turn, can use his private key to decrypt the file and then read it in plain text. If Bob then wants to send an encrypted reply to Alice, the transport takes place the other way around.



Example for encryption in both ways (asymmetric encryption)

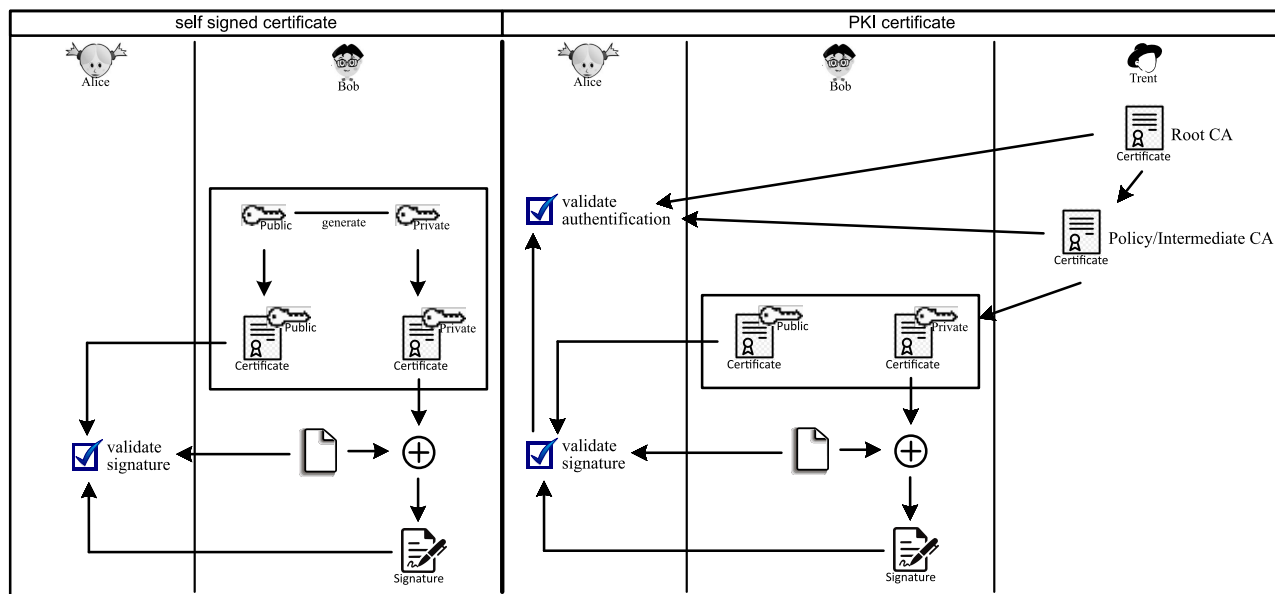
First, Alice generates a pair of keys and puts the public key in a certificate. Then, Bob requests Alice's certificate which contains a key that he can use to encrypt the file. Even if Mallory possesses Alice's public key, she cannot read the file in transit. However, Alice can use the private key to decrypt and read the file.

Basics of security

Certificate handling

Difference between self-signed and PKI certificates

This section contains a very high-level description of certificates. The technical basics cannot be discussed here. In the following picture on the left side is a self-signed certificate and on the right side a PKI certificate is drawn.



Self-Signed Certificates vs. PKI Certificates

The self-signed certificates can be generated by the manufacturer. They consist of a secret part including the private key and a part to be published including the public key. Based on this structure, the user can validate the signature.

On the other hand, there are PKI certificates. The origin of such a certificate lies in a CA (Certificate Authority or Certification Authority). This CA is a trusted entity, a certification authority, which issues digital certificates. With the help of this root CA certificate, a derivation of certificates up to the product certificate can take place. By using such a certificate, not only the signature can be validated, but also the authentication can be checked.

Generate self-signed certificate

The creation of a self-signed certificate with Linux and OpenSSL is described here. There are many other possibilities, so the solution presented here should be understood as an example.

1. Generate a certificate with public key and a file for the private key:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -sha256 -days 365
Enter PEM pass phrase = <pass phrase>
Country: C = e.g. DE
State: ST = e.g. NDS
Locality: L = e.g. Hameln
Organisation: O = e.g. Development
OrgaUnit: OU = e.g. Department-Product-A
Common Name = e.g. Name-Of-Certificate
EMail Address = e.g. Product@Vendor.com
```

file 'cert.pem' includes the certificate with public key

file 'key.pem' includes the private key

2. Change format of certificate with public key:

```
openssl x509 -outform der -in cert.pem -out certificate.cer
```

3. Change format of certificate, including private key:

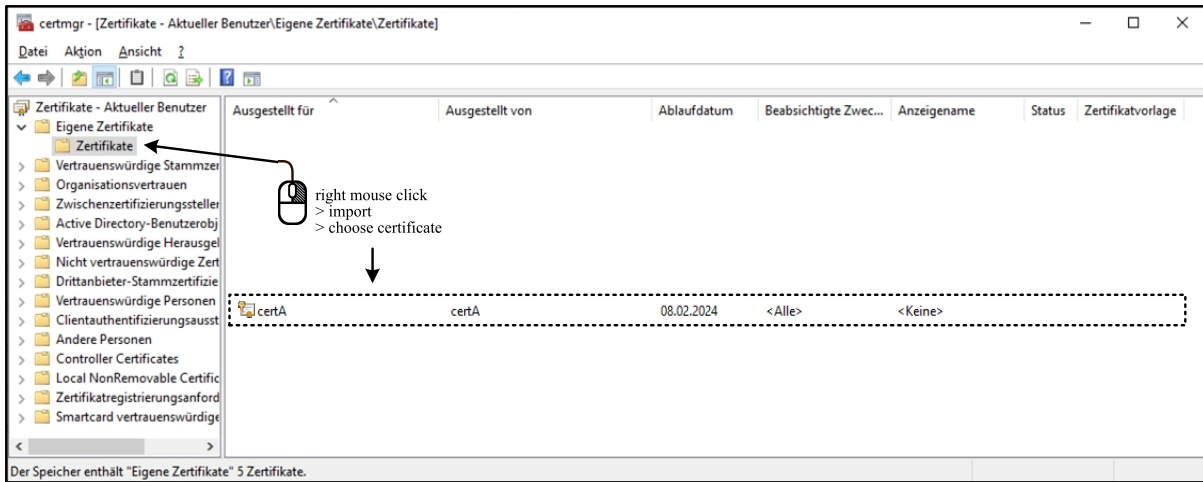
```
openssl pkcs12 -export -out certificate.pfx -inkey key.pem -in cert.pem
```

Basics of security

Certificate handling

Integrate a certificate in the Windows Certificate Store

With 'certmgr.msc' the certificate manager in Windows can be started.



Integrate a certificate in the windows certificate store

1. Open the Certificate Store using 'certmgr.msc'.
2. Open Your own certificate folder and right click on Import.
3. Choose a certificate.
4. The certificate will be integrated and viewed in the table on the right.

Core Automation Platform

The consideration of cyber security in industrial automation systems is based on IEC 62443. It is divided into parts and thus represents the entire supply chain. The classification is made in the following parts:

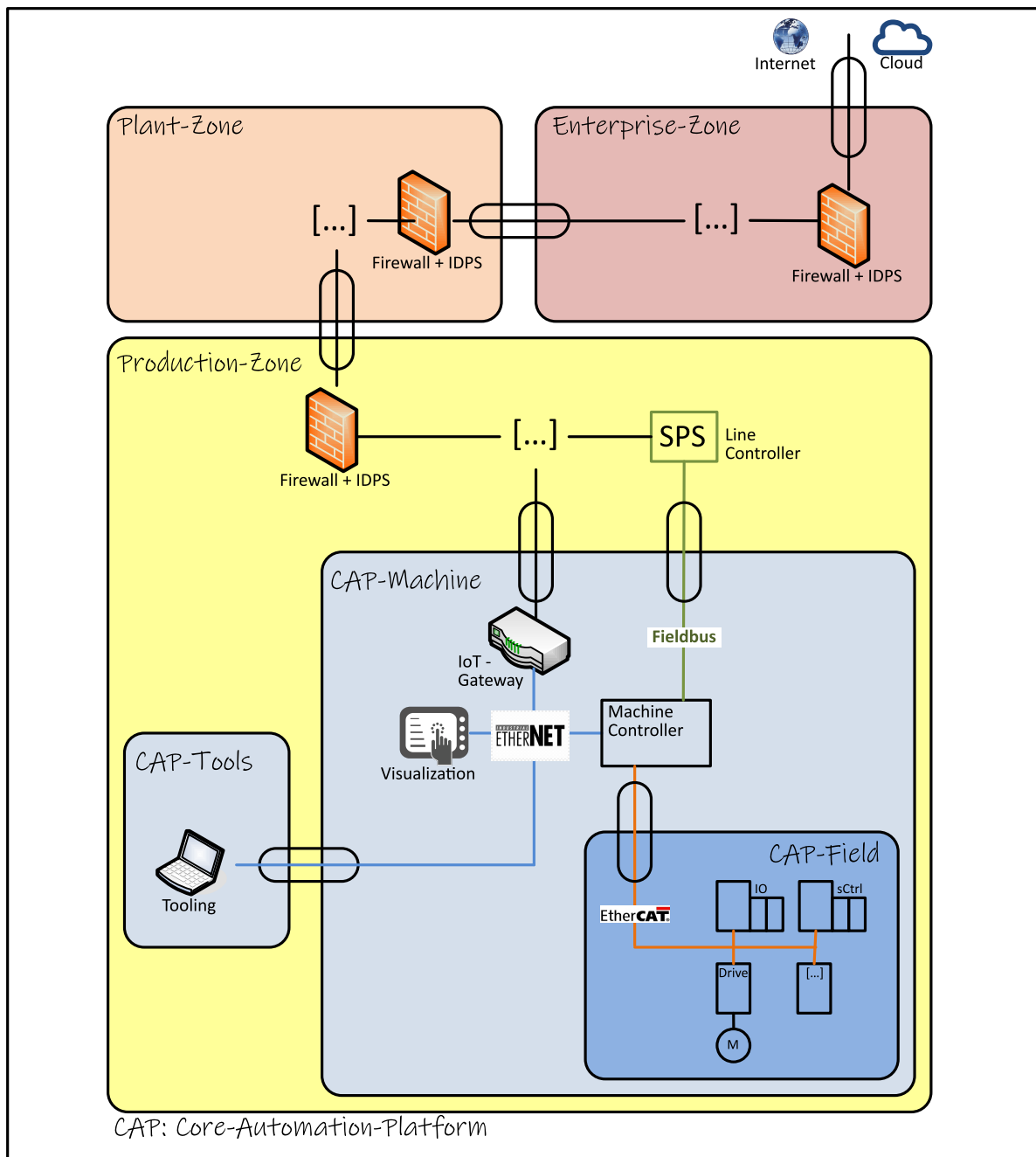
- IEC 62443-1-x: General definitions
- IEC 62443-2-x: Focus on the operator of a plant with high overlap with IEC 2700x
- IEC 62443-3-x: Focus on the system integrator or machine builder
- IEC 62443-4-x: Focus on the component supplier

Lenze acts as a component supplier in accordance with IEC 62443-4-x. In order to put the components in context, this chapter offers an overview at the system level. However, each system integrator or machine builder must adapt it to their own environment.system composition, which is their responsibility. Only a reference architecture is discussed in order to clarify relationships and specify the required system environment for the components.

The following image shows a zoning concept for this reference architecture.

Core Automation Platform

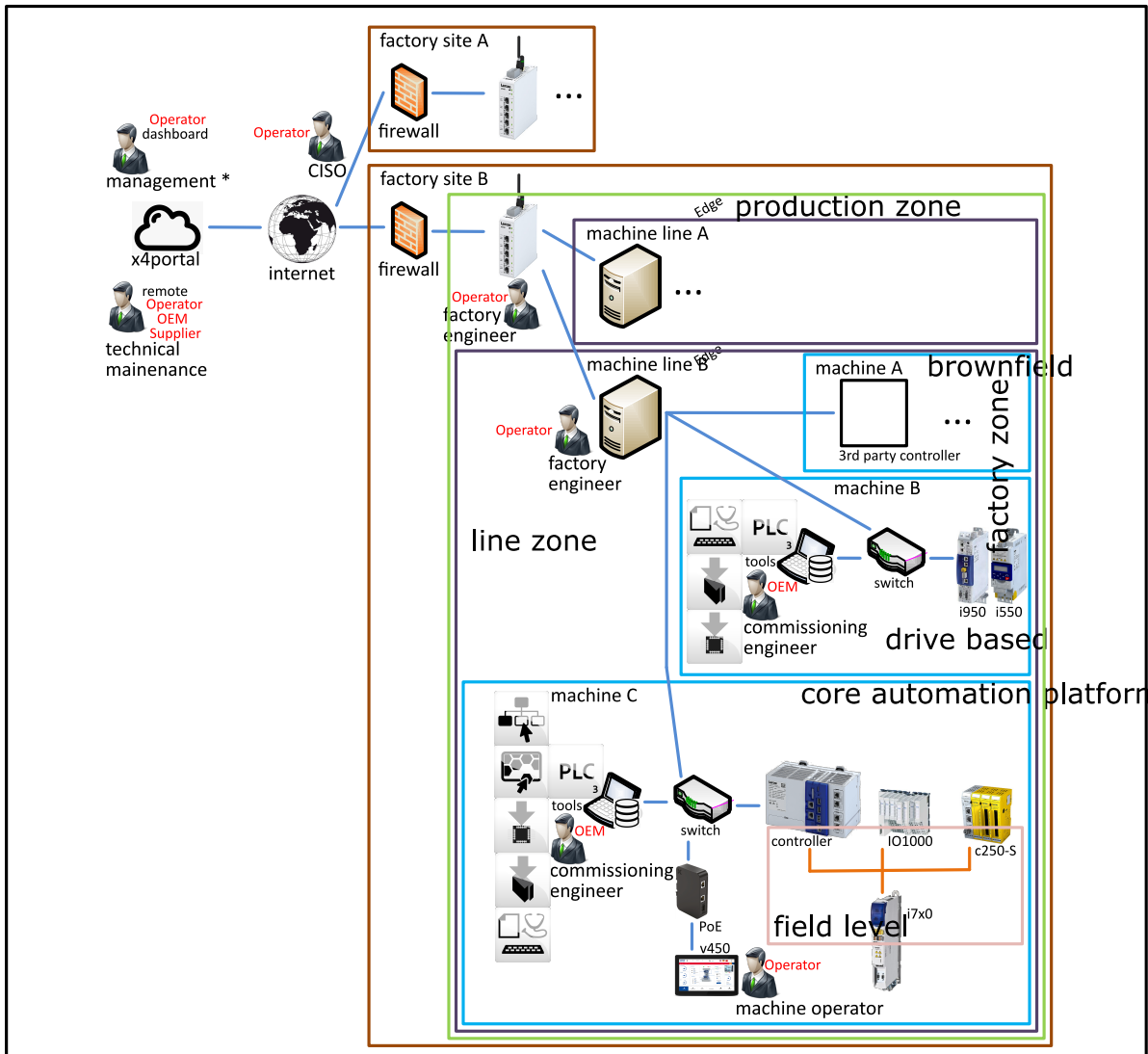
Certificate handling



Zones and Conduits

Overview

The following figure provides an overview of the components and the sorting into the respective security zones.



Overview of the components in the security zones

x5x0 IoT Gateway

The x5x0 components are configured through the X4 Portal and span a VPN tunnel between both. The component itself has no identification or authentication of human users.

Brownfield and drive based

This is not the focus of the documentation.

Core Automation Platform

Overview

»EASY System Designer«

This cloud service has its own user management that can identify and authenticate users and grant them the necessary permissions. These mechanisms are described in the corresponding chapter.

»PLC Designer«

The PLC Designer has its own user management and provides related functions. Projects can be stored and protected, and users and their passwords can be managed centrally in a password manager. These mechanisms are described in the corresponding chapter.

»EASY UI Designer«

The "EASY UI Designer" manages users and their passwords for operators who will work on the visualization later. These users can be managed via the EASY UI Designer, but they can also be changed on the v4x0 web panel later. A user administration system runs on the controller. The mechanisms for this are described in the relevant chapter.

Controller

The controller contains two user administrations. The first is the user management of the controller access, where users and their passwords are managed with the help of the "PLC Designer" and stored on the controller. Access to the controller is via this mechanism. Second, the user administration for the v450 operators is on the controller. Operators can be created initially via the "EASY UI Designer" and changed at runtime on the v4x0 web panel. Both mechanisms are described in the corresponding

chapters.

Both mechanisms are described in the corresponding chapters.

v4x0 web panel

The v4x0 web panel has its own user management for its own functionality. This is described in the corresponding chapter. Additionally, the v4x0 web panel displays user management for operators. However, this is only an ad and not the functionality itself. The actual function runs on the controller.

»Easy Starter«, »Firmware Loader« and »Application Loader«

These three auxiliary tools do not have their own user management but must identify and authenticate themselves on the controller before they can establish a connection.

Field-Level-Components

The components at this level do not have their own identification and authentication strategy for human users and must therefore be protected by organizational measures.

Zones and conduits

"Enterprise-Zone", "Plant-Zone" and "Production-Zone"

Depending on the operator, these zones are responsible for their own structuring and organization. These zones are listed here because states that the components mentioned here may not be operated directly on the open Internet, but require an additional level of protection according to the "Defense-in-Depth" concept. The operator is responsible for designing these protection levels.

"CAP-Machine" Zone

The abbreviation CAP Machine means "Core Automation Platform Machine". This zone contains components that are installed in the machine at runtime. This security zone must be protected by the operator of the automation system for authorized access. This refers to the authorization of data-technical access, but also to the authorization of human access on site. For example, the components must be protected against mechanical manipulation or removal of storage media. In addition, all these components have a communication interface with the machine's Ethernet. For this reason, these components are placed in a security zone and the same security level target requirements (SL-T) apply here. This zone has four conduits.

'IT/OT Gateway' conduit

This conduit connects the Security zone "CAP Machine" with the "Production Zone". This conduit is not generalizable and looks different in different installations, depending on the network configuration. This is typically where the transition from OT (operational technology) to IT (information technology) occurs. From a cyber security perspective, this transition needs to be considered particularly carefully. We recommend assessing risks based on the Golden Rules for Secure Systems (refer to chapter 'Cyber Security/Security strategy/Golden rules for secure systems'), e.g.:

- Minimize Attack Surface: Separate network segments and use NAT technologies
- Separate Systems: Not only separate the IT from the OT technology, but also separate machines from each other.

"Fieldbus" conduit

This conduit connects the security zone "CAP Machine" with the "Production Zone". When integrating the machine into production, a special focus must also be placed on this interface. This is necessary for two reasons.

Firstly, standardized fieldbus systems are used here, which in most cases have not implemented cyber security requirements. These must be classified as SL-0 and included accordingly in the risk assessment during system design.

Secondly, the standardized Ethernet TCP/UDP channel can be used in parallel with some proprietary fieldbus systems. This must be considered separately and taken into account in the cyber security risk assessment during system design.

"Tools" conduit

This conduit connects the security zone "CAP Machine" with the "CAP Tools". It only exists during the commissioning or maintenance of the machine. Here, the system design must be taken into account in the risk assessment to ensure that the accesses are authorized and the

Core Automation Platform

Zones and conduits

employees have been instructed on the components and the machine cyber security concept. Furthermore, it must be ensured that the computer systems on which the necessary tools are installed must comply with the current cybersecurity requirements and correspond to the current state of cybersecurity.

"Field" conduit

This conduit connects the security zone "CAP Machine" with the "CAP Field". The special feature here is the cyber security consideration of the field components. These components are connected via EtherCAT the communication medium and thus represent only a low level of protection in terms of cyber security. The operator must therefore ensure that no unauthorized access to the components can take place.

"CAP-Field" zone

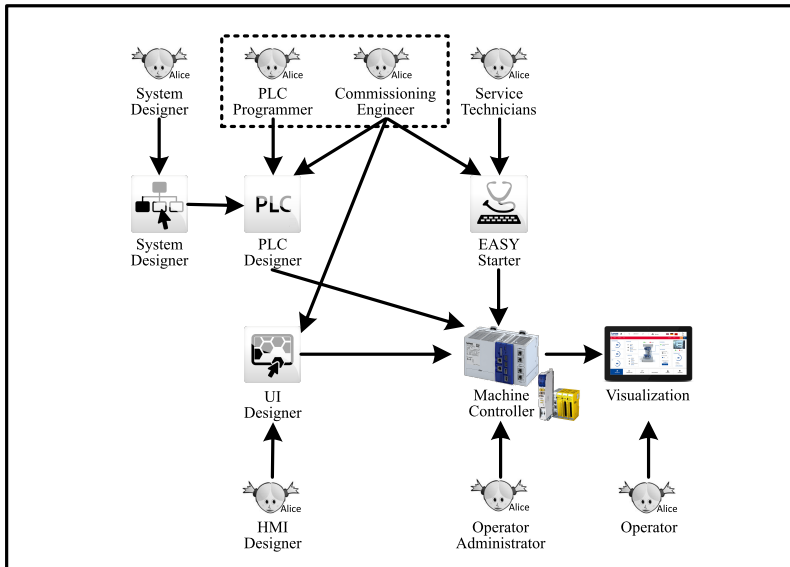
The abbreviation CAP-Field means "Core Automation Platform Field". These are connected via the EtherCAT communication medium and thus represent only a low level of protection in terms of cyber security. The operator must therefore ensure that no unauthorized access to the components can take place. This does not include any data technology or human access.

"CAP-Tools" zone

The abbreviation CAP-Tools means "Core Automation Platform Tools". The user installs the tools on a self-responsible computer hardware. The user is responsible for the correct use and cybersecurity of the computer and updating via patch management. The handling of the project data must also be taken into account and considered by the system integrator or operator in the cyber security risk assessment. Some mechanisms for this are described in the respective tool chapters, but they are only one possibility for cyber security functions.

Roles

The authorized roles are shown in the following picture and described accordingly.



Roles in the System

"System Designer" role

The system designer (role) uses the system designer (tool) to create the system configuration in a phase prior to commissioning. These results are transferred to the commissioning tools.

"PLC Programmer" role

The PLC programmer creates the application for the controller, i.e. the PLC program. In addition, he configures the network interfaces (e.g. the EtherCAT master) and parameterizes the controller and the subordinate devices. He is responsible for configuring groups, users and access rights for the machine and the PLC project.

"HMI Designer" role

The HMI Designer creates the projects for visualizing the machine. It also creates the basic settings for users, user groups and access rights for machine operators.

"Commissioning Engineer" role

The Commissioning Engineer sets up a machine with the PLC and visualization projects. Depending on the rights granted by the PLC programmer, he can also edit the controller application. In addition, he can import and parameterize the prepared visualization for machine programming.

"Service Technicians" role

The Service Technicians provide support for any problems that arise during commissioning or service life of a machine and carry out maintenance work if necessary.

Core Automation Platform

Roles

"Operator" role

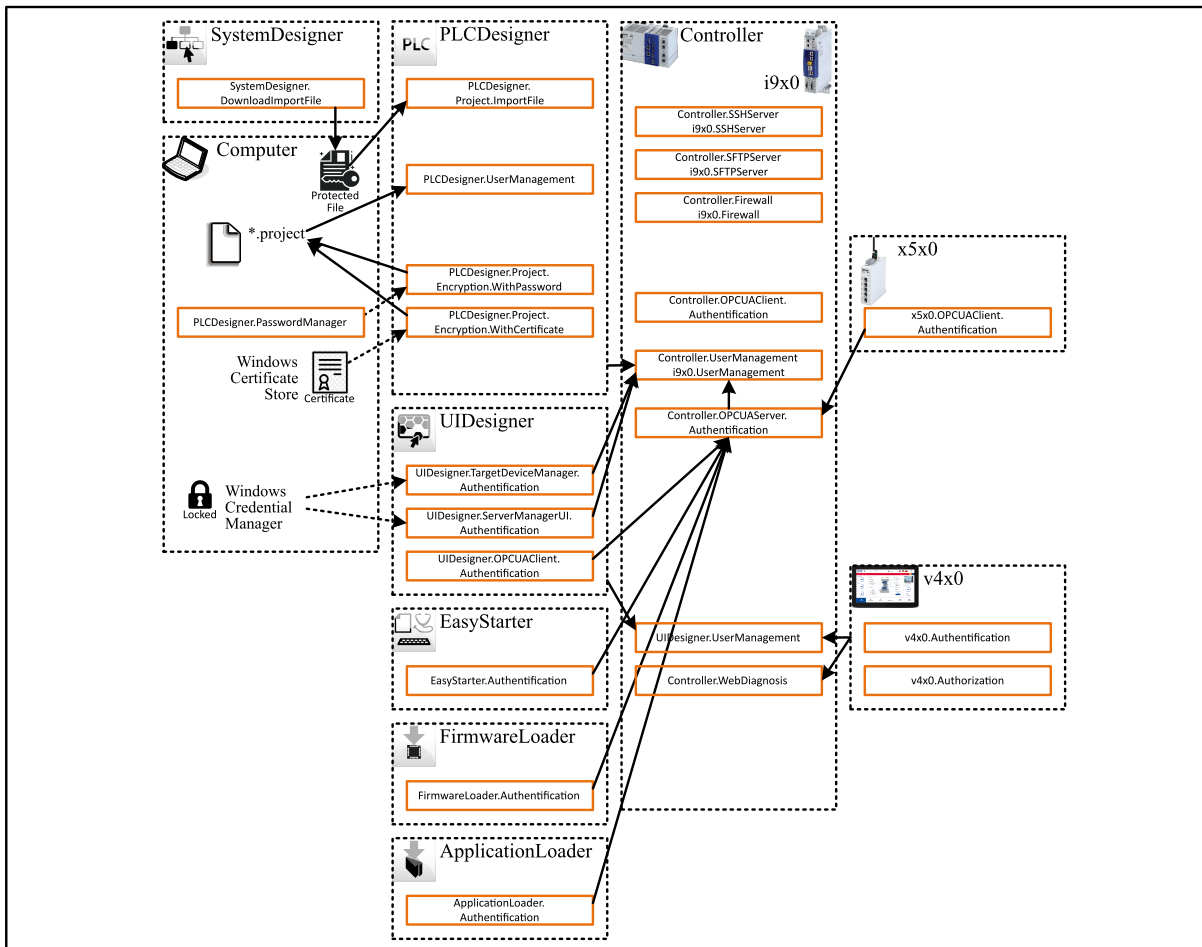
The Operator controls the machine at runtime, usually via an HMI with the configured visualization.

"Operator Administrator" role

The Operator Administrator sets up the device for different users or user groups and controls various device settings from the end customer or operator perspective.

Authentication, identification and authorization

The following image shows an overview of identification, authentication and authorization.



Identification, authentication and authorization

In the following section, the individual functions are grouped in order to be able to recognize the relationships. Furthermore, the goal of this functional unit is briefly described.

Identification and authentication for the transfer file between »EASY System Designer« and »PLC Designer«

- `SystemDesigner.DownloadImportFile`
- `PLCDesigner.ImportFile`

Set a user-defined password in the »EASY System Designer« and open it with the help of the user-defined password in the »PLC Designer« to protect the project during the transfer.

Integrity, identification and authentication for the PLC Project

- `PLCDesigner.Project.Encryption.WithPassword`
- `PLCDesigner.Project.Encryption.WithCertificate`
- `PLCDesigner.PasswordManager`

Core Automation Platform

Authentication, identification and authorization

Secure the PLC Project for unauthorized use with a Password or a Certificate. For ease of use, there is a Password Manager to store the passwords for encryption.

Identification, authentication and authorization within the PLC Project

- PLCDesigner.Project.UserManagement

Set up different users and authorizations within the PLC Project in the »PLC Designer«, to be able to work on a common project with different users and different permissions.

User management of the devices "Controller" and "i9x0"

- Controller.UserManagement
i9x0.UserManagement
- Controller.OPCUAServer.Authentication
- Controller.OPCUAClient.Authentication
- UIDesigner.OPCUAClient.Authentication
- UIDesigner.TargetDeviceManager.Authentication
- UIDesigner.ServerManagerUI.Authentication
- EasyStarter.Authentication
- FirmwareLoader.Authentication
- ApplicationLoader.Authentication
- x5x0.OPCUAClient.Authentication

This is the user management of the controller and i9x0. It is set via the settings in the »PLC Designer« and forms the basis for all identification and authorization mechanisms on the controller. All elements that authenticate to the controller and i9x0 use this mechanism, including the »EASY Starter«, the »EASY UI Designer« (only for the controller), the x5x0 IoT Gateway (only for the controller), the UA Expert (only for the controller), the »EASY Firmware Loader« and the »EASY Application Loader«.

User management for the visualization representations

- UIDesigner.UserManagement
- Controller.WebDiagnosis

The user management of the visualization display is set via the »EASY UI Designer«. Here users, their authentication and authorizations can be managed. These settings apply to visualization to process visualization and diagnostic visualization.

User management of the visualization component

- v4x0.Authentication
- v4x0.Authorization

The v4x0 web panel component has its own user management, which allows you to set rights for two users: admin and user. This regulates the different access authorizations for the different access paths.

Controller firewall

- Controller.Firewall
i9x0.Firewall

The controller and i9x0 firewall are used to minimize the attack surface and close all ports on different networks.

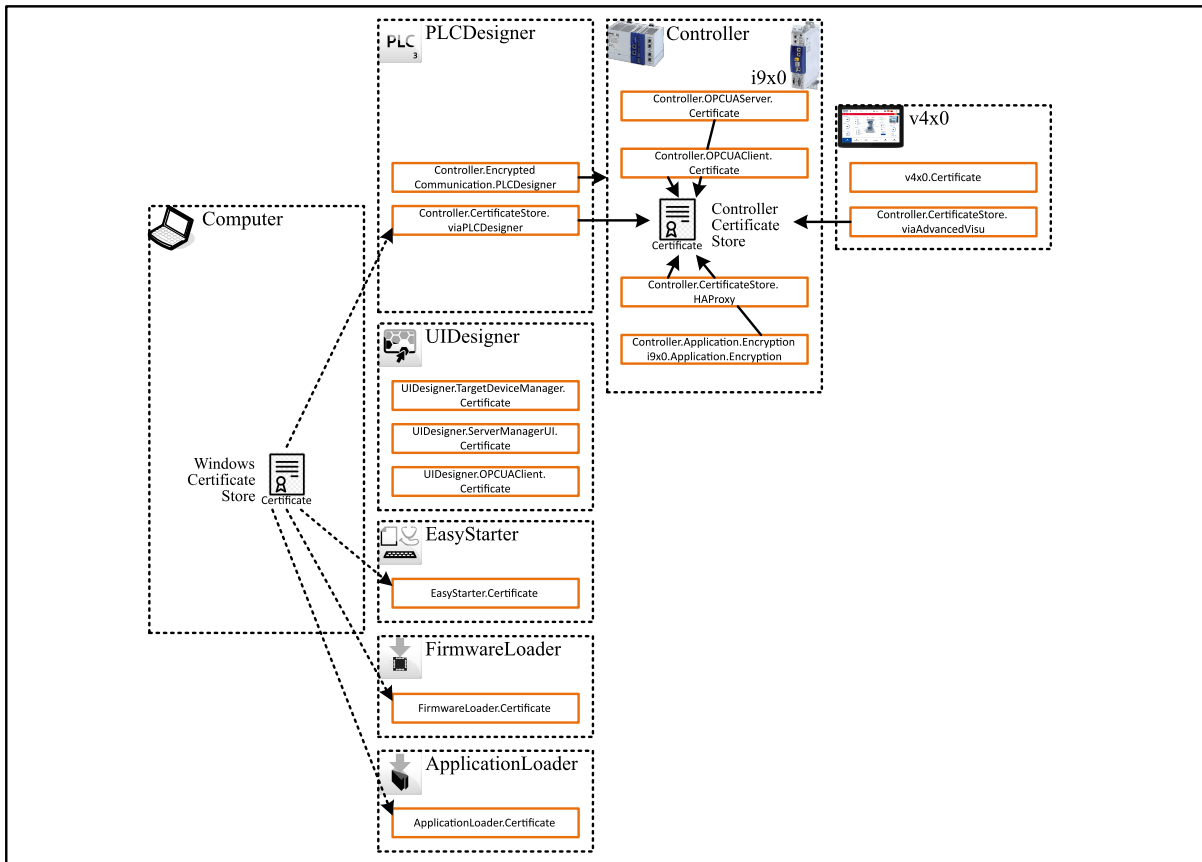
Service access to the controller

- Controller.SSHServer
i9x0.SSHServer
- Controller.SFTPServer
i9x0.SFTPServer

These two protocols are intended for experts or Lenze Service access only.

Certificate handling

The following image shows an overview of the certificate handling.



Certificate Handling

Controller Certificate Store

- Controller.CertificateStore.viaPLCDesigner
- i9x0.CertificateStore.viaPLCDesigner
- Controller.OPCUAServer.Certificate
- Controller.OPCUAClient.Certificate
- Controller.CertificateStore.HAProxy

The Controller and the i9x0 Certificate Store can manage all certificates for the device controller and the i9x0. These certificates can be managed via the PLC Designer.

Handling Controller Certificates via the Visualization

- v4x0.Certificate
- Controller.CertificateStore.viaAdvancedVisu

The user can handle the certificates via the Visualization with the functionality controller.CertificateStore.viaAdvancedVisu.

Encryption of Application

- Controller.Application.Encryption
i9x0.Application.Encryption

This functionality allows users to encrypt the application and manage the needed certificate in the Controller Certificate Store.

Core Automation Platform

Certificate handling

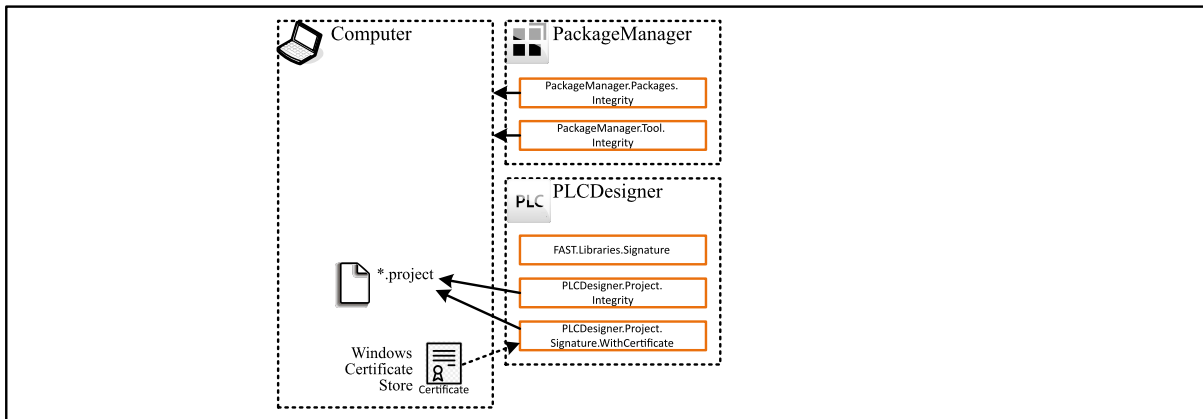
Encrypted Communication Controller

- Controller.EncryptedCommunication.PLCDesigner
i9x0.EncryptedCommunication.PLCDesigner
- UIDesigner.TargetDeviceManager.Certificate
- UIDesigner.ServerManagerUI.Certificate
- EasyStarter.Certificate
- FirmwareLoader.Certificate
- ApplicationLoader.Certificate
- UIDesigner.OPCUAClient.Certificate

There is an encrypted connection between the tools »PLC Designer«, »EASY Starter«, »Firmware Loader«, »Application Loader« and »EASY UI Designer« (only for the controller) and the device controller the transferred data from unauthorized use.

Integrity and Signing

The following image shows an overview of the integrity and signing.



Integrity and Signing

Integrity Values to check the authenticity

- PackageManager.Package.Integrity
- PackageManager.Tool.Integrity

Check the integrity values before installing packages or tools.

Signature for Libraries

- FAST.Libraries.Signature

Check the signature before integrating libraries into the project.

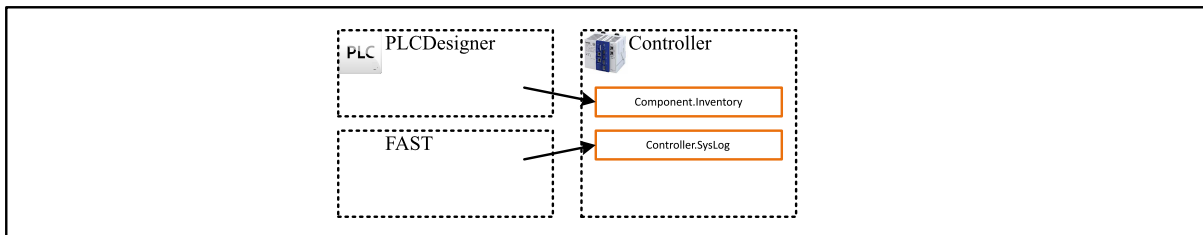
Integrity and Signature for PLC Projects

- PLCDesigner.Project.Integrity
- PLCDesigner.Project.Signature.WithCertificate

Protect the PLC project with integrity or signature.

Inventory and Events

The following image shows an overview of the Inventory and the Events.



Inventory and Events

Component Directory

- Controller.ComponentDirectory

Use the Component Directory to find the information needed for the operator's Security Board.

SysLog

- Controller.SysLog

Use Controller.SysLog to generate auditable events for the controller and send them to a central syslog server.

Conduit IT/OT Gateway

This chapter describes the general functionality of an IT/OT Gateway. This can be freely selected from several providers on the market. Here, the 'WALL IE' Industrial NAT Gateway and Firewall from Helmholz® is described as an example.

First, a basic commissioning must be carried out. This includes

- Set up the correct port configuration `/Device/Ports Config`.
- Choose a hostname `/Device/DNS Hostname`.
- Customize the certificate for HTTPS `/Device/HTTPS`.
- Generate a customer certificate (refer to chapter `Cyber Security/Basics of security/Certificate handling/Generate self-signed certificate`) and upload the certificate to the IT/OT Gateway.
- Limit the `/Device/Web Interface Access` to LAN only to minimize the attack surface.

Handling SysLog

This example describes how a system must be configured so that a controller can send SysLog messages to a SysLog Server in a higher-level network segment that is separated by an IT/OT gateway.

The screenshot displays the configuration interface of the Conduit IT/OT Gateway, showing a network topology and several configuration panels.

Network Topology: A diagram shows a central switch connected to four devices. The devices have the following IP addresses: 192.168.15.126 (top), 192.168.15.124 (middle-top), 192.168.10.125 (middle-bottom), and 192.168.10.100 (bottom).

Configuration Panels:

- 1 /Device/Ports Config:** Shows port configuration with X1P1 set to WAN and X1P2 set to LAN.
- 2 /Device/Operating Mode:** Shows the operating mode set to NAT.
- 3 /Network/Interface:** Shows interface configuration for the WAN interface. WAN IP is 192.168.15.124, WAN Netmask is 255.255.255.0, LAN IP is 192.168.10.125, LAN Netmask is 255.255.255.0, DNS Server is 0.0.0.0, and Default Gateway is 192.168.15.254.
- 4 /Device/Syslog remote Syslog:** Shows Syslog remote configuration. Remote syslog settings are updated successfully. The Syslog Host is 192.168.15.126 and the Syslog Port is 514.
- 5 /NAT/Basic NAT:** Shows Basic NAT configuration. SNAT: WAN to LAN Traffic: Active. The configuration is active.

Table:

#	External IP	Internal IP	Comment
0	192.168.15.100	192.168.10.100	c550

Handling SysLog

(1) Configuration of the Controller

- Set the network address of the controller to 192.168.10.100 with subnet 255.255.255.0 and gateway 192.168.10.125.
- Set the network address for the SysLog Server to 192.168.15.126 with the port tcp/5140.

(2) Port Configuration of the IT/OT Gateway

- Set Port 1 to WAN and Port 2 to LAN in the `/Device/Ports Config` menu.

(3) Activate NAT on the IT/OT Gateway

- Activate NAT in the `/Device/Operating Mode` menu.

(4) Setup the Network Interfaces on the IT/OT Gateway

- Set the network configuration for WAN and LAN in the `/Network/Interface` menu.

(5) Configuration of the Basic NAT on the IT/OT Gateway

- Activate and configure the Basic NAT via the `/NAT/Basic NAT` menu.
- Add a NAT rule for the internal (real) controller IP `192.168.10.100` to the external (virtual) IP `192.168.15.100`.

(6) Configuration of the SysLog remote functionality of the IT/OT Gateway

- Activate the IT/OT Gateway's own syslog logging to the SysLog Server address 192.168.15.126 on port 514.

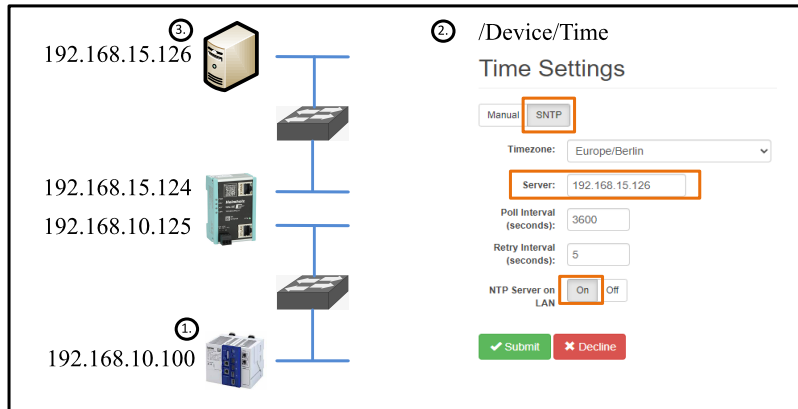
(7) Configuration of the SysLog Server

There are a lot of possibilities to set up a SysLog Server. In the following lines, a scheme is shown for an rsyslog SysLog server based on an Ubuntu Linux distribution.

- Install the rsyslog package.
- Configure the `/etc/rsyslog.conf` file
 - Activate the syslog reception via udp/514.
 - Activate the syslog reception via tcp/5140.
 - Setup the rules for facilities and severities and the log files
- Add template files in `/etc/rsyslog.d`
 - Generate a file for each device if you want to separate the log files
- Install logrotate.
- Configure `/etc/logrotate.conf`
 - Choose the rotate cycle and the creation process of the rotation files
- Configure `/etc/logrotate.d/rsyslog`
 - Add all logfiles for logrotate

Handling NTP

This example describes how a system must be configured so that a controller can use the NTP protocol for datetime synchronization to a NTP Server in a higher-level network segment that is separated by an IT/OT gateway.



Handling NTP

(1) Configuration of the Controller

- Set the parameter 0x245B:001 `System time: Time base` to NTP.
- Set the parameter 0x245A:002 `NTP server addresses: NTP server address 1` to 192.168.10.125. This is the southbound address on the IT/OT-Gateway for the LAN network.

(2) Setup the Device Time on the IT/OT-Gateway

- Activate the SNTP communication on the northbound WAN interface.
- Set the server ip address in this example to 192.168.15.126.
- Activate NTP Server on LAN

(3) Configuration of the NTP Server

There are a lot of possibilities to set up an NTP Server. In the following lines, a scheme is shown for an ntpsec server based on an Ubuntu Linux distribution.

- Disable the local time synchronization service systemd-timesyncd.service
- Remove (if existing) the ntp
- Install ntpsec
- Configure the NTPsec Client in the `/etc/ntpsec/ntp.conf` file.
Choose a nearby pool.
- Configure the NTPsec Server in the `/etc/ntpsec/ntp.conf` file.
Enable certificates for secure datetime transport.

x5x0 IoT Gateway

Product description

x5x0 IoT Gateway

The x5x0 IoT Gateway has the task of representing a data coupler between OT and IT.

Product description

Product identification

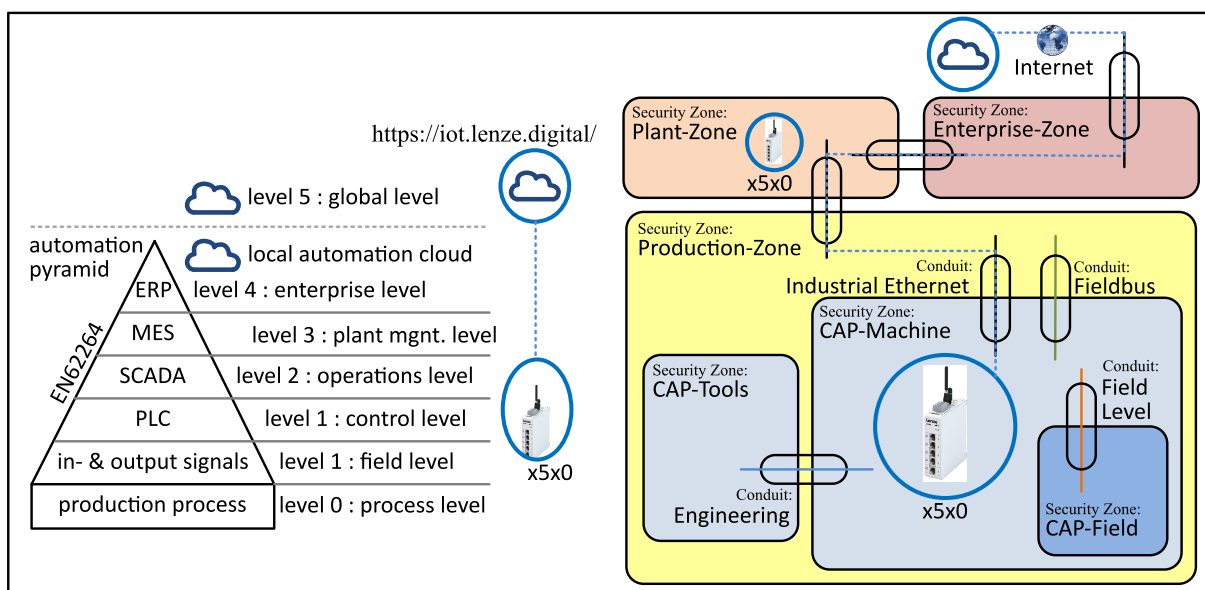
This documentation is applicable to the following components with their identification:

Name of product and product ID

Name of product	Infos	Product ID
x510	LAN	X51AE1001111N000S
x520	LAN+WiFi	X52AE1101111N000S
x530	LAN+4G	X53AE1001111N000S
x540	LAN+WiFi+4G	X54AE1101111N000S

Location in the network

These components are located in the automation pyramid at the control level or operations level. Furthermore, they are located in the security zone "CAP-Machine" ("CAP-Machine" [Zone](#) ([📖 55](#))) or in the Plant-Zone.



Product location in the network

The components addressed here have two relevant interfaces:

- **Conduit: Industrial Ethernet (northbound)**
A VPN tunnel is established to the X4 Remote between the x5x0 IoT Gateway (northbound), through the Production-Zone, Plant-Zone, Enterprise-Zone and the Internet.
- **Conduit: Industrial Ethernet (southbound)**
The x5x0 IoT Gateway (southbound) is connected to the machine's internal network within the security zone 'CAP-Machine'.

Intended purpose

The intended use of these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding cyber security are discussed.

- These components mentioned here are professional equipment and may only be commissioned and decommissioned by specialists.
- These components also require maintenance during their life cycle, which must be carried out by the operator.
- Modifications to the firmware or hardware of the component are not permitted.
- If these components are taken out of operation or disposed of, the instructions here in the documentation must be observed.

Intended environment

The intended environment for these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding cyber security are discussed.

- The products are operated on the machine's internal network. If these components are operated outside this network, the consideration of cyber security is the responsibility of the operator. A cyber security risk analysis is recommended here.
- The components are not operated directly on the open Internet, but must also be operated by the operator via protection systems such as firewall, IDS, and IPS
- In particular, the handling of the USB stick may only be carried out by users authorized by the operator.

Security key indicators

x5x0 IoT Gateway

Commissioning and hardening instructions

Security key indicator (in accordance with IEC 62443-4-2):

- These components are considered embedded devices (EDR).
- These components have a security level of SL-C 0.
- These components have an SL-vector from SL-C(x5x0)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

Commissioning and hardening instructions

General instructions

- General physical access protection must be provided for the components. This applies in particular to the USB port of the device. Installation in a control cabinet or panel housing that offers physical protection is recommended.
- Connecting external devices upstream to provide protection against DoS (Denial of Service) or DDoS (Distributed Denial of Service).

Commissioning and Hardening Instructions

The following commissioning instructions must be followed.

- The configuration data from the x5x0 IoT Gateway is transferred to the device via the USB Stick. This USB stick and the x5x0 IoT Gateway must be protected by the user by organizational measures against unauthorized removal, modification or change.

Periodic security maintenance

- It is recommended to check the password policy periodically for updates and to adjust the requirements if necessary.
- It is recommended to change the passwords cyclically.

Decommissioning instructions

- It is recommended to update the firmware and remove all relevant applications.

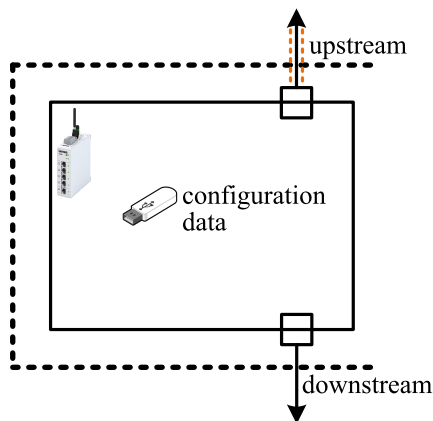
Product removal from environment

- It is recommended that all industrial communication partners of the x5x0 IoT Gateway be removed in order to change its trusted certificates into untrusted ones.
- It is recommended to securely remove the login data for the x5x0 IoT Gateway to be removed, such as name and password for the necessary authentication, from all industrial communication partners.

Security mechanisms

Defense in Depth product

The following image shows the Defense in Depth product concept. For the sake of clarity, some details have been deliberately omitted.

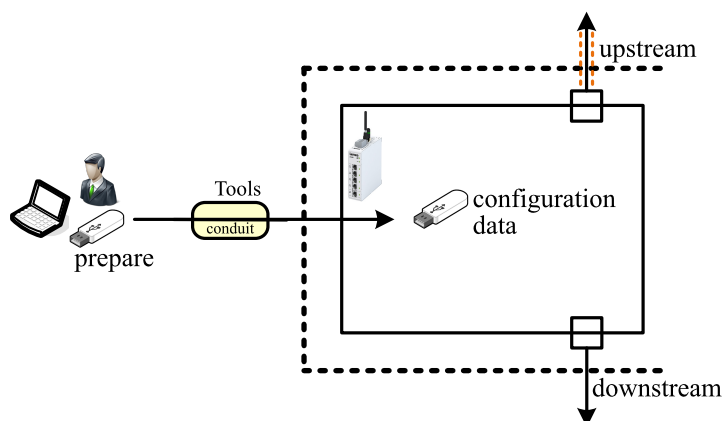


Product Defence in Depth

The x5x0 IoT Gateway concept is an initial configuration via a USB stick.

Expected Defense in Depth in the environment

The following image shows the expected defense in depth for the IoT gateway environment.



Expected Defence in Depth in the environment

Conduit Tools:

- Access from the engineering tools to the components must be limited in terms of organization and time.
- The corresponding engineering tools must be operated on an up-to-date and IT-security-secured computer.
- A special focus must be placed here on the physical access protection of the USB port or the USB stick.

x5x0 IoT Gateway

Security mechanisms

General Environment:

- General physical access protection must be provided for the components. This applies in particular to the USB port of the device where the USB stick can be used. Installing the x5x0 in a control cabinet or other housing that offers physical protection is recommended.
- Existing firmware updates for the x5x0 IoT Gateway, as well as for all other components in the network, should be installed immediately.

Security mechanisms

The following security functions are included in the listed service:

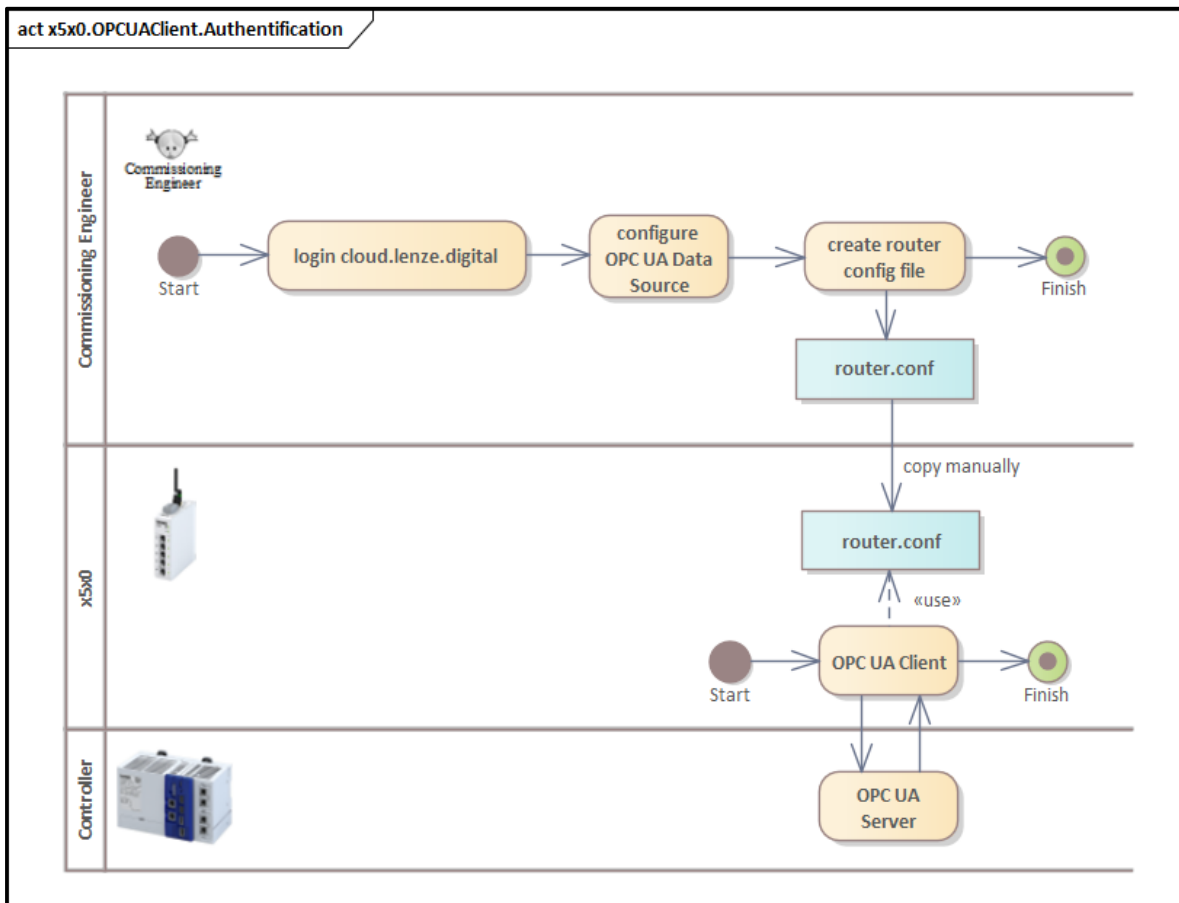
- x5x0.OPCUAClient.Authentication

Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

x5x0.OPCUAClient.Authentication

The x5x0 has an OPC UA client, which can be parameterized via a cloud configuration.



Activity Diagram

To connect the x5x0 to an OPC Server with activated user management, the following steps have to be carried out:

- Start the platform <https://lenze.digital/x4-remote/>
- Open the project
- Start the Fleet Manager
- Open the device via click on the name
- Click on "+" and add a data source "OPC UA"
- Type the OPC UA server data and select the authentication type = username and password
- Enter the username and password

Data source

OPC UA

Name *

Data source

Identifier *

data-source

IP address

192.168.5.99

Port *

4840

Authentication type *

Username and password

Username *

username

Password *

.....

Polling sleep time

100 milliseconds (recommended)

Cancel

Add

Data Sources

Drives DataHub

The Drives DataHub has the task of establishing a connection between legacy inverters and data protocols such as MQTT.

Product description

Product identification

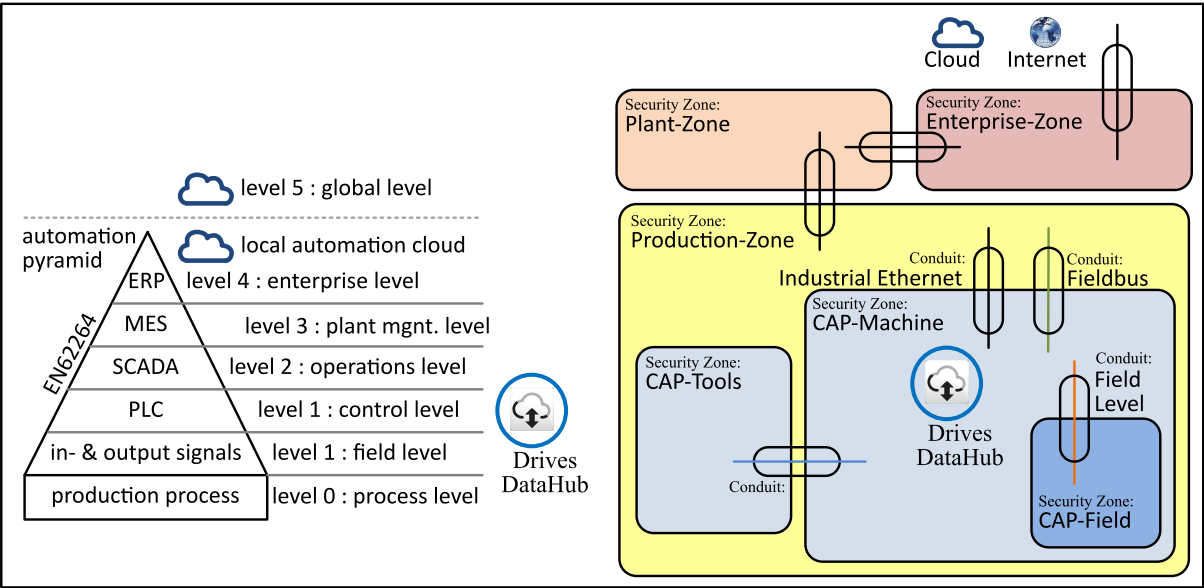
This documentation is applicable to the following components with their identification:

Name of product and product ID

Name of product	Product ID
Drives DataHub	n.a.

Location in the network

This component is located in the automation pyramid at the control level. Furthermore, they are located in the security zone "CAP-Machine" ([Zones and Conduits](#)).



Product location in the network

The software addressed here has three relevant interfaces:

- Conduit: Northbound MQTT

This connection is used to connect the Drives DataHub to the Production-Zone

- Conduit: Southbound GCI

This connection is used to connect the Drives DataHub to the Security Zone CAP-Field, where the inverters are typically positioned.

- Interface: User API

This interface is used for configuration of the Drives DataHub.

Drives DataHub

Product description

Intended purpose

The intended use of this component is described in the application as directed and can be found in the operating instructions in the online help. In the following, some specifics regarding cyber security are discussed.

- The Drives DataHub software must be installed on an up-to-date computer equipped with valid IT protection mechanisms.
- This computer is the responsibility of its owner and must be protected by valid IT protection systems such as firewall, IDS, IPS, etc.
- This component mentioned here is professional software and may only be commissioned and decommissioned by specialists.
- This software also require maintenance during their life cycle, which must be carried out by the operator.
- Modifications to the software are not permitted.
- If this software is taken out of operation or disposed of, the instructions here in the documentation must be considered.

The Drives DataHub is a modular software solution composed of multiple docker containers orchestrated via a docker compose configuration file. This architecture enables scalable deployment and flexible integration into existing infrastructure environments. Two primary roles are involved in the deployment of Drives DataHub.

Administrator:

- Responsible for installing and maintaining the Drives DataHub on a designated computer or server.
- Has access to the docker containers and the docker compose configuration file.
- Must ensure that no modifications are made to the docker compose configuration file that would expose the internal data network to public access. The internal data network must remain isolated and protected from external access. The administrator must actively prevent any exposure of the internal network during installation.
- Is required to perform a Cybersecurity Risk Assessment prior to deployment, particularly due to the nature of the Southbound network, which is classified as a GCI data network. This network is unencrypted and lacks access authorization mechanisms, posing potential security risks.
- Uses only the provided docker configuration file without alterations of the user management unless explicitly approved by the product vendor.



One change to the docker compose configuration file is permitted and necessary, the setting of the environment variable for the Keycloak.

KC_HOSTNAME_URL for Drives DataHub version 1.4.0, or

KC_HOSTNAME -> Drives DataHub version >= 1.5.0



Please read carefully the comments written to the hostname definition line within the provided compose file for the exact necessary format of the URL.

User:

- Interacts with the Drives DataHub via the User API.
- Can configure the system through authenticated access.

- Must undergo authentication before any configuration actions can be performed.

Intended environment

The intended environment for this software is described in the application as directed and can be found in the online help. In the following, some specifics regarding cyber security are discussed:

- The software must be installed on an up-to-date computer equipped with valid IT protection mechanisms.
- The software must be installed on a computer, which uses protection against unauthorized use.
- Use the appropriate authentication mechanisms for your computer. For example, use passwords that are complex and have an appropriate life cycle. Take the current state of the art into account.
- This computer is the responsibility of its owner and must be protected by valid IT protection systems such as firewall, IDS, IPS, etc.

Security key indicators

Security key indicator (in accordance with IEC 62443-4-2):

- This software is considered a software application (SAR).
- This component has a security level of SL-C 0.
- This component has an SL-vector from SL-C(DataHub)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

Security mechanisms

Security mechanisms:

The following security functions are included in the listed components:

- DataHub.UserAPI.Authentication
- DataHub.Northbound.MQTT.Authentication
- DataHub.Southbound.GCI

Commissioning and hardening notes and organizational measures

The following commissioning instructions must be followed:

General instructions

- Only install and operate on a current and security-maintained host. Dangers such as password loggers must be detected and minimized.
- Restrict physical access to the host to authorized persons.
- If the DataHub is running on a host that enables wireless interfaces, this is the customer's responsibility.
- The administrator of the host system on which the DataHub runs must organizationally protect the system time so that no manipulations can be carried out here.
- The administrator must organizationally protect the configuration files (e.g. for the LOS data or the certificates) on the host system on which the DataHub runs.
- The administrator must organizationally protect from public access all docker volumes being declared by the Drives DataHub's compose file.

Drives DataHub

Security functions

- When configuring the DataHub via an authorized Web Browser, you must first log off from the system and then close the browser session.
- The southbound communication from the DataHub (based on the GCI protocol) has no security protection. This means that data can be monitored and manipulated. This means the need for organizational protection by the operator.

Commissioning and hardening instructions

- Sign in to the Drives DataHub application and change the default admin password (refer to chapter '[Security Functions\DataHub.SignInAuthentication](#)')
- Configure the NorthboundMQTT-interface (refer to chapter '[Security Functions\DataHub.NorthboundMQTT](#)')
- Organizational measures are necessary to protect data on the SouthboundGCI Interface (refer to chapter '[Security Functions\DataHub.SouthboundGCI](#)')

Periodic security maintenance

- No periodic security maintenance (with the exception of installing security patches) is necessary.

Decommissioning instructions

- Secure removal from DataHub (includes: removal of stacks, containers, images, volumes, networks, password stores in volumes). For details see Drives DataHub User Guide, chapter 'Remove Drives DataHub containers'.

Product removal from environment

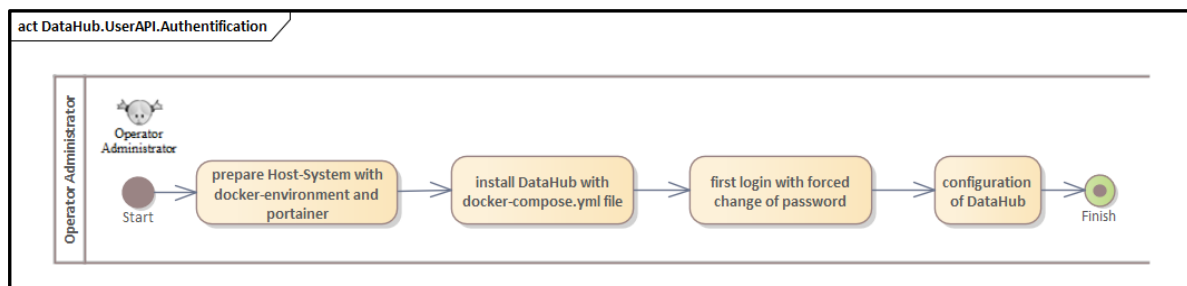
- No additional measure are necessary in the environment after product removal.

Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

DataHub.UserAPI.Authentication

The connection to the DataHub can be established via `https://<URL>:1443`.



Activity Diagram

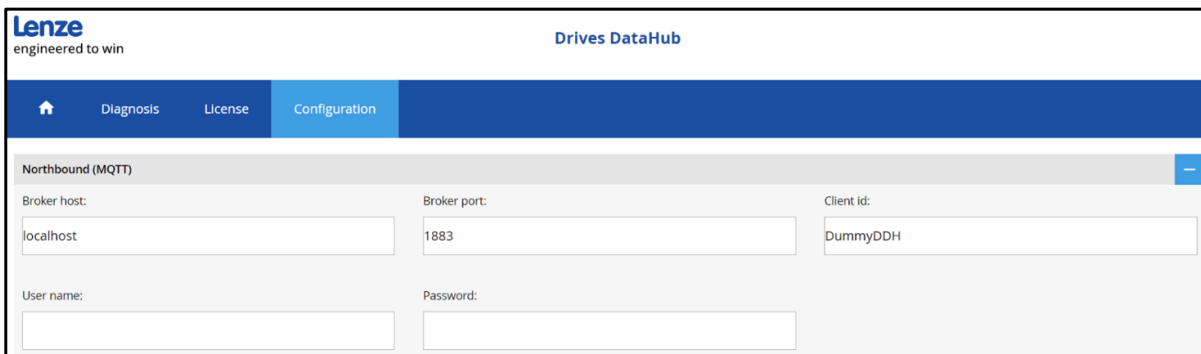
This is followed by a sign-in prompt, where you will log in for the first time. The following credentials are available for this purpose:

- Username: admin
- Default password: LenzeAdmin123

Users are forced to create a new password the first time they log in. (forced change).

DataHub.Northbound.MQTT

The Northbound MQTT connection is configured via the Configuration tab.



The screenshot shows the 'Configuration' tab in the 'Drives DataHub' interface. Under the 'Northbound (MQTT)' section, there are four input fields: 'Broker host' (containing 'localhost'), 'Broker port' (containing '1883'), 'Client id' (containing 'DummyDDH'), and 'User name' (empty). There is also a 'Password' field which is empty. The interface has a blue header with the 'Lenze' logo and 'engineered to win' tagline, and a navigation bar with 'Diagnosis', 'License', and 'Configuration' tabs.

Northbound MQTT configuration

The following configuration must be made:

- Broker host: Specifies the IP address of the MQTT broker
- Broker port: Specifies the MQTT port (typically 1883)
- Client ID: Specify the MQTT broker client ID
- Username: Username used to identify with the MQTT broker.
- Password: Password used to authenticate with the MQTT broker.

DataHub.Southbound.GCI

GCI is an unsecured, southbound protocol that transmits data as plain text. Precautions must be taken during installation to prevent data collection via a man-in-the-middle attack. However, this only applies to modifying and monitoring the data. The influence of southbound GCI on the DataHub component is excluded.

Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

DrivesDataHub.AccountManagementGuidelines

DrivesDataHub.AccountManagementGuidelines :: DrivesDataHub.UserManagement

Policies:

The password for signing in to the DataHub must meet the following requirements:

- At least 8 characters and maximal 128 characters
- Character set: A-Z, a-z, 0-9
- At least one uppercase character.
- At least one lowercase character.
- At least one numerical digit.
- The last 10 passwords must be different.

Drives DataHub

Security data

- The password must not be the same as username.
- The password must not be the same as the e-mail entered in the user account.

DrivesDataHub.Ports

Port List

Docker Name	Port	Portmapping	Protocol
datahub-ui	80/tcp	0.0.0.0:180->80/tcp :::180->80tcp	Hypertext Transfer Protocol (HTTP) Port 80 is open but for automatic redirection purpose only. On access, a redirection to the secured port 1443 takes place, which is the only publicly accessible listening port of the Drives DataHub.
	1443/tcp	0.0.0.0:1443->443/tcp :::1443->443/tcp	Secure Hypertext Transfer Protocol (HTTPS)
datahub-api-gateway	<internal>	<internal>	<internal>
datahub-user-management	<internal>	<internal>	<internal>
datahub-runtime	<internal>	<internal>	<internal>
ld2	<internal>	<internal>	<internal>
broker	<internal>	<internal>	<internal>
db	<internal>	<internal>	<internal>



Ports marked as <internal> are ports which are only accessible within the private local docker network with the docker containers are attached to. They cannot be accessed from the outside network.



The publicly exposed services (datahub-ui (with NGINX inside), datahub-api-gateway and datahub-user-management) are routed to by the inverse proxy NGINX. They are all accessible through the same base URL and its port 1443 only.

EASY System Designer

The EASY System Designer is the central design tool for automation systems and axis designs.

Description

System identification

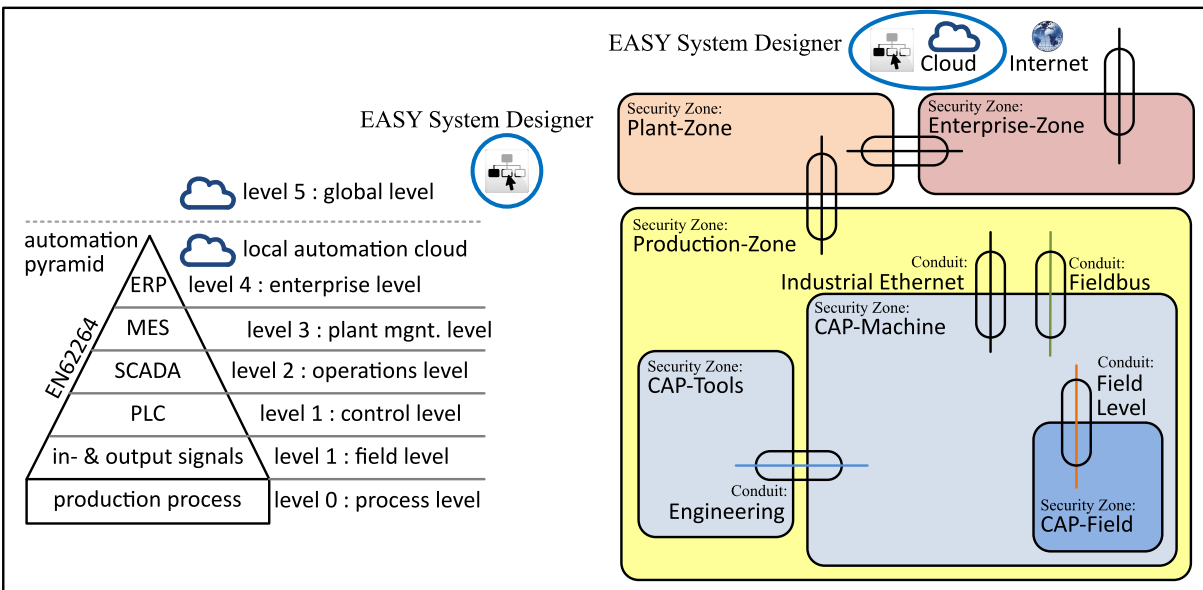
This documentation applies to the following system and its identification:

Name of system and ID:

Name of system	ID
»EASY System Designer«	https://systemdesigner.lenze.com/

Location in the network

This system is located in the automation pyramid at the "level 5 : global level". Furthermore, it is located in the Internet-Zone ([Zones and Conduits](#)).



Location in the network

This is not a component according to IEC 62443-4-x. In order to show correlations, »EASY System Designer« is included here.

Intended purpose

The intended use of this system is described in the application as directed and can be found in the online help of the EASY System Designer. In the following, some specifics regarding cyber security are discussed.

- Both main features of the EASY System Designer, the Drive Sizing and the Machine Design, are relevant for the preparatory phase of commissioning.
- These main features mentioned here are professional tools and may only be used by specialists.

Intended environment

The intended environment for this system is described in the application as directed and can be found in the online help of the EASY System Designer. In the following, some specifics regarding cyber security are discussed.

- Log in to the EASY System Designer only from a computer that meets the current security requirements and has the latest operating system update.
- Deactivate all unused compute interfaces and/or protocols.
- Wherever possible, use a Defense-in-Depth Concept in the environment of the computer.
- Use appropriate authentication mechanisms. This applies, for example, to passwords that have the necessary complexity and an appropriate life cycle. The current state of the art must be taken into account here.
- Handle secrets, such as passwords, appropriately. The focus here is on the handling of secrets stored in the environment of the EASY System Designer.
- Keep the installed firmware version of the computer up to date and install updates.

Security key indicators

Since the EASY System Designer is a service rather than a product, it is not classified according to IEC 62443-4-2, and no security level or security vector is specified.

Security mechanisms

Security mechanisms

- SystemDesigner.DownloadImportFile

Commissioning and hardening notes and organizational measures

The following commissioning instructions must be followed.

General Instructions

- All security-relevant notes on the operation of the »EASY System Designer« must be observed (not part of this documentation).

Commissioning and Hardening Instructions

- If you are downloading a project to use in the »PLC Designer«, use the user-defined password ([SystemDesigner.DownloadImportFile](#)), to protect the import file from unauthorized usage.
- If you are downloading a parameter set to use in the »EASY Starter«, the parameter set is downloaded in clear text and not encrypted. The reason for the plain text transmission is the simple handling which is valid, as there are typically no goods worthy of protection in the parameter set. The transmission takes place within an https channel and is therefore protected within the transmission.

Periodic Security Maintenance

- All security-relevant notes on the periodic security maintenance of the »EASY System Designer« must be observed (not part of this documentation).

Decommissioning Instructions

- All security-relevant notes on the decommissioning instructions of the »EASY System Designer« must be observed (not part of this documentation).

Product removal from Environment:

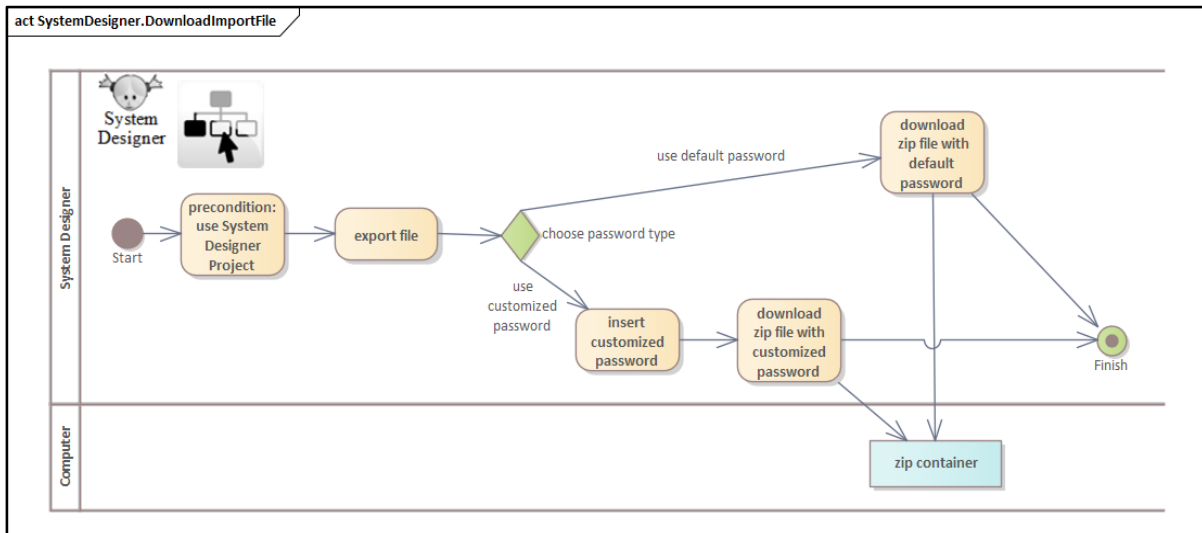
- All security-relevant notes on the product removal from environment of the »EASY System Designer« must be observed (not part of this documentation).

Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

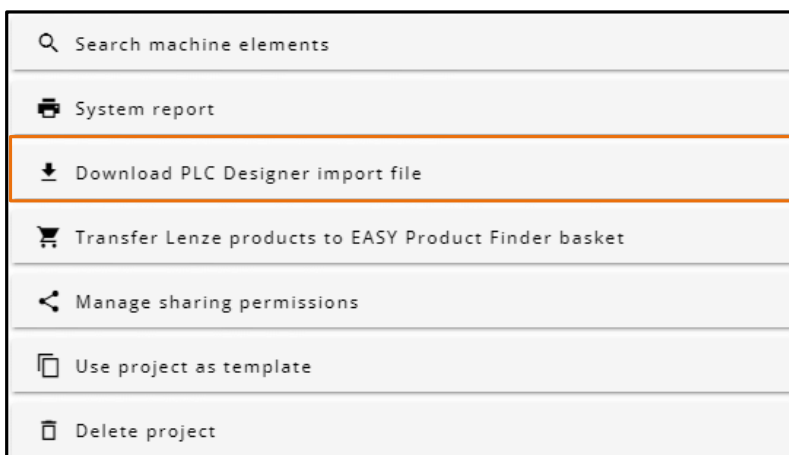
SystemDesigner.DownloadImportFile

An export function is available for transferring project data from the »EASY System Designer« to the »PLC Designer«. The corresponding procedure is shown in the following picture.



Activity Diagram

The »EASY System Designer« has a function that creates and downloads the PLC Designer import file. The following image shows the "Download »PLC Designer« import file" button:



Download »PLC Designer« import file

EASY System Designer

Security data

This is followed by a question as to whether to use the default password or a personalized password to protect the zip container.

The image shows two sequential screenshots of a dialog box titled "Password for PLC Designer import file".

The top screenshot shows the dialog with the following text: "By default the PLC Designer import file is protected by a standard password. Alternatively you can define your own password, which has to be entered in the PLC Designer before you can import this file." Below this text are two radio buttons: "Default password" (which is selected) and "User defined password". An orange box highlights the "User defined password" option, and a black arrow points from it to the bottom screenshot.

The bottom screenshot shows the dialog with the same text, but now "User defined password" is selected. Below the radio buttons are two text input fields: "Password" and "Confirm password". To the right of these fields, the following requirements are listed: "The password has to fulfill the following minimal requirements: - Minimum length of 8 characters - At least one lower (a..z) and one upper case (A..Z) character - At least one number (0..9)". At the bottom right of the dialog are "Cancel" and "Apply" buttons.

Default or user-defined password

Then, the zip container is encrypted and downloaded to the computer in the specified download directory of the used browser. The file extension is specified as *.plcExportFile. To import this file into the »PLC Designer« (refer to chapter [PLCDesigner.Project.ImportFile](#)).

Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

SystemDesigner.DownloadImportFile:UserPasswordRequirements

The requirements for the user-defined password are:

- Minimum length of 8 characters
- At least one lower (a...z) and one upper case (A...Z) character
- At least one number (0...9)
- Allowed characters: a..z, A..Z, 0..9 and ?=.*[!@#\$\$%^&*]

PLC Designer

The PLC Designer is the central programming tool.

Product description

Product identification

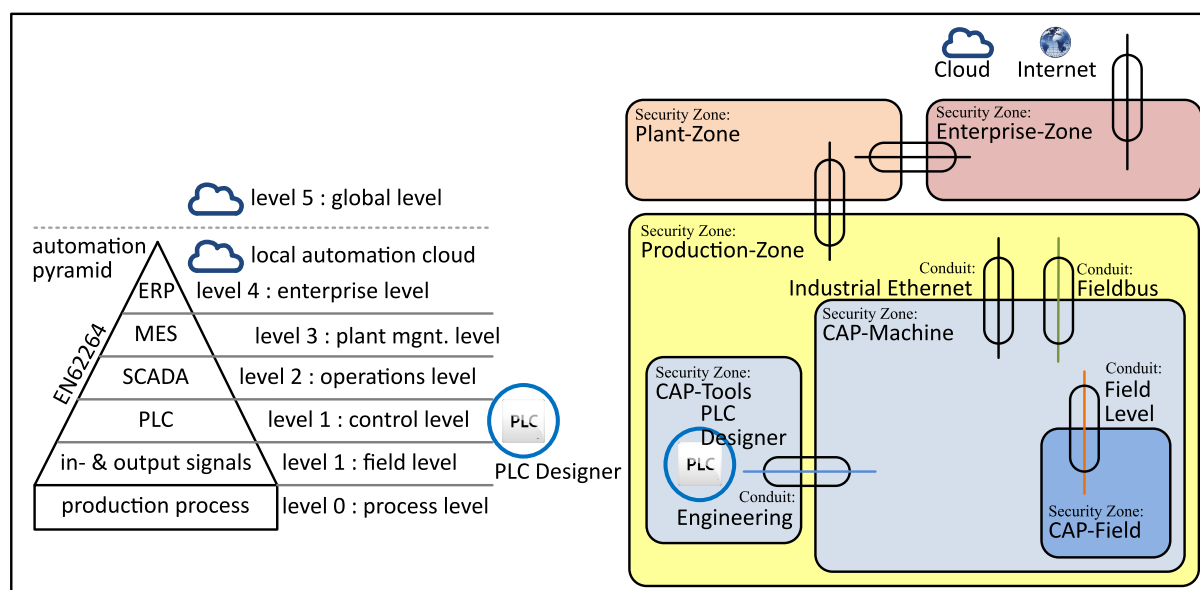
This documentation applies to the following component and its identification:

Name of product and product ID

Name of product	Product ID
PLC Designer 3.x	n.a.
PLC Designer 4.x	n.a.

Location in the network

This component is located in the automation pyramid at the control level. Furthermore it is located in the "CAP-Tools" security zone ([Zones and Conduits](#)).



Location in the Network

The software addressed here has only one relevant interface:

- **Conduit: Engineering**
This connection is used to connect the tool to the CAP-Machine security zone.

Intended purpose

The intended use of this component is described in the application as directed and can be found in the online help for the component. In the following, some specifics regarding cyber security are discussed.

- This software is professional grade and may only be commissioned and decommissioned by specialists.

PLC Designer

Product description

-
- This software also requires maintenance throughout its life cycle, which must be carried out by the operator.
 - Modifications to the software are not permitted.
 - If this software is taken out of operation or disposed of, the instructions here in the documentation must be observed.

Intended environment

The intended environment for this software is described in the application as directed and can be found in the online help for the component. In the following, some specifics regarding cyber security are discussed.

- The software must be installed on an up-to-date computer equipped with valid IT protection mechanisms.
- The software must be installed on a computer, which uses protection against unauthorized use.
- Use appropriate authentication mechanisms for the computer. This includes using passwords that have the necessary complexity and an appropriate life cycle. The current state of the art must be taken into account here.
- The owner of this computer is responsible for protecting it with valid IT protection systems, such as firewalls, IDS, and IPS.

Security key indicators

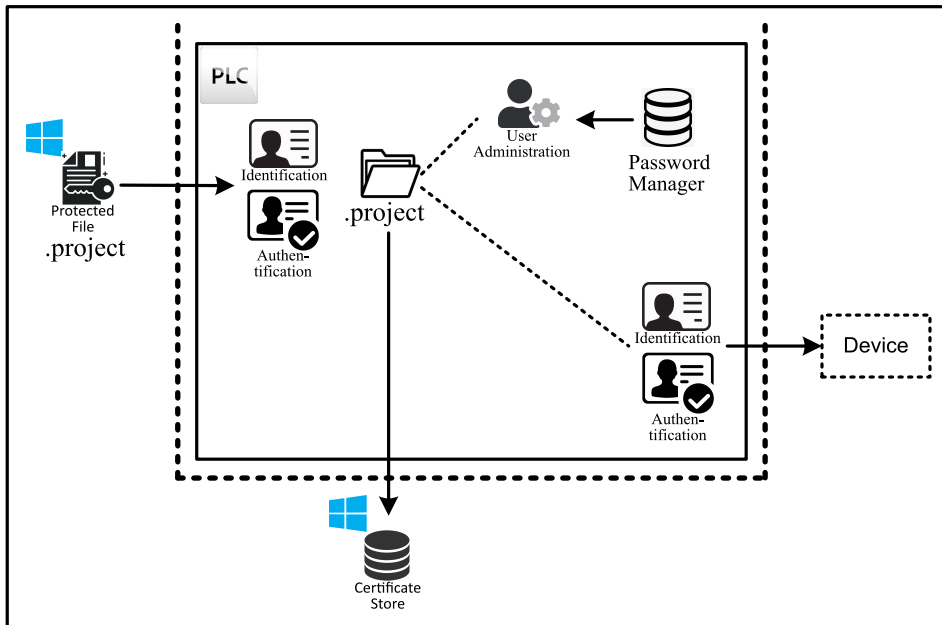
Security key indicator (in accordance with IEC 62443-4-2):

- This software is considered a software application (SAR).
- These components have a security level of SL-C 0.
- These components have an SL vector from SL-C(PLCDesigner)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

Security mechanisms

Product Defense in Depth

The following image shows the defense-in-depth product concept. For the sake of clarity, some details have been deliberately omitted.



Defense in Depth product

The core concept of the PLC Designer is as follows:

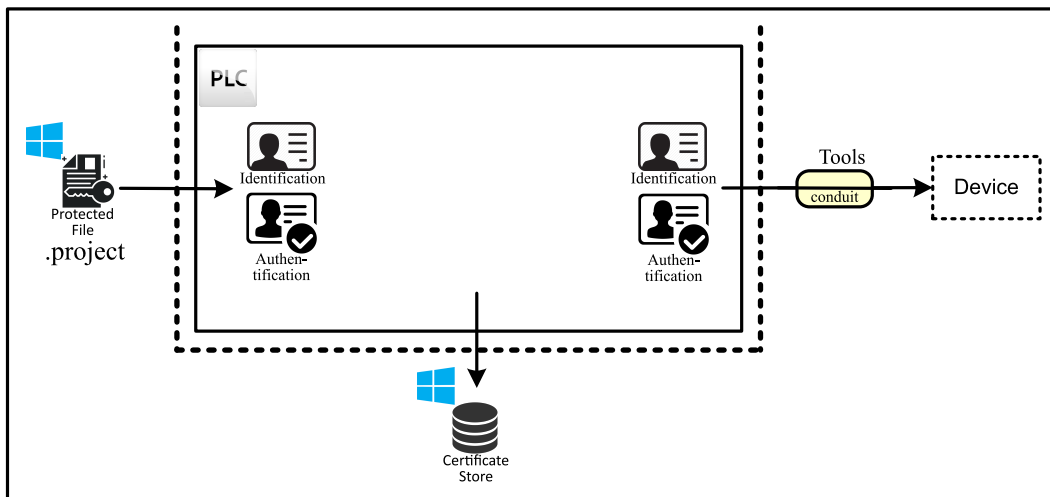
- protecting the project files (shown on the left in the picture),
- the project internal user management for collaborative work (indicated by the password manager symbol),
- the identification and authentication strategy to connect the devices (shown on the right in the picture), and
- the use of the Windows Certificate Store for the certificate handling procedure.

Expected Defense in Depth in the environment

The following image shows the expected defense in depth in the environment of the PLC Designer.

PLC Designer

Security mechanisms



Conduit Tools:

- Access from the PLC Designer to the devices must be limited in terms of organization and time.

General Environment:

- The PLC Designer must be operated on an up-to-date computer with IT security measures in place.
- General physical access protection must be provided for the devices , as well as accessibility from the PLC Designer.
- All updates for the PLC Designer, the computer, and all other network components should be installed immediately.

Security mechanisms

- `PLCDesigner.Project.ImportFile`
- `PLCDesigner.Project.UserManagment`
- `PLCDesigner.PasswordManager`
- `PLCDesigner.Project.Integrity`
- `PLCDesigner.Project.Encryption.WithPassword`
- `PLCDesigner.Project.Encryption.WithCertificate`
- `PLCDesigner.Project.Signature.WithCertificate`

Commissioning, hardening and decommissioning notes and organizational measures

The following commissioning instructions must be followed:

General Instructions:

- Installation and operation are permitted only on current and security-maintained computers. Please refer to chapter 'Security Data/PLCDesigner Installation' for more information.
- Restrict physical and logical access to authorized persons only.
- Change existing default passwords after the initial start-up and also regularly afterwards. Please use only high-strength passwords.
- The PLC Designer is installed on a Windows host. Please ensure that the Windows session lock is activated after a period of inactivity and by manual execution.

Commissioning and Hardening Instructions:

- Use the PLCDesigner.ImportFile to import project data from the »EASY System Designer« ([PLCDesigner.Project.ImportFile](#))
- Use the user management for the »PLC Designer« Project ([PLCDesigner.Project.UserManagement](#)).
- Optional the password manager can be used ([PLCDesigner PasswordManager](#)).
- Activate the »PLC Designer« Project-Encryption with password ([PLCDesigner.Project.Encryption.WithPassword](#)) to protect the secure project from unauthorized access. This is particularly recommended if secrets (such as password) are stored in the PLC project.
- Activate the »PLC Designer« project encryption with certificate ([PLCDesigner.Project.Encryption.WithCertificate](#)) to protect the secure project from unauthorized access. This is particularly recommended if secrets (such as password) are stored in the PLC project.
- Activate the »PLC Designer« project signature ([PLCDesigner.Project.Signature.WithCertificate](#)) to sign the project.

Periodic Security Maintenance:

- It is recommended to check the password policy periodically for updates and to adjust the requirements if necessary.
- It is recommended to change the passwords cyclically.
- It is recommended to check the certificates used with regard to their key lengths for up-to-dateness and to generate new certificates with higher key lengths if necessary.
- It is recommended to exchange the certificates regularly.

Decommissioning Instructions:

- After uninstalling the »PLC Designer«, please remove the data from the PLC Designer.PasswordManager manually ([PLCDesigner PasswordManager](#)).
- After uninstalling the »PLC Designer«, please remove the certificates from the devices manually from the Windows Certificate Store ([Controller EncryptedCommunication](#)).

Remove Product from Environment:

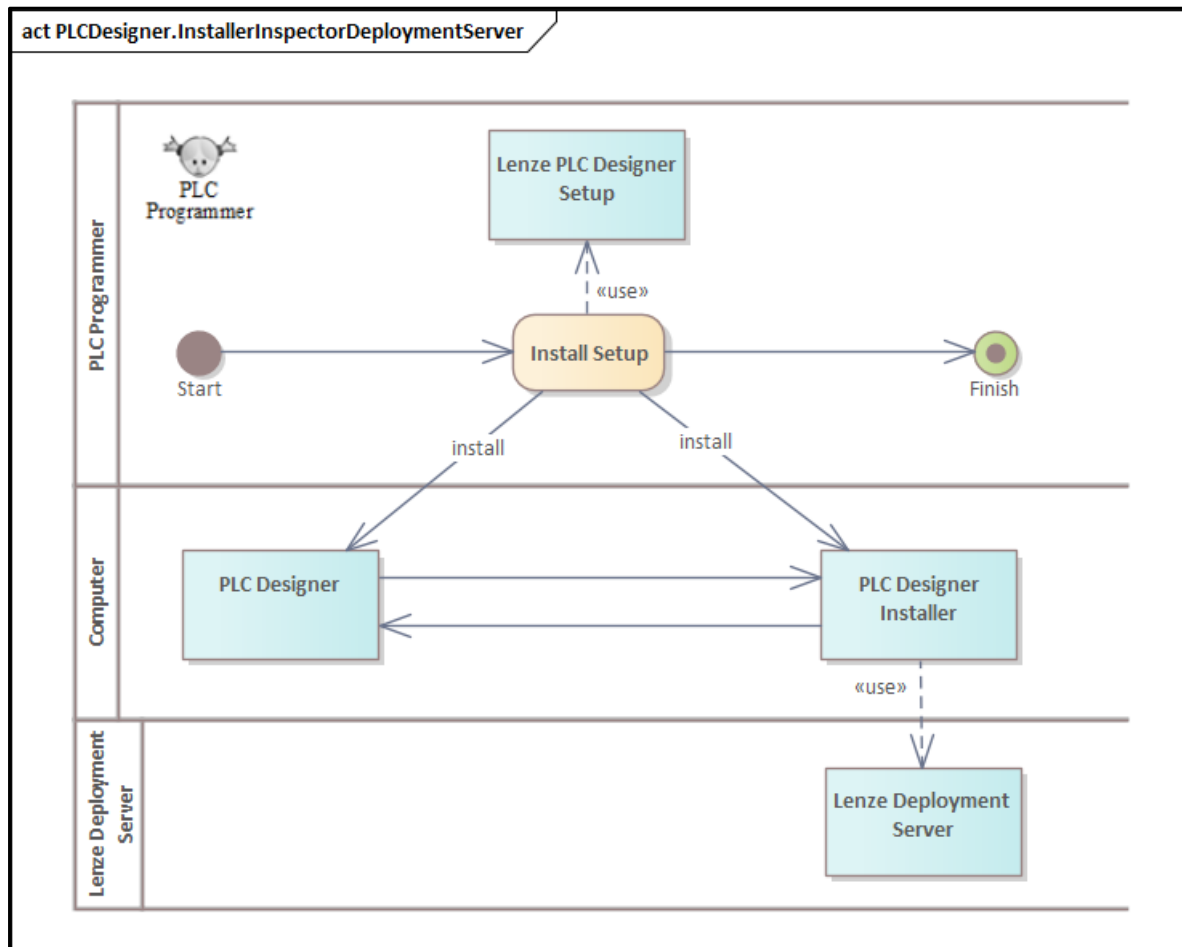
- n.a.

Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

PLCDesigner.InstallerInspectorDeploymentServer

From version v4.1.0, the PLC Designer Setup not only installs the PLC Designer, but also the PLC Designer Installer.



Activity Diagram

In this interaction, PLC Designer and PLC Designer Installer work together as follows:

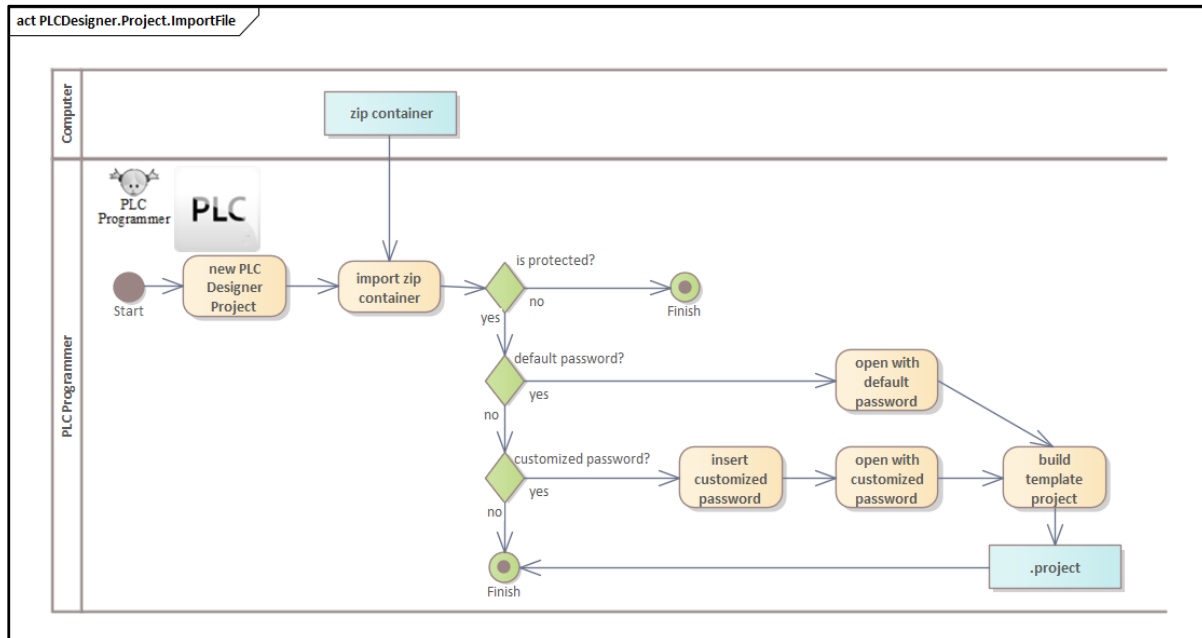
- When PLC Designer opens a project, an inspector is used to scan the project and, if optional software components are missing, PLC Designer Installer is instructed to install them.
- The PLC Designer Installer accesses the Deployment Server and searches for the necessary software components.



- To ensure that the setup and the installer can work without problems, the following accesses from chapter [PLCDesigner.Installation](#).

PLCDesigner.Project.ImportFile

An import function is available for transferring project data from the EASY System Designer to the »PLC Designer«. The corresponding procedure is shown in the following picture.



Activity Diagram

After downloading the import file from the »EASY System Designer« ([SystemDesigner.DownloadImportFile](#)), it can be integrated into the PLC project. When the »PLC Designer« is started, an ESD container can be selected via the call "PLC DesignerWnew projectWimport ESD container", as shown in the next figure.

PLC Designer

Security functions

PLC

Standard Project

×

Select a controllerImport ESD container



Please select an ESD container and adjust the settings for version, programming language and project template below.

Select ESD container

Information:
Name:
Owner:
Date:
Link to ESD:

Information:
Name:
Vendor:
Version:
Runtime software:
Description:

Controller Firmware Version

Compiler-Version: V3.5.17.40 (PLC Designer: V3.26.x.x)

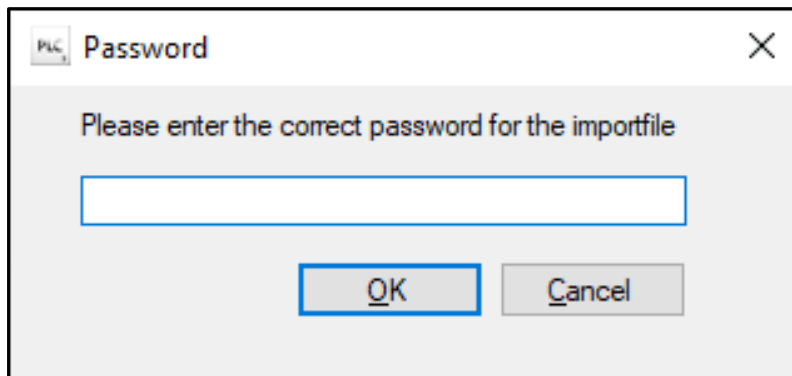
Language main program: Structured Text (ST)

Project template: Standard project

OKCancel

Import ESD container

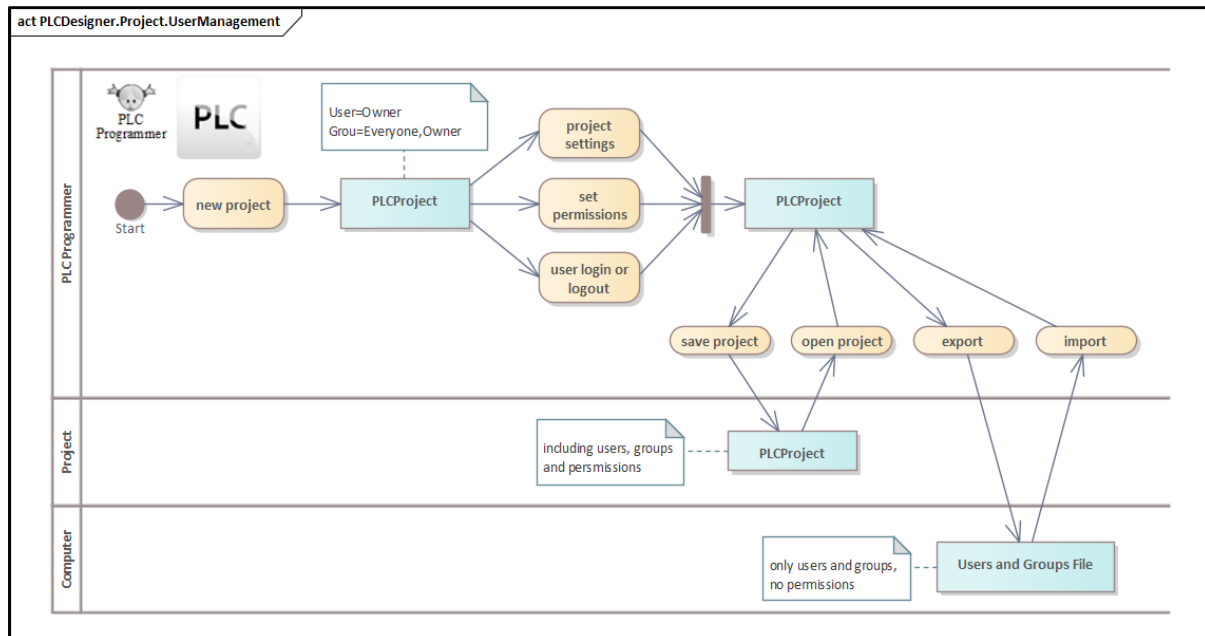
If the zip container is protected with the default password, it is imported. If it is protected via user-defined password, a dialog opens to enter this password.



Enter Password Dialog

PLCDesigner.Project.UserManagement

This chapter describes the functionality of a user management for the »PLC Designer« project. This means that all the properties described here do not apply to the »PLC Designer« as a program, but to the active open project. Using this function, the user can protect individual objects with read/write permissions. An overview is shown in the following image.



Activity Diagram

The following is a brief description of the respective actions. For more details, refer to the documentation of the »PLC Designer«.

New project

If a new project is created, a user "Owner" is created by default. This user is a member of the groups "Everyone" and "Owner". "Nobody" is displayed as project user, because no login has taken place yet.

Project settings

The project settings can be found under "Project/Project Settings/Users and Groups" in the »PLC Designer«. In order to be able to make changes here, first log in to the default user "Owner" with the default password <empty>. After that, additional users and groups can be created. Under Settings, the maximum number of login attempts and the time for an automatic logout in case of inactivity can be set.

If a user enters an incorrect password more times than the maximum number of attempts allowed, he will be blocked and can no longer log in with the correct password. Under "Project/Project Settings/Users and Groups" the user is displayed with a red cross. To activate the user again, set the "Active" property again via "Edit". Only users in the "Owner" group can do this.

Set permissions

Permission Management can be found under "Project/User Management/Permission". Here, the permissions can be set for individual properties for the "Commands", "Object types", "Project objects" and "Users, groups and permissions". Here, the permission "+ ... granted" and "- ... denied" can be set. For clarity, the default setting is displayed in gray, while changed properties are displayed in red or green.

User login and logout

The user login and the user logout can be found at "Project/User Management/User Login and Logout". The respective logged-in user is displayed in the »PLC Designer« at the bottom of the status bar.

Save and load project

Users, groups, and permissions are stored in the »PLC Designer« project.

Export and import

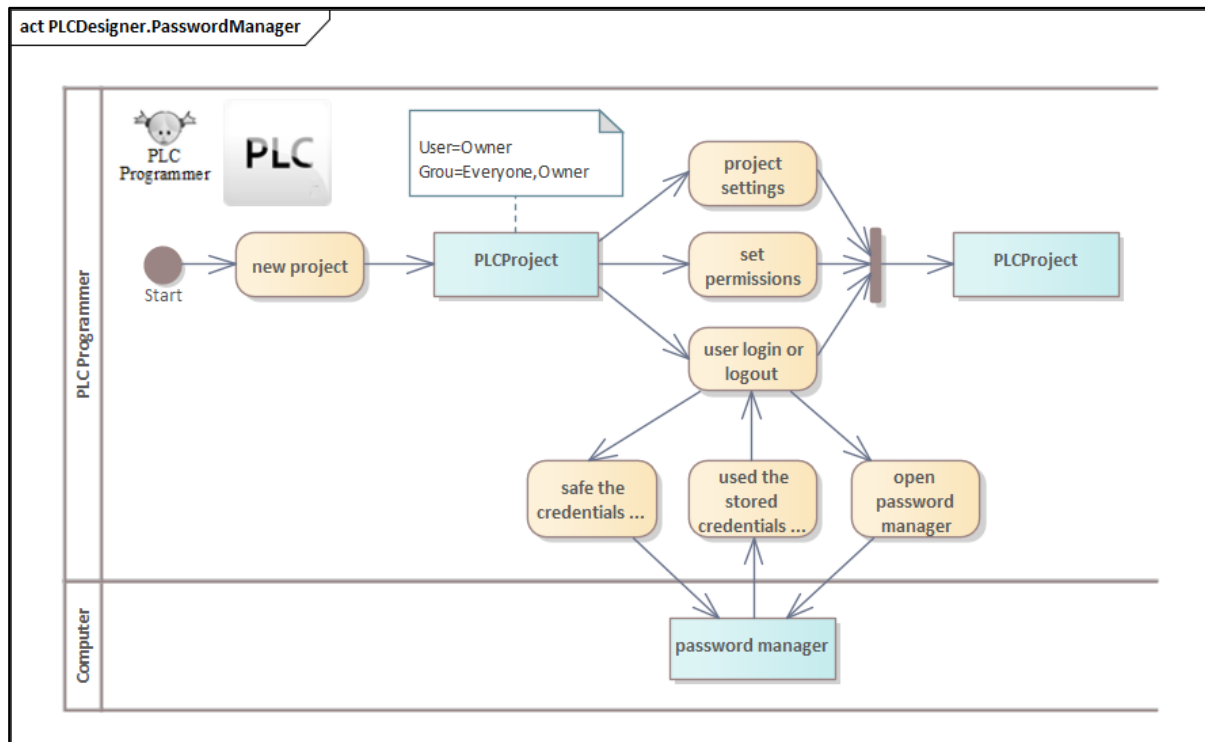
Via export and import, users, groups, and their relationships can be exported or imported into a file (*.user). The respective permission settings are not included here.



If users and groups are to be transferred from one PLC project to another, you can also use the CODESYS export/import feature (to be found in the »PLC Designer« menu under Project). When exporting, select the second POU tab and activate the project settings. A file with the extension *.export will be created. This file can then be integrated to the second project.

PLCDesigner.PasswordManager

This chapter describes the functionality of the Password Manager for the »PLC Designer«. This means that all the properties described here apply to the »PLC Designer« as a program and not to the active open project. An overview is shown in the following figure.



Activity Diagram

The following is a brief description of the respective actions. For more details, refer to the documentation of the »PLC Designer«.

Safe the Credentials locally on this Computer

When using it for the first time, the master password must be defined, which is stored and managed locally on the computer. Then the current user and his password can be stored via the function 'Safe the credentials locally on this computer'.



With the help of the master password, all contained passwords can be read out if the username is known.

Use the Stored Credentials for <user>

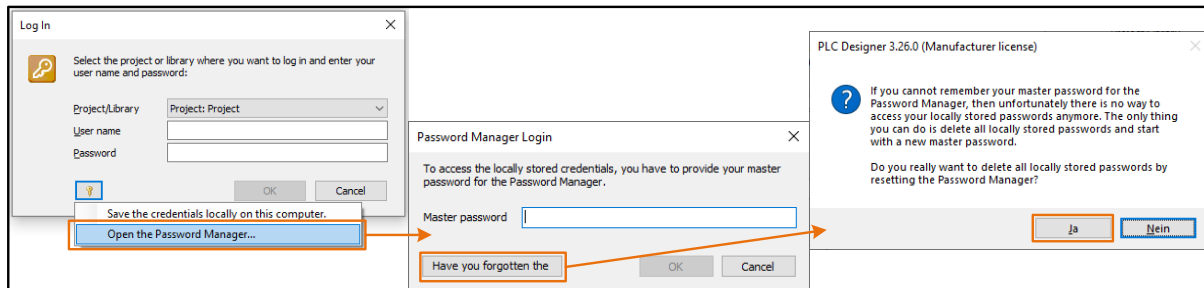
This function can be used to load passwords stored in the password manager.

Open the Password Manager

With this function, the password manager can be started. All locally stored users are displayed and can be removed from the password manager. Furthermore, the master password can be changed.

Forgot the Master Password

The Password Manager is secured with a master password, which is assigned by the user. If this master password has been forgotten, the entire password manager must be reset.

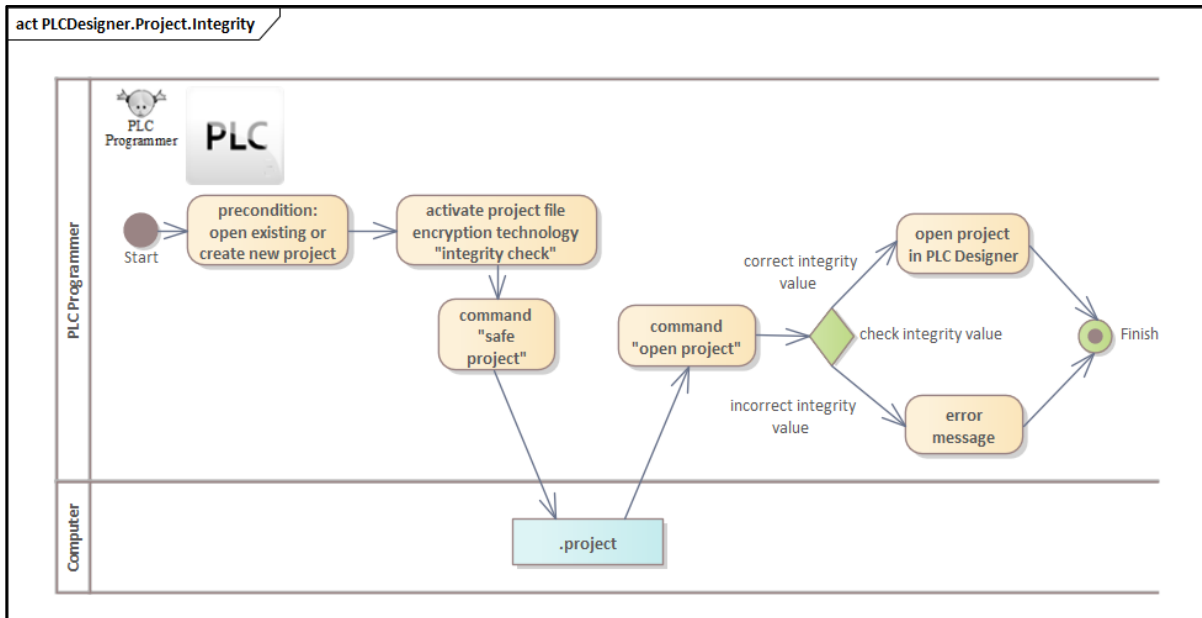


Forgotten Password

This can be done by opening the Password Manager with the following selection of the "Have you forgotten the" button.

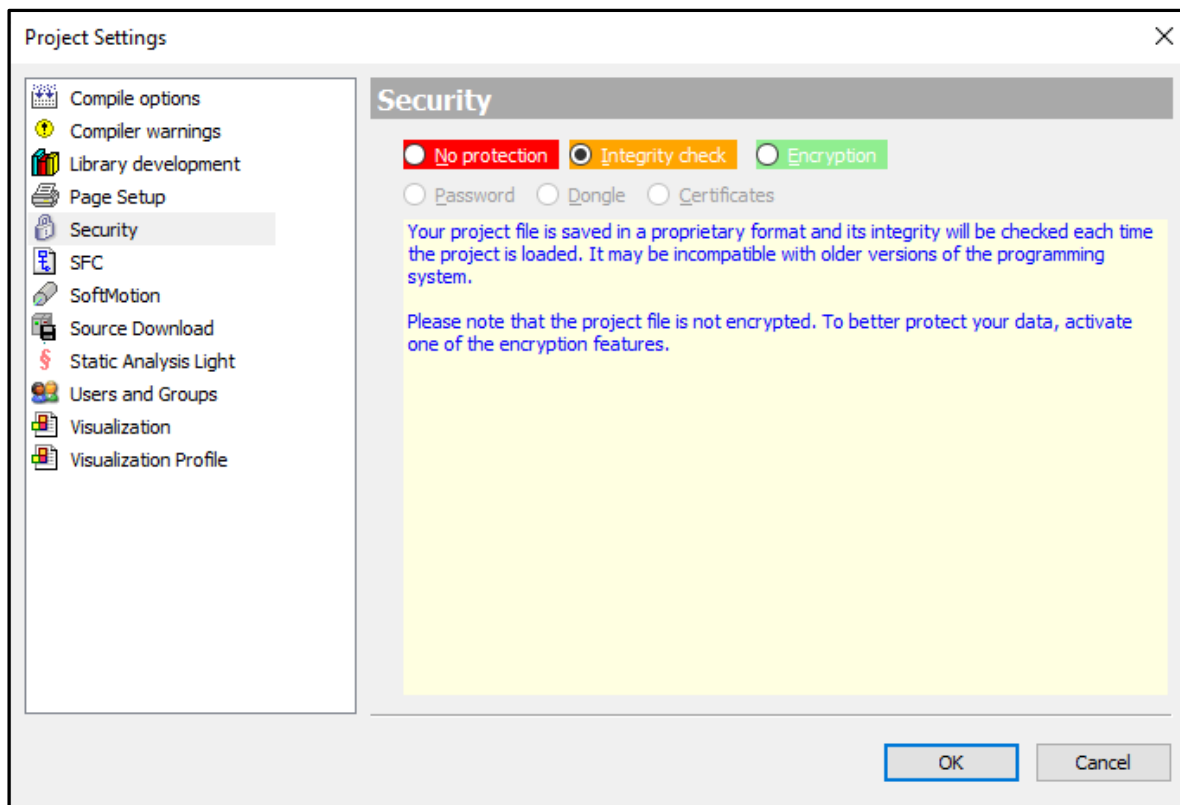
PLCDesigner.Project.Integrity

This functionality generates and verifies a integrity value for the PLC project. To check the integrity of the PLC project, the PLC project is not saved in plain text, but in a proprietary format. When saving, an integrity value is formed and checked when the project is opened. This function only checks integrity. The proprietary format does not represent encryption or confidentiality.



Activity Diagram

This function can be accessed via the »PLC Designer« "\View\Security Screen". If the Project File Encryption Technology is set to "Integrity check" in the Project tab, the function is activated.

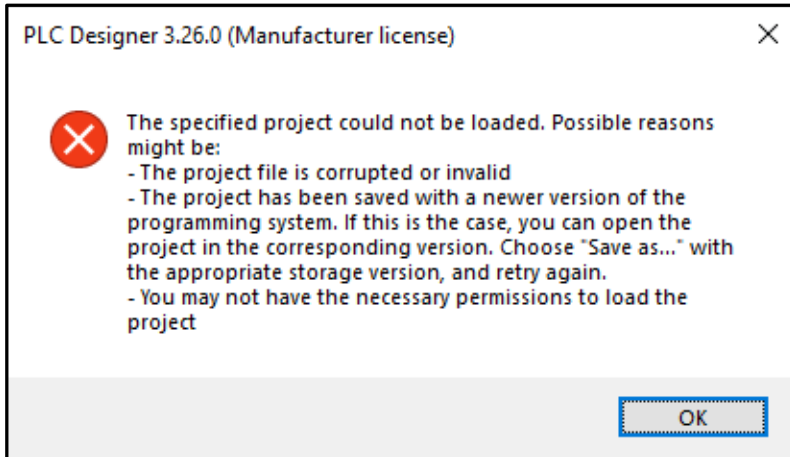


Project Settings

PLC Designer

Security functions

When a PLC project is opened, it is checked for integrity. If the integrity is intact, the project opens without a message. If the integrity is compromised, an error message is displayed and the project does not open.



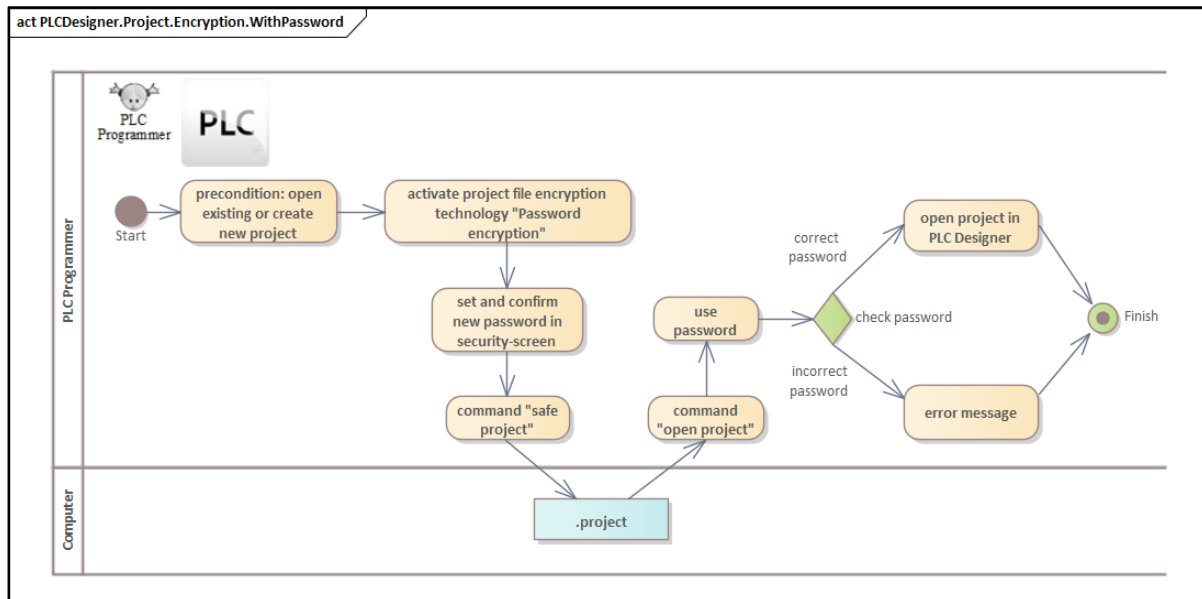
Error Message



This function only applies to the base project file "*.project". When saving the PLC project, additional data is stored. For example, there are xml files for node sets for the OPC-UA model. This function does not protect the integrity of these additional files, so users must protect them organizationally if necessary.

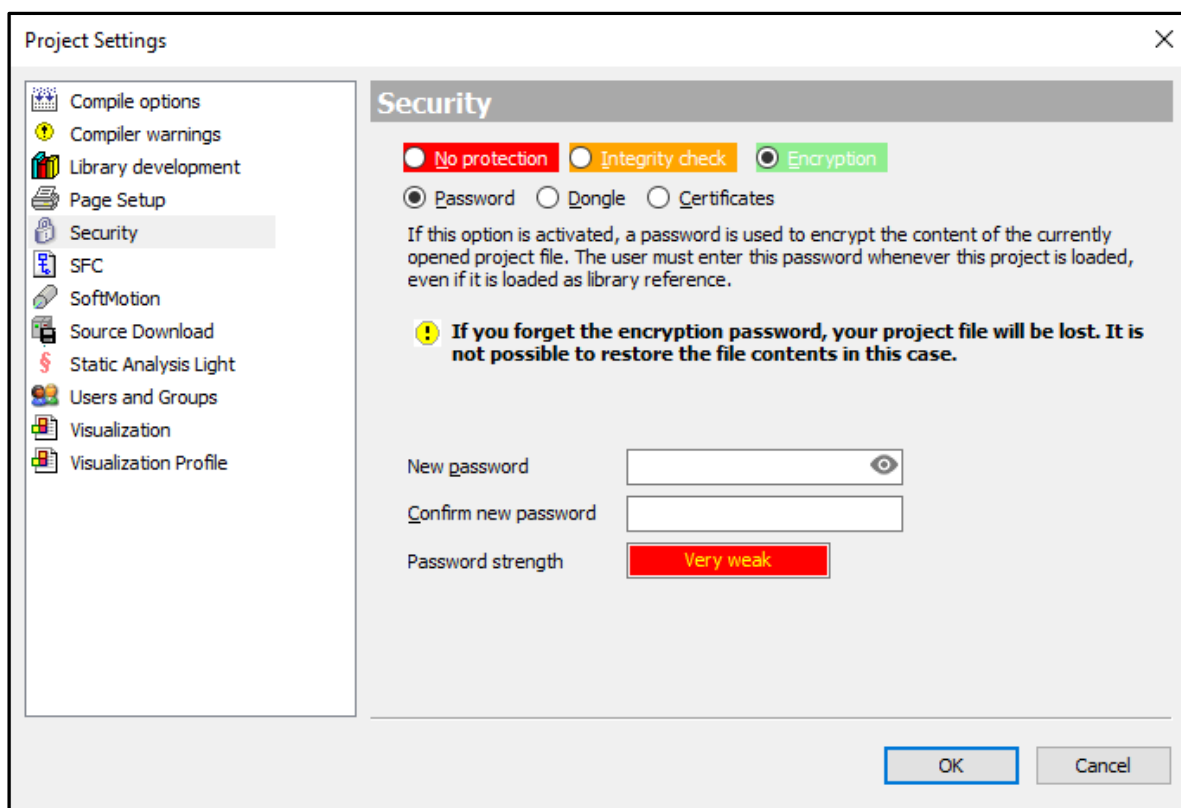
PLCDesigner.Project.Encryption.WithPassword

This functionality encrypts and decrypts the PLC project with a password.



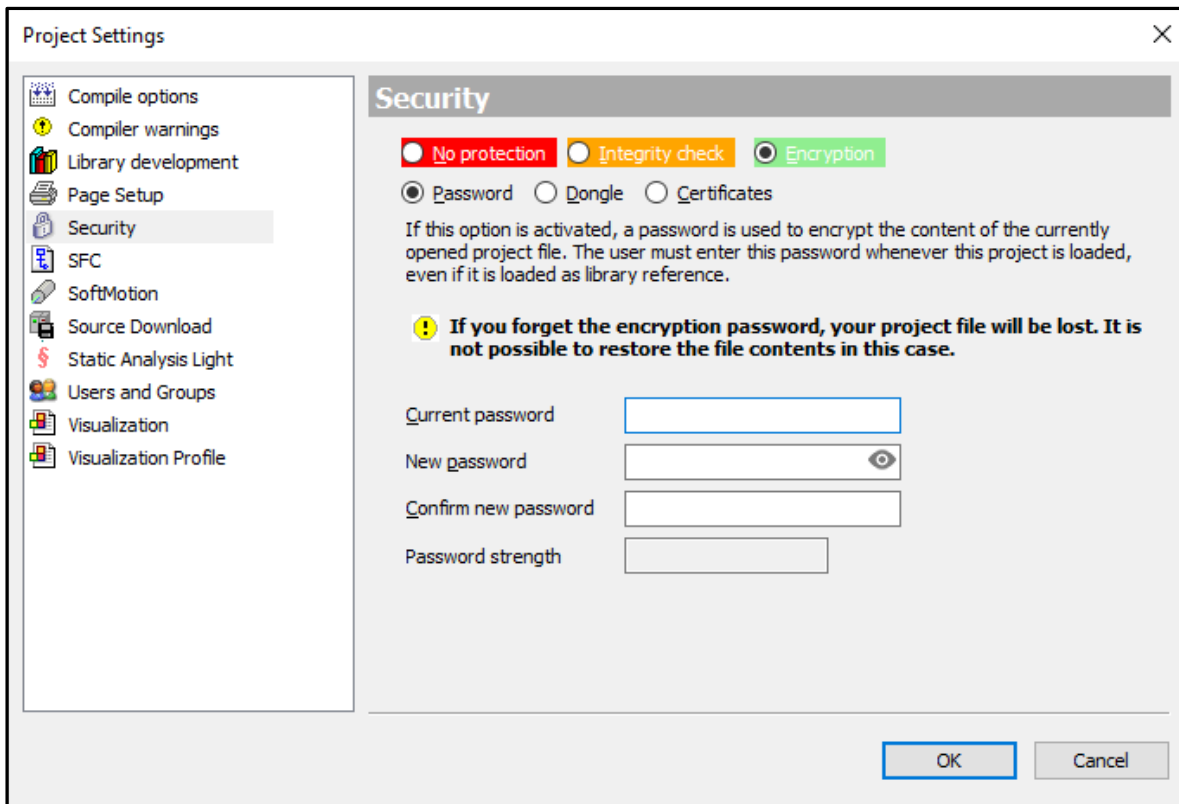
Activity Diagram

This function can be accessed via the »PLC Designer« menu "\View\Security Screen". If the Project File Encryption Technology is set to "Encryption" in the Project tab and the radio-button "Password" is chosen, the function is activated. At this point, a new password must be assigned and confirmed.



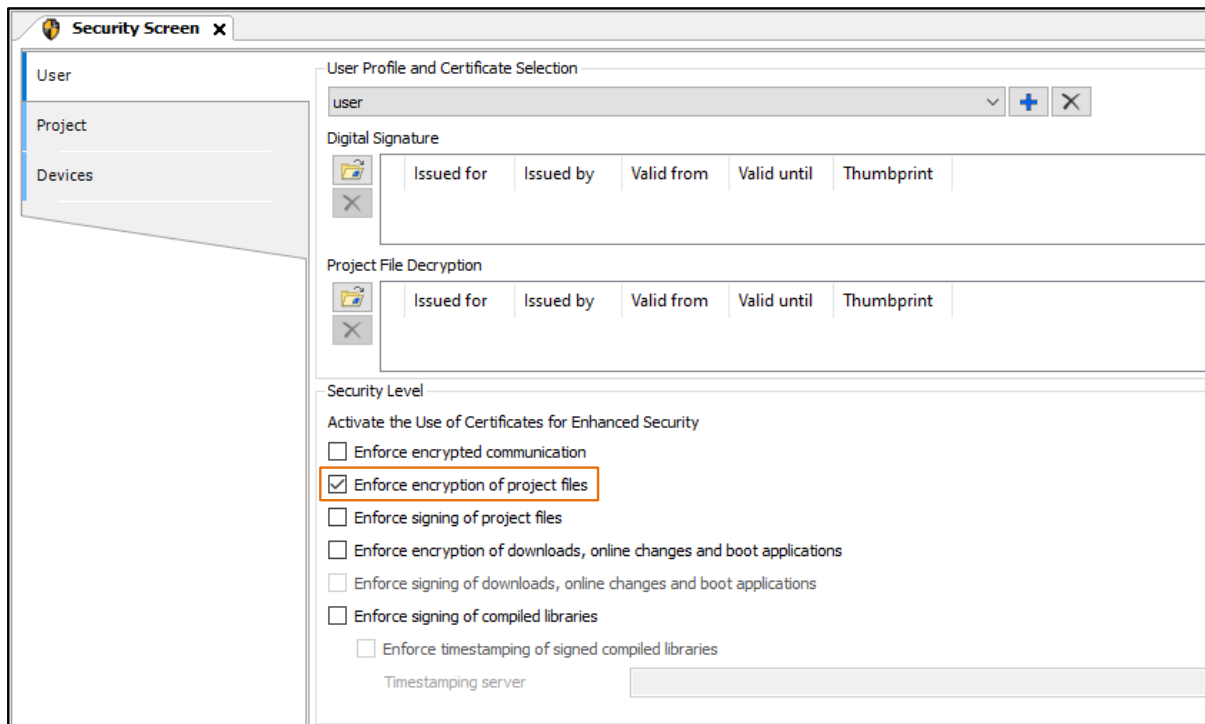
Project Settings

If this dialog is called up again for a project saved with password, the assigned password can be updated and confirmed.



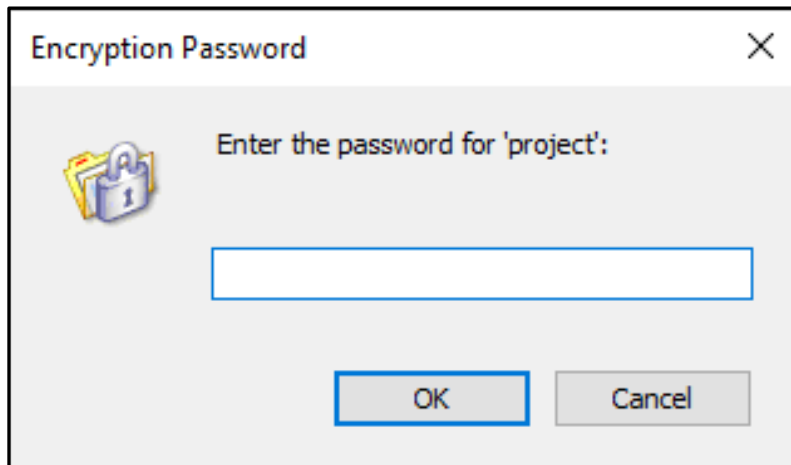
Project Settings for New Password

To enforce encryption of the project file, please activate the checkbox "Enforce encryption of project files" in the Security screen in the User tab.



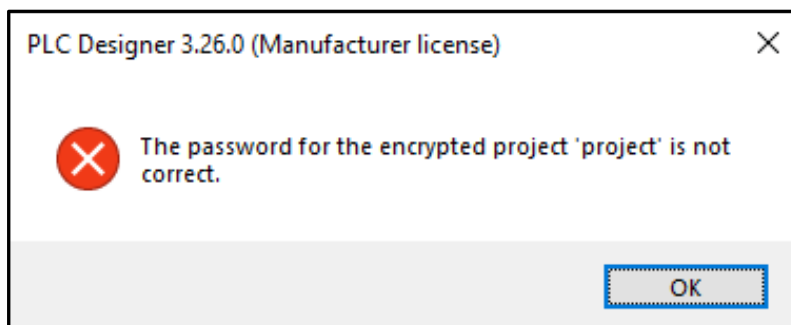
Enforce encryption of project files

When opening a PLC project, the user must enter a password.



Enter Encryption Password

If the password is correct, the project opens without a message. If the password is incorrect, an error message is displayed and the project does not open.



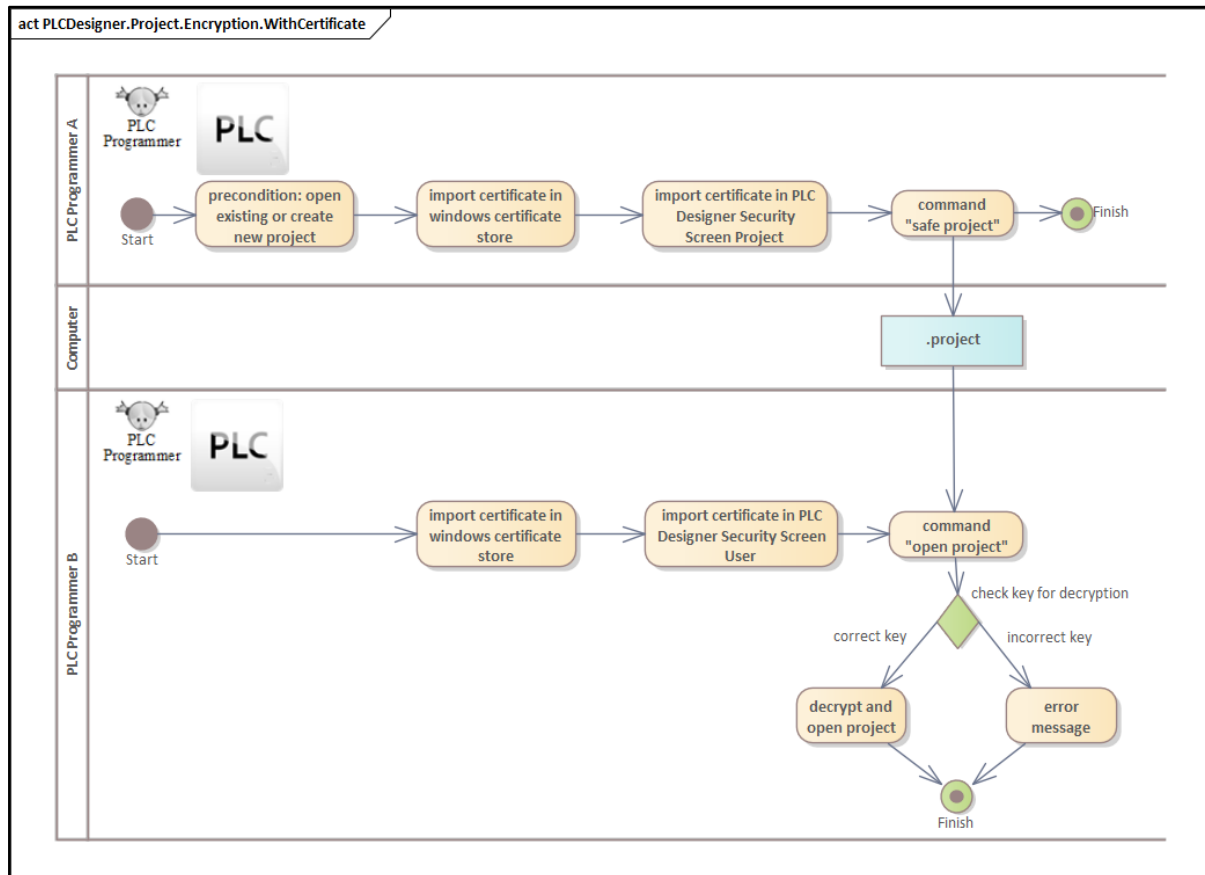
Password not correct



This function only applies to the base project file "*.project". When saving the PLC project, additional data is stored. For example are xml files for node sets for the OPC-UA model. This function does not encrypt these additional files, so users must protect them organizationally if necessary.

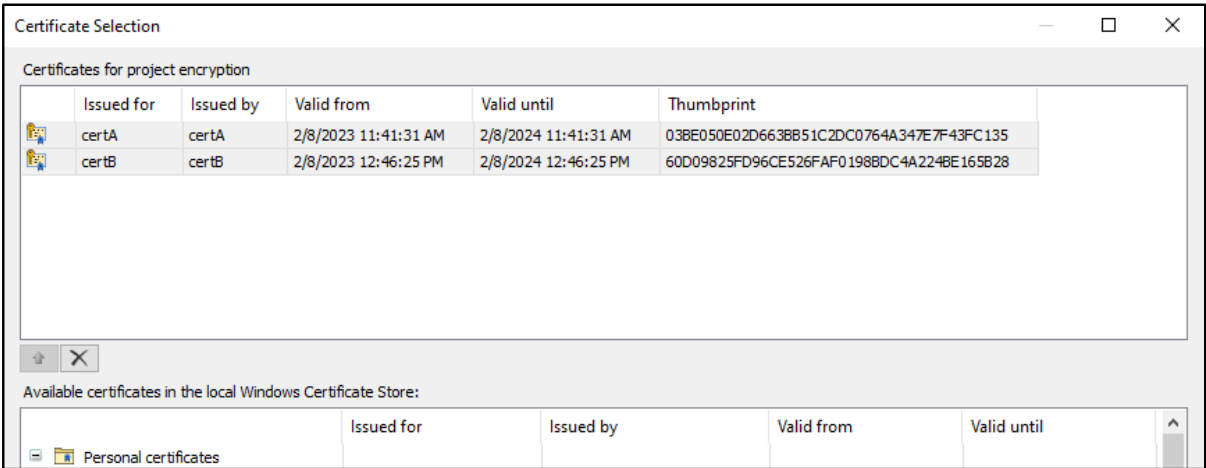
PLCDesigner.Project.Encryption.WithCertificate

This functionality encrypts and decrypts the PLC project using a key from a certificate.



Activity Diagram

This function can be accessed via the »PLC Designer« menu "\View\Security Screen". If the Project File Encryption Technology is set to "Encryption" in the Project tab and the radio-button "Certificate" is chosen, the function is activated. At this point, certificates can be selected from the Windows Certificate Store. It is possible to work with several certificates. It is possible to save a project with several certificates (each with public keys) and to open it with a matching certificate (with private key).



Certificate selection for encryption



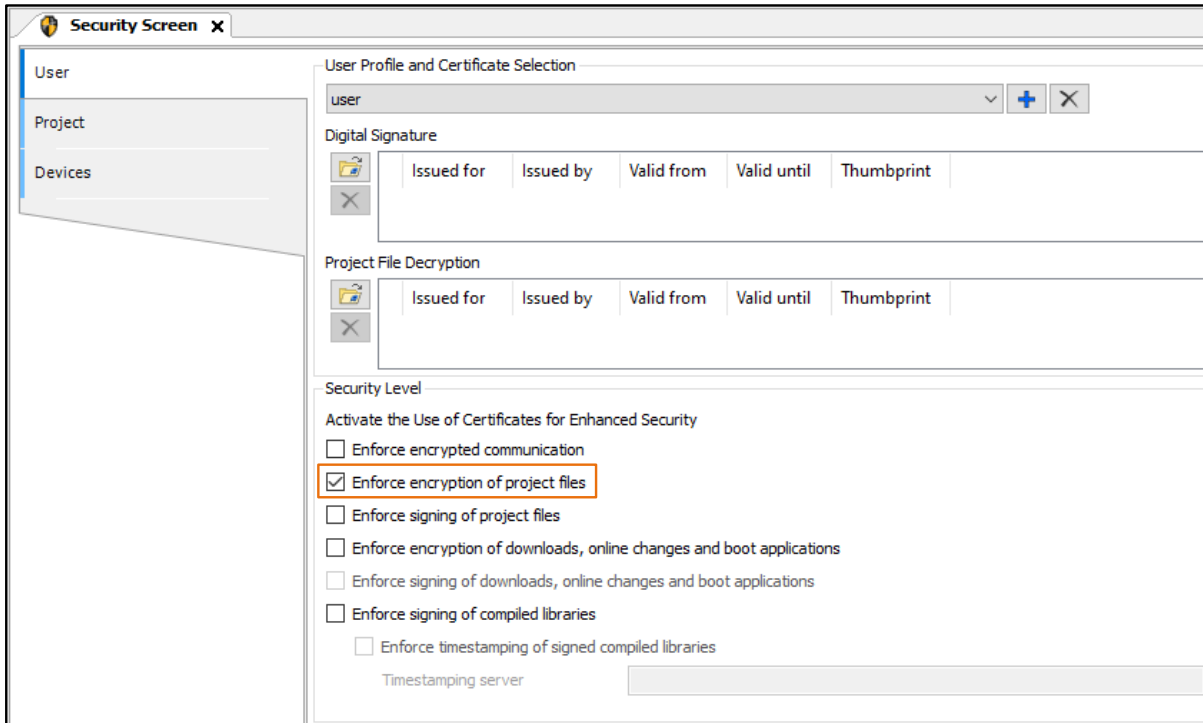
If a certificate is imported into the »PLC Designer« "`\Security Screen\Project\Project File Encryption`" that does not contain a private key, the following warning message will appear: "The project will be encrypted but none of the selected certificates has a private key. You will not be able to decrypt this project on this PC! Do you want to save it anyway?". This message appears because the public key is needed for encryption and the private key for decryption.

PLC Designer

Security functions

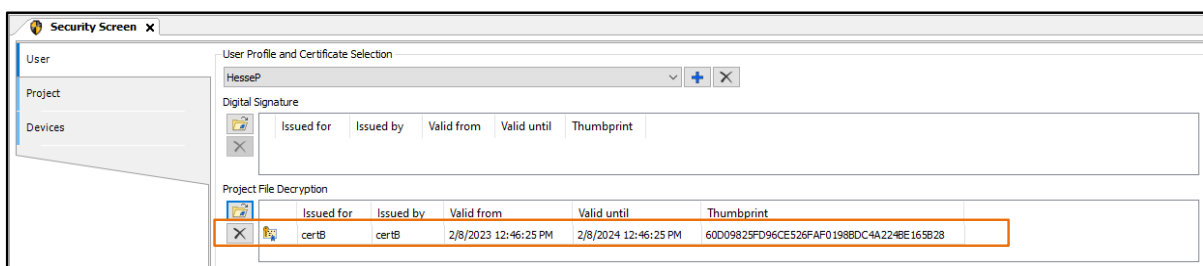
After selecting the certificates, the project can be saved as an encrypted file.

To encrypt the project file, please activate the checkbox "Enforce encryption of project files" in the Security screen in the User tab.



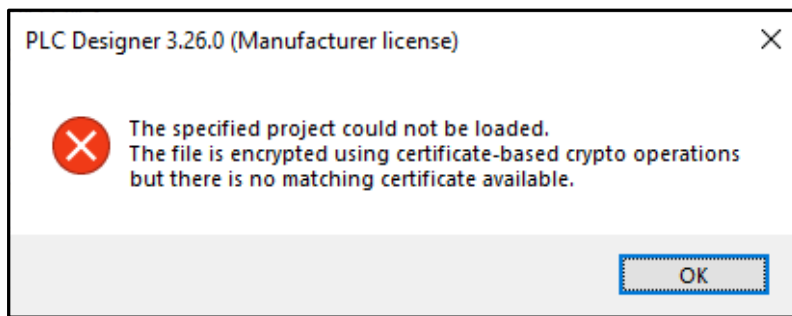
Enforce encryption of project files

Before opening a PLC Project, the user must integrate a correct certificate. For this purpose, the certificate must be selected in the »PLC Designer« "\View\Security Screen" in the "User"-selection in the "Project File Decryption" category. Only certificates including a private key can be selected.



Certificate for Project File decryption

If the private key is correct, the project opens. If not, the following error message appears:



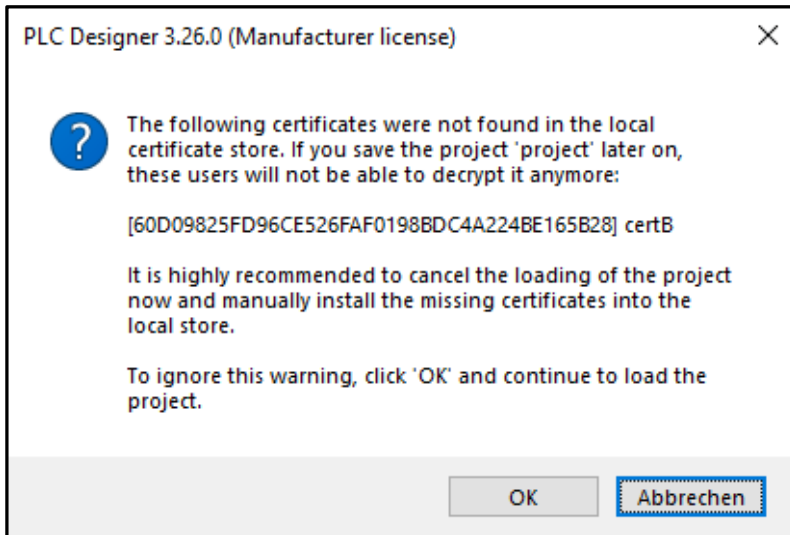
No matching Certificate available

As mentioned above, it is possible to encrypt the project with several public keys and open it with only one private key. There is a special feature to note here if this is done on different computers. For example, if the project is opened with only one private key, the project can be opened, but only that key will be used when saving again.

Example:

The project is encrypted with the public keys CertA and CertB and opened with the private key CertA. After saving the project again, the private key CertB can no longer open.

This circumstance is indicated by a warning message when opening in this configuration..



Missing certificates were not found

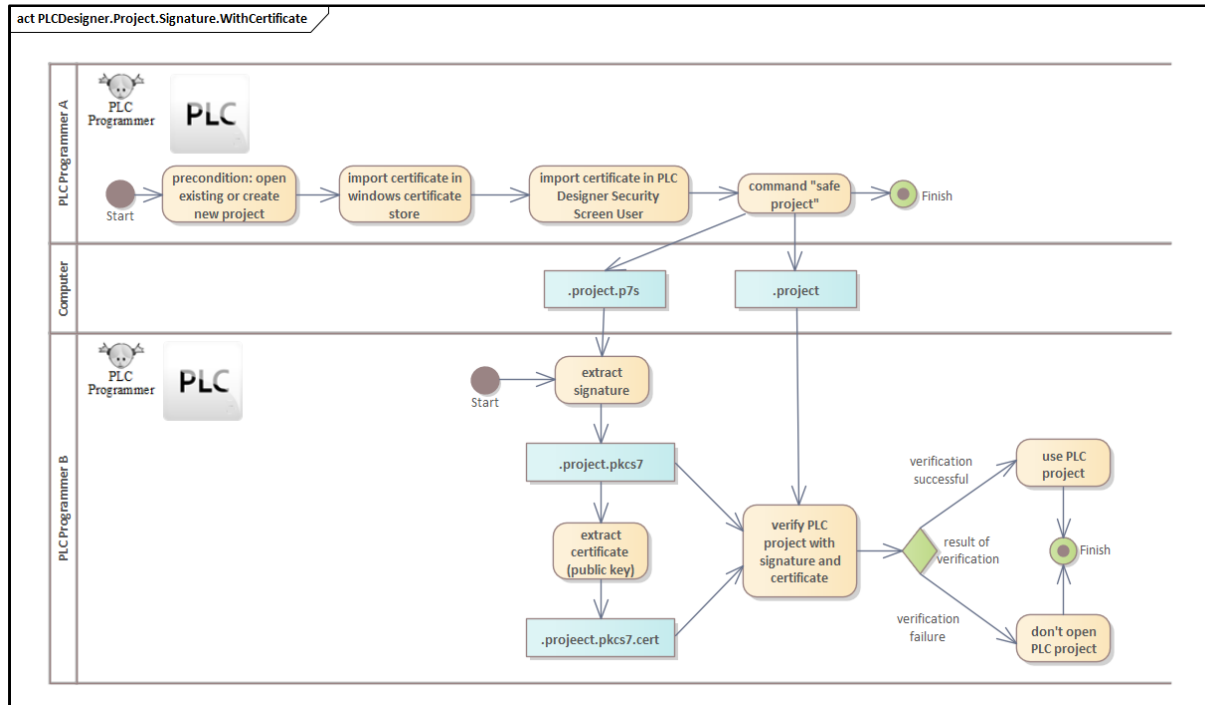


This function only applies to the base project file "*.project". When saving the PLC project, additional data is stored. For example are xml files for nodesets for the OPC-UA model.

This function does not encrypt these additional files, so users must protect them organizationally if necessary.

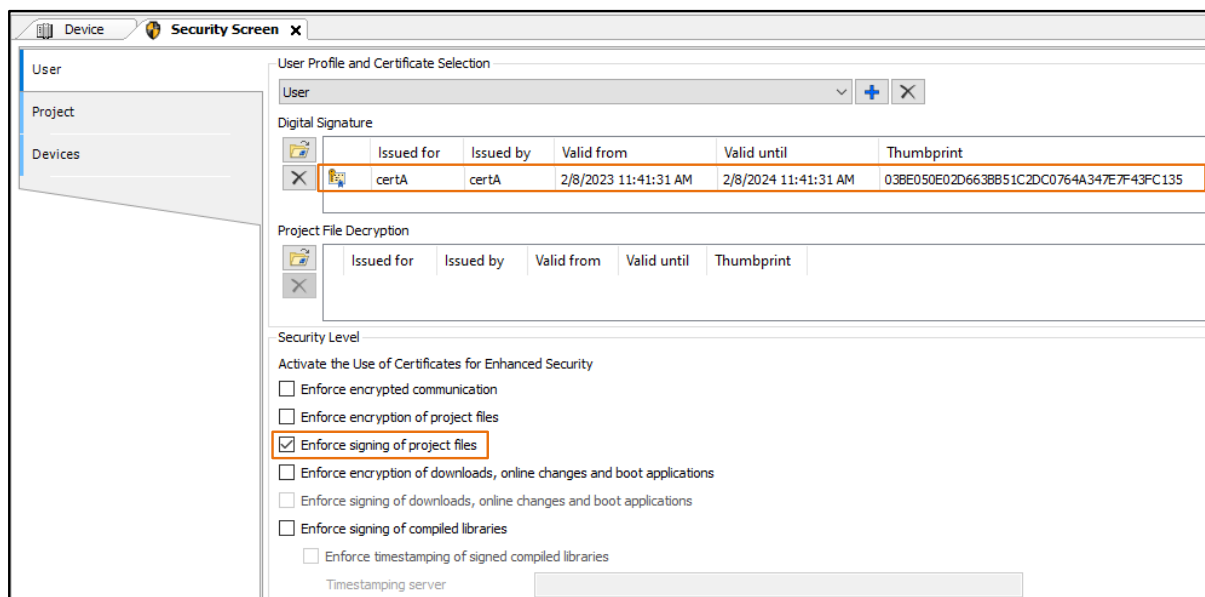
PLCDesigner.Project.Signature.WithCertificate

This feature uses a key from a certificate to sign the PLC project, allowing the project creator to send the project to a second person and verify its origin.



Activity Diagram

To sign a PLC project, select a certificate in the Digital Signature area of the Security screen in the User area of the PLC Designer. This certificate must contain a private key. Additionally, select the option "Enforce signing of project files."



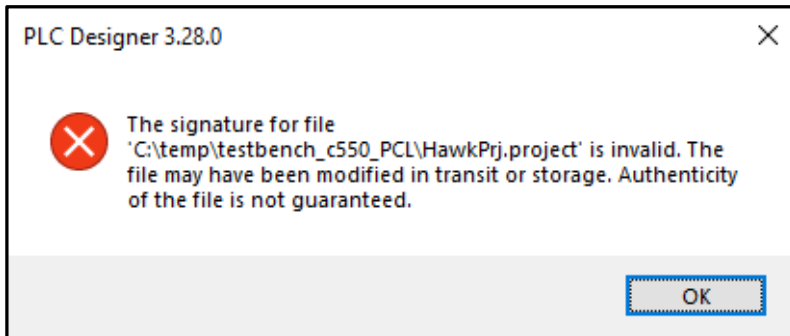
Enforce signing of project files

PLC Designer

Security functions

This creates an additional file with the extension *.p7s in the project directory. The project can now be handed over to a second person. That person can then check the signature.

When the project is opened in the »PLC Designer«, the signature is checked. It is invalid because the project has been changed, a warning is issued.



Validate Signature

There are several methods to additionally verify this signature. The following example describes a procedure in Linux with the help of openssl. In this example, the »PLC Designer« project "plc.project" and the signature file "plc.project.p7s" are available.

1. First, the pkcs7 signature is generated from the p7s file.

```
$ openssl pkcs7 -inform der -in plc.project.p7s -out plc.project.pkcs7
```

2. In a second step, the certificate is extracted from the p7s file.

```
$ openssl pkcs7 -print_certs -in plc.project.pkcs7 -out plc.project.pkcs7.cert
```

3. Finally, the file can be verified.

```
$ openssl smime -verify -binary -inform PEM -in plc.project.pkcs7 -content plc.project -certfile plc.project.pkcs7.cert -nointern -noverify > /dev/null
```

4. The result can be 'Verification successful' or 'Verification failure'.



This function only applies to the base project file "*.project". When saving the PLC project, additional data is stored. For example there are xml files for node sets for the OPC-UA model. This function does not sign these additional files, so the user must protect them organisationally if necessary.

A notice:

The Certificate for Signing remains selected even if the PLC Designer project is closed and the PLC Designer is restarted. It must therefore be replaced by the appropriate certificate or deactivated if a new project is to be opened.

Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

PLCDesigner.AccountManagementGuidelines

The Account Management Guidelines of the PLC Designer are described below.

PLCDesigner.AccountManagementGuidelines :: PLCDesigner.UserManagement

Default / Factory Settings:

The User Management of the PLC Designer project is activated by default. The following accounts are automatically created by default:

- "Owner" (user) | "Everyone" and "Owner" (group) | "" (password)

Account Handling:

- It is recommended that you change the default password for the "Owner" (user), or even better create a new user with the necessary rights and then delete the "Owner" user.

Policies:

It is recommended that you configure the user management settings. This includes

- The maximum number of authentication trials (default = 3).
- The automatic logout time after a period of inactivity (default = 10 minutes).
- The activation of the new hash format for passwords (default is deactivated for compatibility reasons).

PLCDesigner.PasswordManager

The password manager files are located in the following directory on the user's computer:

c:\ProgramData\PlcDesigner\Options\LiveOptions\

The relevant files are:

LIVE_UserRoot_{<ID>}.opt

After uninstalling the PLC Designer, the user must manually remove these data.

Controller.EncryptedCommunication.PLCDesigner

If you store the controller certificates for encrypted communication in the Windows certificate store in the "Controller Certificates/Certificates" directory, these certificates will not be deleted during uninstallation. After uninstalling the PLC Designer, the user must manually remove this data.

For more information see [Integrate a certificate in the windows certificate store](#).

PLCDesigner.Installation

The PLC Designer can be installed completely offline, i.e., without an internet connection. Starting with version 4.0.0, updates to individual components are carried out if an internet connection is available. To enable this, the administrator of the installation computer or the customer network should enable the following internet connections.

For example, if a proxy is being used, the following proxy server settings should be added, except for the addresses:

- update.lenze.com // Lenze Package Manager Server
- deployment.lenze.com // Lenze PLC Designer Deployment Server
- *.windowsupdate.com // Host System Windows
- digicert.edgecastcdn.net // Certificate Validation

EASY UI Designer

The EASY UI Designer is the central web design tool for visualizations.

Product description

Product identification

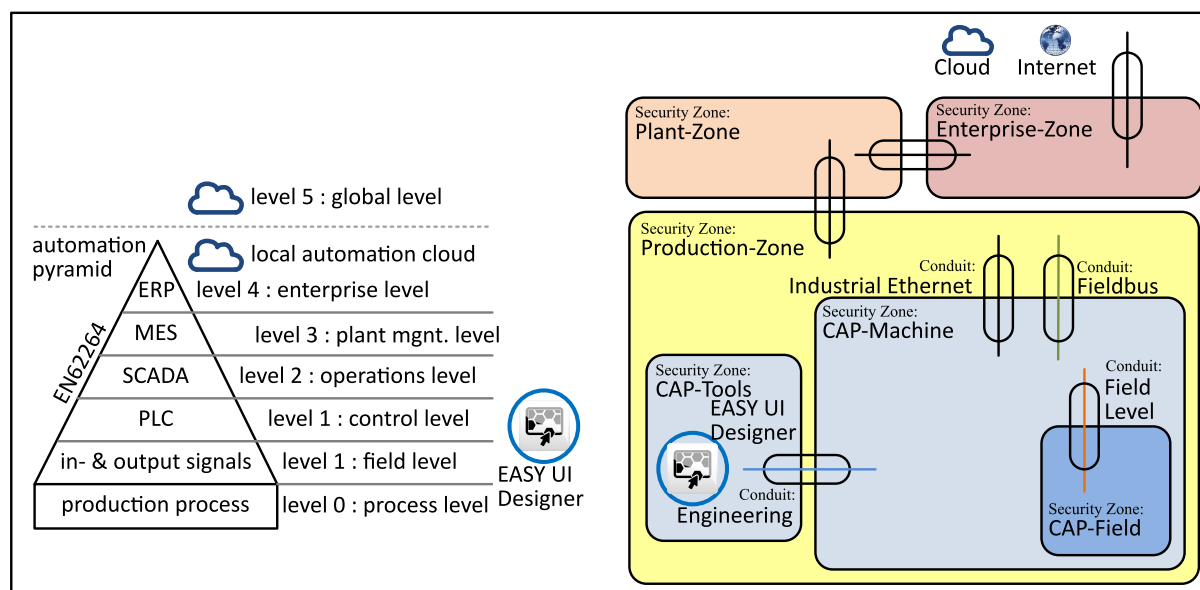
This documentation applies to the following components with their identification:

Name of product and product ID

Name of product	Product ID
»EASY UI Designer«	n.a.

Location in the network

This component is located in the automation pyramid at the control level. Furthermore, it is located in the security zone "CAP-Tools" ([Zones and Conduits](#)).



Product location in the network

The software addressed here has only one relevant interface:

- Conduit: Engineering

This connection is used to connect the tool to the Security Zone CAP-Machine.

Intended purpose

The intended user of this component is described in the application as directed and can be found in the operating instructions in the online help. In the following, some specifics regarding cyber security are discussed.

- The component mentioned here is professional software and may only be commissioned and decommissioned by specialists.
- This software also requires maintenance throughout its life cycle, which must be carried out by the operator.

EASY UI Designer

Product description

- Modifications to the software are not permitted.
- If this software is taken out of operation or disposed of, the instructions in the documentation must be observed.

Intended environment

The intended environment for this software is described in the application as directed and can be found in the online help. In the following, some specifics regarding cyber security are discussed:

- The software must be installed on an up-to-date computer equipped with valid IT protection mechanisms.
- The software must be installed on a computer, which uses protection against unauthorized use.
- Use appropriate authentication mechanisms for the computer. This applies, for example, to passwords that have the necessary complexity and an appropriate life cycle. The current state of the art must be taken into account here.
- This computer is the responsibility of its owner and must be protected by valid IT protection systems such as firewall, IDS, IPS, etc.

Security key indicators

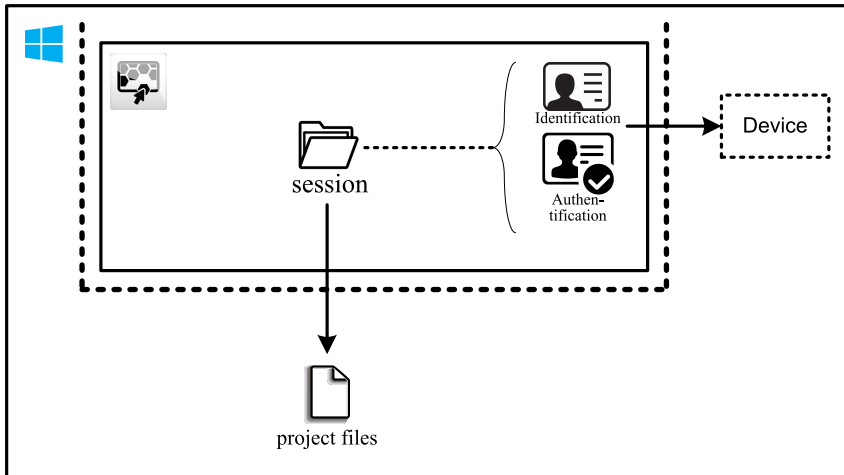
Security key indicator (in accordance with IEC 62443-4-2):

- This software is considered a software application (SAR).
- These components have a security level of SL-C 0.
- These components have an SL-vector from SL-C(UIDesigner)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }

Security mechanisms

Product Defense in Depth

The following image shows the Defense in Depth product concept. For the sake of clarity, some details have been deliberately omitted.

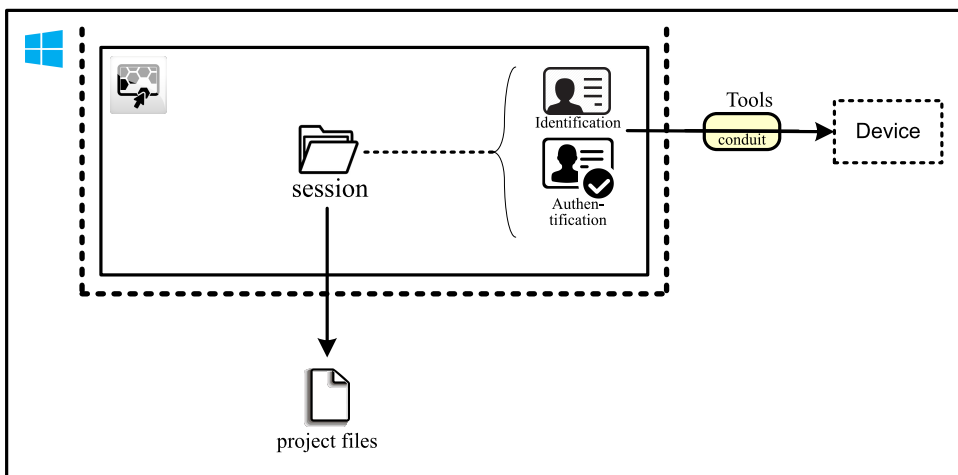


Product Defense in Depth

This EASY UI Designer software can run on a Windows-based host system. The user is responsible for this host system and must establish all relevant security protection mechanisms here or at higher levels.

Expected Defense in Depth in the environment

The following image shows the Expected Defense in Depth in the environment of the EASY UI Designer.



Expected Defence in Depth in the environment

Conduit Tools:

- Access from the engineering tools to the components must be limited in terms of organization and time.

EASY UI Designer

Security mechanisms

- The corresponding engineering tool must be operated on an up-to-date and IT-security-secured computer.

General Environment:

- General physical access protection must be provided for the components.
- Existing firmware updates for the EASY UI Designer as well as for all other components in the network should be installed immediately.

Security mechanisms

The following security functions are included in the listed components:

- UIDesigner.OPCUAClient.Authentication
- UIDesigner.OPCUAClient.Certificate
- UIDesigner.ServerManagerUI.Authentication
- UIDesigner.ServerManagerUI.Certificate
- UIDesigner.ServerManagerUI.Authorization
- UIDesigner.TargetDeviceManager.Authentication
- UIDesigner.TargetDeviceManager.Certificate
- UIDesigner.UserManagement

Commissioning, hardening and decommissioning notes and organizational measures

The following commissioning instructions must be followed:

General instructions

- As far as possible, avoid connecting the »EASY UI Designer« with a target via open networks or the internet.
- For protection, additionally use backup layers such as a VPN for remote access and install firewall mechanisms.
- Restrict physical and logical tool access to authorized persons.
- Change existing default passwords after the first start-up and also regularly afterwards.
- The UI Designer is installed on a Windows host. Please ensure that the Windows session lock is activated after a period of inactivity and by manual execution.

Commissioning and hardening instructions

- If the controller has an enabled user management, the OPC UA Client needs an authentication to access ([UIDesigner.OPCUAClient.Authentication](#)).
- If the controller is forcing an encrypted communication, the OPC UA Client needs a certificate handling for encryption ([UIDesigner.OPCUAClient.Certificate](#)).
- If the controller has an enabled user management, the Server Manager UI needs an authentication to access ([UIDesigner.ServerManagerUI.Authentication](#)).
- If the controller forcing an encrypted communication, the Server Manager UI needs a certificate handling for encryption ([UIDesigner.ServerManagerUI.Certificate](#)).
- If the Server Manager UI can only be executed with certain rights, these must be configured in the »PLC Designer« beforehand ([UIDesigner.ServerManagerUI.Authorization](#)).
- If the controller has an enabled user management, the Target Device Manager needs an authentication to access (refer to chapter [UIDesigner.TargetDeviceManager.Authentication](#)).
- If the controller is forcing an encrypted communication, the Target Device Manager needs a certificate handling for encryption ([UIDesigner.TargetDeviceManager.Certificate](#)).
- If the Target Device Manager can only be executed with certain rights, these must be configured in the »PLC Designer« beforehand ([UIDesigner.TargetDeviceManager.Authorization](#)).
- Use the »EASY UI Designer« authorization concept via the user management ([UIDesigner.UserManagement](#)).
- If required, the text for System Use Notification can be changed ([UIDesigner.SystemUseNotification](#)).

Periodic security maintenance

- It is recommended to check the password policy periodically for updates and to adjust the requirements if necessary.
- It is recommended to change the passwords cyclically.
- It is recommended to check the certificates used with regard to their key lengths for up-to-dateness and to generate new certificates with higher key length if necessary.
- It is recommended to exchange the certificates regularly.

EASY UI Designer

Commissioning, hardening and decommissioning notes and organizational measures

Decommissioning instructions

- After uninstalling the »EASY UI Designer«, the stored credentials must be manually removed from the Windows Credential Store ([Storing Credentials for Authentication](#)).

Removal product from environment

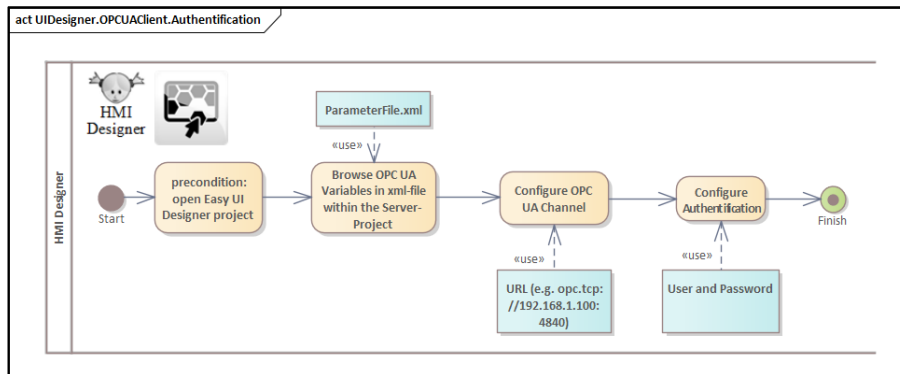
- n.a.

Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

UIDesigner.OPCUAClient.Authentication

The runtime of the »EASY UI Designer« is executed on the Controller. The controller has an internal connection to the OPC UA Server to retrieve the data for display. This internal connection can also be switched from one controller to another, via an external endpoint.



Activity Diagram

Browse OPC UA Variables

The variable connection between the server project and the controller takes place via OPC-UA. This is set in the »EASY UI Designer« in the server project as follows:

- Open the Server Project
- Open Variables / Channels / Controller: OPCUA
- Right mouse click and "Browse Variables ..."
- Add
- Communication type: CoDeSysV3 export file (*.xml)
- Namespace index: 4
- Device type: e.g. c500
- Device name: choose a typical name
- Choose parameter file in the PLC Project Directory
- Then browse through the variable tree and select the wanted variables

Configure communication channel (OPC UA)

After the variables have been imported, communication via OPC UA must be configured.

- Select "Variables / Channels / Controller: OPCUA" in the Server Project.
- Open the device, e.g. c550
- Click on the application

In the Property Page in the Common tab, the basic settings can be configured.

- Name
Choose a name for the device, e.g. controller
- OPC Server name
Choose an OPC Server name, e.g. OPCUA
- URL
Integrate the URL for the OPC UA Server, e.g. opc.tcp://localhost:4855, or opc.tcp://192.168.10.100:4840
- Browser
Please select "VisiWin.LenzeOPCUA.Br.w.dll"
- Default access path
url:Lenze:PLCOpen

Configure authentication

After setting the variables and the communication, the authentication for the OPC UA Client can be parameterized. If there is no active user management running on the controller ([Controller.UserManagement](#))

- Deactivate the checkbox "User authentication" in the tab
"Variables / Channels / Controller: OPCUA / <Device> / <Application>"

If there is an active user management running on the controller

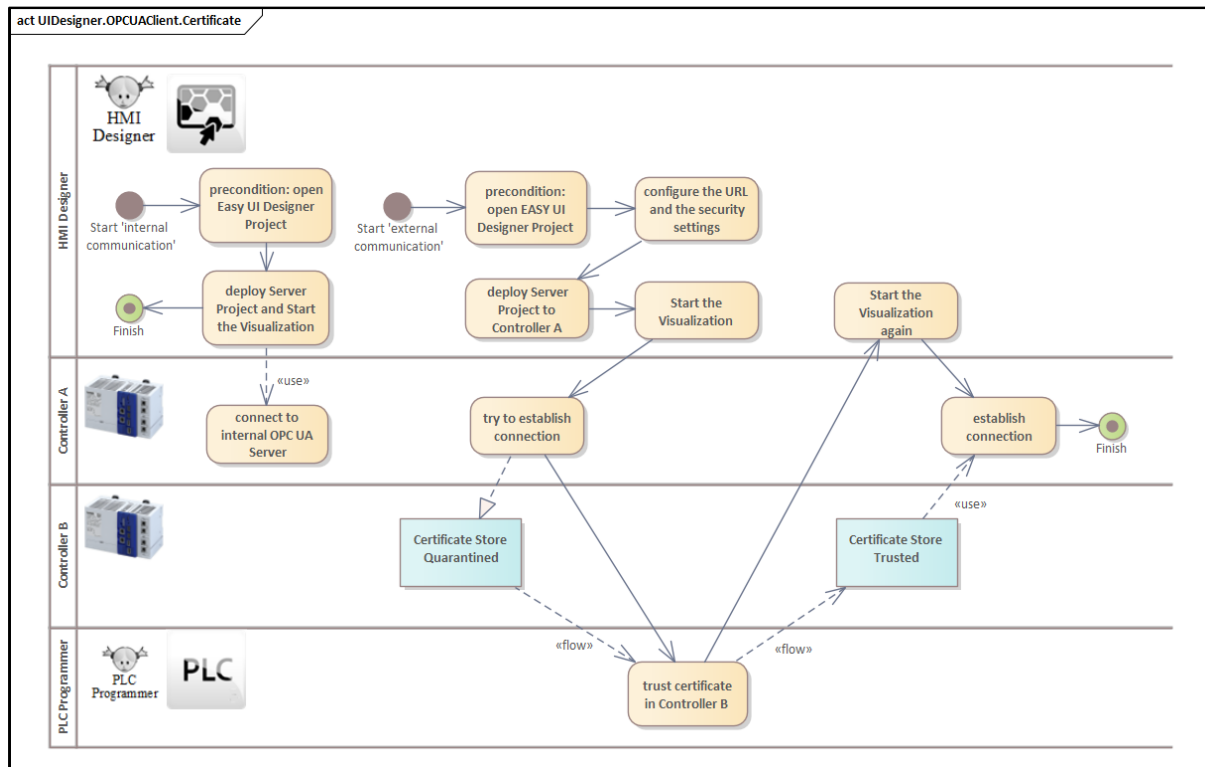
- Activate the checkbox "User authentication" in the tab
"Variables / Channels / Controller: OPCUA / <Device> / <Application>"
- Insert "Login name" and Password
- Click Apply button



When entering the password in plain text, it should be noted that it can be read on the screen. Organizational measures must therefore be taken to ensure that the password cannot be read by third parties. After accepting the login name and password with the Apply button, the password is correctly displayed with ****.

UIDesigner.OPCUAClient.Certificate

If the controller is forcing an encrypted communication, the OPC UA Client needs a certificate handling for encryption.



Activity Diagram

Two different considerations or possible uses must be distinguished here.

Internal Communication

The UI Designer Runtime runs on the same controller as the application program. In this case, the UI Designer Runtime accesses the internal endpoint of the OPC UA Server via an OPC UA Client via internal communication. In this case, authentication ([UIDesigner.OPCUAClient.Authentication](#)) is required, but no encrypted communication, since this takes place internally.

External Communication

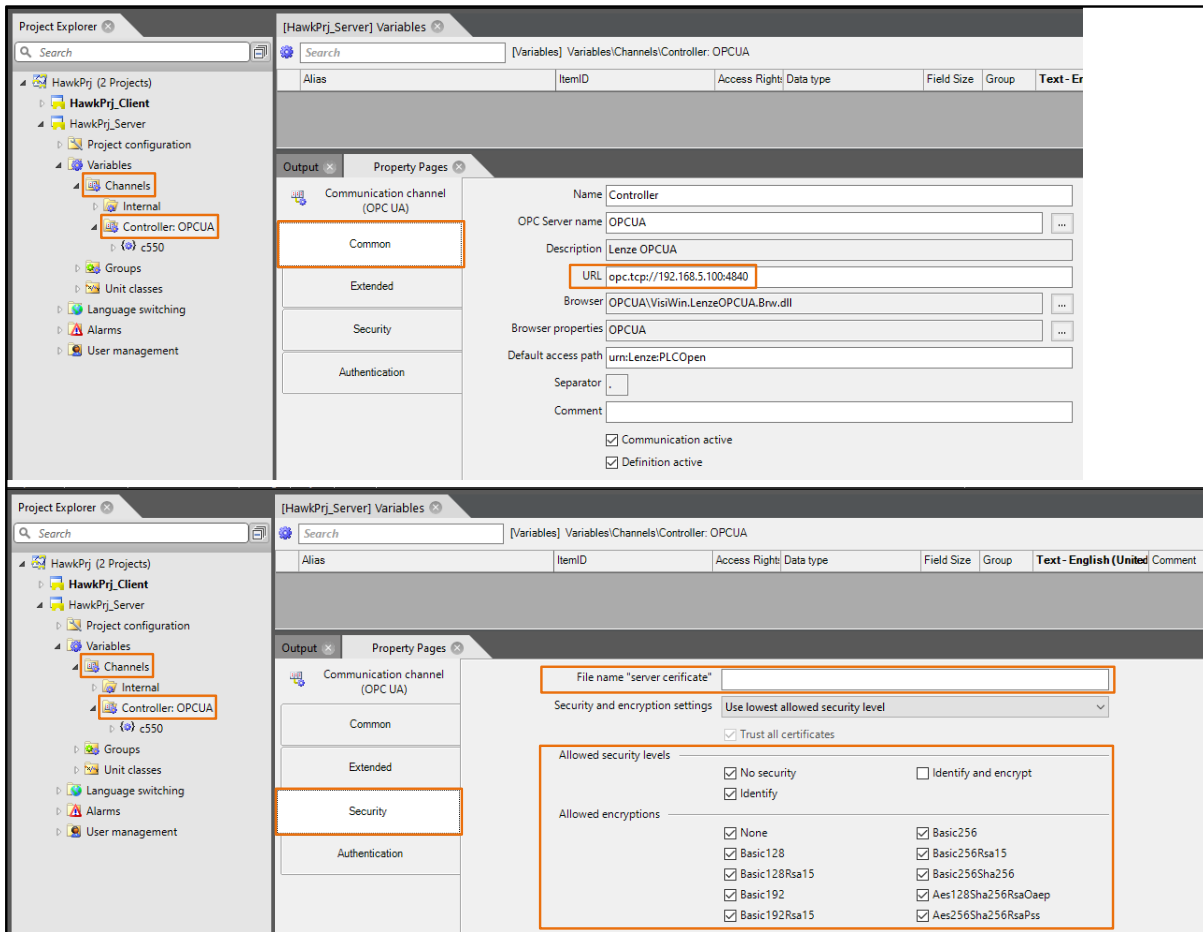
The UI Designer runtime runs on a different controller, than the application program. In this case, the UI Designer Runtime accesses the external endpoint of the OPC UA Server via an OPC UA Client via external communication. In this case, authentication ([UIDesigner.OPCUAClient.Authentication](#)) is required, and encrypted communication if the other controller enforces it.

EASY UI Designer

Security functions

Handling certificates for an external communication and enforced encrypted communication

To configure the OPC UA Client, first set the connectivity under Common in the Server project under Variables / Channels / Controller: OPCUA. Make sure to set the correct IP address with the port of the OPC UA Server.



own "server certificate"

Changing to the Security tab allows you to configure the server certificate for connection.

Security and encryption settings:

- Use lowest allowed security level
- Use highest allowed security level

Allowed security levels:

- No security
- Identify
- Identify and encrypt

Allowed encryptions:

- None
- Basic128
- Basic128Rsa15
- Basic192
- Basic192Rsa15

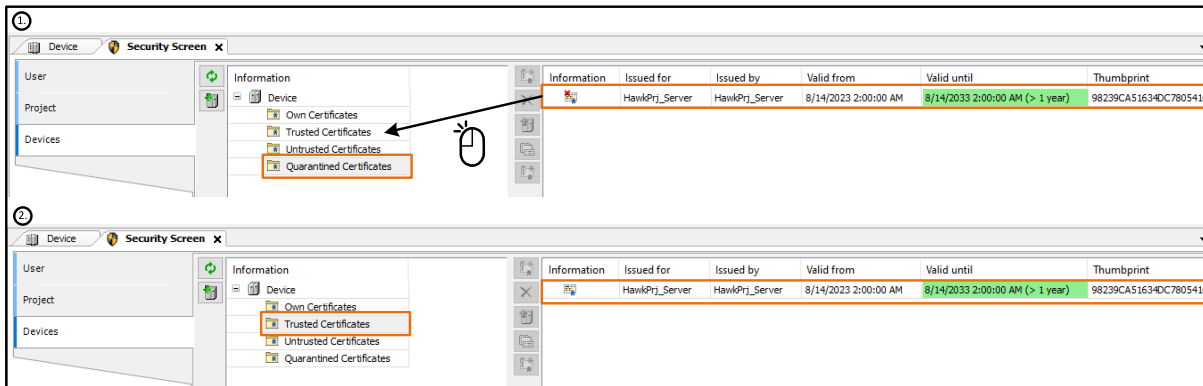
- Basic256
- Basic256Rsa15
- Basic256Sha256
- Aes128Sha256RsaOaep
- Aes256Sha256RsaPss

EASY UI Designer

Security functions

After configuring encrypted communication, deploy the server project to Controller A (see the picture at the beginning of this chapter). When the visualization is started on Controller A, a connection to Controller B is attempted and a certificate is quarantined.

Now, the PLC programmer of Controller B must trust the certificate, e.g., using the "PLC Designer."



Trust Certificate

After the certificate is trusted on Controller B, the EASY UI Designer can start the visualization.

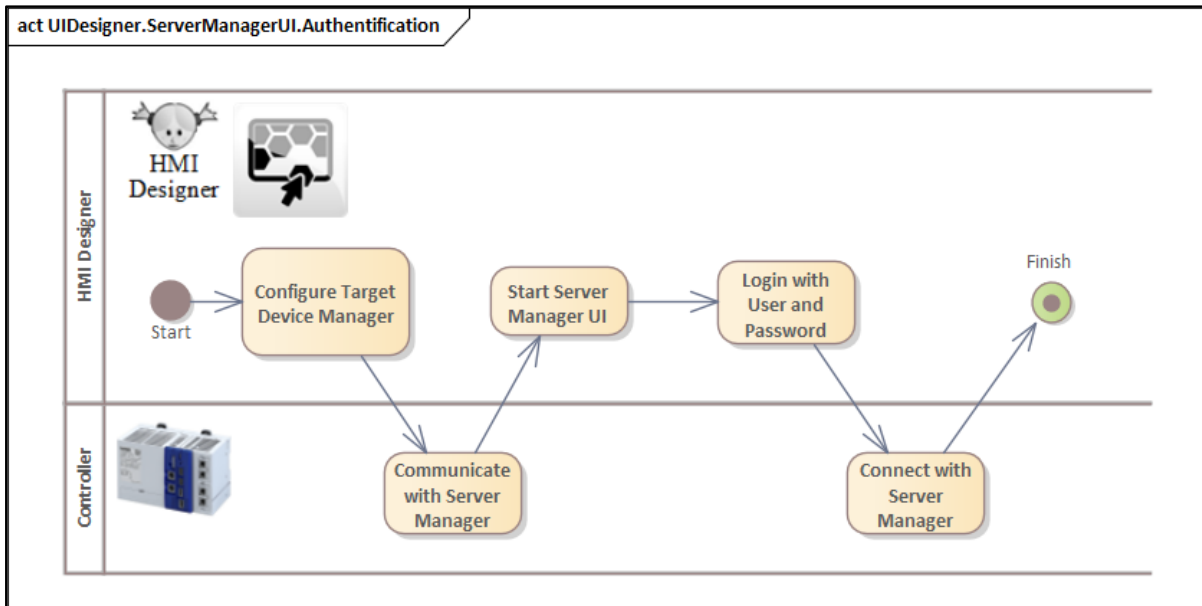


Important:

This own certificate, which is automatically generated for the OPC UA Client, is valid for 10 years and must be renewed before it expires. Otherwise, the OPC UA Client will not be able to connect.

UIDesigner.ServerManagerUI.Authentication

In order to go online with the »EASY UI Designer« when user management of the controller is activated, authentication must be enabled by the "Server Manager UI".



Activity Diagram

The settings for this are made with the following steps:

- Start the "Server Manager UI" with "UI Designer / Tools / Server Manager UI".
- Enter the username and password of a user in the controller user management group "EasyUi" (refer to chapter "Cyber Security\c5x0 controller\Security Functions\Controller.UserManagement\Controller.UserManagent: User for UI-Designer"). Leave the domain field blank.

Login

Username
Password
Domain:
☐ Login anonymous
☐ Save credentials
SUBMIT

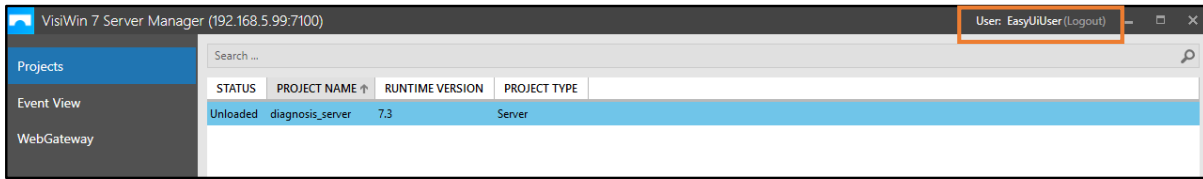
UI-Designer Server Manager UI Login Screen

If the credentials are correct, Server Manager is started. If the access data is not correct, the error message "Login failed – invalid input" appears.

EASY UI Designer

Security functions

To end the user's session, a logout function is available:



Logout



The following characters are not supported in the password:

§ ß ü Ü ö Ö ä Ä

Login anonymous

If the controller has an deactivated user management, the »EASY UI Designer« can use the "Login anonymous" flag. With this option, a login is possible without username and password.

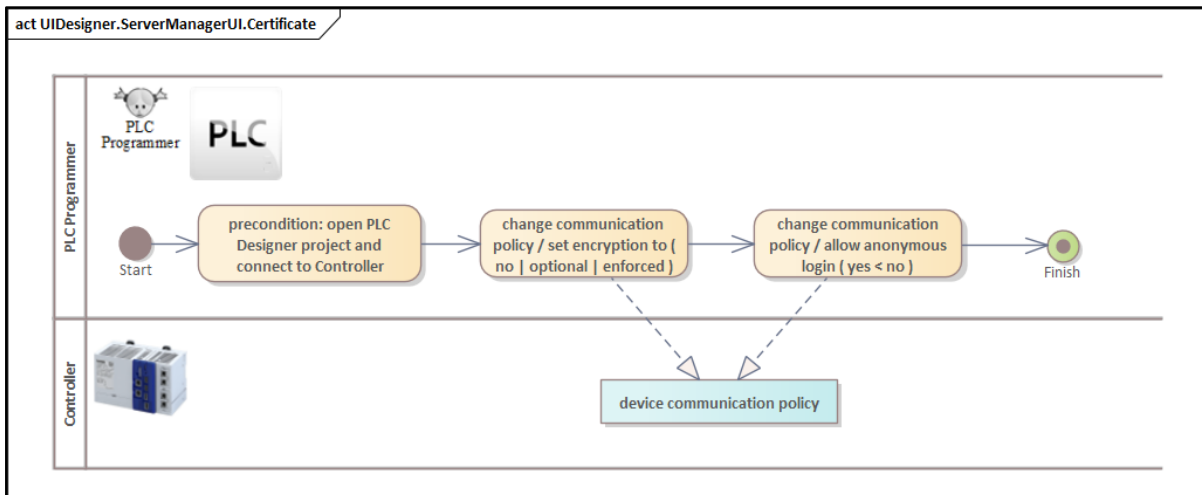
Save credentials

If the user activates the "Save credentials" flag, the Username and the Password will be saved in the Windows Credential Manager, ([Storing Credentials for Authentication](#)). At the next login, the data will be used again.

UIDesigner.ServerManagerUI.Certificate

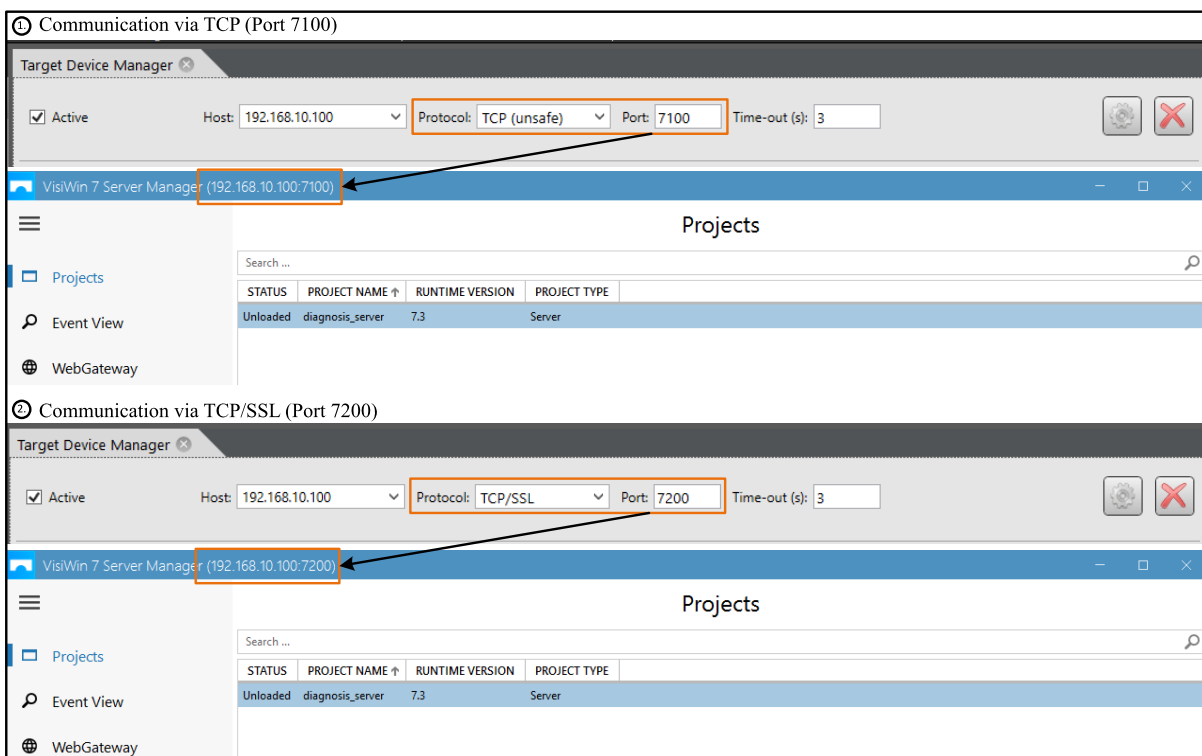
This functionality has been available since »EASY UI Designer« version 01.05.00 and controller firmware version 01.11.00.

If the controller forcing an encrypted communication, the Server Manager UI needs a certificate handling for encryption.



Activity Diagram

The »EASY UI Designer« can be operated with two protocols. The unencrypted TCP protocol is used via port 7100 and the encrypted TCP/SSL protocol is used via port 7200. The »EASY UI Designer« operator configure these settings via the Target Device Manager.



EASY UI Designer

Security functions

Configuration

Depending on the controller setting, a connection can be established. The combinatorics can be found in the following table.

EASY UI Designer	Communication policy		
	No encryption	Optional encryption	Enforced encryption
TCP Port 7100	EASY UI Designer protocol must be TCP via Port 7100	EASY UI Designer protocol can be TCP via Port 7100	not possible
TCP/SSL Port 7200	not possible	EASY UI Designer protocol can be TCP/SSL via Port 7200	EASY UI Designer protocol must be TCP/SSL via Port 7200

If the encrypted connection is selected, a certificate is automatically generated on both ends of the connection, the »EASY UI Designer« and the Runtime on the Controller, which is used for encryption. User interaction is not necessary.

UIDesigner.ServerManagerUI.Authorization

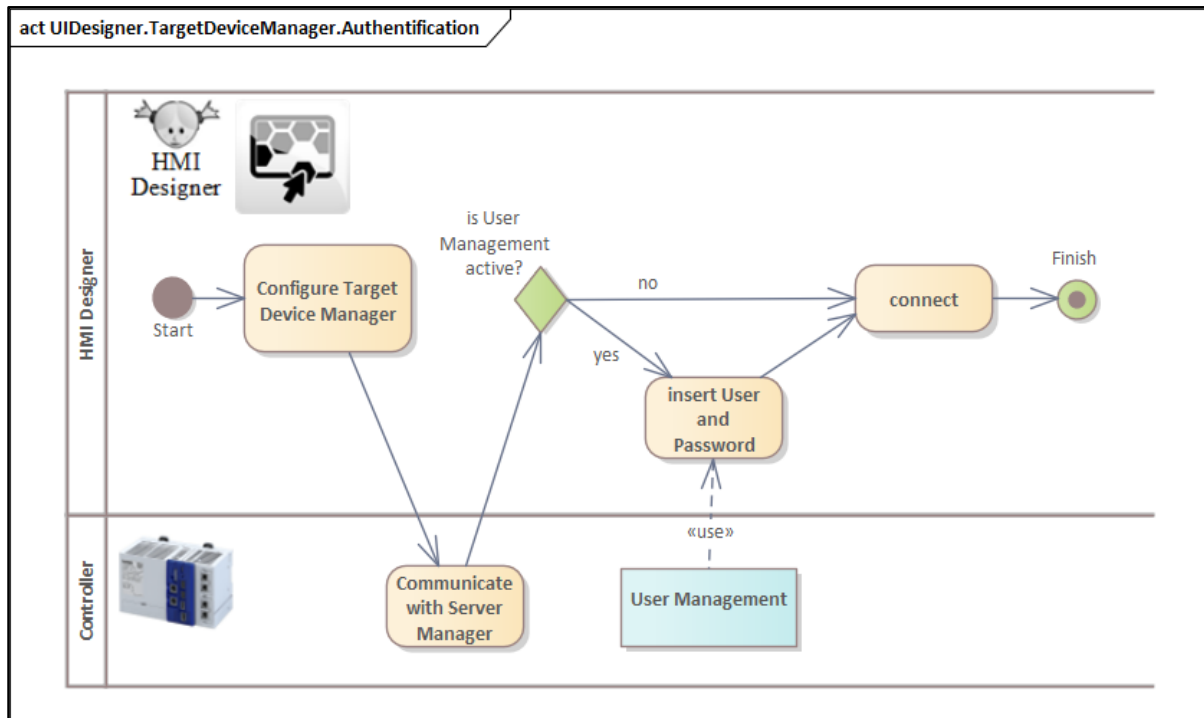
In order to configure the rights for authorization, the »PLC Designer« must be logged in to the controller and the user management must be activated ([Controller.UserManagement](#)).

After activation, the user can open the device window and select the "Users and Groups" tab. The Group EasyUi already exists here. All users in this group can access the controller via the "EASY UI Designer." Selecting the "Access Rights" tab shows the configurable objects. The object "Runtime Object\Device\Remote Connections\EasyUi Interface" is intended for allocating the relevant rights.

PLC Designer Right for Object EasyUiInterface	EASY UI Designer Right for Server Manager UI	Description of Authorization
View	View	View rights are needed to view objects with the Server Manager UI with read only rights.
Execute	Execute	Execute-Rights are needed, so that the Server Manager UI is able to start and stop processes and manage files.
Modify	Change	Modify rights are needed, so that the Server Manager UI can change the configuration of projects and the Server Manager.
Add / Remove	Admin	Is not used.

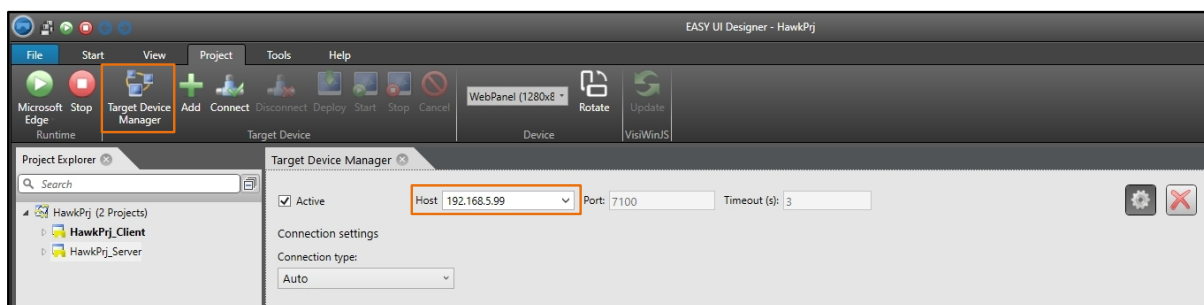
UIDesigner.TargetDeviceManager.Authentication

Since version 01.04.00 of the »EASY UI Designer«, the authentication of the Target Device Manager is available.



Activity Diagram

Integrate the Host-IP and connect to the controller.

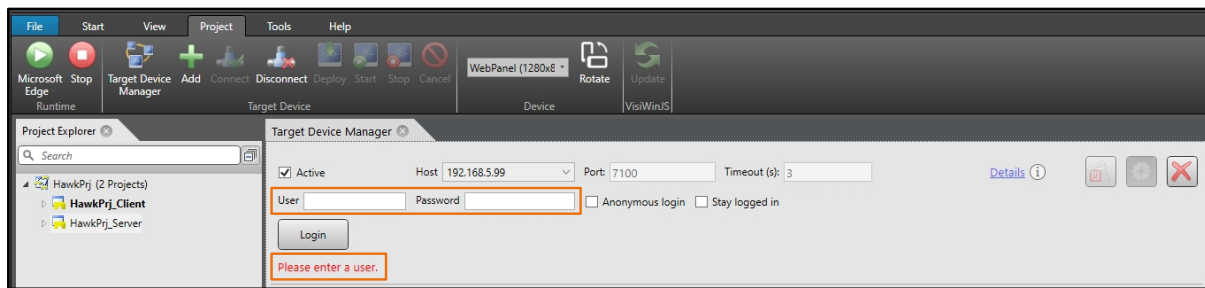


Integrate Host-IP

After that, a message occur "Please enter a user".

EASY UI Designer

Security functions

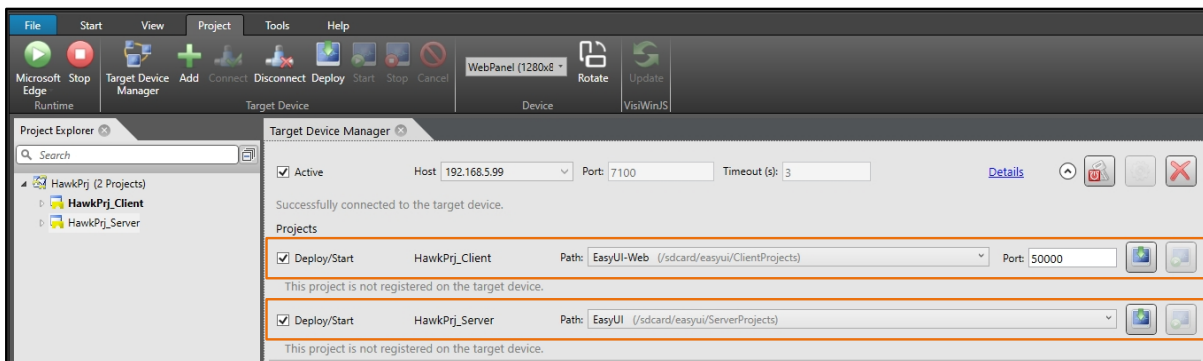


Enter a user

A user with password from a user, created in the `Controller.UserManagement` ([Controller.UserManagement](#)), must be specified.

What happens if authentication is correct?

After entering the correct credentials, it is possible to deploy the client and server projects.



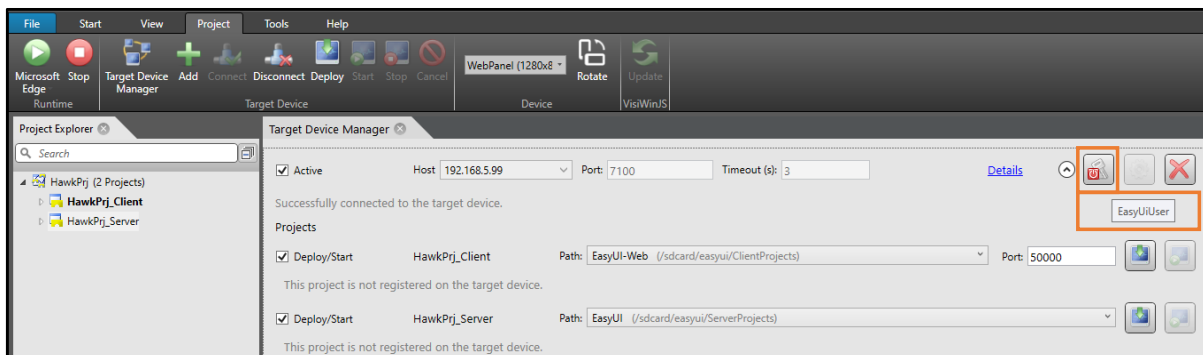
Deployment

What happens if I enter the wrong information?

If you log in with an empty username and password, an error message that says "Please enter a username" appears. If you enter the wrong username and/or password, an error message that says "The user could not be logged in" appears.

Changing a user

The Target Device Manager has a button with a key. The tool tip shows the currently authenticated user (in this example it is "EasyUiUser", see the following image).



Changing a user

By clicking the button, the login authentication appears, allowing another user to be entered and authenticated with their password.

What does "Anonymous login" mean?

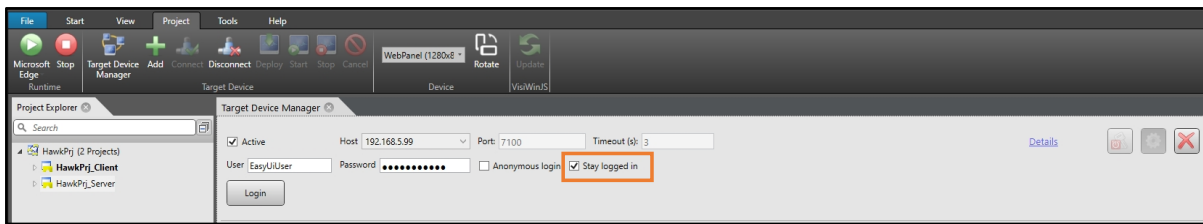
If the controller has a deactivated user management, the »EASY UI Designer« can use the "Login anonymous" flag. With this option a login is possible without username and password.

EASY UI Designer

Security functions

Save credentials

Selecting the "Save credentials" checkbox allows the user's credentials to be saved.



Stay logged in

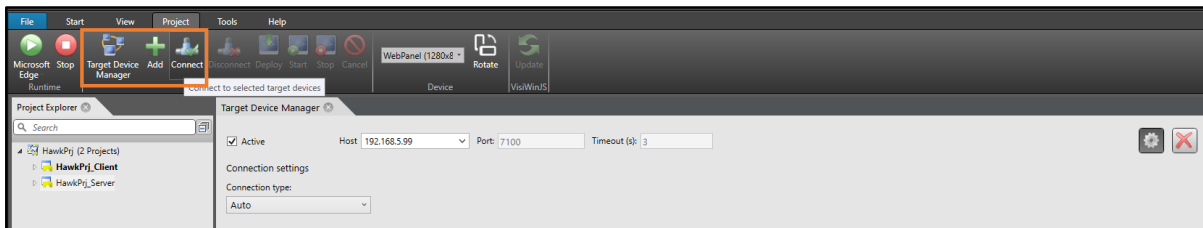
Use case 1: Disconnect from and connect to the target.

Use case 2: Close the UI-Designer Tool and start the UI-Designer Tool with this project again.

If the user activates the "Save credentials" flag, the username and the password will be saved in the Windows Credential Manager, ([Storing Credentials for Authentication](#)). On the next login, the data will be used again.

Behavior when Controller.UserManagement is not enabled

If user management is not enabled on the controller, the »EASY UI Designer« can go online without authentication. To go online to the IP address specified under host, press the "Connect" button.

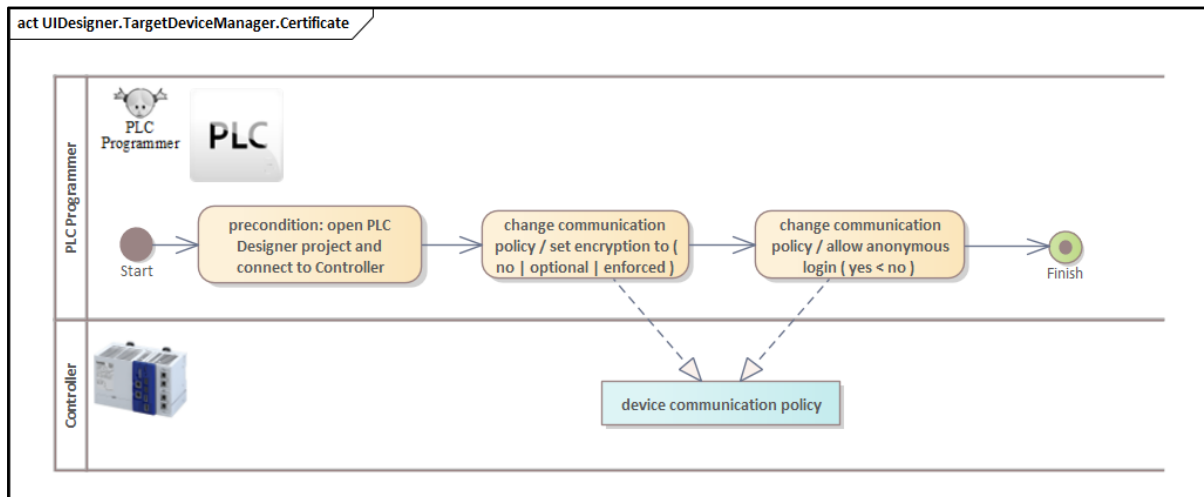


Connect without Controller.UserManagement

UIDesigner.TargetDeviceManager.Certificate

This functionality has been available since »EASY UI Designer« version 01.05.00 and controller firmware version 01.11.00.

If the controller is forcing an encrypted communication, the Target Device Manager needs a certificate handling for encryption.



Activity Diagram



For more information, see [UIDesigner.ServerManagerUI.Certificate](#).

UIDesigner.TargetDeviceManager.Authorization

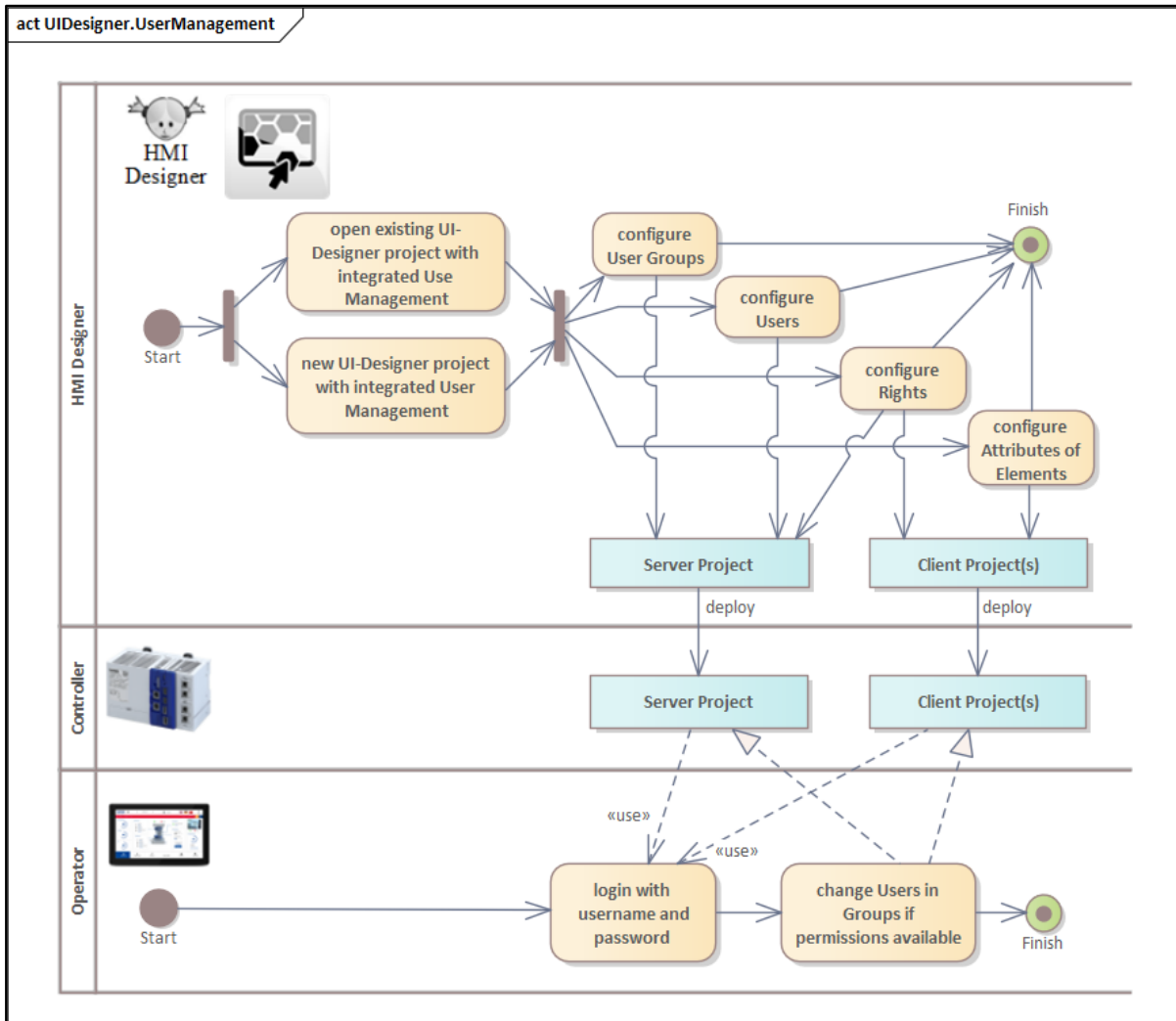
In order to configure the rights for authorization, the »PLC Designer« must be connected to the controller and the user management must be activated ([Controller.UserManagement](#)).

After activation, the user can open the device window and select the "Users and Groups" tab. The Group EasyUi already exists here. All users in this group can access the controller via the "EASY UI Designer." Selecting the "Access Rights" tab shows the configurable objects. The object "Runtime Object\Device\Remote Connections\EasyUi Interface" is intended for allocating the relevant rights.

PLC Designer right for object EasyUiInterface	EASY UI Designer right for Server Manager UI	Description of authorization
View	View	View rights are needed to connect the Target Device Manager to the controller with read-only rights.
Execute	Execute	Execute rights are needed to deploy the Client Project to the controller via the Target Device Manager.
Modify	Change	Modify rights are needed to deploy the Server Project to the controller via the Target Device Manager.
Add / Remove	Admin	Is not used.

UIDesigner.UserManagement

If user management is required for visualization, it can be created with the »EASY UI Designer« and adapted at runtime of the machine via the web panel (e.g. v450).



Activity Diagram

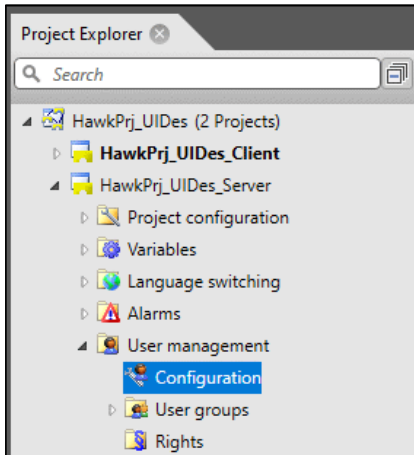
In order to be able to use the authorization within an »EASY UI Designer« project, the user management must be selected at the start wizard.

EASY UI Designer

Security functions

UIDesigner.UserManagement : Configuration

In the server project, the settings can be made under "User management" under "Configuration".



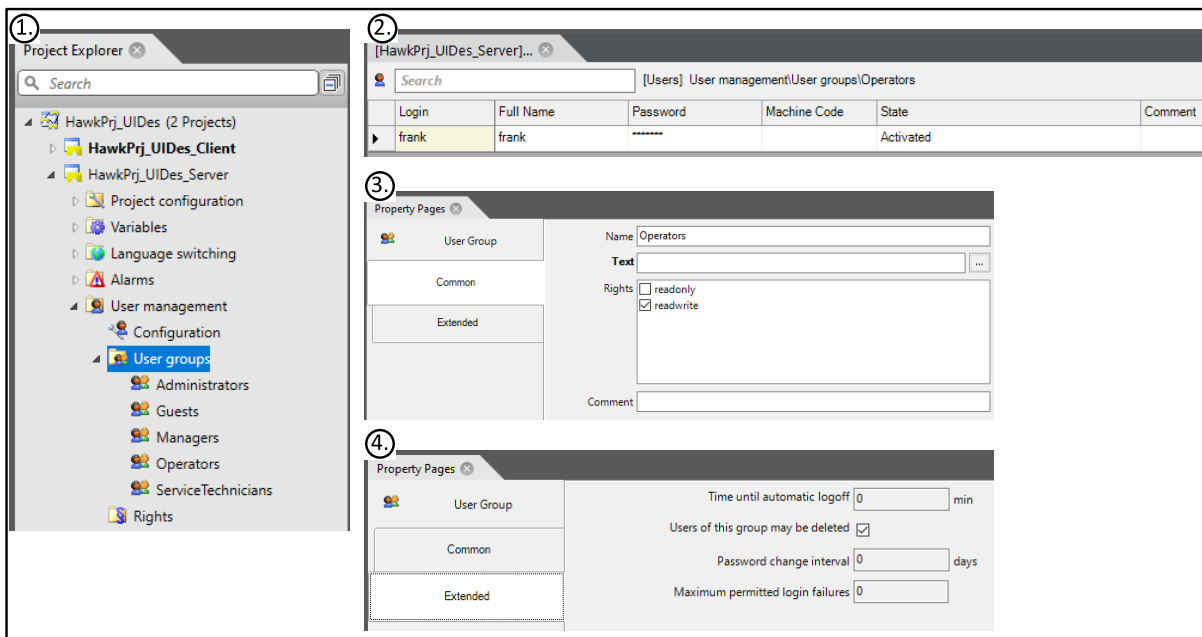
Configuration

These include the following cyber security-relevant features:

- Minimum and maximum length of user names
- Minimum and maximum password length
- Allow password reuse after time
- Allow password reuse after changes
- Minimum difference of passwords
- Maximum subsequent equal characters
- Minimum difference to prior password in characters
- Password must contain letters
- Password must contain digits
- Password must contain special characters
- Password must contain lowercase and uppercase letters
- Password must not be equal to user name

UIDesigner.UserManagement : UserGroups

If the item "User groups" is selected under the "User management" within the server project, the following representations become visible:



User groups

Default "User groups" (depending on the settings previously activated in Wizard commissioning)

The following user groups are available by default:

- Administrators
- Guests
- Managers
- Operators
- ServiceTechnicians

Setting Users

To manage individual users in the screen (refer to the previous picture (2.)) a right mouse-click results in some possibilities. A user can be specified with login and full name and receives a password. Furthermore, it can be activated or deactivated at this point.

Rights

In the screen [User groups](#) (3.) the rights of the user group are shown.

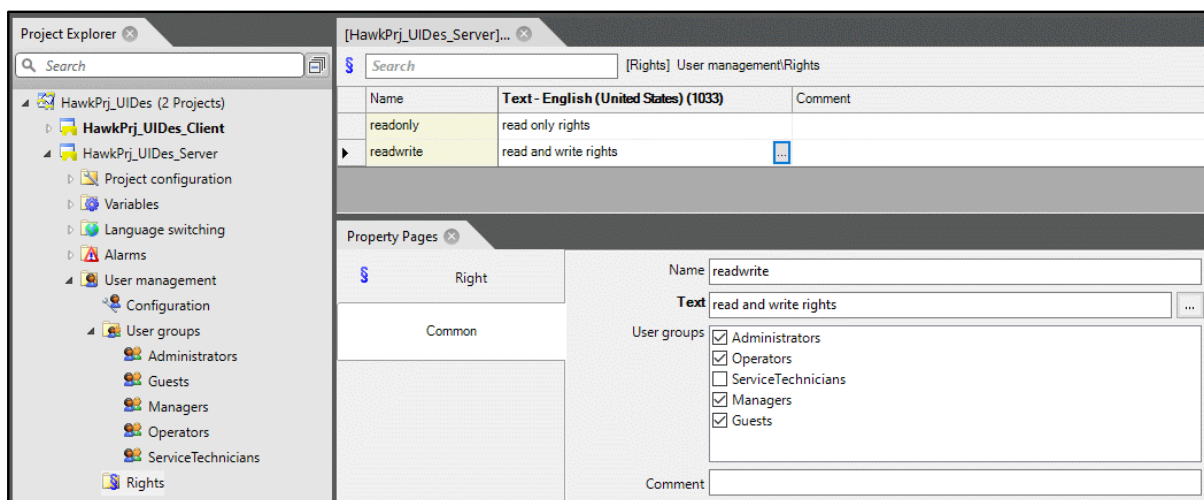
How to set these up, see [UIDesigner.UserManagement : Rights](#) (145).

UIDesigner.UserManagement : Rights

In the server project, the rights management is localized under the item "User management / Rights".

EASY UI Designer

Security functions

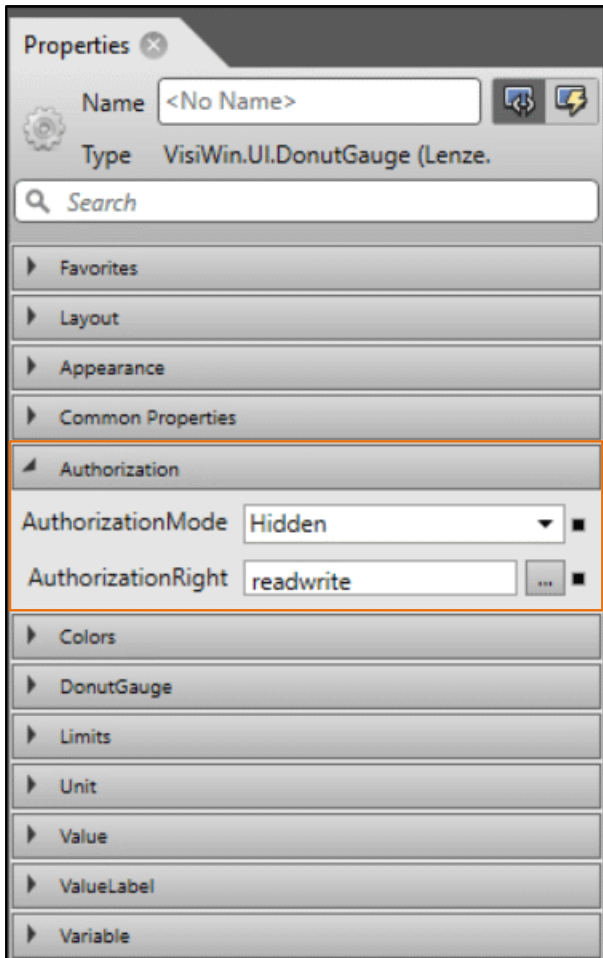


Rights

In the upper right part of the screen, rights can be created with the help of the right mouse click. In the lower right part of the screen, the user groups can be assigned to the respective rights.

UIDesigner.UserManagement : Properties of Elements

In the client project, the actual designs for visualization are defined. For each element, the properties can be set in the "Properties" menu.



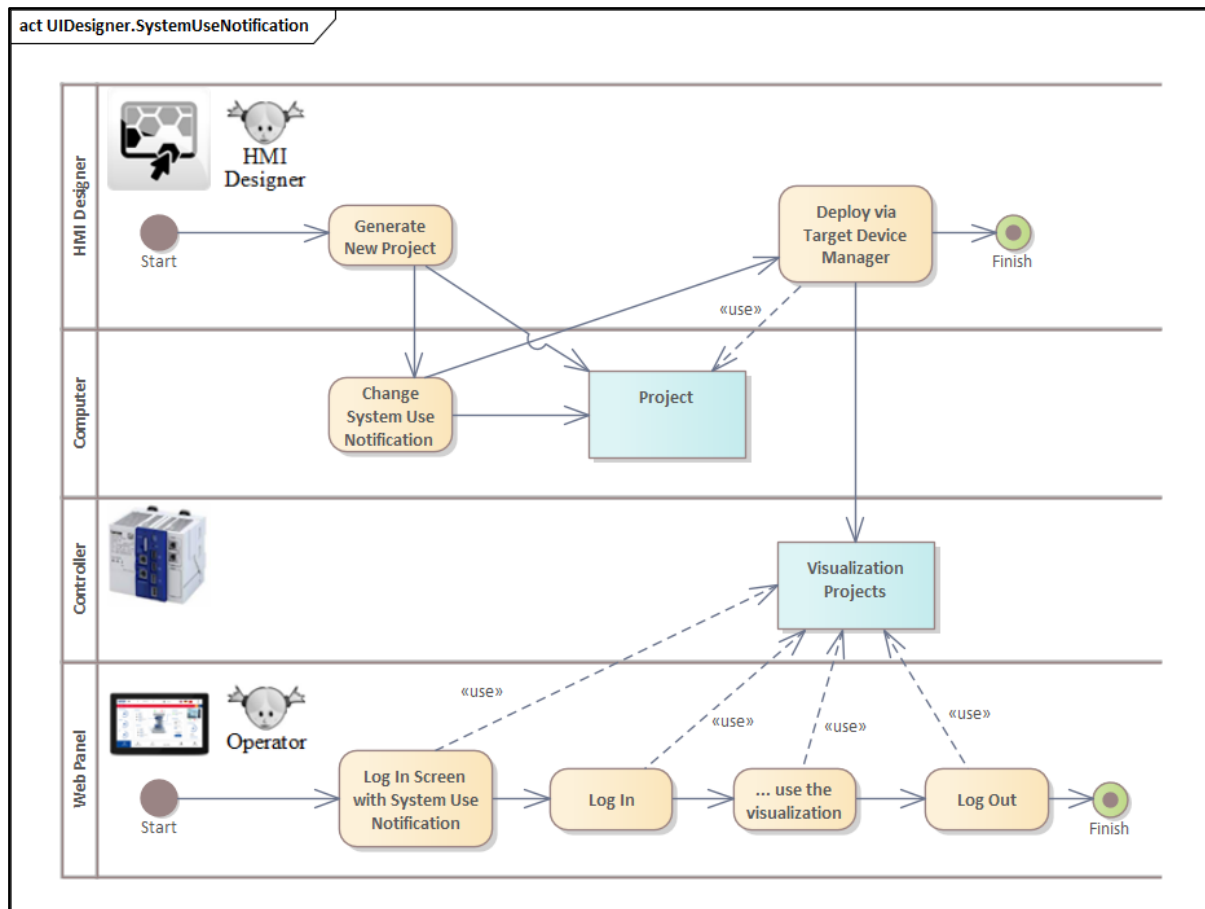
Properties of Elements

The authorization group has the following settings:

- AuthorizationMode: Disabled / Hidden / Collapse
- AuthorizationRight: <choose one of the rights of the Server Project> [UIDesigner.OPCUAClient.Authentication](#)).

UIDesigner.SystemUseNotification

The front end of the machine is visible via a web panel, e.g. the v4x0 web panel. The System Use Notification can be set using the EASY UI Designer.



Activity Diagram

Before the user logs into the visualization, the System Use Notification is visible on the log in screen. By default, the text reads:

By using this system, you consent to the monitoring of your activities and agree to comply with all security and privacy policies.

If the programmer or the HMI-designer wants to change the text, the following steps must be completed:

- Generate a new project with the EASY UI Designer and save the project.
- Right-Mouse-Click on the Client Project in the Project Explorer and choose "Open in Windows Explorer".
- In the Client Project the User will find in ./resources/languageresources directory different directory for each language, e.g. "en-US".
- In diesen jeweiligen Verzeichnissen befindet sich eine json Datei.
- Look for the name "Comment.Dialogs.UserManagement.SystemUseNotificateion" and change the value as intended.
- After deploying the Client Project to the Controller, the changes System Use Notification will be available on the Web Panel.

Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

UIDesigner.AccountManagementGuidelines

The Account Management Guidelines of the EASY UI Designer are described below.

UIDesigner.AccountManagementGuidelines :: UIDesigner.UserManagement

Default / Factory Settings:

User management for the UI Designer project can be activated during the setup of a new project.

Account Handling:

User management for the UI Designer project can be activated during the setup of a new project. Therefore, please select User Management during the Features step in the project wizard. The following accounts are automatically created by default:

- "" (user) | "Administrators" (group) | "" (password)
Please activate this group at the Wizard step during project setup and add users later in the process.
- "" (user) | "Operators" (group) | "" (password)
Please activate this group at the Wizard step during project setup and add users later in the process.
- "" (user) | "Service technicians" (group) | "" (password)
Please activate this group at the Wizard step during project setup and add users later in the process.
- "" (user) | "Managers" (group) | "" (password)
Please activate this group at the Wizard step during project setup and add users later in the process.
- "guest" (user) | "guest" (group) | "guest" (password)
Please change the default "guest" (password) at the wizard step during project setup.

Policies:

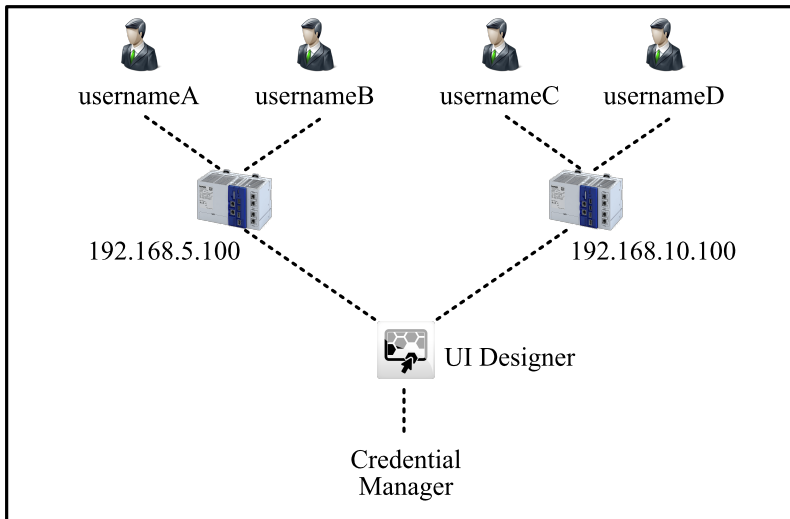
It is recommended to configure the settings for user management. This includes the following:

- When using the AutoLogon function, make sure to check for critical issues in the application. It is not recommended for use in production machines, or exclusively for testing or laboratory purposes.
- Minimum length user name = 4
- Maximum length user name = deactivated
- Minimum password Length = 4
- Maximum password length = deactivated
- Allow password reuse after x days = deactivated
- Allow password reuse after x password changes = deactivated
- Minimum difference = deactivated
- Maximum subsequent equal characters = deactivated
- Minimum difference to prior password x characters = deactivated

-
- Password must contain letters = deactivated
 - Password must contain digits = deactivated
 - Password must contain special characters = deactivated
 - Password must contain lowercase and uppercase letters = deactivated
 - Password must not be equal to user name = deactivated
 - Time until automatic logoff x min = deactivated
 - Password change interval x days = deactivated
 - Maximum permitted login failure = deactivate

Storing credentials for authentication

Referring to the security mechanisms `UIDesigner.ServerManagerUI.Authentication` and `UIDesigner.TargetDeviceManager.Authentication`, there is a function called "Stay logged in". With this function, the »EASY UI Designer« saves the login data for the users of the device to be connected in the Windows Credential Manager.

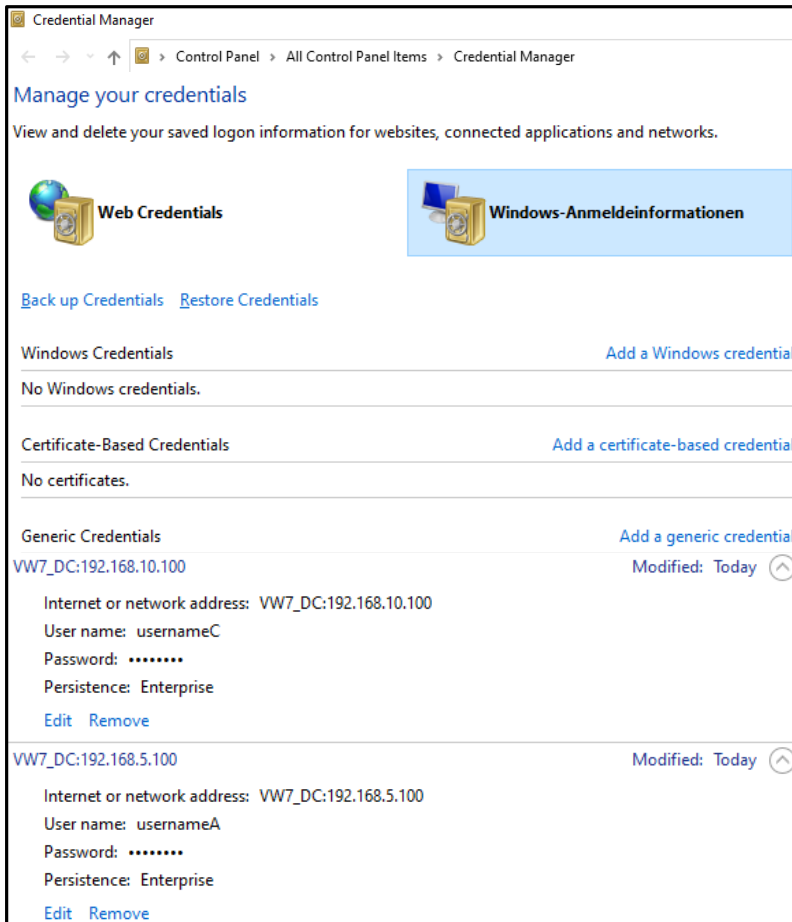


Device User Handling

EASY UI Designer

Security data

An entry is thus created in the Credential Manager for each IP address (and thus for each device) and a user can be stored with his password. If a connection is established with two devices one after the other and both activate the "Stay logged in" field, two entries are created in the Credential Manager. This can be seen in the following image which shows the two entries "VW7_DC:192.168.10.100" and "VW7_DC:192.168.5.100" and the respective users.



Credential Manager

Handling more users and the same device

If user "usernameA" is connected in the »EASY UI Designer« and "Stay logged in" is activated, its credentials are stored in the Credential Manager. If this user is logged out and a new user "usernameB" is connected to the same device in the »EASY UI Designer« and "Stay logged in" is activated, its credentials are stored in the Credential Manager and those of "usernameA" are overwritten. It is only possible to store one user per device.

Remove Credentials after Deinstallation

If the »EASY UI Designer« is uninstalled from the computer, the stored credentials remain in the Windows Credential Manager. These must be removed manually. This is done as follows:

- Call up Windows Credential Manager with "Credential Manager" in an English Windows version and "Anmeldeinformationsverwaltung" in a German Windows version.
- Call up the entry "Windows-Credential-Informationen".
- The entries with the syntax "VW7_DC:<IP address>" can be found in the "Generic Credentials" area.
- These can be opened and removed with "Remove".

Controller

This part of the documentation describes the Linux-based controller.

A distinction is made between

- Controller 1.x
The controller with firmware version 1.x.
This controller version does not yet include all security features.
- Controller 2.x
The controller with firmware version 2.x
This controller version is suitable for implementing the security features.

Controller 1.x

Product description

Controller 1.x

The controller with firmware version 1.x.
This controller version does not yet include all security features

Product description

Product identification

This documentation applies to the Controller product family and consists of the following components and their identification:

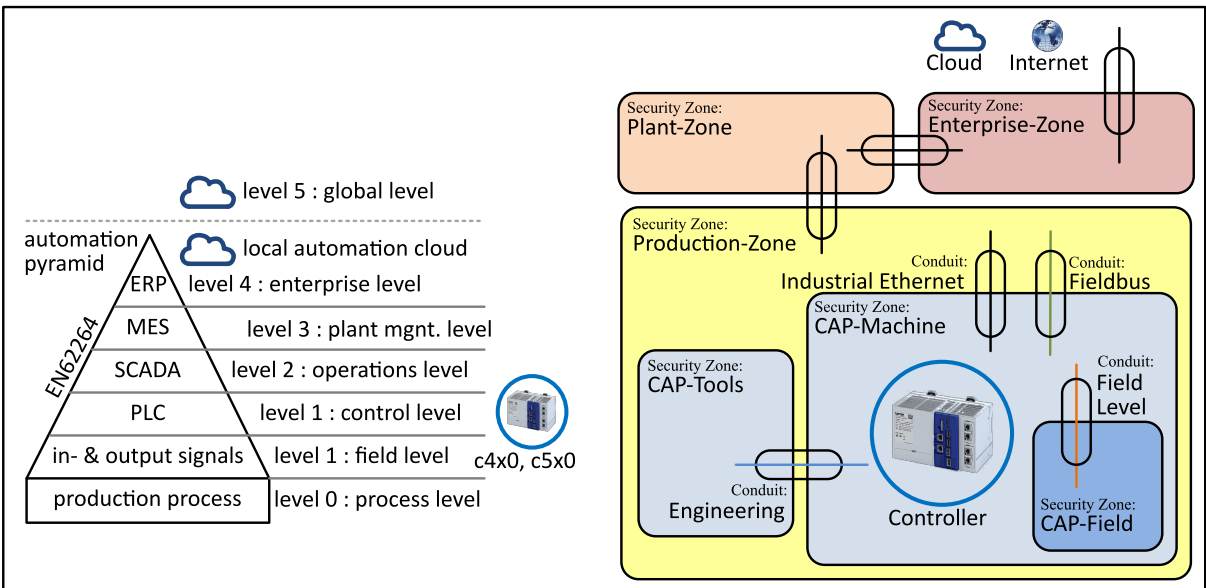
Name of product and product ID

Name of product	Product ID
c430 controller	C43AE50xxxAxxxxxxxx
c520 controller	C52AE10xxxAxxxxxxxx
c550 controller	C55AE40xxxAxxxxxxxx
c520 controller + Extended for customer - specific devices only	C52AE10xxxBxxxxxxxx C52AE10xxxCxxxxxxxx
c550 controller + Extended for customer-specific devices only	C55AE40xxxBxxxxxxxx C55AE40xxxCxxxxxxxx

This chapter describes the functions of the standard device (product ID CxxxxxxxxAxxxxxxxx) and the customer-specific variants (product IDs CxxxxxxxxBxxxxxxxx and CxxxxxxxxCxxxxxxxx). These are shown under "Controller cxx0 + Extended for customer specific - devices only" in engineering tools.

Location in the network

These components are located at the control level of the automation pyramid.. Furthermore, they are located in the security zone "CAP-Machine" [Zones and conduits](#)).



Location in the network

The components addressed here have four relevant interfaces:

- **Conduit: Industrial Ethernet**
Between the controllers and the "Conduit: Industrial Ethernet" is the IoT gateway. Its task is to enable zone protection. If there is no IoT gateway in the system, the operator must ensure appropriate security at the zone border. This interface is not an open interface for direct connection to the Internet. The operator must take appropriate security measures to maintain the security zone.
- **Conduit: Fieldbus**
Fieldbus requires special consideration within cyber security. The fieldbuses are standardized and, in most cases, have no integrated security functions. Thus, this interface must be classified as SL-0 in the risk assessment of the operator.
- **Conduit: Engineering**
This conduit does not exist continuously, but only during commissioning or maintenance of the machine. Here, the system design must take into account in the risk assessment that the accesses are authorized and the employees have been instructed on the components and the machine cyber security concept. Furthermore, it must be ensured that the computer systems on which the necessary tools are installed comply with the current cyber security requirements and correspond to the state of cyber security.
- **Conduit: Field level**
This conduit connects the security zone "CAP Machine" with the "CAP Field". The special feature is in the cyber security consideration of the field components. These are connected via the communication medium EtherCAT and thus represent only a low level of protection in terms of cyber security. The operator must therefore ensure that no unauthorized access to the components can take place. This does not include any data technology or human access. This conduit thus enables a single data interface into the subordinate "CAP Field" security zone.

Intended purpose

The intended use of these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding cyber security are discussed.

- These components are professional equipment and may only be commissioned and decommissioned by specialists.
- These components also require maintenance throughout their life cycle, which must be carried out by the operator.
- Modifications to the firmware or hardware of the components are not permitted.
- If these components are taken out of operation or disposed of, the instructions in this documentation must be observed.
- Do not fit any unused optional modules (minimize attack surface).

Intended environment

The intended environment for these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding cyber security are discussed.

- These components must be mechanically protected against unauthorized use. This can be achieved, for example, via physical access control systems or lockable control cabinets. In this case, access may only be granted to authorized persons and the number of accesses should also be restricted.

Controller 1.x

Product description

- In particular, SD Card may only be removed by users authorized by the operator.
- The components are not operated directly on the open Internet, but must also be operated by the operator via protection systems such as firewall, IDS, IPS,
- Deactivate all unused interfaces and/or protocols, both for the components mentioned here and for all components that are connected to the network.
- The more security-critical an application is, the more systems should be separated. Only combine tasks on one component if they are in the same risk classification.
- Wherever possible, use a Defense-in-Depth Concept in the environment of this component.
- Use appropriate authentication mechanisms. This applies, for example, to passwords that have the necessary complexity and an appropriate life cycle. The current state of the art must be taken into account here.
- Handle secrets, such as passwords, appropriately. The focus here is on the handling of secrets on the components noted here, but also on the data stored in the environment of these components.
- Validate all input options for validity. Pay attention to all human user interfaces as well as the machine software interfaces.
- Keep the installed firmware version up to date and install updates.
- Evaluate the environment, the technical task to be performed and the existing component security in a security-critical consideration and assess whether additional protective measures are necessary for your application.

Security key indicators

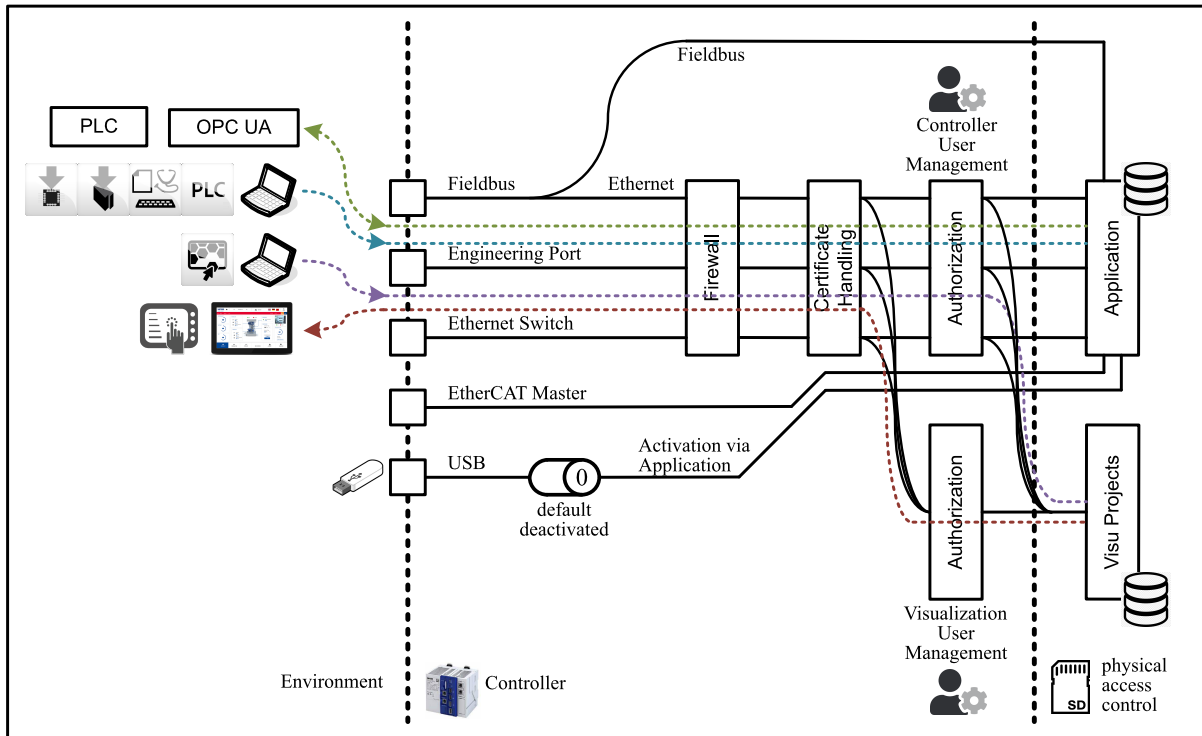
Security key indicator (in accordance with IEC 62443-4-2):

- These components are considered embedded devices (EDR).
- These components have a security level of SL-C 0.
- These components have an SL-vector from SL-C(Controller)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

Security mechanisms

Product Defense in Depth

The following image shows the defense in depth product concept. For the sake of clarity, some details have been deliberately omitted.



Product Defense in Depth

The core concept of the controller is that the Fieldbus, Engineering Port, and Ethernet Switch interfaces are assigned to two different user managements via a firewall. The Firewall minimizes the attack surface. The Certificate Handling takes over the certificate management for the respective encrypted connections.

- **Controller User Management**
Connections to the OPC UA server and client, as well as to Lenze engineering tools such as PLC Designer, EASY Starter, and UI Designer, are authorized in the context of the controller's user management. All access to the controller is viewed via this user management.
- **Visualization User Management**
Only the visualization logins run via authorization in the context of the of the user management of the visualization runtime. All access by machine operators via a web panel to the visualization projects is viewed via this user management.

Special attention must be paid to fieldbuses. Protocols based on Ethernet are routed via the firewall, and access authorizations should be minimized as much as possible. Data via the fieldbuses themselves is not routed via the cyber security functions and runs directly into the application. Protection measures must be implemented within the component's environment.

The USB interfaces are deactivated by default. It is possible to activate the USB ports from the customer's perspective. Organizational measures are necessary here.

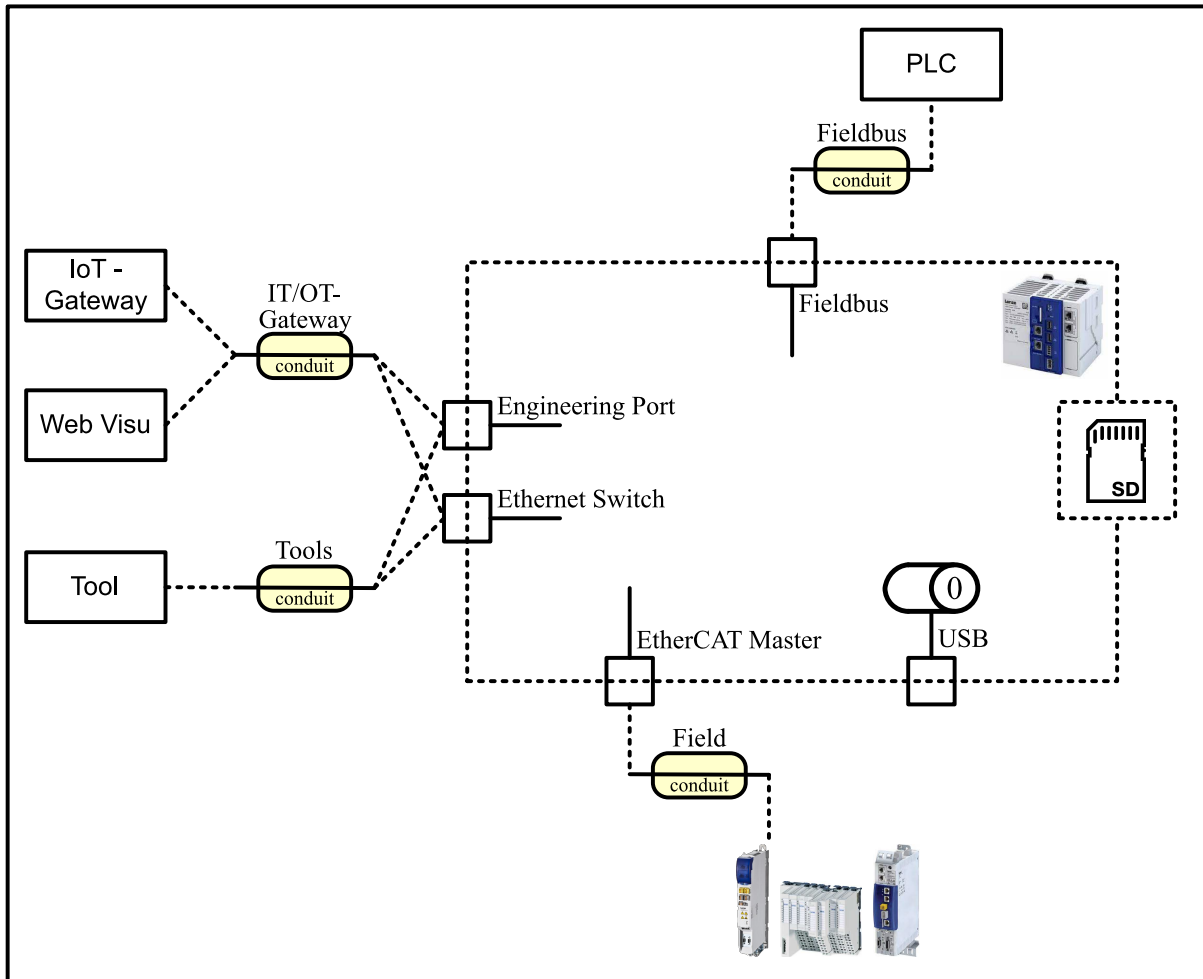
The SD card must be physically protected by an access control.

Controller 1.x

Security mechanisms

Expected Defense in Depth in the environment

The following image shows the Expected Defense in Depth in the environment of the controller.



Expected Defense in Depth in the environment

Conduit IT/OT gateway:

- An IT security-protected network environment is mandatory for operating these components. Operation on the Internet is not permitted.
- An IT/OT gateway is recommended to limit the attack surface so that only the absolutely necessary accesses and protocols are enabled.
- As these components cannot have any DoS / DDoS protection mechanisms from an embedded device perspective, these must be connected externally upstream.

Conduit Tools:

- Access from the engineering tools to the components must be limited in terms of organization and time.
- The corresponding engineering tools must be operated on an up-to-date and IT-security-secured computer.

Conduit Fieldbus:

- In most cases, the actual classic fieldbus protocol does not include any mechanisms to safeguard cyber security.
- Measures to safeguard confidentiality, integrity and availability must be provided by the customer.

Conduit Field:

- In most cases, the actual classic fieldbus protocol does not include any mechanisms to safeguard cyber security.
- Measures to safeguard confidentiality, integrity and availability must be provided by the customer.

General Environment:

- General physical access protection must be provided for the components. This applies in particular to the SD cards in the controllers.
- Existing firmware updates for the controllers as well as for all other components in the network should be installed immediately.

Security mechanisms:

The following security functions are included in the listed components:

- Controller.SFTPServer
- Controller.SSHServer
- Controller.Firewall
- Controller.UserManagement
- Controller.EncryptedCommunication.PLCDesigner
- Controller.Application.Encryption
- Controller.CertificateStore.viaPLCDesigner
- Controller.CertificateStore.viaAdvancedVisu
- Controller.CertificateStore.HAProxy
- Controller.WebDiagnosis
- Controller.OPCUAServer.Authentication
- Controller.OPCUAServer.Certificate
- Controller.OPCUAClient.Authentication
- Controller.OPCUAClient.Certificate
- Controller.ComponentDirectory
- Controller.NTP
- Controller.WebVisu.Activation
- Controller.WebVisu.Certificate
- Controller.WebVisu.UserManagement
- Controller.SysLog
- Controller.USB-Stick

Controller 1.x

Commissioning and hardening notes and organizational measures

Commissioning and hardening notes and organizational measures

The following commissioning instructions must be followed:

General instructions

- As far as possible, avoid connecting the controller to open networks or the internet. We recommend organizational and technical actions for the controller.
- For protection, additionally use data link layers such as a VPN for remote access.
- Install Firewall mechanisms, IPS (Intrusion Protection Systems) and IDS (Intrusion Detection Systems).
- Connect external devices upstream to provide protection against DoS (Denial of Service) or DDoS (Distributed Denial of Service) attacks.
- Restrict physical access to authorized persons only.
- Change existing default passwords after the first start-up and regularly afterwards. Please use only high-strength passwords.
- As soon as the web server functions of the Controller are accessed with a browser, we recommend activating the logging functions of the browser and backing up the certificate store of the browser. In this way, communication to the controller can be traced.

Commissioning and hardening instructions

- Change the key for SFTP server communication ([Controller.SFTPServer](#)).
- Be sure, that there is no ".enable-ssh" file on the SD card for SSH access ([Controller.SSHServer](#)).
- Change the settings of the controller firewall for hardening the component ([Controller.Firewall](#)).
- Activate and use the user management ([Controller.UserManagement](#)).
- Change the standard EngineeringItf-User-Password ([Controller.UserManagement: EngineeringItf](#)) or delete this standard user.
- Prevent the deletion of the user management on the SD card via an organizational measure ([Controller.UserManagement](#)).
- Activate the function "Encrypted Communication" ([Controller.EncryptedCommunication.PLCDesigner](#)).
- Activate encrypted application to secure the application on the controller ([Controller.Application.Encryption](#)).
- Handle the certificates in the programming phase of the machine with the »PLC Designer« ([Controller.CertificateStore.viaPLCDesigner](#)).
- Handle the certificates in the production phase via the Diagnosis Visu ([Controller.CertificateStore.viaAdvancedVisu](#)).
- Change the credentials for the WebDiagnosis ([Controller.WebDiagnosis](#)).
- Change the communication to the web visualization to https ([Controller.CertificateStore.HAProxy](#)).
- When using the OPC-UA Server, please use the authentication ([Controller.OPCUAServer.Authentication](#)) and the certificate handling ([Controller.OPCUAServer.Certificate](#)).
- When using the OPC-UA Client, please use the Authentication ([Controller.OPCUAClient.Authenticatice](#)) and the certificate handling ([Controller.OPCUAClient.Certificate](#)).
- Activate and test the component directory at the controller ([Controller.ComponentDirectory](#)).
- Activation and configuration of the NTP client ([Controller.NTP](#)).
- When using the WebVisu in the extended controller variant, please harden the communication and the web server ([Controller.WebVisu.Activation](#)) and the ([Controller.WebVisu.Certificate](#)) and the ([Controller.WebVisu.UserManagement](#))
- Activate the SysLog functionality for logging security relevant events ([Controller.SysLog](#)).
- Do not activate the USB stick functionality. This will deactivate the security functionality.
- When setting the USB stick parameter to "once for a restore/update" make sure that the functionality is used immediately.

Periodic security maintenance

- It is recommended to check the password policy periodically for updates and to adjust the requirements if necessary.
- It is recommended to change the passwords cyclically.
- It is recommended to check the certificates used with regard to their key lengths for up-to-dateness and to generate new certificates with higher key lengths if necessary.
- It is recommended to exchange the certificates regularly.

Controller 1.x

Commissioning and hardening notes and organizational measures

Decommissioning instructions

- The device command 0x2022:001 "Device command: Load Lenze settings" must be executed. This resets all application settings.
- It is recommended to update the firmware using the EASY Firmware Loader.
- Remove the SD card and format it (in order to retain the Application Credits, the corresponding data must first be memorized and restored on the formatted SD card).

Removal product from environment

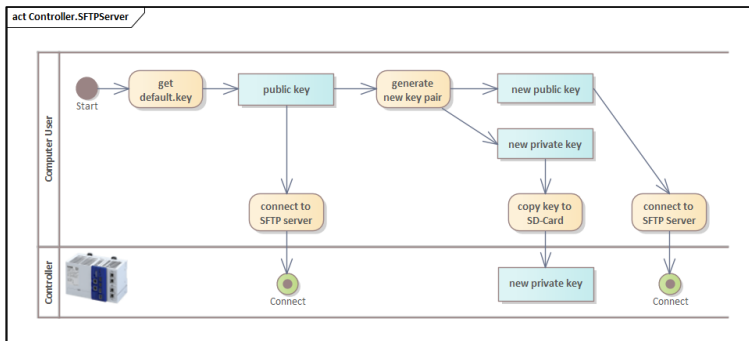
- It is recommended that all industrial communication partners of the controller to be removed, to change the trusted certificates of the controller into untrusted certificates.
- It is recommended to securely remove the login data for the controller to be removed, and such as name and password for the necessary authentication, from all industrial communication partners.

Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

Controller.SFTPServer

With this functionality, some parts of the file system (e.g. the SD card) can be accessed via Ethernet.



Activity Diagram

Physical and logical access

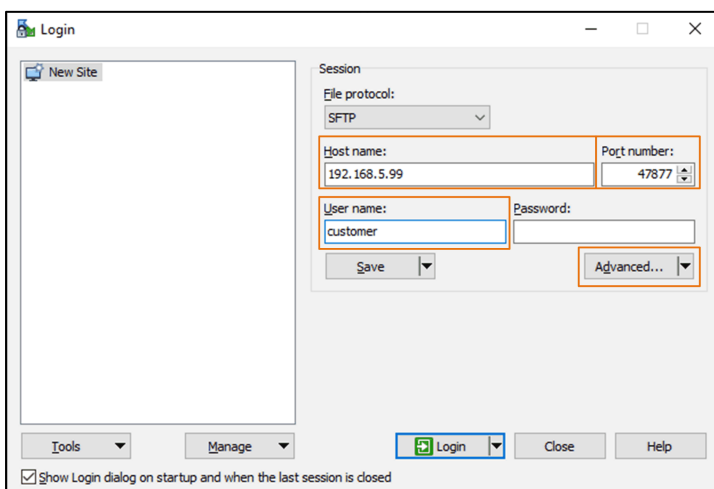
- Connector X16 (Engineering Access)
- Connector X256/X257 (fieldbus device)
Only if a fieldbus (e.g. PROFINET device) is included in the device tree of the controller in the »PLC Designer« and the IP-configuration 0x2381 is set in the parameter set.
- Used port for SFTP is 47877/tcp

Controller.SFTPServer: Access to the SD card

Access to the file system via SFTP is available since FW Version 01.03.00.

A suitable SFTP client has been required for this access. In the following, for example, WinSCP (<https://winscp.net>) is used.

Start WinSCP and insert the necessary data, as shown in the following picture.



Controller 1.x

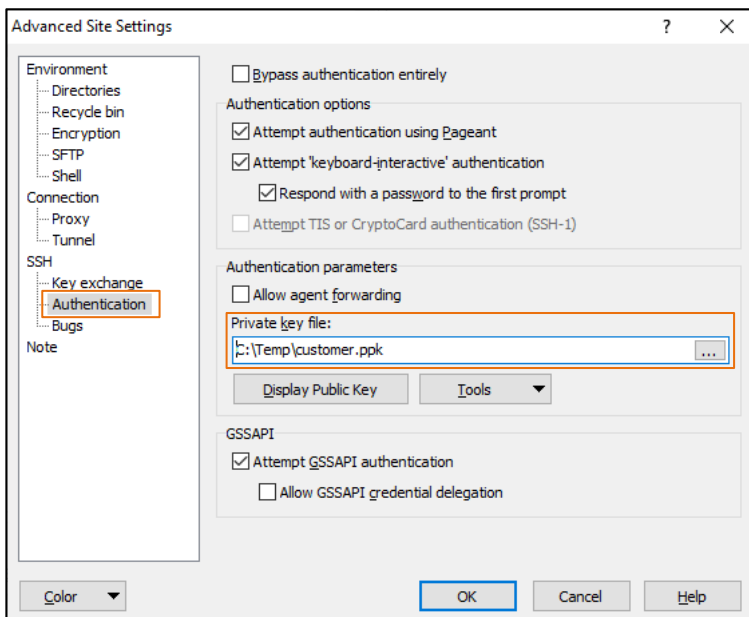
Security functions

WinSCP Login

Insert the following data

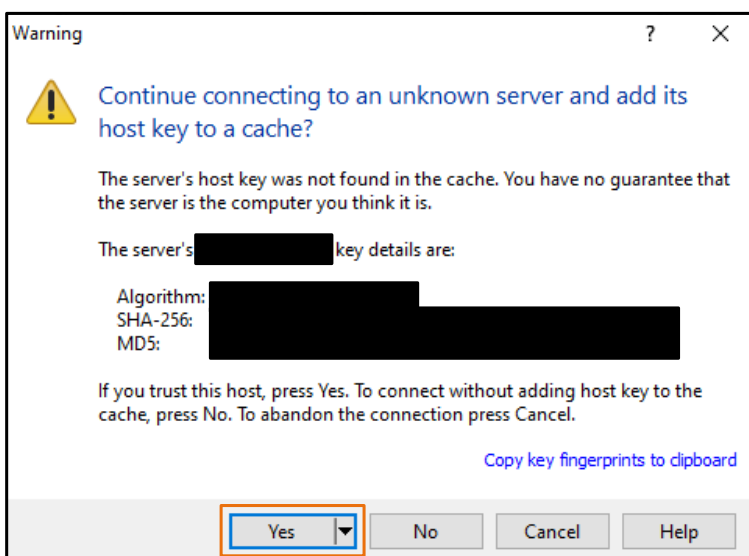
- File protocol: SFTP (communication protocol)
- Host name: IP adress of the controller
- Port number: SFTP-Port number of the controller (c4x0 and c5x0 uses port 47877)
- User name: customer
- Password: keep this password empty

Next, the Advanced dialog must be used. A *.ppk file is needed to insert the private key file into the menu/authentication window. You can find the file in the Lenze internal AKB (document ID 201800294). Please contact Lenze Support.



Insert customer.ppk key-file

After accepting the following warning, the /userData path can be accessed in the controller.



Agree Warning

Controller 1.x

Security functions

Controller.SFTPServer: Changing the customer.ppk

Changing the customer.ppk has been available since FW version 01.04.00.

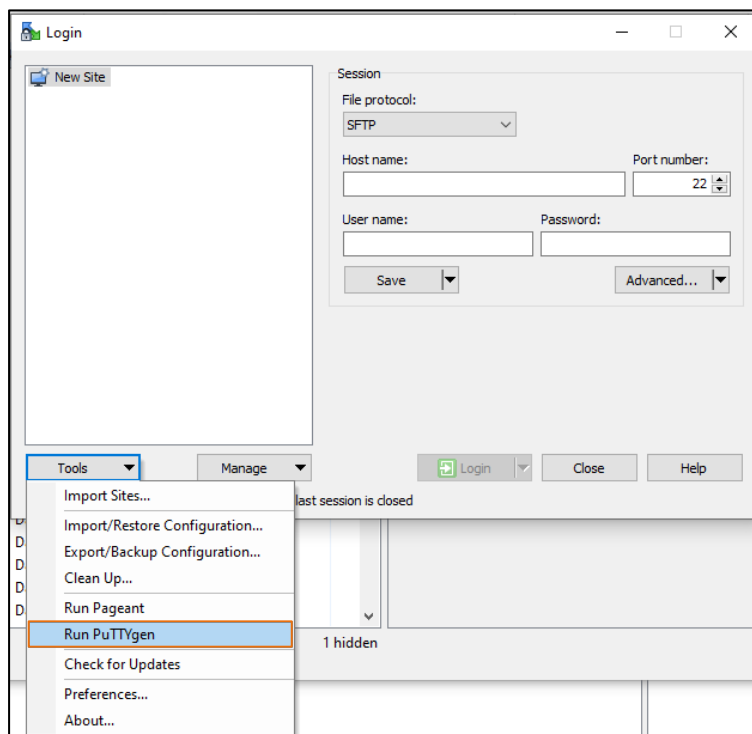
This description is necessary when individualizing the access key (customer.ppk) for SFTP access to the controllers. To do so, a separate key must be generated. Note that resetting a key in the controller can only be carried out by the Lenze service once it has been changed. Therefore, great care must be taken when storing and archiving a new key. A private key that has been changed can be found in a controller backup and will become active automatically during a restore on a new device.

Constraints on the key

- RSA
- minimal length of 2048 Bits

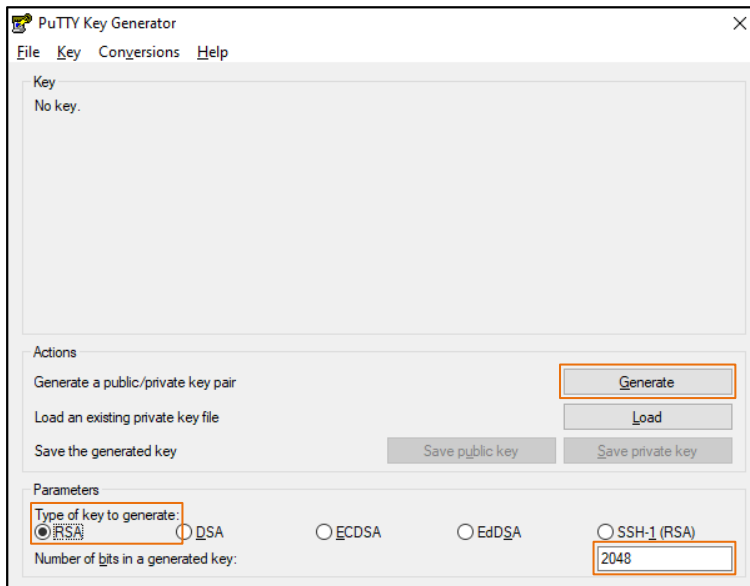
Generate a new key

1. After starting the WinSCP program, press the "Tools" button "Login" dialog that opens automatically. In the menu that appears, the entry "Run PuTTYgen" is selected to start the PuTTYgen program. PuTTYgen is responsible for the key generation. Note: The "Run PuTTYgen" option is not visible when using WinSCP Portable. Please use Setup WinSCP.



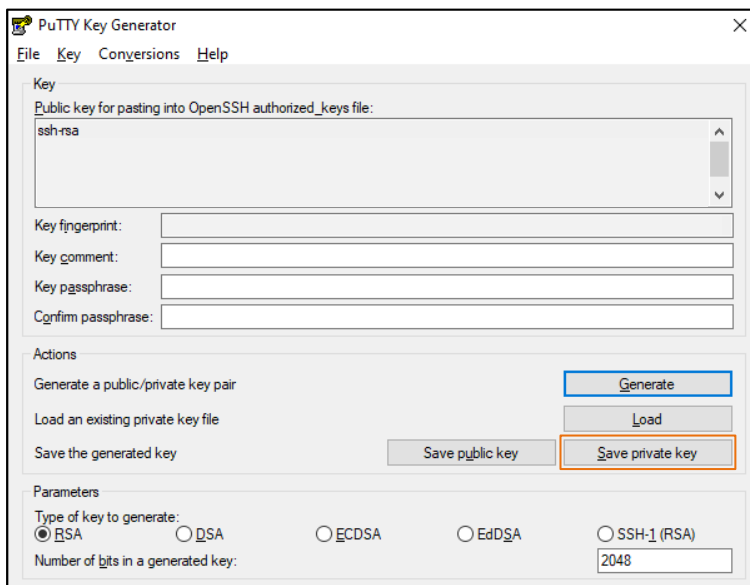
WinSCP using Tools / Run PuTTYgen

2. In PuTTYgen, the key type (RSA) and the key length in bits (minimum 2048) are set. Pressing the "Generate" button generates the new key pair.



PuTTY Key Generator

3. After creating the key, you can enter a comment before saving it. A password, or "passphrase," can also be set, depending on the application. It should be noted that the passphrase must be entered on the PC every time the private key is used. Now, the private key can be saved for later use by selecting "Save private key."

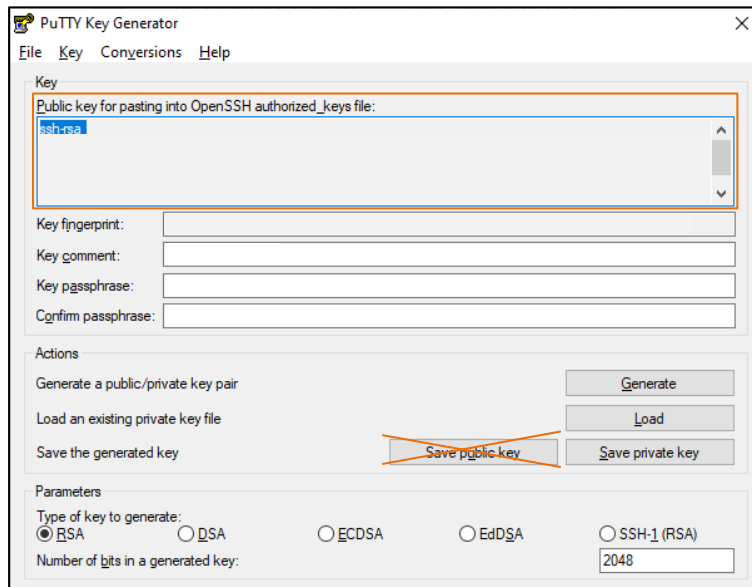


PuTTY Key Generator: Save Private Key

Controller 1.x

Security functions

4. To make this private key accessible to a device, copy the contents of the text box labeled "Public key for pasting into OpenSSH authorized_keys file" and save them in an ASCII text file named "customer.key." Ensure that the contents are not altered; they are a single long line. Note: The file created with "Save public key" cannot be used. To obtain the "public key," copy the text as described above.



Safe Public Key

Generate a new private key in the controller

1. The "customer.key" file must be on the device's SD card in the existing "public-key" directory. For security reasons, this directory can only be accessed via SFTP, so the file must be copied to the SD card from a PC, for example.
2. The currently active private key establishes an SFTP connection to the device.
3. The "customer.key" file is now stored via SFTP in the device in the "/tmp/user_data" directory.
4. The storage process is registered by the device; as a result, the transferred file is stored and checked for correctness:
 - On the SD card, an identical file called file. key must be placed under "public-key/-customer.key".
 - The file may contain only one line with an RSA key (empty lines are ignored).
 - The line with the RSA key must withstand rough validation.
 - The RSA key must be at least 2,048 bits long.No matter what the result of the checks is: The file "/tmp/user_data/customer.key" is automatically deleted from the device.
If a check is not successful, the "/tmp/user_data" directory generates a file called "customer.key.ret" with a corresponding error message.
Possible error messages:
 - unable to read "/sdcard/public-key/customer.key"
 - "/tmp/user_data/customer.key" does not match "/sdcard/public-key/-customer.key"
 - RSA-key required
 - not a valid RSA-key
 - RSA-key of at least 2048 bits required
5. After successful transfer of the file "customer.key", the current SFTP connection must be disconnected and a new SFTP connection must be established using the new private keys. If this fails, it must be checked that the transferred file "customer.key" belongs to the new private key used.
 - the transferred file "customer.key" has been created and saved correctly.
 - the private key used has been saved correctly.If all of these steps are successful, the new private key can be used for future SFTP connections to the device.

Information on handling

- The new key will continue to work if the SD card is changed or deleted.
- Via a "backup" (0x2022:40) and SD card exchange, the key can be transferred to another device.

Controller.SFTPServer: Security functionality verification

Change to the SD Card and delete the "customer.key" file on it. Then, plug the SD Card into the PLC and start it.

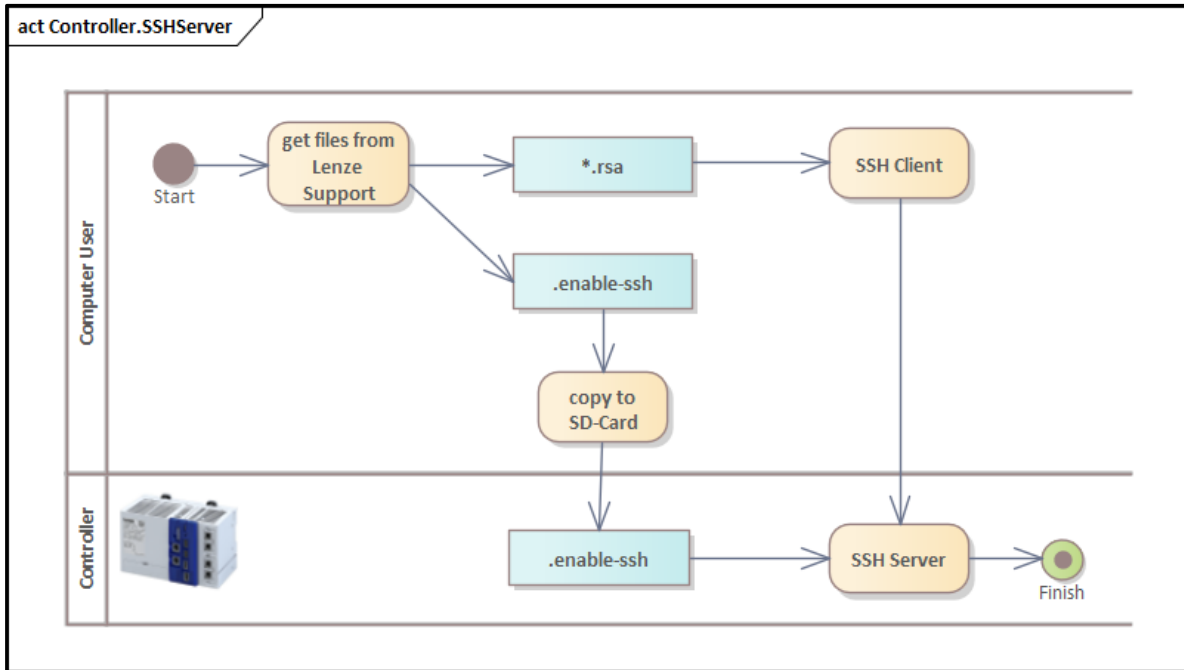
Start an SFTP client such as WinSCP. Try to login. If the security functionality works correctly, no connection will be established.

Controller 1.x

Security functions

Controller.SSHServer

Access to the file system via SSH has been available since FW version 01.04.00. This functionality allows you to access the file system via Ethernet. A SSH key is needed to access the device. Lenze Support generates this key only in special support cases and it should not be used during normal operation.



Activity Diagram

You will receive two files from Lenze Support.

- .enable-ssh
- *.rsa

Both files are personalized for the requester and must be protected accordingly. Do not share or publish these files.

Physical and logical access

- Connector X16 (Engineering Access)
- Used port for SSH is 22/tcp

Controller.SSHServer: Enable SSH access

In order to obtain SSH access to the controller, the following steps must be completed.

- SSH access is not possible in the delivery state. Lenze Support generates this key only in special support cases, and it should not be used during normal operation.
- The .enable-ssh file must be copied to the controller's SD card. Ensure that the leading dot (hidden file in Linux) is included in the file name. The file should be placed directly in the root directory of the SD card.

The following describes how access the controller with a Linux Ubuntu system. Other clients may have a different procedure.

- Copy the *.rsa file to the /home/<user>/.ssh/ directory.
- If the directory does not yet exist, it must be created and provided with the appropriate rights:

- ```
mkdir -p ~/.ssh
```

- ```
chmod 0700 ~/.ssh
```

- The access rights to the file must be adjusted accordingly:

- ```
chmod 0600 <*.rsa>
```

- The key must be added to the ssh:

- ```
ssh-add ~/.ssh/<*.rsa>
```

- After that, the SSH access to the controller can be created with the following command:

- ```
ssh root@<ip>
```

## Controller.SSHServer: Disable SSH access

Remove the .enable-ssh file from controllers SD card.

# Controller 1.x

## Security functions

### Controller.SSHServer: Combination of SSH and SFTP via Ports and Networks

The following table shows the possibility of using SSH and SFTP over the existing ports and over the possible networks. This representation refers to a disabled controller firewall.

Combination of SSH and SFTP via different Ports and Networks:

| Device with Interface                                                                        | Port  | With .enable-ssh file                                                               |                                                                                     |                                                                                     | Without .enable-ssh file                                                 |                                                                          |                                                                          |
|----------------------------------------------------------------------------------------------|-------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|
|                                                                                              |       | c550                                                                                | c520                                                                                | c430                                                                                | c550                                                                     | c520                                                                     | c430                                                                     |
| Engineering<br>c550: X16 onboard<br>c520: X16 onboard<br>c430: X16 onboard                   | 22    | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            |
|                                                                                              | 31855 | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            |
|                                                                                              | 47877 | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP |
| PROFINET Device<br>c550: X257/X258 in E1<br>c520: X257/X258 in E1<br>c430: X396/X397 onboard | 22    | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP                       | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP                       | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP                       | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            |
|                                                                                              | 31855 | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP                       | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP                       | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP                       | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            |
|                                                                                              | 47877 | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP |
| Switch<br>c550: na<br>c520: na<br>c430: X396/X397 onboard                                    | 22    | n.a.                                                                                | n.a.                                                                                | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | n.a.                                                                     | n.a.                                                                     | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            |
|                                                                                              | 31855 | n.a.                                                                                | n.a.                                                                                | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | n.a.                                                                     | n.a.                                                                     | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            |
|                                                                                              | 47877 | n.a.                                                                                | n.a.                                                                                | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | n.a.                                                                     | n.a.                                                                     | <input type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP |

.enable-ssh      Mechanism as described in chapter [Controller.SSHServer](#): Enable SSH-Access  
☒      Possible  
☐      Not possible

### Controller.SSHServer: Security functionality verification

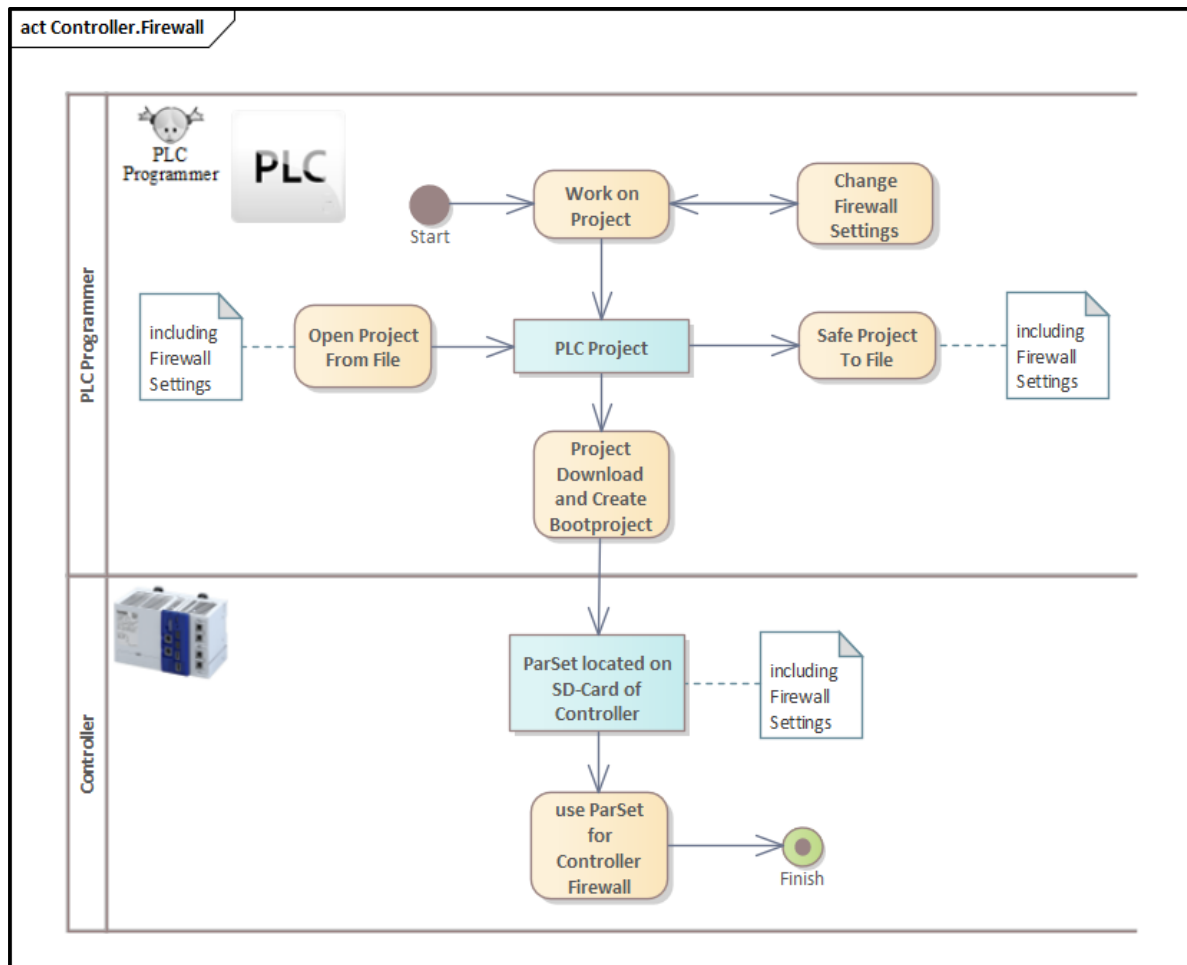
To verify that SSH access is functioning correctly, first establish an SSH connection to the PLC as described in the chapter titled "Controller.SSHServer: Enable SSH Access." After establishing the correct connection, disconnect and switch to offline mode. Then, delete the .enable file on the controller's SD card and try to connect. The connection will not establish.

## Controller.Firewall

The functionality of the Controller Firewall is available since FW Version 01.09.00. The firewall refers exclusively to the Engineering Port X16 and not to the fieldbus interfaces.

Since Firmware Version 01.11.00 the Controller Firewall is also available for Profinet and the dual network.

The »PLC Designer« is used to put the controller firewall into operation and to parameterize it. A general procedure can be found in the following picture.



Activity Diagram

### Controller.Firewall: Configuration

This chapter describes the parameter configuration of the Controller Firewall.

### Controller Firewall Configuration Data

The configuration data of the Controller Firewall is stored in the parameter set of the controller. The individual setting options are mapped to individual indexes, subindices, bitcoding or enumerations. The index range extends from 0x5910 to 0x5913. This parameter set can be parameterized with the help of the »PLC Designer« and is part of the »PLC Designer« project. Likewise, the parameter set is part of the project, which is transferred to the controller. The parameter set is located on the SD card of the controller.

During commissioning, additional measures must be taken to protect this parameter set from unauthorized modification. Therefore, when commissioning a machine, it is necessary to consider and evaluate the individual communication channels from a cyber security point of view. Examples include the following:

- (a) changes made with the "EASY Starter";
- (b) changes made via SSH;
- (c) changes made via SFTP; and
- (d) others.

Furthermore, the SD card must be protected from removal because the data on it can be accessed and modified with any SD card reader. Therefore, it is recommended that the operator mechanically protect the control cabinet from unauthorized use.

|   |               |   |   |   |   |   |   |          |   |          |
|---|---------------|---|---|---|---|---|---|----------|---|----------|
| I | protocol name | I | 0 | - | I | 0 | I | None [0] | I | Drop [0] |
| I | protocol name | I | 0 | - | I | 0 | I | None [0] | I | Drop [0] |
| I | protocol name | I | 0 | - | I | 0 | I | None [0] | I | Drop [0] |
| I | protocol name | I | 0 | - | I | 0 | I | None [0] | I | Drop [0] |

### Settings Dialog for the Controller.Firewall

# Controller 1.x

## Security functions

---

### Parameters for the Controller Firewall

The parameter concept contains four indexes:

- 0x5910: Basic parameters for the Controller Firewall, which apply generically
- 0x5911: Well-Known Port Settings (Ports 1 bis 1.023)
- 0x5912: Registered Port Settings (Ports 1.024 – 49.151)
- 0x5913: Application Port Settings

All four areas are described below.

#### Basic parameters for the Controller Firewall 0x5910

In the default settings, the firewall is deactivated. This is necessary for compatibility reasons with older versions. You can activate it with parameter 0x5910:001.

| Address    | Name                          |             | Info                                |
|------------|-------------------------------|-------------|-------------------------------------|
| 0x5910:001 | Firewall: Firewall activation |             |                                     |
|            | 0                             | Deactivated | Controller Firewall is deactivated. |
|            | 1                             | Activated   | Controller Firewall is activated.   |

The following setting option affects the IP clients that want to access the controller. The IP address ranges of the clients are specified here.

## Example:

If 0x5910:002 and 0x5910:003 are parameterized as 192.168.5.100 and 192.168.5.120, respectively, then the range of IP addresses is allowed. For example, a client with an IP address of 192.168.5.110 could access the network, but a client with an IP address of 192.168.5.90 or 192.168.5.130 could not. You can also select the same start and end addresses to allow only one IP address. Four IP ranges are offered to allow setting IP clients on different networks separately. The parameters for IP client addresses are:

| Address                                              | Name                              | Info                                                                             |
|------------------------------------------------------|-----------------------------------|----------------------------------------------------------------------------------|
| 0x5910:002<br>0x5910:004<br>0x5910:006<br>0x5910:008 | Firewall IP Range: IP Range Start | Start of IP-Range for the IP-Clients<br>Range 1<br>Range 2<br>Range 3<br>Range 4 |
| 0x5910:003<br>0x5910:005<br>0x5910:007<br>0x5910:009 | Firewall IP Range: IP Range End   | End of IP-Range for the IP-Clients<br>Range 1<br>Range 2<br>Range 3<br>Range 4   |

Please remember that, at this point, only the limits of the IP address ranges of the clients are set. The selection and activation take place for the individual protocols. These IP addresses apply to all protocols and are therefore generic.



Setting the IP ranges for clients only affects the engineering port and the switch as a network. Clients on the fieldbus are not considered in terms of their IP addresses.

# Controller 1.x

## Security functions

### Parameters for the Well-Known Port Settings (Port 1 – 1,023)

The firewall settings are stored in the device parameter set. Below the index is the range of subindices. The subindex range is divided into blocks of 10 subindices each. Each block contains parameters for each possible protocol. There are three setting options for each protocol (other subindices are reserved):

| Address    | Name                                 |                  | Info                                             |
|------------|--------------------------------------|------------------|--------------------------------------------------|
| 0x5911:xx1 | Firewall <protocol>: Network         |                  |                                                  |
|            | 0                                    | Engineering Port | Engineering Port via X16                         |
|            | 1                                    | Profinet         | Profinet                                         |
|            | 2                                    | Dual Network     | Dual Network                                     |
| 0x5911:xx2 | Firewall <protocol>: Client IP Range |                  |                                                  |
|            | 0                                    | Any              | All Client-IP-Addresses are allowed.             |
|            | 1                                    | IP Range 1       | IP Range 1 defined in 0x5910:002 and 0x5910:003. |
|            | 2                                    | IP Range 2       | IP Range 2 defined in 0x5910:004 and 0x5910:005. |
|            | 3                                    | IP Range 3       | IP Range 3 defined in 0x5910:006 and 0x5910:007. |
|            | 4                                    | IP Range 4       | IP Range 4 defined in 0x5910:008 and 0x5910:009. |
| 0x5911:xx3 | Firewall <protocol>: Activation      |                  |                                                  |
|            | 0                                    | Drop             | Deny Connection without notifying the Sender.    |
|            | 1                                    | Reject           | Deny Connection with notifying the Sender.       |
|            | 2                                    | Allow            | Allow Connection                                 |

As mentioned above, these options are available for each protocol.

### Parameters for the Registered Port Settings (Ports 1,024 – 49,151)

The subindex range is divided into blocks of 10 subindices each. Each block contains the parameters for each possible protocol. For each protocol there are three setting options that correspond to the setting options of the well-known ports.



### Parameters for the Application Port Settings (Ports 49,152 – 65,535)

In contrast to the previously mentioned ports, it is not possible to perform a factory default setting for the application ports. This is due to the dynamic use of e.g. sockets in the IEC application. This may make it necessary to open additional ports in the firewall. This is precisely what the application ports are designed to do.

The special feature here is that the required protocols behind the ports are unknown and are only defined by the application. In this respect, further setting options are necessary, which are explained below. These setting options are additional. Each protocol still contains the three subindices for Network, Client IP Range and Activation.

In addition, there are four additional parameters for each application port:

| Address    | Name                       | Info                            |
|------------|----------------------------|---------------------------------|
| 0x5911:xx7 | Firewall: Protocol Type    |                                 |
|            | 0                          | None                            |
|            | 1                          | TCP                             |
|            | 2                          | UDP                             |
|            | 3                          | TCP&UDP                         |
| 0x5911:xx8 | Firewall: Port Range Start |                                 |
| 0x5911:xx9 | Firewall: Port Range End   |                                 |
| 0x5910:x10 | Firewall: Protocol Name    |                                 |
|            |                            | Help note for the protocol name |

The user can open an application port with these parameters:

#### 0x5910:x10 Protocol Name

This parameter is only available to give the firewall rule a name. Here, the customer can to assign a name, which is stored in the parameter set and then displayed on the interface of the tool. This name is not relevant to the actual function.

#### 0x5910:xx8 Port Range Start and 0x5910:xx9 Port Range End

These two parameters can be used to set the port range of the firewall rule. In special cases where start and end are the same, one single port is addressed. By default, the port range 49,152 to 65,535 is set here. This is the range where customers should put their ports. However, these parameters can range from 1 to 65,535. This means that by adjusting the parameters accordingly, values in the ranges of the well-known or registered ports are also possible. Only port 0 is prohibited and is outside the addressable range.

Customers may select a port for the application ports, that is already listed as a well-known or registered ports. If the rules for the application port and the well-known or registered port contradict each other, the rule for the well-known or registered ports leads.

# Controller 1.x

## Security functions

---

### 0x5911:xx7 Protocol Type

This parameter can be used to set the log type of the rule. The following settings are offered:

- None  
The firewall rule does not refer to any protocol and is therefore inactive.
- TCP  
The firewall rule applies to TCP protocols.
- UDP  
The firewall rule applies to UDP protocols.
- TCP&UDP  
The firewall rule applies to both UDP and TCP protocols.

### Controller.Firewall: Good to know ...

This chapter discusses some topics that are relevant for the controller firewall.

### Validity of Controller Firewall parameters

The prerequisite is a controller with an executable application. For this purpose, a boot application must be created. Restart the controller. With this configuration, it is possible to describe any parameter of the controller Firewall and it is effective immediately. This can be ideally used to test firewall settings. These changes can be saved using the command "Save parameter sets..." so that they are available again after a restart.

### Handling IP-Ranges

The controller checks the IP range for admissibility in the settings. Among other things, it verifies that the upper value must be greater than the lower value. As a result, the upper value must be entered first, followed by the lower value.

### Exclude from the controller

You can deactivate the currently used protocol and the currently used communication channel which will exclude you from access. There are three workarounds that can be used.

1. Connect via a different communication channel or protocol and reopen the previously closed port.
2. Connect via a different communication channel or protocol and deactivate the complete Controller Firewall.
3. Remove the SD card and delete the parameter set regarding the project and reinstall it.  
**Note:** The parameter set that contains the parameters of the firewall is located on the SD card under /plc/prg/PlcParameterSet/PLC\_0\_0.pprm.

### Handling of the parameter set:

Since the Controller Firewall parameters are part of the parameter set, they are subject to the same mechanisms for the parameter set itself. This means that they are part of the »PLC Designer« project and the Application Loader Package. They are displayed in difference lists and can also be used and changed by the »EASY Starter« if it has passed authentication for the controller.

## Philosophy of Default Assignment

The philosophy for the default assignment of the Controller Firewall parameters is as follows:

Rules for the ports:

1. By default, the Controller Firewall is deactivated and must be activated.
2. In general, all ports are closed by default and must be opened.
3. An exception are the ports for a »PLC Designer« at the interface of the engineering port.
4. An exception are the ports required for the production of the components.

## Prioritization of Controller Firewall Rules

The rules of the Controller Firewall are applied as follows:

1. All ports are closed.
2. The ports in the Well-Known area are opened according to the settings.
3. The ports in the Registered area are opened according to the settings.
4. The ports in the Application area are opened according to the settings.
5. If the settings of the first two areas contradict the application area settings, the settings of the first two areas take precedence.

## Using http via Port 80 or via Port 8080

Since http is no longer the state of the art from a security point of view, the http ports are no longer displayed in the firewall. If the http ports are required, two options are available:

- Applications must be switched from http with port 80 or port 8080 to https with port 443. An example is the connection of the visualization. For a corresponding description see [UIDesigner.TargetDeviceManager.Certificate](#).
- The http ports 80 and/or 8080 must be added to the scope of the Application Port Settings and opened explicitly.
- Deactivate the Controller Firewall (not recommended).



The http port for the Process-Visualization (designed by the UI Designer) or the Diagnose-Visualization is tcp/80. The http port for the Controller.WebVisu (only available with extended Controller versions) is tcp/8080.

## Workaround: Handling of outbound connections

This chapter is relevant for the Controller firmware versions between 01.09.00 and 01.11.00. The Controller.Firewall focuses on incoming rather than outgoing connections. However, if an outgoing connection is established, usually response is made in most cases, which in turn must be taken into account by the firewall. For example, the OPC-UA connection is considered here. If a connection is established from controller A with an OPC-UA Client to controller B with an OPC UA Server, four steps in the respective firewalls of the controllers are relevant:

1. Controller A with OPC-UA Client and an outgoing connection  
The OPC-UA Client communicates via a randomly selected dynamic port (from the range 32,768 – 60,999). Outgoing ports are generally not blocked by the firewall.
2. Controller B with OPC-UA Server and an incoming connection  
In this example, the incoming connection takes place on the OPC-UA Server port 4840, which must be enabled in the firewall.
3. Controller B with OPC-UA Server and an outgoing connection  
The OPC-UA Server responds via port 4840 and creates an outgoing connection. Outgoing ports are generally not blocked by the firewall.

# Controller 1.x

## Security functions

---

### 4. Controller A with OPC-UA Client and an incoming connection

The OPC-UA Client receives the response on the same randomly selected dynamic port.

This port must be opened in the firewall. Since the port is chosen randomly, the dynamic range in the Controller. Firewall must be specified as the application port range.



A Controller. Firewall rule for the controller A might look like this:

- Protocol name: e.g. "Open dynamic ports"
- Port Range Start: 32768
- Port Range End: 60999
- Protocol Type : TCP
- Activation: Allow
- Client IP Range: Any

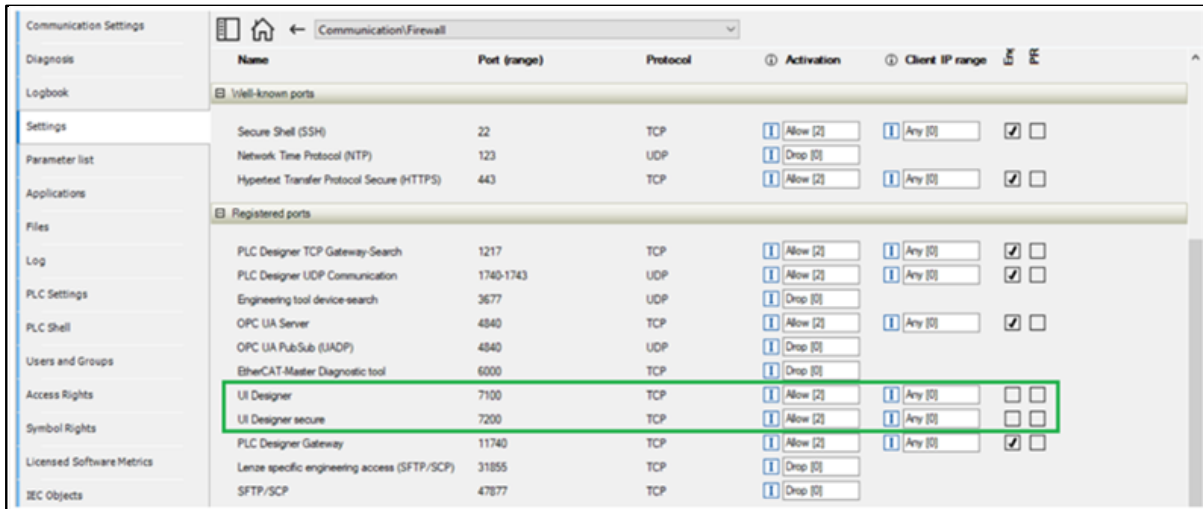
## Controller.Firewall: Security functionality verification

There are different ways to verify the correct functionality of the firewall. The following example explains how this can be tested.

First, a connection must be established to that the PLC connection is working properly.

In order to establish a connection, the firewall must be configured to allow it.. In this example, communication between the PLC and the UI Designer will be established.

At the firewall, configure the ports for UI Designer communication as open.

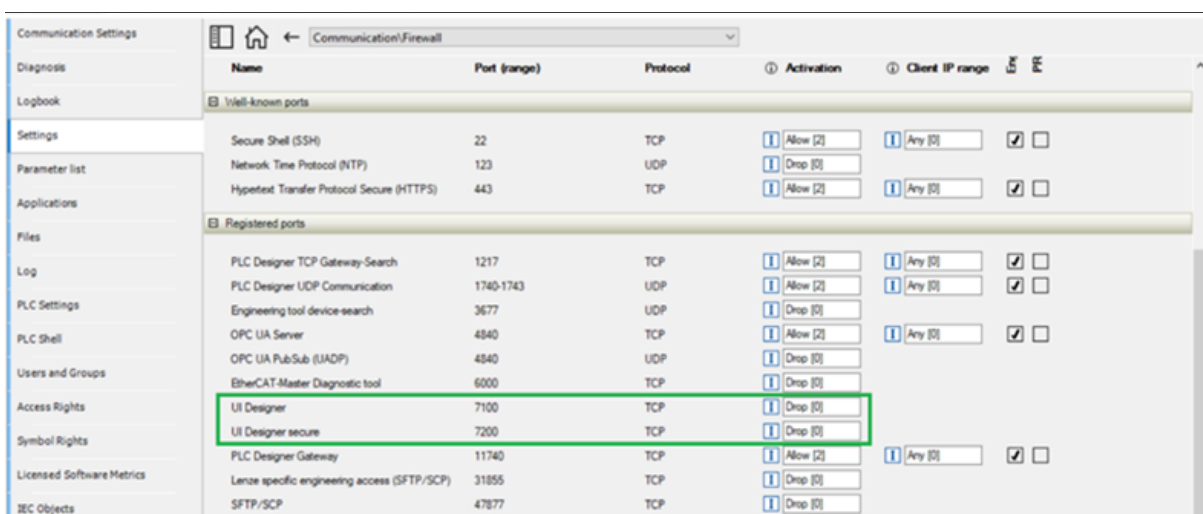


| Name                                         | Port (range) | Protocol | Activation | Client IP range |                                     |
|----------------------------------------------|--------------|----------|------------|-----------------|-------------------------------------|
| <b>Well-known ports</b>                      |              |          |            |                 |                                     |
| Secure Shell (SSH)                           | 22           | TCP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| Network Time Protocol (NTP)                  | 123          | UDP      | Drop [0]   |                 |                                     |
| Hypertext Transfer Protocol Secure (HTTPS)   | 443          | TCP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| <b>Registered ports</b>                      |              |          |            |                 |                                     |
| PLC Designer TCP Gateway-Search              | 1217         | TCP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| PLC Designer UDP Communication               | 1740-1743    | UDP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| Engineering tool device-search               | 3677         | UDP      | Drop [0]   |                 |                                     |
| OPC UA Server                                | 4840         | TCP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| OPC UA PubSub (UADP)                         | 4840         | UDP      | Drop [0]   |                 |                                     |
| EtherCAT-Master Diagnostic tool              | 6000         | TCP      | Drop [0]   |                 |                                     |
| UI Designer                                  | 7100         | TCP      | Allow [2]  | Any [0]         | <input type="checkbox"/>            |
| UI Designer secure                           | 7200         | TCP      | Allow [2]  | Any [0]         | <input type="checkbox"/>            |
| PLC Designer Gateway                         | 11740        | TCP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| Lenze specific engineering access (SFTP/SCP) | 31855        | TCP      | Drop [0]   |                 |                                     |
| SFTP/SCP                                     | 47877        | TCP      | Drop [0]   |                 |                                     |

Firewall.Security functionality verification

The correct parameterization be tested. Follow the instructions in the “UIDesigner.ServerManagerUI.Certificate” chapter to establish a connection between the plc and the UI Designer.

After establishing the connection, switch to offline mode and change the parameterization of the firewall as follows.



| Name                                         | Port (range) | Protocol | Activation | Client IP range |                                     |
|----------------------------------------------|--------------|----------|------------|-----------------|-------------------------------------|
| <b>Well-known ports</b>                      |              |          |            |                 |                                     |
| Secure Shell (SSH)                           | 22           | TCP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| Network Time Protocol (NTP)                  | 123          | UDP      | Drop [0]   |                 |                                     |
| Hypertext Transfer Protocol Secure (HTTPS)   | 443          | TCP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| <b>Registered ports</b>                      |              |          |            |                 |                                     |
| PLC Designer TCP Gateway-Search              | 1217         | TCP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| PLC Designer UDP Communication               | 1740-1743    | UDP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| Engineering tool device-search               | 3677         | UDP      | Drop [0]   |                 |                                     |
| OPC UA Server                                | 4840         | TCP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| OPC UA PubSub (UADP)                         | 4840         | UDP      | Drop [0]   |                 |                                     |
| EtherCAT-Master Diagnostic tool              | 6000         | TCP      | Drop [0]   |                 |                                     |
| UI Designer                                  | 7100         | TCP      | Drop [0]   |                 |                                     |
| UI Designer secure                           | 7200         | TCP      | Drop [0]   |                 |                                     |
| PLC Designer Gateway                         | 11740        | TCP      | Allow [2]  | Any [0]         | <input checked="" type="checkbox"/> |
| Lenze specific engineering access (SFTP/SCP) | 31855        | TCP      | Drop [0]   |                 |                                     |
| SFTP/SCP                                     | 47877        | TCP      | Drop [0]   |                 |                                     |

Firewall.Security functionality verification check

## Controller 1.x

Security functions

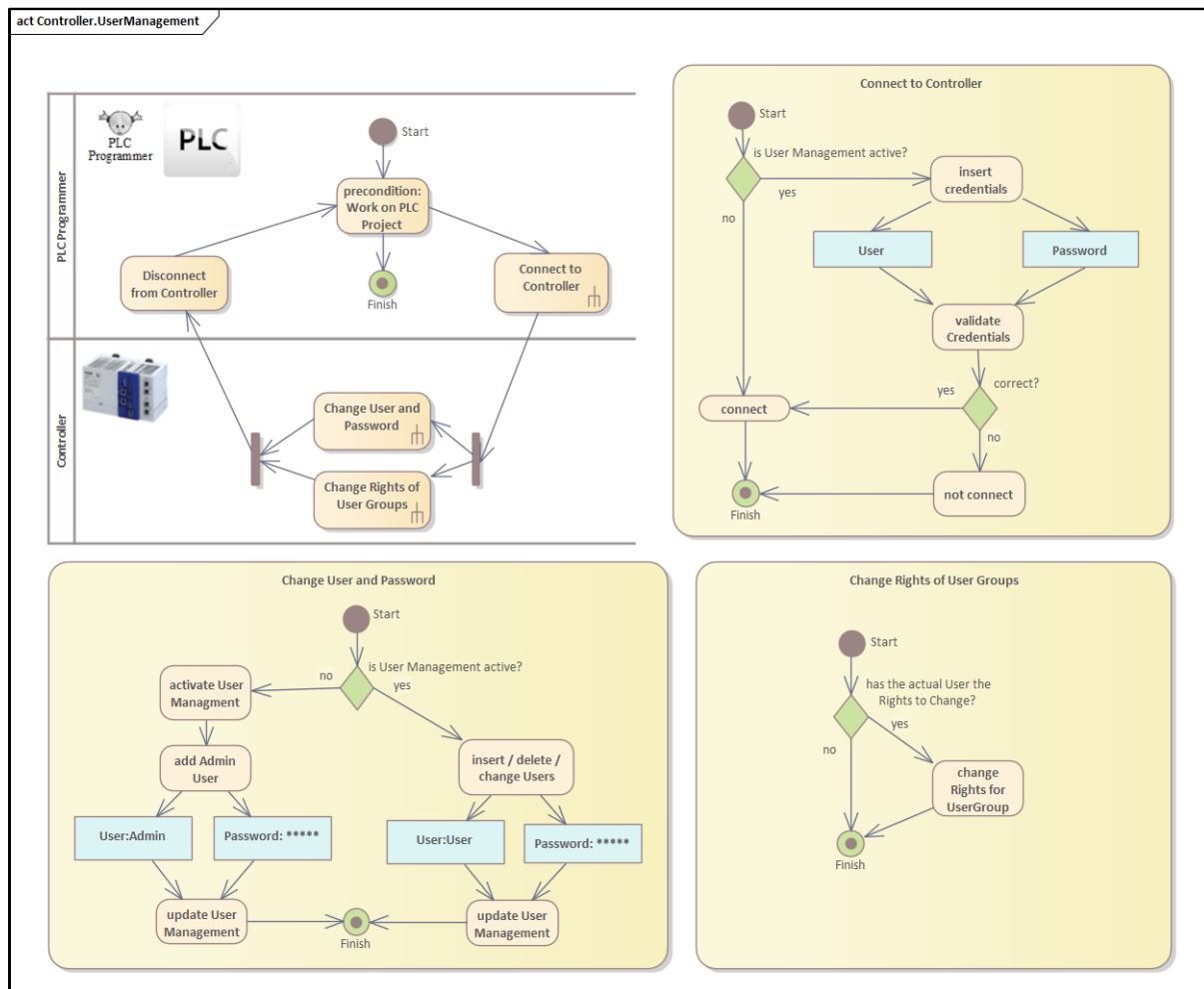
---

To test the correct functionality of the firewall, try to establish a connection with the UI Designer. The connection should be dropped.

## Controller.UserManagement

Controller.UserManagement has been available since FW version 01.07.00.

To implement Controller.UserManagement, the »PLC Designer« offers a user management administration for the c5x0 runtime. Once enabled on the Controller, an anonymous online connection cannot be established with the device. This can be used, for example, to avoid accidentally overwriting a PLC program or transferring it to the wrong controller.



Activity Diagram

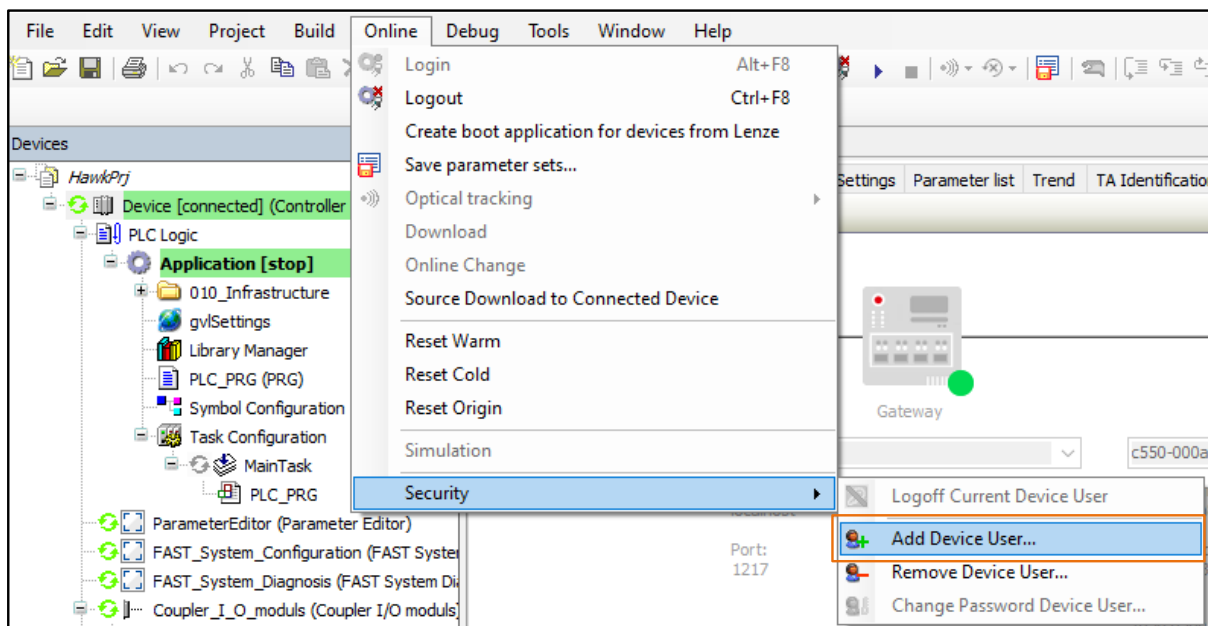
### Controller.UserManagement: Activating

To activate user management, the »PLC Designer« must be connected online to the controller. Go to settings

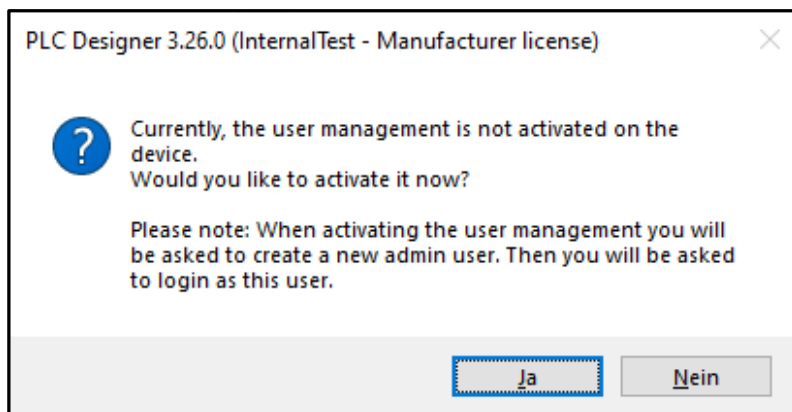
Menu / Online / Security / User Login ...

# Controller 1.x

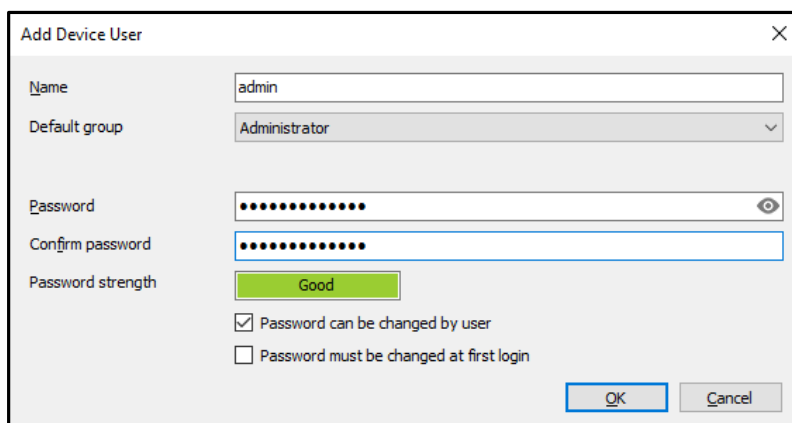
## Security functions



Add Device User



Activate user management



Add Device User Dialog



Device User Logon



You are currently not authorized to perform this operation on the device. Please enter the name and password of an user account which has got the sufficient rights.

Device name

Device (Controller c550)

Device address

User name

admin

Password

••••••••



Operation:

View

Object:

"Device"

OK

Cancel

Device User Logon

# Controller 1.x

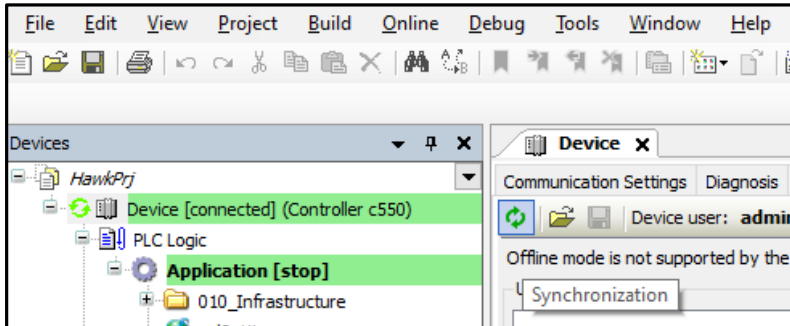
## Security functions

---

### Controller.UserManagement: Change Users and Groups

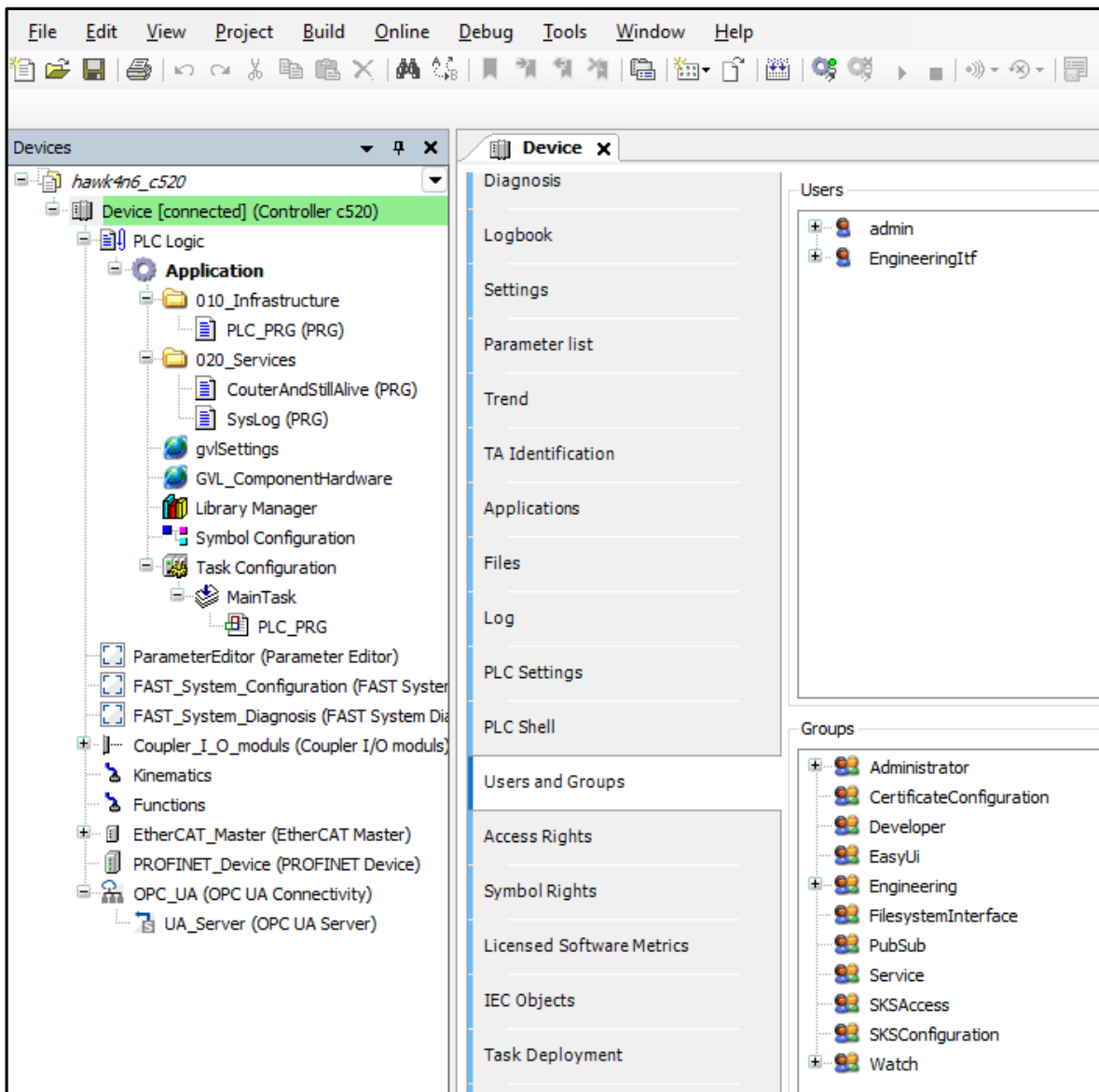
To manage the users, first synchronize the user management, with the following:

Device-Tree / Project / double-click on Device / Menu Users and Groups / Synchronization



Synchronization

Adding a user is accessed via the Add... option.. Between the roles { Administrator | Developer | Service | Watch }. If additional roles are to be created, they can also be created with Add... or deleted with Delete.



Set Users and Groups

## Controller.UserManagement: Groups

- **Administrator:**  
When you log in to the device for the first time, you will be instructed to activate the device user administration and then create a user in the Administrator group. As this user, you can set up additional users and groups and assign access rights.
- **Developer:**  
Rights for download, online change, debugging, forcing.
- **Service:**  
Backup&restore of the IEC application, update of the IEC application (transfer of boot projects), but no programming/debugging of the IEC application.
- **Watch:**  
Read-only authorisation.

# Controller 1.x

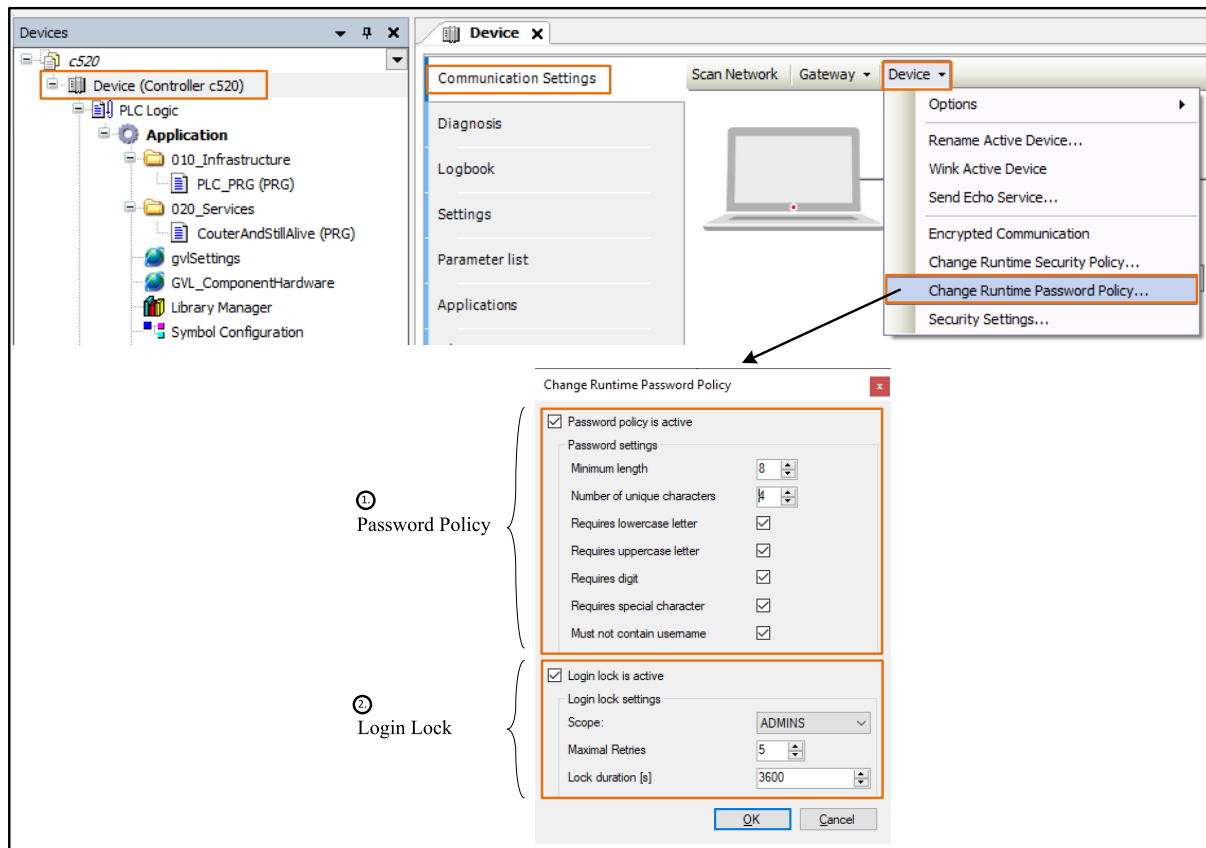
## Security functions

---

- Engineering:  
Group for the access rights of the EASY Starter Suite (consisting of EASY Starter, EASY Firmware Loader and EASY Application Loader).
- EasyUI:  
Group for the access rights of the EASY UI Designer.
- FilesystemInterface:  
Group for the OPC UA Server File Access.
- PubSub:  
Group for dynamically change the OPC UA PubSub configuration.
- CertificateConfiguration:  
Group for pushing certificates from GDS or e.g. UA Expert.
- SKSAccess:  
Group for the OPC UA SKS Server Access.
- SKSConfiguration:  
Group for dynamically change the OPC UA SKS Server configuration.

## Controller.UserManagement: Runtime Password Policy

The Runtime Password Policy has been available since controller firmware version 1.13.0 in combination with PLC Designer 4.0.0. The User can activate the Runtime Password Policy, by clicking on the device in Device-Tree / Communication Settings / Device / Change Runtime Password Policy. Now, the settings for the policy of the device, in this case the controller, can be done.



Runtime Password Policy

In the section `Password settings` the user can specify the minimum requirements of the passwords.

- Minimum length  
Minimum length of password characters (all characters count, whether they are letters, numbers, special characters).
- Number of unique characters  
Minimum number of different unique characters.
- Requires lowercase letter  
{ a-z, ä, ö, ü, ß }
- Requires uppercase letter  
{ A-Z, Ä, Ö, Ü }
- Requires digit  
{ 0-9 }

# Controller 1.x

## Security functions

---

- Requires special character

{ ^, °, !, ", \$, %, &, /, (, ), =, ?, ` , {, [ , ], }, \, ' , +, \*, ~, #, ' , - , \_ , . , : , , , ; , < , > , | , @ , € , μ }

- Must not contain username

The username string is not allowed in the password.



Activating or changing the password policy settings will take effect immediately. However, the changes only apply to the assignment of new passwords. Existing passwords remain valid, even if they do not comply with the policy.

In the section `Login Lock settings` the user can specify the lock after unsuccessful logins.

- Scope

ADMINS: The Login Lock settings are valid for all users in the Administrator Group.

NONADMINS: The Login Lock settings are valid for all users except Administrators.

ALL: The Login Lock settings are valid for all users.

- Maximum Retries
- Lock duration [s].

Lock duration for this locked users in seconds.

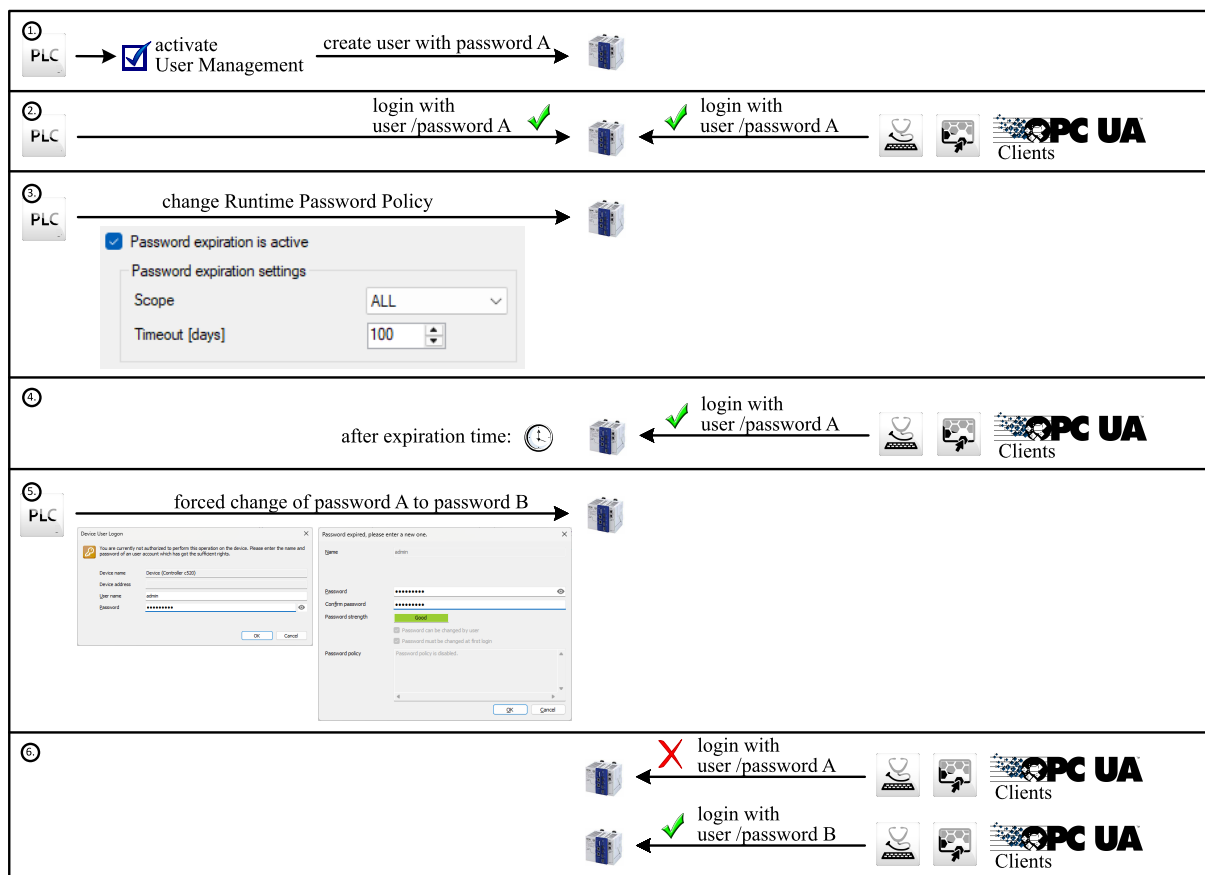


If a user attempts to log in unsuccessfully a maximum number of times, their account will be locked. The login options of other users will remain unaffected.

## Controller.UserManagement: Password Expiration

The Runtime Password Expiration is available since Controller Firmware Version 1.14.0 in Combination with PLC Designer 4.1.0. The User can activate the Runtime Password Expiration, with Click on Device in Device-Tree / Communication Settings / Device / Change Runtime Password Policy. Now the settings for the Policy of the Device, in this case the Controller, can be done. This function is deactivated by default.

- Scope:  
 ADMINS: Password Expiration is valid and active for all admin-Users.  
 NON-ADMINS: Password Expiration is valid and active for all non-admin-Users.  
 ALL: Password Expiration is valid and active for all Users.
- Timeout [days]:  
 1 ... 1000 days for valid password until forced password renewal.



Runtime Password Expiration

The following sequencer describes the mechanism:

- ( 1 ) Firstly, user management must be activated on the device (in this case the controller) by the PLC Designer. A first user with example password A must be assigned.
- ( 2 ) The user can then log in with user and his password A using PLC Designer or other communication channels.
- ( 3 ) If desired, the Runtime Password Policy can be activated.
- ( 4 ) After the set time has elapsed, all other communication channels can continue to log in with the known user and password A. These other communication channels can be, for example, the EASY Starter, the EASY Firmware Loader, the EASY Application Loader, the EASY UI Designer or an OPC UA Client.

# Controller 1.x

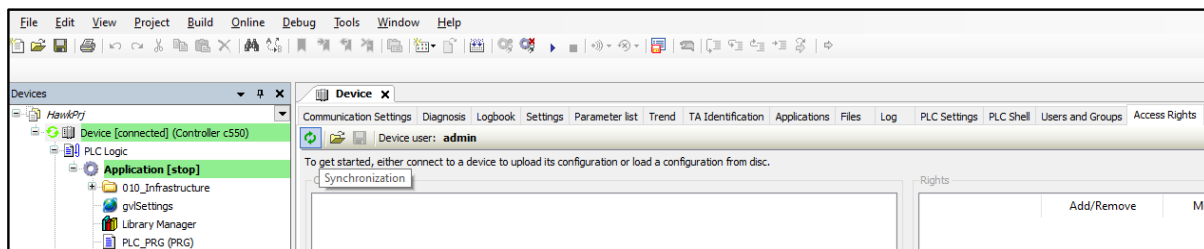
## Security functions

- ( 5 ) The next time the user attempts to log in using the PLC Designer, they will be prompted to change the password.
- ( 6 ) Once the password has been changed, this password is also valid for the other communication channels.

### Controller.UserManagement: Change Access Rights

To manage the access rights, first synchronize the user management with the following:

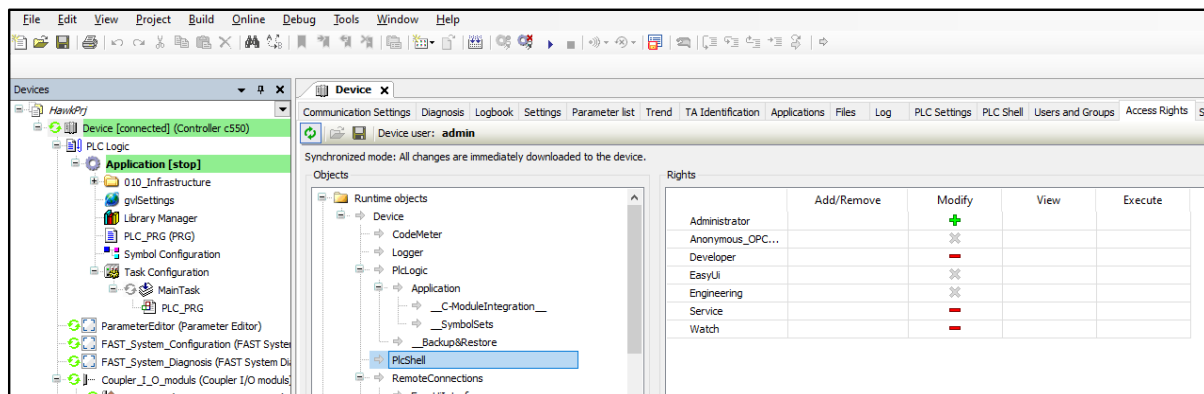
Device-Tree / Project / double-click on Device / Menu Access Rights / Synchronization



Synchronize Access Rights

To manage the access rights to the objects, the following setting option is available.

Device-Tree / Project / double-click on Device / Menu Access Rights



Setting the Access Rights

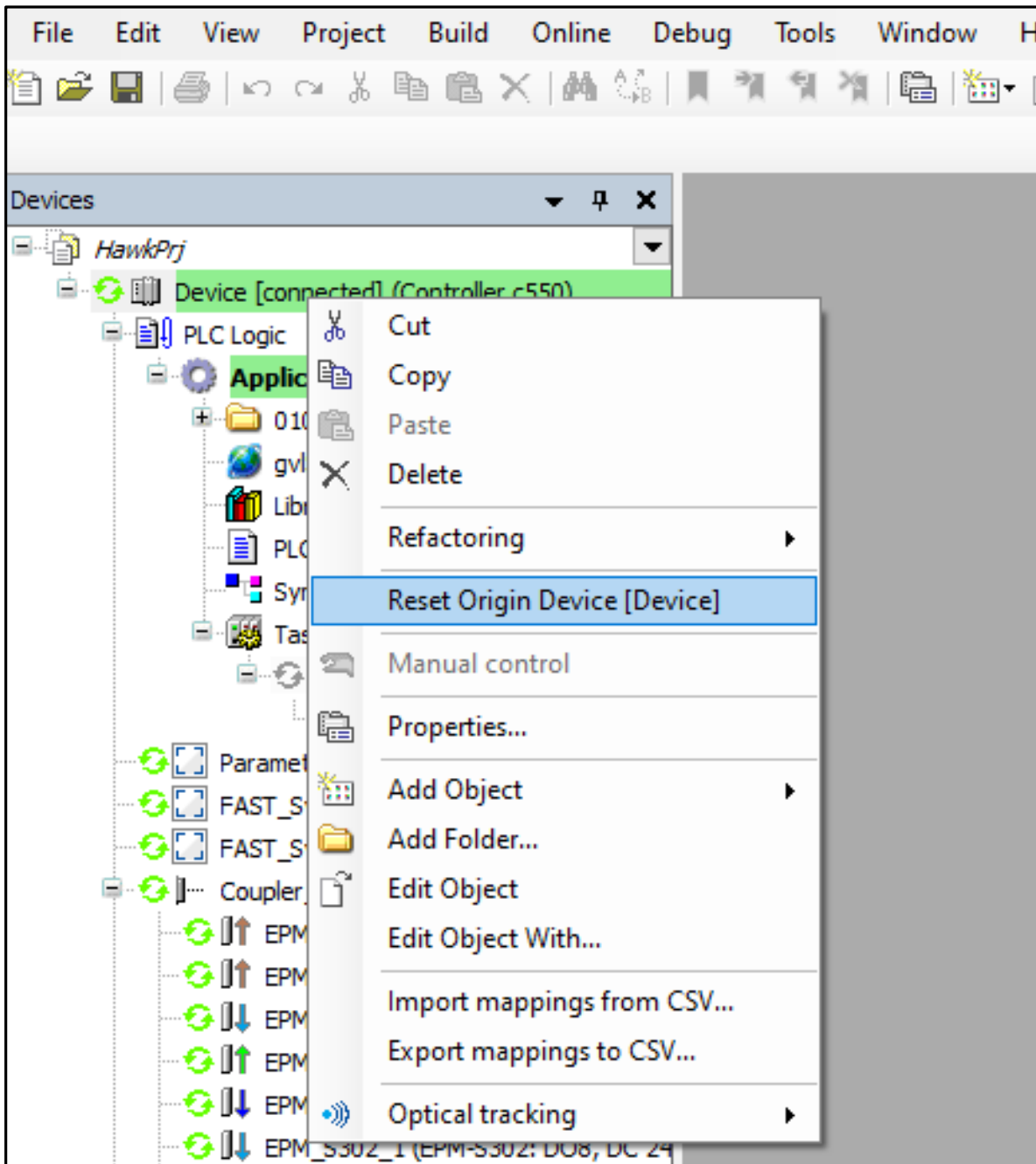
For each node, the setting of the authorization can be set here.

The Administrator group has a special feature. The settings can be changed in the interface, but the group basically receives all rights.



## Controller.UserManagement: Remove

To remove the user management (Attention: All users, groups and access rights will be removed) right-click on the controller device in the device tree of the PLC project and execute the "Reset Origin Device" for the user management.



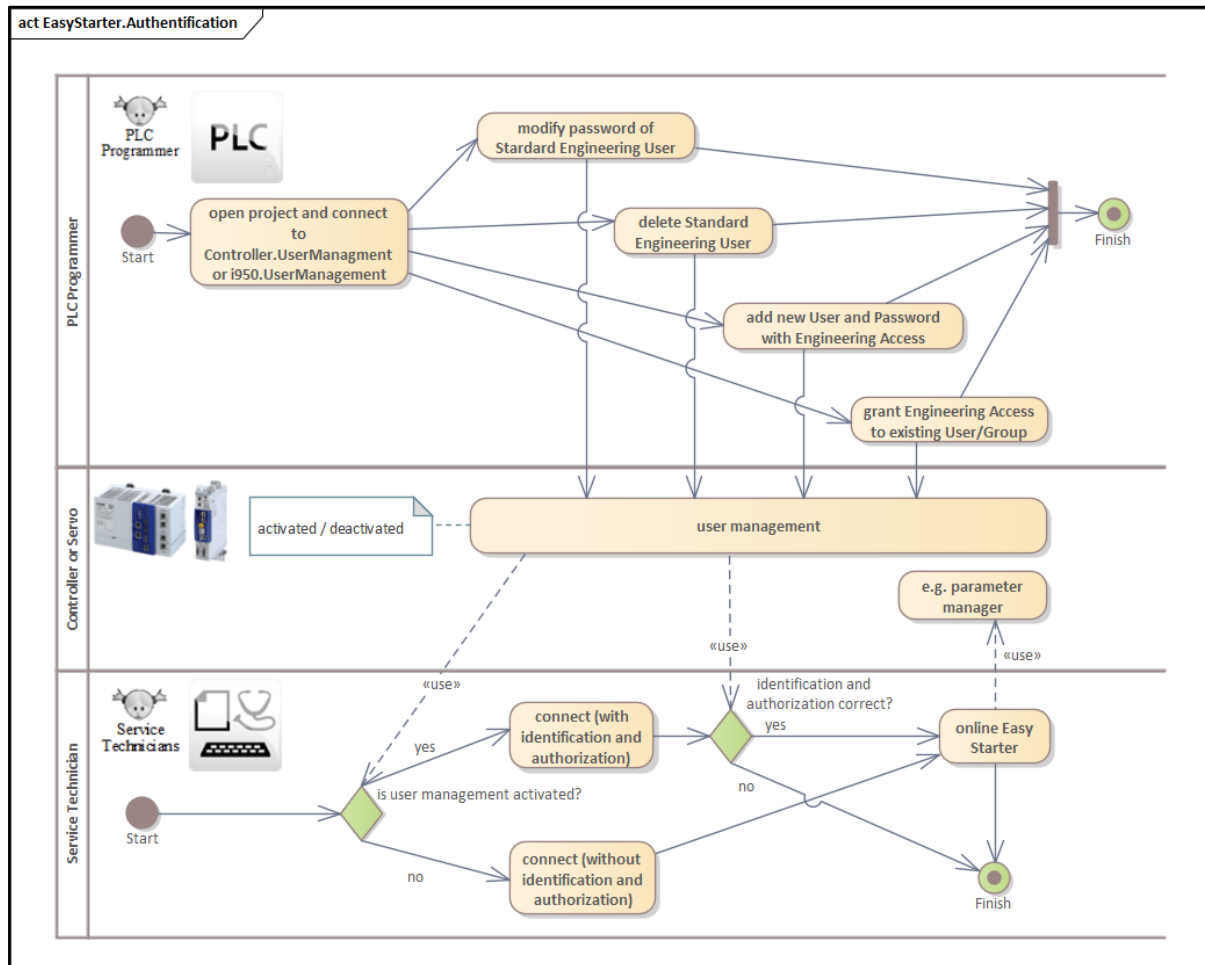
Reset Origin Device [Device]

# Controller 1.x

## Security functions

### Controller.UserManagement: EngineeringItf

User management is not activated in the delivery state. Therefore there is no need for other tools (e.g. EASY Starter, Firmware Loader or Application Loader) to authenticate to this controller. If user management is activated ([Controller.UserManagement: Activating \(185\)](#)), these tools must identify and authenticate themselves before they can go online. The activation and settings of the user management are done with the »PLC Designer«. For this purpose, the user has the possibility to change the necessary settings. A login as administrator is necessary for this. A sequence can be found in the following picture.



Controller.UserManagement: EngineeringItf

### Modify password of Standard Engineering User

When user management is activated, the Engineering group is automatically created with the standard "EngineeringItf" user. A default password is also assigned automatically. It is recommended to change this default password and personalize it. In addition, there is an entry called "EngineeringInterface" in the rights management under the group "RemoteConnections", where the rights for the above-mentioned user can be set.

### Delete Standard Engineering User

If the programmer deletes the user "EngineeringItf", access to the controller from the »EASY Starter Suite« is no longer possible without authentication.

## Add new User and Password with Engineering Access

The programmer can add a new or an existing user to the "Engineering" group. This gives every user the opportunity to connect via »EASY Starter Suite«.

## Grant Engineering Access to existing User/Group

The programmer can also inherit the rights of the "Engineering" group.

## Access Rights

In the »PLC Designer«, the "Runtime objects / Device / RemoteConnections / EngineeringInterface" can be set under the "Access Rights" tab. Only the "Modify" rights can be set here. With this setting, the above access can be consented to or not.

## Anonymous login

For an anonymous login to the »EASY Starter Suite« the user "EngineeringItrf" user is available in the "Engineering" group.

In the settings under "Communication Settings / Device / Change Communication Policy" there is an option in the "Device User Management" category called, which is "Allow anonymous login". This setting affects the OPC UA server. If anonymous login is prohibited, the user "Anonymous\_OPCUAServer" and the group "Anonymous\_OPCUAServer" will be deleted in the Controller.UserManagement.



Do not add a new user to the 'Anonymous\_OPCUAServer' group. If anonymous login is prohibited, the "Anonymous\_OPCUAServer" user and the "Anonymous\_OPCUAServer" group will be deleted. This means that the connection to the previously created user is also lost and he is left alone.

## Controller.UserManagement: User for »EASY UI Designer«

User management is not activated in the delivery state. In this context, no other tools (such as »EASY UI Designer«, »EASY Starter«, »Firmware Loader« or »Application Loader«) are required to authenticate to this controller. If user management is enabled, these tools must identify and authenticate themselves before they can go online. The activation of the user administration as well as its settings takes place with the »PLC Designer«. For this purpose, the user has the possibility to change the necessary settings. This requires logging in as an administrator. For a sequence, see the following figure.

## Use of the »EASY UI Designer« with deactivated user management

If the user management on the controller is deactivated, authentication from the »EASY UI Designer« is not necessary and access can take place without changing the default settings.

## Create a user to be able to use the »EASY UI Designer« with activated user management

If user management is activated on the controller, the following steps must be completed:

- When user management is activated by the »PLC Designer«, an "EasyUI" group is automatically created in the "Users and Groups" menu under "Groups". are no users in this group.
- By adding a new user to the "EasyUI" group, that user can later authenticate to the controller with the name and password assigned here with the »EASY UI Designer«.

# Controller 1.x

## Security functions

---

- Existing users can be also added to the "EasyUI" group. This also gives them permission.
- Furthermore, entire complete other groups can be added to the "EasyUI" group, thereby granting those groups the same permissions.

### Hardening the controller by prohibiting the use of the »EASY UI Designer«

If the »EASY UI Designer« is not required for commissioning, operation and maintenance, the automatically created "EasyUI" group can be deleted. As a result, access is no longer possible with activated user management from the »EASY UI Designer«.

### Hardening of the access rights by the created users for the »EASY UI Designer«

After the configuration of the user management described above, the rights for the "EasyUI" group can be restricted. This is done via the "Access Rights" tab. The setting can be found under "Runtime objects / Device / RemoteConnections / EasyUiInterface". With the settings Modify, View and Execute, the rights can be further restricted.



All users in the group have the same rights.

### Controller.UserManagement: Security functionality verification

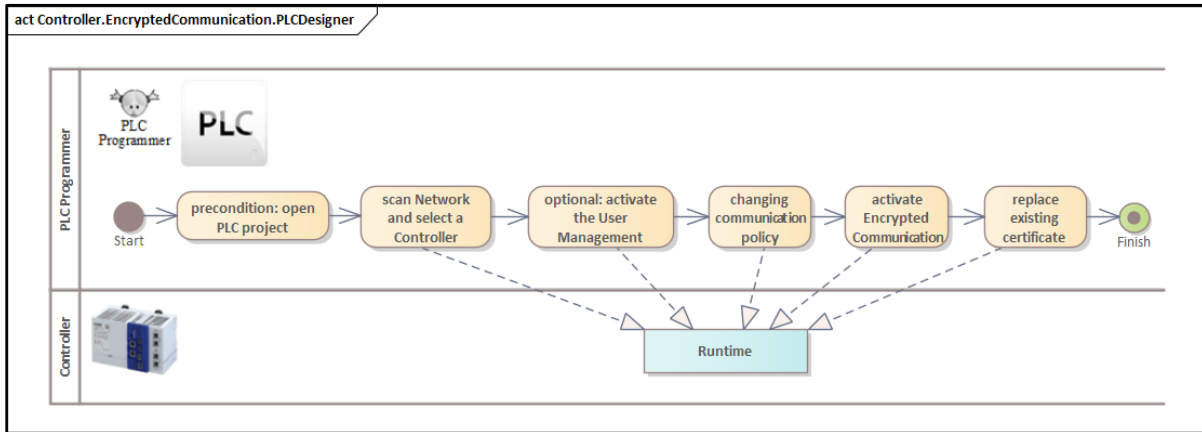
Activate the user management as described in the chapter "Controller.UserManagement: Activating". Connect to the PLC. When the user management opens, type enter correct username and a wrong password. The PLC must deny the connection.

Connect to the PLC. When the user management opens, enter a wrong username and a correct password. The PLC must to deny the connection.

## Controller.EncryptedCommunication.PLCDesigner

This functionality has been available since controller firmware version 01.11.00.

For communication between »PLC Designer« via the gateway to the device, the connection should be encrypted. This is shown in the following image.



Activity Diagram

### Scan Network and select a Controller

To establish a connection please run through the following steps:

- Open the »PLC Designer« project or generate a new project in the »PLC Designer«.
- In the Device Tree, double-click the Device, e.g. c550.
- Open the Communication Settings tab.
- Scan network and select the controller.

### Optional: Activate the user management

Activate the user management ([Controller.UserManagement](#)).

### Changing Communication Policy

The screen to change the communication policy is located in the "Communication Settings" tab within the menu "Device" and "Change Runtime Security Policy ...".

# Controller 1.x

## Security functions

**Change Communication Policy**

**Communication**

Current policy: Optional encryption

New policy: Optional encryption

The device supports both encrypted and unencrypted communication. This can be decided by the user.

**Device User Management**

Current policy: Optional user management

New policy: Optional user management

The user management is optional on the device. It is up to the user to activate the user management or leave the device unprotected.

☒ Allow anonymous login

If anonymous login is activated, certain registered components (e.g. OPC UA) can establish a connection without providing credentials even if user management is enabled.

OK Cancel

Change Runtime Security Policy

### Communication

The device (in this case the controller) supports both encrypted and unencrypted communication. The user can decide if the communication policy is:

- "No encryption"  
Then, the controller only accepts unencrypted communications. In this case, the »PLC Designer« must communicate in cleartext.
- "Optional encryption"  
Then, the controller accepts both, encrypted and unencrypted communications. In this case the user of the »PLC Designer« can decide if the tool will communicate in clear text or encrypted.
- "Enforced encryption"  
Then, the Controller only accepts encrypted communications. In this case, the »PLC Designer« must also, communicate encrypted.

### Device user management

The user management is optional on the device. It is up to the user to activate the user management or leave the device unprotected:

- "Optional user management"  
If a new project is generated the user management is deactivated. The user management can be activated by the user ([Controller.UserManagement](#)).
- Enforced user management

If a new project is generated, the user management is active. When using it for the first time, an administrator-user must be set up.

With the setting "Allow anonymous login" the anonymous login can be prevented. For more details, see [Controller.UserManagement](#).

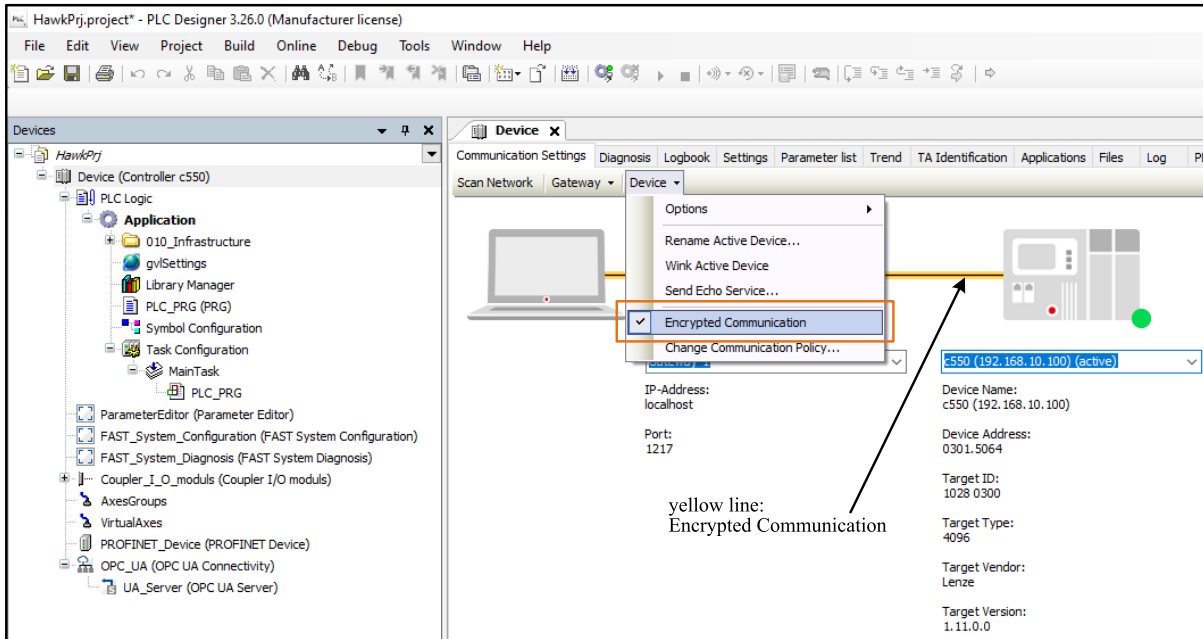
# Controller 1.x

## Security functions

### Activate Encrypted Communication

There are two ways to activate the encrypted communication:

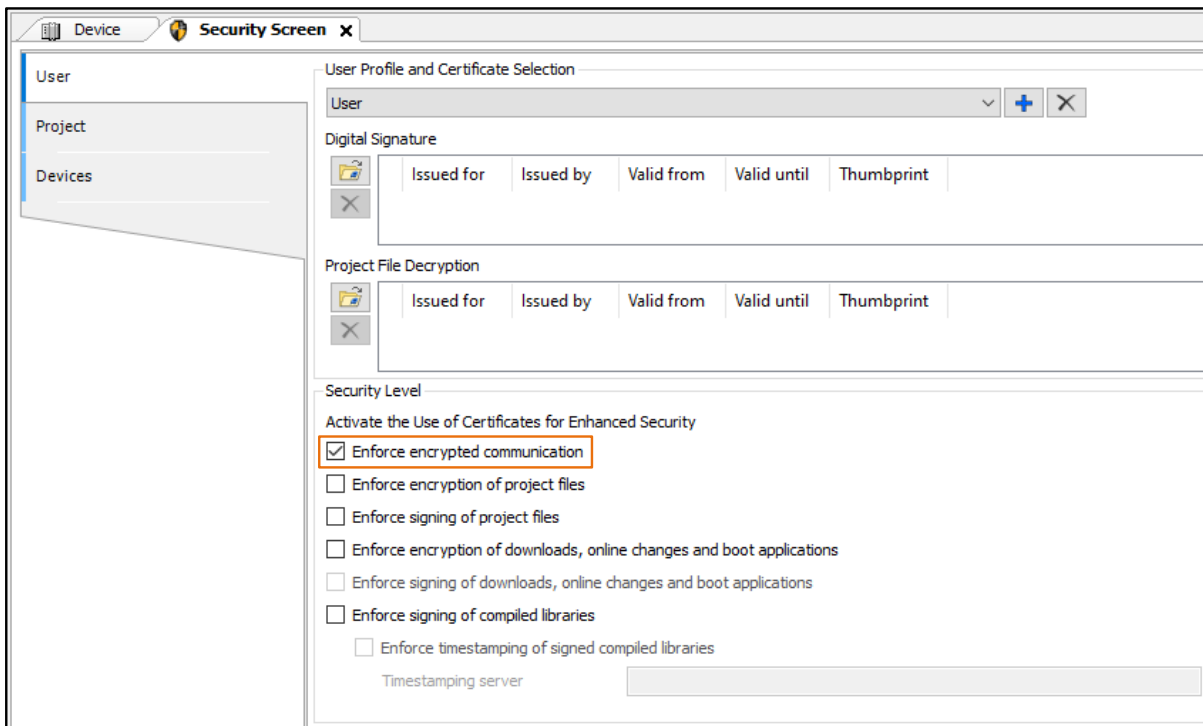
- The menu item to activate the encrypted communication is located in the "Communication Settings" tab in the menu "Device" and "Encrypted Communication". If the "Encrypted Communication" is active, the communication line between the »PLC Designer« and the Controller is marked with a yellow line.



Activate Encrypted Communication

- The second way is to use the Security Screen. The Security Screen is located in the »PLC Designer« menu under "View / Security Screen". Within the "User" tab the "Enforce encrypted communication" check box can be found.





Enforce Encrypted Communication



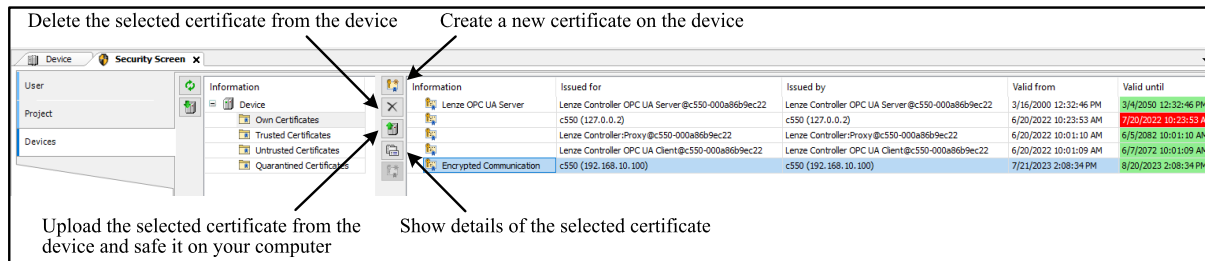
The Device / Encrypted Communication setting defines communication on the part of the PLC Designer.  
The Communication Policy setting defines communication on the part of the controller.  
This can, for example, lead to the situation where the controller is set to forced encryption and the PLC Designer requests clear text communication. The error message "No encryption is not supported by the device" appears.

# Controller 1.x

## Security functions

### Using Encrypted Communication

After activating the "encrypted communication", there will be a certificate for it in the Controller Certificate Store. The security screen is located in the »PLC Designer« Menu "View / Security Screen". Within the tab "Devices / <Name of Device> / Own Certificates", this certificate can be found with the information "Encrypted Communication".



Certificate for Encrypted Communication

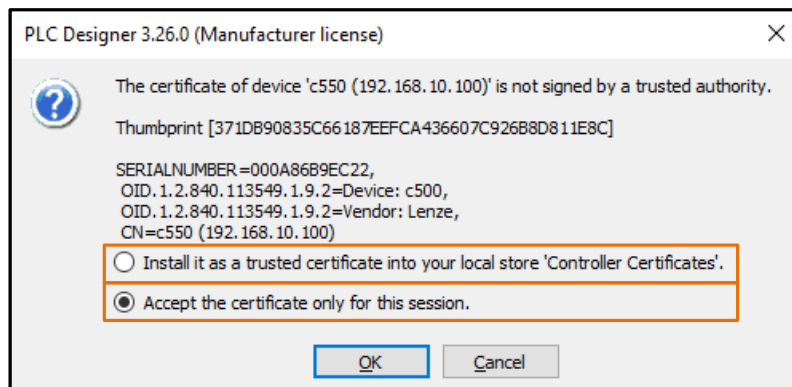
Details of this automatically generated certificate can be found in this documentation: [Controller.EncryptedCommunication.PLCDesigner:Certificate](#)



The automatically generated certificate is valid for 30 days. It is strongly recommended to recreate this certificate with the desired term and key lengths.

For the encrypted communication between »PLC Designer« and the controller, the »PLC Designer« must trust the certificate of the controller. There are two ways to do this:

The first way is to log in to the »PLC Designer« to the controller with activated "Encrypted Communication". The following message box will appear and the user can decide if the certificate will be used only this time or for all sessions:



Login

## Accept the certificate only for this session

The certificate from the controller is used for this session and the connection is established. After the connection is completed and the user logs in again, the message box appears again.



What is **not** a session in this case?

- Stop and start the application.
- Reset warm-1.25
- Reset Cold
- Reset Origin
- Logout and Login
- "Security/Logoff Current User" and Login
- "Security/Logoff Current User", close project, open project, Login

What is a session in this case?

- Closing the »PLC Designer« and starting the »PLC Designer« again.

## Install it as a trusted certificate into your local store "Controller Certificates":

The certificate from the controller is stored in the Windows Certificate Store. This can be found under "Controller Certificates". It is used for this and all subsequent connections as long as the fingerprint of the certificate matches.

More information about the Windows Certificate Store:

- [Security Strategy](#)
- [Integrate a certificate in the windows certificate store](#)

The second way is using the security screen with a logged-in »PLC Designer« to the controller. To do this, follow the steps below:

1. Open the security screen in the »PLC Designer« menu by selecting " View / Security Screen". Within the "Devices / Device / Own Certificates" tab the certificate for the encrypted communication is shown.
2. Click on the "Encrypted Communication" certificate, then click "Upload the selected certificate from the device and save it on your PC". Choose a directory and save the certificate. The name of the certificate will be the type of the controller in combination with the IP Address, e.g. "c550 (192.168.10.100)". The file format will be "\*.cer".



The format of this certificate is \*.cer. It includes the public key for the encrypted communication, but not the private key.

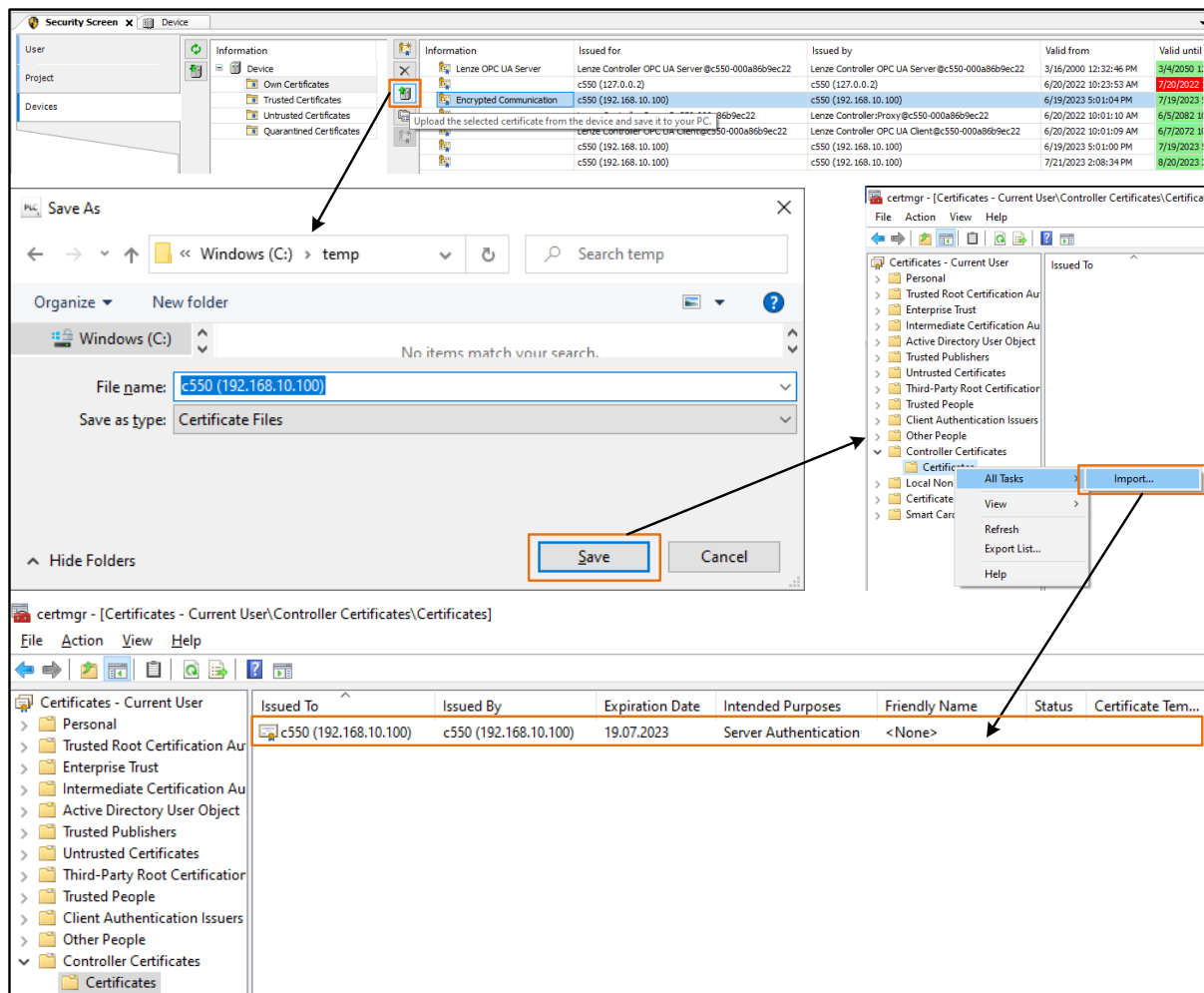
For more information see [Formats and Structures of certificates](#).

3. Open the Windows Certificate Store with the certmgr.msc"command. Choose the directory "Controller Certificates/Certificates" and import the certificate from the uploaded file.

# Controller 1.x

## Security functions

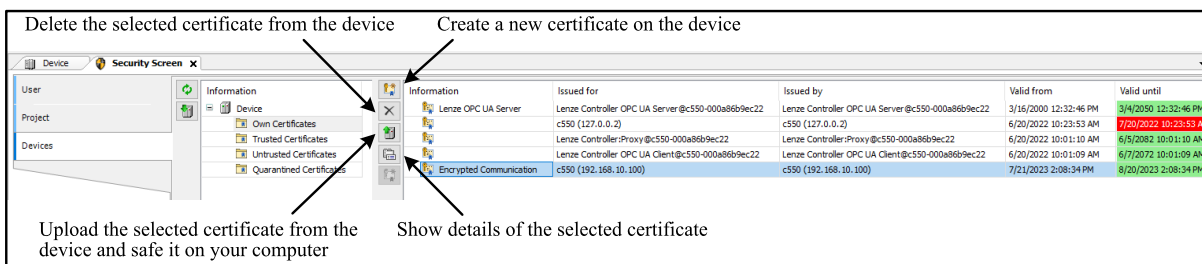
4. After importing the certificate, it will be shown in this directory and the »PLC Designer« will use it for every connection to this controller without asking for trust.



Upload and Import Certificate

## Replace existing Certificate

To replace the existing certificate, for example to extend the valid dates, it can be replaced via the Security Screen. The Security Screen is located in the »PLC Designer« menu "View / Security Screen". Within the tab "Devices / <Name of Device> / Own Certificates" this certificate can be found with the information "Encrypted Communication".



Certificate for Encrypted Communication

## Delete the selected certificate from the device:

Deleting the "Encrypted Communication" certificate will automatically generate a new one with default values. ([Controller.EncryptedCommunication.PLCDesigner](#))

### **Create a new certificate on the device**

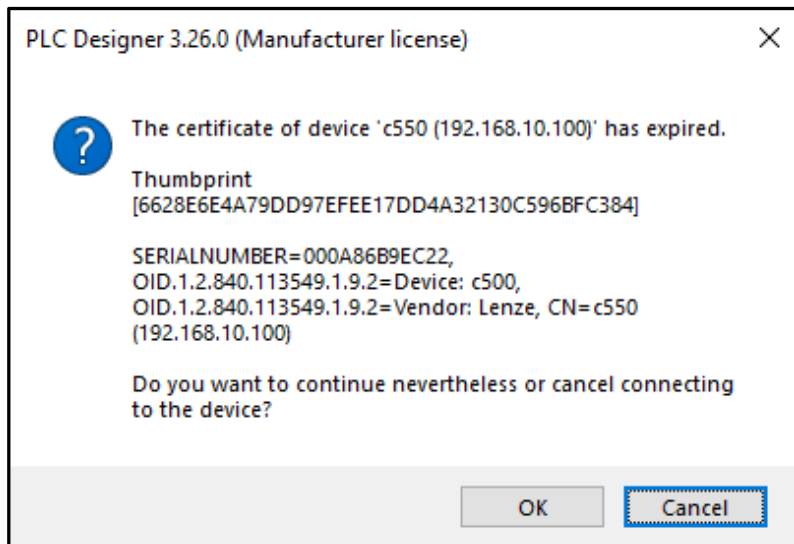
By clicking the "Create a new certificate on the device" button, the user can generate a new certificate and enter the desired key length and validity period.

# Controller 1.x

## Security functions

### Expired certificate

If the certificate of the "Encrypted Communication" no longer valid, and the »PLC Designer« is logged into the controller, a warning will appear:



Valid Warning

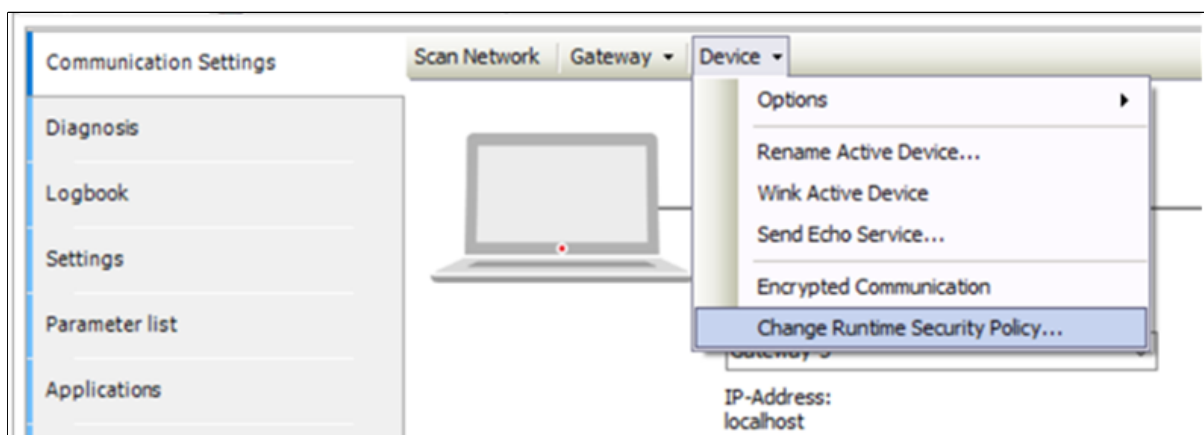
The user can decide whether to cancel or use the expired certificate.

### Controller.EncryptedCommunication: Security Functionality Verification

Have a look at the chapter "Install it as a trusted certificate into your local store". Make sure that the communication using the certificate is running correctly.

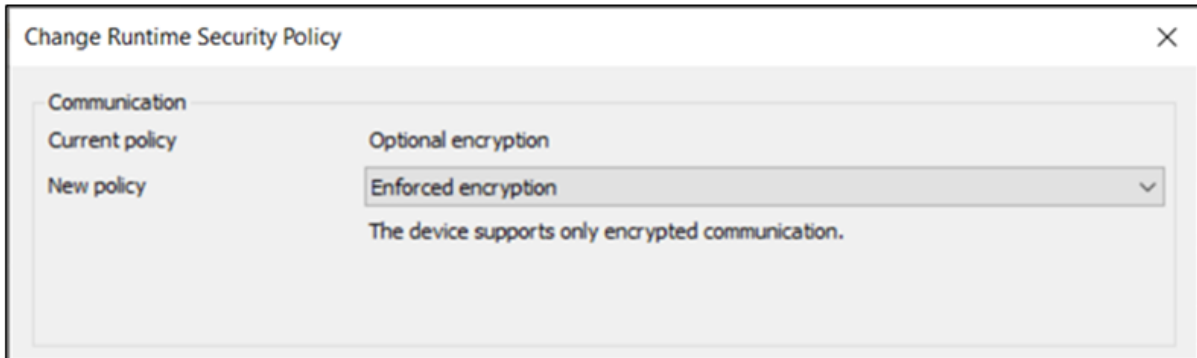
To verify that the encrypted communication is running correctly with regard to security functionality, first of all switch to offline mode.

Switch to "Communication Settings" of the device and choose the option "Change Runtime Security Policy..."



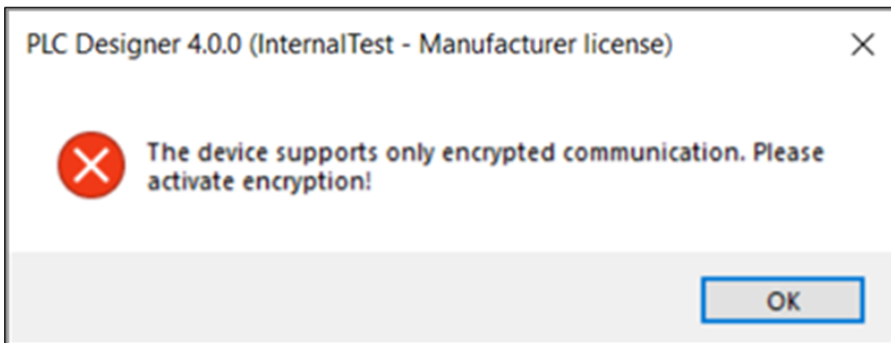
Security Policies

Change the settings “Communication” to “Enforced encryption” and press ok.



Enforce Encryption

To test whether encryption is now necessary for communication, try going online. The following window will appear because encrypted communication hasn't been enabled for PLC Designer communication with the PLC.



Communication error

To establish an encrypted communication with the PLC, the communication settings must to be changed to an encrypted communication.

This is done by switching to the “Security Screen” and marking the parameter “Enforced encryption communication” to ‘TRUE’.

# Controller 1.x

## Security functions

---

User Profile and Certificate Selection

wedekindei

Digital Signature

| Issued for | Issued by | Valid from | Valid until | Thumbprint |
|------------|-----------|------------|-------------|------------|
|            |           |            |             |            |

Project File Decryption

| Issued for | Issued by | Valid from | Valid until | Thumbprint |
|------------|-----------|------------|-------------|------------|
|            |           |            |             |            |

Security Level

Activate the Use of Certificates for Enhanced Security

- ☒ Enforce encrypted communication
- ☐ Enforce encryption of project files
- ☐ Enforce signing of project files
- ☐ Enforce encryption of downloads, online changes and boot applications
- ☐ Enforce signing of downloads, online changes and boot applications
- ☐ Enforce signing of compiled libraries
- ☐ Enforce timestamping of signed compiled libraries

Timestamping server

Enforce Encrypted Communication

Compile the project and go online. communication is now possible.

### Controller.Application.Signature

This functionality is currently not supported by the controller firmware, but it will be available in a future release.



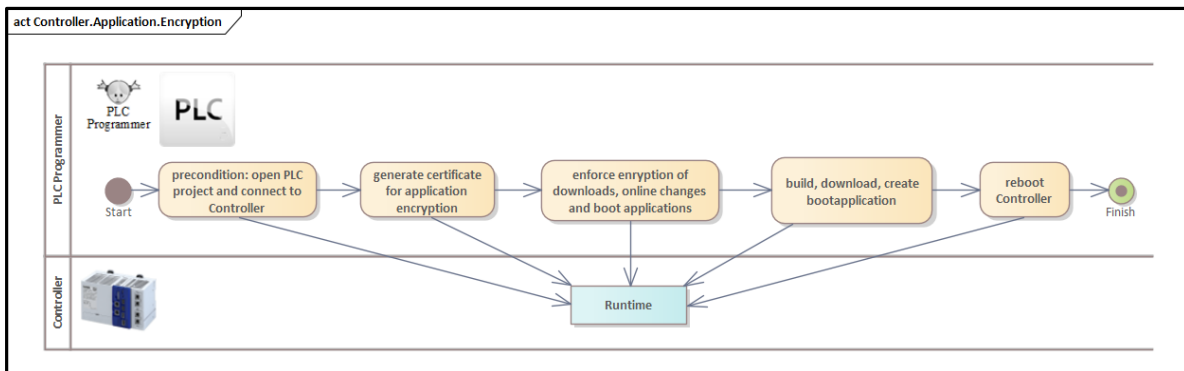
## Controller.Application.Encryption

This functionality has been available since controller firmware version 01.11.00.

With the help of this function, the application of the controller can be encrypted. These include:

- the application itself
- the online change
- the boot application.

The system integrator can use this functionality to protect its intellectual property and thus the application's source code.

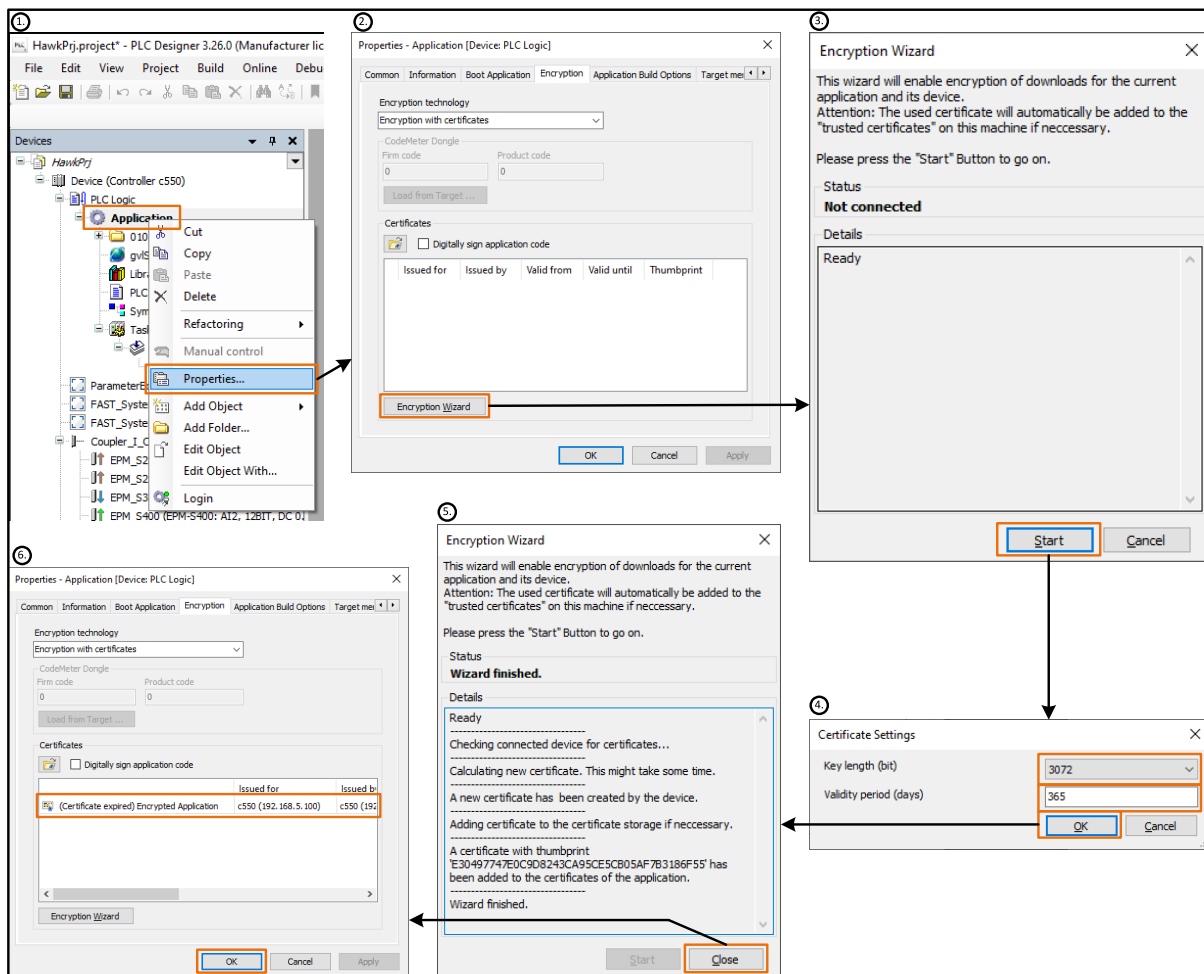


Activity Diagram

In order to use this functionality, a certificate for the application encryption is generated. This is done as shown in the following image.

# Controller 1.x

## Security functions

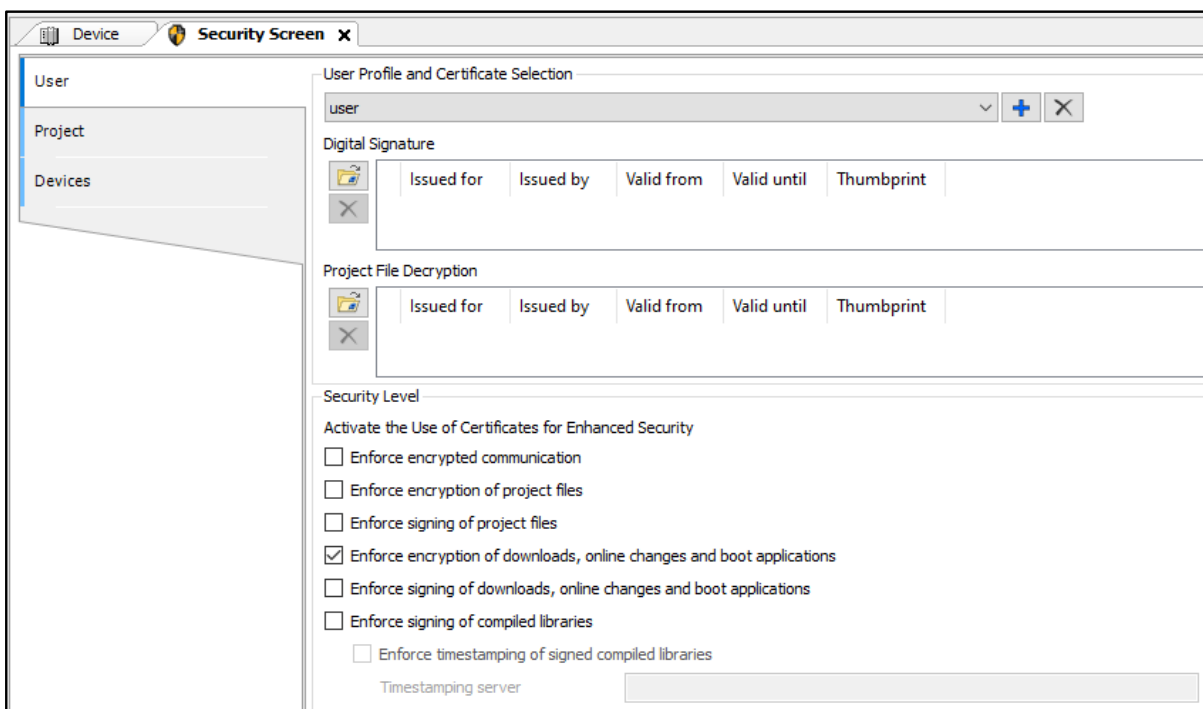


Encryption Wizard

In order to generate a certificate for the encrypted application, the following steps must be carried out:

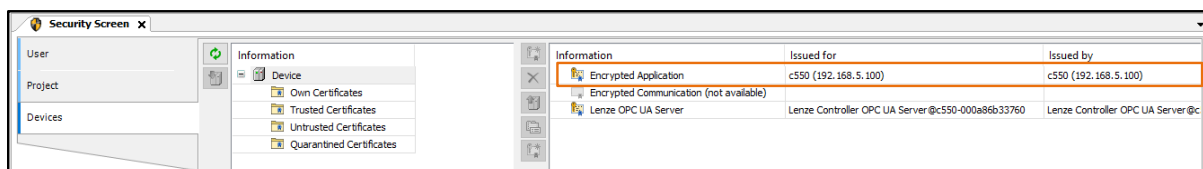
- Open the »PLC Designer« project and select the Application item in the Devices Tree and call up the "Properties..." entry.
- Call the Encryption Wizard in the following dialog. Please choose the encryption technology "Encryption with certificates".
- Start the Encryption Wizard.
- Enter the key length and the validity of the certificate term and confirm with OK.
- Information about the generated certificate is shown. The thumbprint of the certificate is shown to identify the certificate.
- The generated certificate appears in the origination window and is now available.

To enforce the encryption of the application, select the setting "Enforce encryption of downloads, online changes and boot applications" in the »PLC Designer« in the Security Screen.



Enforce encryption of Application

The generated certificate for the Encrypted Application can be found in the Security Screen in the Devices tab. As long as the certificate is not generated, a placeholder labeled "Encrypted Application (not available)" is displayed here.



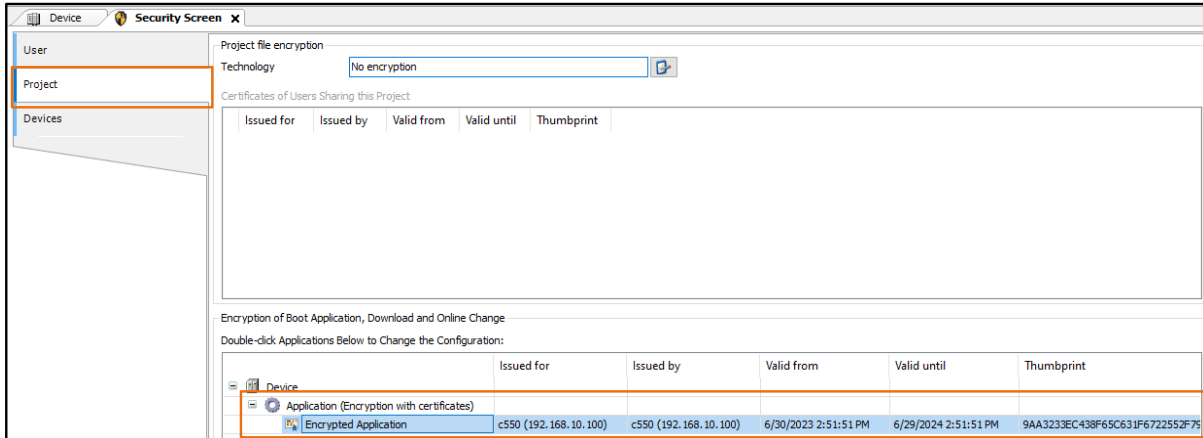
Certificate for Encrypted Application

At this point, the functions are also available to renew the certificate or load it onto the PC ([Controller.CertificateStore.viaPLCDesigner](#)).

# Controller 1.x

## Security functions

In addition, the certificate is also displayed in the Security Screen under Project.



Security Screen Project

After setting up the certificate for the Encrypted Application and Enforce encryption of downloads, online changes and boot applications, the following steps must be completed:

1. Use the »PLC Designer« to rebuild the project.
2. Write the application to the controller.
3. Create boot application.
4. Restart the controller.



Please note that the entire application is not encrypted, only the application.app, i.e. the application program. Additional data such as

- Retain Variables
- Trace Data
- EtherCAT Master Configuration Files
- Parameter Sets of the Devices
- CAM Data
- Firmware Files of Devices located on the EtherCAT (e.g. i7x0)
- OPC UA Nodeset Files

and much more are not included and are unencrypted at the destination.

## Use Case: Controller.Application.Encryption with deleted certificate "Encrypted Application"

The controller's behavior is described below when an encrypted application is stored as a boot project and the certificate is deleted.

### Pre-Condition

The Controller.Encrypted.Application with a Certificate is activated and downloaded, and a boot application is available on the Controller. After restarting the controller the boot application is running.

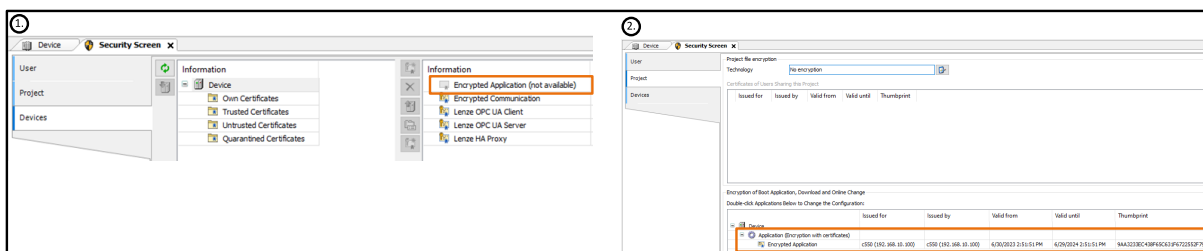
### Delete the Own Certificate "Encrypted Application" on the Controller

The next step is to manually delete the "Encrypted Application" on the controller certificate, e.g. via the »PLC Designer«. After deleting the certificate, the application on the controller is still running.

Behavior of the application after different reset levels:

| Reset Level                   | Behavior                                                                  |
|-------------------------------|---------------------------------------------------------------------------|
| Manually stop the application | After stopping the application, the application can be started.           |
| Reset Warm                    | After "Reset Warm", the application can be started.                       |
| Reset Cold                    | After "Reset Cold", the application can be started.                       |
| Reset Origin                  | After "Reset Origin", the application can not be started again.           |
| Boot of the Controller        | After "Boot of the Controller", the application can not be started again. |

If the »PLC Designer« is still logged in to the controller, the certificate for Encrypted Application in the "Security ScreenWDevices" is shown as deleted, e.g. with the placeholder "Encrypted Application (not available)" (see (1.) in the following figure). Under "Security ScreenWProject", the certificate for the Encryption of the Application is still shown, because the controller application still needs this certificate (see (2.) in the following figure).



Certificate Encrypted Application Deleted



If the certificate is deleted and the user wants to go online on the Controller with the »PLC Designer«, this is not possible. Online changes or creating a boot application are also not possible. The deletion takes effect immediately.

## Security functions

## Certificate Encrypted Application Renew

216



If the certificate has expired and the user wants to go online on the Controller with the »PLC Designer«, this is possible. Online changes and creating boot applications are also possible. However, after the controller has booted it will no longer be possible to start the application, make an online change or create a boot application.

# Controller 1.x

## Security functions

---

### **Use Case: Controller.Application.Encryption in focus of Device Replacement**

The behavior of the controller is described below when an Encrypted Application is stored as a boot project and the controller must be replaced.

#### **Pre-Condition**

The Controller.Encrypted.Application with a certificate is activated and downloaded, and a boot application is available on the controller. After restarting the controller the boot application is running.

#### **Replacement of the controller**

If the controller has to be replaced due to a defect, the SD card is removed and the controller hardware is replaced. After replacing the controller, however, the application does not start. The reason for this is the necessary but missing certificate. A controller exchange is therefore not possible without the previously described certificate renewal process and a new build, download application, creation of a boot project and restart of the controller.



## **Use Case: Controller.Application.Encryption in focus of Backup and Restore**

The behavior of the controller is described when a backup is restored to a changed controller.

### **Precondition**

The Controller.Encrypted.Application with a certificate is activated and downloaded, and a boot application is available on the controller. After restarting the Controller the boot application is running.

### **Backup**

With the help of the backup mechanism, the runtime system (firmware) and the project data on the SD card are copied to the plugged USB stick. Refer to parameter 0x2022:040.

### **Changing the Controller Application**

In this step, the application of the controller is changed. This is to indicate a further development in the life cycle of the PLC project.

### **Restore**

After the change, the original state should be restored. With the help of the restore mechanism, the runtime system (firmware) and project data on the SD card are copied from the plugged USB stick. Refer to parameter 0x2022:043.

Depending on the condition, the behavior may differ.

- If the application encryption certificate was not changed when the application, was changed the restored application starts again without any problems and the restore process can be completed successfully.
- If the application encryption certificate was changed when the application was changed, the restored application will not start. This is due to a mismatch between the required restored application certificate and the actually existing certificate on the controller.

# Controller 1.x

## Security functions

---

### **Use Case: Controller.Application.Encryption in focus of Series Commissioning using the Backup and Restore Mechanism**

The Backup and Restore tool saves the data of the firmware and the application on the USB stick. However, for security reasons, the private keys and certificates are not saved. For this reason, series commissioning cannot be used with this mechanism, since the pair of keys does not exist on the target system. With activated Application Encryption, series commissioning must therefore be carried out via the »PLC Designer«.

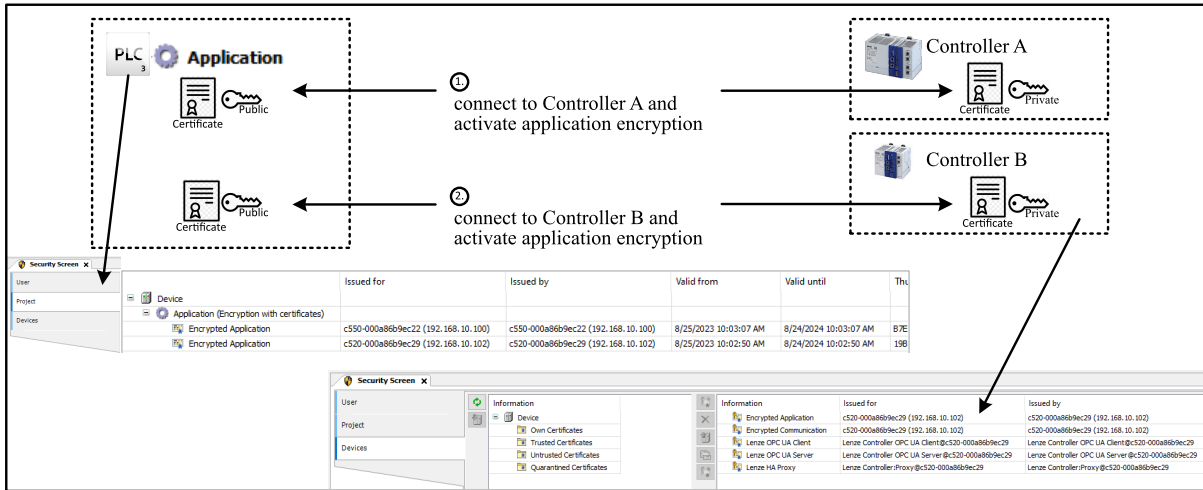
### **Use Case: Controller.Application.Encryption in focus of Application Loader**



The "create boot application" offline function from the »PLC Designer« does not work with the Controller.Application.Encryption. Therefore, an \*.lda cannot be created this way.

## Use Case: Handling one project with Controller.Application.Encryption for more Controller

This use case describes the behavior of a »PLC Designer« project intended for multiple controllers. The process is shown in the following figure.



Project for multiple controllers

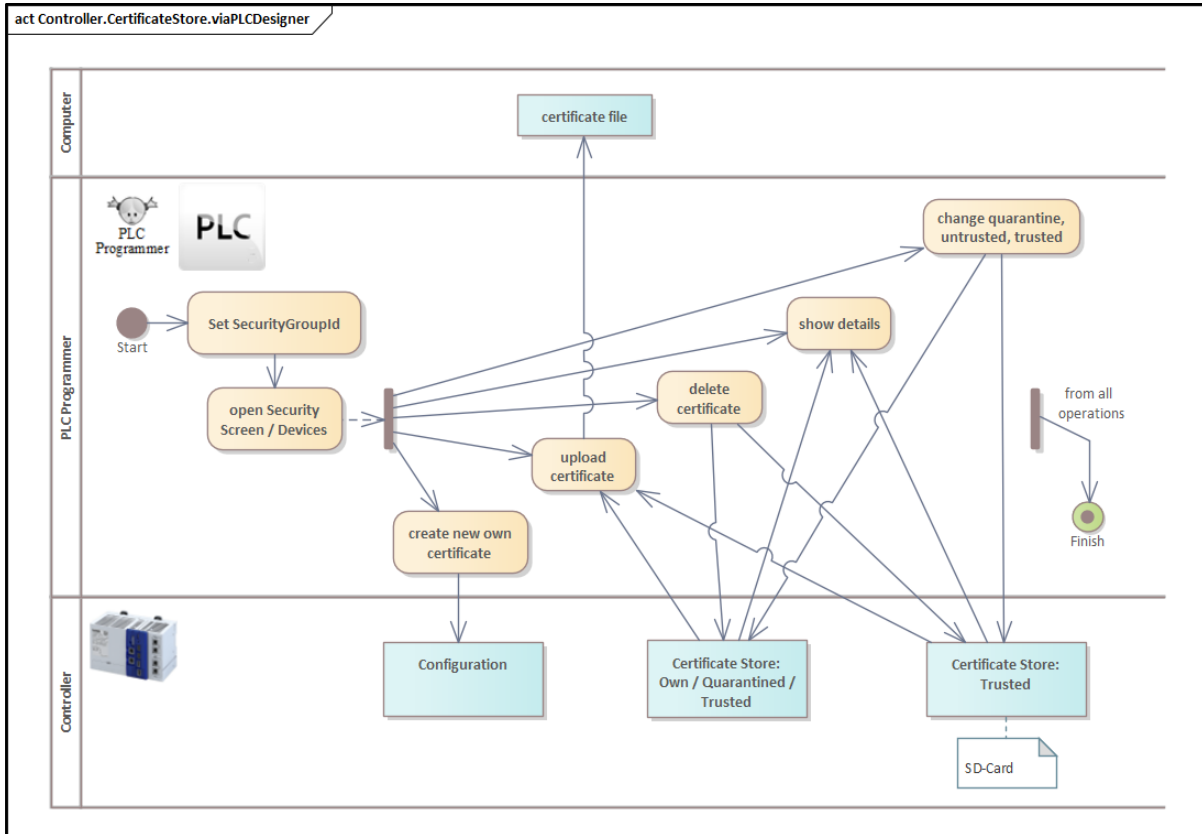
1. Connect the »PLC Designer« to controller A and activate the application encryption using the Encryption Wizard of the application.
2. Controller A will create a certificate including the private key, which will be available in the Certificate Store of controller A as "Encrypted Application" certificate.
3. At the same time the PLC project will include certificate A including the public key, which will be available in the application for the PLC project.
4. Connect the »PLC Designer« to controller B and activate the application encryption using the Encryption Wizard of the application.
5. The controller B will create a certificate including the private key, which will be available in the Certificate Store of Controller B as,"Encrypted Application" certificate.
6. At the same time, the PLC project will include certificate B including the public key, which will be available in the application for the PLC project.
7. Ultimately the application for the PLC project will include both certificates. Depending on the active application, the corresponding certificate is then used for encryption.

# Controller 1.x

## Security functions

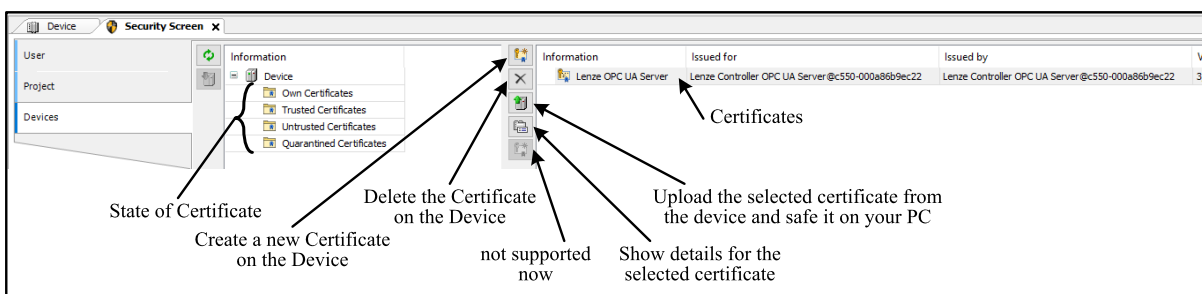
### Controller.CertificateStore.viaPLCDesigner

The controller has its own certificate Store. This can be managed and controlled via the »PLC Designer«.



Activity Diagram

To do this, open the Security Screen and select the "Devices" tab.



Security Screen Devices

In the middle window, the respective status of the certificates can be selected under "Information". The following four statuses are available:

- **Own Certificates:**  
Own certificates of the Controller
- **Trusted Certificates:**  
Certificates from trusted communication partners

- Untrusted Certificates:  
Certificates from untrusted communication partners
- Quarantined Certificates:  
Certificates from communication partners in quarantine

To change a certificate from the status, it can simply be moved from the right window via drag-and-drop to the desired status.

The following possibilities of using the certificates are possible:

# Controller 1.x

## Security functions

---

### Create a new Certificate on the Device

For this purpose, an existing own certificate or a placeholder, i.e. a certificate with the note (not available) must be selected and the button must be pressed. Subsequently, the desired key length and the desired validity can be specified and the certificate can be created.

To change a certificate from the status, it can simply be moved from the right window via drag-and-drop to the desired status.

The following possibilities of using the certificates are possible:

### Create a new Certificate on the Device

For this purpose, an existing own certificate or a placeholder, i.e. a certificate with the note (not available) must be selected and the button must be pressed. Subsequently, the desired key length and the desired validity can be specified and the certificate can be created.

To change a certificate's status, simply drag and drop it from the right window to the desired status.

The following certificate usage options are available:

### Create a new certificate on the device

To do so, select an existing certificate or placeholder (i.e., a certificate with the note "not available") and press the button. Then, you can specify the desired key length and validity period and create the certificate.



If a certificate A exists and another certificate B is created, the certificate with the longer valid time is used, even if it is certificate A. If the "Own Certificate" area is called up, both A and B certificates are displayed. If you want to replace certificate A with certificate B, you should first delete certificate A and then create certificate B.

If a certificate A exists and another certificate B is created, the certificate with the longer valid time is used, even if it is certificate A. If the "Own Certificate" area is called up, both A and B certificates are displayed. If you want to replace certificate A with certificate B, you should first delete certificate A and then create certificate B.

If certificate A exists and certificate B is created, the certificate with the longer valid period is used, even if it is certificate A. If the "Own Certificate" area is called up, both certificates A and B are displayed. If you want to replace certificate A with certificate B, first delete certificate A and then create certificate B.  
>>>>>> .r46270

### Delete the certificate on the device

To do this, select a certificate and press the button. It is important that the certificate is deleted and not moved to "Untrusted Certificates".

### Upload the selected certificate from the device and save it on your PC

For this purpose, select a certificate and press the button. It is important that the respective certificates are loaded onto the PC with the public key. The private key remains on the controller.

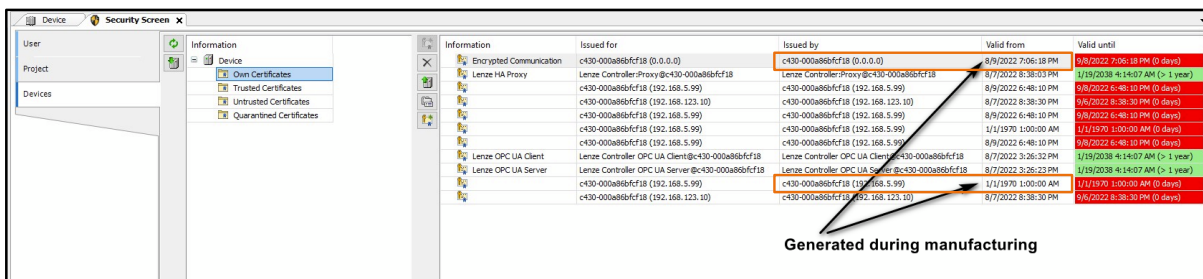
## Show details for the selected certificate

For this purpose, select a certificate and press the button. A window opens where the details of the certificate can be viewed.

## Initial certificates

When the controller boots, some certificates will be generated automatically. This happens for the first time when these devices are produced in manufacturing. Since no time has been set in the controllers for this production step and there is no communication via an NTP connection, the certificates are created with a initial time stamp far in the past. After the devices are sent to the customer, they are switched on again.

When logging into the controller with PLC Designer a pop-up dialog informs that the user some certificates are expired. On the security screen, the expired (validity date in the past) or inactive (empty information field) certificates can be checked. Expired or inactive certificates can be deleted. New certificates will either be generated automatically during the next boot or can be created manually via the security screen.



| Information             | Issued for                                      | Issued by                                       | Valid from          | Valid until                     |
|-------------------------|-------------------------------------------------|-------------------------------------------------|---------------------|---------------------------------|
| Encrypted Communication | c430-000a8b6cf18 (0.0.0.0)                      | c430-000a8b6cf18 (0.0.0.0)                      | 8/8/2022 7:06:18 PM | 8/8/2022 7:06:18 PM (0 days)    |
| Lenze HA Proxy          | Lenze Controller Proxy@c430-000a8b6cf18         | Lenze Controller Proxy@c430-000a8b6cf18         | 8/7/2022 8:38:03 PM | 1/18/2038 4:14:07 AM (> 1 year) |
|                         | c430-000a8b6cf18 (192.168.5.99)                 | c430-000a8b6cf18 (192.168.5.99)                 | 8/7/2022 6:48:10 PM | 9/8/2022 6:48:10 PM (0 days)    |
|                         | c430-000a8b6cf18 (192.168.123.10)               | c430-000a8b6cf18 (192.168.123.10)               | 8/7/2022 8:38:30 PM | 9/8/2022 8:38:30 PM (0 days)    |
|                         | c430-000a8b6cf18 (192.168.5.99)                 | c430-000a8b6cf18 (192.168.5.99)                 | 8/8/2022 6:48:10 PM | 9/8/2022 6:48:10 PM (0 days)    |
| Lenze OPC UA Client     | Lenze Controller OPC UA Client@c430-000a8b6cf18 | Lenze Controller OPC UA Client@c430-000a8b6cf18 | 1/1/1970 1:00:00 AM | 1/1/1970 1:00:00 AM (0 days)    |
| Lenze OPC UA Server     | Lenze Controller OPC UA Server@c430-000a8b6cf18 | Lenze Controller OPC UA Server@c430-000a8b6cf18 | 8/7/2022 3:26:32 PM | 1/18/2038 4:14:07 AM (> 1 year) |
|                         | c430-000a8b6cf18 (192.168.5.99)                 | c430-000a8b6cf18 (192.168.5.99)                 | 1/1/1970 1:00:00 AM | 1/1/1970 1:00:00 AM (0 days)    |
|                         | c430-000a8b6cf18 (192.168.123.10)               | c430-000a8b6cf18 (192.168.123.10)               | 8/7/2022 8:38:30 PM | 9/8/2022 8:38:30 PM (0 days)    |

Generated during manufacturing

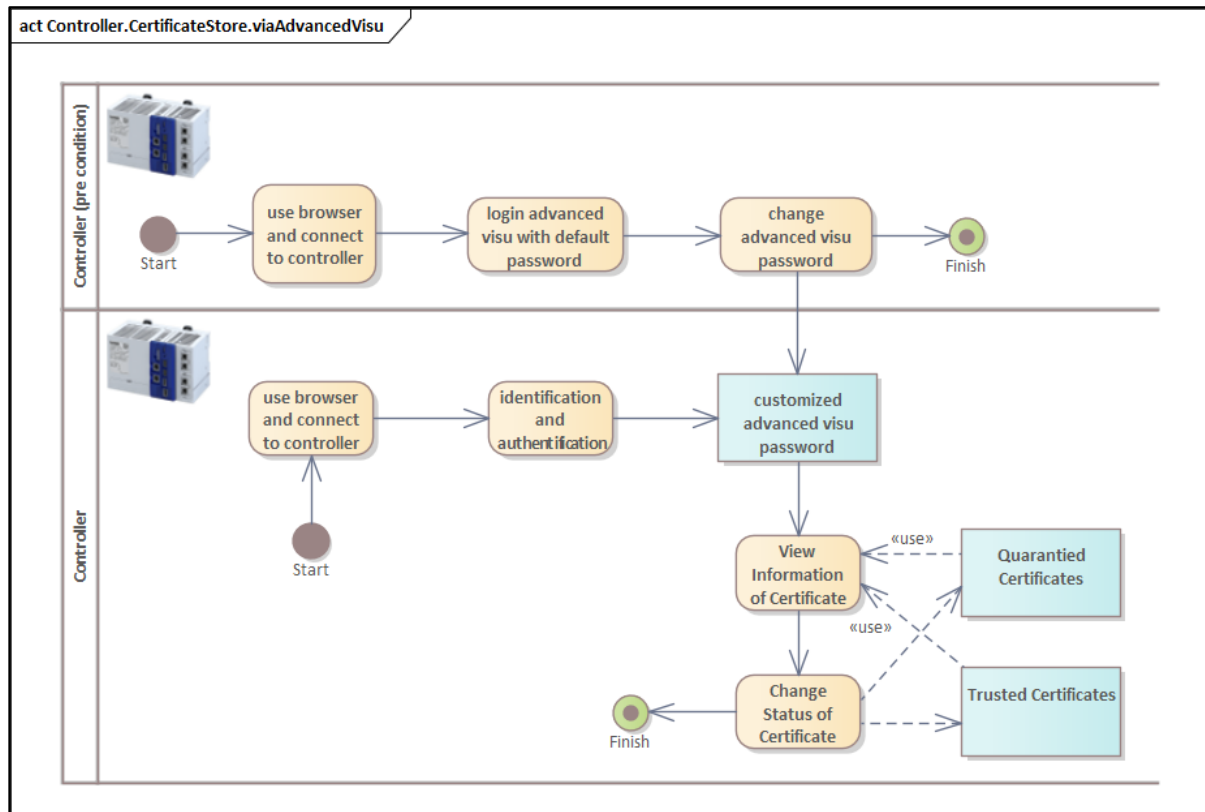
Example for Initial Certificates

# Controller 1.x

## Security functions

### Controller.CertificateStore.viaAdvancedVisu

The functionality to change the status of certificates ([Controller.CertificateStore.viaPLCDesigner](#)) allows the machine programmer to manage the certificates on the controller. Once the machine is delivered to and operated by the end customer, this end customer also needs the ability to manage new certificates on the controller. In most cases, however, the »PLC Designer« is not available for this purpose, as the PLC project usually remains with the machine programmer. For this reason, a function has been established in the diagnostic visualization of the controller, which is presented below. This function has been included in the controller since firmware version 01.11.0.



Activity Diagram

To use this feature, the end customer must follow these steps. First, the user must connect a browser to the diagnostic visualization of the Controller using the IP address. Next the user must identify and authenticate as a human user during diagnostics visualization with the "Advanced" user ([Controller.WebDiagnosis](#)).



**Lenze**

## Log on user

Diagnosis

Our diagnosis service helps you to quickly identify errors.



  
Diagnosis

Name  
advanced

Password  
.....

Log on

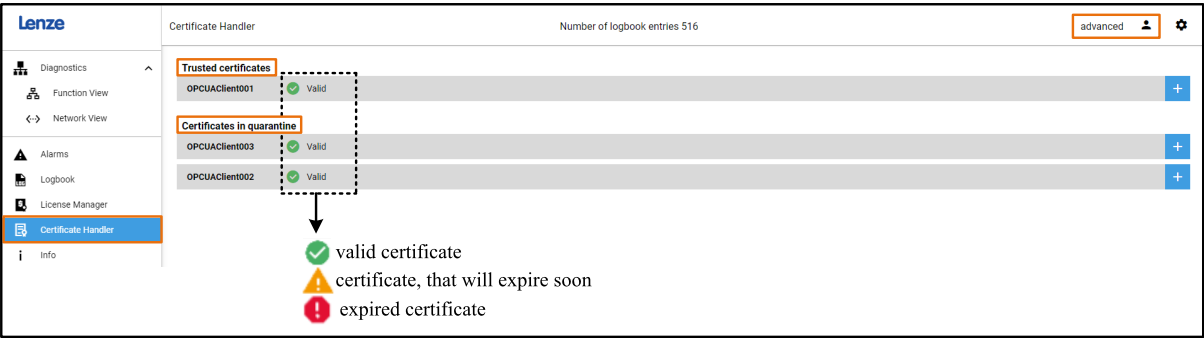
Note: Since the automatic login is not activated, you have to log on to the web visualization using a valid user name and password. Further information can be found in the Cyber-Security documentation within the PLC Designer.

Authenticate as an advanced user.

# Controller 1.x

## Security functions

After authentication is complete, the advanced diagnosis visualization becomes visible, and the "Certificate Handler" menu item can be selected.

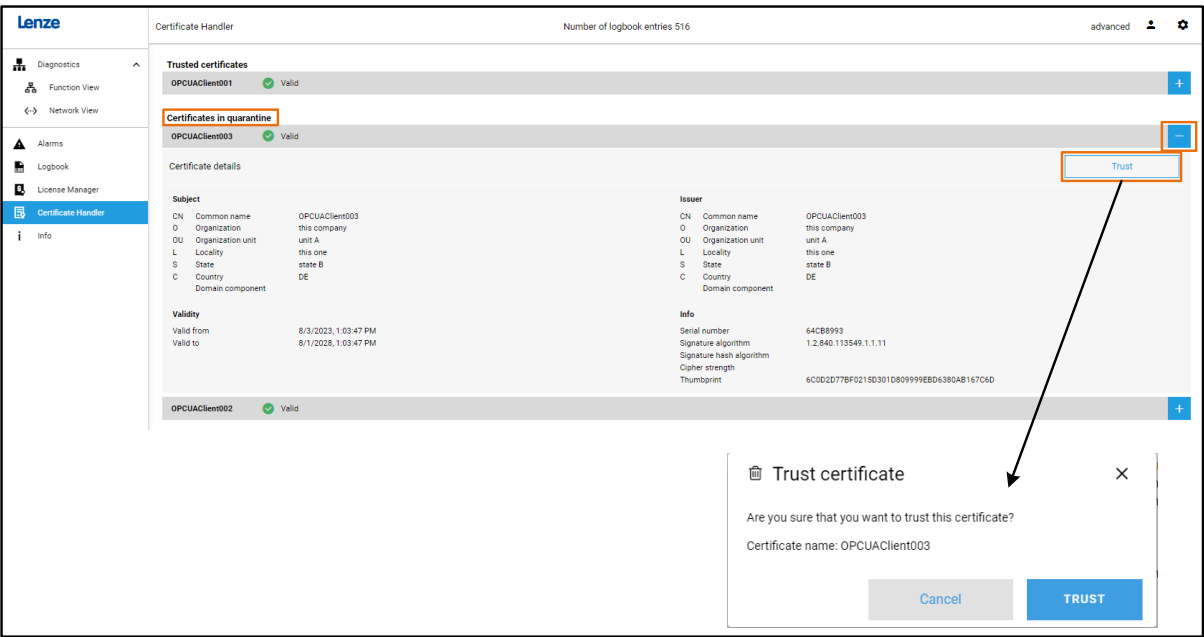


### Overview

Selecting the "Certificate Handler" option makes the trusted and quarantined certificates visible. A symbol indicates the validity status.

| Symbol                  | Legend                                                                                                     |
|-------------------------|------------------------------------------------------------------------------------------------------------|
| green hook              | <b>valid certificate</b><br>The certificate is valid.                                                      |
| yellow exclamation mark | <b>certificate, that will expire soon</b><br>The certificate is valid, but it will expire <= 27 months.    |
| red exclamation mark    | <b>expired certificate</b><br>The certificate is not valid (either it has not yet valid or it is expired). |

When unfolding the detail view of a certificate in the quarantine, some detailed information will be shown. Selecting the Trust button will open a dialog where the user can trust the selected certificate.



---

Trust Certificate

# Controller 1.x

## Security functions

On the other hand, when unfolding the detail view of one certificate in trusted certificates, some detailed information will be shown. Selecting the Delete button will open a dialog where the user can delete the selected certificate.

The screenshot shows the Lenzx Certificate Handler interface. The left sidebar contains navigation options: Diagnostics, Function View, Network View, Alarms, Logbook, License Manager, Certificate Handler (selected), and Info. The main area displays 'Trusted certificates' with a table listing certificates. The first certificate, OPCUAClient001, is selected and its details are shown. The details include Subject, Issuer, Validity, and Info. A 'Delete' button is highlighted with an orange box. An arrow points from this button to a 'Delete certificate' dialog box. The dialog box contains the text: 'Delete certificate', 'Are you sure that you want to delete this certificate? This action cannot be undone.', 'Certificate name: OPCUAClient001', and 'Cancel' and 'DELETE' buttons.

| Subject |                   | Issuer |                   |
|---------|-------------------|--------|-------------------|
| CN      | Common name       | CN     | Common name       |
| O       | Organization      | O      | Organization      |
| OU      | Organization unit | OU     | Organization unit |
| L       | Locality          | L      | Locality          |
| S       | State             | S      | State             |
| C       | Country           | C      | Country           |
|         | Domain component  |        | Domain component  |

| Validity   |                      |
|------------|----------------------|
| Valid from | 8/3/2023, 1:04:35 PM |
| Valid to   | 8/1/2028, 1:04:35 PM |

| Info                     |                                         |
|--------------------------|-----------------------------------------|
| Serial number            | 64C889C3                                |
| Signature algorithm      | 1.2.840.113549.1.1.11                   |
| Signature hash algorithm |                                         |
| Cipher strength          |                                         |
| Thumbprint               | 4AC5F680C3E510875CFE1F9E1A98E92F87BE965 |

| Certificates in quarantine |       |
|----------------------------|-------|
| OPCUAClient003             | Valid |
| OPCUAClient002             | Valid |

Delete Certificate

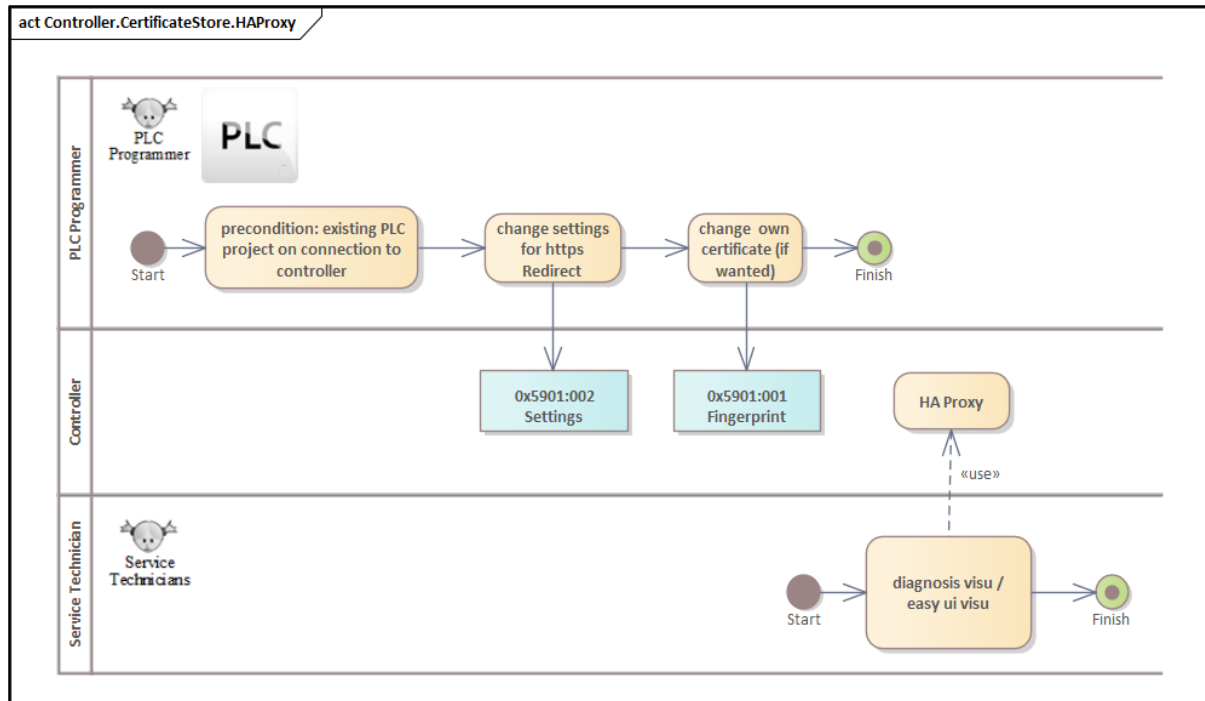


When a certificate is trusted or deleted by a user, the visualization automatically updates. However, if a certificate is created by another participant or its status changes, the changes are not visible automatically. Instead, a refresh must be carried out via the browser.

## Controller.CertificateStore.HAProxy

Secure Communication has been available since FW version 01.04.00.

Handling the certificate for the Secure Communication in the Controller.CertificateStore has been available since FW version 01.11.00.



Activity Diagram

The controller supports communication via the HTTP and HTTPS. Using the HTTPS instead of HTTP offers your data additional protection against unauthorized access. This is because the transmission is encrypted and there are authentication possibilities. However, these additional functionalities can only be achieved through increased resource consumption and organizational effort.

When selecting a communication protocol, consider the given network structure, security needs, capabilities of the web application, and effort (administrative and resource-related).

### Delivery Condition

By default, the controller offers both http and HTTP and HTTPS protocols for various services. It is therefore a decision of the users whether they communicate encrypted (https) or unencrypted (http). For example, a web browser can load a website of the controller via HTTP or HTTPS.

For HTTPS communication, the controller uses a self-signed certificate, which is generated when the hardware is started for the first time. Users can verify this certificate and authenticate the server.

This certificate is not backed up during a backup / device replacement. In the event of a hardware replacement, the users must therefore trust the new certificate.

# Controller 1.x

## Security functions

---

### Parameters for Displaying the Certificate Fingerprint

The 0x5901:001 parameter displays the fingerprint of the certificate that the controller uses to identify itself to the client during an HTTPS connection. To authenticate the server, the string displayed here must exactly match the fingerprint of the server certificate displayed in the web client (e.g., web browser).

| Address    | Name / Setting Range / [Default]        | Info                                                   |
|------------|-----------------------------------------|--------------------------------------------------------|
| 0x5901:001 | Certificate fingerprint<br>Display only | Fingerprint of Certificate for https/wss communication |

### Visualization

The controller provides a visualization system with built-in user management. Login data is considered particularly sensitive information. For this reason, an HTTPS connection with configured user management is recommended for visualization.

To prevent the use of HTTP in the context of visualization, the controller redirects client requests for visualization content to HTTPS. Redirection is an instruction to the user to switch to an HTTPS connection. While a user is not forced to follow this instruction, all current browser versions should fulfill it.

### Parameters for Configuring the https Forwarding of the Visualization

By default forwarding visualization content to an https connection is deactivated. To enable forwarding, the parameter 0x5901:002 must be set to "1".

This parameter represents a security-critical functionality. Therefore, it cannot be changed by engineering tools such as the »EASY Starter« or the »PLC Designer«. The application program can only change the parameter value by appropriately controlling the "L\_IPAP\_ChangeHttpsRedirectSetting4EasyUI" function block.

The function block "L\_IPAP\_ChangeHttpsRedirectSetting4EasyUI" is included in the library "L\_IPAP\_ParameterManagerAccess" as of version 03.24.00 of the »PLC Designer«. This function block enables changing the configuration to "Disabled. Https redirect for EASY UI." or "Enabled. Https redirect for EASY UI.", by writing the appropriate enumeration value to the parameter.

After changing the parameter value, the settings are loaded by the firmware and necessary services are restarted. This can lead to disconnections in the web application. For this reason, among other, it is recommended to write the parameter value only if a new setting is required.

The parameter setting is stored permanently on the device. The setting is not transferred during a device replacement/backup. Therefore, if new hardware is used, the parameter must be set again by the application program.

| Address    | Name / Setting Range / [Default] |                                       | Info                                                                                                                      |
|------------|----------------------------------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 0x5901:002 | Https redirect setting           |                                       | Display of the current setting                                                                                            |
|            | 0                                | Disabled. Https redirect for EASY UI. | http and https requests for visualization content are answered directly                                                   |
|            | 1                                | Enabled. Https redirect for EASY UI.  | http requests for visualization content are answered with a redirect, which prompts the client to use an https connection |
|            | 2                                | Changing. Https redirect for EASY UI. | Status feedback only                                                                                                      |
|            | 3                                | No access. HAProxy not active.        |                                                                                                                           |



Up to version 01.10.00 this redirect only applies to the diagnosis pages (i.e. pages beginning with /diagnosis) and the Easy UI project pages (i.e. pages beginning with /easyui). From version 01.11.00 on wards, the redirect also applies to the actual landing page of the controller and to all HTML pages stored on the SD card by the customer.

### Troubleshooting

#### Web client (e.g., a browser) reports security risks when establishing a connection

As the controller uses self-signed certificates, clients such as web browsers cannot automatically authenticate the server (the controller). This is because clients determine the authenticity of a certificate, and thus of a server, by checking the certificate signature. This check fails for self-signed certificates because they were issued by a certification authority that is unknown and therefore not trustworthy to the client.

To check the authenticity manually, the certificate fingerprint from the above parameter can be read out with an engineering tool such as the »EASY Starter« or the »PLC Designer« and compared with the fingerprint of the certificate received in the web client (e.g. web browser). If the two fingerprints match exactly, it is probably the correct server (complex attacks can be deceiving here).

If the authenticity is established, an exception can be added to the browser for this address and the connection can be continued.

It is recommended to include an exception in the security check for this address only. For security reasons, installing the certificate so that it can be used to authenticate other addresses is not permitted.

#### Website is not working correctly with https

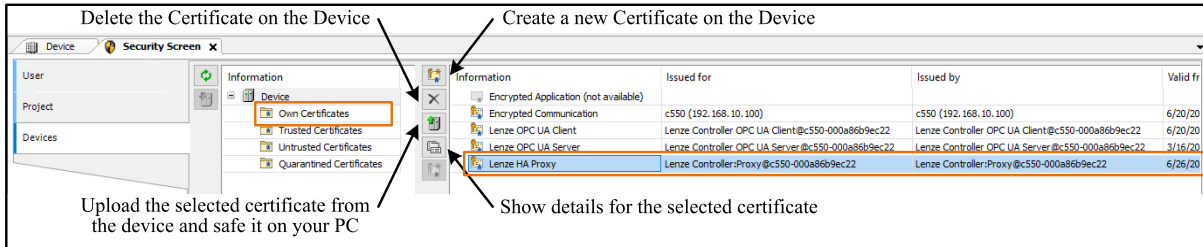
A website can have complex communication channels and load content from different sources, as well as communicate bidirectionally. If a website is loaded via https instead of http, conflicts can easily arise because https requires different resources/addresses and sets new requirements for the web application.

Typically, conflicts arise due to fixed specifications within the website. The most common causes of errors are the rigid specification of a port number and the fixed specification of the communication paths (secured/unsecured). The port number often causes a problem because https is typically offered on a different port than http. The fixed specification of a communication path leads, for example, to problems if unsecured communication is to be made from a website loaded via https. In such cases, most browsers will refuse communication due to the security risk. For example, it is not allowed to open an unsecured web socket or embed http content within an https site.



## Replace Certificate for HA Proxy

To replace the automatically generated certificate, open the Security Screen in the »PLC Designer« and select the "Device" tab.



Replace Certificate

Details of this automatic generated certificate can be found in this documentation, (refer to chapter [Controller.CertificateStore.HAProxy:Certificate](#)

At this point, the certificate for the "Lenze HA Proxy" can be recreated or deleted. Details on this can also be called up.



A certificate is mandatory for a secure https connection. Existing connections are also terminated if the HA Proxy certificate has been deleted and a new one has not yet been generated.

### Example:

A web browser is connected via https to the diagnosis visualization of the controller and the user has passed the authentication successfully. With an existing https connection, the certificate is deleted with the »PLC Designer«. As a reaction, the connection is immediately interrupted and an error message appears in the browser "...Client cannot communicate. Socket is not available...". If now a new HA Proxy certificate is generated with the »PLC Designer« and the user pushes the reload button on the browser page, the https connection will be established and the user has to authenticate again.

Behavior when HA Proxy certificate is deleted after different reset levels:

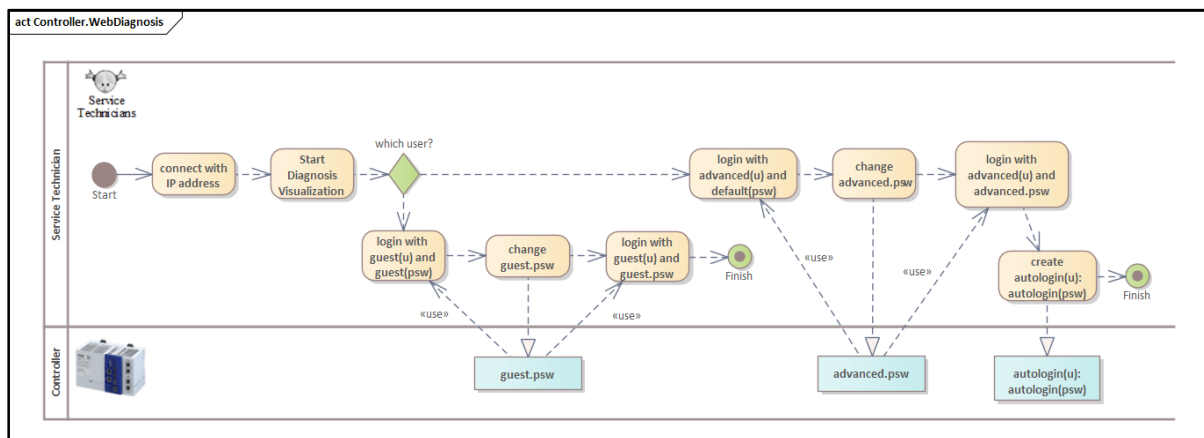
| Reset Level                                   | Behavior                                                 |
|-----------------------------------------------|----------------------------------------------------------|
| Manually stop and start the application       | The HA Proxy Certificate is still deleted.               |
| Reset Warm                                    | The HA Proxy Certificate is still deleted.               |
| Reset Cold                                    | The HA Proxy Certificate is still deleted.               |
| Reset Origin and create the application again | The HA Proxy Certificate is still deleted.               |
| Boot the Controller                           | The HA Proxy Certificate is automatically generated new. |

# Controller 1.x

## Security functions

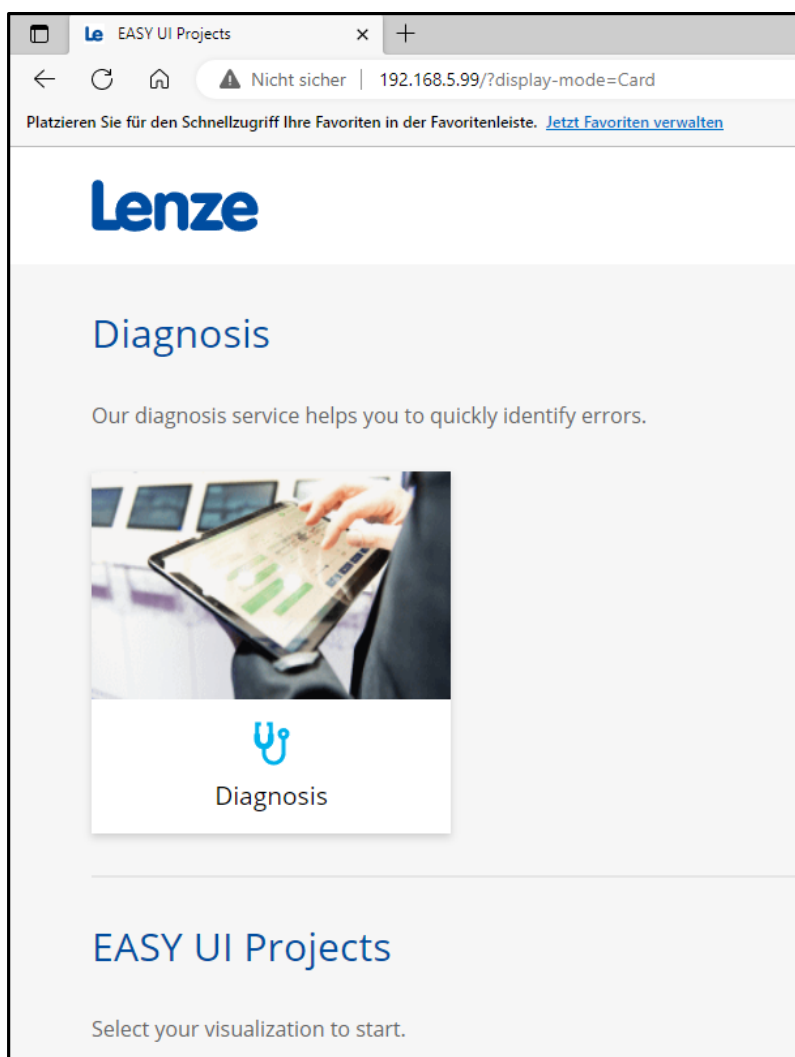
### Controller.WebDiagnosis

The controller has provided diagnostics via web access since firmware version 01.09.00.



Activity Diagram

For this purpose, the web server can be addressed by entering the IP address in a browser.



Web server diagnosis

# Controller 1.x

## Security functions

After calling the web diagnostics, the login screen appears.

# Log on user





Log on

Note: Since the automatic login is not activated, you have to log on to the web visualization using a valid EASY UI user name and password. You can configure the users in the server project under user groups in the user management.

Log on Screen

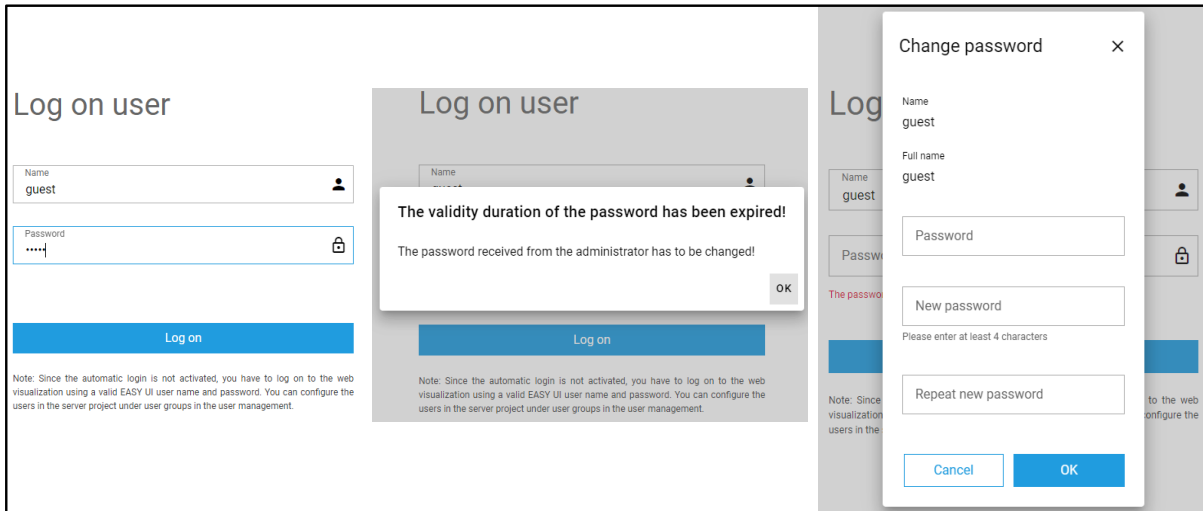
By default, two users / groups / passwords are created:

- User: guest  
member of group: Guests  
Password: guest
- User: advanced  
member of group: Advanced  
Password: default

The Guests group has only read rights on the controller and cannot change any data. The only exception is the "global reset" function, which is also possible as a guest user. The Advanced group also has the right to change the controller's data (e.g. delete the logbook).

## Initial login with a request for a password change

When the two users in the Users and Advanced groups are called up for the first time, the respective password must be changed.



Change password procedure

## Hardening of Guest and Advanced users

The "Guest" and "Advanced" users are created by default and their password must be changed at first use. With the exception mentioned above, the "Guest" user has only read rights on the controller. This user is available by default and cannot be deleted. Use the "User settings" to change the password.

## Activate Autologin

The "Guest" and "Advanced" users are created by default their password must be changed at first use. If a simple call of the WebDiagnosis is desired and the customer waives the security function, he can perform the following steps:

- a logged-in advanced user is the basic requirement, i.e. the guest user may not perform the following steps.
- A new user must be added with "add user".  
Name: autologin  
UserGroup: Guests  
Password: autologin  
State: Active
- Due to the presence of this user, the authorization is skipped and an auto-logon is performed. This mechanism completely disables authorization.

## Deactivate Autologin

After activating auto login, the user can deactivate it via the following steps:

- Log in automatically with the user "autologin".
- Choose "Logon user".
- Log on with "Advanced" user and the advanced password.
- Choose "Remove user".
- Remove user "autologon".

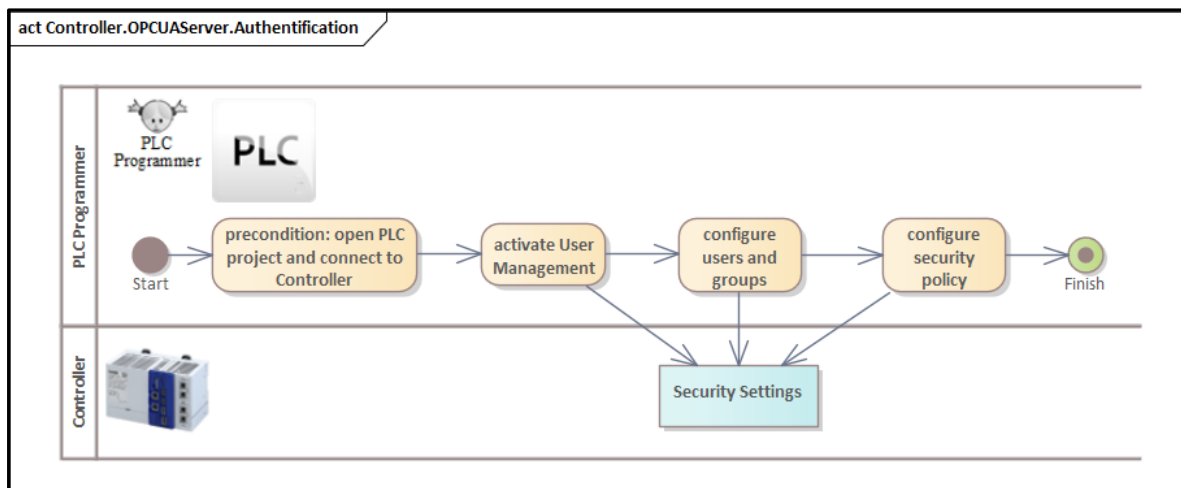
# Controller 1.x

## Security functions

### Controller.OPCUAServer.Authentication

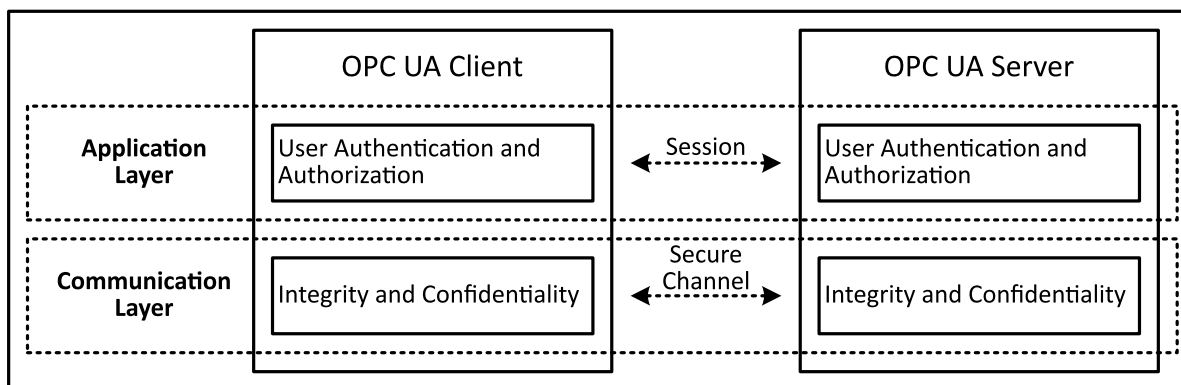
In order to be able to use the authentication of the OPC UA server, the controller user management is required. This process is described in chapter [Controller.UserManagement](#).

The following diagram shows the process.



Activity Diagram

In order to establish a connection to the OPC-UA Server, an OPC-UA Client must use the end-point url and take the corresponding security settings into account. The architecture of OPC-UA provides for a secure channel and a session. Confidentiality and integrity are secured for the Secure Channel and authentication and authorization for the session.



Security Channel and Session

These security settings are described below. Here, the Security Policy and the Message Security Mode are used for the Secure Channel configuration and the authentication for the session.

### Security Policy

When the connection between OPC UA Client and OPC UA Server is started, the security policies are transmitted by the server. Within this Cipher Suite, the OPC UA Client can select a suitable connection. Several settings are usually offered here, such as Basic256Sha256.

## Message Security Mode

The Message Security Mode specifies the type of transmission. The options are None, Sign and Sign & Encrypt.

- None  
Does not include security mechanisms and should only be used for testing purposes and therefore not for productive operation.
- Sign  
Includes security mechanisms to ensure integrity.
- Sign & Encrypt  
Includes security mechanisms to ensure integrity and confidentiality.

## Authentication

In authentication, the user is associated with the session. The following three settings are possible.

- Anonymous  
No dedicated user is used for the session, but the connection is created anonymously.
- Username and Password  
A user must identify himself with username and password and will be associated with the session.
- Certificate and Private Key  
Authentication of a user with the help of certificates. Not currently supported.

## Authenticate an OPC-UA Client without an activated user management

In the following, the connection to the OPC-UA Server is described without user management being activated on the Controller. An OPC-UA Client can connect without having to authenticate the user.



In the »PLC Designer«, the following setting option exists for the device: Device > Communication Settings > Device > Change Runtime Security Policy ... > [Check-box] Allow anonymous login. Without an activated user management, the following setting in the »PLC Designer« has no effect, i.e. when deselecting Allow anonymous login, an anonymous connection is possible.



If an OPC-UA Client with a username and password authentication connects to the OPC-UA Server without active user management, a connection is generally possible. Neither the username nor the password is checked, as there is no activated user management with corresponding data. The connection is therefore synonymous with anonymous authentication.

# Controller 1.x

## Security functions

---

### Authenticate an OPC-UA Client with activated user management

With an activated user management, an OPC-UA Client can connect in two authentication modes:

- Anonymous  
No dedicated user is used for the session, but the connection is created anonymously.
- Username and Password  
A user must identify himself with Username and Password and will be associated with the session.
- Certificate and Private Key  
Not currently supported.

### Anonymous

Regardless of the user in the user management, OPC-UA Clients can connect anonymously with this authentication mode, if allowed by the OPC-UA Server.

### Username and Password

If the OPC-UA Client selects the authentication Mode username and Password, these must match a user in the user management to establish a connection. To restrict the user access to specific symbols the usage of symbol sets and the symbol rights configuration are required. Otherwise, all users can access all symbols. If the user does not exist or the password does not match, a connection is refused.

### Prohibit anonymous login

To prohibit the Anonymous Login, please use the setting option in the »PLC Designer« for the device: Device > Communication Settings > Device > Change Runtime Security Policy ... > [Checkbox] Allow anonymous login. With an activated user management, this checkbox can be used to deactivate the Anonymous Login.

If an OPC-UA Client now wants to connect via Anonymous, this is prohibited. If an OPC UA Client wants to connect to the authentication mode Username and Password, and these match a user in the user management, the connection is allowed.



## Delete user Anonymous\_OPCUAServer

The following procedure is provided for informational purposes only and is not recommended. In order to prohibit an anonymous connection of an OPC-UA Client, the previously described method should be used.

If user management is activated, an Anonymous\_OPCUAServer user is automatically created. This can be permanently removed manually.

If an OPC-UA Client now wants to connect via Anonymous, this is prohibited. If an OPC-UA Client wants to connect to the authentication mode Username and Password, and these match a user in the user management, the connection is allowed.



If you want to restore the user Anonymous\_OPCUAServer after deleting it, there are two options. The first is to delete the complete user management on the SD card from the controller. Afterwards, user management must be activated via the »PLC Designer«. This step restores the previously manually deleted user Anonymous\_OPCUAServer. Previously created users and groups must be rebuilt manually. The second option is to disable and re-enable the Allow anonymous log in setting. As a result, the user is Anonymous\_OPCUAServer created again.

# Controller 1.x

## Security functions

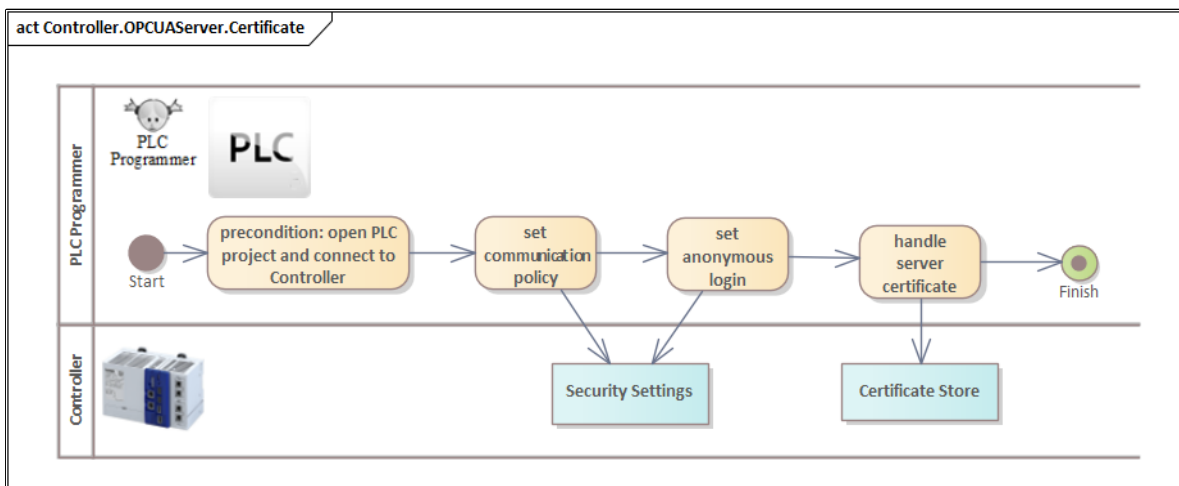
### Controller.OPCUAServer.Certificate

The OPC-UA Server offers the following message security modes:

- None  
Does not include security mechanisms and should only be used for testing purposes and therefore not for productive operation.
- Sign  
Includes security mechanisms to ensure integrity.
- Sign & Encrypt  
Includes security mechanisms to ensure integrity and confidentiality.

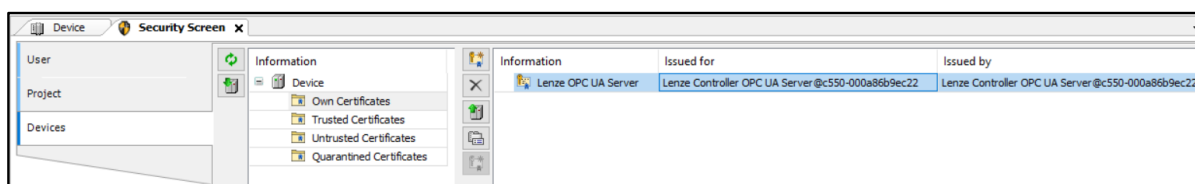
If the selection "Sign" or "Sign & Encrypt" is selected here, certificate handling is required.

This can be set on the server side as follows.



Activity Diagram

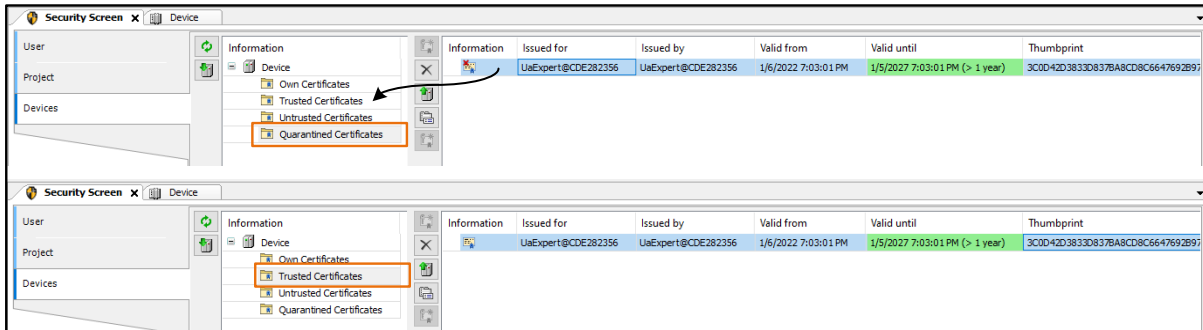
When the controller is started for the first time, a separate certificate is created for the OPC-UA Server. This can be seen in the Security Screen under Devices in the "Own Certificates" section.



Own Certificate

The certificate automatically created here is a self-signed certificate with a term of 50 years. If the runtime is to be reduced for security reasons, the certificate can be replaced using the function "Create a new certificate on the device" ([Controller.CertificateStore.viaPLCDesigner](#)).

When an OPC-UA Client connects to the OPC-UA Server, the respective own certificates are exchanged. With the OPC-UA Server, the received client certificate will then be found under "Quarantined Certificates".



Handling Client Certificates

This must then be moved from quarantine to the "Trusted Certificates" section. For this purpose, the »PLC Designer« can be used as shown ([Controller.CertificateStore.viaPLCDesigner](#)) or the diagnostic visualization ([Controller.CertificateStore.viaAdvancedVisu](#)). Once it has been moved to the trusted area, the connection between client and server can be established.

## Controller.OPCUAServer.GDS

This functionality has been available since controller firmware version 01.13.00.

### In general

OPC UA provides the functionality to use a global discovery server (GDS). The GDS is used for a centralized certificate handling. The GDS sends certificates and trust lists to the different OPC UA Clients and Servers in the network. A Global Discovery Server is used for a centralized and automated certificate management. In this scenario all device certificates are signed by a certificate authority. It is therefore no longer necessary to manage self-signed certificates decentrally with a manufacturer-specific engineering tool.

The GDS can send the certificates using the "push" mode, or the servers and clients can call for them using the "pull" mode.

The GDS will watch the validity period of the different certificates and will update/exchange them before the period ends.

The complete communication is done by certified secured OPC UA communication.

Lenze doesn't provide a GDS. However, the Lenze OPC UA Server on the controller is able to connect to an external GDS for registration and certificate management.

## Controller.OPCUAServer.GDS.Provisioning

The provisioning mode is used for the initial deployment of certificates on the server. In this mode the server will accept all client certificates although they aren't trusted.

The Lenze OPC UA Server has the parameter 0x2471:129 for enabling the provisioning mode.

### 0. Disabled[default]

- The provisioning mode is disabled.

### 1. Enabled Automatic:

- The provisioning mode is only enabled if there is no trust list (trusted certificates) available.

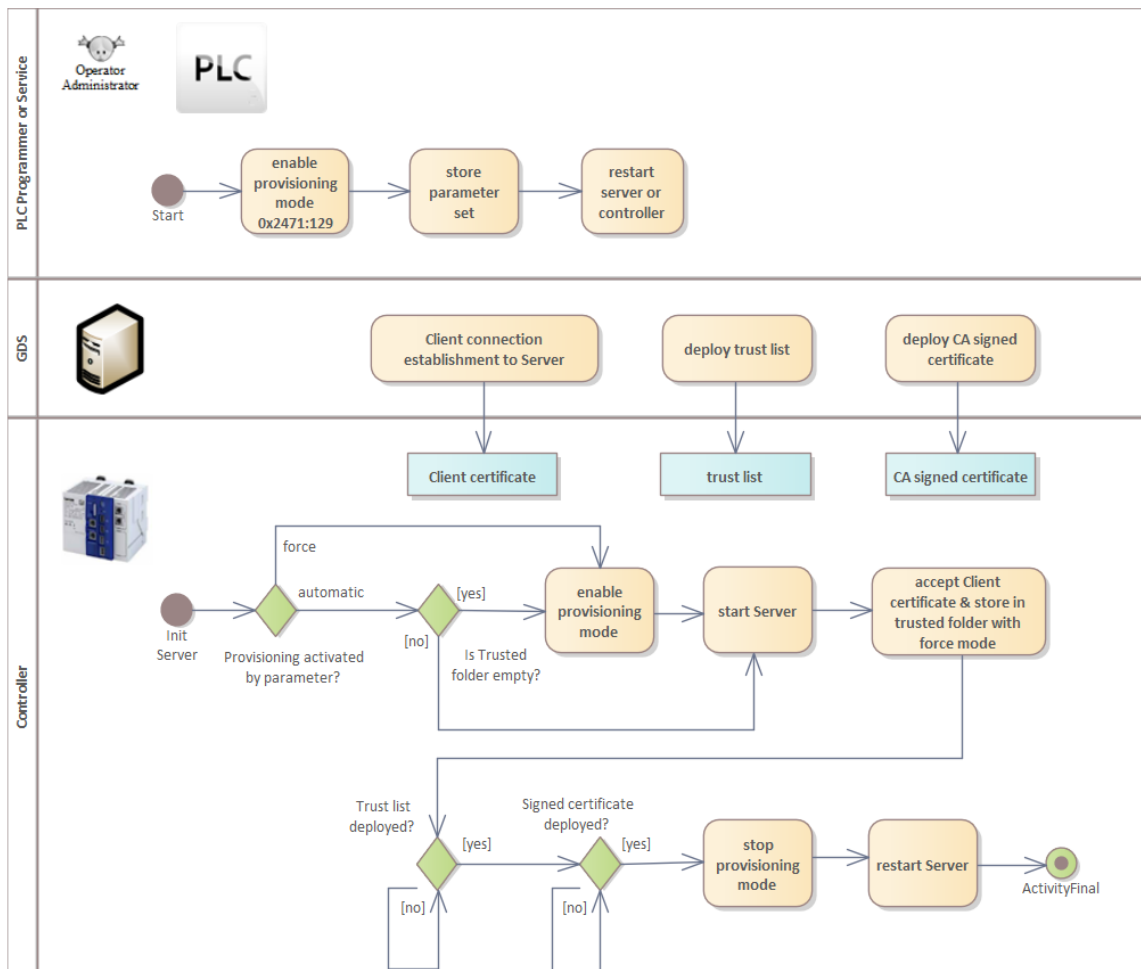
# Controller 1.x

## Security functions

- The provisioning mode is ended automatically if a trust list and CA signed certificate is deployed or one hour has passed.

### 2. Enabled Force

- This provisioning mode stores the accepted certificates in the trust list..
- This provisioning mode is always enabled after server restart.
- The provisioning mode is ended automatically if a trust list and CA signed certificate is deployed.
- Caution: This mode has to be deactivated by the setting parameter otherwise the mode will be enabled again after server restart.



Activity Diagram



Is the provisioning mode active, the server will accept all client certificates!

- Activate the user management to protect the server from unauthorized access.
- Publish just for the application necessary services (e.g. file system) and PLC variables.

## Controller.OPCUAClient.Authenticate

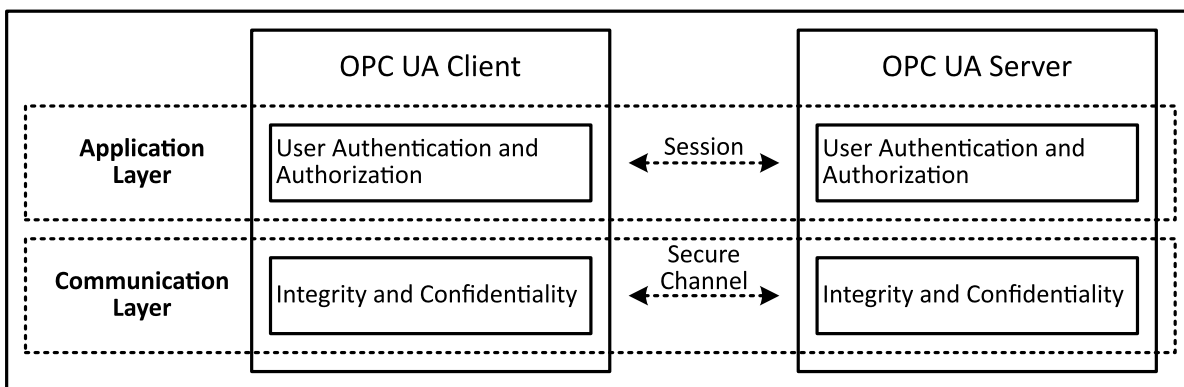
This function has been available since firmware version 01.09.00 of the controller.

To be able to use an OPC-UA Client, the complete communication must be programmed in the »PLC Designer«. The »PLC Designer« therefor provides several function blocks:

- UA\_Connect
- UA\_Disconnect
- UA\_NamespaceGetIndexList
- UA\_ConnectionGetStatus
- UA\_NodeGetHandleList
- UA\_NodeReleaseHandleList

The authentication of the OPC-UA Client is done by the function block "UA\_Connect". The authentication handling is done by the input structure "UserIdentityToken" and "SessionConnectInfo".

To establish a connection to the OPC-UA Server, an OPC-UA Client must use the endpoint url and take the corresponding security settings into account. The architecture of OPC-UA provides for a secure channel and a session. Confidentiality and integrity are secured for the Secure Channel and authentication and authorization for the session.



Security Channel and Session

These security settings are described below. Here, the "SecurityMsgMode", Security Policy and "UserIdentityToken" are used for the Secure Channel configuration and the authentication for the session.

# Controller 1.x

## Security functions

---

### SecurityMsgMode

The variable is part of the "SessionConnectInfo" structure. The following list shows the options that can be selected.

- BestAvailable  
Best available message security mode to the UA server. The client receives the available message security from the server and selects the best. This could also result in level "none security".
- None  
No security is applied.
- Sign  
All messages are signed but not encrypted.
- SignEncrypt  
All messages are signed and encrypted.

### Security Policy

When the connection between OPC-UA Client and OPC-UA Server is started, the security policies are transmitted by the server. Within this Cipher Suite, the OPC-UA Client can select a suitable connection. Several settings are usually offered here, such as Basic256Sha256.

This is done by the "SecurityPolicy" variable which is part of the "SessionConnectInfo" structure.

The "SecurityPolicy" specifies the type of encryption of the transaction. The options available are Best Available, None, Basic256Sha256 and Aes256Sha256RsaPss.

- BestAvailable  
Best available message security mode to the UA server. The client receives the available message security from the server and selects the best. This could also result in level "none security".
- None  
<http://opcfoundation.org/UA/SecurityPolicy#None>
- Basic256Sha256  
<http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256>
- Aes256Sha256RsaPss  
[http://opcfoundation.org/UA/SecurityPolicy#Aes256\\_Sha256\\_RsaPss](http://opcfoundation.org/UA/SecurityPolicy#Aes256_Sha256_RsaPss)

### UserIdentityToken

In "UserIdentityToken", the user is associated with the session. This is not used to encrypt the transaction. This is used to identify the user at the server. The following three settings are possible.

- Anonymous  
No dedicated user is used for the session, but the connection is created anonymously.
- Username and Password  
A user must identify himself with username and password and will be associated with the session.
- Certificate and Private Key  
Authentication of a user with the help of certificates. Not currently supported.

## Authenticate an OPC-UA Client without an activated user management

In the following, the connection to the OPC-UA Server is described without user management being activated on the controller. An OPC-UA Client can connect without having to authenticate the user.



In the »PLC Designer«, the following setting option exists for the device: Device > Communication Settings > Device > Change Runtime Security Policy ... > [Check-box] Allow anonymous login. Without an activated user management, the following setting in the »PLC Designer« has no effect, i.e. when deselecting Allow anonymous login, an anonymous connection is possible.



If an OPC-UA client with a username and password authentication connects to the OPC-UA server without active user management, a connection is generally possible. Neither the username nor the password is checked, as there is no activated user management with corresponding data. The connection is therefore synonymous with anonymous authentication.

## Anonymous

Regardless of the user in the user management, OPC-UA Clients can dial in anonymously with this authentication mode, if allowed by the OPC-UA Server.

# Controller 1.x

## Security functions

### Controller.OPCUAClient.Certificate

This functionality has been available since controller firmware version 01.11.00.

In contrast to the server, the OPC UA communication settings for clients must be programmed in the »PLC Designer«. The »PLC Designer« therefor provides several function blocks:

- UA\_Connect
- UA\_Disconnect
- UA\_NamespaceGetIndexList
- UA\_ConnectionGetStatus
- UA\_NodeGetHandleList
- UA\_NodeReleaseHandleList

The certificate handling of the OPC-UA client is done by the function block "UA\_Connect" function block. The certificate handling is done by the variable "SecurityMsgMode" variable.

#### SecurityMsgMode

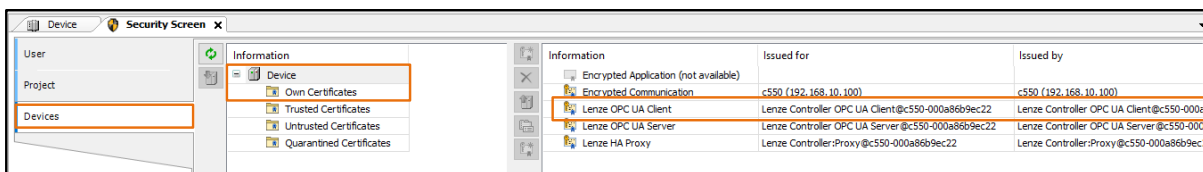
The variable "SecurityMsgMode" which is part of the structure "SessionConnectInfo".

- BestAvailable  
Best available message security mode to the UA server. The client receives the available message security from the server and selects the best. This could also result in level "none security".
- None  
No security is applied.
- Sign  
All messages are signed but not encrypted.
- SignEncrypt  
All messages are signed and encrypted.

If the selection "Sign" or "Sign & Encrypt" is selected here, certificate handling is required.

This can be set on the client side as follows.

When the controller is started for the first time, a separate certificate is created for the OPC-UA Client. This can be seen in the Security Screen under Devices in the "Own Certificates" section.

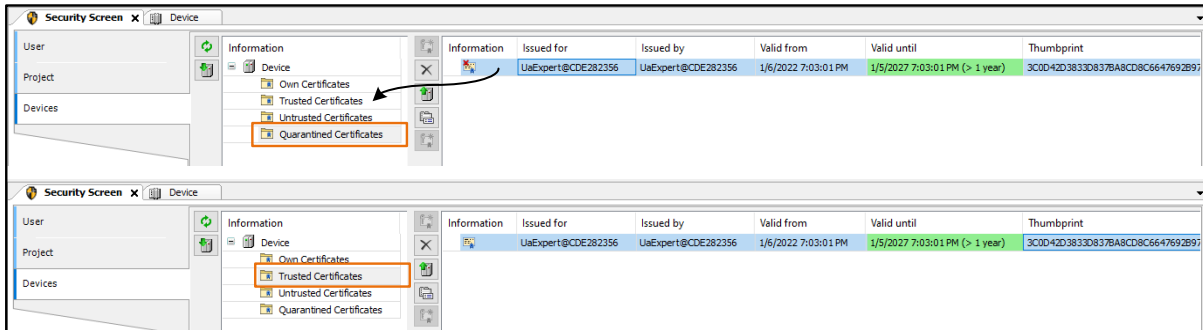


Own Certificate

The certificate automatically created here is a self-signed certificate with a term of 50 years. If the runtime is to be reduced for security reasons, the certificate can be replaced using the function "Create a new certificate on the device" ([Controller.CertificateStore.viaPLCDesigner](#)).



When an OPC-UA Client connects to, the respective own certificates are exchanged. With the OPC-UA Client, the received server certificate will then be found under "Quarantined Certificates".

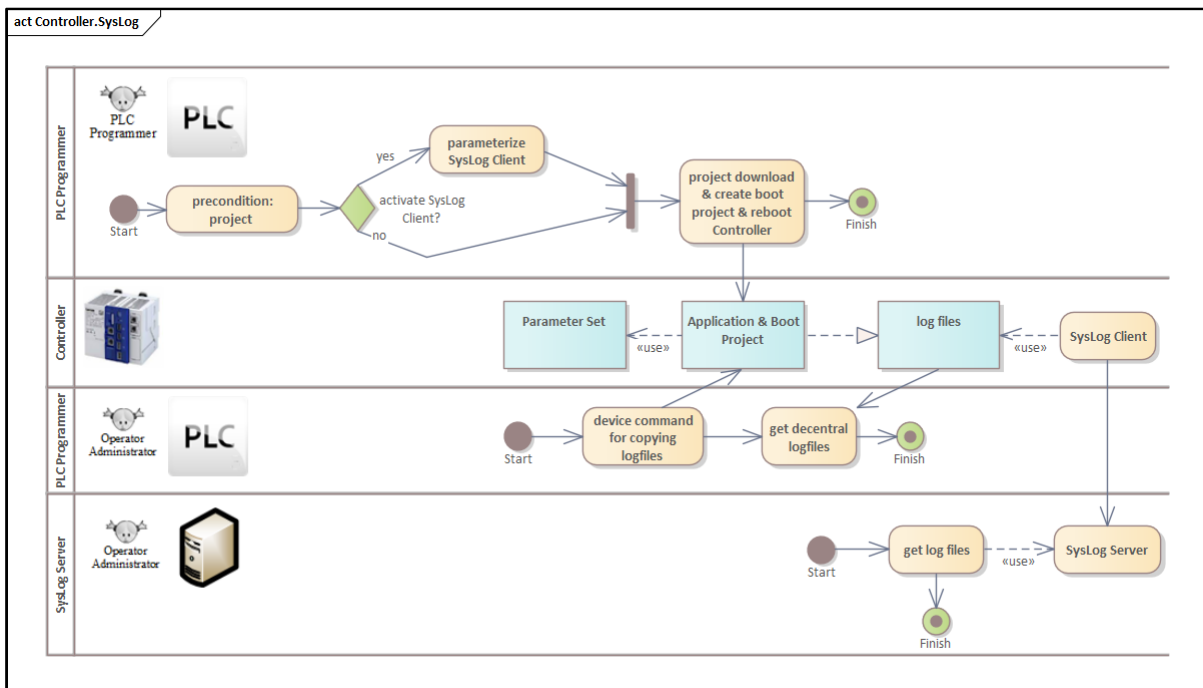


Handling Client Certificates

This must then be moved from "Quarantined Certificates" to the "Trusted Certificates" section. For this purpose, the »PLC Designer« can be used as shown ([Controller.CertificateStore.viaPLCDesigner](#)) or the diagnostic visualization ([Controller.CertificateStore.viaAdvancedVisu](#)). Once it has been moved to the trusted area, the connection between Client and Server can be established.

## Controller.SysLog

The SysLog (System Logging Protocol) function enables the controller to log its important activities in local log files and optionally send them to a central SysLog server via a SysLog protocol. This enables the end user to monitor their infrastructure. This functionality is available from firmware version 1.13.0 on.



Activity Diagram

# Controller 1.x

## Security functions

1. Activate and parameterize the SysLog Client
2. Prepare the controller to access the local logfiles
3. Get local logfiles
4. Get logfiles from SysLog Server



In the event of a power failure, the local log file messages and messages sent via the syslog client are not guaranteed. Messages may not be saved or transmitted. One solution could be to use a UPS.

### Activate and parameterize the SysLog Client

The function can be parameterized using the following parameters. Please note that these parameters must be saved persistently in the parameter set and the controller must be restarted for the parameters to become valid.

#### Activate SysLog Client

The controller has two logging options:

- Internal logging into local log files
- Sending of logging messages via the SysLog protocol to a SysLog Server

The local logging is always active, but the sending of logging messages can be activated with the following parameter.

Parameter for SysLog Client activation

| Address    | Name                                   |                       | Info                         |
|------------|----------------------------------------|-----------------------|------------------------------|
| 0x5914:001 | SysLog Client: SysLogClient activation |                       | SysLog Client activation     |
|            | enum 0                                 | Deactivated (default) | SysLog Client is deactivated |
|            | enum 1                                 | Activated             | SysLog Client is activated   |

#### SysLog Server IP address.

This is the IP v4 address of the SysLog Server.

Parameter for SysLog Server IP address

| Address    | Name                                                                                              | Info                        |
|------------|---------------------------------------------------------------------------------------------------|-----------------------------|
| 0x5914:002 | SysLog Client: IP address of SysLog Server<br>UDINT 4 bytes<br>0.0.0.0 (default) –255.255.255.255 | IP address of SysLog Server |

#### SysLog Server Port

This is the parameter for the port of the SysLog Server. This setting is independent of whether a protocol udp or tcp is selected.

Parameter for SysLog Server Port

| Address    | Name                                                                               | Info                  |
|------------|------------------------------------------------------------------------------------|-----------------------|
| 0x5914:003 | SysLog Client: Port of SysLog Server<br>UDINT 2 bytes<br>0 – 514 (default) - 65535 | Port of SysLog Server |



Due to blocked outgoing TCP sockets in the Linux environment, ports up to 1000 cannot be used for TCP. A port greater than 1000 must therefore be selected to send TCP Messages.

## SysLog Protocol Type

This is the parameter for the protocol of the SysLog Messages.

Parameter for SysLog Protocol Type

| Address    | Name                               |               | Info                        |
|------------|------------------------------------|---------------|-----------------------------|
| 0x5914:004 | SysLog Client: SysLog ProtocolType |               | SysLog Client Protocol Type |
|            | enum 0                             | UDP (default) | SysLog Messages via UDP     |
|            | enum 1                             | TCP           | SysLog Messages via TCP     |

## SysLog Message Encryption

This is the parameters for setting the optional encryption of the SysLog Messages.

Parameter for encryption of the SysLog messages

| Address    | Name                                     |                                    | Info                          |
|------------|------------------------------------------|------------------------------------|-------------------------------|
| 0x5914:005 | SysLog Client: SysLog Message Encryption |                                    | SysLog Message Encryption     |
|            | enum 0                                   | not encrypted SysLog protocol      | Cleartext Messages via SysLog |
|            | enum 1                                   | with TLS encrypted SysLog protocol | TLS Encrypted SysLog Messages |

## SysLog Message Severity Filter

These are the parameters for filtering the SysLog Messages via Severity.

Parameter for filtering the SysLog severities

# Controller 1.x

## Security functions

| Address    | Name                              |                                 | Info                                                     |
|------------|-----------------------------------|---------------------------------|----------------------------------------------------------|
| 0x5914:006 | SysLog Client: Message Severities |                                 | Filter for SysLog Message Severities                     |
|            | bit 0                             | emerg (default = activated)     | Severity Emergencies "System unusable"                   |
|            | bit 1                             | alert (default = activated)     | Severity Alerts "Immediate action needed"                |
|            | bit 2                             | crit (default = activated)      | Severity Severity Critical "Critical conditions"         |
|            | bit 3                             | err (default = activated)       | Severity Severity Error "Error conditions"               |
|            | bit 4                             | warning (default = deactivated) | Severity Warning "Warning conditions"                    |
|            | bit 5                             | notice (default = deactivated)  | Severity Notification "Normal but significant condition" |
|            | bit 6                             | info (default = deactivated)    | Severity Information "Informational messages only"       |
|            | bit 7                             | debug (default = deactivated)   | Severity Debugging "Debugging messages"                  |



The parameter 0x5914:006 for filtering the Severities is working for the SysLog-Client functionality and the local logfiles on the controller. The filter works on local log files even if the SysLog Client is deactivated.

These parameters can be modified for example via the parameter list or the user dialog via Settings \ Communication \ System Logging Protocol (SysLog).

Diagnosis
Settings
Parameter list
Trend

Communication\System Logging Protocol (SysLog)

SysLog (System Logging Protocol) is a standard for logging and transmitting log messages in an IT- and OT- network.

|                            |                   |
|----------------------------|-------------------|
| SysLog Client activation   | Activated [1]     |
| IP address of SysLog Se... | 192.168.15.126    |
| Port of SysLog Server      | 514               |
| SysLog Protocol Type       | UDP [0]           |
| SysLog Message Encryp...   | not encrypted [0] |
| Message Severities         | 0x1F              |

☒ emerg
☒ alert
☒ crit
☒ err
☒ warning
☐ notice
☐ info
☐ debug

Settings Dialog

### Certificate Handling for encrypted SysLog

If the user wants to secure remote logging on syslog servers, the user can activate encrypting the protocol with TLS.

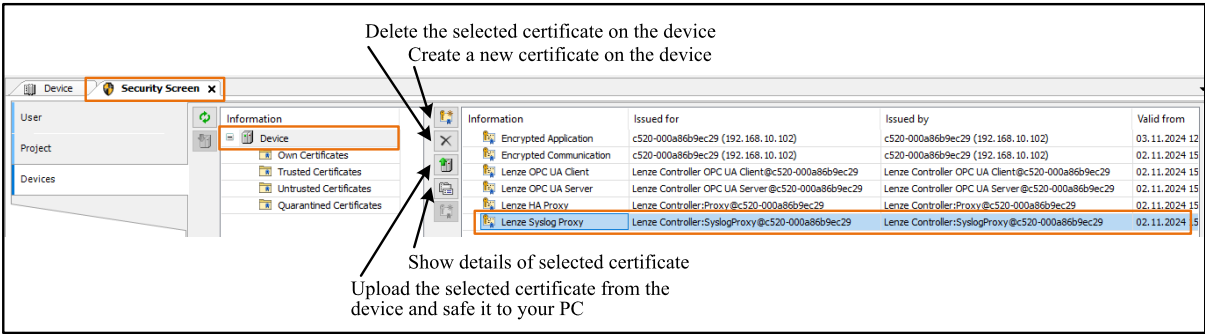


The encrypted SysLog protocol is only specified for the TCP connection and not for UCP connections. Therefore, if the user has activated the UDP SysLog Protocol Type (0x5914:004), and the user switches from unencrypted to TLS encrypted (0x5914:005), the Protocol Type will automatically switch to TCP.

When setting the encrypted SysLog protocol with parameter 0x5914:005, a certificate is needed for the encryption. The user can handle this certificate via the Security Screen of the PLC Designer via the menu View / Security Screen. When choosing the Device tab and the Device itself, the actual certificates are shown after `Refresh the list of available devices and their certificate stores`.

# Controller 1.x

## Security functions



Certificate for SysLog

The user can use the auto-generated certificate for 'Lenze Syslog Proxy', or delete this and create a new one. The user can also upload this certificate to the user computer or show the details.

Details of this automatically generated certificate can be found in this documentation, ([Controller.CertificateStore.SysLogProxy:Certificate](#))

- i** A certificate is mandatory for a secure SysLog connection. If the user manually deletes the SysLog Proxy Certificate during operation, the SysLog Client of the controller will send information about missing certificates to the SysLog Server. Therefore the Client will use the 'deleted' certificate until rebooting.
- i** A certificate is mandatory for a secure SysLog connection. If the user manually generate a new SysLog Proxy Certificate during operation, the SysLog Client will terminate the TLS connection based on the old certificate and will start a new TLS connection based on the new certificate.
- i** If the SysLog connection is used in an encrypted manner and the certificate expires during operation, communication continues based on the then invalid certificate. If the controller is restarted, a new valid certificate is automatically generated and the SysLog connection is opened based on the new valid certificate.

Behavior when SysLog Proxy Certificate is deleted after different reset levels

| Reset Level                                   | Behavior                                                     |
|-----------------------------------------------|--------------------------------------------------------------|
| Manually stop and start the application       | The SysLog Proxy Certificate is still deleted.               |
| Reset Warm                                    | The SysLog Proxy Certificate is still deleted.               |
| Reset Cold                                    | The SysLog Proxy Certificate is still deleted.               |
| Reset Origin and create the application again | The SysLog Proxy Certificate is still deleted.               |
| Boot the Controller                           | The SysLog Proxy Certificate is automatically generated new. |

## File Monitoring

In addition to the SysLog, a file monitoring was initialized to log information about configuration changes.



This file monitoring is only available at runtime, i.e. changes to the file system when the system is turned off are not logged. The SD card must therefore be protected against unauthorized removal and modification.



The focus of this file monitoring is on static files that change frequently during commissioning, but should not or rarely change during machine runtime ([Controller.SysLog:MonitoredFilesAndDirectories](#)). The focus is not on files that are subject to permanent change, e.g. an application logbook.

The type of monitoring and the response in the log lines can be seen in the following two tables.

### Monitoring of Files

| File Monitoring                          | Example Log Line<br>(Log lines may vary depending on the tool used) |
|------------------------------------------|---------------------------------------------------------------------|
| Create file if it does not exists        | /<path>/<file>: CREATE<br>/<path>/<file>: CLOSE_WRITE               |
| Delete existing file                     | /<path>/<file>: DELETE                                              |
| Change and safe content of existing file | /<path>/<file>: CLOSE_WRITE                                         |
| Change rights of existing file           | /<path>/<file>: ATTRIB                                              |

### Monitoring of Directories

| Directory Monitoring                         | Example Log Line<br>(Log lines may vary depending on the tool used) |
|----------------------------------------------|---------------------------------------------------------------------|
| Rename existing file in directory            | /<path>/<oldfile>: MOVED_FROM                                       |
| Change content of existing file in directory | /<path>/<file>: CLOSE_WRITE                                         |
| Change rights of existing file in directory  | /<path>/<file>: ATTRIB                                              |
| Delete existing file in directory            | /<path>/<file>: DELETE                                              |



This file and directory monitoring procedure cannot process files or directories with the special character “;” (semicolon). The Lenze Tools do not create files or directories with this character. This means that the user may not use customized files or directories with this special character.

If a file or directory with this special character exists and this file or directory is being monitored, the application will not start for security reasons.

# Controller 1.x

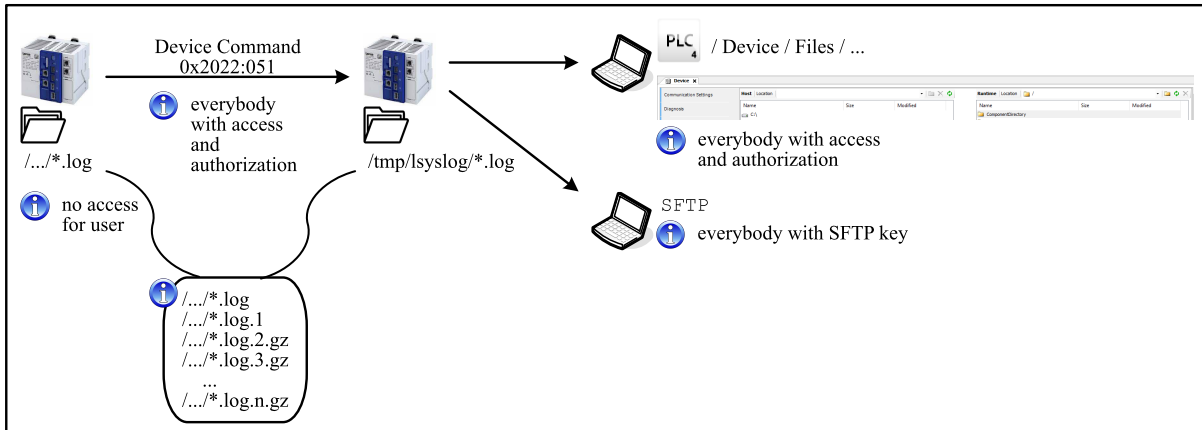
## Security functions

### Application Logging via FB AddSysLog

Please refer to chapter [SysLog](#) to get more information about this function block.

#### Get logfiles from controller

To a limited extent, the controller records the SysLog data and can make it available via a defined path, as shown in the following image.



#### Get local Logfiles

- All Logfiles are stored on the controller in a protected inaccessible area.
- Users with access to the controller's parameter set can execute the device command to copy log files to the /tmp/lsyslog directory.
- Users with a PLC Designer and access to the controller can retrieve these files via the Files tab.
- If the user has an SFTP client and an SFTP key, they can access the files via SFTP.

The structure of the log files is shown in the figure before.

- The first logfile is written without compression.
- After reaching a file size, a new log file will be generated with .1-extension.
- After reaching the file size again, a new log file will be generated and compressed with a .2.gz-extension.
- After reaching the maximum number of log files, the oldest file will be dropped.

Log files with their focus and an example of content

| Log file | Example of content                                                                                                                       |
|----------|------------------------------------------------------------------------------------------------------------------------------------------|
| kern     | e.g. `mmc0: card 5048 removed` -> SD card was removed                                                                                    |
| user     | e.g. ` <user message="">` -&gt; User messages, generated by the FB</user>                                                                |
| daemon   | e.g. `check-and-mount@mmcbk0p1.service: Succeeded<br>finished check and mount device mmcbk0p1` -> a new SD card was detected.            |
| auth     | e.g. `session opened for local user customer from [192.168.10.201]<br>realpath"/sdcard" ` -> SFTP Session opened and path set to /sdcard |
| authpriv | e.g. `child connection from 192.168.10.201:63287` -> SFTP-Child connection from given IP address                                         |
| ntp      | Reserved for ntp-logging                                                                                                                 |



| Log file | Example of content                                                                                              |
|----------|-----------------------------------------------------------------------------------------------------------------|
| local0   | e.g. `Sessioninfo: client: 'PLC Designer 4.0.0', host: '<hostname>'` -> PLC Designer logged into the Controller |
| local1   | Reserved for EtherCAT-Master-Debugging (only for Lenze developer)                                               |
| local2   | e.g. `ViwiWin7.Server.Manager: WebGateway Server   WebGateway:WebGateway Server started`                        |

## Persistence of log files

This chapter describes some use cases related to the persistence of log files.

Persistence of SysLog log files

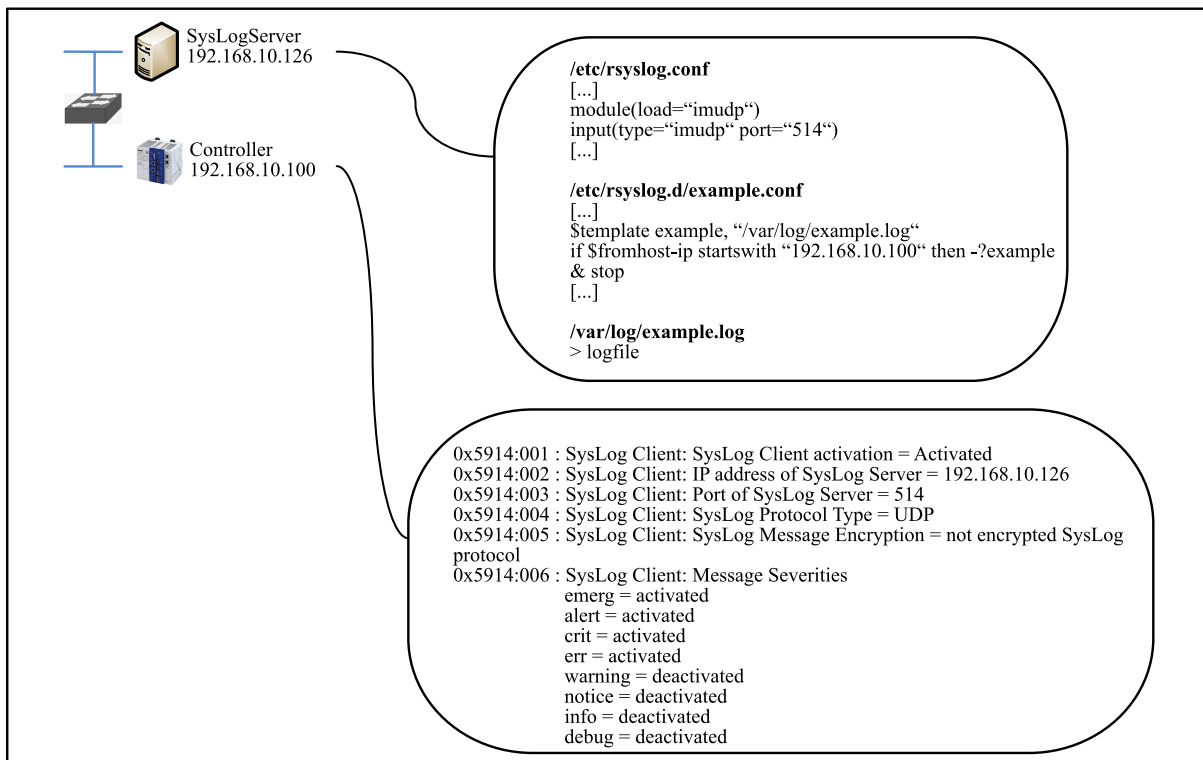
| Use Case                                                                                                                                                                                                    | Persistence of log files                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Using the Firmware Loader for updating or downgrading the firmware of the Controller.                                                                                                                       | The log files are retained and continue to be written.                                                                                                                                                                                       |
| Using the Firmware Loader for copying the firmware file on the USB stick in the <USB-Stick>\firmware\active directory. Then plug the USB stick in the Controller (X61 or X62) and switch on the Controller. | The log files are retained and continue to be written.                                                                                                                                                                                       |
| Manually copy the firmware file on the SD card and rename the file in update.fw (only for Lenze).                                                                                                           | The log files are retained and continue to be written.                                                                                                                                                                                       |
| Using the Backup & Restore Mechanisms via USB Stick for Device Exchange (using the same Controller again).                                                                                                  | The log files are retained and continue to be written. These log files are not included in the restore mechanisms.                                                                                                                           |
| Using the Backup & Restore Mechanisms via USB Stick for Serial Commissioning (change the Controller).                                                                                                       | The log files are retained and continue to be written in both Controllers (the first Controller with the backup procedure and the second Controller with the restore procedure). These log files are not included in the restore mechanisms. |
| Perform the software reset by pressing the reset button when switching on the Controller for 15 seconds.                                                                                                    | The log files are deleted and recreated when new entries are made.                                                                                                                                                                           |
| Using the `--factory-install` command via SSH (only for Lenze)                                                                                                                                              | The log files are deleted and recreated when new entries are made.                                                                                                                                                                           |

## Get logfiles from SysLog Server

There are a lot of different ways to setup a SysLog Server. In this example, a SysLog Server based on an Ubuntu Linux system with the functionality of the rsyslog service is described and shown in the following figure.

# Controller 1.x

## Security functions



Get Lofile from SysLog Server

Set up the controller:

- In this example, the controller has the IP address of 192.168.10.100.
- Set the parameter 0x5914:001 to `activated` to activate the SysLog Client of the Controller.
- Set the parameter 0x5914:002 to the IP address of the SysLog Server.
- Set the parameter 0x5914:003 to the Port of the SysLog Server.
- Set the parameter 0x5914:004 to the Protocol Type UDP.
- Set the parameter 0x5914:005 to not encrypted.
- Set the flags of parameter 0x5914:006 of the wanted severities.

Setup the SysLog Server:

- Use the Ubuntu Linux Distribution and install the `rsyslog` service.
- Configuration `/etc/rsyslog.conf` and activate the syslog reception via udp/514 with the following lines:  
module(load="imudp")  
input(type="imudp" port="514")
- Generate a template file `/etc/rsyslog.d/example.conf`:  
\$template example, "/var/log/example.log"  
if \$fromhost-ip startswith "192.168.10.100" then -?example  
& stop
- Restart the Service:systemctl restart rsyslog
- When using the Controller in this settings, the SysLog Messages will be found in the SysLog Server in the /var/log/example.log.



To ensure that the time stamps in the logbooks on the controller and the higher-level SysLog server match and that the logs in the SysLog server also match those of other devices in the system, it is recommended that the SysLog server, the

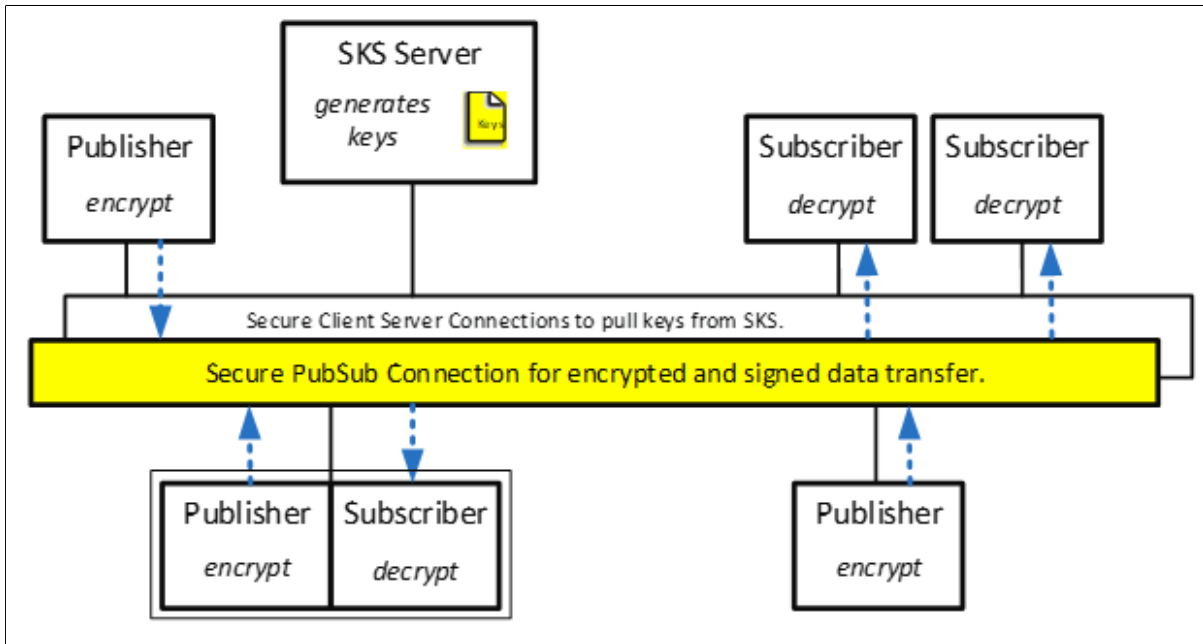


controller and all other devices that use this service be connected to a central time source via NTP and synchronized.

## Controller.SecurityKeyService (SKS)

This functionality is available since Controller firmware version 1.13.0.

An overview of the SKS can be found in the following figure.



Overview

In most systems, the SKS part of the Global Discovery Server (GDS).

The access and usage of the SKS is secured by a user management with user name and password. The SKS allows you to configure different devices and tools that belong to various security groups.

Security groups define which devices and tools are allowed to exchange data with each other. In a security group, publishers send data, and subscribers receive it. Other devices and tools cannot exchange data. First, the PLC must be assigned to a security group in order to exchange data. This is done by the PLC Designer.

The user must be an admin or has to be added to the groups "PubSub" and "SKSConfiguration". The user management must be activated to use of PubSub with SKS.

To add a user to the user management, please have a look at the chapter "UserManagement".

### WriteRolePermission

The WriteRolePermission defines whether a device or tool is allowed to be part of the security group.

When the security group and the permissions are parameterized to the security key service, the SKS writes back a security ID.

# Controller 1.x

Security functions

---

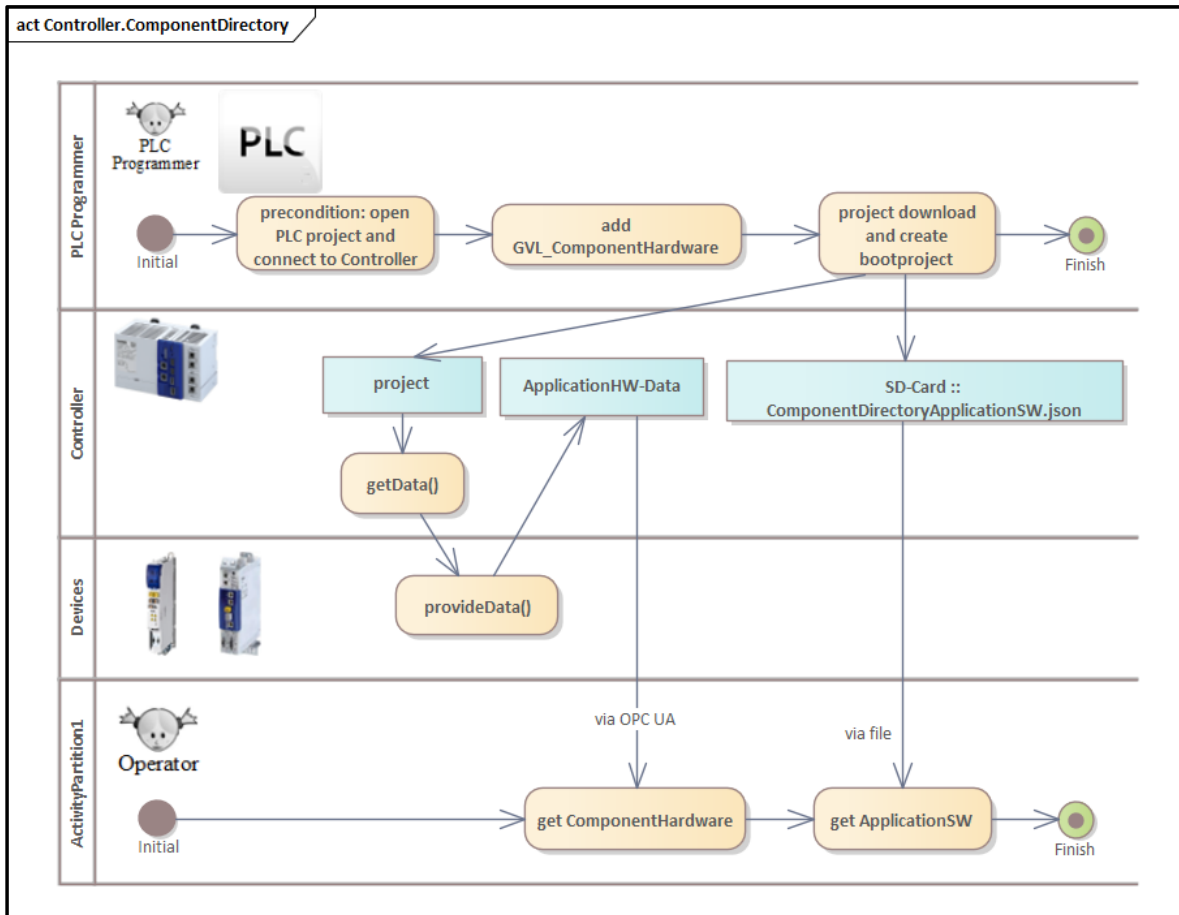
## Configuration

Then, the configuration the security ID to the PLC. This security ID defines the security group and the permission the PLC will have for the PubSub communication.

## Controller.ComponentDirectory

This functionality has been available since controller firmware version 01.11.00.

An overview of the Component Directory can be found in the following figure:



Activity Diagram

The following steps are relevant here:

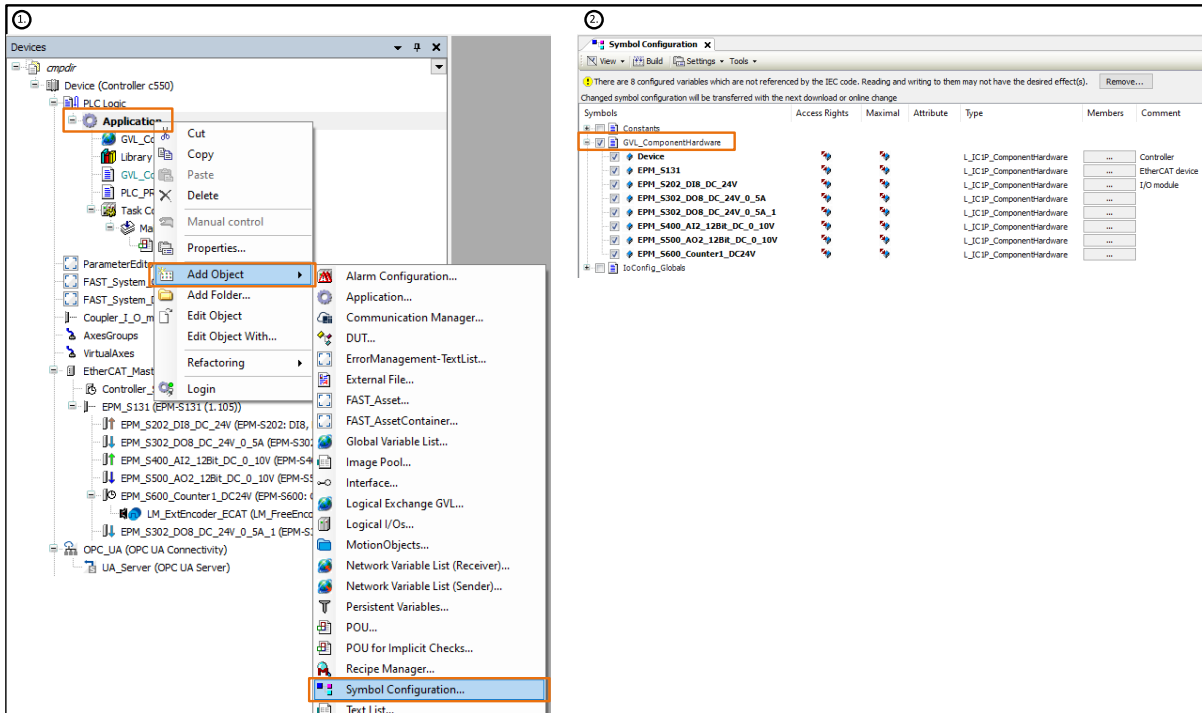
- Add GVL\_ComponentHardware
- Get ComponentHardware
- Get ApplicationSW

# Controller 1.x

## Security functions

### Add GVL\_ComponentHardware

The hardware components are not mapped in OPC UA by default. The reason for this is to minimize the data to be transferred. If the programmer wants to make the data available, two steps must be carried out. First, the "Symbol Configuration" object must be created below the application. Second, the global variables of "GVL\_ComponentHardware" must be activated within the "Symbol Configuration".



Add GVL\_ComponentHardware

These are then available with a project download and subsequent creation of a boot project. It is possible to limit data availability. Please refer to the documentation in the Component Directory.

### Get ComponentHardware

During runtime, the Controller can be accessed with an OPC UA Client and the data from the Component Directory can be viewed in the node set. This is done via the node ID:

- NS4|String| |var|<Device>.<Application>.GVL\_ComponentHardware

**Project**

- Project
  - Servers
    - Lenze Controller OPC UA Server@c550-000a86b9ec22
  - Documents
    - Data Access View

**Address Space**

- No Highlight
- ServerStatus
  - ServiceLevel
  - SetSubscriptionDurable
  - UriVersion
  - VendorServerInfo
  - c500
    - Resources
      - Application
        - DeviceManual
        - DeviceRevision
        - GlobalVars
          - GVL\_ComponentHardware
            - Device
            - EPM\_S131
            - EPM\_S202\_DI8\_DC\_24V
            - EPM\_S302\_DO8\_DC\_24V\_0\_5A
            - EPM\_S302\_DO8\_DC\_24V\_0\_5A\_1
            - EPM\_S400\_AI2\_12Bit\_DC\_0\_10V
            - EPM\_S500\_AO2\_12Bit\_DC\_0\_10V
            - EPM\_S600\_Counter1\_DC24V

**Data Access View**

| # | Server             | Node Id        | Display Name         | Value                            | Datatype | Source Timestamp | Server Timestamp | Statuscode |
|---|--------------------|----------------|----------------------|----------------------------------|----------|------------------|------------------|------------|
| 1 | Lenze Controlle... | NS4[String]... | sDeviceClass         | Controller                       | String   | 13:52:29.190     | 13:52:29.190     | Good       |
| 2 | Lenze Controlle... | NS4[String]... | sHardwareRevision    | 0.0.32.48                        | String   | 13:52:29.190     | 13:52:29.190     | Good       |
| 3 | Lenze Controlle... | NS4[String]... | sManufacturer        | Lenze                            | String   | 13:52:29.190     | 13:52:29.190     | Good       |
| 4 | Lenze Controlle... | NS4[String]... | sProductCode         | c35AE40R00A11000A...             | String   | 13:52:29.190     | 13:52:29.190     | Good       |
| 5 | Lenze Controlle... | NS4[String]... | sSerialNumber        | 1648986211075534000001           | String   | 13:52:29.190     | 13:52:29.190     | Good       |
| 6 | Lenze Controlle... | NS4[String]... | sSoftwareRevision    | 1.11.0.3948 release candidate... | String   | 13:52:29.190     | 13:52:29.190     | Good       |
| 7 | Lenze Controlle... | NS4[String]... | xAutomaticDataUpdate | true                             | Boolean  | 13:52:29.190     | 13:52:29.190     | Good       |
| 8 | Lenze Controlle... | NS4[String]... | xDataAvailable       | true                             | Boolean  | 13:52:29.190     | 13:52:29.190     | Good       |

Get ComponentHardware

# Controller 1.x

## Security functions

---

### Get ApplicationSW

Information about the ApplicationSW is available on the SD Card of the Controller.

- \sdcard\plc\prg\pta1\ComponentDirectory\ComponentDirectoryApplicationSW.json

This file is a .json file and contains all library information in CycloneDX format. For more information, please refer to the documentation in the Component Directory.

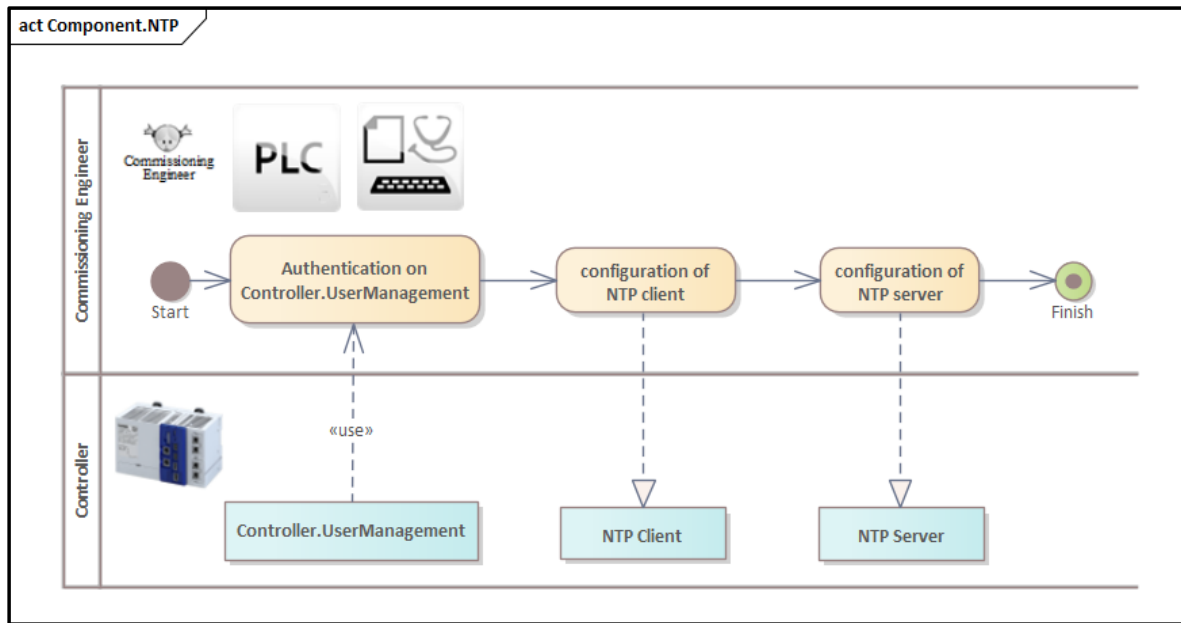
```
{
 "bomFormat": "",
 "specVersion": "1.4",
 "serialNumber": "urn:uuid:1453cc98-0032-4045-8178-cf41b74d397d",
 "version": 1,
 "metadata": {
 "tools": [],
 "component": {
 "type": "application",
 "bomref": "",
 "name": "PLCDesigner",
 "version": "3.28.0.0"
 }
 },
 "components": [
 {
 "type": "library",
 "bomref": "",
 "publisher": "3S - Smart Software Solutions GmbH",
 "name": "3SLicense",
 "version": "3.4.1.0",
 "description": "",
 "scope": "required",
 "hashes": [],
 "licenses": [],
 "purl": "",
 "externalReferences": [],
 "copyright": ""
 },
 {
 [...]
 }
]
}
```

Get ApplicationSW

### Controller.NTP

To synchronize the time of the Controller to a central time server, the NTP Client and / or the NTP Server can be used





Activity Diagram

To set up the time manually, the following parameters can be used:

Parameters for configuring the datetime

| Address    | Name /Setting Range / [Default] | Info                                                        |
|------------|---------------------------------|-------------------------------------------------------------|
| 0x245B:002 | System time: Current time       | This is the datetime for the main system of the Controller. |
| 0x245C:001 | Local time: Current timezone    | This is the configuration of the local timezone.            |
| 0x245C:002 | Local time: Current time        | This is the local time in the timezone.                     |

To change to the NTP client functionality, the following parameters are necessary:

Parameters for configuring the datetime

| Address    | Name /Setting Range / [Default]            | Info                                           |
|------------|--------------------------------------------|------------------------------------------------|
| 0x245B:001 | openSystem time: Time base                 | Please switch from manually set [2] to NTP [0] |
| 0x245A:002 | NTP server addresses: NTP server address 1 | NTP server addresses                           |
| 0x245A:003 | NTP server addresses: NTP server address 2 |                                                |
| 0x245A:004 | NTP server addresses: NTP server address 3 |                                                |
| 0x245A:005 | NTP server addresses: NTP server address 4 |                                                |

After the parameter set is saved, the new configuration is active.



The datetime will be synchronized via the NTP client from the NTP server

\* once after activation of the NTP client and

\* once during the boot process of the controller and

# Controller 1.x

## Security functions



\* cyclically every 60 Minutes during operation.

Since firmware version 1.12, there is also a NTP Server available on the c5x0 Controller. To activate this NTP Server the following parameter can be used:

Parameters for configuring the NTP server

| Address    | Name /Setting Range / [Default]                              | Info |
|------------|--------------------------------------------------------------|------|
| 0x245B:003 | System time:_ NTP server<br>Deactivated [0]<br>Activated [1] |      |

After the parameter set is saved, the NTP Server is active and available under udp/123 port.



If the NTP server is not available after activation, please check the Controller.Firewall settings for this port. NTP server and NTP client are using the same port '123'.

## Controller.WebVisu.Activation

The Controller.WebVisu is only available with the extended controller variants and from the firmware version 1.8.0.11.

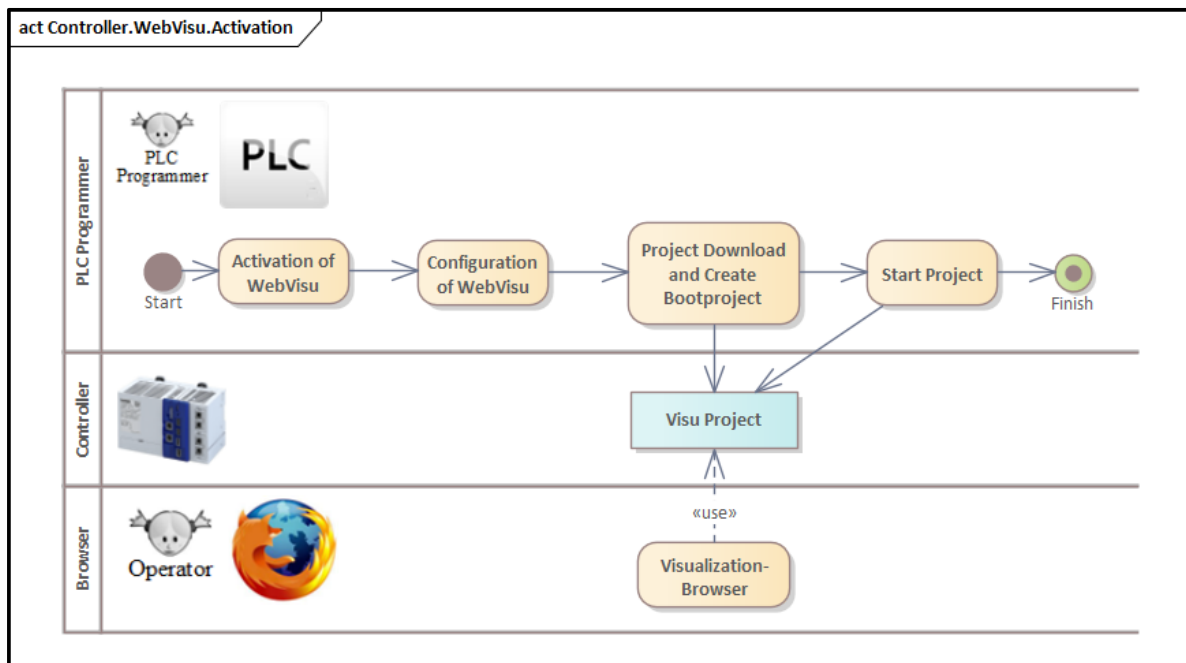


Be sure to use a target device in the PLC Designer with the name of the controller and the added note "Extended for customer specific devices only".

The identification of these products can be done in two ways:

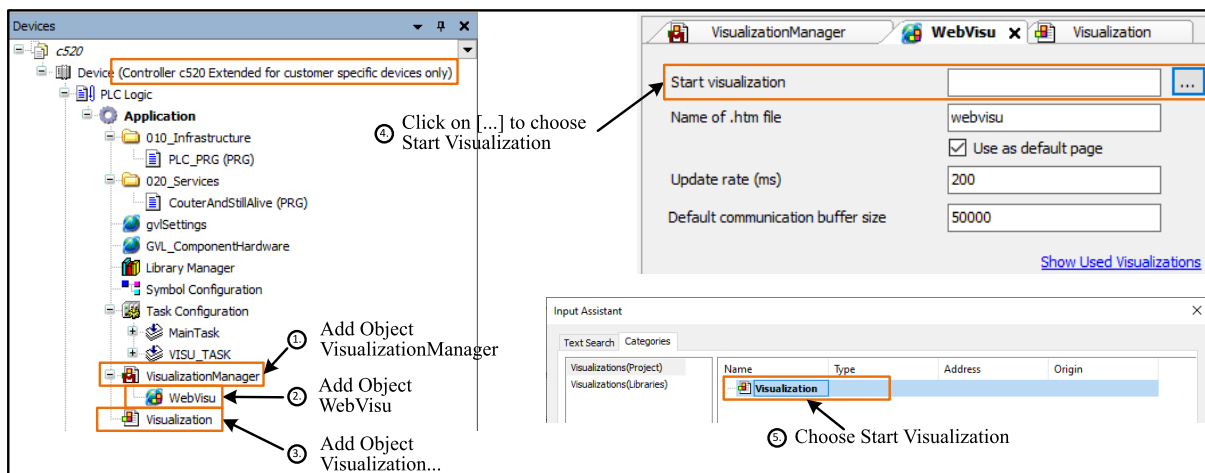
\* The product ID is CxxxxxxxxBxxxxxxx or CxxxxxxxxCxxxxxxx.

\* The parameter 0x2012:008 ends with 0x....C01.) The „1“ in the penultimate position shows the extended controller variante including the WebVisu.



Activity Diagram

To activate WebVisu, please follow these steps:



Activation of the WebVisu in the PLC Designer

1. After adding a controller device with the extension "Extended for customer-specific devices only," add an object called "VisualizationManager" as a child of the application. During this procedure, activate the "VisuSymbols (System)" symbol library.
2. Add an object called "WebVisu" as a child of the "VisualizationManager."
3. Add an object "Visualization..." as a child of the application.
4. Open the tab for WebVisu and start the input assistant for the start visualization by clicking the [...].
5. Choose the Start Visualization.

# Controller 1.x

## Security functions

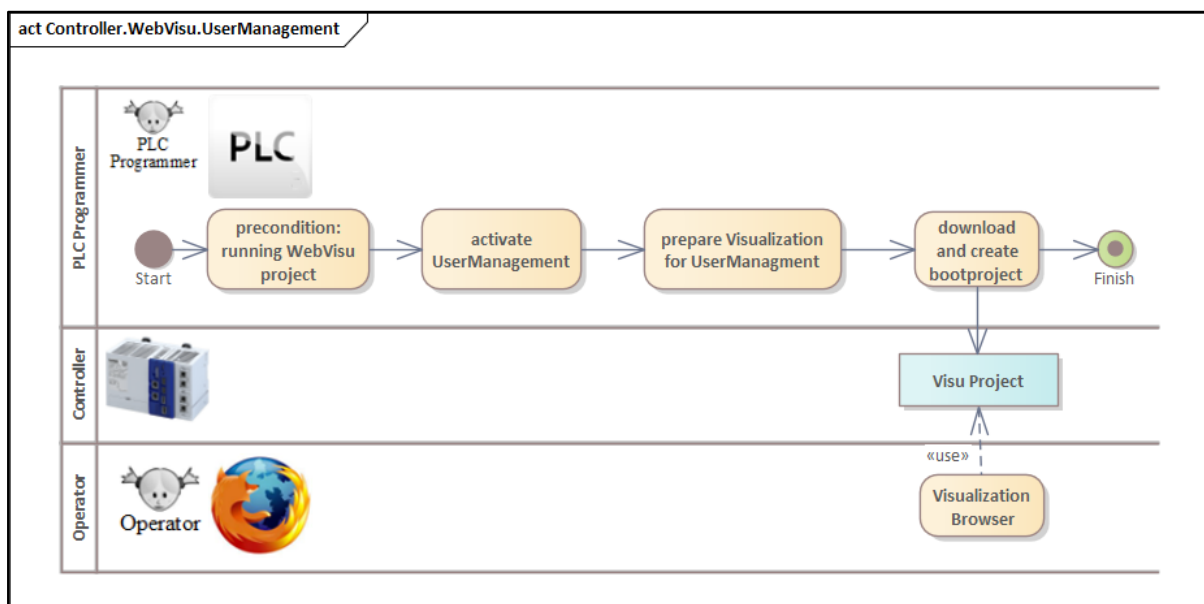
Select Start Visualization. Afterwards, build and download the project to the controller. Finish by creating the boot application.

The visualization can be shown in a browser of a panel when connecting to the IP address, the port 8080 and the name of the htm file (shown in the WebVisu-Tab), e.g.:

<http://192.168.10.102:8080/webvisu.htm>

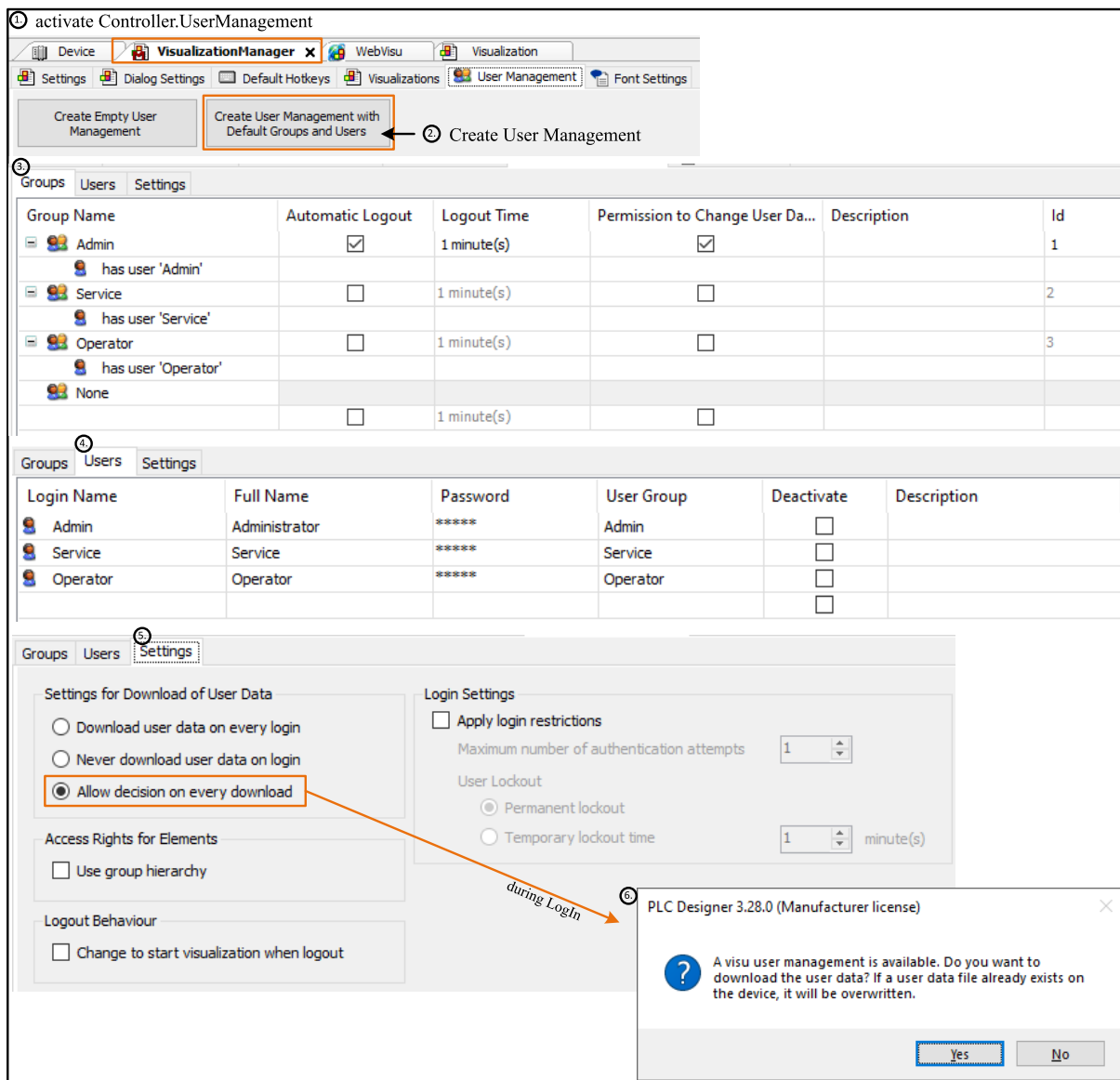
## Controller.WebVisu.UserManagement

It is strongly recommended to activate the User Management for the WebVisu of the extended controller.



Activity Diagram

To activate the User Management for the WebVisu, please follow these steps:



Activate User Management

1. Double-click the "VisualizationManager" component. Select "User Management" tab.
2. Click the "Create User Management with Default Groups and Users" button. User management will now activate.
3. After activation, you can view more information about the groups in the Groups tab.
4. After activation, you can view more information about users in the "Users" tab. It is strongly recommended that you change all Usernames and Passwords from the default settings to personalized ones.
5. After activation, you can view more information about the security settings in the "Settings" tab.
6. Pay special attention to the "Settings for Download of User Data" option. The "Allow decision on every download" setting is recommended. With this setting, a pop-up menu will appear when logging in, which allows the user to make a decision based on the situation.

# Controller 1.x

## Security functions



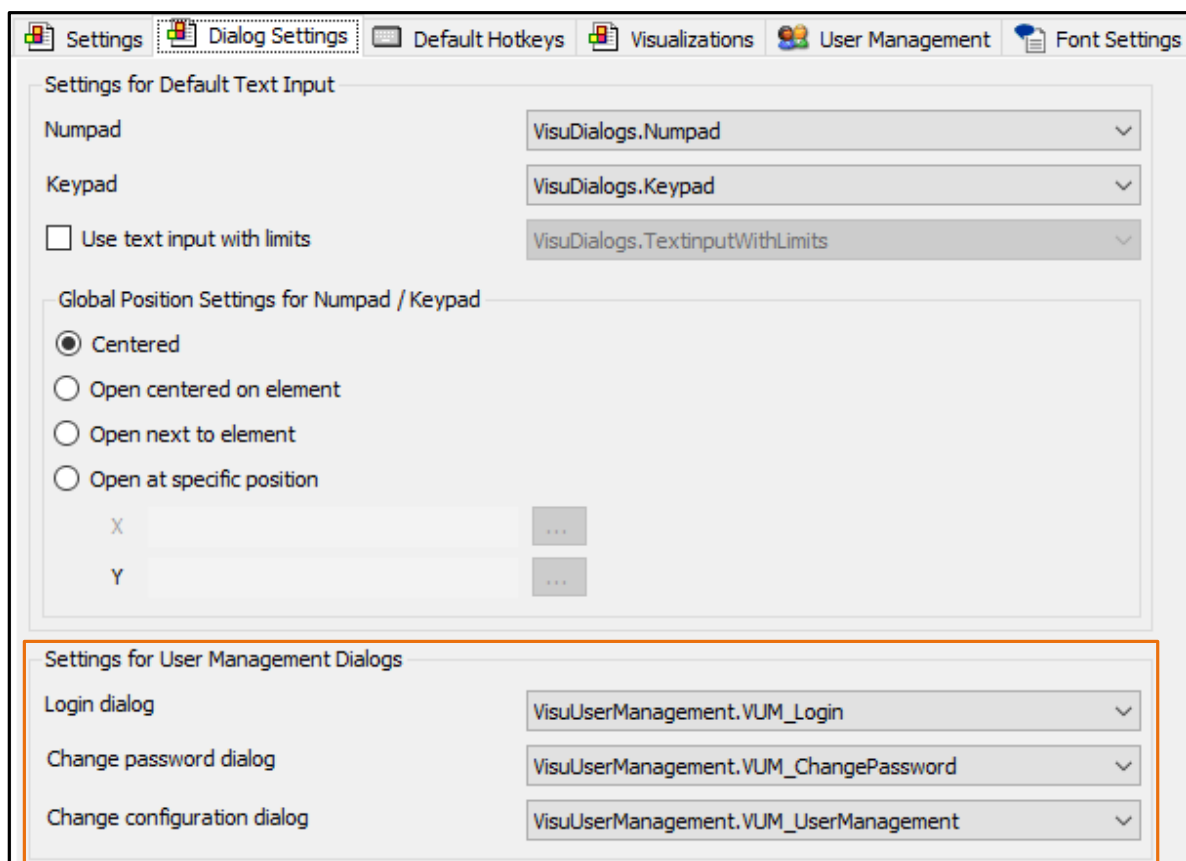
The default settings for the default user are:

User Admin / Password Admin

User Service / Password Service

User Operator / Password Operator

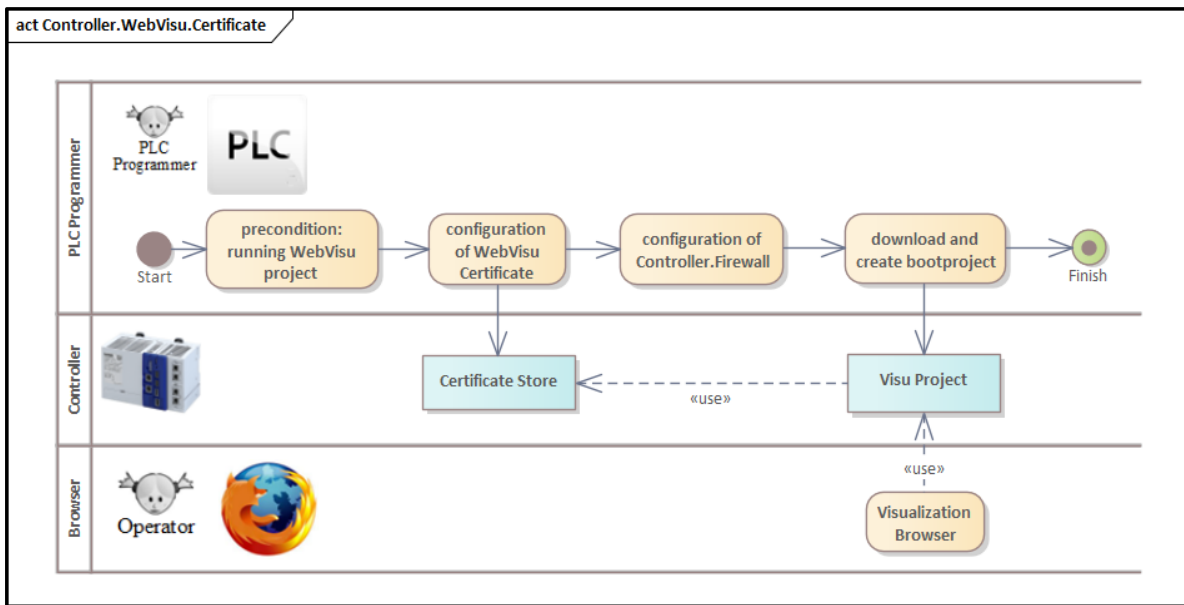
After setting up the User Management, please check the settings of the dialogs and design the wanted layout for the visualization components:



Prepare Visualization for User Management

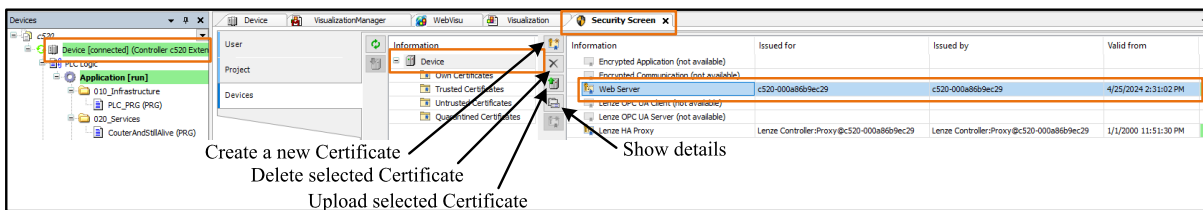
## Controller.WebVisu.Certificate

For using the HTTP security protocol, WebVisu also has the option to communicate via HTTPS.



Activity Diagram

To use this communication, please follow these steps:



Handling the Certificate for the WebServer

1. Open the Security Screen via the security icon on the bottom right corner, or via the PLC Designer Menu / View / Security Screen.
2. Select the Devices tab and click Devices
3. Refresh the Certificate Store.
4. The used certificate is located in the placeholder with the name "Web Server".
5. After selecting this "Web Server" certificate, the user can delete this certificate and generate a new one, The user can upload the public certificate or can show the details of it.
6. When changing the certificate, please stop and start the controller to activate the changes.



It is strongly recommended to activate the Controller.Firewall (refer to chapter /Security Functions/Controller.Firewall). The activation of the Firewall will block the port 8080, so that the browser cannot connect to the port 8080 via http anymore.

Now, the visualization can be shown in a browser of a panel when connecting to the IP address, the port 443 and the name of the htm file (shown in the WebVisu-Tab), e.g.:

<https://192.168.10.102:443/webvisu.htm>

# Controller 1.x

## Security functions



On some browsers, a warning message appears that the https connection is based on a self-signed certificate and therefore cannot be checked in a PKI structure. This warning message must be acknowledged so that the visualization can be displayed.

### Controller.USB-Interface

This functionality has been available since controller firmware version 1.13.0. Using a USB stick is a critical attack vector for hackers and cyberattacks. The USB interface is therefore deactivated by default.

As of V1.13 of the controller firmware, a plugged-in USB stick is not mounted by default so that no malicious code can be executed on the controller in this way.

For brand new controllers, mounting a USB stick is initially active to enable initial commissioning.

This state is indicated by a flashing ready LED every second.

After installing a firmware update, mounting the USB stick is deactivated.

The mounting of the USB stick is also deactivated as soon as a boot project is loaded onto the controller.

If a boot project is already available during the initial startup of a brand new PLC, mounting the USB stick will be deactivated.

The PLC is brand new when the ready LED blinks green and yellow.

The PLC can be parameterized in two different ways.

- Deactivated [0]
- Activated [1]

This is done by the parameter 0x5902.

|        |   |                          |                 |
|--------|---|--------------------------|-----------------|
| 0x5902 | 0 | Security device settings | 1               |
| 0x5902 | 1 | Mount USB stick          | Deactivated [0] |
| 0x5910 | 0 | Firewall                 | 9               |

USB-Interface

Activating the USB interface deactivates the security functionality, leaving the PLC vulnerable to cyberattacks.



The USB interface must be disabled to fulfill the CR 3.2 of the IEC 62443 which is the standard for the Cyber Resilience Act of the EU. Activating the USB interface deactivates the security functionality, leaving the PLC vulnerable to cyberattacks.

### Backup & Restore

Backup and restore functions are the main features of different controllers. Deactivation of the USB interface is still present in firmware 1.13.xx.



When a user activates the PLC command to perform a backup or restore, the PLC will activate the USB interface and execute the command. Afterwards, the USB interface will return to its previous state.

### **Controller.USB-Stick:Security functionality verification**

To verify that the USB deactivation is functioning correctly, you must use a USB stick. Copy a firmware file to the “firmware\active” folder on the USB stick. Then, plug in the USB stick and restart the PLC. After restarting, restart again and check the PLC's firmware version.

If the PLC has the same firmware as before, the deactivation is working correctly. This security feature only works on a PLC with a non-blinking RDY LED.



When a PLC is first started, the RDY LED flashes every second for 100 ms. If it is not flashing, then the PLC is not brand new and has been used by someone else.

### Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

#### Controller.AccountManagementGuidelines

The Account Management Guidelines of the controller are described below. The focus here is on Controller.UserManagement, Controller.WebDiagnosis, Controller.ProcessVisualization and the SSH / SFTP access.

#### Controller.AccountManagementGuidelines :: Controller.UserManagement

##### Default / Factory Settings:

The user management of the controller is deactivated and must be activated via the PLC Designer. If this is done, the following accounts are automatically created by default:

- <name> (user) | "Administrator" (group) | <password> (password)  
<name> and <password> must be assigned upon activation of the user management.
- "Anonymous\_OPCUAServer" (user) | "Anonymous\_OPCUAServer" (group) | "" (password)  
The empty string password is not relevant, as this user is intended exclusively for anonymous use of the OPC UA server, and it is precisely this anonymous use that does not require a password.
- "EngineeringItf" (user) | "Engineering" (group) | Default Password (password)  
For reasons of compatibility with older firmware versions, this default user is provided with a default password.

##### Account Handling:

- It is recommended to remove the "EngineeringItf" (user), which is included due to compatibility with older firmware versions, when reconfiguring or changing its password.
- New users and groups can be defined using the PLC Designer.

##### Policies:

The Runtime Password Policy is deactivated by default. It is recommended to activate it and adapt it to the current password strength requirements. Current default settings after activation are:

- Minimum length = 8
- Number of unique characters = 4
- Requires lowercase letter = activated
- Requires uppercase letter = activated
- Requires digit = activated
- Requires special character = activated
- Must not contain username = activated

## Controller.AccountManagementGuidelines :: Controller.WebDiagnosis

### Default / Factory Settings:

- "guest" (user) | "guest" (group) | "guest" (password)  
After logging in for the first time, a new password must be assigned.
- "advanced" (user) | "advanced" (group) | "default" (password)  
After logging in for the first time, a new password must be assigned.

### Account Handling:

- After logging in for the first time, new passwords for the "guest" and the "advanced" user must be assigned.
- After a successful login, each user can change their own password.

### Policies:

- Minimum length = 4 characters

## Controller.AccountManagementGuidelines :: Controller.ProcessVisualization

### Default / Factory Settings:

The controller is delivered without process visualization. This must be created and installed by the customer using the UI Designer.

### Account Handling:

User management for the process visualization must be activated when creating the process visualisation with the UI Designer. The following settings can be selected.

- It is possible to create four user roles for "Administrators", "Operators", "Service technicians" and "Managers".
- It is possible to activate an auto-logon for test purposes. A message appears stating that the login page will no longer appear. It is only recommended to use this auto-logon for test purposes and not in a productive plant.
- It is possible to create a guest account. If activated, the "guest" (user) is prompted with the "guest" (password), which can be changed immediately by the customer. It is recommended that you change the default password.

### Policies:

The policy can be specified. The following values are stored by default:

- Minimum Password Length = 4
- Maximum password length = deactivated
- Allow password reuse after <> days = deactivated
- Allow password reuse after <> Password changes = deactivated
- Minimum difference = deactivated
- Maximum subsequent equal characters = deactivated
- Minimum difference to prior password <> characters = deactivated
- Password must contain letters = deactivated
- Password must contain digits = deactivated
- Password must contain special characters = deactivated

# Controller 1.x

## Security data

- Password must contain lowercase and uppercase letters = deactivated
- Password must not be equal to user name = deactivated

### Controller.AccountManagementGuidelines :: SFTP

#### Default / Factory Settings:

By default, no customer keys are present in the delivery state.

#### Key Handling:

- The customer can store their own customer key.

#### Policies:

The customer.pkk customer key has the following requirements:

- RSA
- min. 2048 bits

### Controller.Firewall : PortList with deactivate firewall

#### Port List with deactivated firewall

The following table shows the ports, scanned with nmap -sT (TCP connect scan) without activated Controller.Firewall.

Open TCP Ports with deactivated Controller.Firewall

| Port      | Engineering Port X16                        | PROFINET Device*1)                          | Ethernet Switch*2)                          | Protocol                                                             |
|-----------|---------------------------------------------|---------------------------------------------|---------------------------------------------|----------------------------------------------------------------------|
| 22/tcp    | <input checked="" type="checkbox"/> open*3) | <input type="checkbox"/> filtered           | <input checked="" type="checkbox"/> open*3) | <a href="#">Secure Shell (SSH)</a>                                   |
| 80/tcp    | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered           | <input checked="" type="checkbox"/> open    | <a href="#">Hypertext Transfer Protocol (HTTP)</a>                   |
| 443/tcp   | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open    | <a href="#">Secure Hypertext Transfer Protocol (HTTPS)</a>           |
| 1217/tcp  | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered           | <input checked="" type="checkbox"/> open    | <a href="#">PLC-Designer TCP Gateway-Search</a>                      |
| 4840/tcp  | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open    | <a href="#">Lenze OPC-UA Server</a>                                  |
| 6000/tcp  | <input checked="" type="checkbox"/> open*4) | <input type="checkbox"/> filtered           | <input type="checkbox"/> closed             | <a href="#">EtherCAT Master Diagnosis</a>                            |
| 7100/tcp  | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered           | <input checked="" type="checkbox"/> open    | <a href="#">UI-Designer RAW</a>                                      |
| 7200/tcp  | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open    | <a href="#">UI-Designer secure-RAW</a>                               |
| 8080/tcp  | <input checked="" type="checkbox"/> open*5) | <input type="checkbox"/> filtered           | <input checked="" type="checkbox"/> open*5) | Web Visu Server (only available for the extended Controller variant) |
| 11740/tcp | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open    | <a href="#">PLC-Designer Gateway</a>                                 |
| 31855/tcp | <input checked="" type="checkbox"/> open*3) | <input type="checkbox"/> filtered           | <input checked="" type="checkbox"/> open*3) | <a href="#">SFTP (SSH File Transfer Protocol)</a>                    |
| 47877/tcp | <input checked="" type="checkbox"/> open*3) | <input checked="" type="checkbox"/> open*3) | <input checked="" type="checkbox"/> open*3) | <a href="#">SFTP (SSH File Transfer Protocol)</a>                    |

\*1) ProfiNET Device via ProfiNET IO-Device module with X256/X257 for c5x0 controller and via onboard network with X396/X397 for c430 controller.

\*2) Ethernet switch not available for c5x0 Controller and via onboard network with X396/397 for c430 controller.

\*3) For more information please refer chapter [Controller.SSHServer](#): Combination of SSH and SFTP via ports and networks

\*4) Port 6000/tcp is only open if the application contains an EtherCAT-master object.

\*5) Port 8080/tcp is only open if the 'Extended for customer specific devices only' variant of the controller is used and will be filtered if the firewall with default parameter is activated.

# Controller 1.x

## Security data

The following table shows the ports, scanned with nmap -sU (UDP scan) with activated Controller.Firewall and default parameter set.

Open UDP Ports with activated Controller.Firewall

| Port     | Engineering Port X16                                | PROFINET Device*1)                           | Ethernet Switch*2)                                  | Protocol                                       |
|----------|-----------------------------------------------------|----------------------------------------------|-----------------------------------------------------|------------------------------------------------|
| 68/udp   | <input type="checkbox"/> open   filtered            | <input type="checkbox"/> open   filtered     | <input type="checkbox"/> open   filtered            | DHCP Client                                    |
| 123/udp  | <input checked="" type="checkbox"/> open *4)        | <input type="checkbox"/> open   filtered     | <input checked="" type="checkbox"/> open *4)        | <a href="#">NTP Client and Server</a>          |
| 161/udp  | <input type="checkbox"/> closed                     | <input checked="" type="checkbox"/> open     | <input type="checkbox"/> closed                     | SNMP                                           |
| 1740/udp | <input checked="" type="checkbox"/> open   filtered | <input type="checkbox"/> open   filtered     | <input checked="" type="checkbox"/> open   filtered | <a href="#">PLC-Designer UDP Communication</a> |
| 1741/udp | <input type="checkbox"/> closed                     | <input type="checkbox"/> open   filtered     | <input type="checkbox"/> closed                     |                                                |
| 1742/udp | <input type="checkbox"/> closed                     | <input type="checkbox"/> open   filtered     | <input type="checkbox"/> closed                     |                                                |
| 1743/udp | <input type="checkbox"/> closed*3)                  | <input type="checkbox"/> open   filtered*3)  | <input type="checkbox"/> closed*3)                  |                                                |
| 3677/udp | <input type="checkbox"/> open   filtered            | <input type="checkbox"/> open   filtered     | <input type="checkbox"/> open   filtered            | ESDCP                                          |
| 4840/udp | <input checked="" type="checkbox"/> open *5)        | <input checked="" type="checkbox"/> open *5) | <input checked="" type="checkbox"/> open *5)        | <a href="#">Lenze OPC-UA PubSub</a>            |

\*1) ProfiNET Device via ProfiNET IO-Device module with X256/X257 for c5x0 controller and via onboard network with X396/X397 for c430 controller.

\*2) Ethernet switch not available for c5x0 controller and via onboard network with X396/397 for c430 controller.

\*3) Due to the scanning properties of nmap for UDP ports, these UDP ports are displayed as 'open | filtered'. However, UDP communication can only take place via the engineering port and Ethernet switch and not via PPROFINET.

\*4) UDP port available if NTP server is activated with parameter 0x245B:003 = Activated [1].

\*5) UDP port available if OPC-UA is configured with the feature publisher / subscriber.

## Controller.Firewall : PortList with activated firewall and default parameter set

The following table shows the ports, scanned with nmap -sT (TCP connect scan) with activated Controller.Firewall and a default parameter set.

Open TCP Ports with activated Controller.Firewall and default parameter set

| Port     | Engineering Port X16                        | PROFINET Device*1)                | Ethernet Switch*3)                       | Protocol                                                   |
|----------|---------------------------------------------|-----------------------------------|------------------------------------------|------------------------------------------------------------|
| 22/tcp   | <input checked="" type="checkbox"/> open*3) | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered        | <a href="#">Secure Shell (SSH)</a>                         |
| 80/tcp   | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered        | <a href="#">Hypertext Transfer Protocol (HTTP)</a>         |
| 443/tcp  | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered        | <a href="#">Secure Hypertext Transfer Protocol (HTTPS)</a> |
| 1217/tcp | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered        | <a href="#">PLC-Designer TCP Gateway-Search</a>            |
| 4840/tcp | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered | <input checked="" type="checkbox"/> open | <a href="#">Lenze OPC-UA Server</a>                        |
| 6000/tcp | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered        | <a href="#">EtherCAT Master Diagnosis</a>                  |
| 7100/tcp | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered        | <a href="#">UI-Designer RAW</a>                            |
| 7200/tcp | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered        | <a href="#">UI-Designer secure-RAW</a>                     |

| Port      | Engineering Port X16                     | PROFINET Device*1)                | Ethernet Switch*3)                | Protocol                                                             |
|-----------|------------------------------------------|-----------------------------------|-----------------------------------|----------------------------------------------------------------------|
| 8080/tcp  | <input type="checkbox"/> filtered*5)     | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered | Web Visu Server (only available for the extended Controller variant) |
| 9410/tcp  | <input type="checkbox"/> filtered        | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered | <a href="#">PLC-Designer Gateway</a>                                 |
| 11740/tcp | <input checked="" type="checkbox"/> open | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered | <a href="#">SFTP (SSH File Transfer Protocol)</a>                    |
| 31855/tcp | <input type="checkbox"/> filtered        | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered | <a href="#">SFTP (SSH File Transfer Protocol)</a>                    |
| 47877/tcp | <input type="checkbox"/> filtered        | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered | <a href="#">Secure Shell (SSH)</a>                                   |

\*1) ProfiNET Device via ProfiNET IO-Device module with X256/X257 for c5x0 controller and via onboard network with X396/X397 for c430 controller.

\*2) Ethernet switch not available for c5x0 controller and via onboard network with X396/397 for c430 controller.

\*3) For more information please refer to chapter [Controller.SSHServer](#): Combination of SSH and SFTP via Ports and Networks

\*4) Port 6000/tcp is only open if the application contains an EtherCAT-master object.

\*5) Port 8080/tcp is only open if the 'Extended for customer specific devices only' variant of the Controller is used and will be filtered if the firewall with default parameter is activated.

The following table shows the ports, scanned with nmap -sU (UDP scan) with activated Controller.Firewall and default parameter set.

Open UDP ports with activated Controller.Firewall and default parameter set

| Port     | Engineering Port X16                                | PROFINET Device*1)                                     | Ethernet Switch*2)                          | Protocol                                       |
|----------|-----------------------------------------------------|--------------------------------------------------------|---------------------------------------------|------------------------------------------------|
| 68/udp   | <input type="checkbox"/> open   filtered            | <input type="checkbox"/> open   filtered               | <input type="checkbox"/> open   filtered    | DHCP Client                                    |
| 123/udp  | <input type="checkbox"/> open   filtered            | <input type="checkbox"/> open   filtered               | <input type="checkbox"/> open   filtered    | <a href="#">NTP Client and Server</a>          |
| 161/udp  | <input type="checkbox"/> open   filtered            | <input checked="" type="checkbox"/> open               | <input type="checkbox"/> open   filtered    | SNMP                                           |
| 1740/udp | <input checked="" type="checkbox"/> open   filtered | <input checked="" type="checkbox"/> open   filtered    | <input type="checkbox"/> open   filtered    | <a href="#">PLC-Designer UDP Communication</a> |
| 1741/udp | <input type="checkbox"/> closed                     | <input checked="" type="checkbox"/> open   filtered    | <input type="checkbox"/> open   filtered    |                                                |
| 1742/udp | <input type="checkbox"/> closed                     | <input checked="" type="checkbox"/> open   filtered    | <input type="checkbox"/> open   filtered    |                                                |
| 1743/udp | <input type="checkbox"/> closed*3)                  | <input checked="" type="checkbox"/> open   filtered*3) | <input type="checkbox"/> open   filtered*3) |                                                |
| 3677/udp | <input type="checkbox"/> open   filtered            | <input type="checkbox"/> open   filtered               | <input type="checkbox"/> open   filtered    | ESDCP                                          |
| 4840/udp | <input type="checkbox"/> open   filtered            | <input type="checkbox"/> open   filtered               | <input type="checkbox"/> open   filtered    | <a href="#">Lenze OPC-UA PubSub</a>            |

\*1) ProfiNET Device via ProfiNET IO-Device module with X256/X257 for c5x0 Controller and via onboard network with X396/X397 for c430 Controller.

\*2) Ethernet Switch not available for c5x0 Controller and via onboard network with X396/397 for c430 Controller.

\*3) Due to the scanning properties of nmap for UDP ports, these UDP ports are displayed as 'open | filtered'. However, UDP communication can only take place via the engineering port and Ethernet Switch and not via PROFINET.

# Controller 1.x

## Security data

---

### Controller.EncryptedCommunication.PLCDesigner : Certificate

The automatically created certificate for encrypted communication has the following identifiers:

Fields of the certificate for the encrypted communication

| Field                     | Description and Value                                                               |
|---------------------------|-------------------------------------------------------------------------------------|
| Issuer, SERIALNUMBER      | The serial number is the MAC address of the X16 engineering port of the controller. |
| Issuer, Unstructured Name | Device: Controller,<br>e.g. device: c500                                            |
| Issuer, Unstructured Name | Vendor: Lenze                                                                       |
| Issuer, CN                | Combination of controller type and IP Address,<br>e.g. c550 (192.168.10.100)        |
| Valid from<br>Valid to    | The automatically created certificate is valid for 30 days.                         |

### Controller.CertificateStore.HAProxy : Certificate

The automatically created certificate for the HA Proxy has the following identifiers:

Fields of the Certificate for the HA Proxy

| Field                  | Description and Value                                                                                                                                                                                                                                       |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Issuer                 | CN = Lenze controller:Proxy@c550-000a86b9ec22<br>The CN is "Lenze controller:Proxy@" with the controller type and the MAC address of the X16 engineering port of the controller.<br>OU = Controls<br>O = Lenze<br>L = Aerzen<br>S = Niedersachsen<br>C = DE |
| Valid from<br>Valid to | The automatically created certificate is valid for 60 year.                                                                                                                                                                                                 |

### Controller.CertificateStore.SysLogProxy : Certificate

The automatically created certificate for the SysLog Proxy has the following identifiers:

Fields of the Certificate for the SysLog Proxy



| Field                  | Description and Value                                                                                                                                                                                                                                                   |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Issuer                 | CN = Lenze Controller:SysLogProxy@c550-000a86b9ec22<br>The CN is 'Lenze Controller:SysLogProxy@' with the controller type and the MAC address of the X16 engineering port of the controller.<br>OU = Controls<br>O = Lenze<br>L = Aerzen<br>S = Niedersachsen<br>C = DE |
| Valid from<br>Valid to | The automatically created certificate is valid for 60 year.                                                                                                                                                                                                             |

## Controller.SysLog : MonitoredFilesAndDirectories

This chapter lists the files and directories that are monitored in the file monitoring. For more information, refer to chapter [Controller.SysLog](#).

The recursion depth is specified for directories being monitored. The recursion depth of the monitoring is also specified here. A recursion depth of 0 means that only the directory and its files are monitored. A recursion depth of 1 means that the directory and its subdirectories are monitored. A recursion depth of \* means that all subdirectories and their files are monitored.

### Static monitoring of files:

- /sdcard/.enable-ssh
- /sdcard/ip.txt
- /sdcard/ip-old.txt
- /sdcard/update.fw
- /sdcard/public-key/customer.ppk
- /sdcard/Licenses\_do\_not\_delete/LicenseFile.lic
- /sdcard/Licenses\_do\_not\_delete/VerificationFile.lic
- /sdcard/plc/CODESYSControl\_User.cfg
- /sdcard/plc/CODESYSControl\_UserSec.cfg
- /sdcard/plc/SysFileMap.cfg
- /sdcard/plc/prg/pta1/.UserDatabase.csv
- /sdcard/plc/prg/pta1/.GroupDatabase.csv
- /sdcard/plc/prg/pta1/.UserMgmtRightsDB.lcsv
- /sdcard/plc/prg/pta1/.UserMgmtExt.csv
- /sdcard/plc/prg/pta1/.PswDB.csv
- /sdcard/plc/prg/pta1/ecat\_master\_0.xml
- /sdcard/plc/prg/pta1/ecat\_master\_0\_boot.xml
- /sdcard/plc/prg/pta1/ParameterSets/ParSetConfig.cprm
- /sdcard/easyui/data/ProjectRegistration.xml

### Static monitoring of directories:

- /sdcard/firmware/ (recursive 0)
- /sdcard/plc/.pki/ (recursive \*)
- /sdcard/plc/prg/PlcParameterSet/ (recursive 0)
- /sdcard/plc/prg/pta1/Recipes/ (recursive \*)

# Controller 1.x

Security data

---

## Dynamic monitoring of files:

- /sdcard/plc/prg/pta1/<Application>.app
- /sdcard/plc/prg/pta1/<Application>.crc
- /sdcard/<\*>.lpk
- /sdcard/easyui/ServerProjects/<name>/<name>.vw7
- /sdcard/easyui/ServerProjects/<name>/<ctrlName>.0.0.lic
- /sdcard/easyui/ServerProjects/<name>/Data/UserManagerRuntimeConfig.urc
- /sdcard/easyui/ServerProjects/<name>/Data/<name>.rtvw7
- /sdcard/easyui/ClientProjects/<name>/<name>\_Client.vw7
- /sdcard/easyui/ClientProjects/<name>/index.html
- /sdcard/easyui/ClientProjects/<name>/service-worker.js
- /sdcard/easyui/ClientProjects/<name>/manifest.json
- /sdcard/easyui/ClientProjects/<name>/tsconfig.json
- /sdcard/easyui/ClientProjects/<name>/web.Release.config
- /sdcard/easyui/ClientProjects/<name>/web.Debug.config
- /sdcard/easyui/ClientProjects/<name>/web.config

## Dynamic monitoring of directories:

- /sdcard/easyui/ClientProjects/<name>/usercontrols/ (recursiv \*)
- /sdcard/easyui/ClientProjects/<name>/actions/ (recursiv \*)
- /sdcard/easyui/ClientProjects/<name>/views/ (recursiv \*)
- /sdcard/easyui/ClientProjects/<name>/pages/ (recursiv \*)
- /sdcard/easyui/ClientProjects/<name>/libs/ (recursiv \*)
- /sdcard/easyui/ClientProjects/<name>/services/ (recursiv \*)
- /sdcard/easyui/ClientProjects/<name>/resources/ (recursiv \*)
- /sdcard/easyui/ClientProjects/<name>/properties/ (recursiv \*)
- /sdcard/easyui/ClientProjects/<name>/images/ (recursiv \*)
- /sdcard/easyui/ClientProjects/<name>/dialogs/ (recursiv \*)
- /sdcard/easyui/ClientProjects/<name>/converters/ (recursiv \*)
- /sdcard/easyui/ClientProjects/<name>/appsettings/ (recursiv \*)

# FAST

FAST refers to the libraries that are required for the PLC Designer programming tool.

## Product description

## Product identification

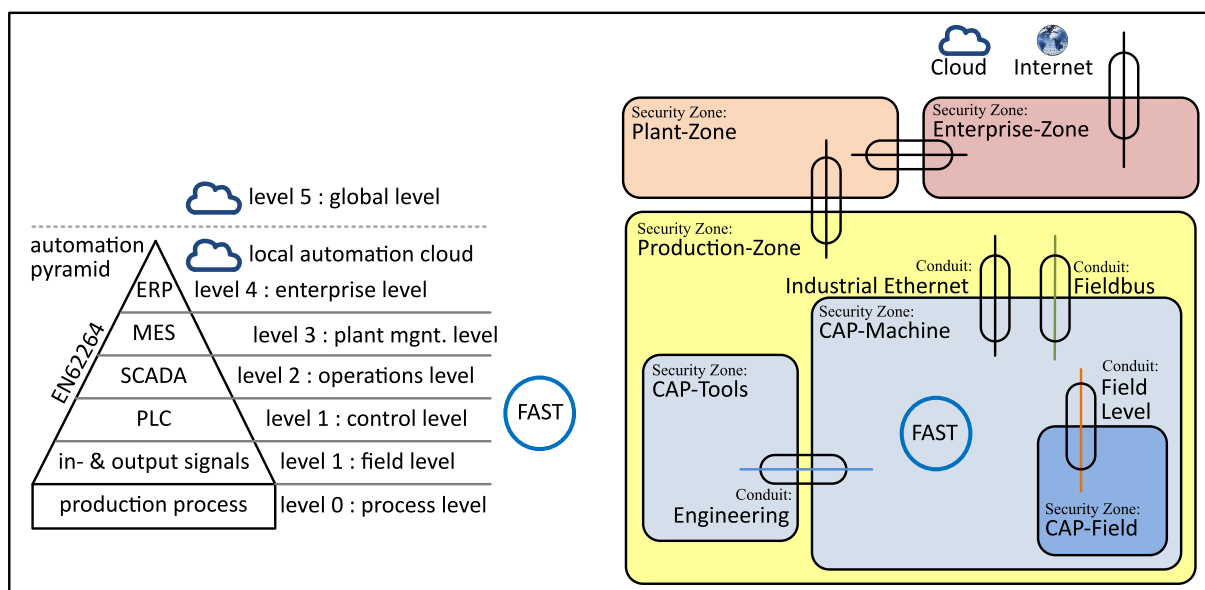
This documentation applies to the following software functionalities with their identification:

Name of software functionalities and ID

| Name of software-functionalities | ID   |
|----------------------------------|------|
| FAST                             | n.a. |

### Location in the network

These software functionalities are located in the automation pyramid at the control level. Furthermore, they are located in the security zone "CAP-Machine" ([Zones and Conduits](#)).



Product location in the network

This software functionality runs on the [Controller](#) and therefore has no hardware interfaces of its own.

### Intended purpose

The intended user of this component is described in the application as directed and can be found in the operating instructions in the online help. In the following, some specifics regarding cyber security are discussed.

- This component mentioned here is professional software and may only be commissioned and decommissioned by specialists.
- This software also requires maintenance throughout its life cycle, which must be carried out by the operator.
- Modifications to the software are not permitted.

# FAST

## Product description

- 
- If this software is taken out of operation or disposed of, the instructions in the documentation must be observed.

### Intended environment

The intended environment for this software is described in the application as directed and can be found in the online help. In the following, some specifics regarding cyber security are discussed:

- The software libraries may only be used with the PLC Designer and only on Lenze devices.
- The configuration of the functionalities, their parameterization and the additional programming of the application is the responsibility of the user.

### Security key indicators

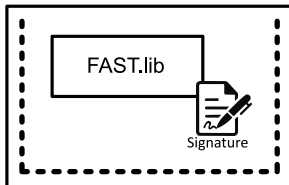
Security key indicator (in accordance with IEC 62443-4-2):

- These components are considered a software application (SAR).
- These components have a security level of SL-C 0.
- These components have an SL-vector from SL-C(FAST)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

## Security mechanisms

### Product Defense in Depth

The following image shows the Defense in Depth product concept. For the sake of clarity, some details have been deliberately omitted.

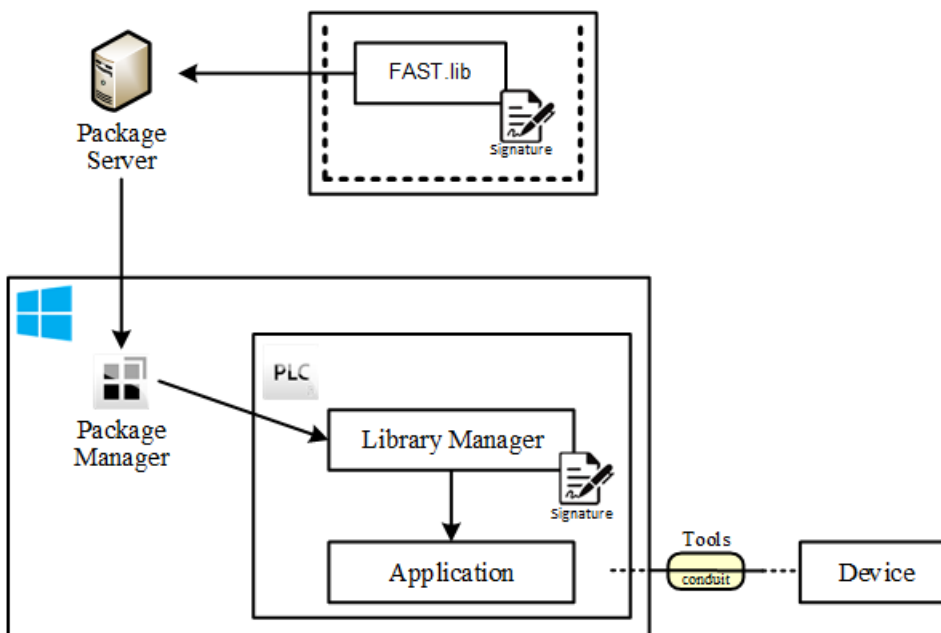


Product Defense in Depth

This FAST Libraries are signed with an Lenze Certificate.

### Expected Defence in Depth in the environment

The following image shows the Expected Defense in Depth in the environment of the FAST libraries.



Expected Defence in Depth in the environment

- The FAST libraries are signed and are made available to the Package Manager via the Package Server mechanism. The protection mechanisms described in the Package Manager apply here.
- The PLC Designer can use the FAST Libraries in the Library Manager and check the signature.
- The user can use the libraries contained in the Library Manager to create his application.
- The created application can be protected with the mechanisms described in the controller chapter (encryption, signing, ...) and written to the device.

# FAST

## Commissioning and hardening instructions

---

### Security mechanisms

The following security functions are included in the listed components:

- FAST.Library.Signature

## Commissioning and hardening instructions

The following commissioning instructions must be followed.

### General instructions

- n.a.

### Commissioning and hardening instructions

- Before adding libraries to the library manager, validate the signature of the library ([FAST.Library.Signature](#)).
- When using the SysLog functionality of the controller, the programmer can use the SysLog function block (refer to chapter \Security Functions\FAST.SysLog).

### Periodic security maintenance

- n.a.

### Decommissioning instructions

- n.a.

### Removal product from environment

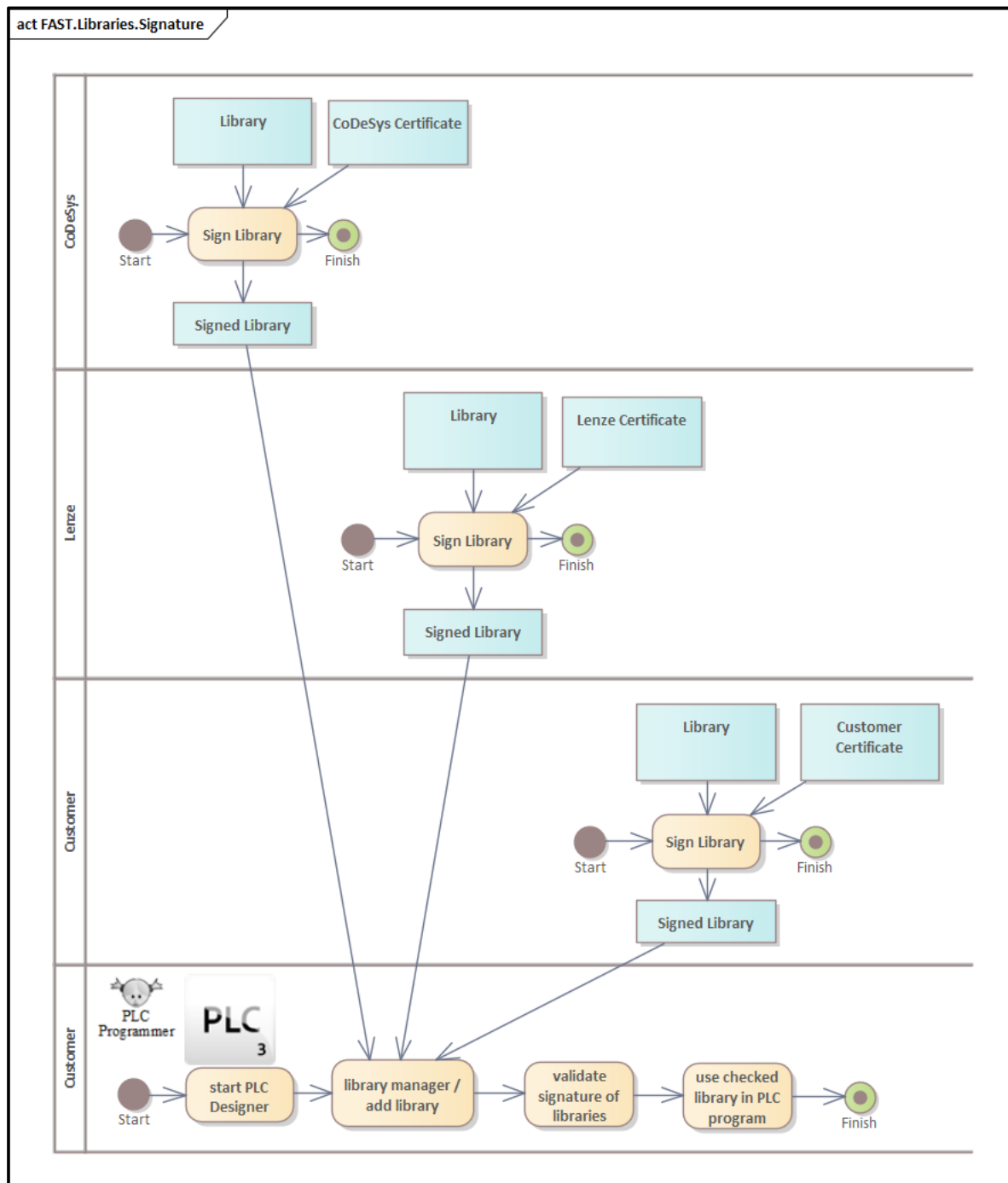
- n.a.

## Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

### **FAST.Library.Signature**

To make sure that the used libraries also come from the specified sender, they should be signed. Source code protection can be achieved via the compiled library mechanism. In this context, the signature increases security because the integrity and authenticity of the library can also be checked.



Activity Diagram

Four use cases are presented below

- Signed Libraries from CODESYS
- Signed Libraries from LENZE
- Signed Libraries from the User
- Validate signed Libraries



### Signed Libraries from CODESYS

Some libraries of CODESYS are already signed. No action by the user is required.

### Signed Libraries from LENZE

Some libraries of Lenze are already signed. No action by the user is required.

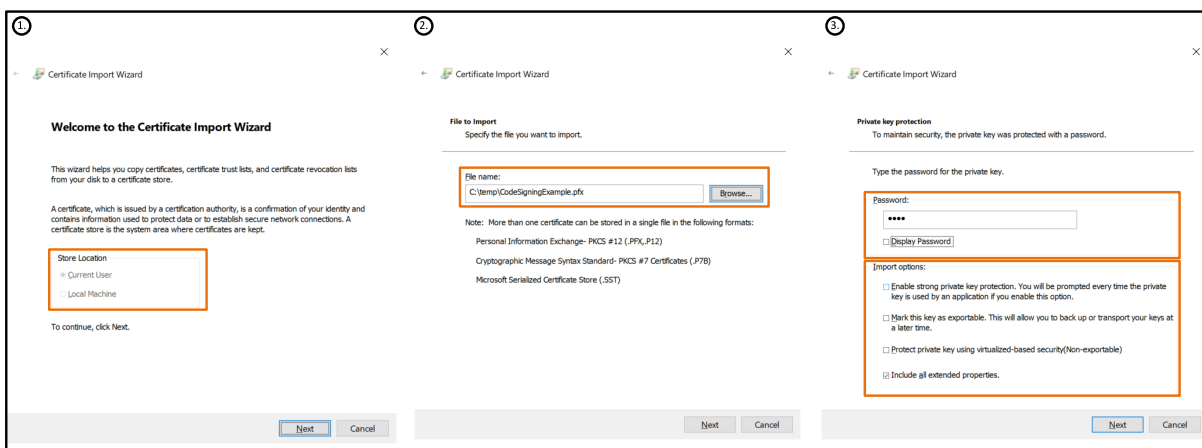
### Signed Libraries from the User

This section describes how a customer can sign their own libraries with their own certificate.

Requirements for signing a library and requirements for the needed certificate:

- »PLC Designer« with version > V3.22
- X509.Certificate for Code Signing (keyUsage = digitalSignatur) in \*.pfx file.
- Extended-Validation-Certificate (EV-Certificate)
- Recommendation of an additional timestamping certificate to guarantee a forgery-proof time at the time of signing. Access to RFC-3161 Timestamping-Server

In the first step, the own code-signing certificate must be integrated into the Windows Certificate Store. This can be accessed using the Windows command "certmgr".



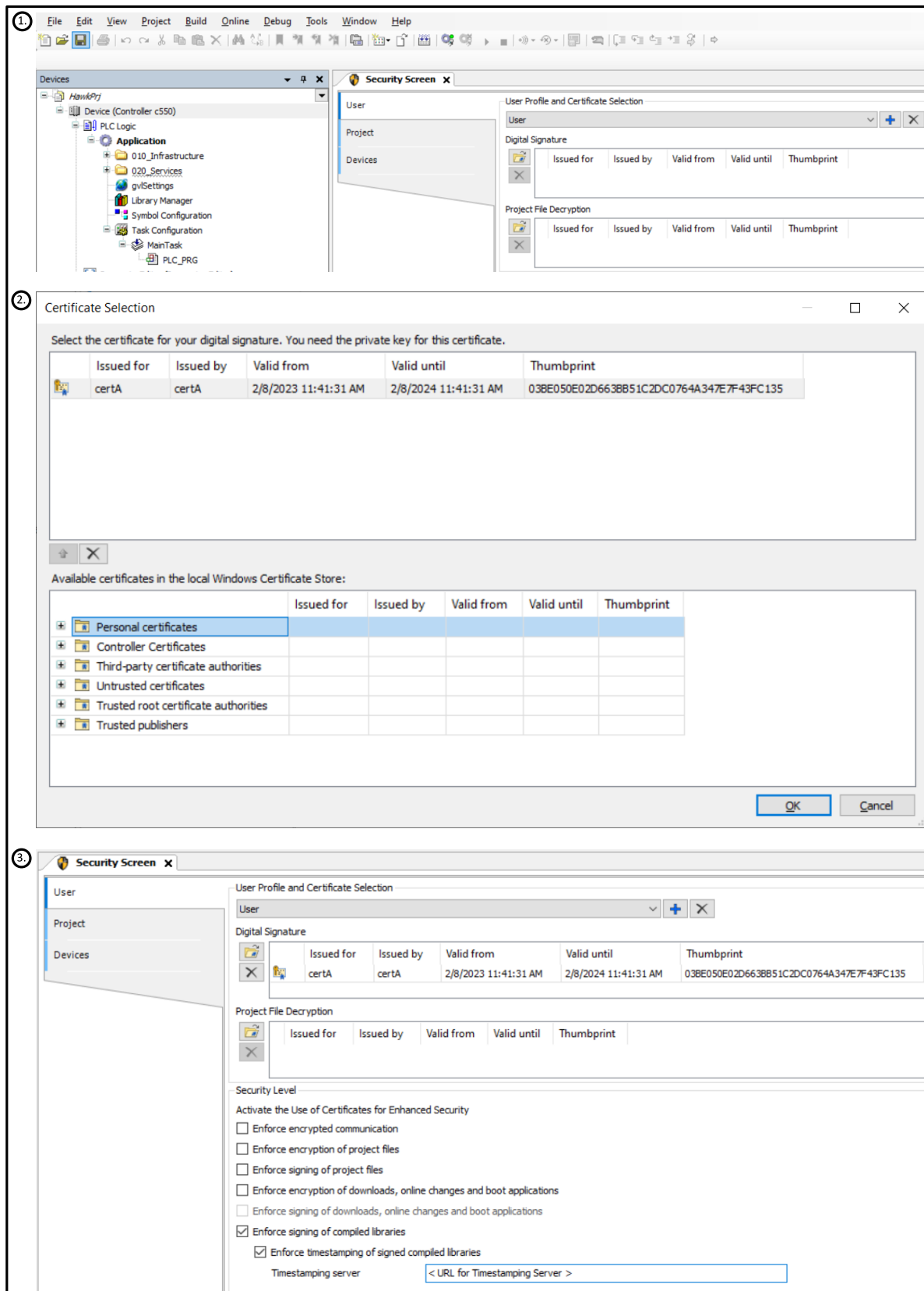
Import Certificate

# FAST

## Security functions

---

Now, the PLC Designer must be started, and a new project must be generated with the category "Libraries" and the template "Empty Library." Open the Security Screen with the menu option "View" > "Security Screen." After selecting the "User" tab, the certificate for the digital signature can be selected.



Signing Libraries

# FAST

## Security functions

---

The last activity is to save the library as a compiled library with the command "Save Project and Install into Library Repository". The library will be saved as a "COMPILED-LIBRARY-V3" format.



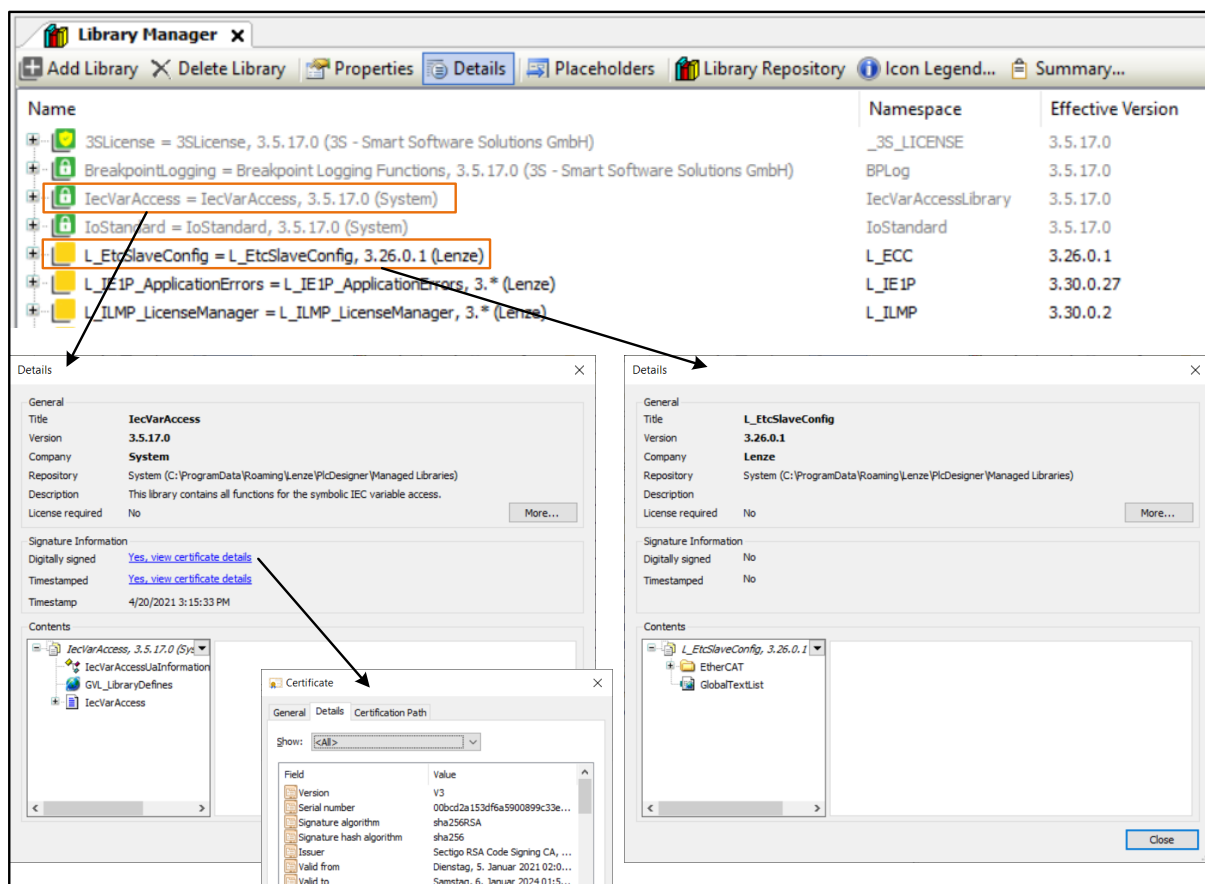
Once the library is signed, the public keys of the signing and timestamping certificates are integrated into it.

## Validate signed Libraries

When integrating libraries, the Library Manager must be called in the »PLC Designer«. The existing libraries are displayed with a respective icon:

- Yellow sign on a green background  
Library is signed with a trusted certificate, but the library uses at least one dependent unsigned library
- White lock on a green background  
Library is signed with a trusted certificate
- Yellow Box  
Library is not signed

When selecting the library, the Details button shows information, including the signing certificates.



Verify Signature

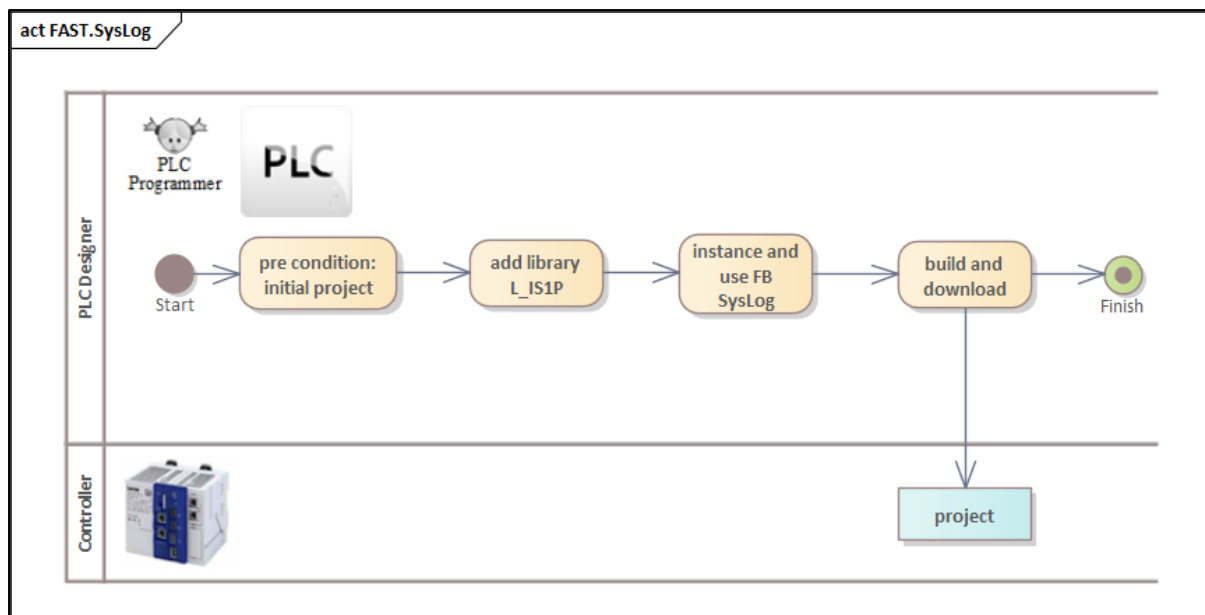
## FAST.SysLog

This functionality has been available since version 3.32.0 of the L\_IS1P\_Security Library for using in combination with a c430, c520 or c550 controller from version 1.13.0.

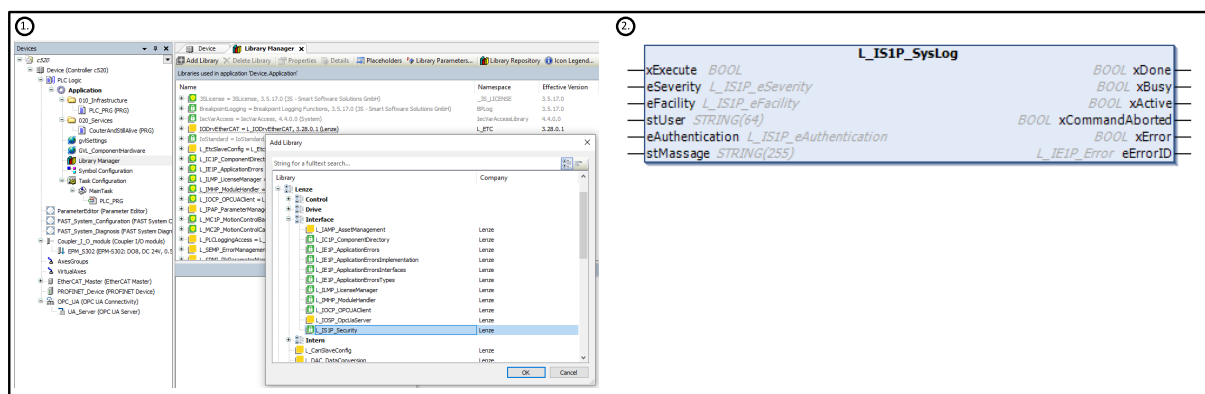
The function block can be found in the library "Lenze/Interface/L\_IS1P\_Security." With this function block, the programmer can add customer messages to the SysLog log files on the controller, or send them to an external SysLog server via the SysLog client. For more information about SysLog handling on the controller

# FAST

## Security functions



Activity Diagram



Integrate SysLog FB

### Inputs of FB

| Name            | Type                                                      |
|-----------------|-----------------------------------------------------------|
| xExecute        | BOOL                                                      |
| eSeverity       | enum L_IS1P_Severity                                      |
| eFacility       | enum L_IS1P_Severity                                      |
| stUser          | STRING(64)                                                |
| eAuthentication | enum L_IS1P_Authentication { none   successful   failed } |
| stMessage       | STRING(255)                                               |

### xExecute

The message will be sent at rising edge.

### eSeverity

The severity can be selected from the following list:

- emergency = 0
- alert = 1
- critical = 2
- error = 3
- warning = 4
- notice = 5
- information = 6
- debug = 7
- none = 8

### eFacility

The facility can be selected from the following list:

- user = 1
- auth = 4

### stUser

The programmer can add the name of the user for the message. This can be used for the human user, but also for the software user to trigger the syslog message.

### eAuthentication

The authentication Information can be selected from the following list:

- none
- successful
- failed

### stMessage

The Programmer can add a 255 character text for the message.

Outputs of FB

| Name            | Type              |
|-----------------|-------------------|
| xDone           | BOOL              |
| xBusy           | BOOL              |
| xActive         | BOOL              |
| xCommandAborted | BOOL              |
| xError          | BOOL              |
| eErrorID        | enum L_IE1P_Error |

These messages become visible in the log files of the controller:

- <timestamp> localhost PLC application[...]: <date> <time>; <User>; <Authentication>; <Message>



The timestamp <date> and <time> indicates when the log was created in the application. The timestamp <timestamp> indicates when the log was written to the SysLog. There is a small queue in between. In most cases, the timestamps will match or differ only minimally.

## Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

### **FAST.AccountManagementGuidelines**

The FAST Libraries have no user management, and for this reason no account management guidelines need to be considered.



## v4x0 Web Panel

The v4x0 Web Panel is a stand alone component, which can be used, to visualized web pages hosted on the Controller (refer to chapter [Controller](#)) or the i950 Servo Inverter (refer to chapter [i9x0 Servo Inverter](#)).

## Product description

### Product identification

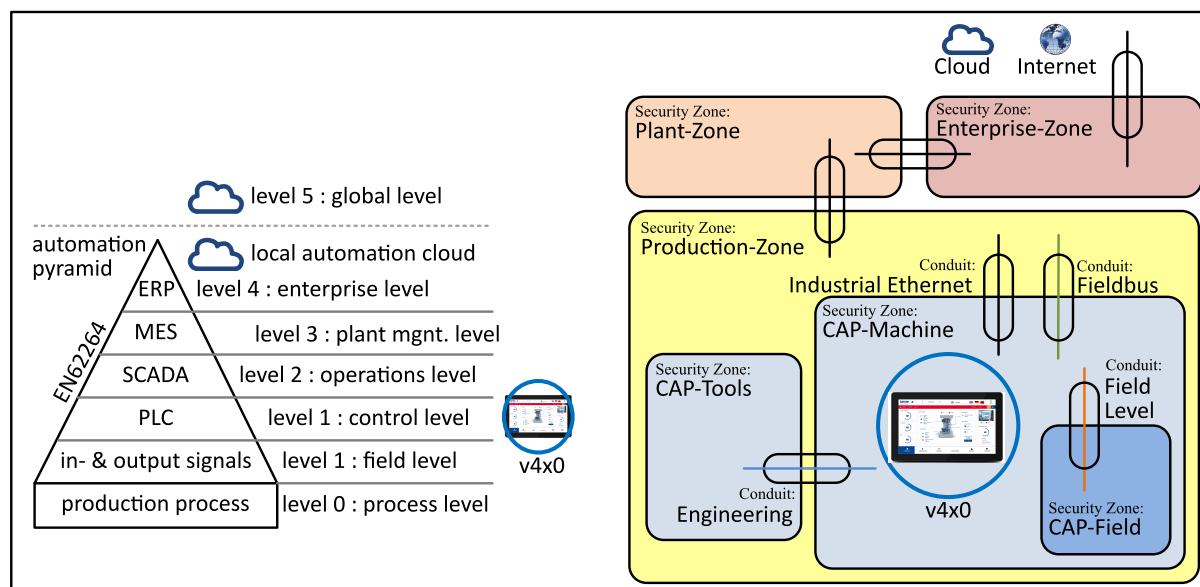
This documentation applies to the following components with their identification:

Name of product and product ID

| Name of product   | Product ID      |
|-------------------|-----------------|
| v430 7in          | V43AE70000000S  |
| v430 10.1in       | V43AEA00000000S |
| v430 15.6in       | V43AEF00000000S |
| v450 7in          | V45AP78000000S  |
| v450 10.1in       | V45APA80000000S |
| v450 15.6in       | V45APF80000000S |
| v450 PoE-Injector | V4ZA0AP010000S  |

### Location in the network

These components are located in the automation pyramid at the control level. Furthermore, they are located in the security zone "CAP-Machine" ([Zones and Conduits](#)).



Location in the network

# v4x0 Web Panel

## Product description

---

The components addressed here have one relevant interface:

- Conduit: Industrial Ethernet  
The visualization products are operated on the machine's internal network. If these components are operated outside this network, the consideration of cyber security is the responsibility of the operator. A cyber security risk analysis is recommended here.
- Conduit: USB  
The USB port (on board for the v430, can be realized via Y-cable for the v450) is only to be used for firmware updates and not for daily use. It is recommended to keep it deactivated.

### Intended purpose

The intended use of these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding cyber security are discussed.

- These components mentioned here are professional equipment and may only be commissioned and decommissioned by specialists.
- These components also require maintenance during their life cycle, which must be carried out by the operator.
- Modifications to the firmware or hardware of the component are not permitted.
- If these components are taken out of operation or disposed of, the instructions here in the documentation must be observed.
- The USB stick used for a firmware update must be physically removed and not kept plugged in.

### Intended environment

The intended environment for these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding cyber security are discussed.

- The visualization products are operated on the machine's internal network. If these components are operated outside this network, the consideration of cyber security is the responsibility of the operator. A cyber security risk analysis is recommended here.
- The components are not operated directly on the open Internet, but must also be operated by the operator via protection systems such as firewall, IDS, IPS, ... be protected.

### Security key indicators

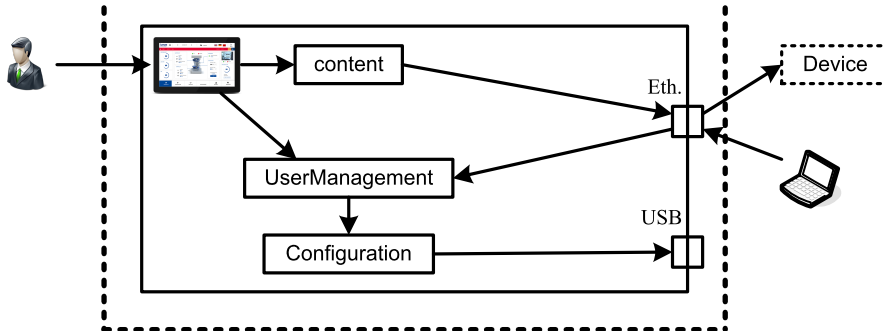
Security key indicator (in accordance with IEC 62443-4-2):

- These components are considered embedded devices (EDR).
- These components have a security level of SL-C 0.
- These components have an SL-vector from SL-C(v4x0)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }

## Security mechanisms

### Product Defense in Depth

The following image shows the Defense in Depth product concept. For the sake of clarity, some details have been deliberately omitted.

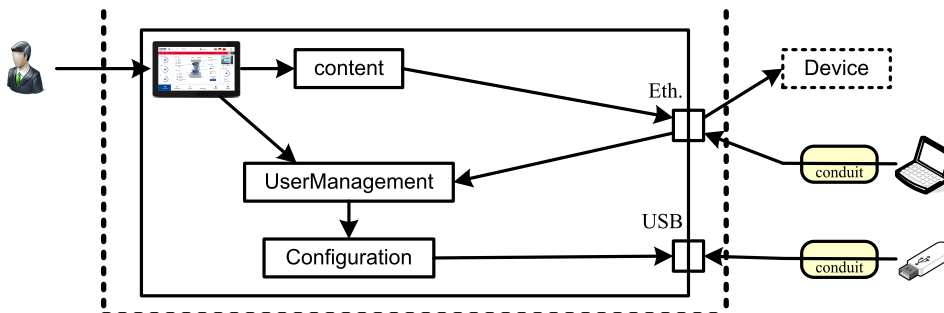


Product Defense in Depth

The core concept of the v4x0 web visualization is the in the component included web browser for presenting a web based content of an external device. The configuration is separated via an User Management and can be used via identification and authentication from a local user at the panel and some industrial communication protocols at the web panel itself.

### Expected Defense in Depth in the environment

The following image shows the Expected Defense in Depth in the environment of the controller.



Expected Defense in Depth in the environment

#### Conduit Tools:

- Access from the engineering tools to the components must be limited in terms of organization and time.
- The corresponding engineering tools must be operated on an up-to-date and IT-security-secured computer.

#### General Environment:

- General physical access protection must be provided for the components. This applies in particular to the rear of the device where the connections are made. Installation in a control cabinet or panel housing that offers physical protection is recommended.
- Existing firmware updates for the controllers as well as for all other components in the network should be installed immediately.

# v4x0 Web Panel

## Commissioning, Hardening and Decommissioning Notes and Organizational Measures

---

### Security mechanisms

The following security functions are included in the listed components (except for the PoE-Injector):

- [v4x0.FirmwareUpdate](#)
- [v4x0.Authentication](#)
- [v4x0.Authorization](#)
- [v4x0.Certificate](#)
- [v4x0.Session](#)
- [v4x0.NTP](#)
- [v4x0.Services](#)
- [v4x0.WebBrowser](#)
- [v4x0.Logging](#)
- [v4x0.Services](#)
- [v4x0.Security](#)
- [v4x0.BackupAndRestore](#)

## Commissioning, Hardening and Decommissioning Notes and Organizational Measures

The following commissioning instructions must be followed.

### General instructions

- General physical access protection must be provided for the components. This applies at the v430 in particular to the rear of the device and at the v450 at the Y-cable, where the connections are made. Installation in a control cabinet or panel housing that offers physical protection is recommended.
- In general, the USB flash drive must be organizationally protected so that written data cannot be used without authorization.
- Connecting external devices upstream to provide protection against DoS (Denial of Service) or DDoS (Distributed Denial of Service).

### Commissioning and Hardening Instructions

The following commissioning instructions must be followed.

- Update component to the latest available version ([v4x0.FirmwareUpdate](#)).
- Set up the initial `admin` account and setup more needed accounts ([4x0.Authentication](#)).
- Configure the authorization of the different roles ([v4x0.Authorization](#)).
- Create a new own certificate for the v4x0 Web Panel ([v4x0.Certificate](#)).
- Configuration of the Session Management ([v4x0.Session](#)).
- Set up and configure the NTP client, and if needed, the NTP server for time synchronization ([v4x0.NTP](#)).
- Configuration of different Services, running on the v4x0 Web Panel ([v4x0.Services](#)). Consideration of the minimization of the attack surface ([Golden Rules for Security Systems](#)), i.e. unused services should be deactivated.
- The user is recommended to carry out a risk assessment to evaluate whether the options `Enable device restore via TAP` `TAP option` or `Enable device restore via USB` should be deactivated from a security point of view ([v4x0.Services](#)).
- Check the settings for the Web Browser ([v4x0.WebBrowser](#)).
- Configure the OS- and Security-Logging ([v4x0.Logging](#)).
- Setup the configuration of the Security Settings ([v4x0.Security](#)).

### Periodic security maintenance

- It is recommended to check the password policy periodically for updates and adjust the requirements if necessary.
- It is recommended to change the passwords cyclically. Info: It is also possible to set an account as expired in days.
- It is recommended to check the certificates used with regard to their key lengths for up-to-dateness and to generate new certificates with higher key lengths if necessary.
- It is recommended to exchange the certificates regularly.
- Check if new firmware for the product is available and install to newest version.

### Decommissioning instructions

- It is recommended to update the firmware and remove all relevant applications. If the component is already up to date, a device reset ([v4x0.FirmwareUpdate](#)) is recommended.

### Removal product from environment

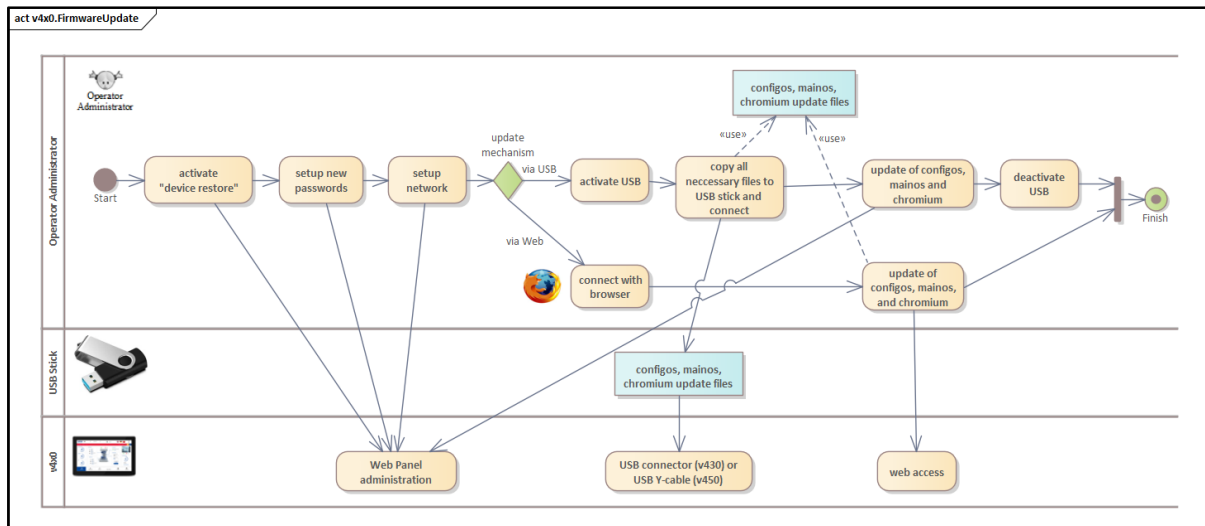
- It is recommended for all industrial communication partners of the v4x0 Web Panel to be removed, to change the trusted certificates of the v4x0 into untrusted certificates.
- It is recommended to securely remove the login data for the v4x0 Web Panel to be removed, such as name and password for the necessary authentication, from all industrial communication partners.

### Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

#### v4x0.FirmwareUpdate

The Component v4x0 has the possibility for a firmware update.



Activity Diagram



**Reset authentication management:**

If the authentication features have been lost, the components can be reset. With this procedure, all settings (not only the authentication features) are lost.



Working in the `System Settings > Management` are a critical operation and, if not performed correctly, may cause product damages requiring service of the product. Only firmware updates are recommended, a firmware downgrade may be technically possible, but is not specified as a product feature. A firmware downgrade should therefore only be carried out in exceptional situations.



**Prepare the device reset or firmware update**

1. Ask the Lenze Support for the necessary files:
  - ...configos....tar.gz
  - ...configos....tar.gz.md5
  - ...mainos....tar.gz
  - ...mainos....tar.gz.md5
  - chromium....zip
  - chromium...zip.md5
2. If you want to update via USB stick, please prepare the USB stick with one of the following file systems:
  - FAT16/32
  - Linux Ext2, Ext3 or Ext4
3. If you want to update via USB stick, please copy all files in root of the USB stick.



**To reset the component, follow these instructions:**

1. Restart the component and do a tap-tap on the left upper corner of the panel.
2. A message will appear:
  - TAP-TAP DETECTED
  - RESTART: CONFIG OS
  - >> SYSTEM SETTINGSChoose "SYSTEM SETTINGS"
3. Another message will appear:
  - ENTERING SYSTEM SETTINGS
  - >> DEFAULT MODE
  - DEVICE RESTOREChoose "DEVICE RESTORE"
4. An information will appear:
  - Restoring device to defaults  
This operation could take few minutes, please wait ...
  - Device restore successful  
Rebooting ...
5. After some time, the component will reboot automatically.

# v4x0 Web Panel

## Security functions

6. A message will appear:
  - Empty boot sequence
7. Two buttons are located on the display.
  - System Settings
  - Startup sequence
8. Start the System Settings.
9. A request appears to assign a password (and its confirmation) to the admin user.
10. Change the IP address in the System Settings menu under the Network tab:

The screenshot shows the 'System Settings' web interface. On the left is a sidebar menu with options: Basic View, Localisation, Date & Time, Network (highlighted with an orange border), Security, Applications, and Authentication. At the bottom of the sidebar is an 'EXIT' button. The main content area is titled 'System Settings' and has 'SAVE' and 'CANCEL' buttons at the top right. It is divided into sections: 'General Settings' (with fields for Hostname 'HMI-541a' and Avahi Hostname 'HMI-541a.local') and 'Network Interfaces'. The 'Network Interfaces' section contains a table with columns: Name, Label, MAC, DHCP, Address, Netmask, Gateway, and Bridged. The first row shows 'eth0' with Label 'WAN', MAC '00:0a:86:74:54:1a', and a DHCP toggle switch. The 'Address' field is highlighted with an orange border and contains '192.168.5.124'. The 'Netmask' field contains '255.255.255.0' and the 'Gateway' field contains '192.168.5.254'. Below the table is a 'DNS' section with a 'Restore' button.

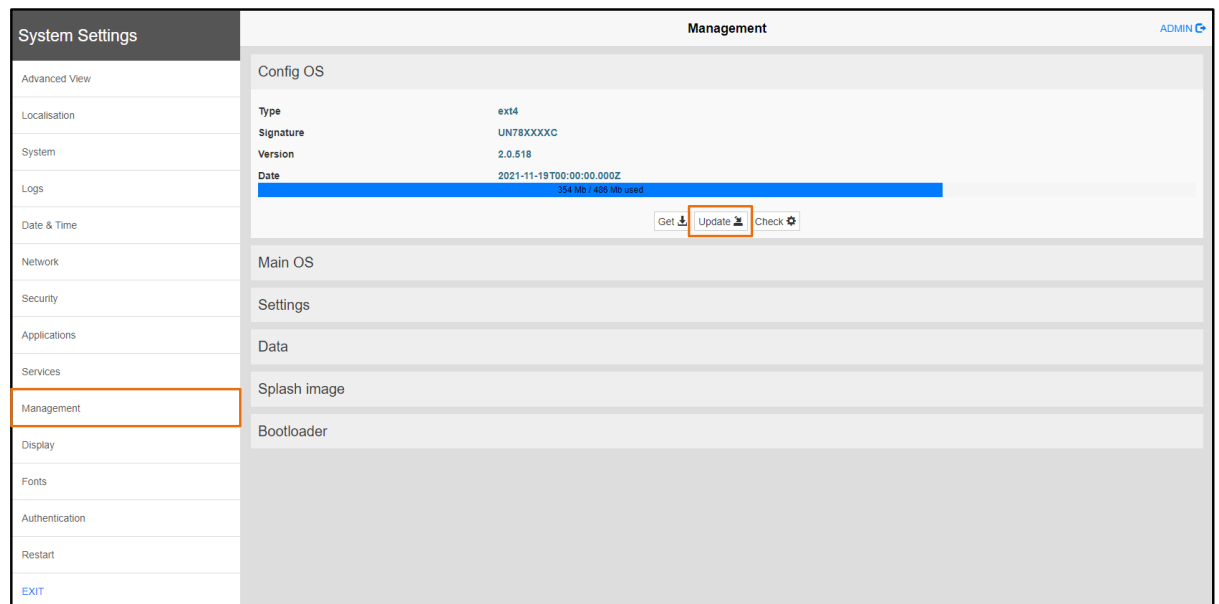
| Name | Label | MAC               | DHCP                     | Address       | Netmask       | Gateway       | Bridged |
|------|-------|-------------------|--------------------------|---------------|---------------|---------------|---------|
| eth0 | WAN   | 00:0a:86:74:54:1a | <input type="checkbox"/> | 192.168.5.124 | 255.255.255.0 | 192.168.5.254 |         |

Change IP Address

11. There are two ways to transport these files to the v4x0 component:
  - a) via USB stick to the v430 web panel
  - b) via USB stick and an Y-cable to the v450 web panel
  - c) via online web browserIf using the USB stick, you have to activate the USB Connection first via System Settings / Security / USB Devices.

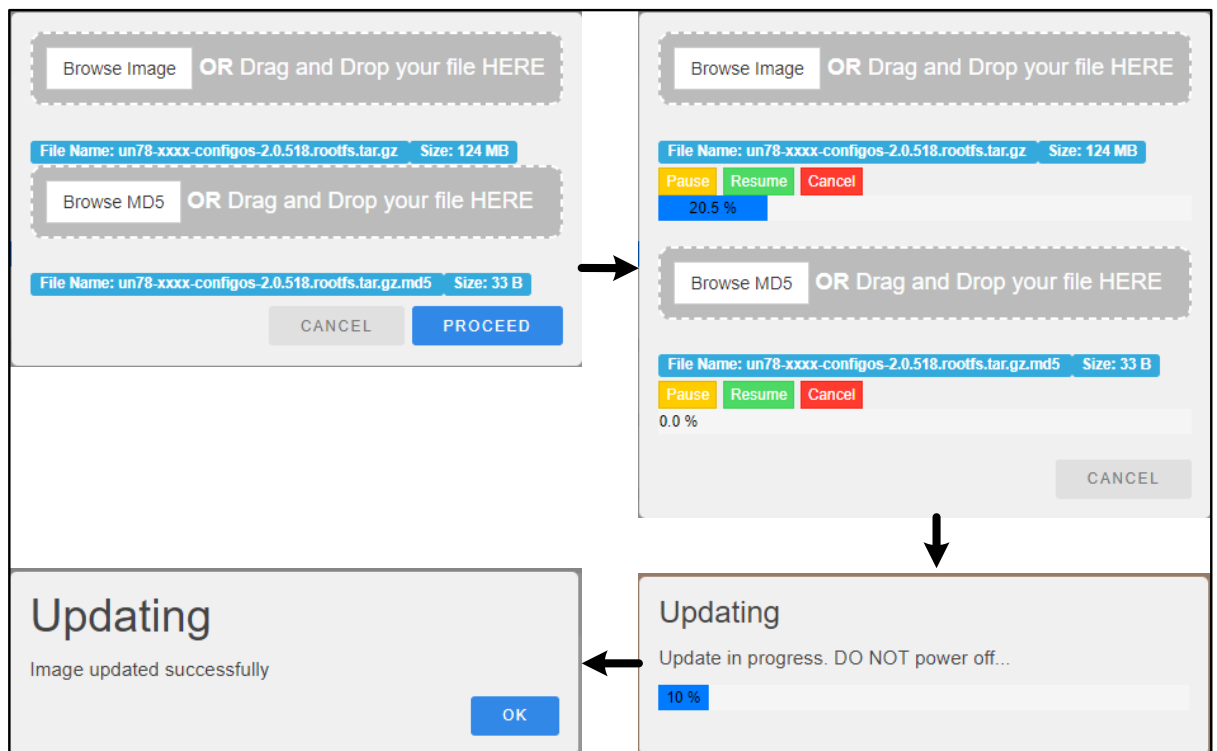


12. Update the "Config OS" via the System Settings (in Advanced View) and the Management Tab and choose Config OS and the Update button:



Config OS

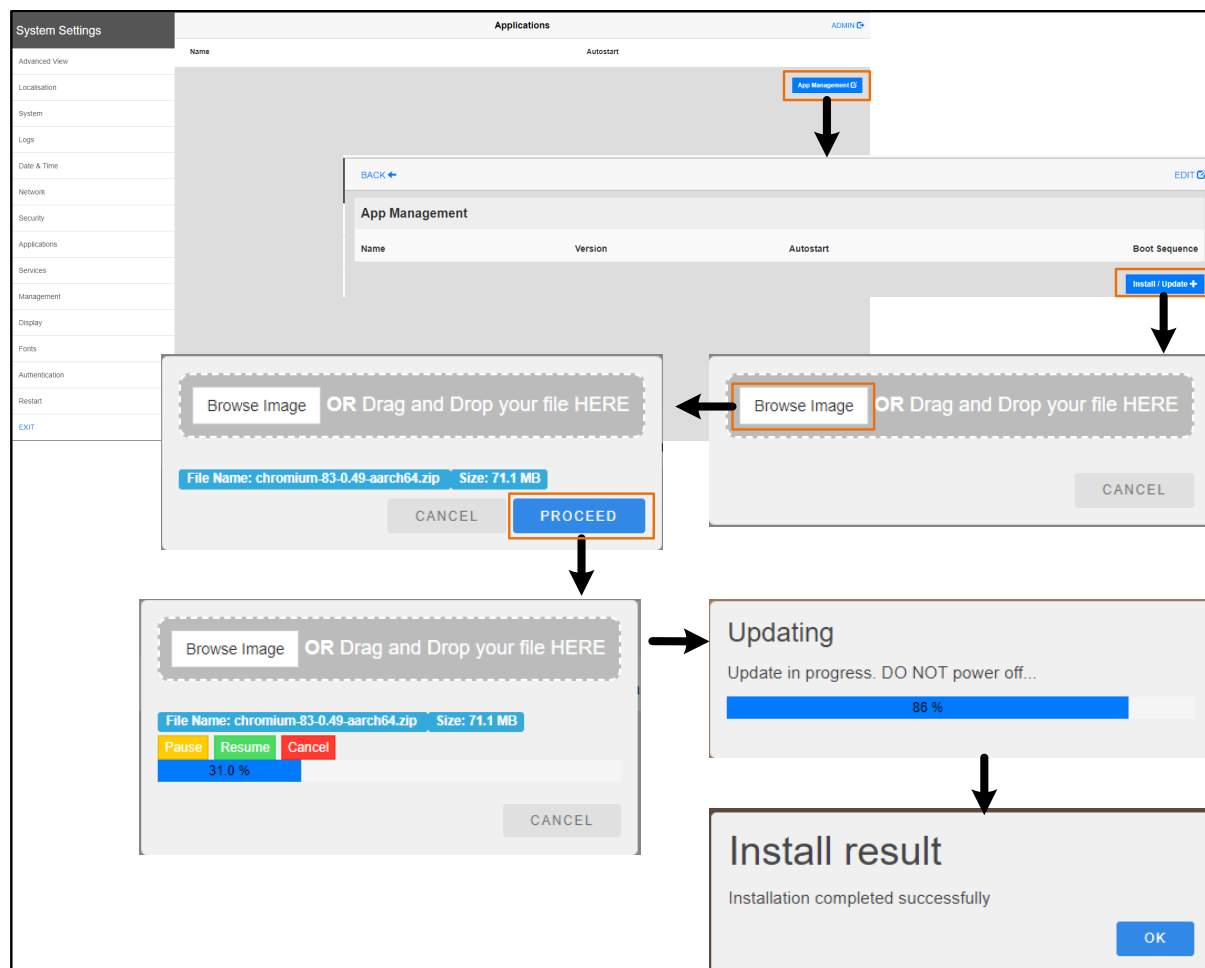
After that, please select the `configos.tar.gz` file and the `configos.tar.gz.md5` file, and then proceed, e.g. if using an USB stick update, you will find the file `/mnt/usbmemory/...`



Config OS Status

- Update the "Main OS" via the `System Settings` (in Advanced View) and Management tab. Select "Main OS" and then click the Update button.

14. In the final step, the Chromium application must be loaded. For this purpose, the application must be added in the *System Settings* (in *Advanced View*) under *Applications*.

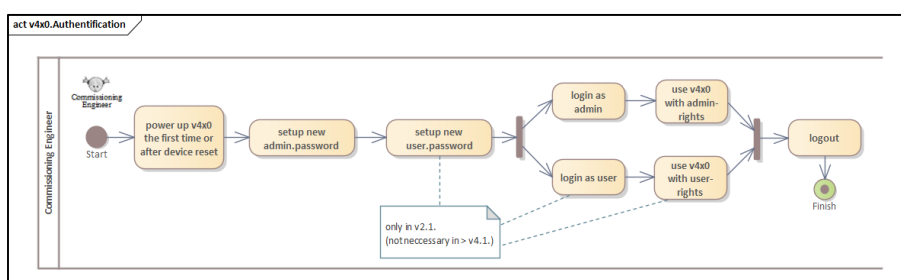


Applications

15. After a reboot, the *System Settings* contains a *Web Browser* entry. At this point, the homepage and the startup behavior can be entered.
16. If the USB connection was activated for the update, it is recommended to deactivate it again.

## v4x0 Authentication

The component v4x0 has a user management that allows users to authenticate themselves.



# v4x0 Web Panel

## Security functions

---

### Activity Diagram

There are only the admin and (depending on the version) the user account. This is delivered with

- admin name = admin,
- admin password = admin,
- user name = user (only available in version v2.1. and not in >= v4.1),
- user password = user (only available in version v2.1. and not in >= v4.1).

and must be changed when starting for the first time.

These accounts can be used in different ways.

## Login to the Panel

These accounts are needed when directly login at the web panel. There are two options:

- Double tap on the screen during startup  
Choose System Settings  
Enter Username and Password
- Long-press the upper left corner for about three seconds.  
Enter Username and Password

| System Settings | System Settings |
|-----------------|-----------------|
| Basic View      | Advanced View   |
| Localisation    | Localisation    |
| Date & Time     | System          |
| Network         | Logs            |
| Authentication  | Date & Time     |
| Web Browser     | Network         |
| EXIT            | Services        |
|                 | Management      |
|                 | Display         |
|                 | Fonts           |
|                 | Authentication  |
|                 | Restart         |
|                 | Web Browser     |
|                 | EXIT            |

System Settings for user (Basic View) and admin (Advanced View)

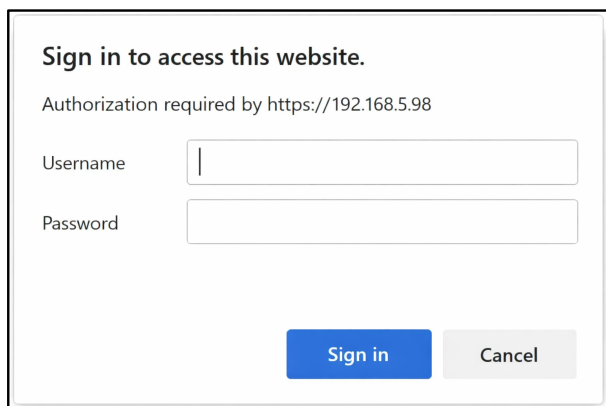
# v4x0 Web Panel

## Security functions

### Using a Web-Browser for Login

These accounts are also needed when connecting a device to the web panel via a web browser.

- Open web browser
- Connect to IP address of the web panel
- Enter Username and Password

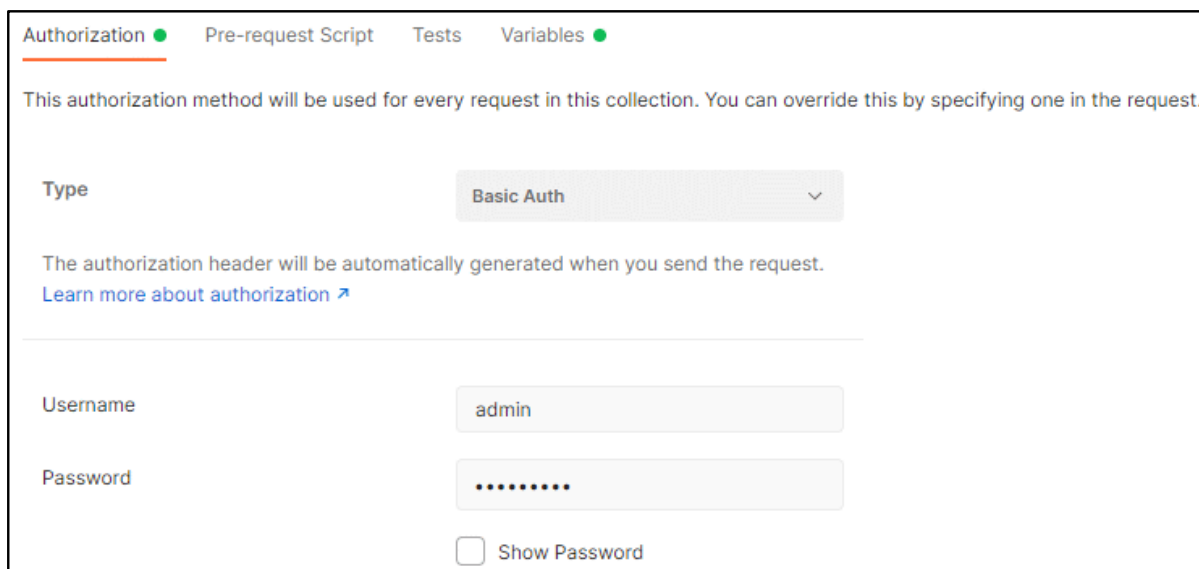
A screenshot of a web browser login dialog box. The title is "Sign in to access this website." Below the title, it says "Authorization required by https://192.168.5.98". There are two input fields: "Username" and "Password". At the bottom, there are two buttons: "Sign in" (blue) and "Cancel" (gray).

Authentication via Web-Browser

### Using e.g. Postman for API-connection

These accounts are also needed when using the API via e.g. POSTMAN:

- Start Postman
- Create new collection
- Choose "Type: Basic Auth"
- Enter Username and Password
- Using url `https://<ip>/rest/api/v1`

A screenshot of the Postman interface showing the "Authorization" tab. The title is "Authorization" with a green dot. Below the title, it says "This authorization method will be used for every request in this collection. You can override this by specifying one in the request." There is a dropdown menu for "Type" with "Basic Auth" selected. Below the dropdown, it says "The authorization header will be automatically generated when you send the request." and there is a link "Learn more about authorization". There are two input fields: "Username" with the value "admin" and "Password" with masked characters ".....". At the bottom, there is a checkbox labeled "Show Password" which is unchecked.

Authentication via postman



A GET request to the URL returns all the setting options. A GET request to the URL followed by a parameter returns the value of that parameter.

### Handling Roles

This functionality is available from v4.1 and only visible if logged in as `admin`.

By default, an `admin` role is created in which the default `admin` user is located.

In `System Settings > Authentication > Roles [Edit]` the `admin` user is able to add new roles with the "+" button. After assigning a role-name, the role can be added via `Add Role` button. There is a limitation of 30 roles.

Once new roles have been created, they can be removed again (except for the `admin` role).

### Handling Rights of the Roles

For more information, refer to chapter [v4x0.Authorization](#).

### Handling Users

This functionality is available in v2.1 but is extended in v4.1 and only visible if logged in as `admin`.

By default, an `admin` user is assigned in `admin` role with `never` expiration.

In `System Settings > Authentication > Users [Edit]` the `admin` user is able to add new Users with the "+" button. After filling the following information, the user can be added via `Add User` button. There is a limitation of 50 users.

| Object                           | Description                                                                                                                                                                                                                                                                                       |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username                         | Set a new username.                                                                                                                                                                                                                                                                               |
| Role                             | Select one of the existing Roles.                                                                                                                                                                                                                                                                 |
| New Password<br>Confirm Password | Choose and confirm a new password in the given password policy (refer to chapter <a href="#">v4x0.AccountManagementGuidelines</a> ).                                                                                                                                                              |
| Password validity (days)         | Select the validity time of the password. If the password should not be limited in time, delete the default number so that there is an empty field and Forever appears. This makes the password permanently valid.<br><br>After the validation date, the user is required to change the password. |

The `admin` user is also able to enable or disable other users.

If a new added user log in the first time, the user has to change the initial password, giving from the `admin`.

### Forgot password

In the event that all `admin` users have forgotten their password, access to the device configuration will be irrevocably lost. To restore functionality, a device reset must be performed, refer to chapter [v4x0.FirmwareUpdate](#)



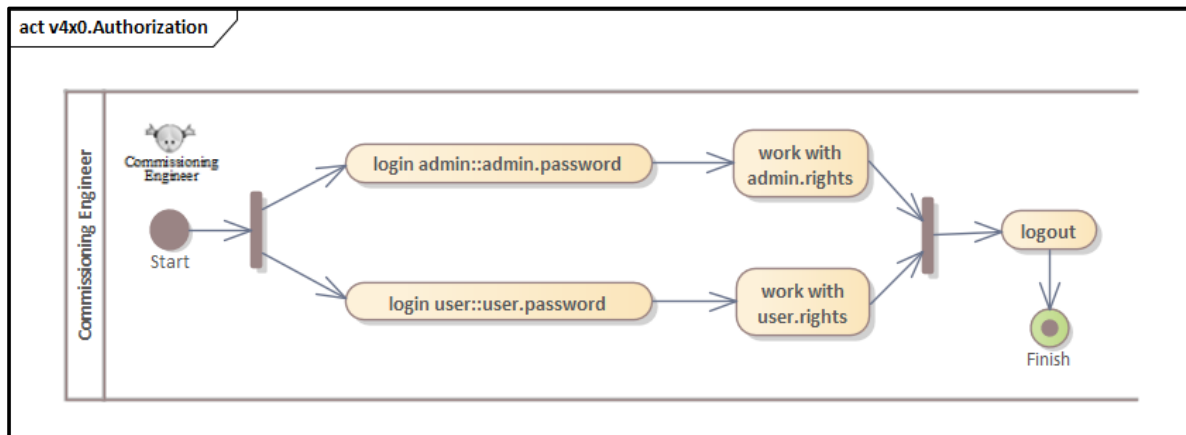


## v4x0.Authorization

Authorization management has changed between versions v2.1 and v4.1.

### Authorization in version v2.1

Since there are only two users on this component, the admin and the user, there is no need to configure the rights. These are fixed.



Activity Diagram

The services are permanently assigned to the necessary authorizations. Some examples are listed below.

Admin or user rights required:

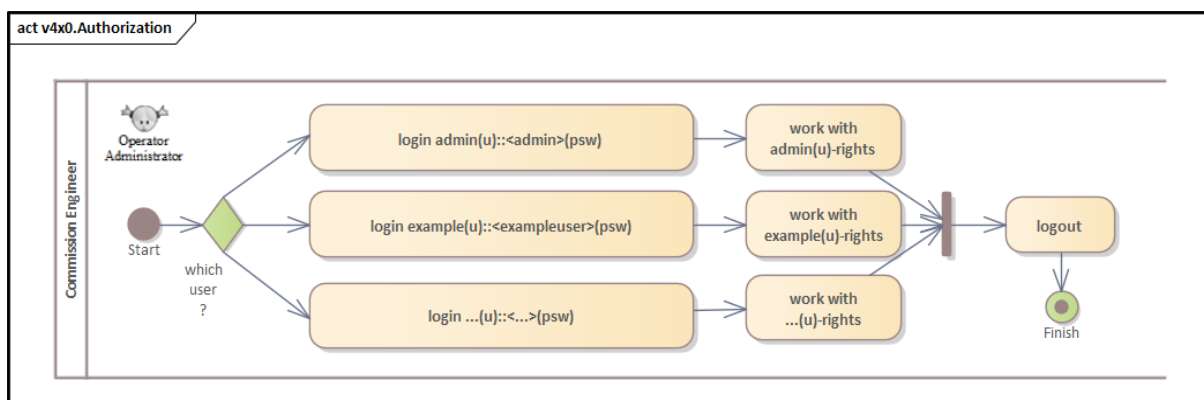
- Set Homepage in the Web Browser
- Change User Password
- Display Settings

Admin rights required:

- Change Admin Password
- Create new x.509 Certificate
- Change App Management

### Authorization from v4.1 onwards

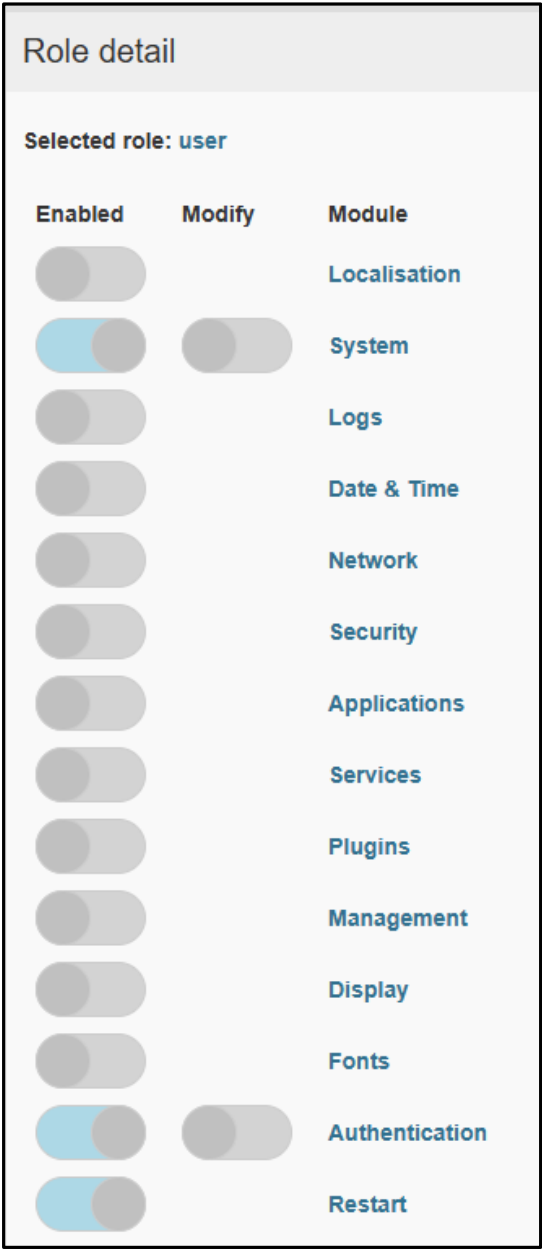
In v4x0 version  $\geq 4.1$ , there is only the default admin user. All other users can be added during runtime.



Activity Diagram

In `System Settings > Authentication > Roles` the admin user is able to set the Rights of each existing role (with the exception of the admin role, which has all rights).

Choose one of the Roles and click the ">" button.

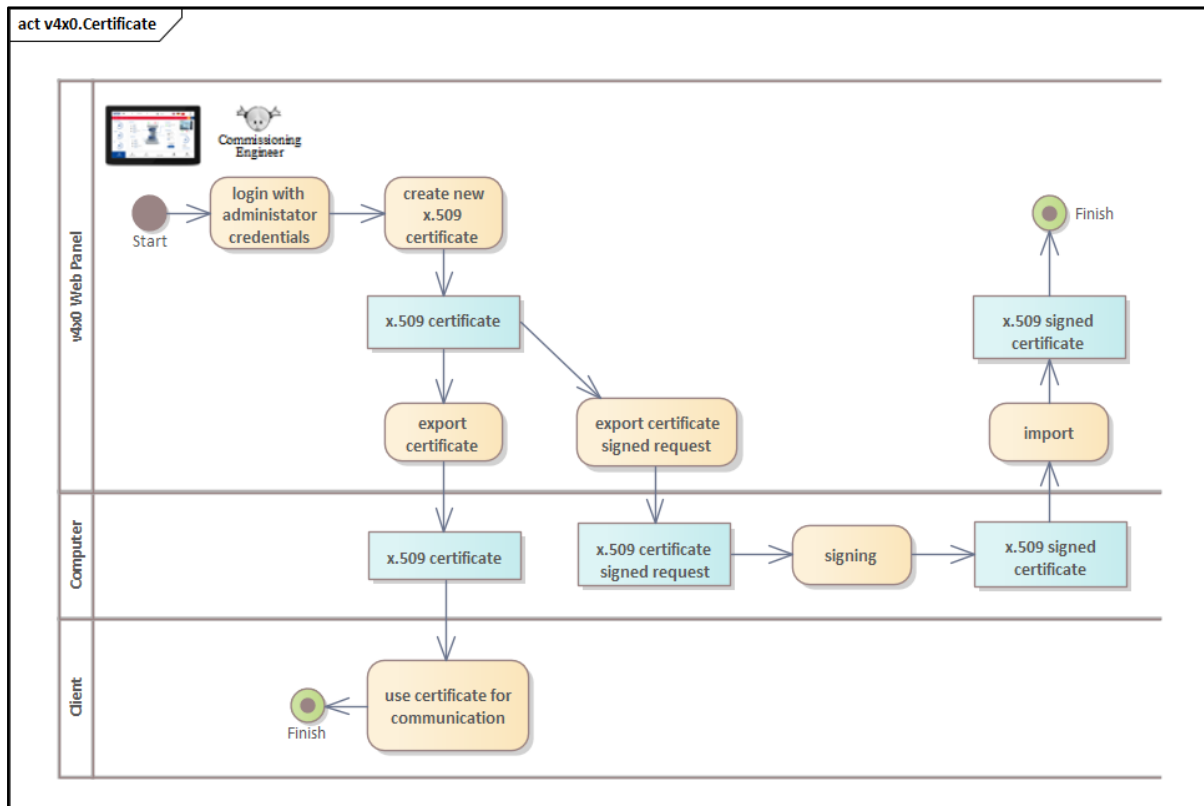


Role detail

For the selected user, the setting for `Enable` and for some modules also the selection `Modify` can be made for the respective modules.

## v4x0.Certificate

In order to use certificates, they must be created in advance on the component.



Activity Diagram

To do this, you must first create your own certificate on the component. This is done using the `System Settings` option in the `Authentication` menu under the `x.509 Certificate` heading. You will need to log in as admin to do this.

You can then define the data for the certificate, the validity period in days and the key length. Click `Generate` to create the certificate.

# v4x0 Web Panel

## Security functions

System Settings

Advanced View

Localisation

System

Logs

Date & Time

Network

Security

Applications

Services

Management

Display

Fonts

Authentication

Restart

Web Browser

EXIT

CANCEL ✕

Users

Username

admin

Old Password

New Password

Confirm Password

Change Password ⚙

Passwords are required to include:

At least 8 characters in total

At least one lower case and one upper case letter

At least one numeric character

At least one special character (eg. # ! @ ?)

x.509 Certificate

Device Name

Organization

Unit

State

Location

Country

Valid (days)

Key Length

v450

Lenze

SE

Niedersachsen

Hamel

DE

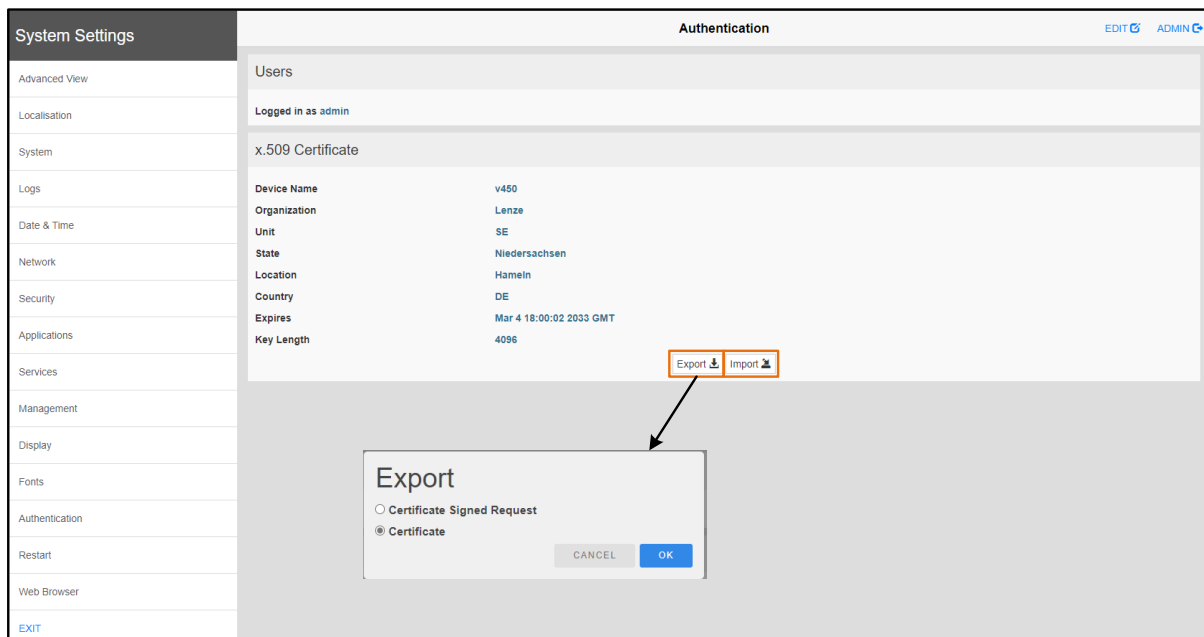
365

4096

Generate ⚙

System Settings

Once the certificate has been generated, an `Export` and an `Import` button will be available.

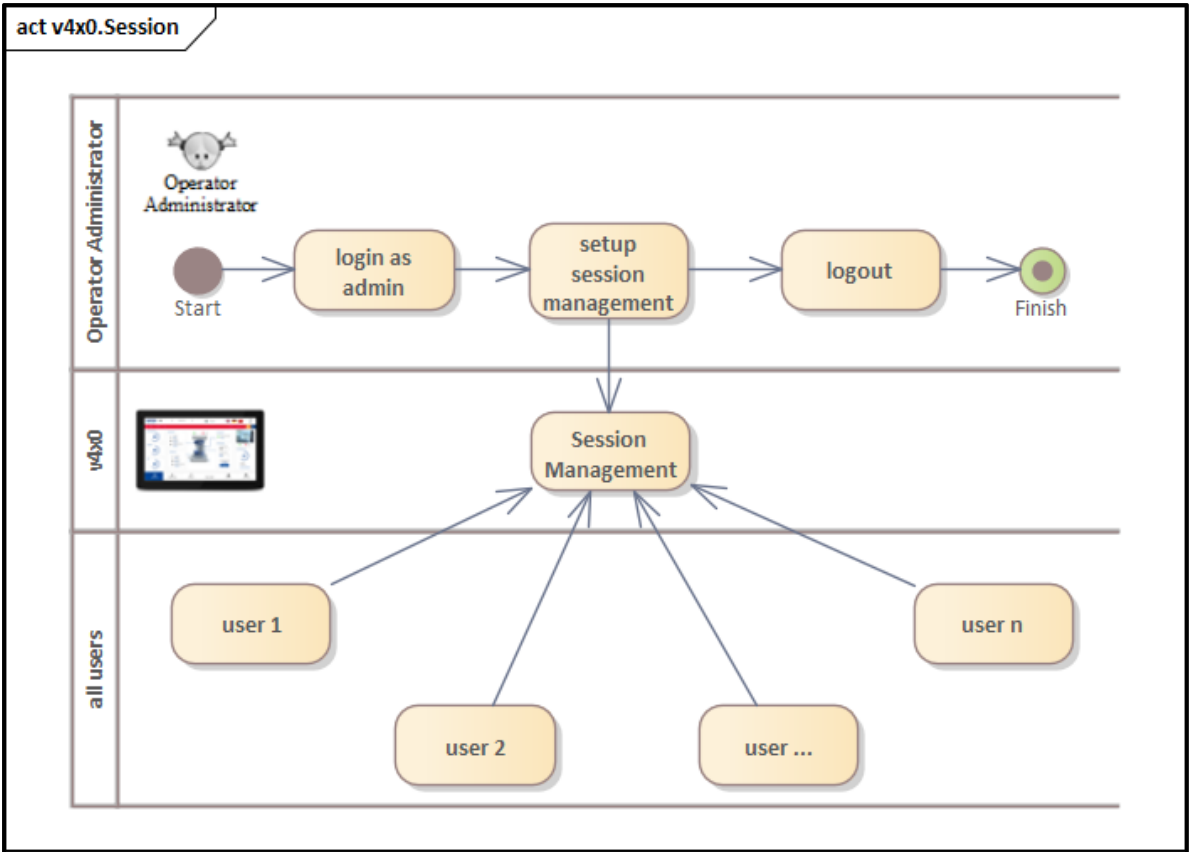


Export and Import of Certificates

At this point, there are two options. Firstly, the certificate can be exported to use it e.g. for encrypted communication. Secondly, the certificate can be exported with a signed request to sign it. The signed certificate can then be imported again.

## v4x0.Session

From v4.1 onwards, there is a session handling dialog, where the `admin` can setup the session parameter.



Activity Diagram

The timeouts can be set with the first two settings.

| Object                       | Description                                                                 |
|------------------------------|-----------------------------------------------------------------------------|
| Inactivity Timeout (minutes) | Time after user-inactivity before the session expires and loses.            |
| Session Timeout (minutes)    | Allowed duration for a work session, after the user has to re-authenticate. |

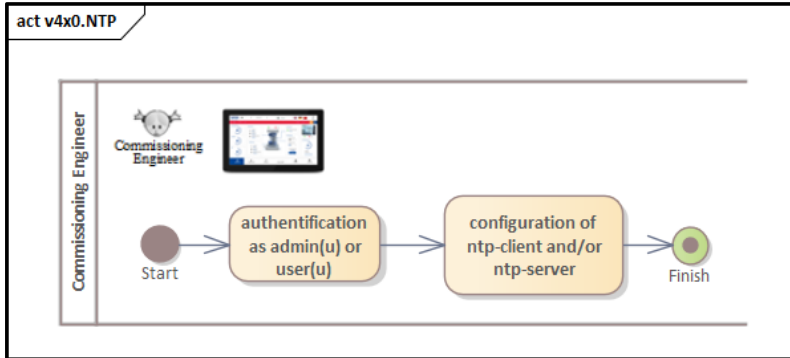
The number of failed attempts can be specified.

| Object                  | Description                                                                                                         |
|-------------------------|---------------------------------------------------------------------------------------------------------------------|
| Max user login attempts | The number of failed attempts can be specified. If this number of failed attempts is reached, the user is excluded. |
| Max host login attempts | The number of failed attempts can be specified. If this number of failed attempts is reached, the user is excluded. |

The access can be specified per minute, per hour and per day. The blocked account will be unlocked after expiration of the time limit or device reset.

## v4x0.NTP

To configure time synchronization via NTP poll process ([Network Time Protocol](#)), the user admin must first authenticate on the v4x0 Web Panel.



Activity Diagram

All configurations can be found in the System Settings > Date & Time [EDIT] menu.

The screenshot shows the 'Date & Time' configuration page. It includes fields for 'Current Timezone' (set to Universal), 'Current Date' (Sunday, April 12, 2026), and 'Local Time' (10:29 AM). Below these are four configuration options, each with a numbered callout:

- 1. Automatic Update (NTP) slider (checked).
- 2. NTP server address input field (containing pool.ntp.org).
- 3. Slow time adjustment (not more than one minute a day) slider (checked).
- 4. Accept NTP requests slider (checked).

Configuration

### Configuration of the NTP client:

- ( 1 ) Activate the Automatic Update (NTP) slider.
- ( 2 ) Add the address of the pool or the IP address of the time server.
- ( 3 ) Activate or Deactivate the signification correction.  
Deactive: The NTP can apply a signification correction.  
Active: Slow time adjustment is set to 500 ppm. 500 ppm is 0.5 ms per Second (Example: 1 hour timeshift will need about 43 days).  
"This feature is available in v4.1 and not in older versions like v2.1"

The configuration is saved by clicking the save button.



The datetime will be synchronized via the NTP client from the NTP server\* cyclic each ~ 30 seconds during operation.

### Configuration of the NTP server:

- Activate the Accept NTP requests.

# v4x0 Web Panel

## Security functions

The configuration is taken over with the save button. After activation the NTP Server will be reachable on port udp/123.

### v4x0.Services

This chapter only deals with the services that are relevant to security. They are located in `System Settings > Services`.

#### Autorun scripts from external storage

This setting is relevant for an autostart of an `autoexec.sh` script file on a USB stick. From a security point of view, it is strongly recommended to leave this setting deactivated.

#### Avahi Daemon

Avahi is a system which enables programs to publish and discover services and hosts running on a local network. So the user can access the device via host name and not via IP address.



Avahi Daemon runs on port udp/5353. From a security point of view, it is recommended that the Avahi daemon is only activated if it is actually used.

#### DHCP Server

DHCP Server can be activated and used with following parameters:

| Object                | Description                                                          |
|-----------------------|----------------------------------------------------------------------|
| Start<br>IP<br>End IP | IP addresses distributed from the DHCP Server.                       |
| Gateway               | Gateway address.                                                     |
| Netmask               | Netmask.                                                             |
| DNS Server            | DNS Server address.                                                  |
| Lease Time (seconds)  | Lease Time<br>[ 60s   86400s (1 day) is default   864000 (10 days) ] |

#### Enable device restore via TAP TAP options

When enabled, it gives the possibility to reset the v4x0 Web Panel in case the admin password is forgotten.



This option is enabled by default. The user is recommended to carry out a risk assessment to evaluate whether this option should be deactivated from a security point of view.

#### Enable device restore via USB

When enabled, it gives the possibility to reset the v4x0 Web Panel in case the admin password is forgotten.





This option is enabled by default. The user is recommended to carry out a risk assessment to evaluate whether this option should be deactivated from a security point of view.

## Firewall Service

There is a firewall in the v4x0 Web Panel, which can be found under `System Settings > Services > Firewall Service [EDIT]`.

Firewall Settings

First, the user has to enable the Firewall service.

After activation, a general Allow decision can be made for each stored protocol. The typical protocols are already included in the table and can be extended individually for each customer using the "+" button.

| Object           | Description                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allow            | Enable / Disable Firewall Rule.                                                                                                                                                                                                |
| Name             | Name of Firewall Rule.                                                                                                                                                                                                         |
| Source Interface | Network Interfaces:<br>any : applies to all networks<br>eth0 : applies to Ethernet-Interface<br>ppp0 : applies to WLAN-Interface (not available on v4x0)<br>tun0 : applies to VPN-Interface<br>tap0 : applies to TAP-Interface |

# v4x0 Web Panel

## Security functions

| Object               | Description                                                                                                                                                                                                                                    |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source IP or Network | If this field remains empty, the source IP is not checked and all accesses are permitted. Access can be restricted by entering a specific IP address (e.g. 192.168.100.100) or a range of IP addresses in CIDR format (e.g. 192.168.100.0/24). |
| Port or Range        | Single port (e.g. 443) or port range (440-450).                                                                                                                                                                                                |
| Protocol             | BOTH   TCP   UDP                                                                                                                                                                                                                               |
| ^ v                  | change order of firewall rule lines                                                                                                                                                                                                            |
| copy (blue icon)     | copy firewall rule line                                                                                                                                                                                                                        |
| delete (red icon)    | remove firewall rule line                                                                                                                                                                                                                      |

In the last section, the network traffic to a DNS server can be limited. A distinction can be made between whitelist (only allow certain DNS) and blacklist (prohibit certain DNS).

### Network Rate Limiter

There is a Network Rate Limiter in the v4x0 Web Panel, which can be found under **System Settings > Services > Network Rate Limiter [EDIT]**.

| Object            | Description                                                                                                                                                                                                                    |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active            | Enable / Disable Limiter Rule.                                                                                                                                                                                                 |
| Name              | Name of Limiter Rule.                                                                                                                                                                                                          |
| Source Interface  | Network Interfaces:<br>any : applies to all networks<br>eth0 : applies to Ethernet-Interface<br>ppp0 : applies to WLAN-Interface (not available on v4x0)<br>tun0 : applies to VPN-Interface<br>tap0 : applies to TAP-Interface |
| Type              | Network Package Type:<br>ETHER : Ethernet Packages<br>IP : IP Packages<br>SYN : TCP-SYN Packages<br>UNI : Unicast Packages                                                                                                     |
| Rate              | Rate over time period                                                                                                                                                                                                          |
| Measure           | Time period<br>Pcks/sec : Packages per second<br>Pcks/min : Packages per minute<br>Mbps : Megabytes per second                                                                                                                 |
| Port or Range     | Assign Filter to a single port (e.g. 20) or port range (e.g. 20-30).                                                                                                                                                           |
| Protocol          | IPv4 : Internet Layer Protocol, including TCP, UDP, ICMP<br>ARP : Address Resolution Protocol<br>TCP : Transmission Control Protocol<br>UDP : User Datagram Protocol<br>ICMP : Internet Control Message Protocol               |
| ^ v               | change order of limiter rule lines                                                                                                                                                                                             |
| copy (blue icon)  | copy limiter rule line                                                                                                                                                                                                         |
| delete (red icon) | remove limiter rule line                                                                                                                                                                                                       |

### SNMP Server

The SNMP Server can use the Simple Network Management Protocol (SNMP) to deliver measured values to a central management system on request. Configuration can be made via `System Settings > Services > SNMP Server [EDIT]`.

If the SNMP service is enabled, an external SNMP manager can obtain and process information from the v4x0 Web Panel. The SNMP server runs on UDP port 161.



As long as the SNMP Server is not required, it is strongly recommended to deactivate it for security reasons.

### SSH Server

The SSH server enables external access to the v4x0 Web Panel. This can be done via an external SSH client. The SSH server runs on port tcp/22 and can only be used by the `admin` user. Configuration can be made via `System Settings > Services > SSH Server [EDIT]`.



As long as the SSH Server is not required, it is strongly recommended to deactivate it for security reasons. The Autostart setting in particular is not recommended, as access is otherwise always possible.

### VNC Service

The VNC Service enables external access to the v4x0 Web Panel via VNC. This allowed remote access to the display of the v4x0 Web Panel. The VNC Service runs on port tcp/5900. Configuration can be made via `System Settings > Services > VNC Service [EDIT]`.



As long as the VNC Service is not required, it is strongly recommended to deactivate it for security reasons.

### Web Server

The Web Server configuration can be found in `System Settings > Services > Web Server [EDIT]`.

| Object                              | Description                                                                                                                                                                          |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allow only Secure HTTPS connections | Disabled by default to maintain backward compatibility, but it is recommended to enable this option.                                                                                 |
| CORS domains enabled                | When disabled (default), access to external domains is not allowed. If this setting is activated, the following filter is applied.                                                   |
| CORS domains filter                 | One or more domains can be specified.<br><br>Example of a domain:<br><code>www.test.com</code><br><br>Example for multiple domains:<br><code>re:(www.test1.com www.test2.com)</code> |

# v4x0 Web Panel

## Security functions

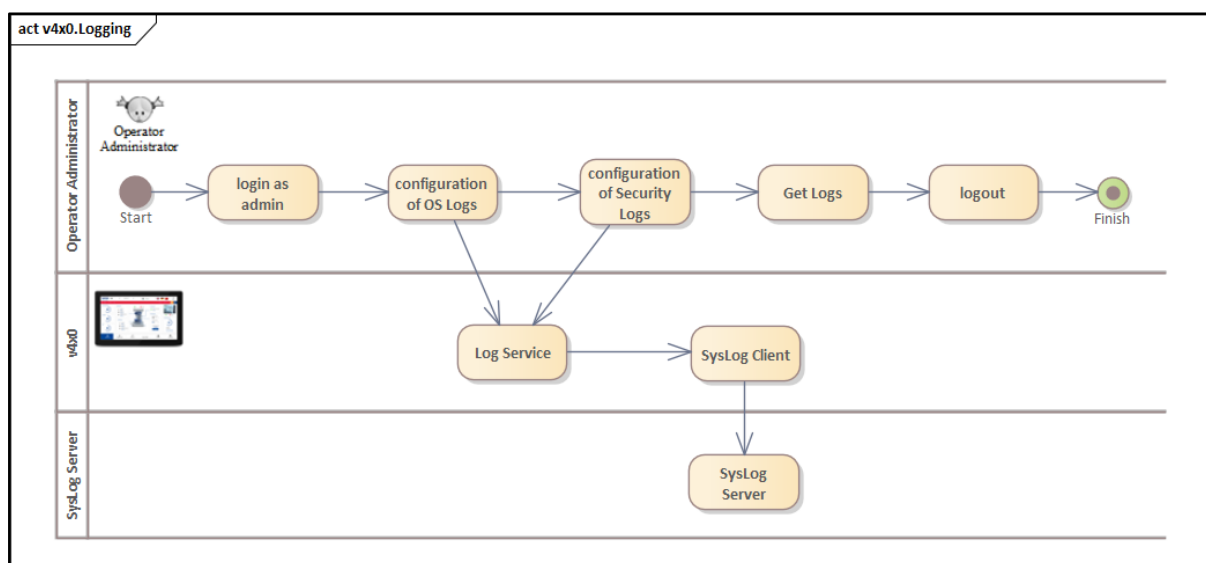
### v4x0.WebBrowser

The configuration of the Web Browser is available via `System Settings > Web Browser [EDIT]`. A lot of configuration can be done via this setting page. The following parameters are relevant for the security of the product.

| Object                                             | Description                                                                                                                                                                                                                   |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allow downloading files                            | Enable download files into /mnt/-data/storage/chromium/home/Downloads folder.<br><br>From a security point of view, this function, which is deactivated by default, should only be activated if the feature is really needed. |
| Change UserAgent                                   | This overrides the default browser user agent.<br><br>From a security point of view, this setting should be deactivated by default.                                                                                           |
| Certificates<br>(only available on local settings) | This function will open the Certificate Manager of the v4x0 Web Panel. Own Certificates, Server Certificates, Authority Certificates and Other Certificates can be viewed and imported / exported.                            |
| Certificate preferences                            | Clear all white listed sites in the Web Browser.                                                                                                                                                                              |
| Enable password management                         | The password management in the browser is default deactivated.<br><br>From a security point of view, this function should only be activated if the feature is really needed.                                                  |

### v4x0.Logging

The v4x0 Web Panel has integrated Logging functions.



Activity Diagram

## OS Logs

In `System Settings > Logs > OS Logs [EDIT]` the admin user can set the following two parameters for the OS Logging:

| Object             | Description                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------|
| Persistent (debug) | The OS Logs will be saved persistent, so the log files are available after shutdown and rebooting the v4x0. |
| Size (MB)          | Maximum size of Logfile.                                                                                    |

## Security Logs

In `System Settings > Logs > Security Logs [EDIT]` the admin user can set the following parameters of the RFC 5424 compliant Security Log:

| Object         | Description                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------------------|
| Persistent     | The Security Logs will be saved persistent, so the log files are available after shutdown and rebooting the v4x0. |
| Size (MB)      | Maximum size of Logfile. Info: The internal logging routine will generate three rotating files of this size.      |
| Remote Logging | Activation of the SysLog Client.                                                                                  |
| Server         | IP address of the SysLog Server.                                                                                  |
| Port           | Port of the SysLog Server. Info: The typical port is udp/514 and tcp/514.                                         |

## v4x0.Security

The main security configuration is located in `System Settings > Security [EDIT]`.

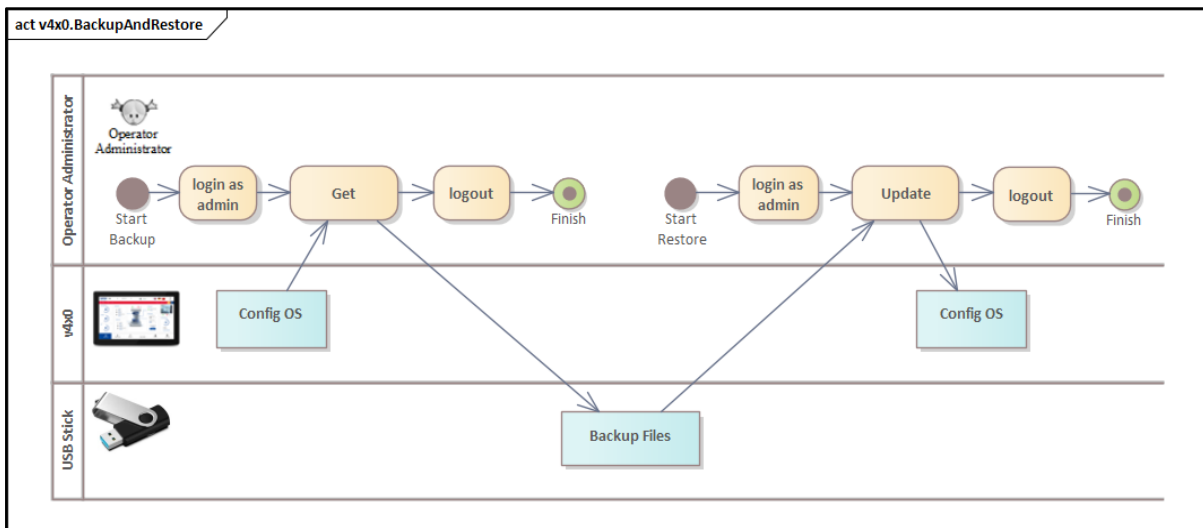
| Object              | Description                                                                                                                                                                                          |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Credentials         | This is an integrated Credential Manager. It can be used by installed applications that have the rights to use it.<br><br>It is not recommended to create and use your own third party applications. |
| External Devices    | If disabled, unknown USB devices are not accessible.                                                                                                                                                 |
| Software components | Allow installation of unsigned modules (insecure mode).<br><br>It is recommended to disable this feature from a security perspective.                                                                |

## v4x0.BackupAndRestore

For Backup and Restore use the `System Settings > Management > Config OS [EDIT]` function.

# v4x0 Web Panel

## Security data



Activity Diagram

### Backup

Use a USB Stick (v430: on the USB port, v450: on the Y-cable) and activate the USB connector.

Then activate the **Get** function in **System Settings > Management > Config OS [EDIT]**.

A .tar.gz file is written to the USB stick.



The backup file is a .tar.gz file and contains unencrypted information about the backup. It must therefore be organizationally protected against unauthorized access.



An integrity file is also required for the restore process. To generate this, it is recommended to generate it during the backup process.

There are many ways to create an MD5 file. As an example, the following function can be used by Windows:

```
CertUtil -hashfile data.tar.gz MD5 > data.tar.gz.md5
```

### Restore

Use a USB Stick (v430: on the USB port, v450: on the Y-cable) and activate the USB connector with an valid backup file and the md5 integrity file.

Then activate the **Update** function in **System Settings > Management > Config OS [EDIT]**.

A .tar.gz file is loaded from the USB stick and will restore the system of the v4x0 Web Panel.

## Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

## v4x0.AccountManagementGuidelines

The Account Management Guidelines of the v4x0 Web Panel are described below. The focus here is on the TAP TAP login, login via browser, login via API, login via SSH or login via SFTP.

### v4x0.AccountManagementGuidelines :: v4x0.UserManagement

#### Default / Factory Settings:

The User Management of the v4x0 Web Panel is activated per default.

In v2.1 the User Management of the v4x0 Web Panel is delivered with

- "admin" (user) | "admin" (group) | "admin" (password)
- "user" (user) | "user" (group) | "user" (password)

From v4.1 onwards, the User Management of the v4x0 Web Panel is delivered with

- "admin" (user) | "admin" (group) | "admin" (password)

#### Account Handling:

- During the first start and first login, the user has to change the password of the v4x0 Web Panel.

#### Policies:

The password policy is activated by default. The current default settings are as follows:

Password policy for user and admin passwords:-

- min. 8 and max. 128 characters
- at least one lower case letter
- at least one upper case letter
- at least one numeric character
- at least one special character [@\$!%\*\_|/./:;(){}?&^+=+<>#]

The admin user is able to change the password policy via System Settings > Authentication > Password policy [Edit].

## v4x0.PortList

From v4.1 onwards, the following ports are available in the v4x0 Web Panel (if activating these functionalities and open the ports in the firewall).

| Port            | Description      |
|-----------------|------------------|
| tcp/21          | FTP Command Port |
| tcp/22          | SSH Server       |
| tcp/80          | HTTP             |
| tcp/443         | HTTPS            |
| tcp/5900        | VNC Service      |
| tcp/18756-18760 | FTP Passive mode |
| udp/67          | DHCP Server      |
| udp/123         | NTP Server       |

# v4x0 Web Panel

Security data

---

| Port        | Description      |
|-------------|------------------|
| udp/161     | SNMP Server      |
| udp/990-991 | Device Discovery |
| udp/5353    | Avahi Daemon     |



## EASY Starter Suite

This chapter describes all the functions of the EASY Starter Suite

- EASY Package Manager
- EASY Starter
- EASY Firmware Loader
- EASY Application Loader

EASY Starter

Product description

Product identification

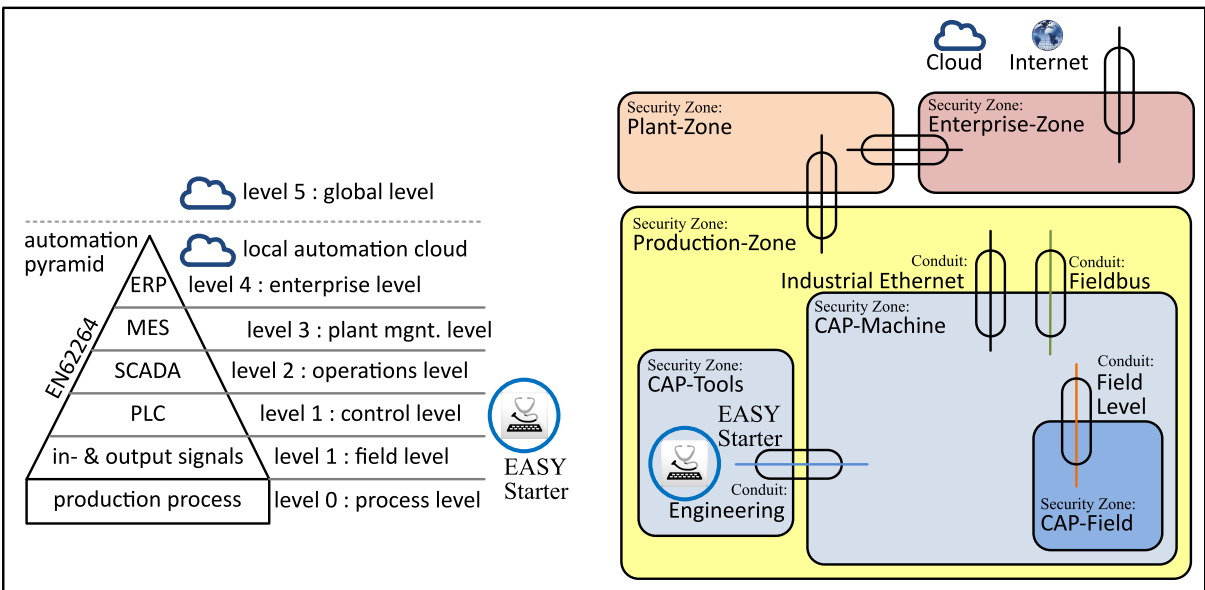
This documentation applies is applicable to the following components with their identification:

Name of product and product ID

| Name of product                                      | Product ID |
|------------------------------------------------------|------------|
| »EASY Starter«<br>(part of the »EASY Starter Suite«) | n.a.       |

Location in the network

This component is located in the automation pyramid at the control level. Furthermore, they it is located in the security zone "CAP-Tools" ([Zones and Conduits](#)).



Product location in the network

The software addressed here has only one relevant interface:

- Conduit: Engineering  
This connection is used to connect the tool to the Security Zone CAP-Machine.

Intended purpose

The intended user of this component is described in the application as directed and can be found in the operating instructions in the online help. In the following, some specifics regarding cyber security are discussed.

- This component mentioned here is professional software and may only be commissioned and decommissioned by specialists.

- This software also requires maintenance throughout its life cycle, which must be carried out by the operator.
- Modifications to the software are not permitted.
- If this software is taken out of operation or disposed of, the instructions in the documentation must be observed.

#### Intended environment

The intended environment for this software is described in the application as directed and can be found in the online help. In the following, some specifics regarding cyber security are discussed:

- The software must be installed on an up-to-date computer equipped with valid IT protection mechanisms.
- The software must be installed on a computer, which uses protection against unauthorized use.
- Use appropriate authentication mechanisms for the computer. This applies, for example, to passwords that have the necessary complexity and an appropriate life cycle. The current state of the art must be taken into account here.
- This computer is the responsibility of its owner and must be protected by valid IT protection systems such as firewall, IDS, IPS, etc.

#### Security key indicators

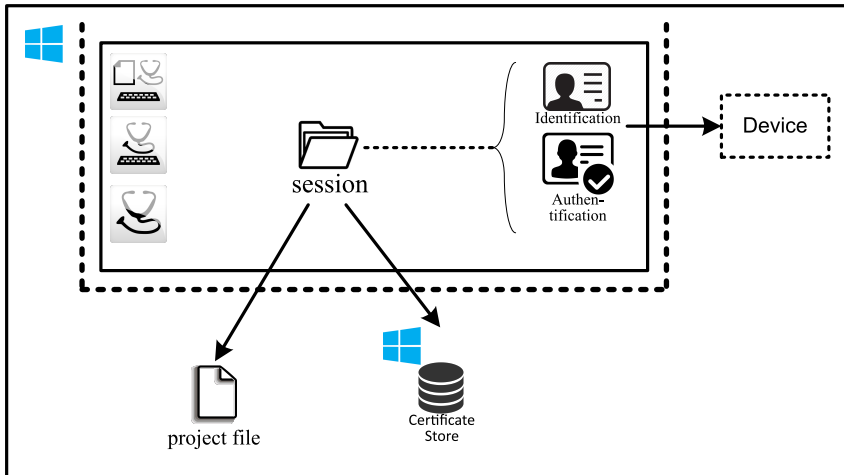
Security key indicator (in accordance with IEC 62443-4-2):

- This software is considered a software application (SAR).
- This component has a security level of SL-C 0.
- This component has an SL-vector from SL-C(EasyStarter)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

## Security mechanisms

### Product Defense in Depth

The following image shows the Defense in Depth product concept. For the sake of clarity, some details have been deliberately omitted.

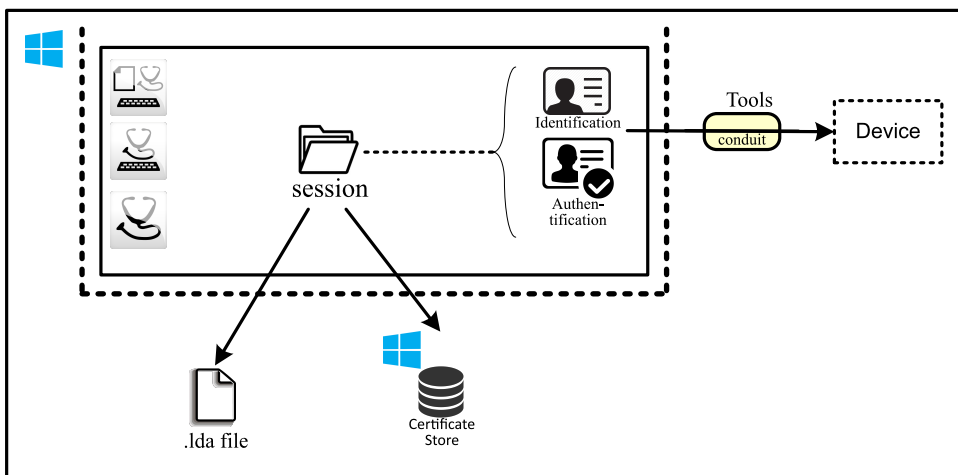


Product Defense in Depth

This EASY Starter software is able to run on a Windows-based host system. The user is responsible for this host system and must establish all relevant security protection mechanisms here or at higher levels.

### Expected Defense in Depth in the environment

The following image shows the Expected Defense in Depth in the environment of the EASY Starter.



Expected Defense in Depth in the environment

#### Conduit Tools:

- Access from the engineering tools to the components must be limited in terms of organization and time.

- 
- The corresponding engineering tool must be operated on an up-to-date and IT-security-secured computer.

#### General Environment:

- General physical access protection must be provided for the components.
- Existing firmware updates for the EASY Starter as well as for all other components in the network should be installed immediately.
- If a WLAN connection is used as the connection path, this is based on the WLAN mechanisms of the underlying Windows. The Windows mechanisms for WLAN configuration must be kept up to date.

#### Security mechanisms

The following security functions are included in the listed components:

- EasyStarter.Authentication
- EasyStarter.Certificate

## Commissioning, hardening and decommissioning notes

The following commissioning instructions must be followed:

#### General instructions

- This software can only be used on a computer with up-to-date IT security.
- Restrict physical and logical access to authorized persons only.
- The EASY Starter is installed on a Windows host. Please ensure that the Windows session lock is activated after a period of inactivity and by manual execution.

#### Commissioning and hardening instructions

- Before installing a tool, the hash value should be checked ([PackageManager.Tool.Integrity](#)).
- Before individual firmware packages are installed, they must be checked for integrity ([PackageManager.Package.Integrity](#)).
- When using the »EASY Starter« that has a controller with activated user management, the human user authentication of the »EASY Starter« must be used ([EasyStarter.Authentication](#)).
- When using the "EASY Starter" with a controller that has forced encrypted communication, the handling of certificates is explained ([EasyStarter.Certificate](#)).

#### Periodic security maintenance

- It is recommended to check the certificates used with regard to their key lengths for up-to-dateness and to generate new certificates with a higher key length if necessary.
- It is recommended to exchange the certificates regularly.

#### Decommissioning instructions

- After uninstalling the »EASY Starter Suite«, please remove the certificates manually from the Windows Certificate Store ([EasyStarter.Certificate](#)).

#### Removal product from environment

- n.a.

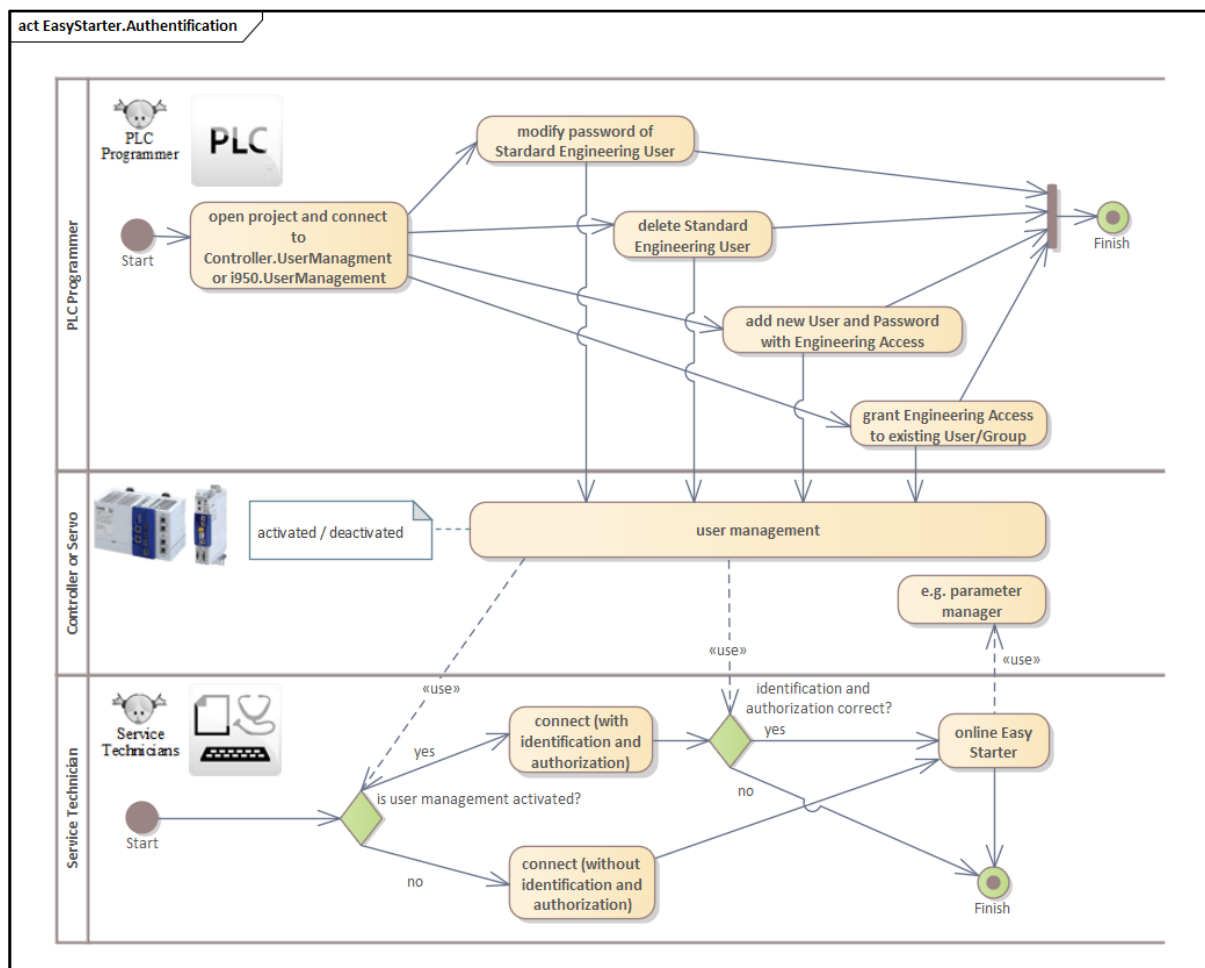
### Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

#### EasyStarter.Authentication

This function is available up to version 01.24.00 of the EASY Starter.

This chapter describes the authentication from the »EASY Starter« while connecting the controller. An overview is shown in the following figure.



EasyStarter.Authentication

#### Connect (with deactivated user management)

If the Controller.UserManagement is deactivated, an »EASY Starter« can connect without prior identification and authentication.

#### Connect (with activated user management)

If the Controller.UserManagement is activated, the user must first identify and authenticate himself via the EASY Starter. This is done via username and password. This occurs when esta-

---

blishing a connection to the controller, but also when the controller establishes a connection to subordinate devices.

### EasyStarter.Certificate

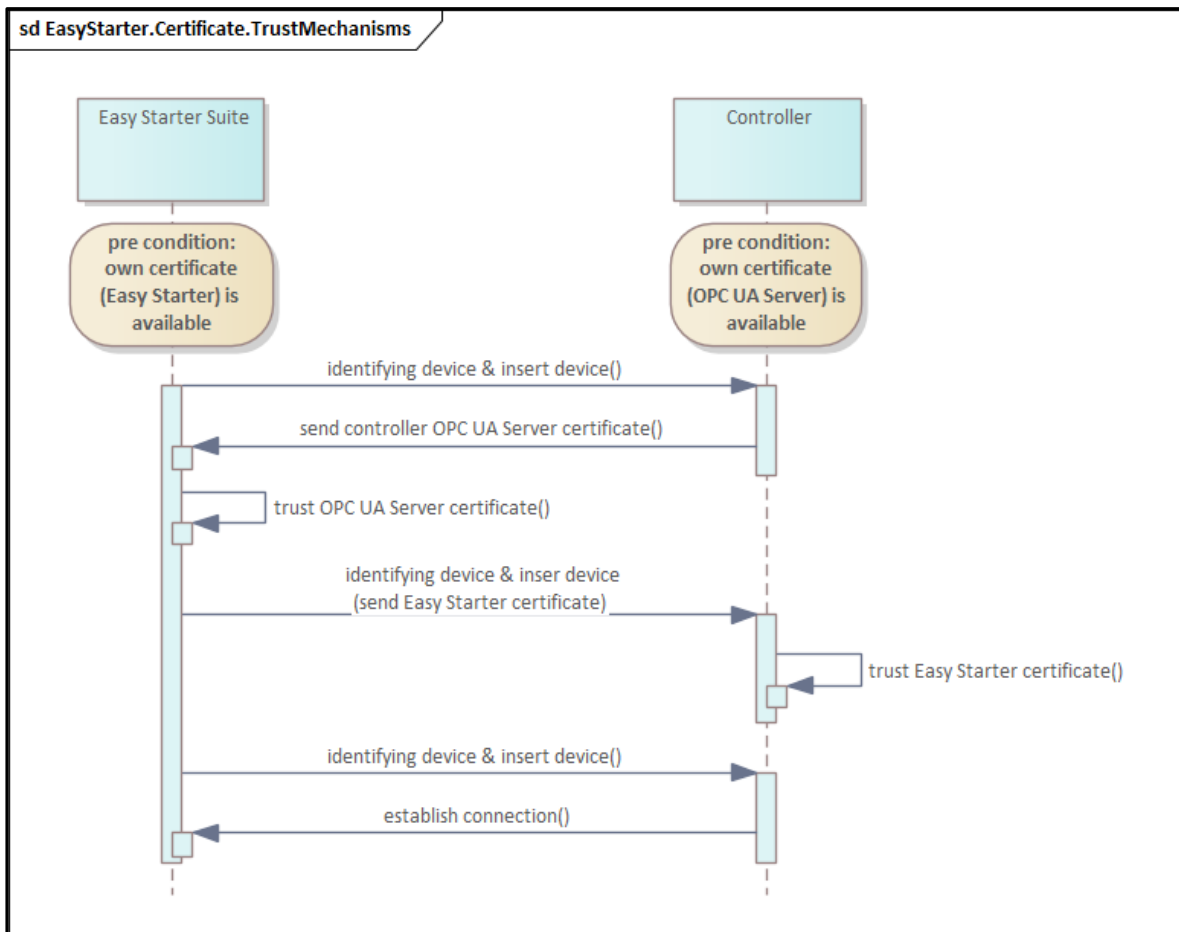
This function has been available since version 01.25.00 of the »EASY Starter Suite«.

First, we will describe when the »EASY Starter Suite« requires certificate handling. This decision does not lie with the »EASY Starter Suite«, but rather with the communication partner, in this context the controller. Furthermore, the behavior is the same for the »EASY Starter«, the »EASY Firmware Loader« and the Application Loader and therefore the term »EASY Starter Suite« is used in the following table.

| Configuration of the Controller                                                                 | Certificate Handling for »EASY Starter« Suite                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Controller.UserManagement<br>( <a href="#">Controller.UserManagement</a> )                      | The Certificate Handling is not dependent on the Controller.UserManagement activation.                                                                                                                                                                                                                                                                                                                                                                          |
| EngineeringItf-User<br>( <a href="#">Controller.UserManagement</a> )                            | The Certificate Handling is not dependent on the existence of the default Engineering User "EngineeringItf".                                                                                                                                                                                                                                                                                                                                                    |
| Anonymous Login<br>( <a href="#">Controller.UserManagement</a> )                                | The Certificate Handling is not dependent on the existence of the activation of the Anonymous Login.                                                                                                                                                                                                                                                                                                                                                            |
| Encrypted Communication<br>( <a href="#">Controller.EncryptedCommunication.PLCDesigner</a> )    | The Certificate Handling is not dependent on the encrypted communication between »PLC Designer« and Controller.                                                                                                                                                                                                                                                                                                                                                 |
| User Enforced Encryption<br>( <a href="#">Controller.EncryptedCommunication.PLCDesigner</a> )   | The Certificate Handling is not dependent on the User "Enforced Encrypted Communication" in the Security Screen of »PLC Designer«.                                                                                                                                                                                                                                                                                                                              |
| Device Enforced Encryption<br>( <a href="#">Controller.EncryptedCommunication.PLCDesigner</a> ) | <p>The Certificate Handling is only dependent on the Device "Enforced Encrypted Communication" in the Security Screen of »PLC Designer«.</p> <p>No encryption:<br/>The »EASY Starter Suite« will not handle certificates for communication.</p> <p>Optional encryption:<br/>The »EASY Starter Suite« will not handle certificates for communication.</p> <p>Enforced encryption:<br/>The »EASY Starter Suite« has to handle certificates for communication.</p> |



In the following, the procedure for mutual trusting is described using the example of a connection setup between the »EASY Starter« and the controller.



Trust Mechanisms

## Handling own certificates

As a prerequisite, the »EASY Starter Suite« and the controller must create their own certificates.

- The »EASY Starter Suite« creates its own certificate automatically during the first connection to the controller. For more information see [EasyStarter.Certificate](#).
- The controller creates its own certificate "Lenze OPC UA Server" automatically at the first boot. For more information, see [Controller.OPCUAServer.Certificate](#).

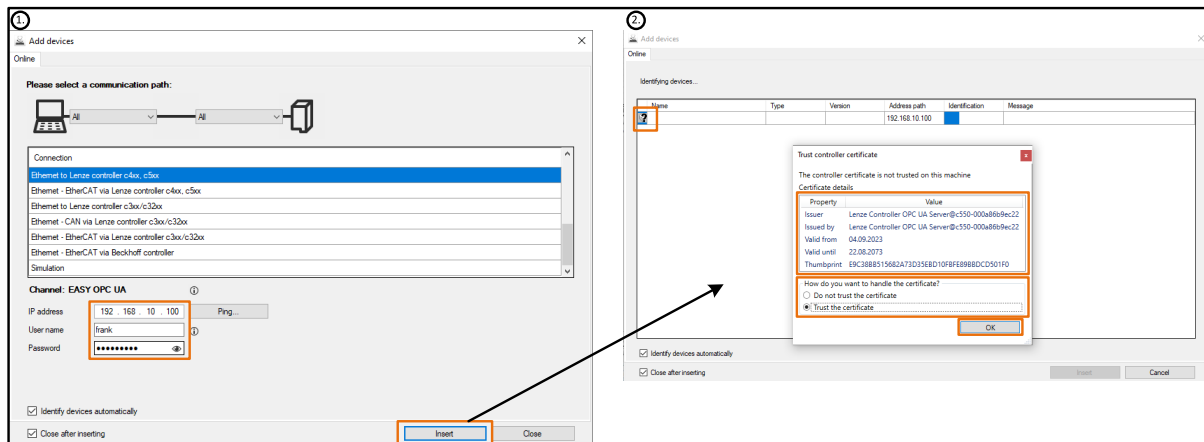
In both cases, the user does not have to take any action. This step does not require any interaction, but is described in order to better understand the function.

# EASY Starter

## Security functions

### First connection and trust Controller Certificate in the »EASY Starter Suite«

A new device can be added to the »EASY Starter« on the basis described above (see the following figure under (1)). To do this, the IP address and, if Controller.UseManagement is activated, the "User name" and the "Password" must be entered. After pressing the Insert button, another window opens where the connection setup is initialized.



Trust Controller Certificate

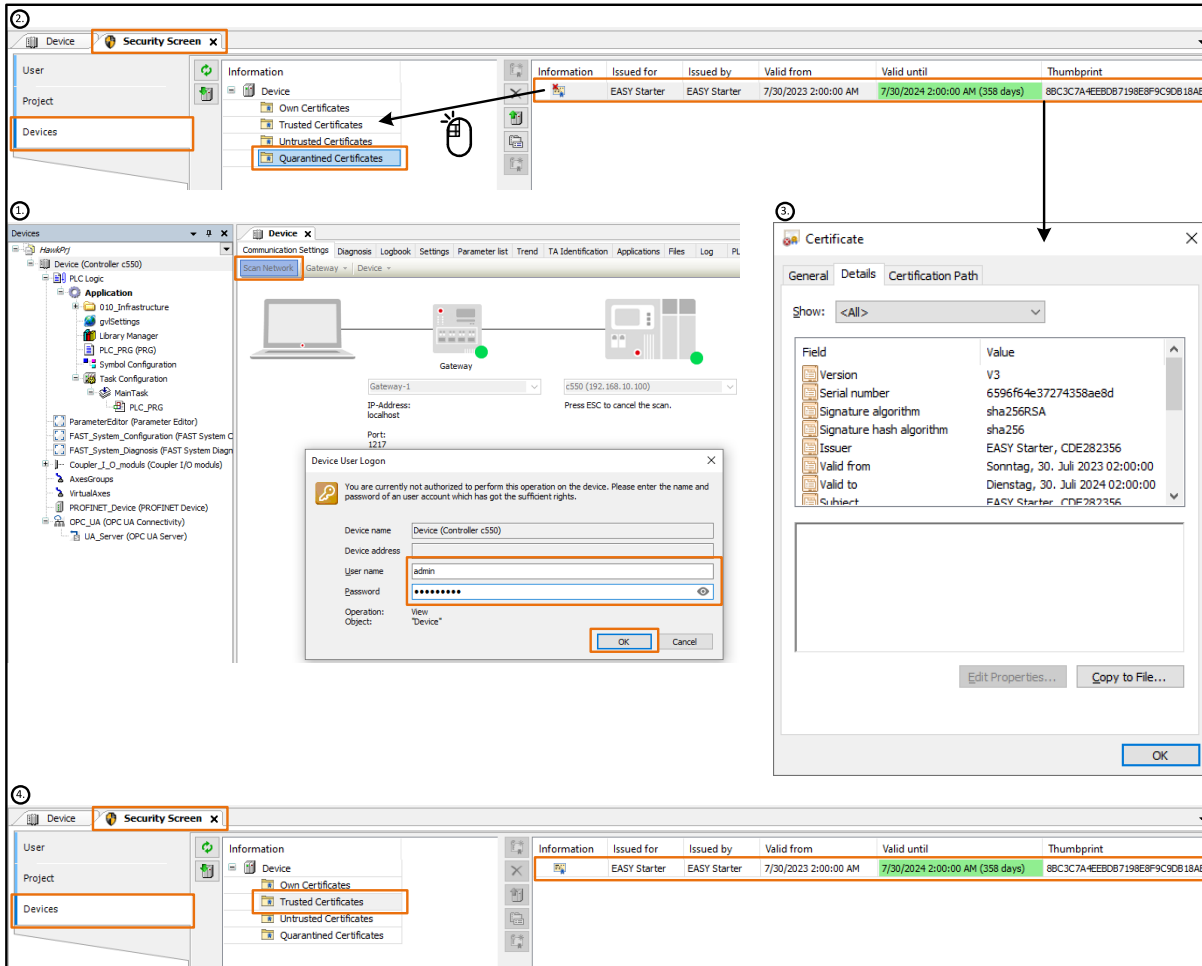
The controller is displayed as a device with its IP address and the connection setup is initialized. The controller's certificate is sent to the »EASY Starter« and displayed in the window with some data for Identification.

The User now has three different options:

- Do not trust the certificate  
The certificate is not trusted and the connection is terminated. At the same time, the certificate is stored in the Windows Certificate Store under "\\Untrusted Certificates\\Certificates" so that when a connection is established again, it is immediately recognized that this certificate is not trusted.
- Trust the certificate  
The certificate is trusted and the connection is further established. At the same time, the certificate is stored in the Windows Certificate Store under "\\Controller Certificates\\Certificates" so that when a connection is established again, it is immediately recognized that this certificate is trusted.
- Close the window  
The certificate is not trusted and the connection is terminated. At the same time, the certificate is stored in the Windows Certificate Store under "\\Untrusted Certificates\\Certificates" so that when a connection is established again, it is immediately recognized that this certificate is not trusted.

## Trust »EASY Starter« Certificate in the »PLC Designer« (Commissioning Use Case)

In the commissioning phase of the machine, the programmer has to start the »PLC Designer«, connect to the controller and trust the certificate from the EASY Starter.



Trust »EASY Starter« Certificate

The following steps must be carried out here:

1. With the help of the »PLC Designer«, a "Scan Network" must be carried out and if the Controller.UserManagement is activated, the "User name" and the "Password" must be entered.
2. After the connection has been established, open the security screen and open the "Devices" tab. After synchronization, the certificates can be viewed. The »EASY Starter« certificate is located in the "Quarantined Certificates" directory.
3. For better identification, the certificate can be opened with a double click and details can be viewed.
4. The certificate can be moved from "Quarantined Certificates" to "Trusted Certificates" using drag-and-drop.

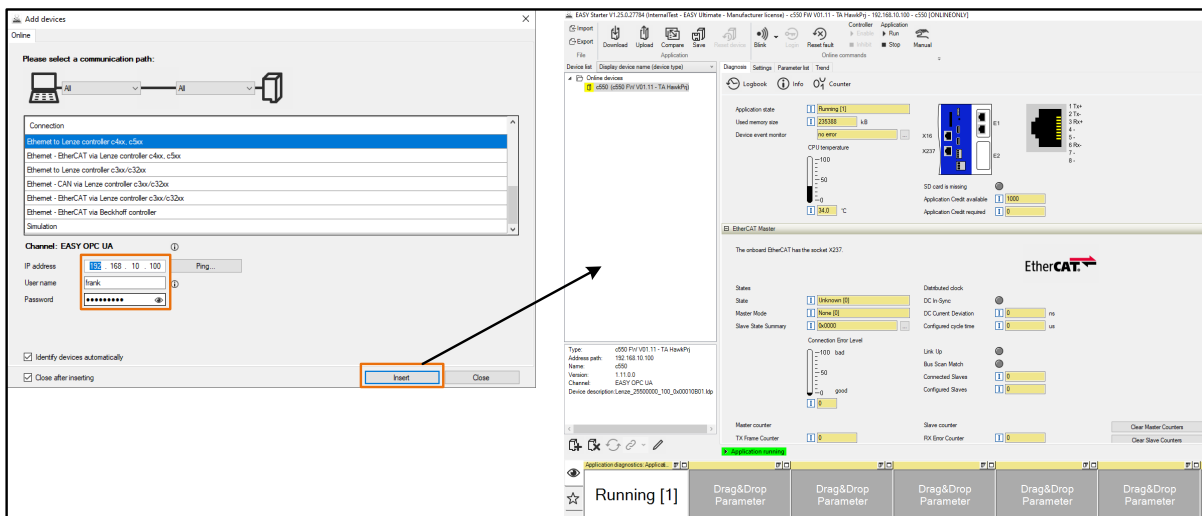
This completes the trust of the »EASY Starter« certificate.

### Trust »EASY Starter« Certificate in the Advanced Visualization (Production Use Case)

The connection of the »EASY Starter« in production is the same in the Production as in commissioning. The only difference here is that the »PLC Designer« cannot be used by the controller for trust, since the operator usually does not have the »PLC Designer« project. For this use case, a Certificate Handler was developed as part of the web visualization of the controller. With the help of this mechanism, the certificate can be trusted for the »EASY Starter« ([Controller.CertificateStore.viaAdvancedVisu](#)).

### Establish Connection

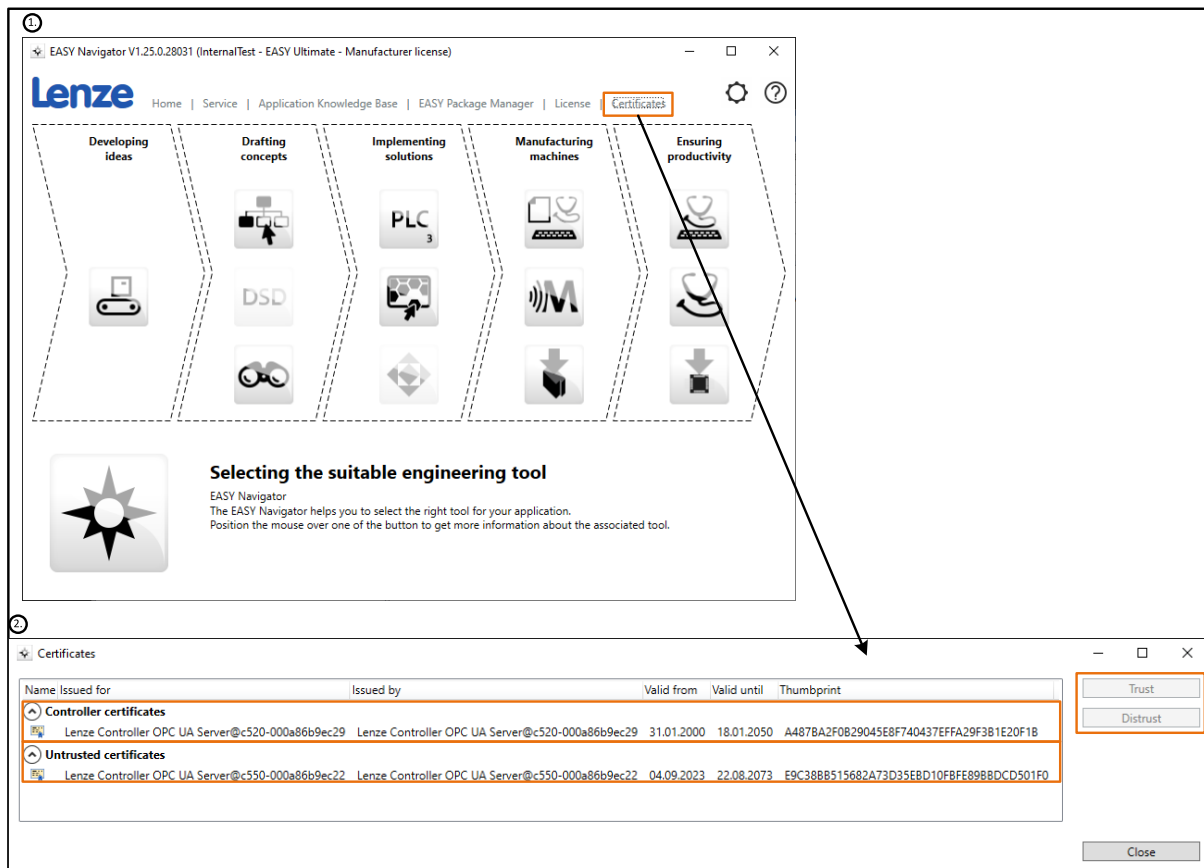
After trusting the certificates on both sides, the user can insert the controller into the »EASY Starter« and go online.



Establish Connection

### Handling existing certificates in the »EASY Starter Suite«

In order to handle the existing certificates, it is possible to call up an overview in the »EASY Navigator« under the link "Certificates".



Handling existing Certificates

A window opens here that shows all trusted and untrusted certificates. In addition to displaying information, two actions can be performed:

- When selecting an untrusted Certificate, the user can trust this certificate.
- When selecting an trusted Certificate, the user can untrust this certificate.

## EasyStarter Security Functionality Verification

The user management has to be activated. Establishing a connection with the EasyStarter without usage of the correct name and password is not possible.

To use an encrypted communication, the EasyStarter uses a certificate which is located in the trust folder of the PLC Designer or the certificate has been trusted with the EASY Starter Suite. To test the security functionality, move the certificate to the untrusted folder of the PLC Designer or untrust the certificate with the EASY Starter Suite.

## Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

### EasyStarter.AccountManagementGuidelines

The EASY Starter has no user management, and for this reason no account management guidelines need to be considered.

### EasyStarter.Certificate

When using encrypted communication, the EASY Starter Suite stores its own certificate and the controller certificates for encrypted communication in the Windows Certificate Store.

The EASY Starter Suite certificate is stored in the Windows Certificate Store in the "Personal/Certificates" directory with the following information:

- Issuer and Subject  
CN = urn:<Device name>:Lenze:EASYStarter  
<Device name> is the Device name of the Windows System.
- Valid from  
Today minus 2 days. Therefore, the certificate will certainly be valid in different time zones when maintenance or repair work is critical.
- Valid to  
The Certificate is valid for 1 year.

The controller certificate will also be stored in the Windows Certificate Store in the "Controller Certificates/Certificates" directory.



All these certificates will not be deleted during deinstallation of the »EASY Starter Suite«. After deinstallation of the »EASY Starter Suite«, these data must be removed manually from the user. For more information, please have a look at [Integrate a certificate in the windows certificate store](#).

## EASY Firmware Loader

### Product description

#### Product identification

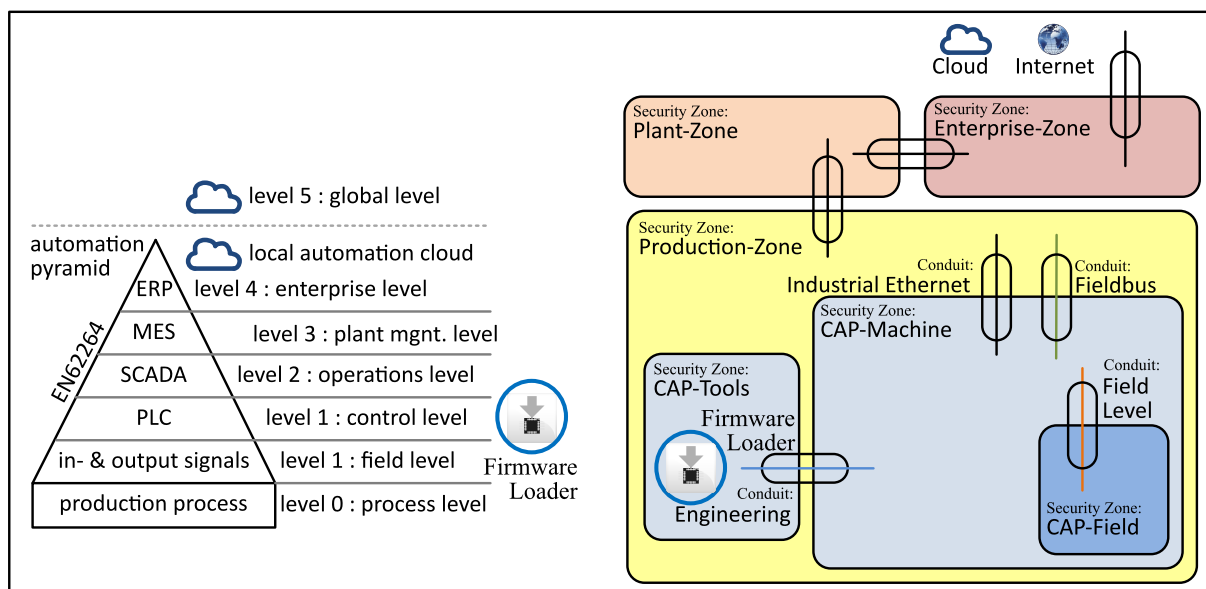
This documentation applies to the following components with their identification:

Name of product and product ID

| Name of product                                              | Product ID |
|--------------------------------------------------------------|------------|
| »EASY Firmware Loader«<br>(part of the »EASY Starter Suite«) | n.a.       |

#### Location in the network

This component is located in the automation pyramid at the control level. Furthermore, they are located in the security zone "CAP-Tools" ([Zones and Conduits](#)).



Product location in the network

The software addressed here has only one relevant interface:

- Conduit: Engineering  
This connection is used to connect the tool to the Security Zone CAP-Machine.

#### Intended purpose

The intended user of this component is described in the application as directed and can be found in the operation instructions in the online help. In the following, some specifics regarding cyber security are discussed.

- This component mentioned here is professional software and may only be commissioned and decommissioned by specialists.
- This software also requires maintenance throughout its life cycle, which must be carried out by the operator.

# EASY Firmware Loader

## Security mechanisms

- Modifications to the software are not permitted.
- If this software is taken out of operation or disposed of, the instructions in the documentation must be observed.

### Intended environment

The intended environment for this software is described in the application as directed and can be found in the online help. In the following, some specifics regarding cyber security are discussed:

- The software must be installed on an up-to-date computer equipped with valid IT protection mechanisms.
- The software must be installed on a computer which uses protection against unauthorized use.
- Use appropriate authentication mechanisms for the computer. This includes passwords that have the necessary complexity and an appropriate life cycle. The current state of the art must be taken into account here.
- This computer is the responsibility of its owner and must be protected by valid IT protection systems such as firewall, IDS, IPS, etc.

### Security key indicators

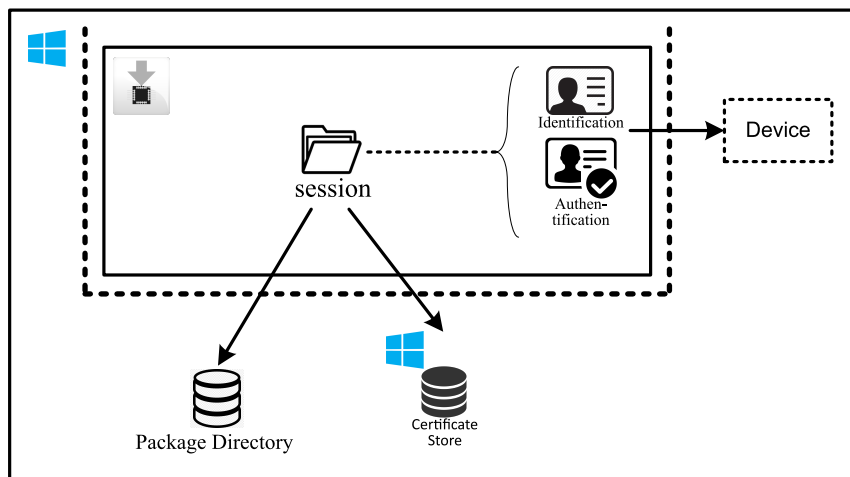
Security key indicator (in accordance with IEC 62443-4-2):

- This software is considered a software application (SAR).
- These components have a security level of SL-C 0.
- These components have an SL-vector from SL-C(FirmwareLoader)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

## Security mechanisms

### Product Defense in Depth

The following image shows the Defense in Depth product concept. For the sake of clarity, some details have been deliberately omitted.



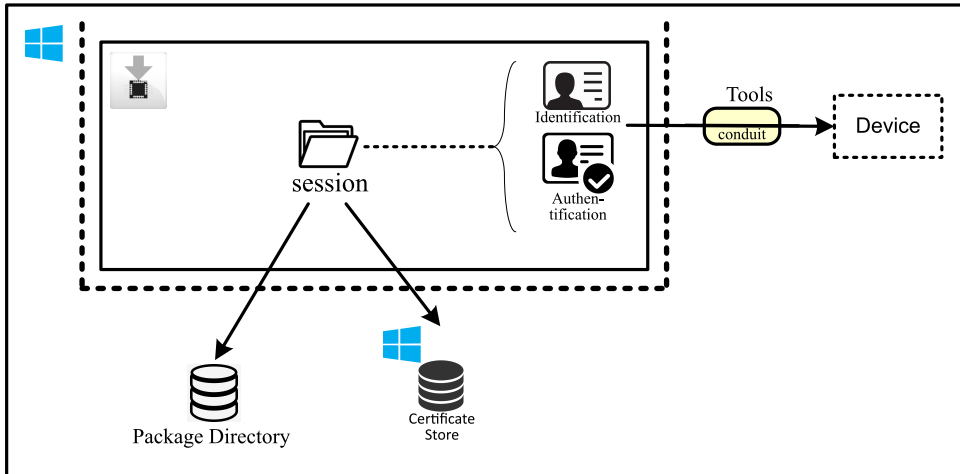
Product Defense in Depth

This EASY Firmware Loader software is able to run on a Windows-based host system. The user is responsible for this host system and must establish all relevant security protection mechanisms here or at higher levels.



## Expected Defense in Depth in the environment

The following image shows the Expected Defense in Depth in the environment of the EASY Firmware Loader.



Expected Defense in Depth in the environment

### Conduit Tools:

- Access from the engineering tools to the components must be limited in terms of organization and time.
- The corresponding engineering tool must be operated on an up-to-date and IT-security-secured computer.

### General Environment:

- General physical access protection must be provided for the components.
- Existing firmware updates for the EASY Firmware Loader as well as for all other components in the network should be installed immediately.
- If a WLAN connection is used as the connection path, this is based on the WLAN mechanisms of the underlying Windows. The Windows mechanisms for WLAN configuration must be kept up to date.

## Security mechanisms

- FirmwareLoader.Authentication
- FirmwareLoader.Certificate

## Commissioning and hardening instructions

The following commissioning instructions must be followed:

### General instructions

- This software can only be used on a computer with up-to-date IT security.
- Restrict physical and logical access to authorized persons only.
- The EASY Firmware Loader is installed on a Windows host. Please ensure that the Windows session lock is activated after a period of inactivity and by manual execution.

# EASY Firmware Loader

## Commissioning and hardening instructions

---

### Commissioning and hardening instructions

- Before installing a tool, the hash value should be checked ([PackageManager.Tool.Integrity](#)).
- Before individual firmware packages are installed, they must be checked for integrity ([PackageManager.Package.Integrity](#)).
- When using the »EASY Firmware Loader« with a controller that has activated user management, the human user authentication of the »EASY Firmware Loader« must be used ([FirmwareLoader.Authentication](#)).
- When using the »EASY Firmware Loader« that has a controller with forced encrypted communication, the handling of the certificates is explained ([FirmwareLoader.Certificate](#)).
- If the »EASY Firmware Loader« is controlled via batch mode, the credentials must be passed to the respective devices. This is done via a control file. The access data AuthenticateUser and AuthenticatePassword are given here in plain text. In this respect, increased attention must be given to the procedure of these files, and the user must ensure their confidentiality organizationally.

#### Example:

- [DEVICE004]
- NodeAddress=Lenze OPC ADS Ethercat Server.1003
- IP=172\_20\_102\_56
- NetId=172\_31\_203\_220\_2\_1
- AuthenticateUser=<TestUser>
- AuthenticatePassword=<TestPassword>
- FirmwareFileSet="C:\file"

### Periodic security maintenance

- It is recommended to check the certificates used with regard to their key lengths for up-to-dateness and to generate new certificates with a higher key length if necessary.
- It is recommended to exchange the certificates regularly.

### Decommissioning instructions

- After uninstalling the EASY Firmware Loader, please check the Windows Certificate Store for certificates that are no longer required and remove them.

### Removal product from environment

- n.a.

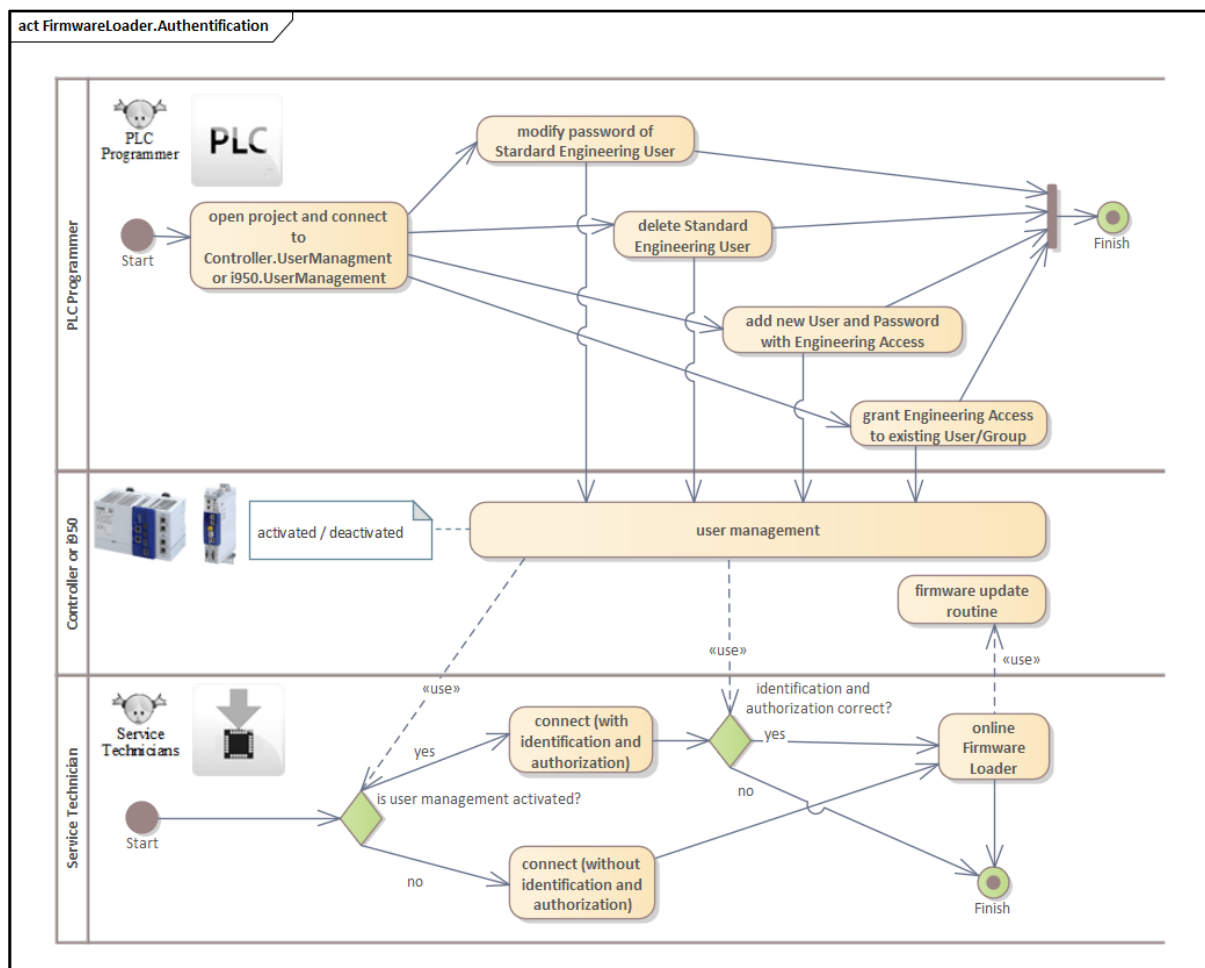
## Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

### FirmwareLoader.Authentication

This function has been available since »EASY Firmware Loader« version 01.24.00.

This chapter describes the authentication from the »EASY Firmware Loader« while connecting the controller. An overview is shown in the following figure.



Activity Diagram

#### Connect (with deactivated user management)

If the Controller.UserManagement is deactivated, the Firmware Loader can connect without prior identification and authentication.

#### Connect (with activated user management)

If the Controller.UserManagement is activated, the user must first identify and authenticate himself via the Firmware Loader. This is done via username and password. This occurs when

# EASY Firmware Loader

## Security functions

---

establishing a connection to the controller, but also when the controller establishes a connection to subordinate devices.

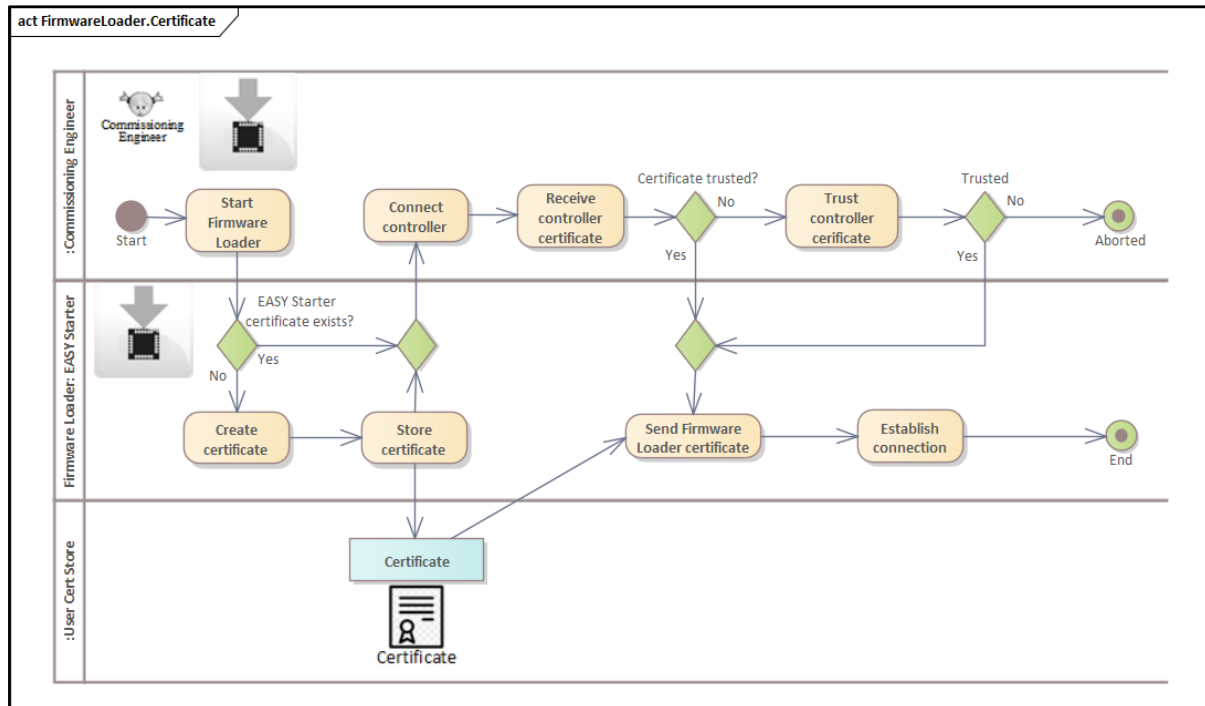
### Using the firmware-loader in batchmode

The firmware loader has a batch mode. This can be used to automatically update several devices with a new firmware. In this batch file, the authentication features, i.e. username and password, can be specified for establishing the connection. This file must be organizationally protected, as the passwords are contained here in plain text.

## FirmwareLoader.Certificate

This function has been available since Firmware Loader version 01.25.00.

The certificate handling of the Firmware Loader is the same as the certificate handling of the »EASY Starter« ([EasyStarter.Certificate](#)).



Activity Diagram

## Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

### FirmwareLoader.AccountManagementGuidelines

The EASY Firmware Loader has no user management, and for this reason no account management guidelines need to be considered.

EASY Application Loader

Product description

Product identification

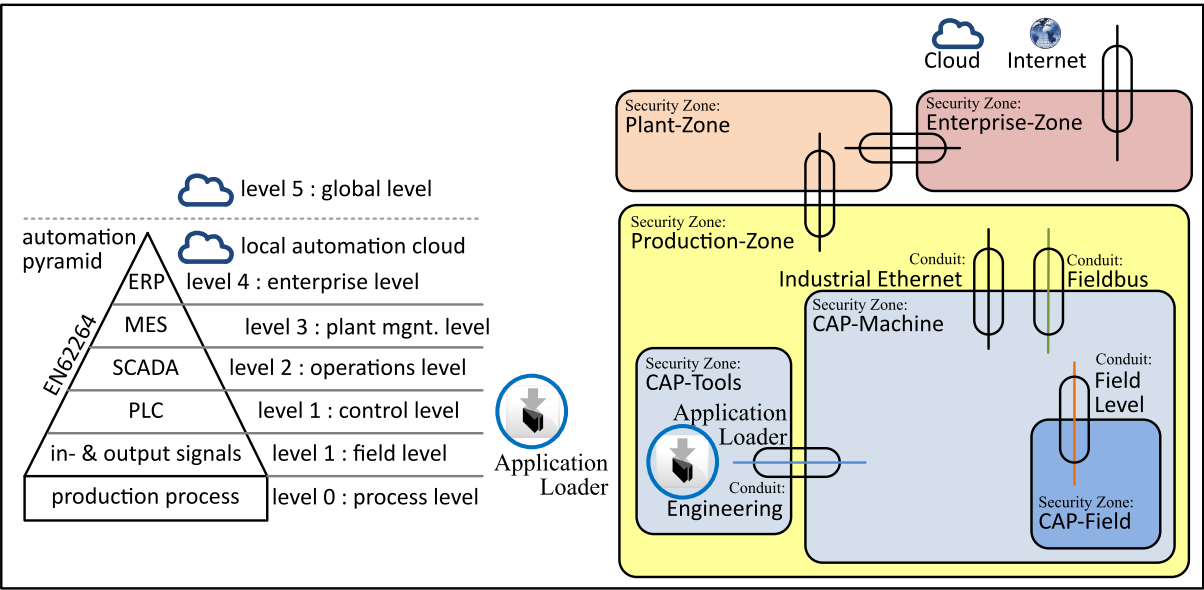
This documentation applies to the following components with their identification:

Name of product and product ID

| Name of product                                                 | Product ID |
|-----------------------------------------------------------------|------------|
| »EASY Application Loader«<br>(part of the »EASY Starter Suite«) | n.a.       |

Location in the network

This component is located in the automation pyramid at the control level. Furthermore, they are located in the security zone "CAP-Tools" ([Zones and Conduits](#)).



Product location in the network

The software addressed here has only one relevant interface:

- Conduit: Engineering  
This connection is used to connect the tool to the Security Zone CAP-Machine.

Intended purpose

The intended user of this component is described in the application as directed and can be found in the operation instructions in the online help. In the following, some specifics regarding cyber security are discussed.

- This component mentioned here is professional software and may only be commissioned and decommissioned by specialists.
- This software also requires maintenance throughout its life cycle, which must be carried out by the operator.

- Modifications to the software are not permitted.
- If this software is taken out of operation or disposed of, the instructions in the documentation must be observed.

## Intended environment

The intended environment for this software is described in the application as directed and can be found in the online help. In the following, some specifics regarding cyber security are discussed:

- The software must be installed on an up-to-date computer equipped with valid IT protection mechanisms.
- The software must be installed on a computer, which uses protection against unauthorized use.
- Use appropriate authentication mechanisms for the computer. This includes passwords that have the necessary complexity and an appropriate life cycle. The current state of the art must be taken into account here.
- This computer is the responsibility of its owner and must be protected by valid IT protection systems such as firewall, IDS, IPS, etc.

## Security key indicators

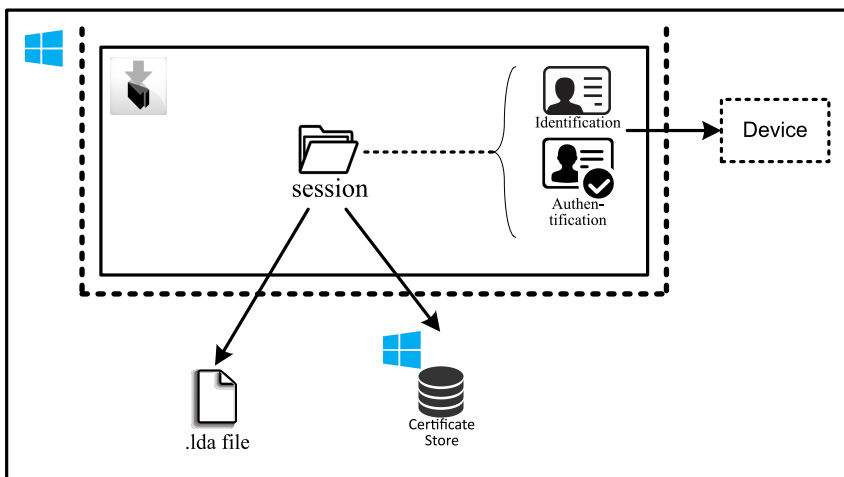
Security key indicator (in accordance with IEC 62443-4-2):

- These software are considered software application (SAR).
- These components have a security level of SL-C 0.
- These components have an SL-vector from SL-C(ApplicationLoader)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

## Security mechanisms

### Product Defence in Depth

The following image shows the Defence in Depth product concept. For the sake of clarity, some details have been deliberately omitted.



Product Defence in Depth

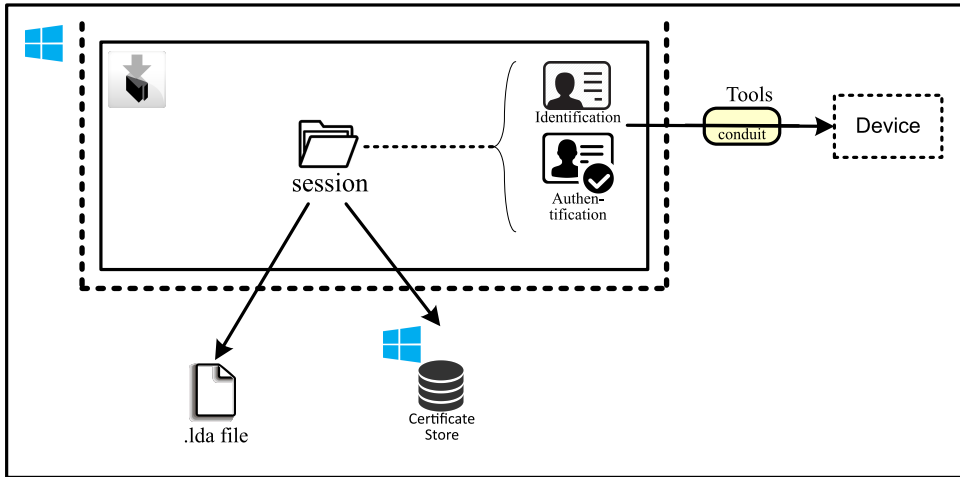
This EASY Application Loader software is able to run on a Windows-based host system. This host system is the responsibility of the user and all relevant security protection mechanisms must be established here or at higher levels.

# EASY Application Loader

## Commissioning and hardening instructions

### Expected Defense in Depth in the environment

The following image shows the Expected Defense in Depth in the environment of the EASY Application Loader.



Expected Defense in Depth in the environment

#### Conduit Tools:

- Access from the engineering tools to the components must be limited in terms of organization and time.
- The corresponding engineering tool must be operated on an up-to-date and IT-security-secured computer.

#### General Environment:

- General physical access protection must be provided for the components.
- Existing firmware updates for the EASY Application Loader as well as for all other components in the network should be installed immediately.
- If a WLAN connection is used as the connection path, this is based on the WLAN mechanisms of the underlying Windows. The Windows mechanisms for WLAN configuration must be kept up to date.

### Security mechanisms

- ApplicationLoader.Authentication
- ApplicationLoader.Certificate

## Commissioning and hardening instructions

The following commissioning instructions must be followed:

### General instructions

- This software can only be used on a computer with up-to-date IT security.
- Restrict physical and logical access to authorized persons only.
- The EASY Application Loader is installed on a Windows host. Please ensure that the Windows session lock is activated after a period of inactivity and by manual execution.



## Commissioning and hardening instructions

- Before installing a tool, the hash value should be checked ([PackageManager.Tool.Integrity](#)).
- Before individual firmware packages are installed, they must be checked for integrity ([PackageManager.Package.Integrity](#)).
- If using the »EASY Application Loader« with a controller with activated user management, the human user authentication of the »EASY Application Loader« has to be use ([ApplicationLoader.Authentication](#)).
- When using the »EASY Application Loader« with a controller that has forced encrypted communication the handling of the certificates are explained ([App-licationLoader.Certificate](#)).
- When the »EASY Application Loader« is controlled via batch mode, the credentials must be passed to the respective devices. This is done via a control file. The access data AuthenticateUser and AuthenticatePassword are given here in plain text. In this respect, increased attention must be given to the procedure of these files, and the user must ensure their confidentiality organizationally.

### Example:

- [DEVICE004]
- NodeAddress=Lenze OPC ADS Ethercat Server.1003
- IP=172\_20\_102\_56
- NetId=172\_31\_203\_220\_2\_1
- AuthenticateUser=<TestUser>
- AuthenticatePassword=<TestPassword>
- FirmwareFileSet="C:\file"

## Periodic security maintenance

- It is recommended to check the certificates used with regard to their key lengths for up-to-dateness and to generate new certificates with a higher key length if necessary.
- It is recommended to exchange the certificates regularly.

## Decommissioning instructions

- After uninstalling the EASY Firmware Loader, please check the Windows Certificate Store for certificates that are no longer required and remove them.

## Removal product from environment

- n.a.

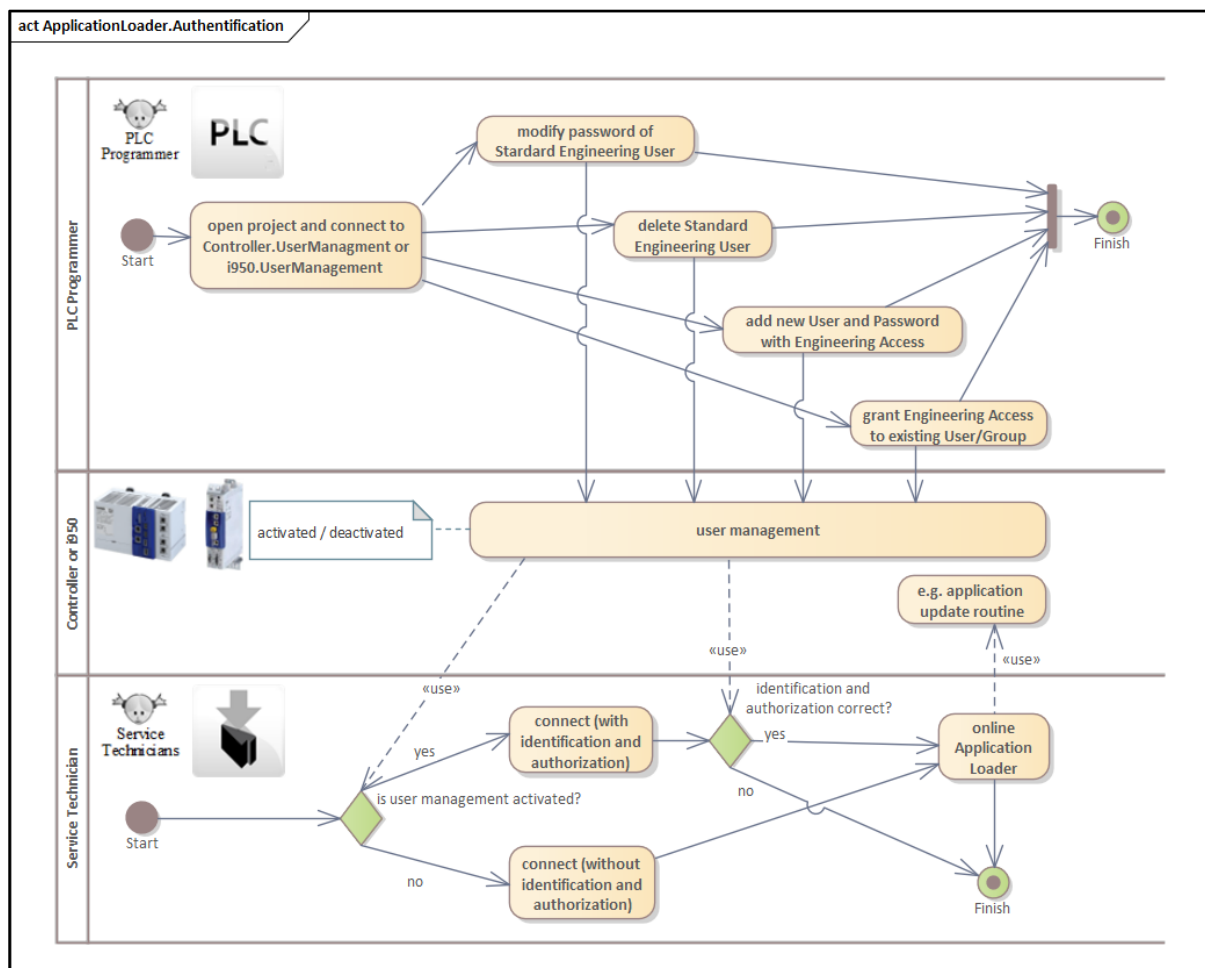
### Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

#### ApplicationLoader.Authentication

This function has been available since »EASY Application Loader« version 01.24.00.

This chapter describes the authentication from the »EASY Application Loader« while connecting the controller. An overview is shown in the following figure.



Activity Diagram

#### Connect (with deactivated user management)

If the Controller.UserManagement is deactivated, the »EASY Application Loader« can connect without prior identification and authentication.

#### Connect (with activated user management)

If the Controller.UserManagement is activated, the user must first identify and authenticate himself via the Application Loader. This is done via username and password. This occurs done

---

when establishing a connection to the controller, but also when the controller establishes a connection to subordinate devices.



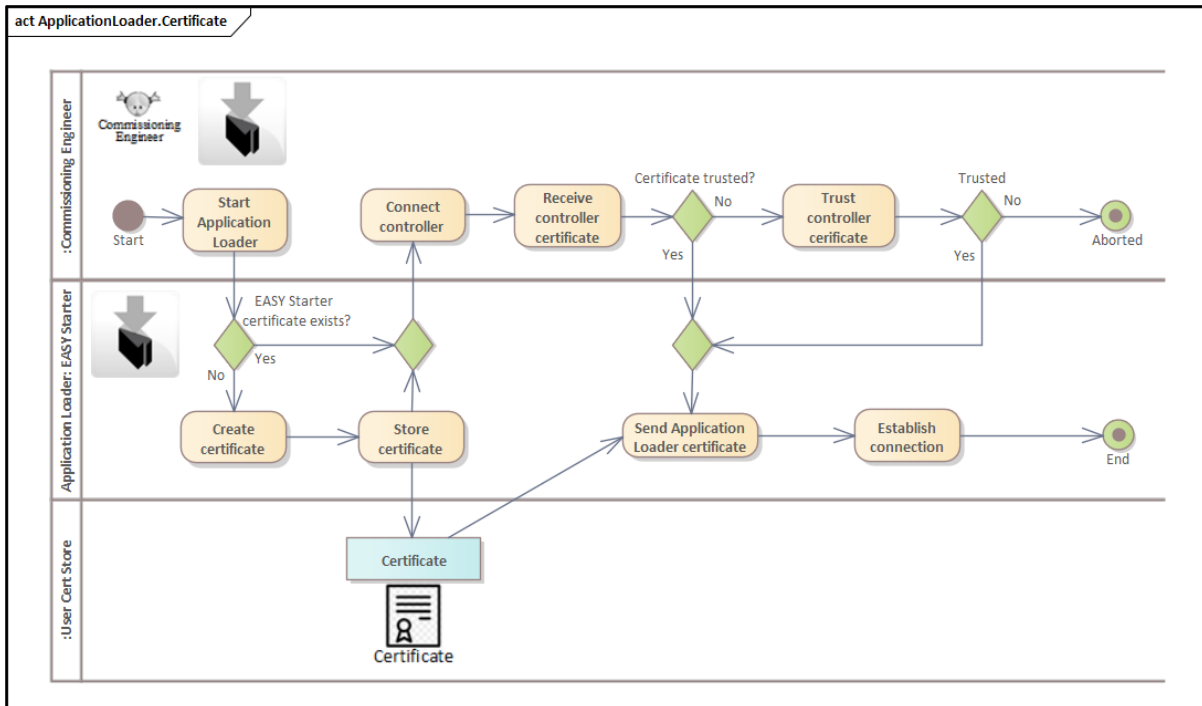
An application can be created with the help of the »PLC Designer«. For this purpose, the entry "EASY Export..." is displayed in the menu under "Project". and created a "Complete device application \*.lda". It is important to know that the Controller.UserManagement is not part of the dla. file. This has security-related reasons.

If, in a second step, a connection is established with the help of the »EASY Application Loader« to a controller that has an active Controller.UserManagement, it must first authenticate itself. After successful authentication, the application can be written to the controller. When the application is written, the contents of the Controller.UserManagement except the Controller.UserManagement are deleted. Thus, the user management remains even after a download with the »EASY Application Loader«.

## ApplicationLoader.Certificate

This function has been available since »EASY Application Loader« version 01.25.00.

The certificate handling of the »EASY Application Loader« is the same as the certificate handling of the »EASY Starter« ([EasyStarter.Certificate](#)).



Activity Diagram

## Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

### ApplicationLoader.AccountManagementGuidelines

The EASY Application Loader has no user management, and for this reason no account management guidelines need to be considered.

EASY Package Manager

Product description

Product identification

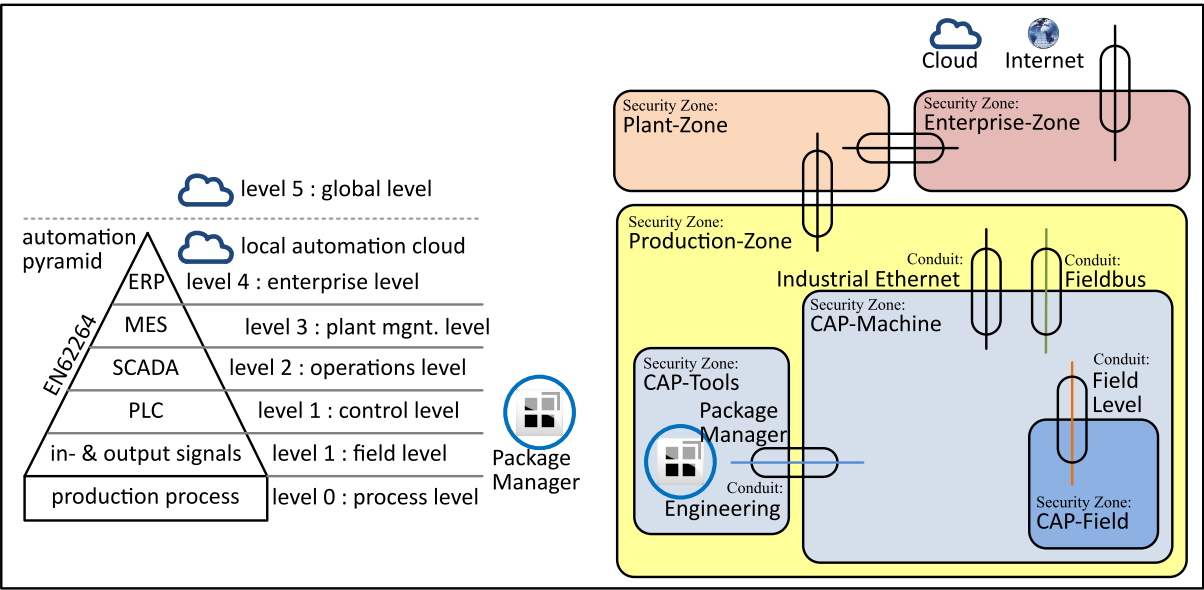
This documentation applies to the following component with its identification:

Name of product and product ID

| Name of product                                              | Product ID |
|--------------------------------------------------------------|------------|
| »EASY Package Manager«<br>(part of the »EASY Starter Suite«) | n.a.       |

Location in the network

This component is located in the automation pyramid at the control level. Furthermore, they are located in the security zone "CAP-Tools" ([Zones and Conduits](#)).



Product location in the network

The software addressed here has only one relevant interface:

- Connection through the Production-, Plant- and Enterprise-Zone to the Internet:  
This connection is used to search for and load new packages.

Intended purpose

The intended user of this component is described in the application as directed and can be found in the operation instructions in the online help. In the following, some specifics regarding cyber security are discussed.

- This component mentioned here is professional software and may only be commissioned and decommissioned by specialists.
- This software also requires maintenance throughout its life cycle, which must be carried out by the operator.

- Modifications to the software are not permitted.
- If this software is taken out of operation or disposed of, the instructions in the documentation must be observed.

## Intended environment

The intended environment for this software is described in the application as directed and can be found in the online help. In the following, some specifics regarding cyber security are discussed:

- The software must be installed on an up-to-date computer equipped with valid IT protection mechanisms.
- The software must be installed on a computer, which uses protection against unauthorized use.
- Use appropriate authentication mechanisms for the computer. This includes passwords that have the necessary complexity and an appropriate life cycle. The current state of the art must be taken into account here.
- This computer is the responsibility of its owner and must be protected by valid IT protection systems such as firewall, IDS, IPS, etc.

## Security key indicators

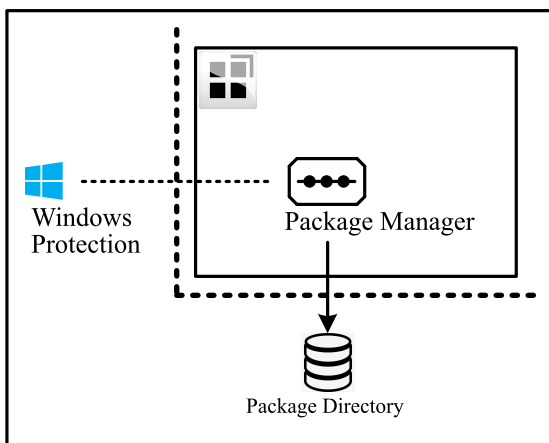
Security key indicator (in accordance with IEC 62443-4-2):

- This software is considered a software application (SAR).
- These components have a security level of SL-C 0.
- These components have an SL-vector from SL-C(PackageManager)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

## Security mechanisms

### Product Defense in Depth

The following image shows the Defense in Depth product concept. For the sake of clarity, some details have been deliberately omitted.



Product Defense in Depth

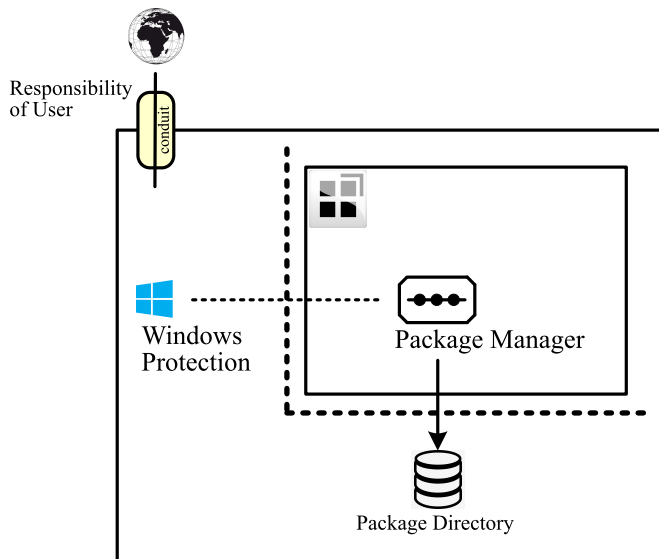
This Package Manager software is able to run on a Windows-based host system. The user is responsible for this host system and must establish all relevant security protection mechanisms here or at higher levels.

# EASY Package Manager

Commissioning and hardening notes and organizational measures

## Expected Defense in Depth in the environment

The following image shows the Expected Defense in Depth in the environment of the EASY Package Manager.



This Package Manager software is able to run on an windows based host system. This host system is in responsibility of the user and all relevant security protection mechanisms must be established here or at higher levels.

Access protection is necessary for both the online connection and the protection of data in the Package Directory.

## Security mechanisms

The following security functions are included in the listed components:

- PackageManager.Tool.Integrity
- PackageManager.Package.Integrity

## Commissioning and hardening notes and organizational measures

The following commissioning instructions must be followed:

### General instructions

- This software can only be used on a computer with up-to-date IT security.
- Restrict physical and logical access to authorized persons only.

### Commissioning and hardening instructions

- Before installing a tool, the hash value should be checked ([PackageManager.Tool.Integrity](#)).
- Before individual firmware packages are installed, they must be checked for integrity ([PackageManager.Package.Integrity](#)).

### Periodic security maintenance

- n.a.



---

## Decommissioning instructions

- n.a.

## Removal of product from environment

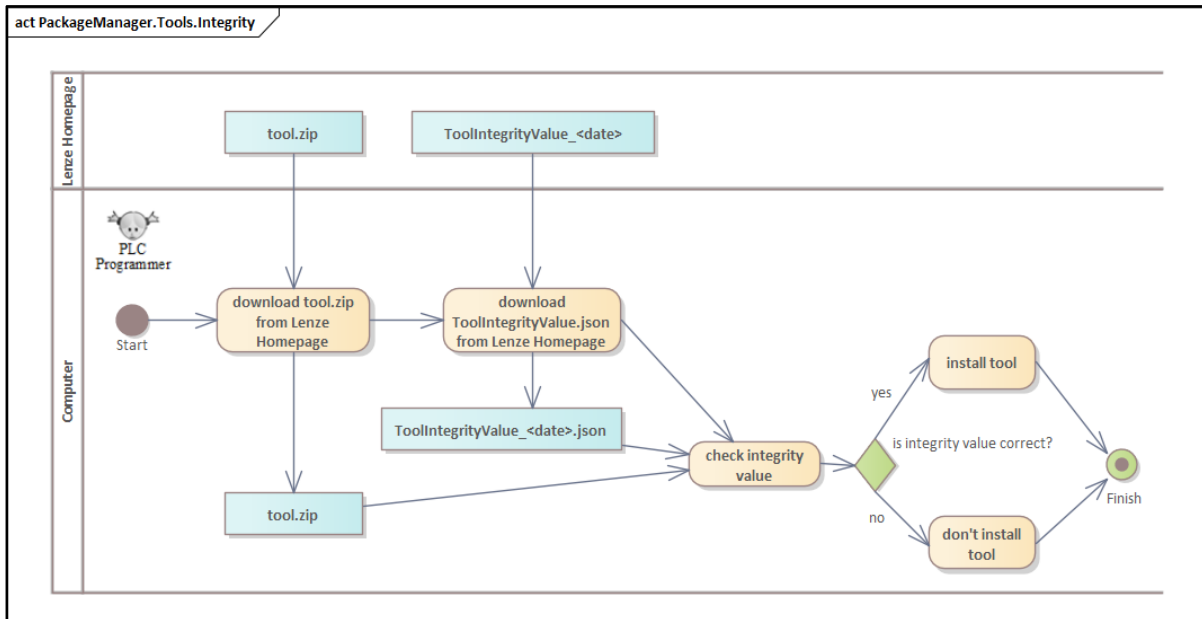
- n.a.

### Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

#### PackageManager.Tool.Integrity

To check the integrity of a tool before installation, it can be downloaded as a zip file from the Lenze homepage. A second file can be used to check the integrity.



Activity Diagram

The following two options are available here.

- First, an integrity file exists at the tool's download location. This file contains the integrity value of this exact version of the tool. This option is ideal for those who want to install a tool individually.
- Secondly, there is an integrity file containing all tools and versions released so far. This can be found under:

<https://www.lenze.com/en-de/services/cyber-security>

All health values are included here. This option is ideal for those who want to check several tools in different versions, possibly even by automatism. These users do not have to download various integrity files, only the latest version of the sum file is sufficient.

Regardless of whether the single file or the sum file was downloaded, a zip file is created. Unpacking this zip file results in three files. These are a \*.csv, a \*.json, and a \*.xml. All three files contain the same content, that is, the same integrity values, and only differ in format.

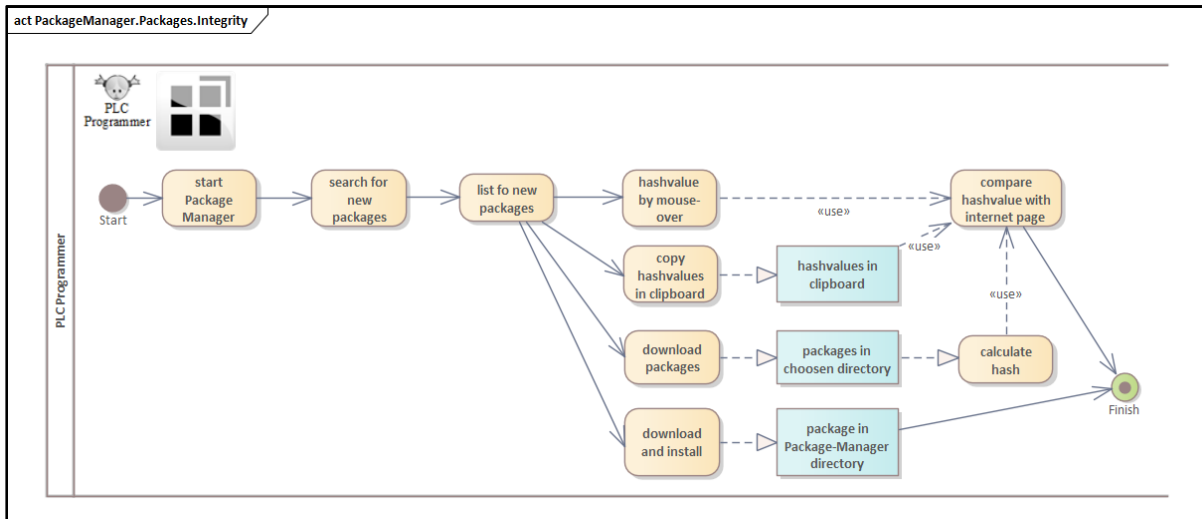


One way to calculate the integrity value of a file is shown in this documentation. Refer to chapter "[Strategy and Basics\Integrity\Validate Integrity](#)".

## PackageManager.Package.Integrity

This functionality has been integrated since version 01.24.00.

This chapter describes the integrity procedure of the firmware packages. A sequence can be found in the following picture.



Activity Diagram

After starting the Package Manager, you can search for new packages. The result is a list of all new packages that have not yet been installed. The following functions can be performed on this list.

A list of the hash values associated with the packages can be found on the website via the link <https://www.lenze.com/en-de/services/cyber-security>

### Hash value by mouse-over

On the list of packages, the hash value can be displayed with a mouse-over. This value can then be manually compared with the published hash values.

### Copy hash values to clipboard

Via the button "Copy hash values to clipboard" the hash values of the selected packages can be transferred to the clipboard. These values can then be manually compared with the published hash values.

### Download packages

With this function, the selected packages are written to a directory to be selected. An installation does not yet take place. These loaded packages can be manually checked for integrity by calculating the hash value and menu. This function installs the packages directly and compares them with the published hash values.

### Download and install

This function installs the packages directly.

### Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

#### **PackageManager.AccountManagementGuidelines**

The EASY Package Manager has no user management, and for this reason no account management guidelines need to be considered.

#### **PackageManager.FirmwarePackage.Integrity: Hash Function**

The method for calculating integrity is:

- SHA512

#### **PackageManager.Tools.Integrity: Hash Function**

The method for calculating integrity is:

- SHA512

## i9x0 servo inverters

The i9x0 servo inverter is the central servo element in drive technology.

## Product description

### Product identification

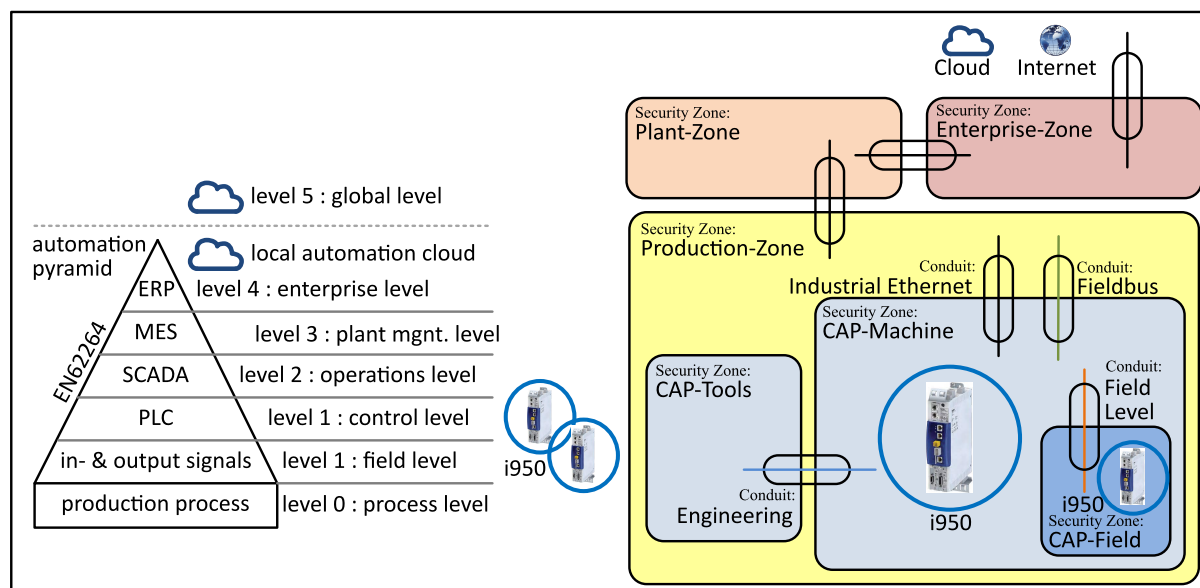
This documentation is applicable to the following components with their identification:

Name of product and product ID

| Name of product                                           | Product ID                             |
|-----------------------------------------------------------|----------------------------------------|
| i9x0 servo inverters                                      | I95Bxxxxxxxx0xxxx<br>I95Bxxxxxxxx7xxxx |
| i9x0 servo inverters, DC link                             | I95Cxxxxxxxx0xxxx<br>I95Cxxxxxxxx7xxxx |
| i9x0 servo inverters, Extended customer specific          | I95BxxxxxxxxWxxxx<br>I95BxxxxxxxxVxxxx |
| i9x0 servo inverters, DC link, Extended customer specific | I95CxxxxxxxxWxxxx<br>I95CxxxxxxxxVxxxx |

### Location in the network

These components are located in the automation pyramid at the control level or the field level. Furthermore, they are located in the security zone 'CAP-Machine' or security zone 'CAP-Field' ([Zones and conduits](#)).



Location in the Network

The level or zone in which the i9x0 servo inverters is placed depends on the area of use. A distinction can be made between three modes, which the customer can choose with the device parameter 0x4000.

# i9x0 servo inverters

## Product description

---

- The parameter 0x4000 is set to CiA402, e.g. 'CIA 402 [0]'. The i9x0 is then operated as a follower drive under motion control and thus falls into the field level and the security zone [CAP-Field](#).
- The parameter 0x4000 is set to a prepared TA (technology application), e.g. 'TA Table Positioning [20]'. The i9x0 is then operated as a drive under logic control and thus falls into the field level and the security zone [CAP-Field](#).
- The parameter 0x4000 is set to a free programmable device, e.g. 'TA User [10000]'. The i9x0 is then operated as a really small Controller and thus falls into the control level and the security zone [CAP-Machine](#).

The components addressed here have four relevant interfaces:

- **Conduit: Industrial Ethernet**  
Between the i9x0 and the 'Conduit: Industrial Ethernet' is the IoT gateway. Its task is to enable zone protection. If there is no IoT gateway in the system, the operator must ensure appropriate security at the zone border. This interface is not an open interface for direct connection to the Internet. The operator must interpose appropriate security measures to maintain the security zone.
- **Conduit: Fieldbus**  
The fieldbus requires special consideration within cyber security. The fieldbuses are standardized and, in most cases, have no integrated security functions. Thus, this interface must be considered with a classification SL-0 in the risk assessment of the operator.
- **Conduit: Engineering**  
This conduit has the property that it does not exist continuously, but only during commissioning or maintenance of the machine. Here, the system design must take into account in the risk assessment that the accesses are authorized and the employees have been instructed on the components and the machine cyber security concept. Furthermore, it must be ensured that the computer systems on which the necessary tools are installed comply with the current cyber security requirements and correspond to the state of cyber security.
- **Conduit: Field level**  
This conduit connects the i9x0 to other devices via EtherCAT. These other devices are for example i9x0 servo inverters of the same type or I/O systems for extending the onboard IOs.

### Intended purpose

The intended use of these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding cyber security are discussed.

- These components mentioned here are professional equipment and may only be commissioned and decommissioned by specialists.
- These components also require maintenance during their life cycle, which must be carried out by the operator.
- Modifications to the firmware or hardware of these components are not permitted.
- If these components are taken out of operation or disposed of, the instructions here in the documentation must be observed.
- Do not install any optional unused modules (minimize attack surface).

### Intended environment

The intended environment for these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding cyber security are discussed.

- 
- These components must be mechanically protected against unauthorized use. This can be achieved, for example, via physical access control systems or lockable control cabinets. In this case, access may only be granted to authorized persons and the number of accesses should also be restricted.
  - In particular, the removal of the SD Card may only be carried out by users authorized by the operator.
  - The components are not operated directly on the open Internet, but must also be operated by the operator via protection systems such as firewall, IDS, IPS, ... .
  - Deactivate all unused interfaces and/or protocols, both for the components mentioned here and for all components that are connected to the network.
  - The more security-critical an application is, the more systems should be separated. Only combine tasks on one component if they are in the same risk classification.
  - Wherever possible, use a Defense-in-Depth Concept in the environment of this component.
  - Use appropriate authentication mechanisms. This applies, for example, passwords that have the necessary complexity and an appropriate life cycle. The current state of the art must be taken into account here.
  - Handle secrets, such as passwords, appropriately. The focus here is on handling of secrets on the noted components, but also on the data stored in the environment of these components.
  - Validate all input options for validity. Pay attention to all human user interfaces as well as the machine software interfaces.
  - Keep the installed firmware version up to date and install updates.
  - Evaluate the environment, the technical task to be performed and the existing component security in a security-critical consideration and assess whether additional protective measures are necessary for your application.

### Security key indicators

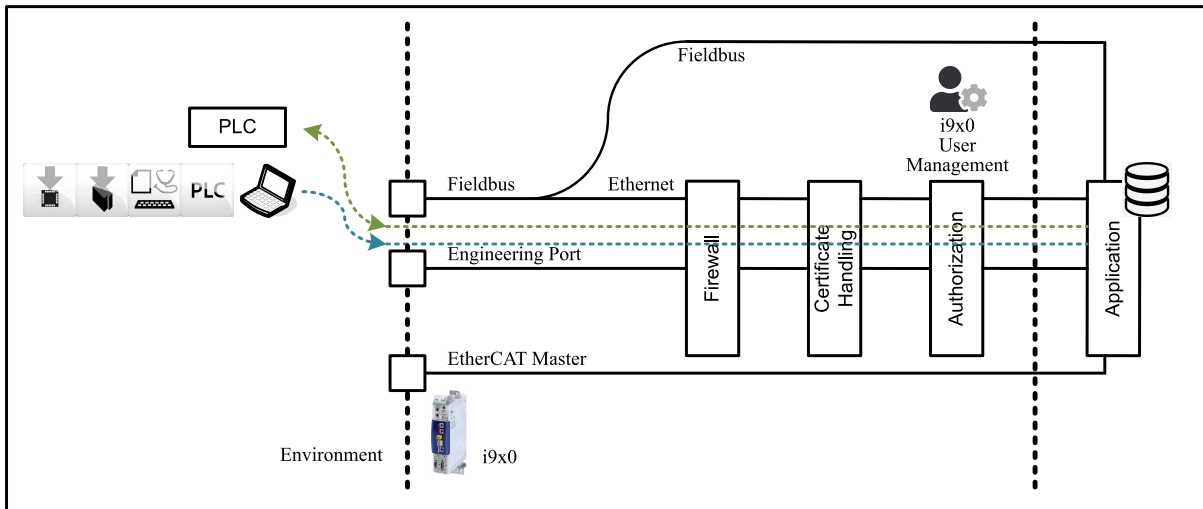
Security key indicator (in accordance with IEC 62443-4-2):

- These components are considered embedded devices (EDR).
- These components have a security level of SL-C 0.
- These components have an SL-vector from SL-C(i9x0)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }

### Security mechanisms

#### Product Defense in Depth

The following image shows the Defense in Depth product concept. For the sake of clarity, some details have been deliberately omitted.



Product Defense in Depth

The core concept of the i9x0 servo inverter is that the fieldbus and Engineering Port interfaces are assigned to User Management via a firewall. The firewall minimizes the attack surface. Certificate handling takes over certificate management for the respective encrypted connections.

- **i9x0 User Management**

Connections to Lenze engineering tools, such as the PLC Designer and EASY Starter, are made through authorization in the context of user management on the i9x0. All access to the servo inverter is viewed through this User Management.

Special attention must be paid to fieldbuses. Protocols based on Ethernet are routed via the firewall, and access authorizations should be minimized as much as possible. Data via the fieldbuses themselves is not routed via the cybersecurity functions and runs directly into the application. Protection measures must be implemented in the component's environment.

The SD Card must be physically protected with an access control.



When accessing this component from the Tools menu, certificates are not checked within a Public Key Infrastructure (PKI) structure. Instead, the certificates are automatically trusted via an AutoTrust function. The application does not perform manual verification.

- \* Without a PKI check or manual verification, attackers can use forged certificates to impersonate trusted entities and intercept sensitive data.

- \* Attackers could create fake certificates to impersonate legitimate users or systems, which can lead to unauthorized access to confidential information.

- \* Blind trust in certificates without verification can lead to malicious certificates being accepted, which jeopardizes the security of the entire system.

Recommended measures:

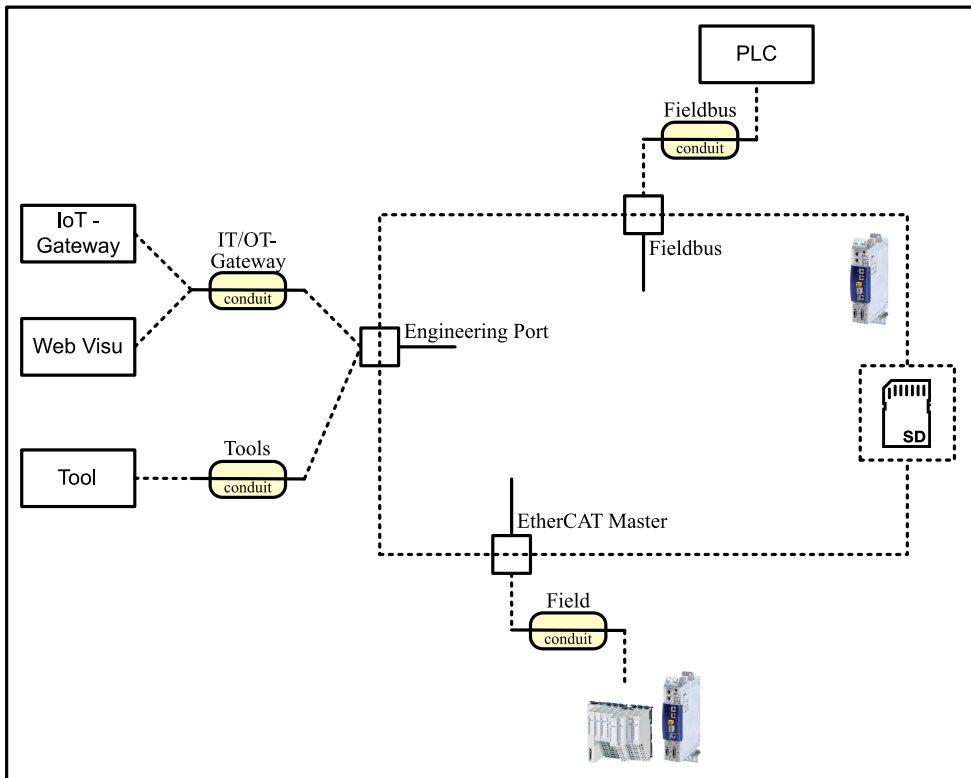




\* Use additional security mechanisms such as intrusion detection systems (IDS) and perform regular security audits.

### Expected Defense in Depth in the environment

The following image shows the Expected Defense in Depth in the environment of the i9x0 servo inverter.



Expected Defense in Depth in the environment

#### Conduit IT/OT gateway:

- An IT security-protected network environment is mandatory for the operation of these components. Operation on the Internet is not permitted.
- An IT/OT gateway is recommended to limit the attack surface so that only the absolutely necessary accesses and protocols are enabled.
- As the components cannot have any DoS / DDoS protection mechanisms from an embedded device perspective, these must be connected externally upstream.

#### Conduit Tools:

- Access from the engineering tools to the components must be limited in terms of organization and time.
- The corresponding engineering tools must be operated on an up-to-date and IT-security-secured computer.

#### Conduit Fieldbus:

- In most cases, the actual classic fieldbus protocol does not include any mechanisms to safeguard cyber security.

# i9x0 servo inverters

## Security mechanisms

---

- Measures to safeguard confidentiality, integrity and availability must be provided by the customer.

### Conduit Field:

- In most cases, the actual classic fieldbus protocol does not include any mechanisms to safeguard cyber security.
- Measures to safeguard confidentiality, integrity and availability must be provided by the customer.

### General Environment:

- General physical access protection must be provided for the components. This applies in particular to the SD cards in the controllers.
- Existing firmware updates for the i9x0 servo inverters as well as for all other components in the network should be installed immediately.

### Security mechanisms:

The following security functions are included in the listed components.



#### Note:

The functions mentioned are currently part of a prototypical firmware. If you are interested in this firmware, please contact your Lenze sales representative.

- i9x0.SFTPServer
- i9x0.SSHTServer
- i9x0.MinimumAndDefaultSecurity
- i9x0.SecureFactoryReset
- i9x0.Firewall
- i9x0.UserManagement
- i9x0.EncryptedCommunication.PLCDesigner
- i9x0.CertificateStore.viaPLCDesigner
- i9x0.OPCUAServer.Authentication
- i9x0.OPCUAServer.Certificate
- i9x0.Application.Encryption
- i9x0.Application.Signature
- i9x0.EncryptedApplicationData
- i9x0.NTP
- i9x0.SecureBoot
- i9x0.FirmwareUpdate
- i9x0.DeviceReplacement
- i9x0.SysLog
- i9x0.WebVisu.Activation
- i9x0.WebVisu.Certificate
- i9x0.WebVisu.UserManagement

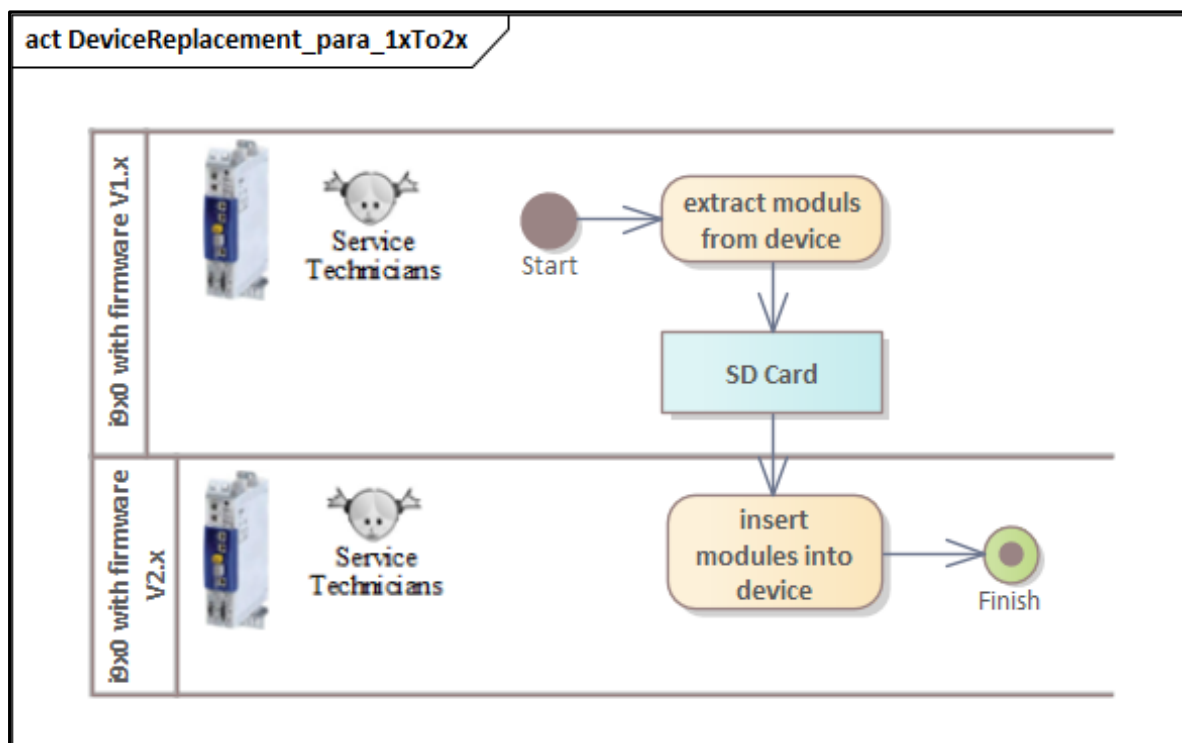
## Security mechanisms : Device Replacement

### Device Replacement (i9x0-base) from Version V1.x to Version V2.x

If the i9x0 is used in the base variant, i.e. the parameter 0x4000 is set to CiA 402, the parameter set is located and persists on the higher-level Controller regardless of whether the firmware is in V1.x or V2.x and is transferred to the i9x0 Servo Inverter at startup. This means that no further steps are required for a device replacement.

### Device Replacement (i9x0-para) from Version V1.x to Version 2.x

If the i9x0 is used in the para variant, i.e. the parameter 0x4000 is set to TA [...] (with the exception of TA User), the parameter set persists on the SD Card of the i9x0 Servo Inverter.



i9x0 Device Replacement i9x0-para from Version V1.x to Version V2.x

With the i9x0 para, device replacement is only possible by taking the SD card with you. The following behavior applies here:

- No initial query for the Security Configuration (refer to chapter [i9x0.MinimumAndDefaultSecurity](#)). The i9x0-para is always preset with "Minimal Security".
- The display for Secure Factory Setting does not flash (refer to chapter [i9x0.MinimumAndDefaultSecurity](#)).
- If executing the device command for Secure Factory Reset (refer to chapter [i9x0.SecureFactoryReset](#)), the settings of the Secure Configuration will always "Minimum Security".
- The Firewall will be deactivated by default.

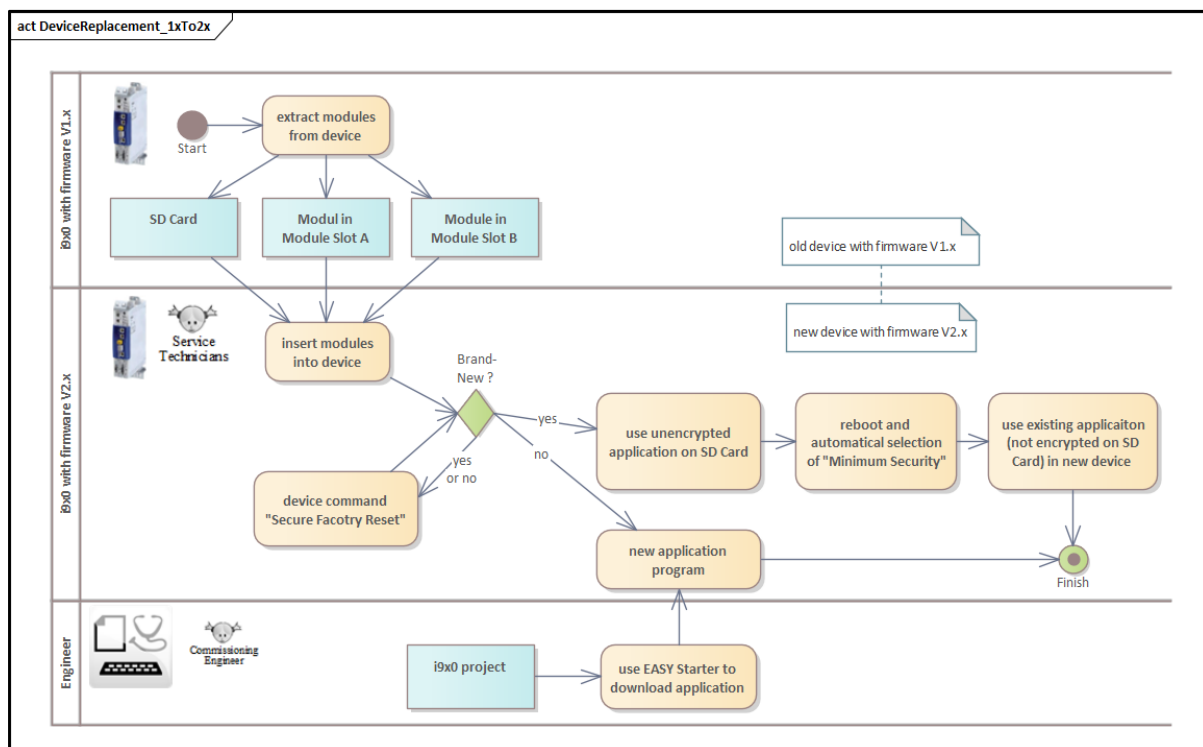
# i9x0 servo inverters

## Security mechanisms : Device Replacement

- The Communication will be in plain text by default.
- The application or the parameter set on the SD card is not encrypted.

### Device Replacement (i9x0-prog) from Version V1.x to Version V2.x

If the i9x0 is used in the prog variant, i.e. the parameter 0x4000 is set to TA User, the following diagram shows the device replacement process for a transition from firmware 1.x to a device with firmware 2.x.



i9x0 Device Replacement i9x0-prog from Version V1.x to Version V2.x

### Precondition

Info: From firmware V2.x, the data on the SD Card is encrypted for a new project, if default security is used in the i950 (refer to chapter [i9x0.MinimumAndDefaultSecurity](#)). This applies to the application data, but not to the SD Card itself.

- If an i9x0 Servo Inverter with V1.x firmware is used, the application data is still unencrypted on the SD Card.
- Optionally, an unencrypted backup can be stored on the SD Card.

### Replacement Scenario

- The SD Card is removed from the old firmware V1.x device and inserted into the new firmware V2.x device.
- All existing Encoder Modules in module slot A and module slot B are also replaced from the old to the new device.

- 
- When the new i9x0 Servo Inverter is switched on, it checks whether it is still in the brand-new state (indicated by the blink code Brandnew, refer to chapter [i9x0.MinimumAndDefaultSecurity](#)).  
Info: In the actual Firmware V2.x the i950 Servo Inverter will immediately switch to Minimum Security, so the blink code will not be visible.  
Info: If the i9x0 Servo Inverter is no longer in this state, it can be reset using the Reset Origin device command, refer to chapter [i9x0.SecureFactoryReset](#).
  - Is the brand-new state given:
    - The i9x0 Servo Inverter finds the unencrypted application on the SD Card and automatically sets its own security mode to "Minimal Security", refer to chapter [i9x0.MinimumAndDefaultSecurity](#).
    - A subsequent reboot is necessary for correct operation.
    - The i9x0 Servo Inverter can then work with the unencrypted application data on the SD Card (although it is in firmware V2.x).
    - This information is important for the customer, as in this scenario the customer is using an i9x0 Servo Inverter with V2.x firmware and can therefore use a simple migration and replacement scenario, but the application program is still stored unencrypted on the SD Card. This must be organizationally protected.
  - Is the brand-new state not given:
    - The i9x0 Servo Inverter does not accept the unencrypted application program and does not automatically set itself to "minimum security". The user must either run through the Secure Factory Reset device command (refer to chapter [i9x0.SecureFactoryReset](#)) or commissioning with the help of the EASY Starter and thus set the initial security configuration (refer to chapter [i9x0.MinimumAndDefaultSecurity](#)) manually.



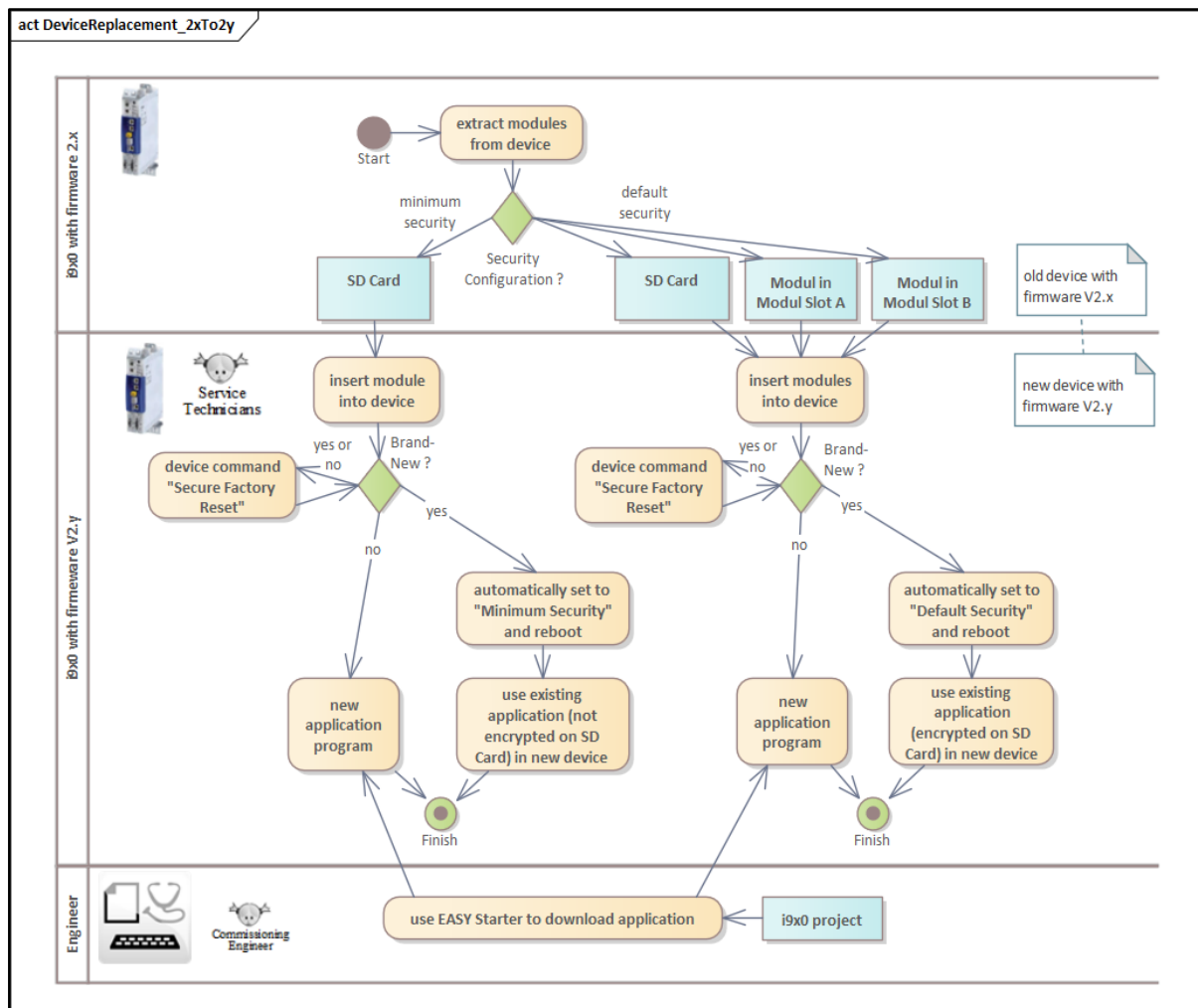
For further detailed descriptions, please refer to the [Device Replacement](#) security function.

### Device Replacement (i9x0-prog) from Version V2.x to Version V2.y

If the i9x0 is used in the prog variant, i.e. the parameter 0x4000 is set to TA User, the following diagram shows the device replacement process for a transition from firmware 2.x to a device with higher version of firmware 2.y. An i9x0 Servo Inverter stores the application on the SD card depending on the security configuration. How the device replacement runs depends on this.

# i9x0 servo inverters

## Security mechanisms : Device Replacement



i9x0 Device Replacement i9x0-prog from Version V2.x to Version V2.y

### Precondition

Info: From firmware V2.x, the data on the SD Card is encrypted for a new project. This applies to the application data, but not to the SD Card itself.

- If an i9x0 Servo Inverter with V2.x firmware is used, the application data is unencrypted or encrypted on the SD card, depending on the security configuration.

### Replacement Scenario

- The SD Card is removed from the old firmware V2.x device and inserted into the new firmware V2.y device.
- Depending on the security configuration, different modules must also be replaced:
  - Minimal Security:  
If the security configuration is set to Minimal Security, the application on the SD Card is not encrypted. Only the SD card must be transferred from the old to the new device.
  - Default Security:  
If the security configuration is set to Default Security, the application on the SD card is encrypted. The SD card and both encoder modules in module slot A and module slot B must be transferred from the old to the new device.

- **Unknown Security:**  
To be on the safe side, the SD card and both encoder modules should be transferred to module slot A and module slot B.

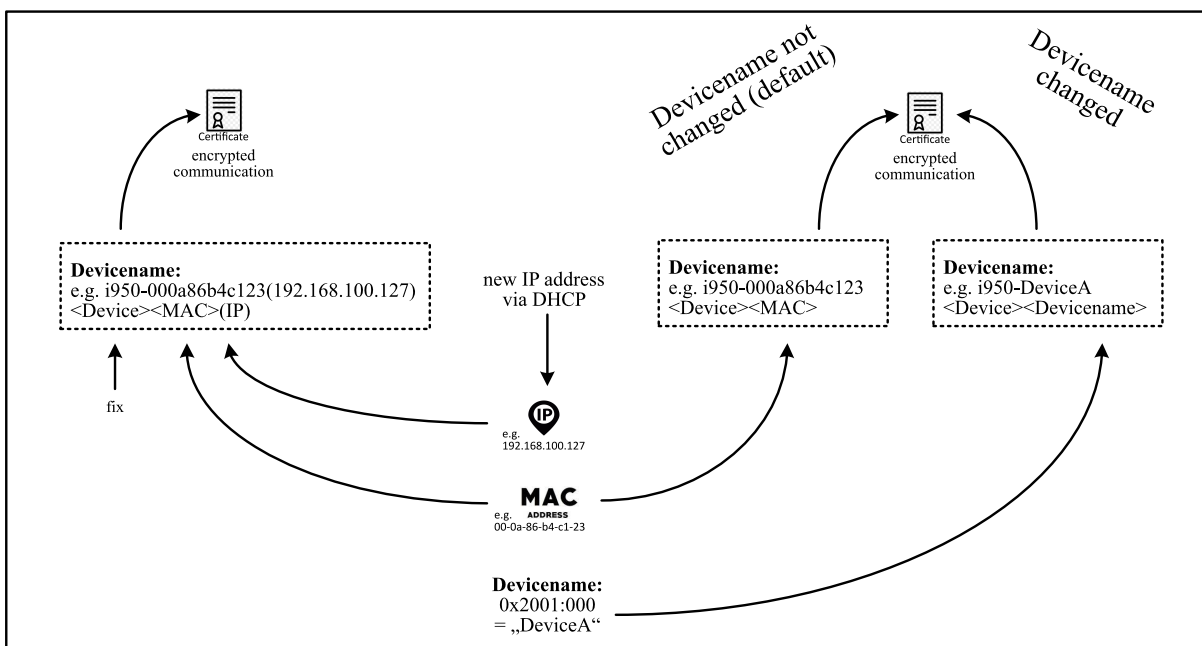


For further detailed descriptions, please refer to the [Device Replacement](#) security function.

## Security mechanisms : Nodename

This chapter does not directly describe a security function, but a behavior that has changed from version 1.x to version 2.x. It is about the NodeName, which has:

- A central function in the communication, identification and verification of devices.
- It represents the communication level between the PLC Designer (development environment) and the device (the SoftPLC).
- Enables unique identification of participants.
- And provides a basis for encrypted communication.



i9x0 Nodename Handling

### Behavior in Firmware version V1.x

The device name is composed of

- a fixed device name (e.g. i950)
- the MAC address and
- the IP address.

It is precisely this device name that is included as a data component in the certificate for encrypted communication.

# i9x0 servo inverters

Security mechanisms : Nodename

---

Advantage:

- Lots of information (name, MAC, IP) for recognizing the device.

Disadvantage:

- If the IP address changes (e.g. via DHCP), the device name changes and the certificate changes. This must be re-trusted when establishing a connection via encrypted communication.

## Behavior in Firmware version V2.x

If the device name remains unchanged (i.e. in the factory setting), only the fixed device name and the MAC address are included in the device name. If the device name is changed, only the fixed device designation and the changed device name are included.

Advantage:

- The customer can decide whether they want to see the MAC address or the device name they have set themselves.
- If the IP address is changed (e.g. via DHCP), the device name does not change and the certificate is retained. The certificate does not have to be re-trusted when a new connection is established.

Disadvantage:

- The IP address is no longer visible.



## Commissioning, Hardening and Decommissioning Notes and Organizational Measures

The following commissioning instructions must be followed.

### General instructions

- As far as possible, avoid connecting the i9x0 Servo Inverter to open networks or the internet. We recommend organizational and technical actions for the i9x0 Servo Inverter.
- For protection, additionally use data link layers such as a VPN for remote access.
- Install Firewall mechanisms, IPS (Intrusion Protection Systems) and IDS (Intrusion Detection Systems).
- Connecting external devices upstream to provide protection against DoS (Denial of Service) or DDos (Distributed Denial of Service).
- Restrict access to authorized persons only. A particular focus here is on physical access to the SD card. This concerns access to the data on the SD card, but also the physical swapping of SD cards between servo inverters.
- Change existing default passwords after the first start-up and also regularly afterwards. Please use only high-strength passwords.
- As soon as the web visu functions of the i9x0 Servo Inverter (refer to chapter [i9x0.WebVisu.Activation](#)) are accessed with a browser, we recommend activating the logging functions of the browser and backing up the certificate store of the browser. In this way, communication to the i9x0 servo inverter can be traced.

### Commissioning and hardening instructions

- Change the Key for SFTP-Server-Communication ([i9x0.SFTPServer](#)).
- Be sure, that there is no '.enable-ssh' file on the SD card for SSH-Access ([i9x0.SSHServer](#)).
- If you are using the i9x0-prog variant, please choose the security configuration ([i9x0.MinimumAndDefaultSecurity](#)).
- In the event of accidental incorrect parameterization, the Secure Factory Reset can be used to return to the delivery status (refer to chapter [i9x0.SecureFactoryReset](#)).
- Change the settings of the i9x0 Firewall for hardening the component ([i9x0.Firewall](#)).
- Activate and use the User Management ([i9x0.UserManagement](#)).
- Change the standard EngineeringItf-User-Password ([i950.UserManagement:EngineeringItf](#)) or delete this standard user.
- Prevent the deletion of the User Management on the SD card via an organizational measure ([i9x0.UserManagement](#)).
- Activate the function 'Encrypted Communication' ([i9x0.EncryptedCommunication.PLCDesigner](#)).
- Handle the certificates in the programming phase of the machine with the PLC Designer ([i9x0.CertificateStore.viaPLCDesigner](#)).
- If you are using the OPC-UA Server, please use the Authentication ([i950.OPCUAServer.Authentication](#)) and the Certificate handling ([i9x0.OPCUAServer.Certificate](#)).
- Activate encrypted application to secure the Application on the i9x0 ([i9x0.Application.Encryption](#)).
- Activation and configuration of the NTP client ([i9x0.NTP](#)).
- For users information, have a look at the secure boot ([i9x0.SecureBoot](#)).
- If needed an firmware update, please use the EASY Firmware Loader ([i9x0.FirmwareUpdate](#)).

# i9x0 servo inverters

## Commissioning, Hardening and Decommissioning Notes and Organizational Measures

---

- For easy device replacement the i9x0 has an specified replacement function ([i9x0.DeviceReplacement](#)).
- Activate the SysLog functionality for logging security relevant events ([i9x0.SysLog](#)).
- If using the WebVisu in the customer-specific variant, please hardening the communication and the web server ([i9x0.WebVisu.Activation](#)) ([i9x0.WebVisu.Certificate](#)) ([i9x0.WebVisu.UserManagement](#))

### Periodic security maintenance

- It is recommended to check the password policy periodically for updates and to adjust the requirements if necessary.
- It is recommended to change the passwords cyclically.
- It is recommended to check the certificates used with regard to their key lengths for up-to-dateness and to generate new certificates with higher key lengths if necessary.
- It is recommended to exchange the certificates regularly.

### Decommissioning instructions

- The device command 0x2022:001 "Device command: Load Lenze settings" must be executed. This resets all application settings.
- It is recommended to update the firmware using the EASY Firmware Loader.
- Remove the SD card and format it (in order to retain the Application Credits, the corresponding data must first be memorized and restored on the formatted SD card).

### Removal of product from environment

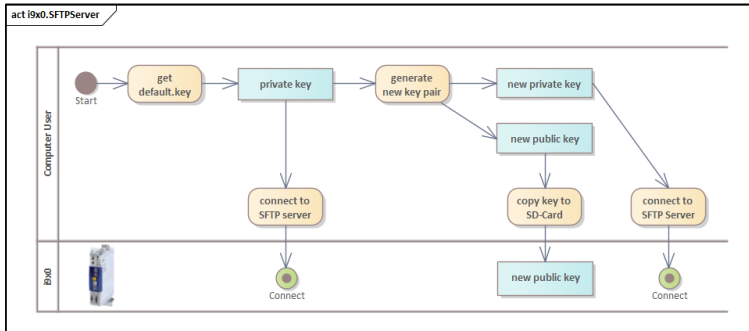
- It is recommended for all industrial communication partners of the i9x0 servo inverters to be removed, to change the trusted certificates of the i9x0 into untrusted certificates.
- It is recommended to securely remove the login data for the controller to be removed, such as name and password for the necessary authentication, from all industrial communication partners.

## Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

### i9x0.SFTPServer

With this functionality, some parts of the file system (e.g. the SD card) can be accessed via Ethernet.



Activity Diagram

### Physical and logical access

- Connector X16 (Engineering Access)
- Connector X2x6/X2x7 (fieldbus device)  
Only if a fieldbus (e.g. PROFINET Device with X256/X257 or EthernetIP Adapter X266/X267) is included in the device tree of the i9x0 servo inverters in the PLC Designer and the IP-Configuration 0x2381 is set in the parameter set.
- Used port for SFTP is 47877/tcp

### i9x0.SFTPServer: Access to the SD-Card

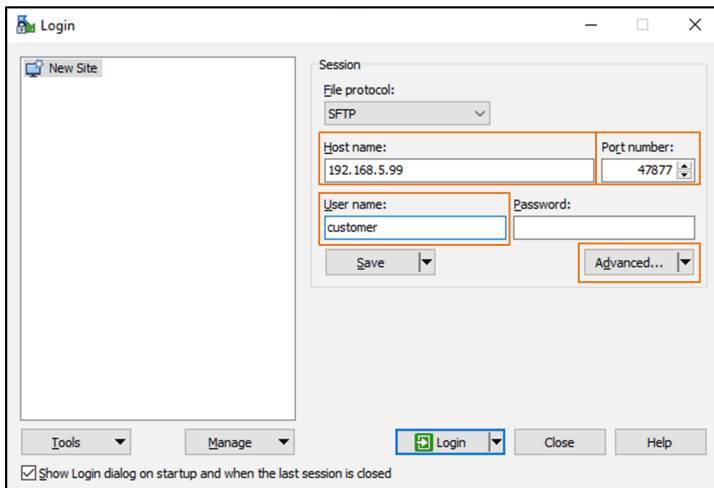
Access to the file system via SFTP has been available since firmware version 01.00.00.

A suitable SFTP client is required for this access. In the following, for example, WinSCP(<https://winscp.net>) is used.

Start WinSCP and enter the necessary data, as shown in the following picture.

# i9x0 servo inverters

## Security functions

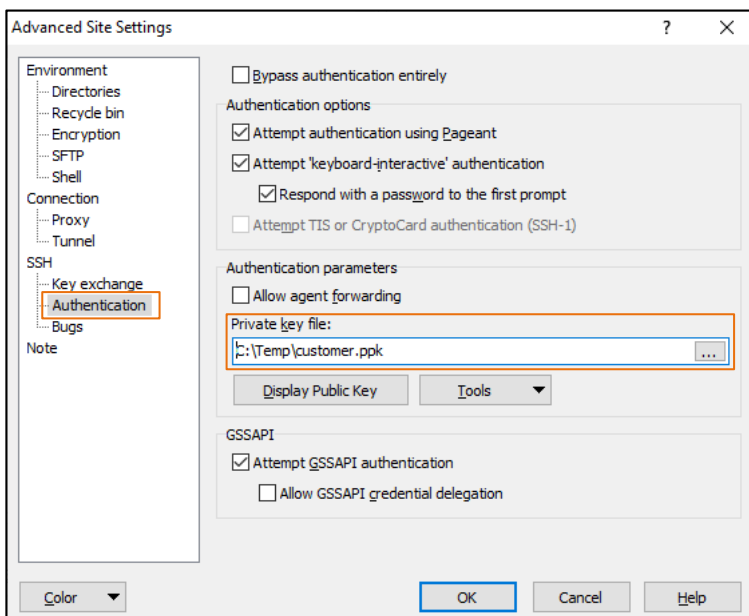


WinSCP Login

### Insert the following data

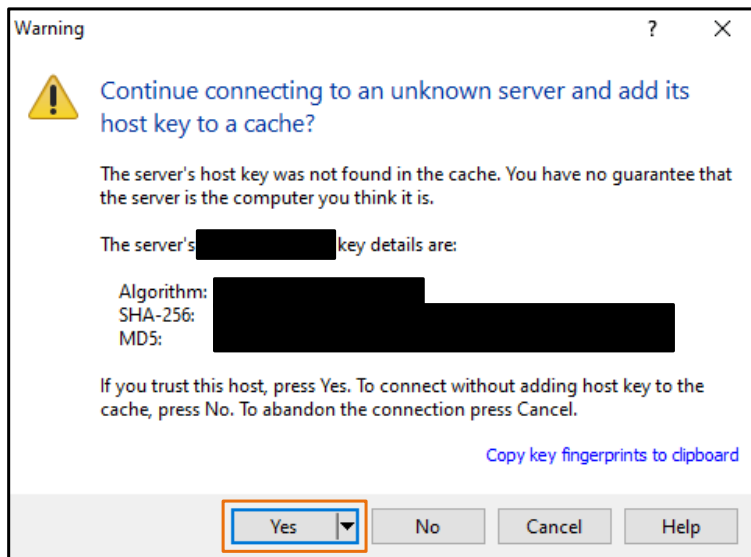
- File protocol: SFTP (communication protocol)
- Host Name: IP address of the i9x0 servo inverter
- Port Number: SFTP port number of the i9x0 (use port 47877)
- User Name: customer
- Password: keep this password empty

Next, the Advanced dialog must be used. A .ppk file is needed to insert the private key file into the Menu/Authentication window. You can find the file in the Lenze internal AKB (document ID 201800294). Please contact Lenze Support.



Insert customer.ppk key-file

After agreeing to the following warning, some directory paths can be accessed on the i9x0 Servo Inverters.



Agree to Warning

### i9x0.SFTPServer: Changing the customer.ppk

Changing the customer.ppk has been available since FW version 01.05.00.

This description is required if the access key (customer.ppk) for SFTP access to the i9x0 is to be individualized. To do this, a separate key must be generated.

Note that the resetting of a key in the i9x0 once changed can only be carried out by the "reset to factory settings" device command (refer to chapter [i9x0.SecureFactoryReset](#)). Therefore, great care must be taken when storing and archiving a new key.

A private key once changed can also be found in a backup of an i9x0 and thus automatically becomes active during a restore on a new device.

### Constraints on the key

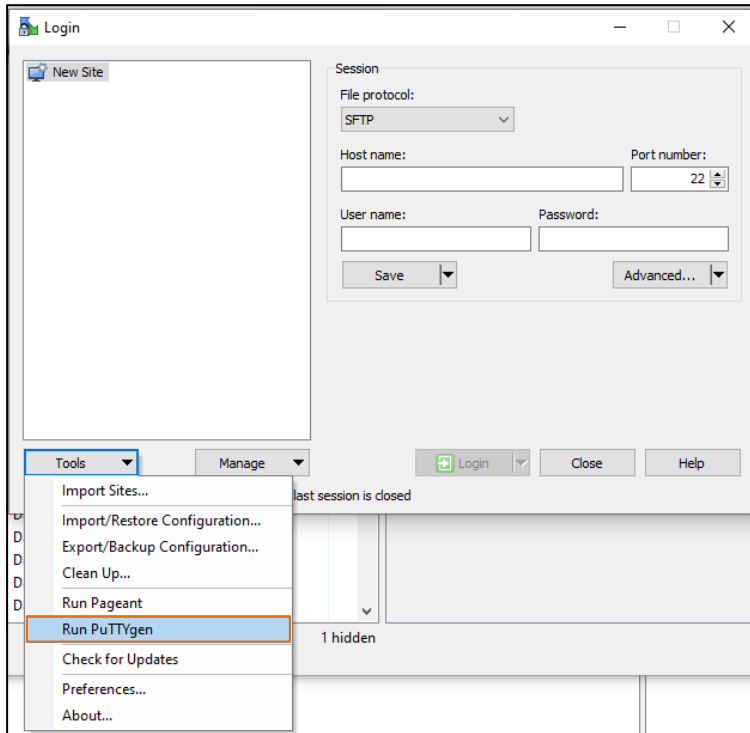
- RSA
- minimal length of 2048 Bits

# i9x0 servo inverters

## Security functions

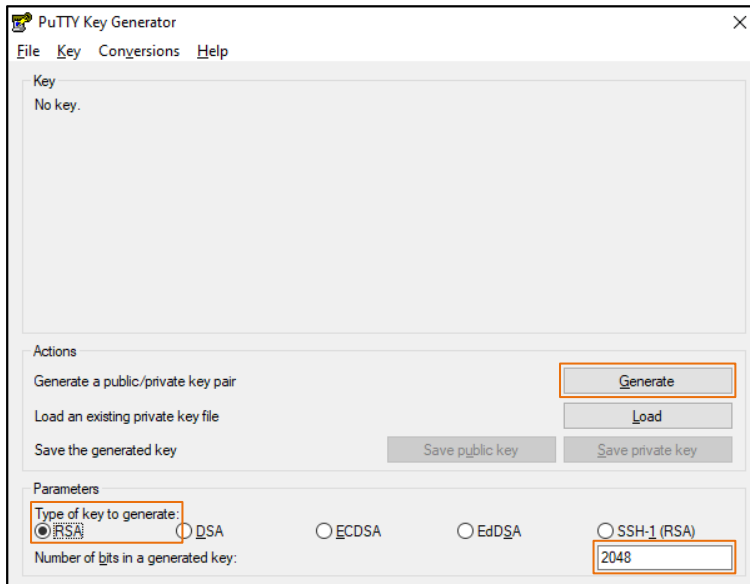
### Generate a new key

1. After starting the WinSCP program, press the "Tools" button in the "Login" dialog that opens automatically. From the menu that appears, select "Run PuTTYgen" to start the PuTTYgen program. PuTTYgen is responsible for key generation. Note: The "Run PuTTYgen" entry is not visible when using WinSCP Portable.



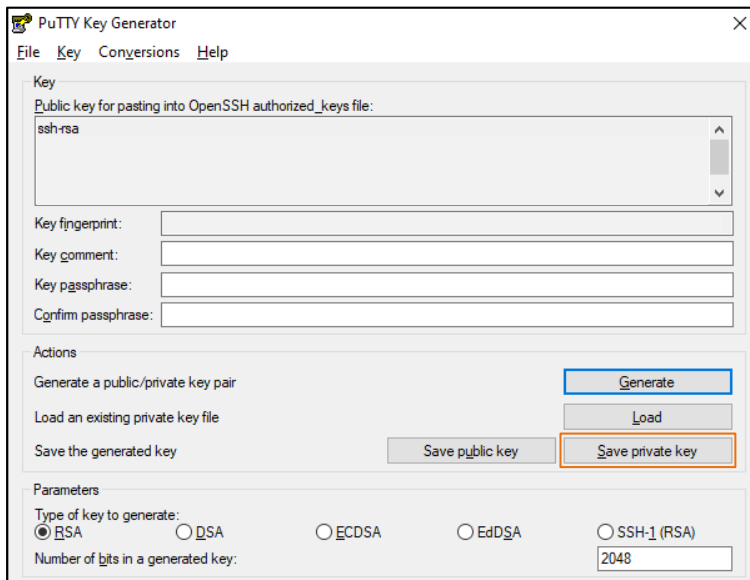
WinSCP using Tools / Run PuTTYgen

2. In PuTTYgen, the key type to be generated (RSA) is set and the length of the keys is specified in bits (minimum 2048 bits). By pressing the “Generate” button the new key pair is generated.



PuTTY Key Generator

3. After creating the key, you can enter a comment before saving. A password (here called “passphrase”) can also be set; the necessity for this must be decided depending on the application. Among other things, it should be taken into account that this “passphrase” must be entered on the PC every time the private key is used. The private key can now be saved for later use using “Save private key”.

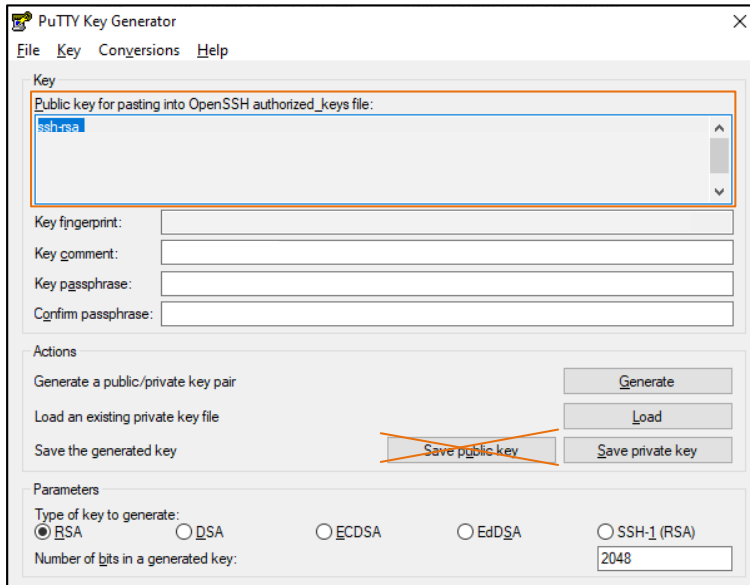


PuTTY Key Generator: Save Private Key

# i9x0 servo inverters

## Security functions

4. In order to make this private key known to a device, the contents of the text box “Public key for pasting into Open SSH authorized\_keys file” must be copied and saved in an ASCII text file named “customer.key”. Care must be taken to ensure that the content is not changed: it is a single long line. Note: The file created with “Save public key” cannot be used. For the “public key”, the text must be copied as described above.



Safe Public Key

### Advertise a new Private Key in the i9x0:

1. The file “customer.key” must be on the device's SD card in the existing "public key" directory. For security reasons, the directory “/sdcard/public-key” can only be accessed via SFTP in read-only mode; therefore the file must be copied to the SD card, e.g. on a PC.
2. The currently active private key establishes an SFTP connection to the device.
3. The file "customer.key" is now stored via SFTP in the device in the directory "/tmp/user\_data".
4. The storage process is registered by the device; as a result, the transferred file is stored and checked for correctness:
  - On the SD card, an identical file .key must be placed under "public-key/customer.key".
  - The file may contain only one line with an RSA key (empty lines are ignored).
  - The line with the RSA key must withstand rough validation.
  - The RSA key must be at least 2048 bits long.No matter what the result of the checks is: The file "/tmp/user\_data/customer.key" is automatically deleted from the device.  
If a check is not successful, the directory "/tmp/user\_data" generates a file called "customer.key.ret" with a corresponding error message.  
Possible error messages:
  - unable to read "/sdcard/public-key/customer.key"
  - "/tmp/user\_data/customer.key" does not match "/sdcard/public-key/customer.key"
  - RSA key required
  - not a valid RSA key
  - RSA key of at least 2048 bits required



- 
5. After a successful transfer of the file "customer.key", the current SFTP connection must be disconnected and a new SFTP connection must be established using the new private keys. If this fails, it must be checked that the transferred file "customer.key" belongs to the new private key used.
- The transferred file "customer.key" has been correctly created and saved.
  - The private key used has been saved correctly.
- If successful, the new private key can now be used for SFTP connections to the device.

#### Information on handling

- The new key will continue to work if the SD Card is changed or deleted.

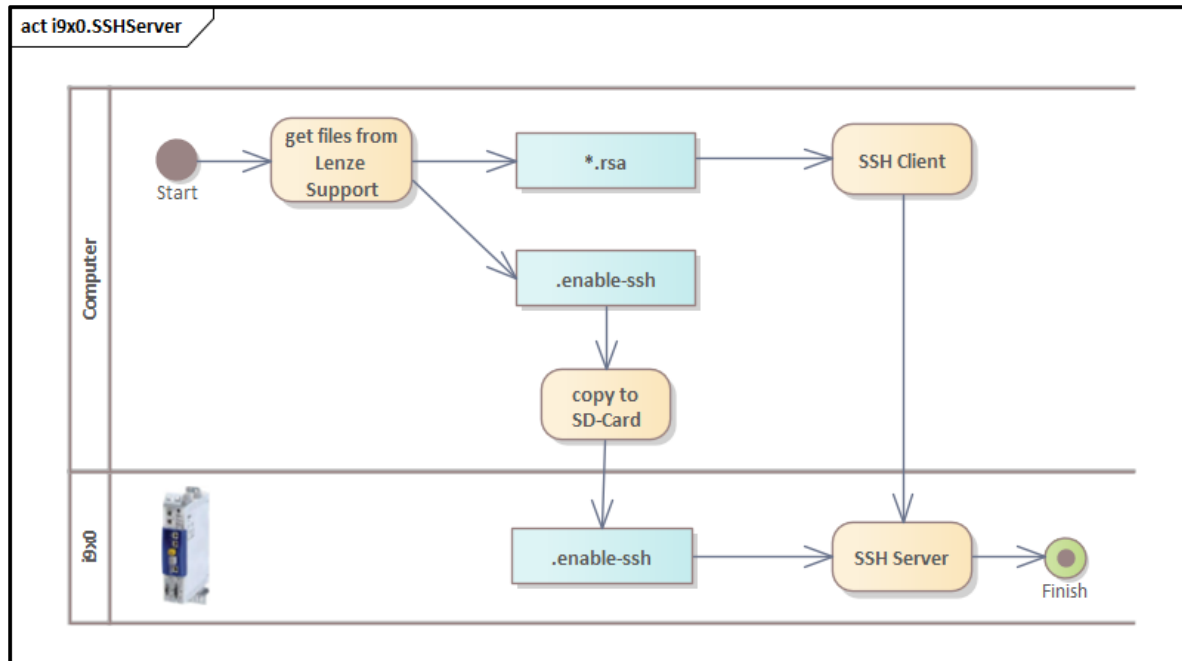
# i9x0 servo inverters

## Security functions

### i9x0.SSHServer

Accessing the device via SSH has been available since FW version 01.00.00.

This functionality allows you to access the file system via Ethernet. A SSH key is needed to access the device. Lenze Support generates this key only in special support cases and it should not be used during normal operation.



Activity Diagram

You will receive two files from Lenze Support.

- .enable-ssh
- \*.rsa

Both files are personalized for the requester and must be protected accordingly. Do not share or publish these files.

#### Physical and logical access

- Connector X16 (Engineering Access)
- Used port for SSH is 22/tcp

#### i9x0.SSHServer: Enable SSH-Access

In order to obtain SSH access to the i9x0, the following steps must be completed.

- SSH access is not possible in the delivery state. This key is generated by Lenze Support only in special support cases and should not be used during normal operation.
- The .enable-ssh file must be copied to the i9x0's SD card. It should be ensured that the leading point (hidden file in Linux) is included in the file name. The location for the file is directly in the root directory of the SD card.

The following is a description of how to access the i9x0 with a Linux Ubuntu system. Other clients may have a different procedure.

- 
- Copy the \*.rsa file to the /home/<user>/ssh/ directory.
  - If the directory does not yet exist, it must be created and provided with appropriate rights:
    - mkdir -p ~/.ssh
    - chmod 0700 ~/.ssh
  - The access rights to the file must be adjusted accordingly:
    - chmod 0600 <\*.rsa>
  - The key must be added to the ssh:
    - ssh-add "~/.ssh/<\*.rsa>"
  - After that, the SSH access to the controller can be created with the following command:
    - ssh root@<ip>

#### i9x0.SSHServer: Disable SSH-Access

Remove the .enable-ssh file from i9x0's SD Card.

#### i9x0.SSHServer: Combination of SSH and SFTP via Ports and Networks

The following table shows the possibility of using SSH and SFTP via the existing ports and via the possible networks. This representation refers to a disabled i9x0.Firewall.

Combination of SSH and SFTP via different ports and networks:

| Device with Interface                      | Port  | with .enable-ssh file                                                               | without .enable-ssh file                                                 |
|--------------------------------------------|-------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Engineering-port X16 onboard               | 22    | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            |
|                                            | 47877 | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP |
| PROFINET Device X256/X257 in E1            | 22    | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            |
|                                            | 47877 | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            |
| EthernetIP Adapter x266/x267 in E1         | 22    | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            |
|                                            | 47877 | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP |
| EoE via onboard EtherCAT X236/X237 onboard | 22    | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input type="checkbox"/> SFTP            |
|                                            | 47877 | <input checked="" type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP | <input type="checkbox"/> SSH<br><input checked="" type="checkbox"/> SFTP |

## i9x0.MinimumAndDefaultSecurity

This chapter is divided into

- identification of the secure default delivery status,
- set the security configuration,
- behavior with minimum security and
- behavior with default security.

## Identification of the secure default delivery status

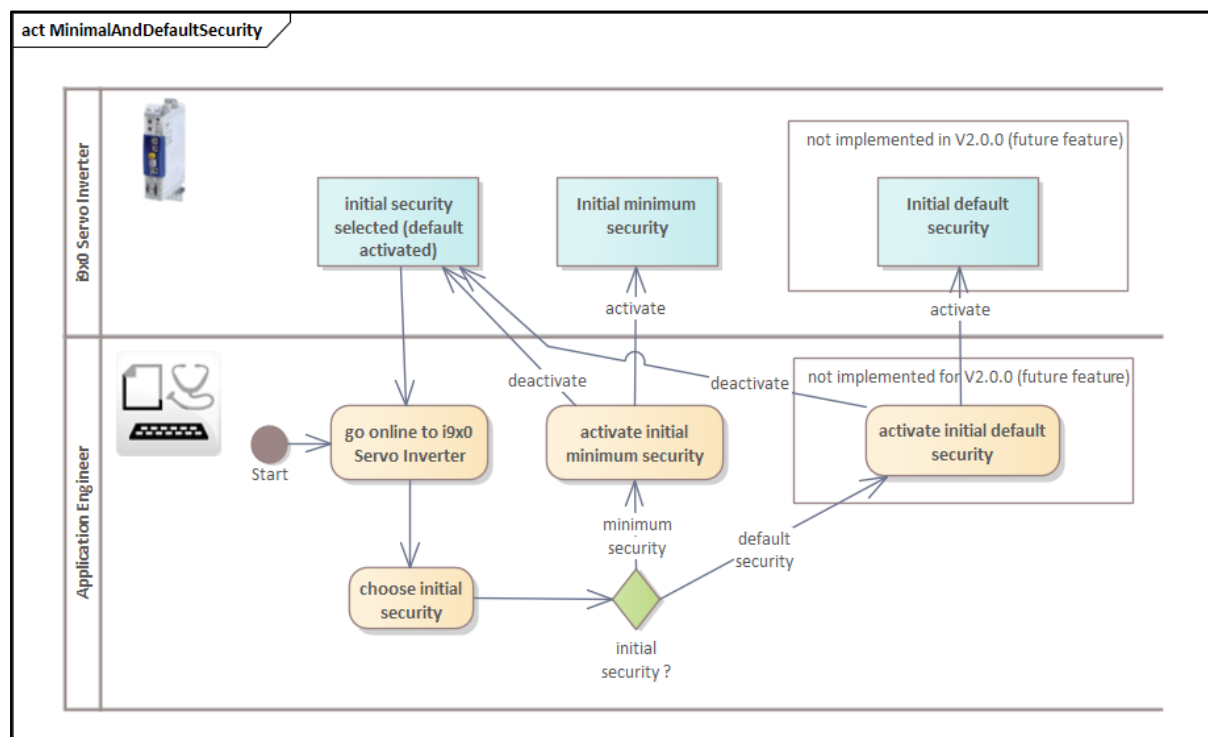
The i9x0 Servo Inverter flashes in the delivery state and after a successful device command set factory reset.

| Blinking pattern of the RDY-LED | Status    | Status/meaning                                 |
|---------------------------------|-----------|------------------------------------------------|
| flashing each second            | Brand-New | The i9x0 Servo Inverter is in brand-new state. |

**i** If the Firmware 2.x is started in the factory-new state, the security state "minimum security" is automatically selected. In this respect, the flashing is not visible. This module has already been implemented for later versions, where the user can choose between minimum security or default security on initial switch-on (refer to chapter [i9x0.MinimalAndDefaultSecurity](#)).

## Set the secure configuration

As of firmware v2.0.0, the i9x0 Servo Inverter is in the state 0x5905:010 Bit 0 = activated on delivery and after Secure Factory Setting, i.e. initial security is selected. On this basis, the user must decide which security configuration is to be selected.



i9x0 Security Configuration

The setting is made via the following parameter in the parameter set.

| Address    | Name                                           |                               | Info                                                                                                    |
|------------|------------------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------|
| 0x5905:010 | Security user settings: Status device security |                               |                                                                                                         |
|            | Bit 0                                          | Initial security selected     | This bit is set by default.                                                                             |
|            | Bit 1                                          | Initial Minimum security      | In version 2.0, the i950 will automatically switch to "Minimum Security" mode in the factory new state. |
|            | Bit 2                                          | Initial Default security      | This bit is created for use in future firmware versions, but is currently not assigned.                 |
|            | Bit 3                                          | reserved, shall be zero       |                                                                                                         |
|            | Bit 4                                          | Customer specific security    |                                                                                                         |
|            | Bit 5                                          | reserved, shall be zero       |                                                                                                         |
|            | Bit 6                                          |                               |                                                                                                         |
|            | Bit 7                                          |                               |                                                                                                         |
|            | Bit 8                                          | Access Control active         |                                                                                                         |
|            | Bit 9                                          | Firewall active               |                                                                                                         |
|            | Bit 10                                         | Secure Communication enforced |                                                                                                         |
|            | Bit 11                                         | Secure Communication enforced |                                                                                                         |
|            | Bit 12                                         | Secure Bootloader active      |                                                                                                         |

### Behavior with minimum security

This selection option and function is included in firmware version V2.0.0 and will be selected by default.

Cybersecurity distinguishes between its own device protection and customer-selectable features. The device protection functions are included as standard and cannot be deactivated. This is in contrast to the customer-selectable features. These are all deactivated in the initial minimal security setting and can subsequently be reactivated individually by the customer (opt-in approach).

The following settings are set for initial minimum security:

- Deactivated Firewall
- Deactivated Encrypted Communication
- Deactivated User Management
- Deactivated Data Encryption

# i9x0 servo inverters

## i9x0.SecureFactoryReset

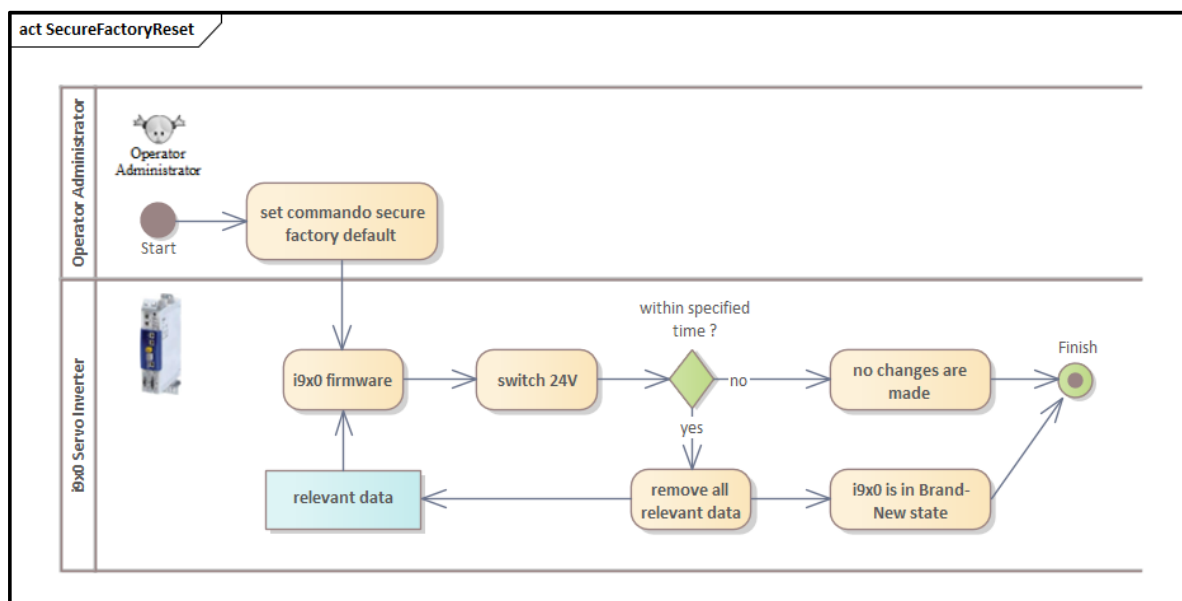
### Behavior with default security

This selection option and function is not included in firmware version V2.0 and will be implemented in future versions.

Cybersecurity distinguishes between its own device protection and customer-selectable features. The device protection functions are included as standard and cannot be deactivated. This is in contrast to the customer-selectable features. These are all activated in the initial default security setting and can subsequently be deactivated individually by the customer (opt-out approach).

### i9x0.SecureFactoryReset

This function resets the i9x0 servo inverter and is available from firmware version V2.0.0.



i9x0 Secure Factory Reset

This functionality is executed in two stages:

- In the first stage, a device command must be sent.
- In the second stage, mains switching must be carried out within a specified time.

Necessary conditions:

- The mains switching must take place physically on site, which means that the 24V must be switched on site. Executing a device command such as a reboot is not permitted. This also applies to the execution of the "set secure factory reset" command.
- The timeout time is 60 seconds. The mains switching must take place within this time. If mains switching takes place after this time, no deletion routine is triggered.
- Once the command has been executed correctly, the i9x0 Servo Inverter returns to its default state and the flashing pattern for Brand-New is visible again, however, is switched to "minimum security" as soon as it is switched on and is no longer visible(refer to chapter [i9x0.MinimumAndDefaultSecurity](#)).

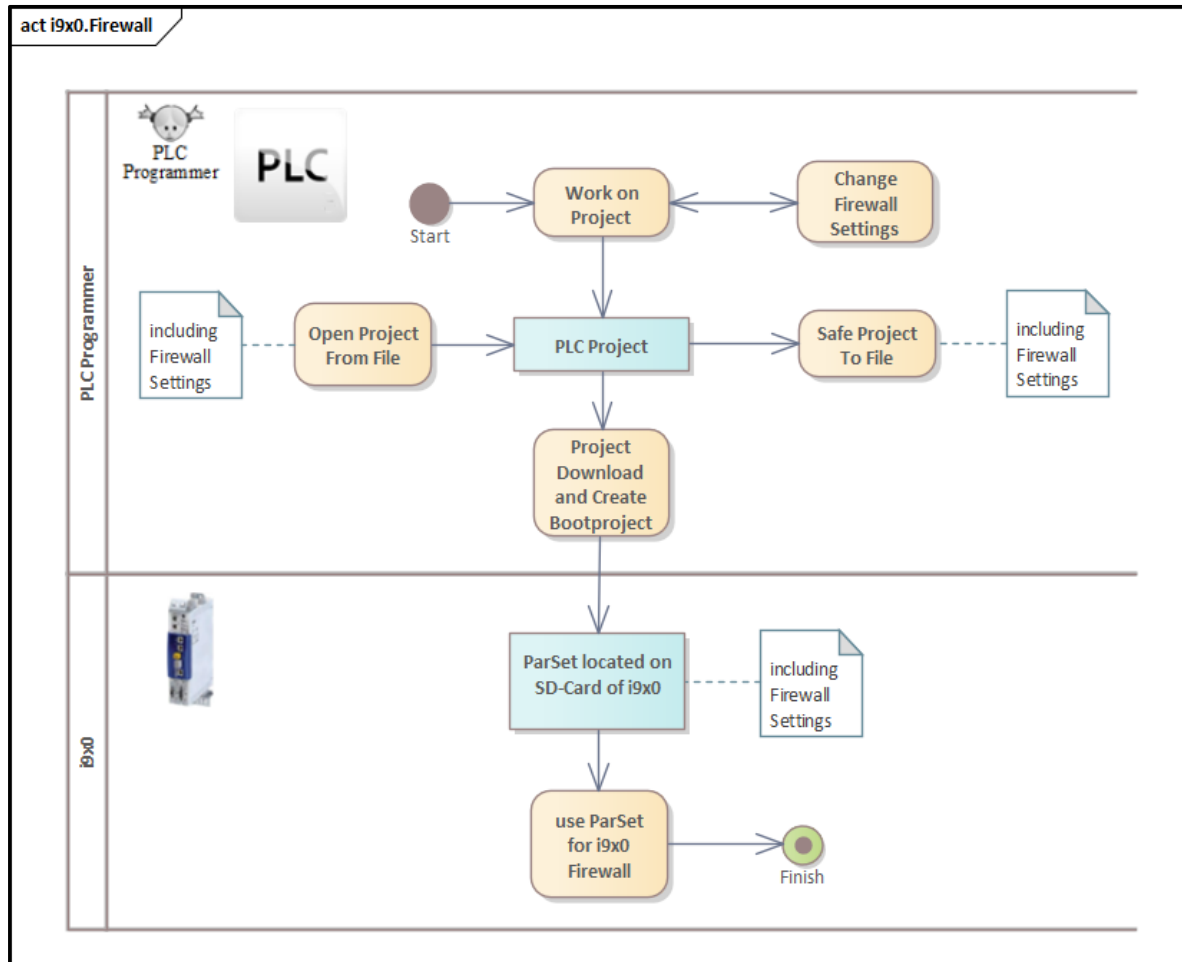
---

| Address    | Name                       |             | Info |
|------------|----------------------------|-------------|------|
| 0x2022:052 | set secure factory default |             |      |
|            | 0                          | Deactivated |      |
|            | 1                          | Activated   |      |

## i9x0.Firewall

The functionality of the i9x0 Firewall is available from versions 2.0.0 on.

The »PLC Designer« is used to put the i9x0 Firewall into operation and to parameterize it. A general procedure can be found in the following picture.



Activity Diagram

## i9x0.Firewall: Configuration

This chapter describes the configuration regarding parameterization of the i9x0 Firewall.

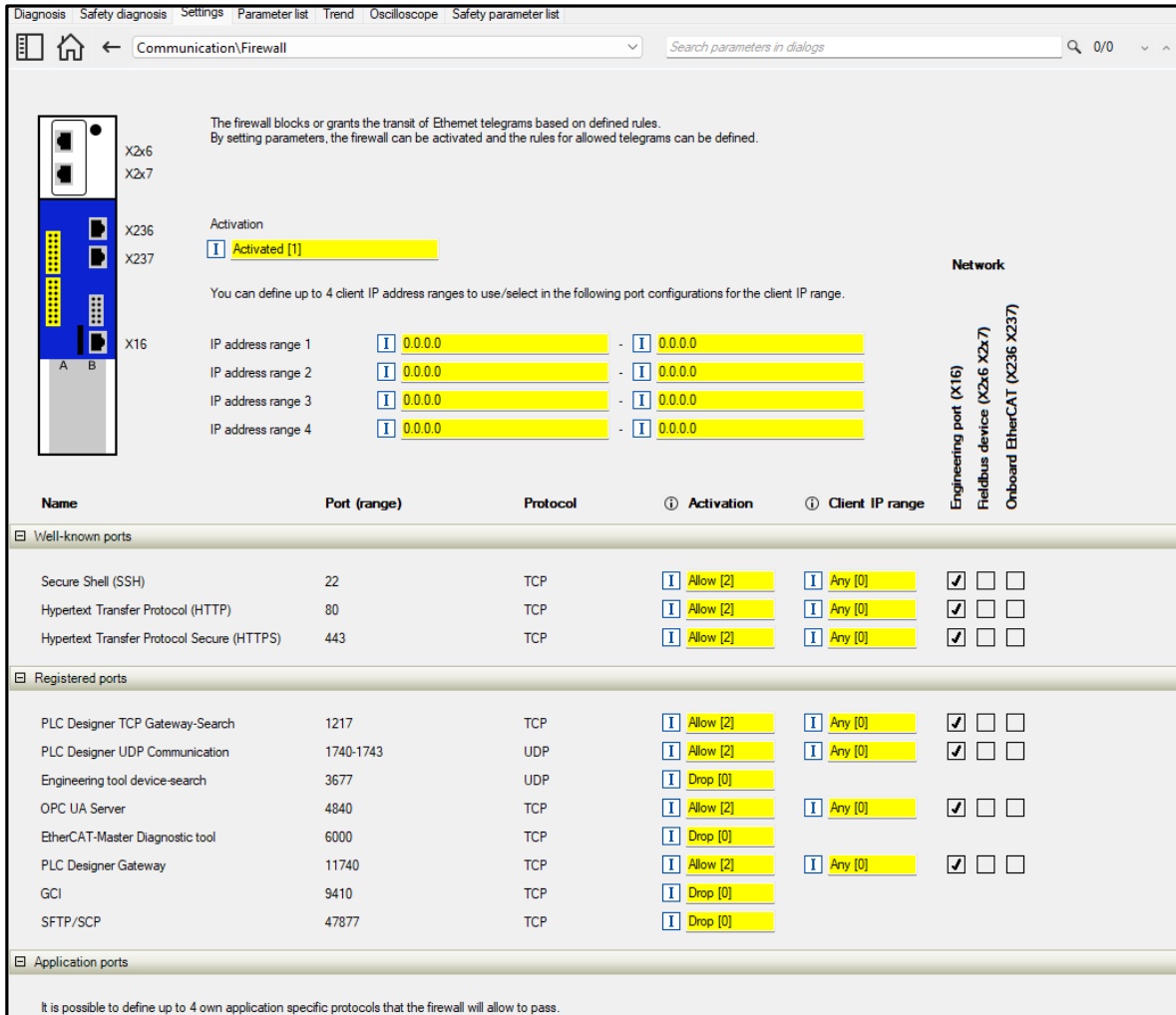
### i9x0 Firewall Configuration Data:

The configuration data of the i9x0 Firewall is stored in the parameter set of the i9x0. The individual setting options are mapped to individual indexes, subindexes, bit coding or enumerations. The index range extends from 0x5910 to 0x5913. This parameter set can be configured in the PLC Designer and is part of the PLC Designer project. Likewise, the parameter set is part of the project, which is transferred to the i9x0. The parameter set is located on the SD card of the i9x0.

During commissioning, this parameter set must be protected from unauthorized modification by additional measures. When commissioning a machine, it is therefore necessary that the individual communication channels are considered and evaluated from a cyber security point



of view. Examples include: (a) Change with the EASY Starter (b) Change via SSH (c) Change SFTP (d) etc.. Furthermore, the SD card must be protected from removal, as the format on it can be read and changed with the help of any SD card reader. It is therefore recommended to the operator to mechanically protect the control cabinet from unauthorized use.



Settings Dialog for the i9x0.Firewall

### Parameter for the i9x0 Firewall:

The parameter concept contains four indexes:

- 0x5910: Basic parameters for the i9x0 Firewall, which apply generically
- 0x5911: Well-Known Port Settings (Ports 1 bis 1.023)
- 0x5912: Registered Port Settings (Ports 1.024 – 49.151)
- 0x5913: Application Port Settings

All four areas are described below.

### Basic parameters for the i9x0 Firewall 0x5910:

In the default settings, the firewall is deactivated. This is necessary for compatibility reasons with older versions. The activation is possible with parameter 0x5910:001.

Parameter for activating the i9x0 Firewall

# i9x0 servo inverters

i9x0.SecureFactoryReset

| Address    | Name                          | Info                                         |
|------------|-------------------------------|----------------------------------------------|
| 0x5910:001 | Firewall: Firewall activation |                                              |
|            | 0                             | Deactivated<br>i9x0 Firewall is deactivated. |
|            | 1                             | Activated<br>i9x0 Firewall is activated.     |

The following setting option affects the IP clients that want to access the i9x0. The IP address ranges of the clients are specified here.

## Example:

If 0x5910:002=192.168.5.100 and 0x5910:003=192.168.5.120 are parameterized, the range of IP addresses is allowed, e.g. a client with the IP address of 192.168.5.110 may access, but a client with the IP address of 192.168.5.90 or 192.168.5.130 may not. It is also possible to select the same start and end address to allow only a single IP address. Four IP ranges are offered in order to be able to set the IP clients on the different networks separately.

Parameter for the IP Client Addresses:

| Address                                              | Name                              | Info                                                                             |
|------------------------------------------------------|-----------------------------------|----------------------------------------------------------------------------------|
| 0x5910:002<br>0x5910:004<br>0x5910:006<br>0x5910:008 | Firewall IP Range: IP Range Start | Start of IP Range for the IP Clients<br>Range 1<br>Range 2<br>Range 3<br>Range 4 |
| 0x5910:003<br>0x5910:005<br>0x5910:007<br>0x5910:009 | Firewall IP Range: IP Range End   | End of IP Range for the IP Clients<br>Range 1<br>Range 2<br>Range 3<br>Range 4   |

Please remember that, at this point, only the limits of the IP address ranges of the clients are set. The selection and activation takes place for the individual protocols. These IP addresses apply to all protocols and are therefore generic.



Setting the IP ranges of clients only affects the engineering port and the EoE network. Clients on the fieldbus are not considered in terms of their IP addresses. Furthermore, changes to the parameters for the IP ranges only affect new sessions and not existing ones.

## Parameters for the Well-Known Port Settings (Port 1 – 1,023) 0x5911:

The firewall settings are stored in the device parameter set. Below the index is the range of subindices. The subindex range is divided into blocks of 10 subindices each. Each block contains the parameters for each possible protocol. There are three setting options for each protocol (other subindices are reserved):

| Address    | Name                                 |                        | Info                                                                          |
|------------|--------------------------------------|------------------------|-------------------------------------------------------------------------------|
| 0x5911:xx1 | Firewall <protocol>: Network         |                        |                                                                               |
|            | 0                                    | Engineering Port       | Engineering Port via X16                                                      |
|            | 1                                    | Fieldbus slave         | Fieldbus slave via Profinet Device X256/X257 or Ethernet/IP Adapter X266/X267 |
|            | 4                                    | Onboard EtherCAT (EoE) | EoE (Ethernet over EtherCAT) via onboard X236/X237                            |
| 0x5911:xx2 | Firewall <protocol>: Client IP Range |                        |                                                                               |
|            | 0                                    | Any                    | All Client IP Addresses are allowed.                                          |
|            | 1                                    | IP Range 1             | IP Range 1 defined in 0x5910:002 and 0x5910:003.                              |
|            | 2                                    | IP Range 2             | IP Range 2 defined in 0x5910:004 and 0x5910:005.                              |
|            | 3                                    | IP Range 3             | IP Range 3 defined in 0x5910:006 and 0x5910:007.                              |
|            | 4                                    | IP Range 4             | IP Range 4 defined in 0x5910:008 and 0x5910:009.                              |
| 0x5911:xx3 | Firewall <protocol>: Activation      |                        |                                                                               |
|            | 0                                    | Drop                   | Deny Connection without notifying the Sender.                                 |
|            | 1                                    | Reject                 | Deny Connection with notifying the Sender.                                    |
|            | 2                                    | Allow                  | Allow Connection                                                              |

As mentioned above, these choices are available for each protocol.

#### Parameters for the Registered Port Settings (Ports 1,024 – 49,151) 0x5912:

The range of subindices is divided into blocks of ten. Each block contains the parameters for one possible protocol. There are three setting options for each protocol that correspond to the settings of the well-known ports.

#### Parameters for the Application Port Settings (Ports 49,152 – 65,535) 0x5913:

In contrast to the first mentioned ports, it is not possible to perform a factory default setting for the application ports. The reason lies in the dynamic use of e.g. sockets in the IEC application. This may make it necessary to open additional ports in the firewall. This is exactly where the application ports aim.

The special feature here is that the protocols required by the ports are unknown and defined only by the application. Further setting options are necessary for this purpose, which are explained below.. These setting options are additional, e.g. each protocol still contains the three subindices for Network, Client IP Range and Activation.

In addition, there are four additional parameters for each application port:

# i9x0 servo inverters

i9x0.SecureFactoryReset

| Address    | Name                       | Info                            |
|------------|----------------------------|---------------------------------|
| 0x5913:xx7 | Firewall: Protocol Type    |                                 |
|            | 0                          | None                            |
|            | 1                          | TCP                             |
|            | 2                          | UDP                             |
|            | 3                          | TCP&UDP                         |
| 0x5913:xx8 | Firewall: Port Range Start | Start Port Address              |
| 0x5913:xx9 | Firewall: Port Range End   | End Port Address                |
| 0x5913:x10 | Firewall: Protocol Name    | Help note for the protocol name |

With these parameters, the user can open an application port with these parameters:

## 0x5913:x10 Protocol Name

This parameter is only available to give the firewall rule a name. The customer can assign a name, which is stored in the parameter set and displayed on the tool's interface. This name is not relevant to the actual function.

## 0x5913:xx8 Port Range Start and 0x5910:xx9 Port Range End

These two parameters can be used to set the port range of the firewall rule. In special cases where start and end are the same, only a single port is addressed. By default, the port range 49,152 to 65,535 is set here. This is the range where customers should place their ports. However, the value range of these parameters is possible from 1 to 65,535. This means that, by adjusting the parameters accordingly, values in the range of the well-known or registered ports are also possible. Only port 0 is prohibited and is outside the addressable range.

It is possible that the customer selects a port for the application ports, that is already listed under well-known or registered ports. If the rules for the application port and well-known or registered ports contradict each other, the rule for well-known or registered ports leads.

## 0x5913:xx7 Protocol Type

This parameter can be used to set the log type of the rule. The following settings are offered:

- None  
The firewall rule does not refer to any protocol and is therefore inactive.
- TCP  
The firewall rule applies to TCP protocols.
- UDP  
The firewall rule applies to UDP protocols.
- TCP&UDP  
The firewall rule applies to both UDP and TCP protocols.

## i9x0.Firewall: Good to know ...

This chapter discusses some topics that are relevant for the i9x0 firewall.

## Validity of i9x0 Firewall parameters:

The prerequisite is an i9x0 with an executable application. For this purpose, a boot application must be created. Restart the i9x0. With this configuration, it is possible to describe any parameter of the i9x0 Firewall and it is effective immediately. This can be ideally used to test fire-

wall settings. These changes can be saved using the command "Save parameter sets..." so that they are available again after a restart.

### Handling IP ranges

The i9x0 checks the IP range for admissibility in the settings. Among other things, the rule that the upper value must be greater than the lower value is checked. As a result, the upper value must be entered first and, followed by the lower value..

### Exclude from the i9x0:

It is possible to deactivate the currently used protocol and the currently used communication channel and thus exclude yourself from access. There are three workarounds that can be used.

1. Connect via a different communication channel or protocol and reopen the previously closed port.
2. Connect via a different communication channel or protocol and deactivate the complete i9x0 Firewall.
3. Remove the SD card and delete the parameter set regarding the project and reinstall it.  
**Note:** The parameter set that contains the parameters of the firewall is located on the SD card under /plc/prg/PlcParameterSet/PLC\_0\_0.pprm.

### Handling of the parameter set:

Since the i9x0 Firewall parameters are part of the parameter set, they are subject to the same mechanisms that apply to the parameter set itself. This means that they are included in both the PLC Designer project and the Application Loader Package. They are displayed in difference lists and can also be used and changed by the EASY Starter if it has passed authentication for the i9x0.

### Philosophy of Default Assignment

The philosophy for the default assignment of the i9x0 Firewall parameters is as follows: Rules for the ports:

1. By default, the i9x0 Firewall is deactivated and must be activated.
2. In general, all ports are closed by default and must be opened.
3. An exception are the ports for a PLC Designer at the interface of the engineering port.
4. An exception are the ports that are required within the production for the production of the components.

For more information about the ports with deactivated firewall and activated firewall with default parameter [i9x0.Firewall:PortList](#)

### Prioritization of i9x0 Firewall Rules:

The rules of the i9x0 Firewall are applied as follows:

1. All ports are closed.
2. The ports in the Well-Known area are opened according to the settings.
3. The ports in the Registered area are opened according to the settings.
4. The ports in the Application area are opened according to the settings.
5. If the settings of the first two areas contradict each other with the application area, the rule of the first two areas counts.

# i9x0 servo inverters

i9x0.SecureFactoryReset

---

## Using http via Port 80 or via Port 8080

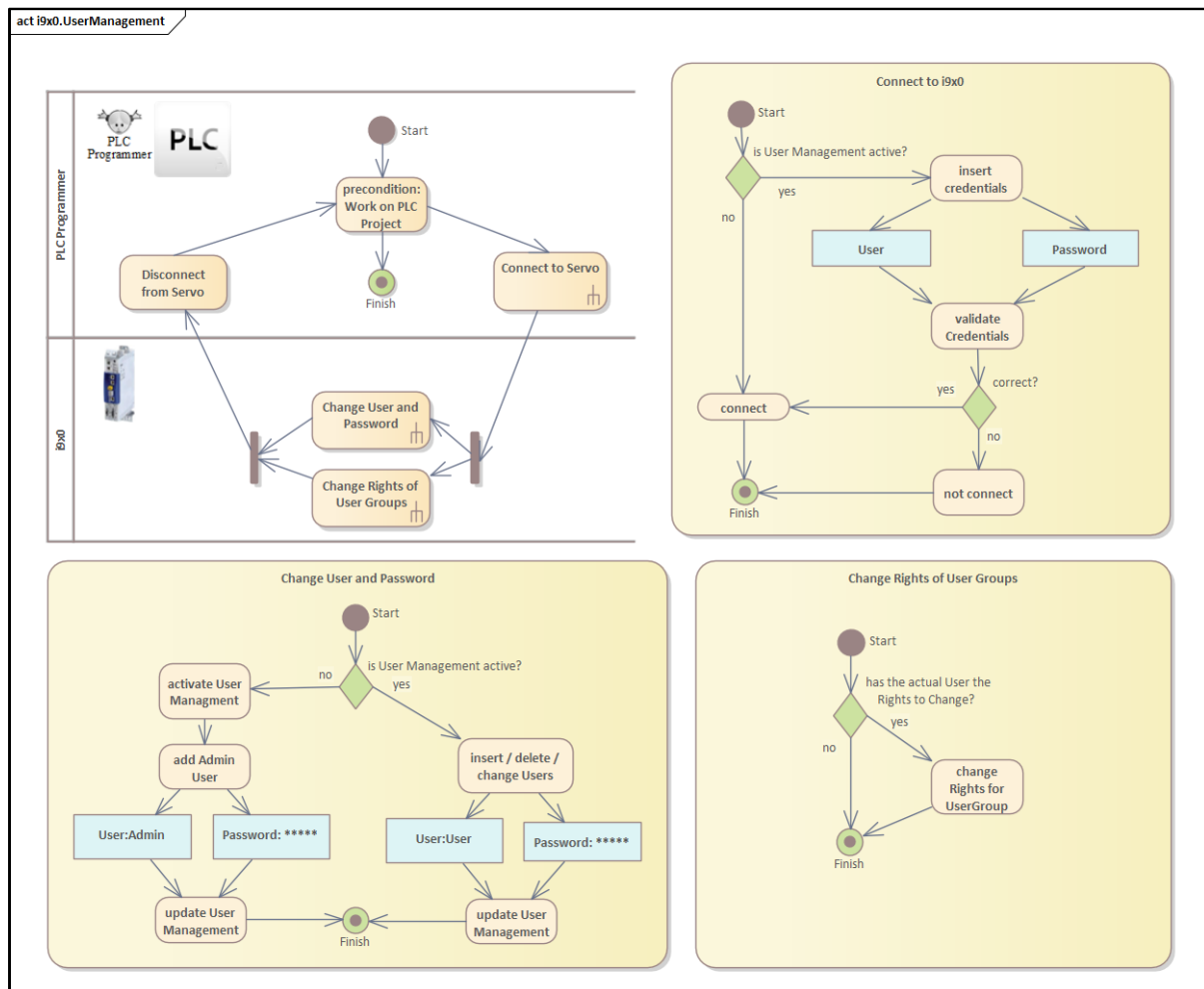
Port tcp/80 on the i950 is intended for http communication in order to access the Free and Open Source Software (FOSS) list. This port is active by default and can be deactivated via the firewall for further hardening.

Port tcp/8080 on the i950 Servo Inverter is only intended for the extended version with integrated WebVisu. This port is deactivated by default and must be opened for use via the firewall using the application parameters 0x5913.

## i9x0.UserManagement

i9x0.UserManagement has been available in firmware versions V2.x release.

To implement i9x0.UserManagement, the »PLC Designer« offers a user management administration for the i9x0 runtime. Once enabled on the i9x0, an anonymous online connection cannot be established with the device. This can be used, for example, to avoid accidentally overwriting a PLC program or transferring it to the wrong i9x0.



Activity Diagram

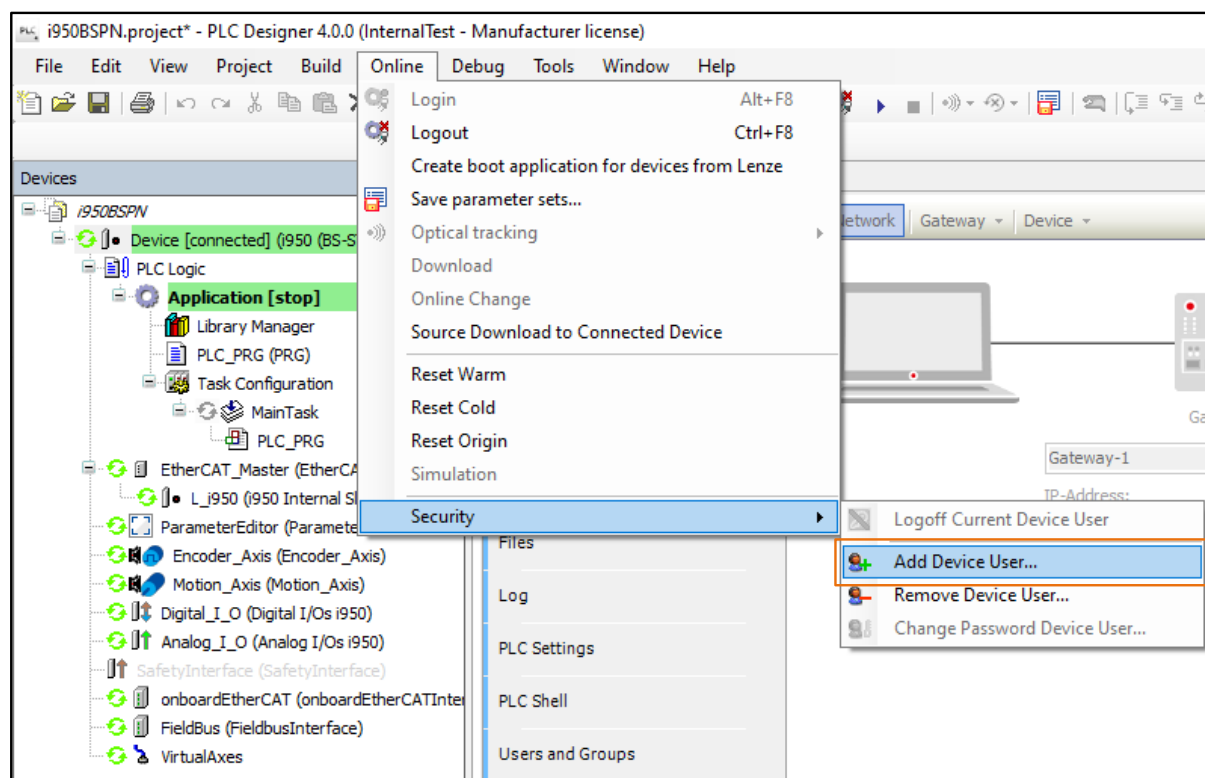
### i9x0.UserManagement: Activating

To activate user management, the PLC Designer must be connected online to the i9x0. Select the setting

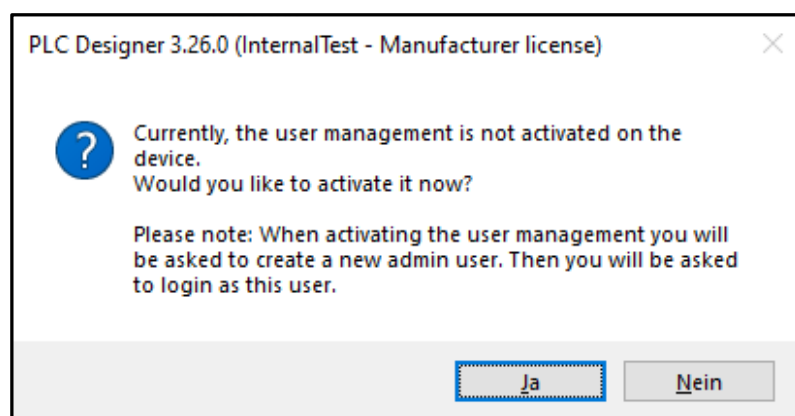
Menu / Online / Security / User Login ...

# i9x0 servo inverters

i9x0.SecureFactoryReset

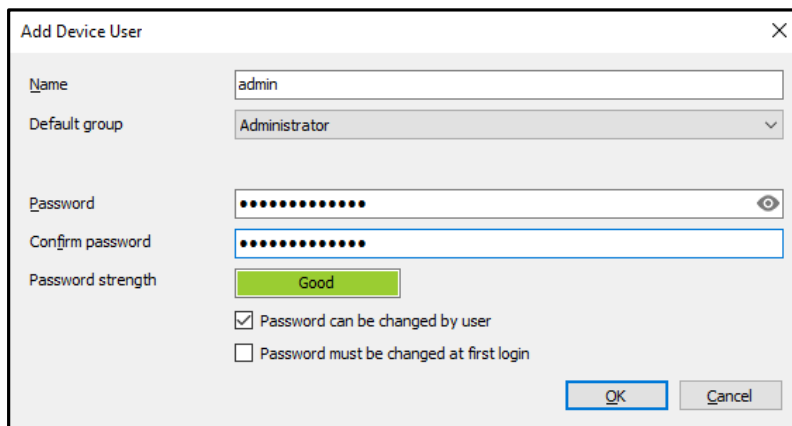


Add Device User



Activate user management

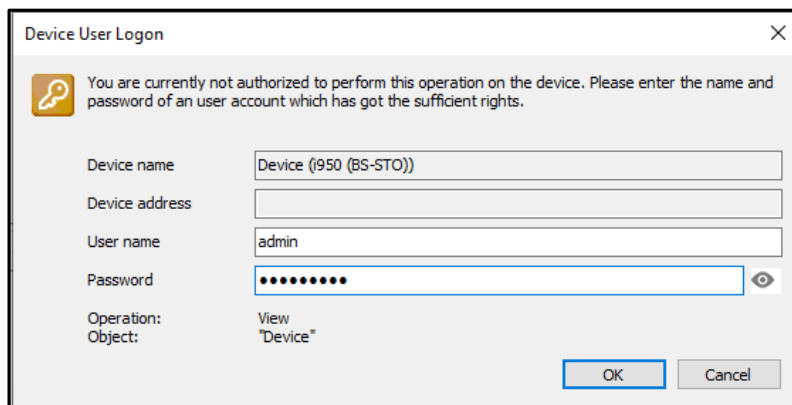




The 'Add Device User' dialog box contains the following fields and options:

- Name:** Text field with 'admin' entered.
- Default group:** Dropdown menu showing 'Administrator'.
- Password:** Password field with masked characters.
- Confirm password:** Password field with masked characters.
- Password strength:** A green bar labeled 'Good'.
- ☒ Password can be changed by user
- ☐ Password must be changed at first login
- Buttons:** 'OK' and 'Cancel' at the bottom right.

Add Device User Dialog



The 'Device User Logon' dialog box contains the following fields and options:

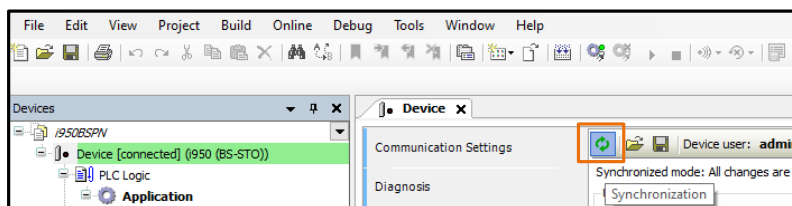
- Message:** 'You are currently not authorized to perform this operation on the device. Please enter the name and password of a user account which has got the sufficient rights.'
- Device name:** Text field with 'Device (i950 (BS-STO))' entered.
- Device address:** Empty text field.
- User name:** Text field with 'admin' entered.
- Password:** Password field with masked characters.
- Operation:** 'View'
- Object:** 'Device'
- Buttons:** 'OK' and 'Cancel' at the bottom right.

Device User Logon

### i9x0.UserManagement: Change Users and Groups

To manage the users, first synchronize the user management, with:

Device Tree / Project / double-click on Device / Menu Users and Groups / Synchronization



Synchronization

Adding a user is accessed via the Add... option. Select from the following roles: roles { Administrator | Developer | Service | Watch }. If additional roles are to be created, they can also be created with Add... or deleted with Delete.

### i9x0.UserManagement: Groups

- **Administrator:**  
When you log in to the device for the first time, you will be instructed to activate the device user administration and then create a user in the Administrator group. As this user,

# i9x0 servo inverters

i9x0.SecureFactoryReset

you can set up additional users and groups and assign access rights.

- Anonymous:  
Group has read-only authorization for the parameter set.

The following parameter can be used to read out the currently associated security group that belongs to this session and is active.

| Address    | Name                                      | Info                                                                                     |
|------------|-------------------------------------------|------------------------------------------------------------------------------------------|
| 0x5905:004 | Security user settings: Access Group Name | The currently active security group (e.g. Administrator or Anonymous) is displayed here. |

| Address    | Name                                                         | Info |
|------------|--------------------------------------------------------------|------|
| 0x5905:011 | Security user settings: Activate selection of security level |      |

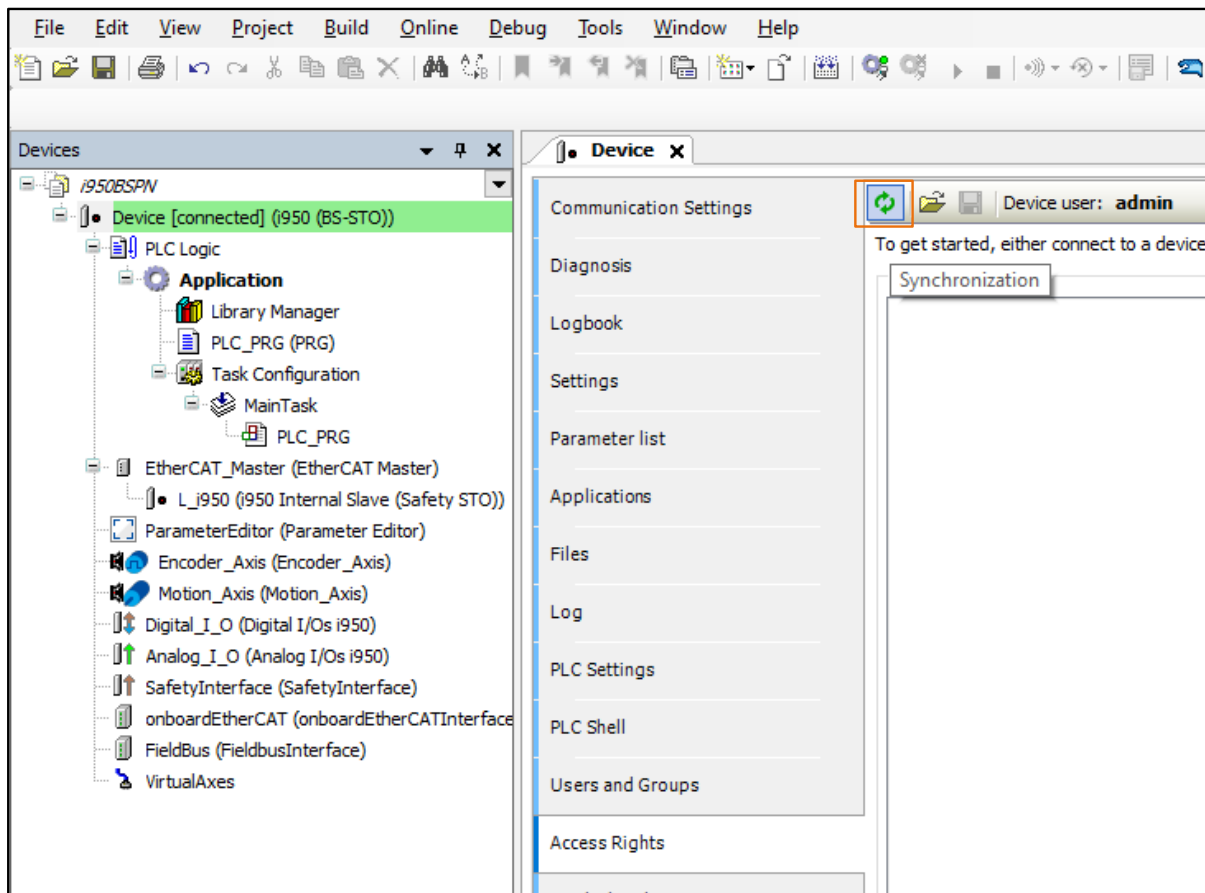
| Address    | Name                                                | Info |
|------------|-----------------------------------------------------|------|
| 0x5905:012 | Security user settings: Selection of security level |      |

| Address    | Name                                              | Info |
|------------|---------------------------------------------------|------|
| 0x5905:003 | Security user settings: Status active user rights |      |

## i9x0.UserManagement: Change Access Rights

To manage the Access Rights, first synchronize the user management, with:

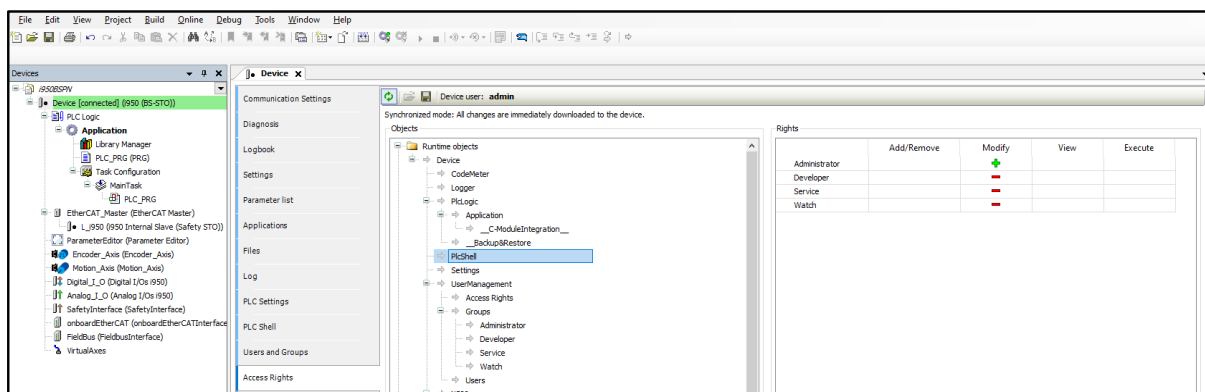
Device Tree / Project / double-click on Device / Menu Users and Groups / Synchronization



Synchronize Access Rights

To manage the access rights to the objects, the following setting option is available.

Device Tree / Project / double-click on Device / Menu Access Rights



Setting the Access Rights

For each node, the setting of the authorization can be set here.

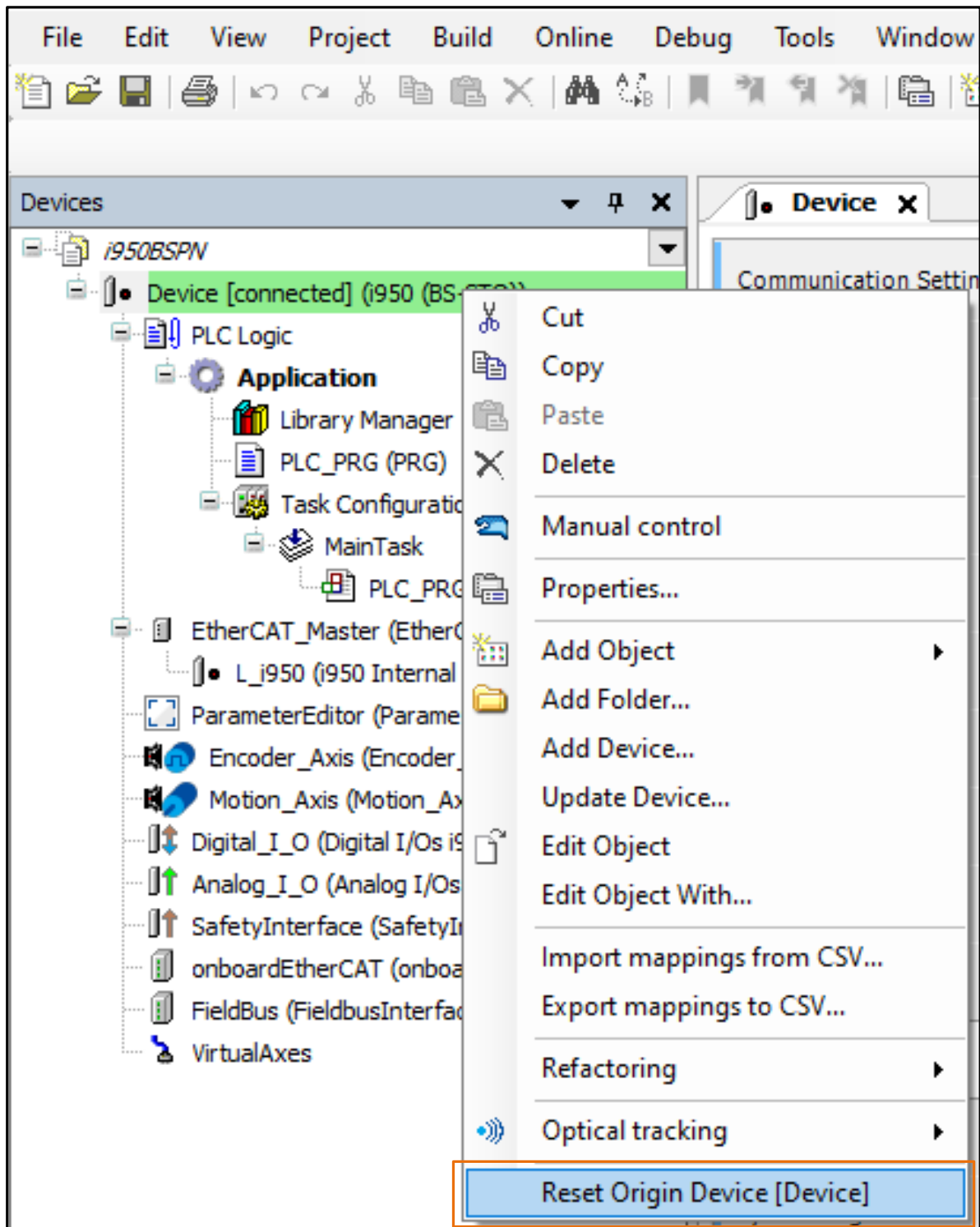
The Administrator group has a special feature. The settings can be changed in the interface, but the group basically receives all rights.

# i9x0 servo inverters

i9x0.SecureFactoryReset

## i9x0.UserManagement: Remove

To remove the user management (note: all users, groups and access rights will be removed) right-click on the i9x0 device in the device tree of the PLC project and execute the 'Reset Origin Device' for the User Management.



Reset Origin Device [Device]

### Access Rights

In the »PLC Designer«, the object "Runtime objects / Device / RemoteConnections / EngineeringInterface" object can be set under the "Access Rights" tab. Only the "Modify" rights can be set here. With this setting, the above access can be consented to or not.

### Anonymous login

In the settings under 'Communication Settings / Device / Change Communication Policy' there is a selection in the 'Device User Management' category called, 'Allow anonymous login'. This setting affects the OPC UA server. If anonymous login is prohibited, the user "Anonymous\_OPCUAServer" and the group "Anonymous\_OPCUAServer" will be deleted in the i9x0.UserManagement.



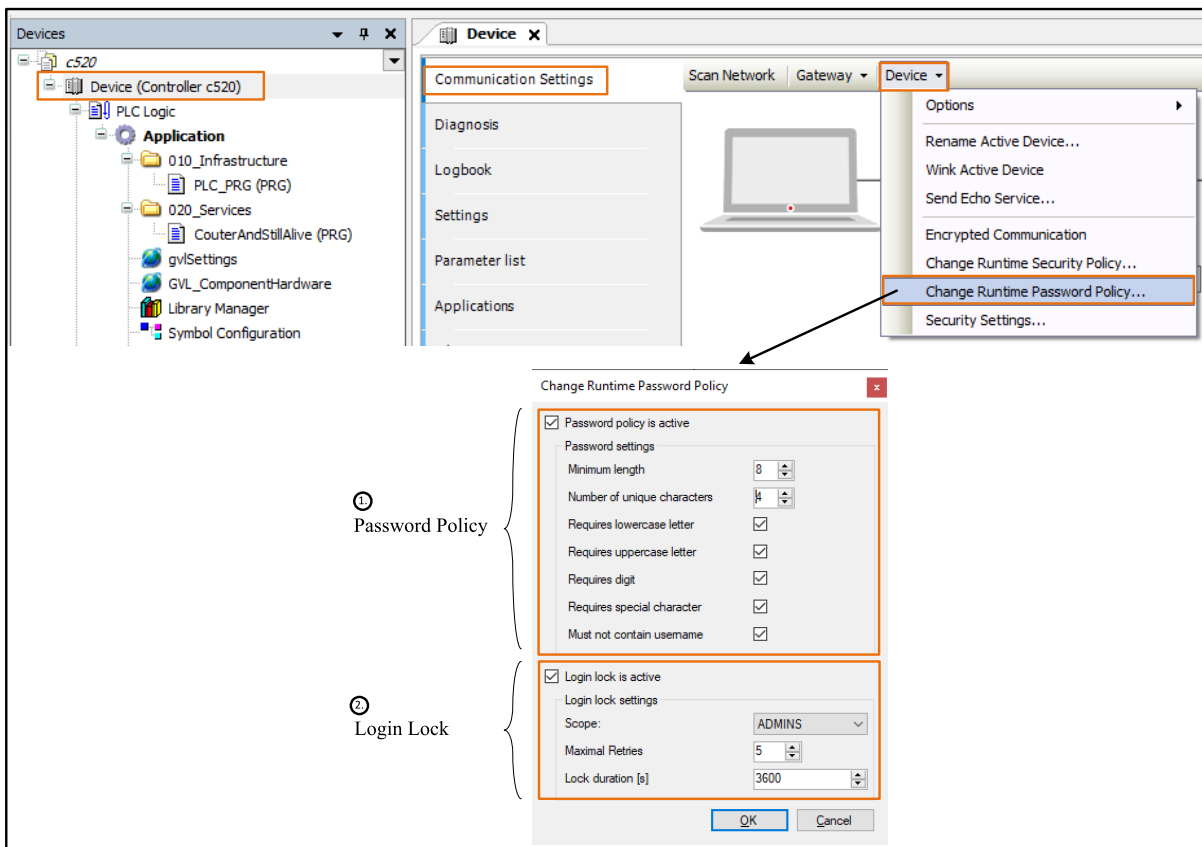
Please do not add a new user to the 'Anonymous\_OPCUAServer' group. The reason is as follows. If anonymous login is prohibited, the user "Anonymous\_OPCUAServer" and the group "Anonymous\_OPCUAServer" will be deleted. This means that the connection to the previously created user will be lost and he is left alone.

### i9x0.UserManagement: Runtime Password Policy

The Runtime Password Policy has been available since i9x0 firmware version 2.0.0 in combination with PLC Designer 4.0.0. The User can activate the Runtime Password Policy, by clicking on the device in Device-Tree / Communication Settings / Device / Change Runtime Password Policy. Now, the settings for the policy of the device, in this case the controller, can be done.

# i9x0 servo inverters

i9x0.SecureFactoryReset



i9x0 Runtime Password Policy

In the section `Password settings` the user can specify the minimum requirements of the passwords.

- Minimum length  
Minimum length of password characters (all characters count, whether they are letters, numbers, special characters).
- Number of unique characters  
Minimum number of different unique characters.
- Requires lowercase letter  
{ a-z, ä, ö, ü, ß }
- Requires uppercase letter  
{ A-Z, Ä, Ö, Ü }
- Requires digit  
{ 0-9 }
- Requires special character  
{ ^, °, !, ", \$, %, &, /, (, ), =, ?, ` , {, [ , ] , \, ' , +, \*, ~, #, ' , - , \_ , . , : , ; , < , > , | , @ , € , μ }
- Must not contain username  
The username string is not allowed in the password.



Activating or changing the password policy settings will take effect immediately. However, the changes only apply to the assignment of new passwords. Existing passwords remain valid, even if they do not comply with the policy.

In the section `Login Lock settings` the user can specify the lock after unsuccessful logins.

- 
- Scope  
ADMINS: The Login Lock settings are valid for all users in the Administrator Group.  
NONADMINS: The Login Lock settings are valid for all users except Administrators.  
ALL: The Login Lock settings are valid for all users.
  - Maximum Retries
  - Lock duration [s].  
Lock duration for this locked users in seconds.

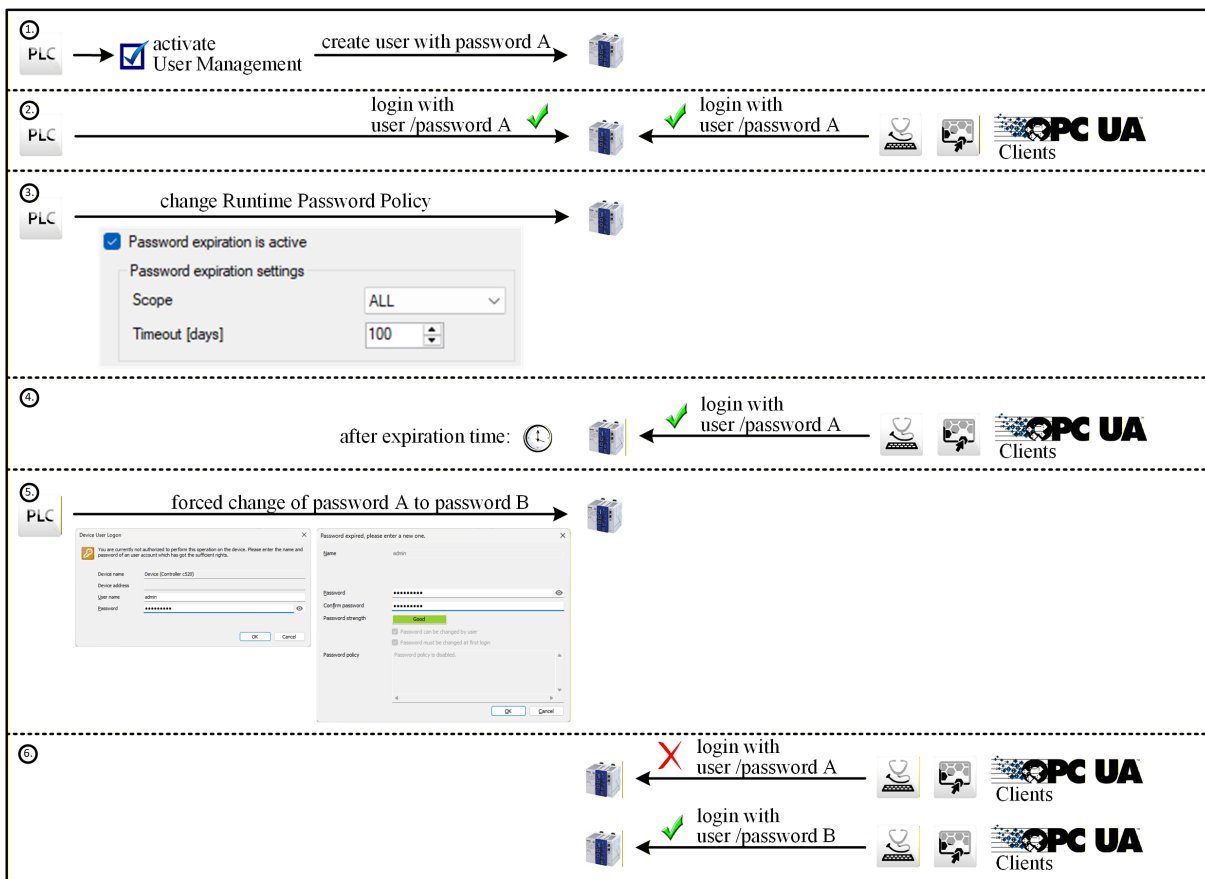


If a user attempts to log in unsuccessfully a maximum number of times, their account will be locked. The login options of other users will remain unaffected.

### i9x0.UserManagement: Password Expiration

The Runtime Password Expiration is available since Controller Firmware Version V2.0.0 in Combination with PLC Designer 4.1.0. The User can activate the Runtime Password Expiration, with Click on Device in Device-Tree / Communication Settings / Device / Change Runtime Password Policy. Now the settings for the Policy of the Device, in this case the Controller, can be done. This function is deactivated by default.

- Scope:
  - ADMINS: Password Expiration is valid and active for all admin-Users.
  - NON-ADMINS: Password Expiration is valid and active for all non-admin-Users.
  - ALL: Password Expiration is valid and active for all Users.
- Timeout [days]:
  - 1 ... 1000 days for valid password until forced password renewal.



i9x0 Runtime Password Expiration

The following sequencer describes the mechanism:

- ( 1 ) Firstly, user management must be activated on the device (in this case the i9x0 Servo Inverter) by the PLC Designer. A first user with example password A must be assigned.
- ( 2 ) The user can then log in with user and his password A using PLC Designer or other communication channels.
- ( 3 ) If desired, the Runtime Password Policy can be activated.
- ( 4 ) After the set time has elapsed, all other communication channels can continue to log in with the known user and password A. These other communication channels can be, for example, the EASY Starter, the EASY Firmware Loader or the EASY Application Loader.



- 
- ( 5 ) The next time the user attempts to log in using the PLC Designer, they will be prompted to change the password.
  - ( 6 ) Once the password has been changed, this password is also valid for the other communication channels.

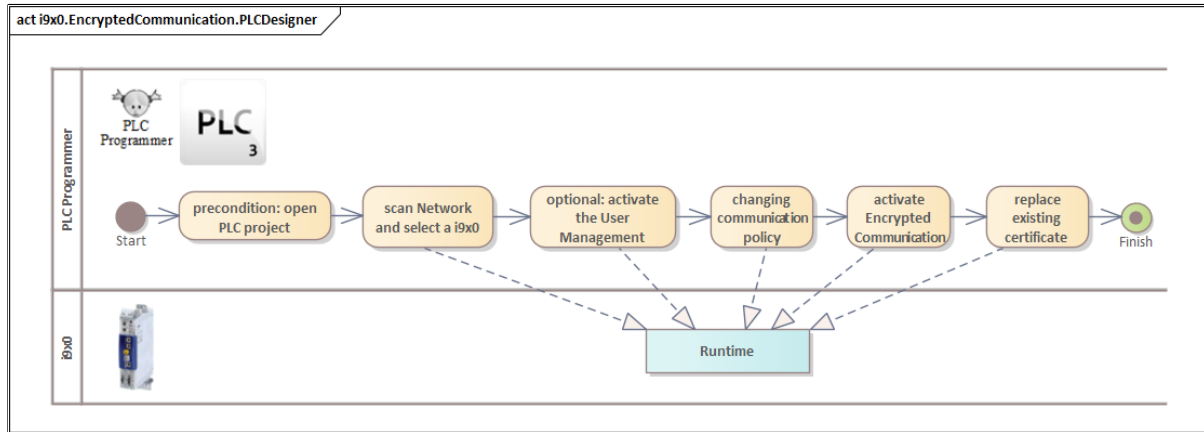
# i9x0 servo inverters

i9x0.SecureFactoryReset

## i9x0.EncryptedCommunication.PLCDesigner

This functionality has been available from versions 2.0.0 on.

For communication between PLC Designer via the gateway to the device, the connection should be encrypted. This is shown in the following image.



Activity Diagram

### Scan Network and select a i9x0:

To establish a connection please follow these steps:

- Open the »PLC Designer« project or generate a new project in the »PLC Designer«.
- In the Device Tree, double-click the Device, e.g. i9x0 servo inverters.
- Open the Communication Settings tab.
- Scan Network and select the i9x0.

### Optional: Activate the user management

Activate the User Management ([i9x0.UserManagement](#)).

### Changing Communication Policy

The screen to change the communication policy is located in the "Communication Settings" tab within the "Device" menu and "Change Runtime Security Policy ...".

**Change Communication Policy**

**Communication**

Current policy: Optional encryption

New policy: Optional encryption

The device supports both encrypted and unencrypted communication. This can be decided by the user.

**Device User Management**

Current policy: Optional user management

New policy: Optional user management

The user management is optional on the device. It is up to the user to activate the user management or leave the device unprotected.

☒ Allow anonymous login

If anonymous login is activated, certain registered components (e.g. OPC UA) can establish a connection without providing credentials even if user management is enabled.

OK Cancel

Change Runtime Security Policy

### Communication

The device (in this case the Servo Inverters) supports both encrypted and unencrypted communication. The user can decide if the communication policy is:

- "No encryption"  
Then the i9x0 accepts only unencrypted communications. In this case the PLC Designer has to communicate in clear text.
- "Optional encryption"  
Then the i9x0 accepts both, encrypted or unencrypted communications. In this case the user of the PLC Designer can decide if the tool will communicate in clear text or encrypted.
- "Enforced encryption"  
Then the i9x0 accepts only encrypted communications. In this case the PLC Designer has to communicate in encrypted communication.

### Device user management

The User Management is optional on the device. It is up to the user to activate the user management or leave the device unprotected:

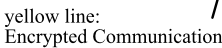
- "Optional user management"  
If a new project is generated, the user management is deactivated. The user management can be activated by the user ([i9x0.UserManagement](#)).
- Enforced user management

## i9x0.SecureFactoryReset

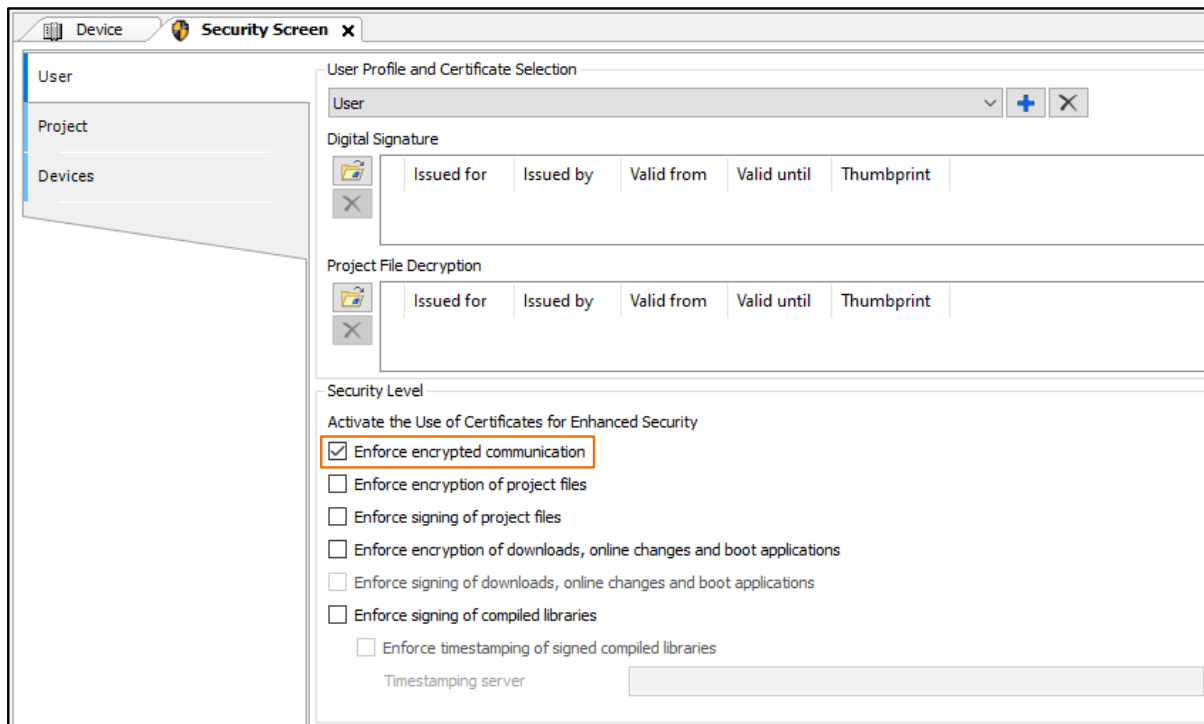
With the setting 'Allow anonymous login', the anonymous login can be prevented ([i9x0.U-serManagement](#)) for more details.

There are two ways to activate the encrypted communication:

- The menu item to activate the encrypted communication is located in the 'Communication Settings' tab within the menu 'Device' and 'Encrypted Communication'. If the 'Encrypted Communication' is active, the communication line between the PLC Designer and the i9x0 is marked with a yellow line.



- The second way is to use the Security Screen. The Security Screen is located in the PLC Designer Menu 'View / Security Screen'. Within the 'User' tab the 'Enforce encrypted communication' checkbox can be found.



Enforce Encrypted Communication



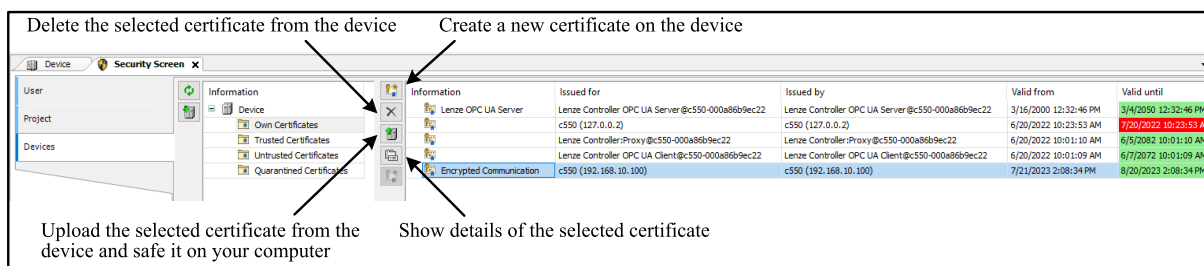
The Device / Encrypted Communication setting defines communication on the part of the PLC Designer.

The Communication Policy setting defines communication on the part of the i9x0 servo inverters.

This can, for example, lead to the situation where the i9x0 servo inverters is set to forced encryption and the PLC Designer requests clear text communication. The error message "No encryption is not supported by the device" appears.

### Using Encrypted Communication

After activating the 'encrypted communication' there will be a certificate for it in the i9x0 Certificate Store. The Security Screen is located in the PLC Designer Menu 'View / Security Screen'. Within the tab 'Devices / <Name of Device> / Own Certificates' this certificate can be found with the Information ,Encrypted Communication'.



Certificate for Encrypted Communication

# i9x0 servo inverters

i9x0.SecureFactoryReset

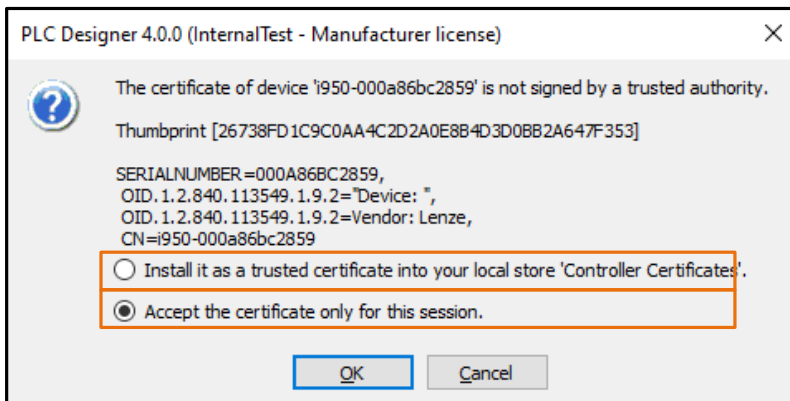
Details of this automatically generated certificate can be found in this documentation:  
([i9x0.EncryptedCommunication.PLCDesigner:Certificate](#))



The automatically generated certificate has a valid time of 30 days. It is strongly recommended to recreate this certificate with the desired term and key lengths.

For the encrypted communication between PLC Designer and the i9x0, the PLC Designer has to trust the Certificate of the i9x0. There are two ways to do this:

The first way is to login the PLC Designer to the i9x0 with activated 'Encrypted Communication'. The following message box will appear and the user can decide, if the Certificate is only used this time or for all sessions:



Login

## Accept the certificate only for this session

The certificate of the i9x0 is used for this session and the connection is established. After the connection is completed and the user logs in again, the message box appears again.



What is **not** a session in this case?

- Stop and Start the Application.
- Reset Warm
- Reset Cold
- Reset Origin
- Logout and Login
- "Security/Logoff Current User" and Login
- "Security/Logoff Current User", close project, open project, login

What is a session in this case?

- Closing the »PLC Designer« and starting the »PLC Designer« again.

## Install it as a trusted certificate into your local store "Controller Certificates":

The certificate of the i9x0 is stored in the Windows Certificate Store. This can be found under Controller Certificates. It is used for this connection and for all subsequent connections as long as the fingerprint of the certificate matches.

For more information about the Windows Certificate Store:

- [Security Strategy](#)
- [Integrate a certificate in the windows certificate store](#)

The second way is using the Security Screen with a logged- in PLC Designer to the i9x0. To do this, follow the steps below:

1. Open the Security Screen in the PLC Designer Menu 'View / Security Screen'. Within the tab 'Devices / Device / Own Certificates' the certificate for the encrypted communication is shown.
2. Click on the 'Encrypted Communication' certificate and push the button 'Upload the selected certificate from the device and save it on your PC'. Choose an directory and save the certificate. The certificate name will be the i9x0 type combined with the IP address, e.g., 'i9x0 (192.168.10.100)'. The file format will be '\*.cer'.



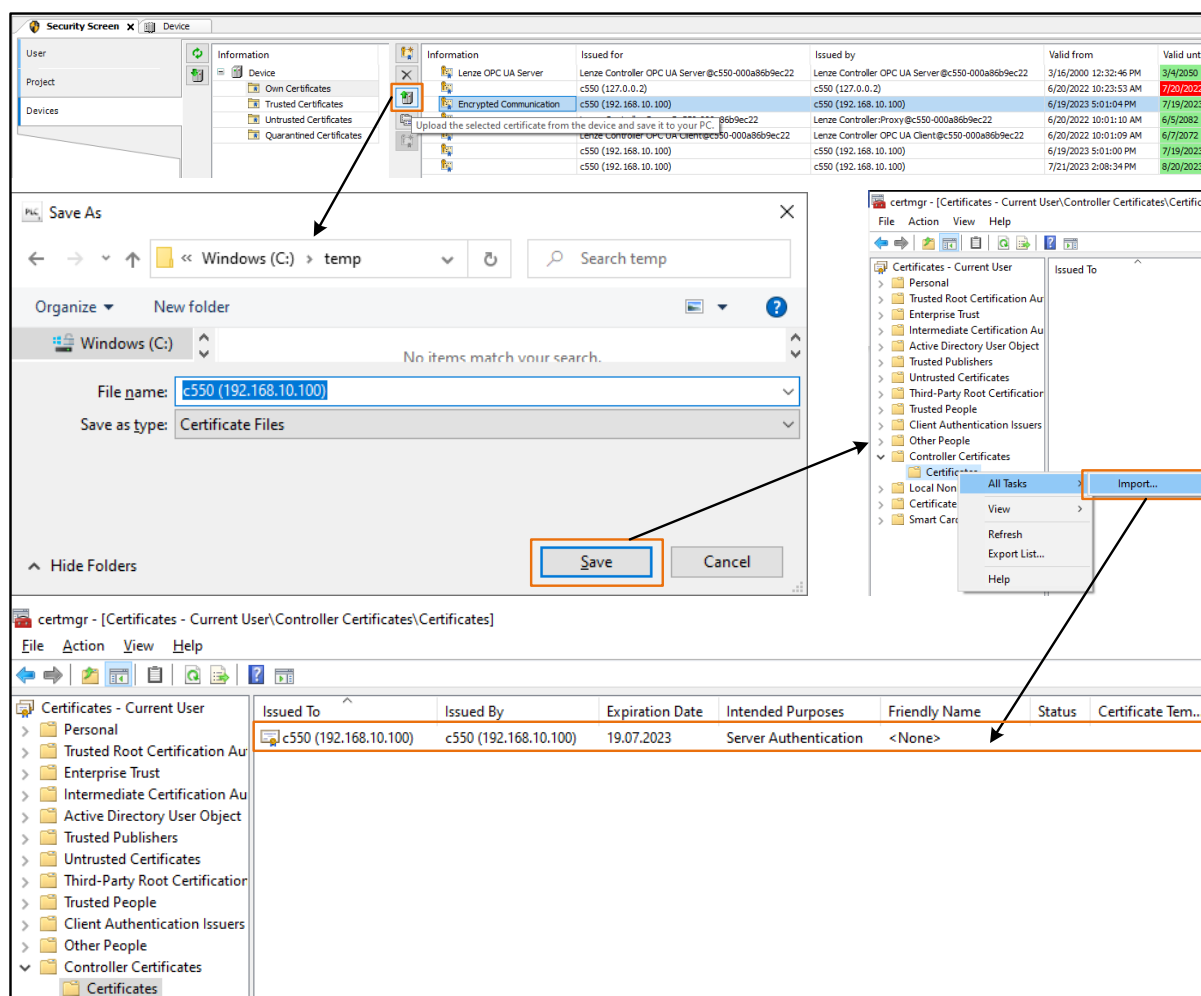
The format of this certificate is \*.cer. It will include the public key for the encrypted communication, but of course not the private key.  
For more information see [Formats and Structures of certificates](#).

3. Open the Windows Certificate Store with the command ,certmgr.msc'. Select the directory, Controller Certificates/Certificates' and import the certificate from the uploaded file.

# i9x0 servo inverters

i9x0.SecureFactoryReset

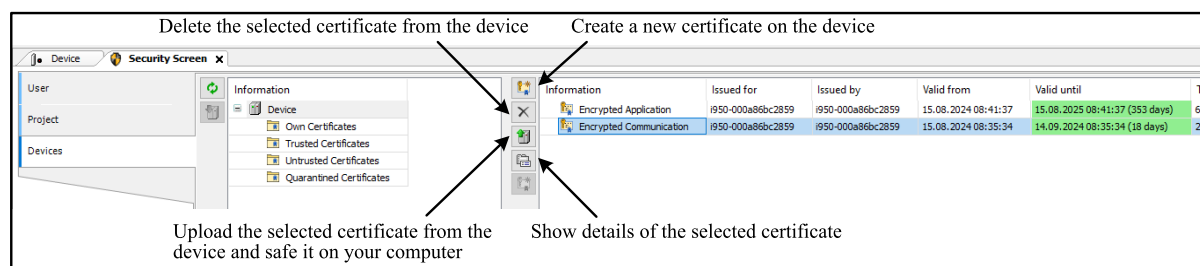
4. After the import, the certificate is shown in this directory and the PLC Designer will use it for every connection to this i9x0 without asking for trust.



Upload and Import Certificate

## Replace existing Certificate

To replace an existing certificate, for example to extend the valid dates, the certificate can be replaced via the Security Screen. The Security Screen is located in the PLC Designer Menu 'View / Security Screen'. Within the tab 'Devices / <Name of Device> / Own Certificates' this certificate can be found with the information 'Encrypted Communication'.



Certificate for Encrypted Communication

Delete the selected certificate from the device:



---

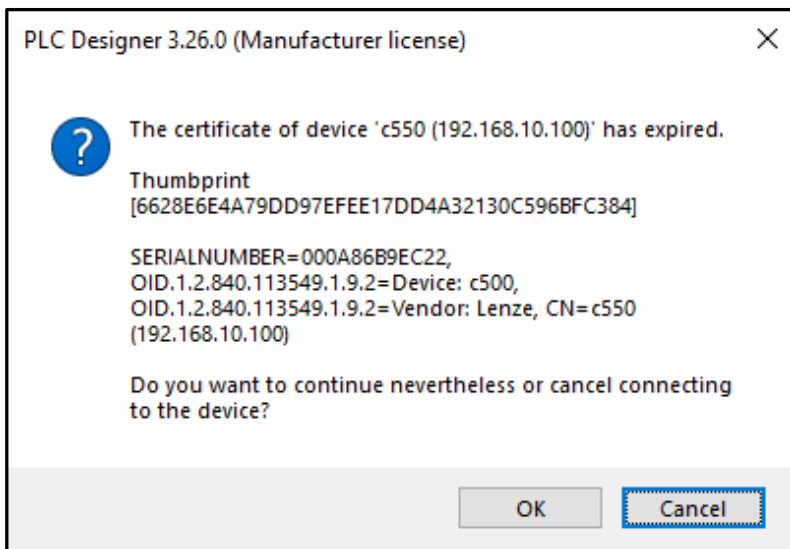
Deleting the "Encrypted Communication" certificate will automatically generate a new one with default values. ([i9x0.EncryptedCommunication.PLCDesigner:Certificate](#))

#### Create a new certificate on the device

By clicking the "Create a new certificate on the device" button, the user can generate a new certificate and enter the desired key length and validity period.

#### Good to know ... : Using expired Certificates

If the certificate for encrypted communication is no longer valid and the PLC designer logs into the i9x0, a warning will appear.



Valid Warning

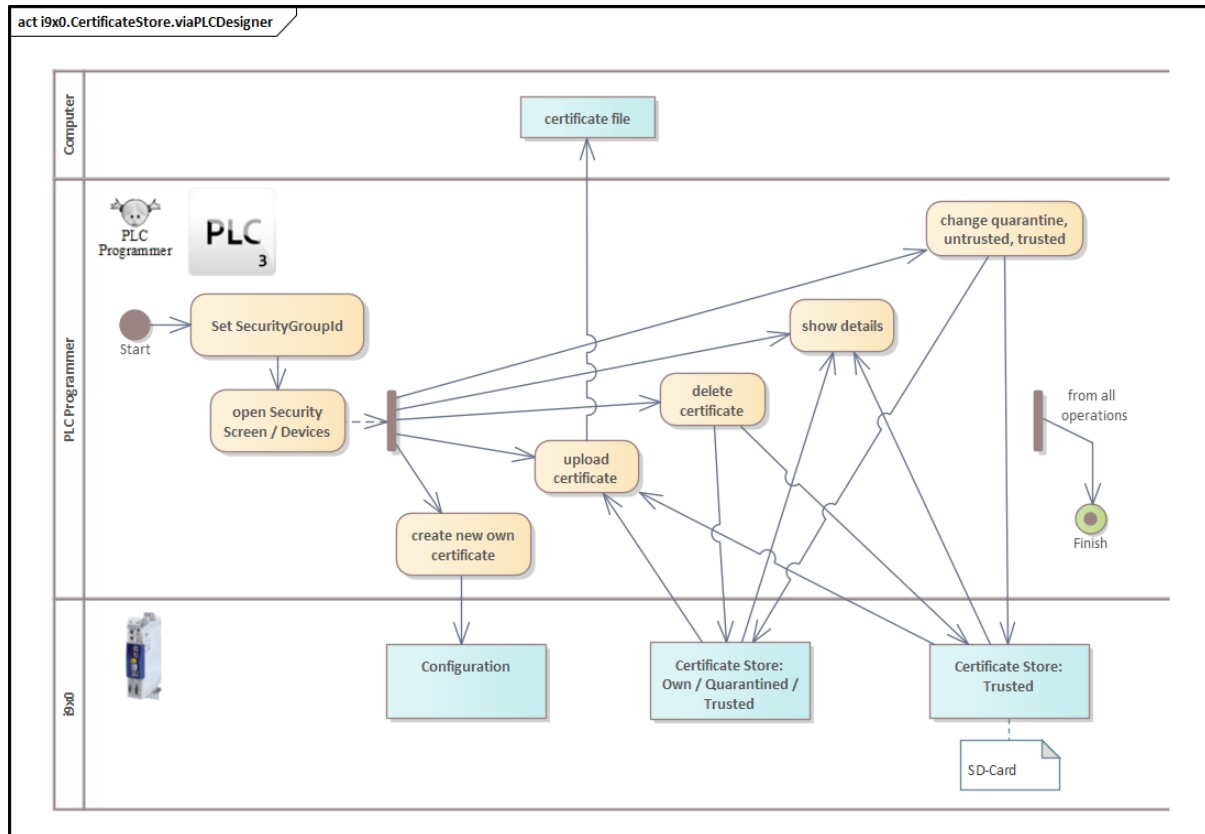
The user can decide whether to cancel or use the expired certificate.

# i9x0 servo inverters

i9x0.SecureFactoryReset

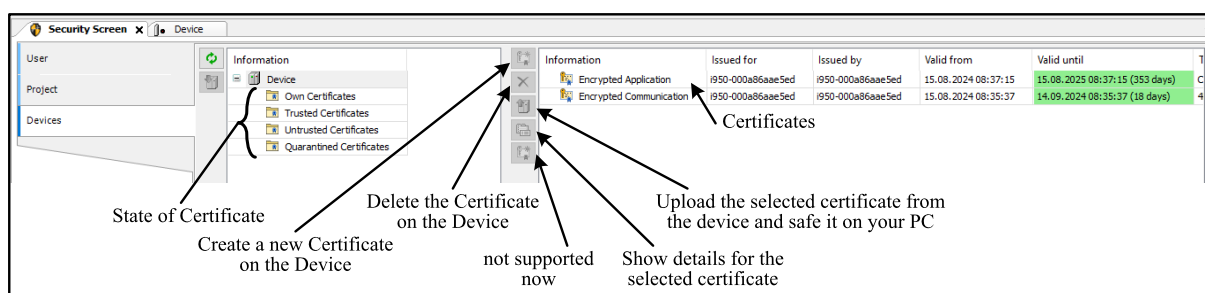
## i9x0.CertificateStore.viaPLCDesigner

The i9x0 Servo Inverter from version 2.0.0 on, has its own Certificate Store. This can be managed and controlled via the PLC Designer.



Activity Diagram

To do this, open the Security Screen with the "Devices" tab.



Security Screen Devices

In the middle window, the respective status of the certificates can be selected under Information. The following four status are available:

- **Own Certificates:**  
Own certificates of the i9x0
- **Trusted Certificates:**  
Certificates from trusted communication partners

- 
- **Untrusted Certificates:**  
Certificates from untrusted communication partners
  - **Quarantined Certificates:**  
Certificates from communication partners who are in quarantine

To change a certificate's status, simply drag and drop it from the right window to the desired status. The following certificate usage options are available:

#### Create a new certificate on the i9x0

For this purpose, an existing own certificate or a placeholder, i.e. a certificate with the note (not available) must be selected and the button must be pressed. Subsequently, the desired key length and validity can be specified and the certificate can be created.



If a certificate A exists and another certificate B is created, the certificate with the longer valid time is used, even if it is certificate A. If the 'Own Certificate' area is called up, both A and B certificates are displayed. If you want to replace certificate A with certificate B, you should first delete certificate A and then create certificate B.

#### Delete the Certificate on the Device

To do this, select a certificate and press the button. It is important that the certificate is deleted and not moved to "Untrusted Certificates". To do this, select a certificate and press the button. It is important that the certificate is deleted and not moved to 'Untrusted Certificates'.

#### Upload the selected certificate from the device and save it on your PC

For this purpose, a certificate must be selected and the button must be pressed. It is important that the respective certificates are loaded onto the PC with the public key. The private key remains on the i9x0 servo inverter.

#### Show details for the selected certificate

For this purpose, a certificate must be selected and the button must be pressed. A window opens where the details of the certificate can be viewed.

#### Initial Certificates

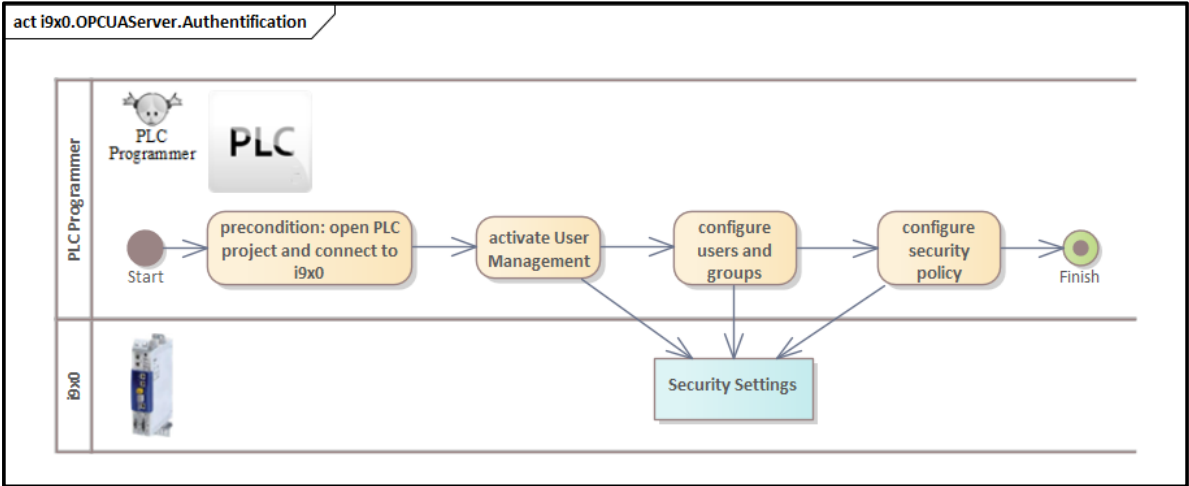
When the i9x0 boots, some certificates will be generated automatically. This happens for the first time when these devices are produced in manufacturing. Since no time has been set in the i9x0 for this production step and since there is no communication via an NTP connection, the certificates are created with a initial time stamp far in the past. After the devices are sent to the customer, they are switched on again.

When logging into the i9x0 with PLC Designer, a pop up dialog informs that some certificates are expired. On the security screen, the expired (validity date in the past) or inactive (empty information field) certificates can be checked. Expired or inactive certificates can be deleted. New certificates will either be generated automatically during the next boot or can be created manually via the security screen.

**i9x0.OPCUAServer.Authentication**

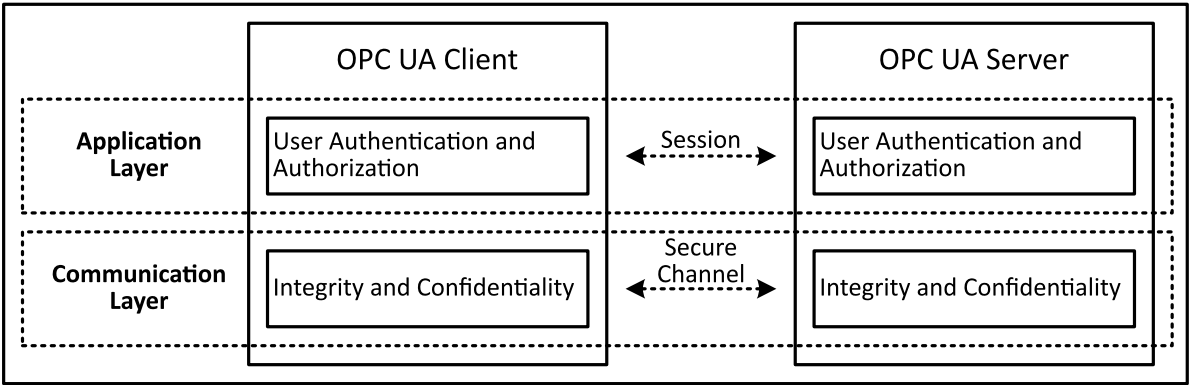
In order to be able to use the authentication of the OPC UA Server, the i9x0 User Management is required. The activation of this is described in chapter [i9x0.UserManagement](#).

The following diagram shows the process.



Activity Diagram

In order to establish a connection to the OPC-UA Server, an OPC-UA Client must use the end-point url and take the corresponding security settings into account. The architecture of OPC-UA provides for a secure channel and a session. Confidentiality and integrity are secured for the Secure Channel and authentication and authorization for the session.



Security Channel and Session

These security settings are described below. Here, the Security Policy and the Message Security Mode are used for the Secure Channel configuration and the authentication for the session.

**Security Policy**

When the connection between OPC UA Client and OPC UA Server is started, the security policies are transmitted by the server. Within this Cipher Suite, the OPC UA Client can select a suitable connection. Several settings are usually offered here, such as Basic256Sha256.

### Message Security Mode

The Message Security Mode specifies the type of transmission. Here the selection None, Sign and Sign & Encrypt is offered.

- None  
Does not include security mechanisms and should only be used for test facilities and therefore not for productive operation.
- Sign  
Includes security mechanisms to ensure integrity.
- Sign & Encrypt  
Includes security mechanism to ensure integrity and confidentiality.

### Authentication

In authentication, the user is associated with the session. The following three settings are possible.

- Anonymous  
No dedicated user is used for the session, but the connection is created anonymously.
- Username and Password  
A user must identify himself with username and password and will be associated with the session.
- Certificate and Private Key  
Authentication of a user with the help of certificates. Not currently supported.

### Authenticate an OPC-UA Client without an activated user management

In the following, the connection to the OPC-UA Server is described without user management being activated on the i9x0. An OPC-UA Client can connect without having to authenticate the user.



In the »PLC Designer«, the following setting option exists for the device: Device > Communication Settings > Device > Change Runtime Security Policy ... > [Check-box] Allow anonymous login. Without an activated user management, the following setting in the PLC Designer has no effect, i.e. when deselecting Allow anonymous login, an anonymous connection is possible.



If an OPC-UA Client with a username and password authentication connects to the OPC-UA Server without active user management, a connection is generally possible. Neither the username nor the password is checked, as there is no activated user management with corresponding data. The connection is therefore synonymous with anonymous authentication.

### Authenticate an OPC-UA Client with activated user management

With an activated user management, an OPC-UA Client can connect in two authentication modes:

- Anonymous  
No dedicated user is used for the session, but the connection is created anonymously.
- Username and Password  
A user must identify himself with Username and Password and will be associated with the session.

- Certificate and Private Key  
Not currently supported.

## Anonymous

Regardless of the user in the user management, OPC-UA Clients can connect anonymously with this authentication mode, if allowed by the OPC-UA Server.

## Username and Password

If the OPC-UA Client selects the authentication mode Username and Password, these must match a user in the user management to establish a connection. To restrict the user access to specific symbols the usage of symbol sets and the symbol rights configuration are required. Otherwise, all users can access all symbols. If the user does not exist or the password does not match, a connection is refused.

## Prohibit anonymous login

To prohibit the Anonymous Login, please use the setting option in the »PLC Designer« for the device: Device > Communication Settings > Device > Change Runtime Security Policy ... > [Checkbox] Allow anonymous login. With an activated user management, this checkbox can be used to deactivate the Anonymous Login.

If an OPC-UA Client now wants to connect via Anonymous, this is prohibited. If an OPC-UA Client wants to connect to the authentication mode Username and Password, and these match a user in the user management, the connection is allowed.

## Delete user Anonymous\_OPCUAServer

The following procedure is provided for informational purposes only and is not recommended. In order to prohibit an anonymous connection of an OPC-UA Client, the previously described method should be used.

If user management is activated, an Anonymous\_OPCUAServer user is automatically created. This can be permanently removed manually.

If an OPC-UA Client now wants to connect via Anonymous, this is prohibited. If an OPC-UA Client wants to connect to the authentication mode Username and Password, and these match a user in the user management, the connection is allowed.



If you want to restore the user Anonymous\_OPCUAServer after deleting it, there are two options. The first is to delete the complete user management on the SD card from the controller. Afterwards, user management must be activated via the »PLC Designer«. This step restores the previously manually deleted user Anonymous\_OPCUAServer. Previously created users and groups must be rebuilt manually. The second option is to disable and re-enable the Allow anonymous log in setting. As a result, the user is Anonymous\_OPCUAServer created again.

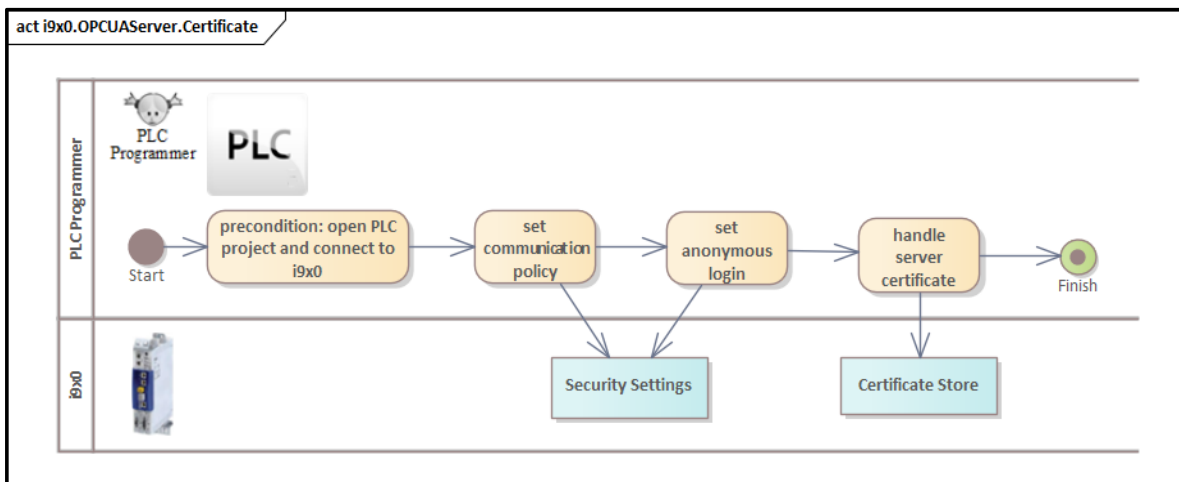
## i9x0.OPCUAServer.Certificate

The OPC UA Server offers the following message security modes:

- None  
Does not include security mechanisms and should only be used for testing purposes and therefore not for productive operation.
- Sign  
Includes security mechanisms to ensure integrity.
- Sign & Encrypt  
Includes security mechanisms to ensure integrity and confidentiality.

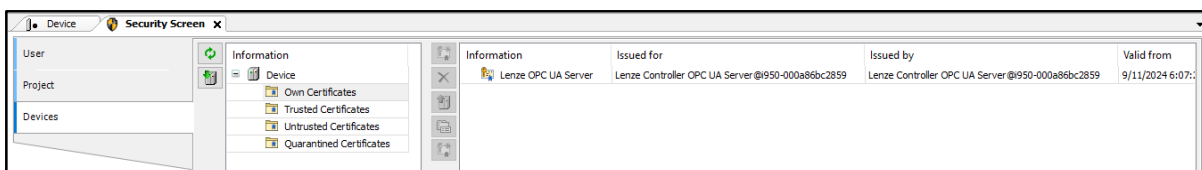
If the selection "Sign" or "Sign & Encrypt" is selected here, certificate handling is required.

This can be set on the server side as follows.



Activity Diagram

When the i9x0 is started for the first time, a separate certificate is created for the OPC-UA Server. This can be seen in the Security Screen under Devices in the 'Own Certificates' section.



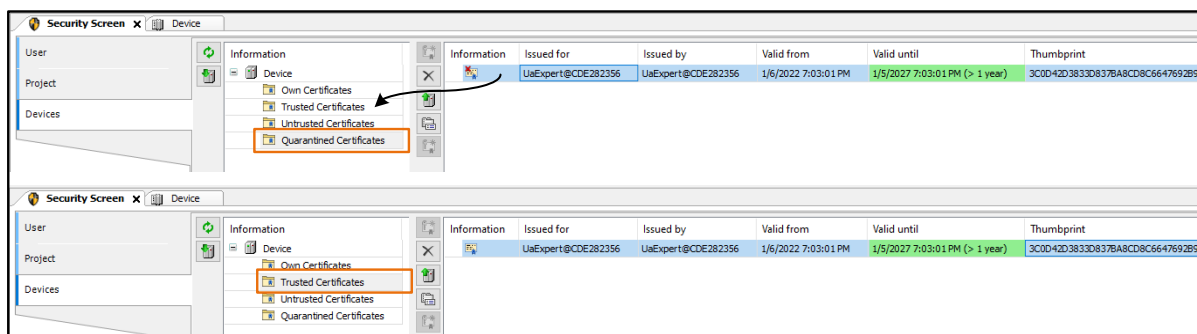
Own Certificate

The certificate automatically created here is a self-signed certificate with a valid to date in the year 2038. If the runtime is to be reduced for security reasons, the certificate can be replaced using the function 'Create a new certificate on the device' ([i9x0.CertificateStore.viaPLCDesigner](#))

# i9x0 servo inverters

i9x0.SecureFactoryReset

When an OPC-UA Client connects to the OPC UA Server, the respective own certificates are exchanged. With the OPC UA Server, the received client certificate will then be found under 'Quarantined Certificates'.



Handling Client Certificates

This must then be moved from quarantine to the "Trusted Certificates" section.



## i9x0.Application.Encryption

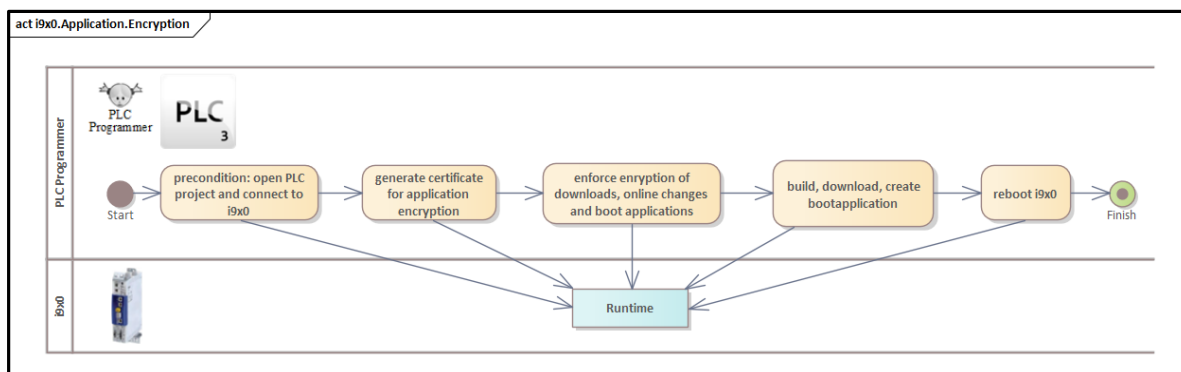
This functionality has been available from version 2.0.0 on.

With the help of this function, the application of the i9x0 Servo Inverter can be encrypted.

These include:

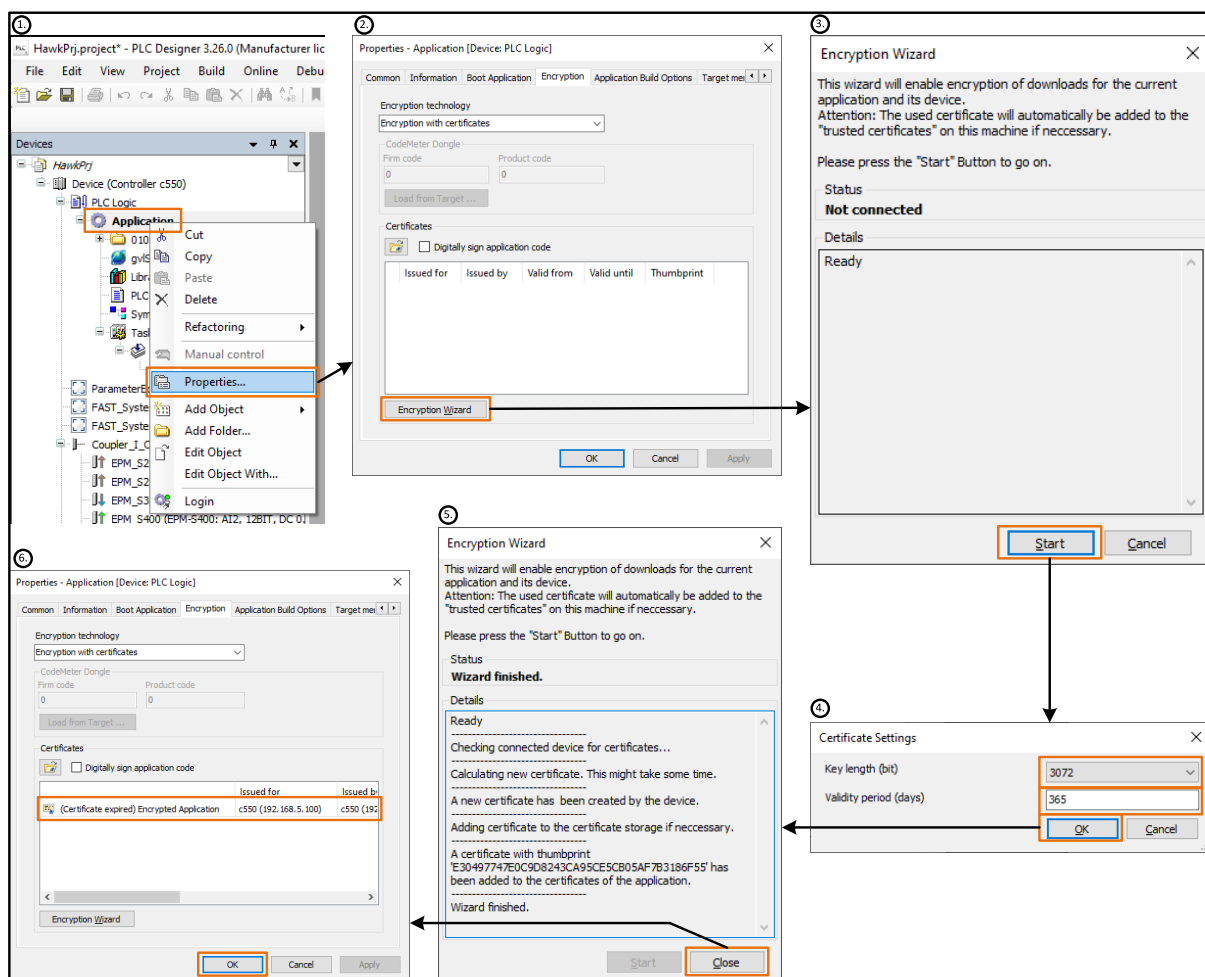
- the application itself
- the online change
- the boot application.

The system integrator can use this functionality to protect its intellectual property and thus the of its applications source code.



Activity Diagram

In order to use this functionality, a certificate for the application encryption is generated. This is done as shown in the following image.

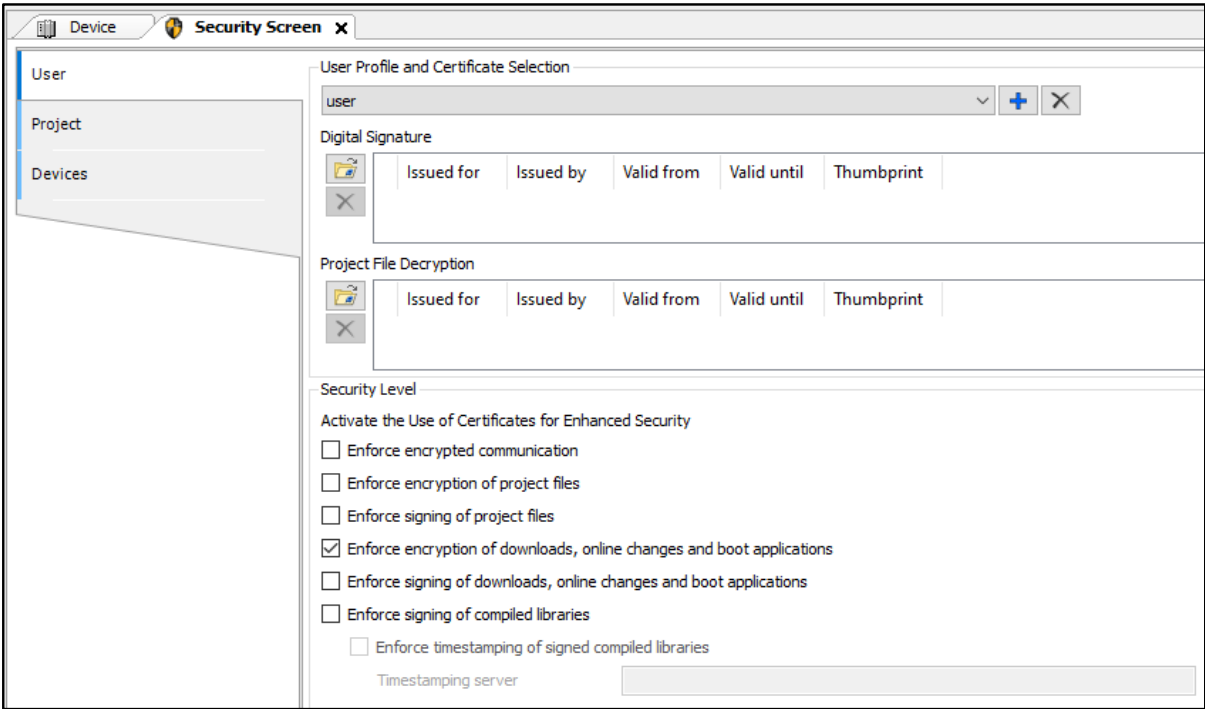


Encryption Wizard

In order to generate a certificate for the encrypted application, the following steps must be carried out:

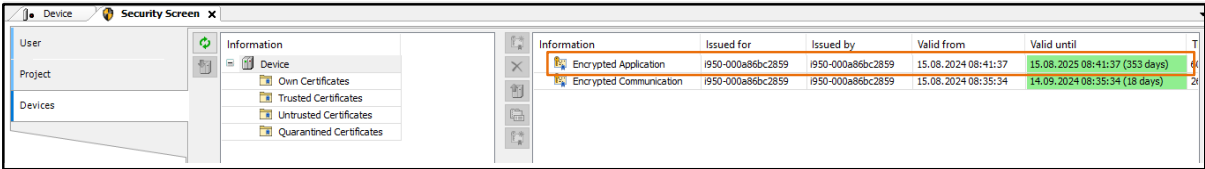
- Open the PLC Designer project and select the Application item in the Devices Tree and call up the 'Properties...' entry.
- Call the Encryption Wizard in the following dialog. Please select the encryption technology 'Encryption with certificates'.
- Start the Encryption Wizard.
- Enter the key length and the validity of the certificate term and confirm with OK.
- Information about the generated certificate is shown. The thumbprint of the certificate is shown to identify the certificate.
- The generated certificate appears in the origination window and is now available.

To enforce the encryption of the application, select the setting 'Enforce encryption of downloads, online changes and boot applications' in the PLC Designer in the Security Screen.



Enforce encryption of Application

The generated certificate for the Encrypted Application can be found in the Security Screen in the Devices tab. As long as the certificate is not generated, a placeholder labeled 'Encrypted Application (not available)' is displayed here.



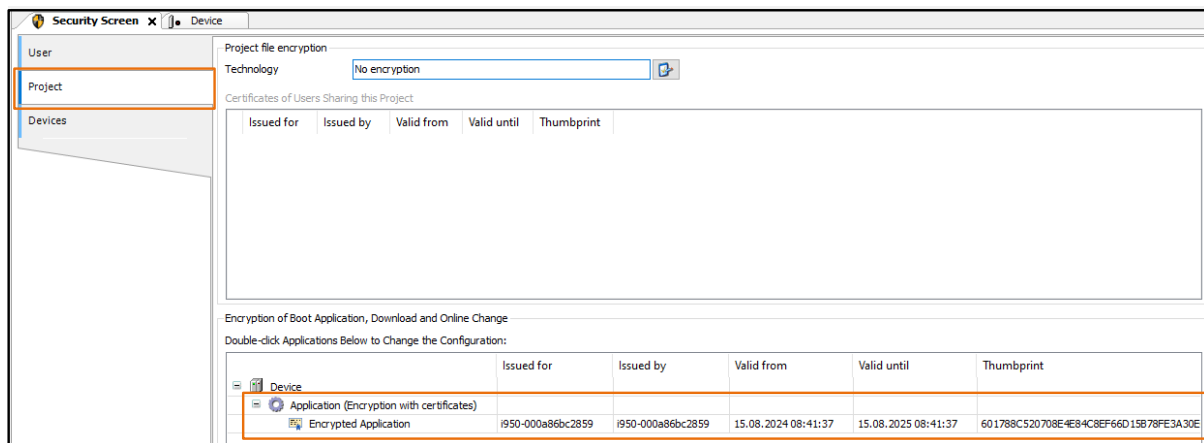
Certificate for Encrypted Application

At this point, the functions are also available to renew the certificate or load it onto the PC ([i9x0.CertificateStore.viaPLCDesigner](#))

In addition, the certificate is also displayed in the Security Screen under project.

# i9x0 servo inverters

i9x0.SecureFactoryReset



Security Screen Project

After setting up the certificate for the Encrypted Application and Enforce encryption of downloads, online changes and boot applications, the following steps must be completed:

1. Use the »PLC Designer« to build the project again.
2. Write the application to the i9x0.
3. Create the boot application.
4. Restart the i9x0.



Please note that the entire application is not encrypted, only the application. app, i.e. the application program. Additional data such as

- Retain Variables
- Trace Data
- EtherCAT Master Configuration Files
- Parameter Sets of the Devices
- CAM Data

and much more are not included and are unencrypted at the destination.

### Use Case: i9x0.Application.Encryption with deleted certificate 'Encrypted Application'

The behavior of the i9x0 is described below if an Encrypted Application was stored as a boot project and the certificate is then deleted.

#### Pre-Condition

The i9x0.Encrypted.Application with a certificate is activated, downloaded and a boot application is available on the i9x0. After restarting the i9x0, the boot application is running.

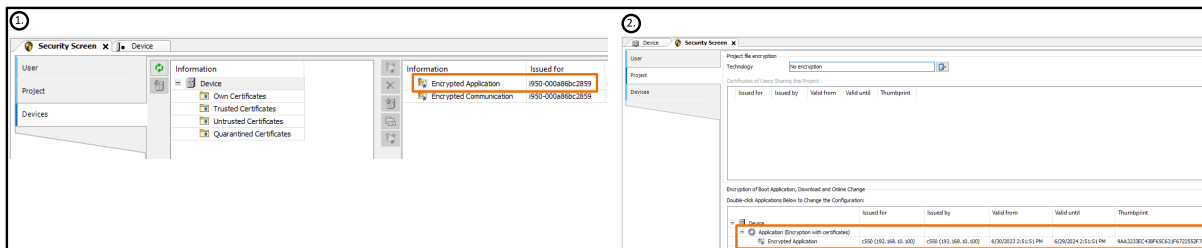
#### Delete the Own Certificate 'Encrypted Application' on the i9x0:

The next step is to manually delete the 'Encrypted Application' certificate on the i9x0, e.g. via the PLC Designer. After deleting the certificate, the application on the i9x0 is still running.

Behavior of the application after different reset levels:

| Reset Level                   | Behavior                                                            |
|-------------------------------|---------------------------------------------------------------------|
| Manually stop the application | After stopping the application, the application can be started.     |
| Reset Warm                    | After "Reset Warm", the application can be started.                 |
| Reset Cold                    | After "Reset Cold", the application can be started.                 |
| Reset Origin                  | After "Reset Origin", the application can not be started again.     |
| Boot of the i9x0              | After 'Boot of the i9x0', the application can not be started again. |

If the PLC Designer is still logged in to the i9x0, the certificate for Encrypted Application in the Security ScreenWDevices is shown as deleted, e.g. with the placeholder 'Encrypted Application (not available)'- Refer to next figure (1.). Under "Security ScreenWProject" the certificate for the Encryption of the Application is still shown, because the application of the i9x0 still needs this certificate-Refer to next figure (2.).



Certificate Encrypted Application Deleted



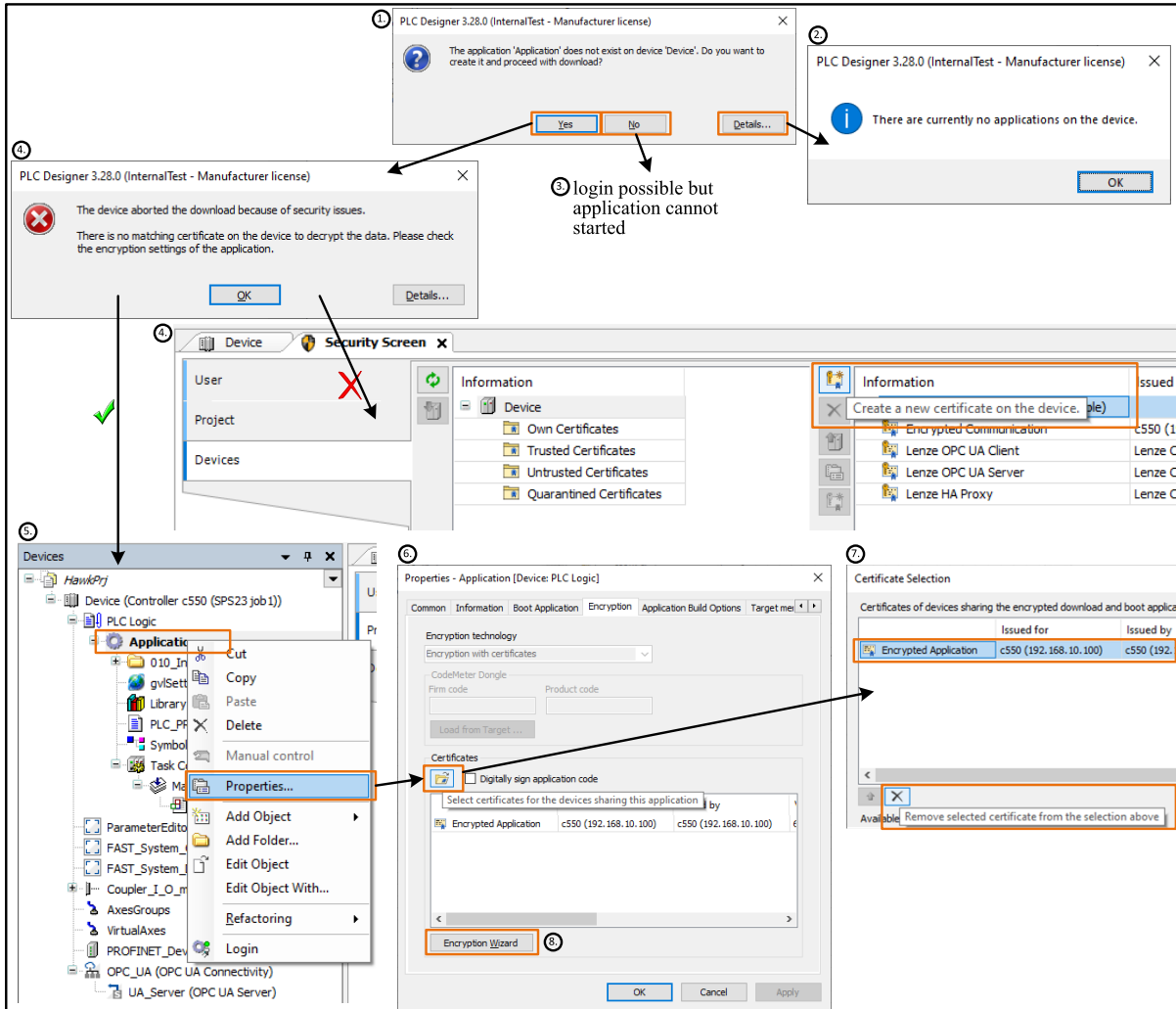
If the Certificate is deleted and the user wants to go online on the i9x0 with the PLC Designer, this is not possible. An online change or creating a boot application is also not possible. The deletion has an immediate effect.

# i9x0 servo inverters

i9x0.SecureFactoryReset

## Replace the Own Certificate 'Encrypted Application' on the i9x0:

After 'Log Off Current Device User' and 'Login' again, the message 'The application does not exist' appears- Refer to next figure (1.).



Certificate Encrypted Application Renew

The existing application cannot be downloaded to the i9x0, because there is no matching certificate on the i9x0 available. To solve this problem, please do not generate a new certificate with the Security Screen on the Device for the Encrypted Application, because the certificate will not match the needed certificate for the application.

To solve this problem, open the properties of the application again and delete the existing certificate and generate a new one with the help of the Encryption Wizard. After these steps, build, download the application Then, generate the boot application and restart the i9x0, The application should be running again.

---

**Use Case: Controller.Application.Encryption with non valid certificate "Encrypted Application"**

The behavior of expired Application Encryption Certificate is the same as with a deleted certificate, the application can no longer be started at "Reset Origin" or "Device Boot". The certificate has to be renewed, as previously described.



If the certificate has expired and the user wants to go online on the controller with the »PLC Designer«, this is possible. An online change or creating a boot application is also possible. Only after the controller has booted, is it no longer possible to start the application, make an online change or create a boot application.

# i9x0 servo inverters

i9x0.SecureFactoryReset

---

## Use Case: i9x0.Application.Encryption in focus of Device Replacement

The behavior of the i9x0 is described below if an Encrypted Application was stored as a boot project and the i9x0 has to be replaced.

### Pre condition

The i9x0.Encrypted.Application with a Certificate is activated and downloaded, and a boot application is available on the i9x0. After restarting the i9x0 the boot application is running.

### Replacement of the i9x0:

If the i9x0 has to be replaced due to a defect, the SD card is removed and the i9x0 hardware is replaced. After replacing the i9x0, however, the application does not start. The reason for this is the necessary but missing certificate. An i9x0 exchange is therefore not possible without the previously described certificate renewal process and a new build, download application, creation of a boot project and a restart of i9x0.



---

## Use Case: i9x0.Application.Encryption in focus of Application Loader



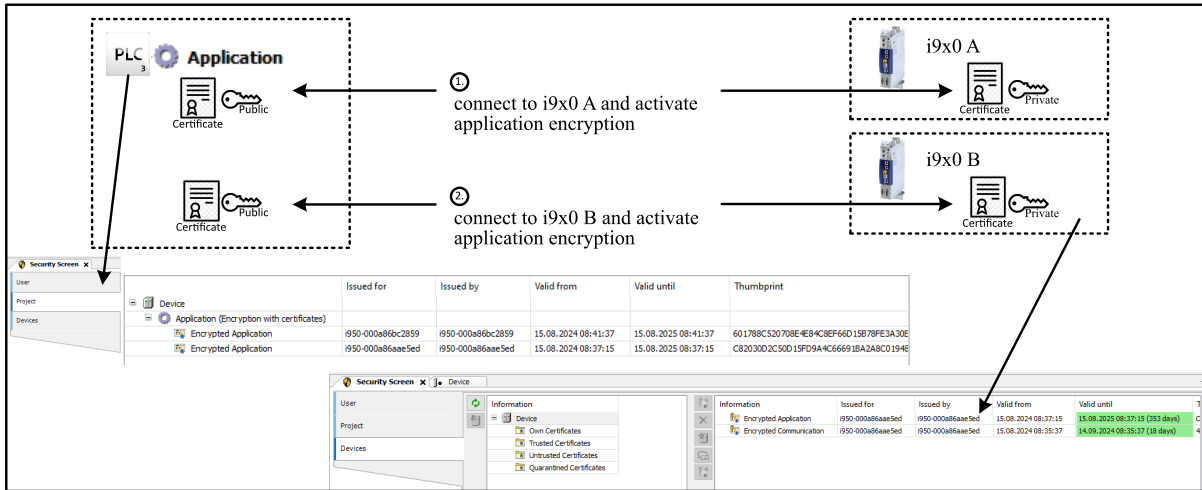
The offline 'create boot application' function from the PLC Designer does not work with the i9x0.Application.Encryption. Therefore, an \*.lda cannot be created in this way.

# i9x0 servo inverters

i9x0.SecureFactoryReset

## Use Case: Handling one project with i9x0.Application.Encryption for more i9x0

The use case here describes the behavior of a PLC Designer project that is to be used for multiple i9x0. The process is shown in the following figure.

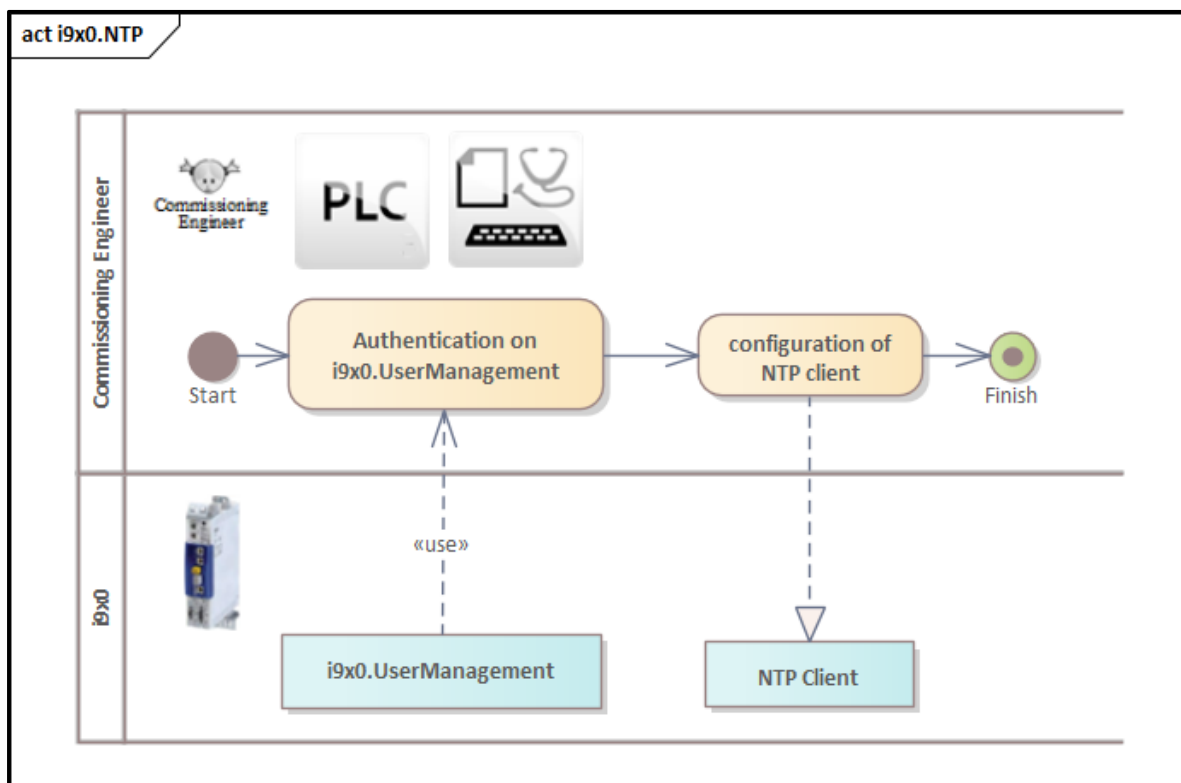


Project for multiple i9x0

1. Connect the PLC Designer to i9x0 A and activate the application encryption using the Encryption Wizard of the Application.
2. The i9x0 A will create a certificate including the private key and it will be available in the Certificate Store of i9x0 A as 'Encrypted Application' certificate.
3. At the same time, the PLC Project will include the Certificate A including the public key and it will be available in the application for the PLC project.
4. Connect the PLC Designer to i9x0 B and activate the application encryption using the Encryption Wizard of the Application.
5. The i9x0 B will create a certificate including the private key and it will be available in the Certificate Store of i9x0 B as 'Encrypted Application' certificate.
6. At the same time, the PLC project will include the certificate B including the public key and it will be available in the application for the PLC project.
7. In the end, the application for the PLC project will include both certificates. Depending on the active application, the corresponding certificate is then used for encryption.

## i9x0.NTP

To synchronize the time of the i9x0 Servo Inverter to a central time server, the NTP Client can be used.



Activity Diagram

To set up the time manually, the following parameters can be used:

Parameters for configuring the datetime

| Address    | Name /Setting Range / [Default] | Info                                                  |
|------------|---------------------------------|-------------------------------------------------------|
| 0x245B:002 | System time: Current time       | This is the timedate for the main system of the i9x0. |

To change to the NTP client functionality, the following parameters are necessary:

Parameters for configuring the datetime

| Address    | Name /Setting Range / [Default]                 | Info                                                  |
|------------|-------------------------------------------------|-------------------------------------------------------|
| 0x245B:001 | System time: Setting method                     | Please switch from Manual input [2] to NTP server [0] |
| 0x245A:002 | NTP server addresses: NTP server address 1      | NTP server addresses                                  |
| 0x245A:003 | NTP server addresses: NTP server address 2      |                                                       |
| 0x245A:004 | NTP server addresses: NTP server address 3      |                                                       |
| 0x245A:005 | NTP server addresses: NTP server address 4      |                                                       |
| 0x245A:001 | NTP server addresses: Activate NTP server addr. | Device command for activating NTP client              |

After configuration, the new parameters are transferred via the device command 0x245A:001.

# i9x0 servo inverters

i9x0.SecureFactoryReset



The datetime will be synchronized via the NTP client from the NTP server

\* cyclic each ~ 32 seconds during operation.



An NTP client checks the quality of the NTP server. Among other things, the Leap Indicator is checked here. Here the values:

0 - Time valid, synchronized

1 - Last minute has a leap second

2 - Unsynchronized, server has no valid time

3 - Clock defective, unknown status

The i950 expects a Lead Indicator of 0.

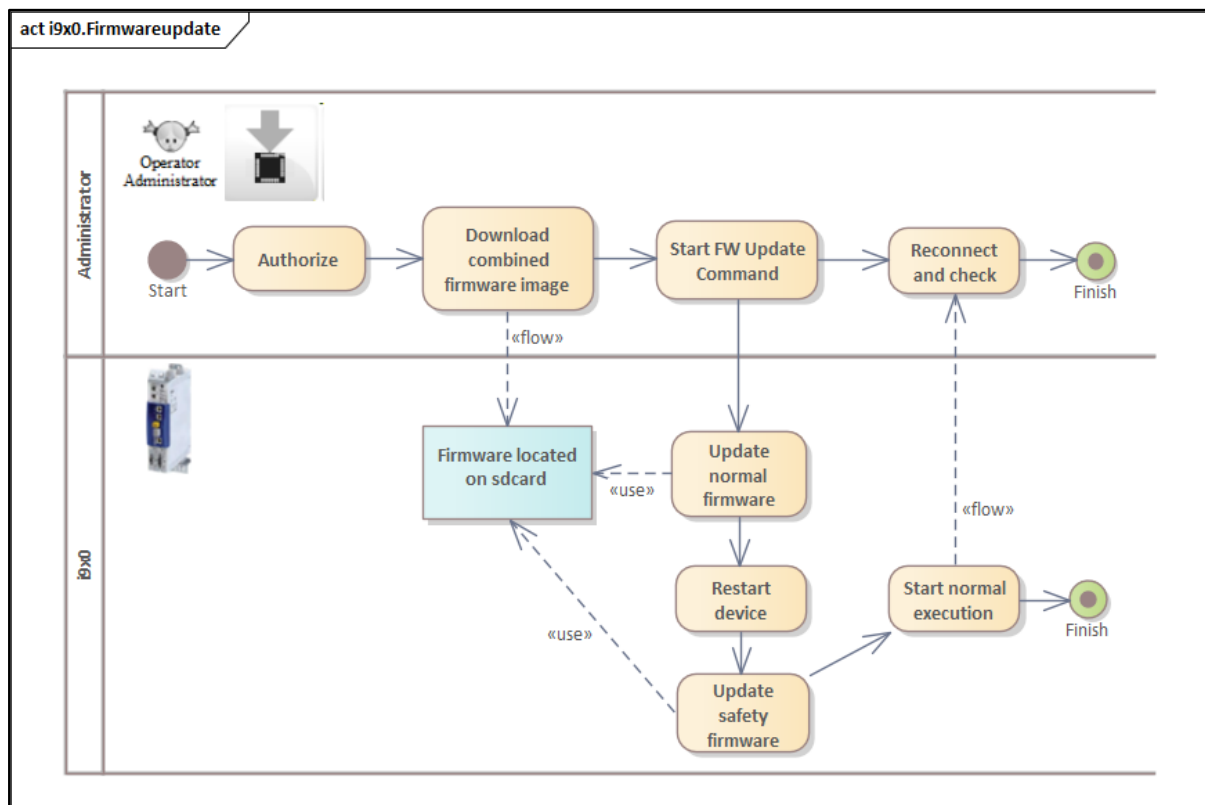
## i9x0.SecureBoot

From firmware V2.0.0, the i9x0 Servo Inverter has a secure boot chain.

There is no setting option for the user of the component here, as this security function is one of the device protection functions and is always active and cannot be configured.

## i9x0.FirmwareUpdate

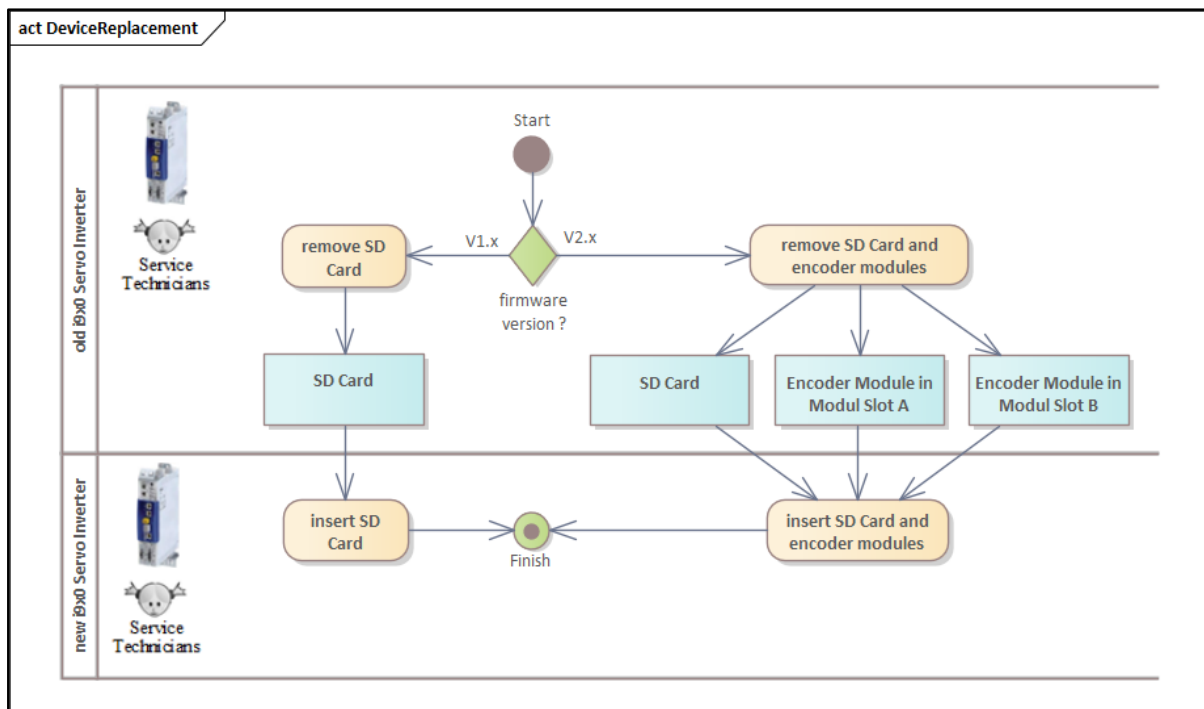
The firmware of the i9x0 servo inverter can be upgraded or downgraded via the firmware loader (refer to chapter xyz). From firmware version V2.0.0, the same firmware download can be used to update not only the firmware of the basic device but also the safety firmware.



Firmware Update

## i9x0.DeviceReplacement

A device replacement is a scenario in which a fully commissioned i9x0 Servo Inverter is to be replaced by a replacement product due to damage. A distinction is made here between the firmware versions V1.x and V2.x.



i9x0 Device Replacement

### Behavior with Firmware V1.x

All relevant project data (application data, parameter set, ...) is stored on the SD card. In the event of a device replacement, the SD card must be transferred from the defective device to the replacement device. All necessary data is then available in the replacement device.

### Behavior with Firmware V2.x

In the firmware V2.x, a distinction must be made between the behavior of the i9x0-para and i9x0-prog (for more information, refer to chapter [i9x0.SecurityMechanisms.DeviceReplacement](#)).

With i9x0-para, the data on the SD Card is still not encrypted and therefore the behavior during device replacement is the same as with the V1.x firmware. Only the SD Card needs to be transferred to the new device.

With the i9x0-prog, the data on the SD Card is encrypted, when choosing "default security". A stored key is required for encryption. This is automatically generated by the i9x0 and stored securely. In the event of a device replacement, this key must be transferred in addition to the data on the SD Card. A mechanism has been established to enable this as soon as the encoder modules in module slot A and / or module slot B are also transferred to the new device.

# i9x0 servo inverters

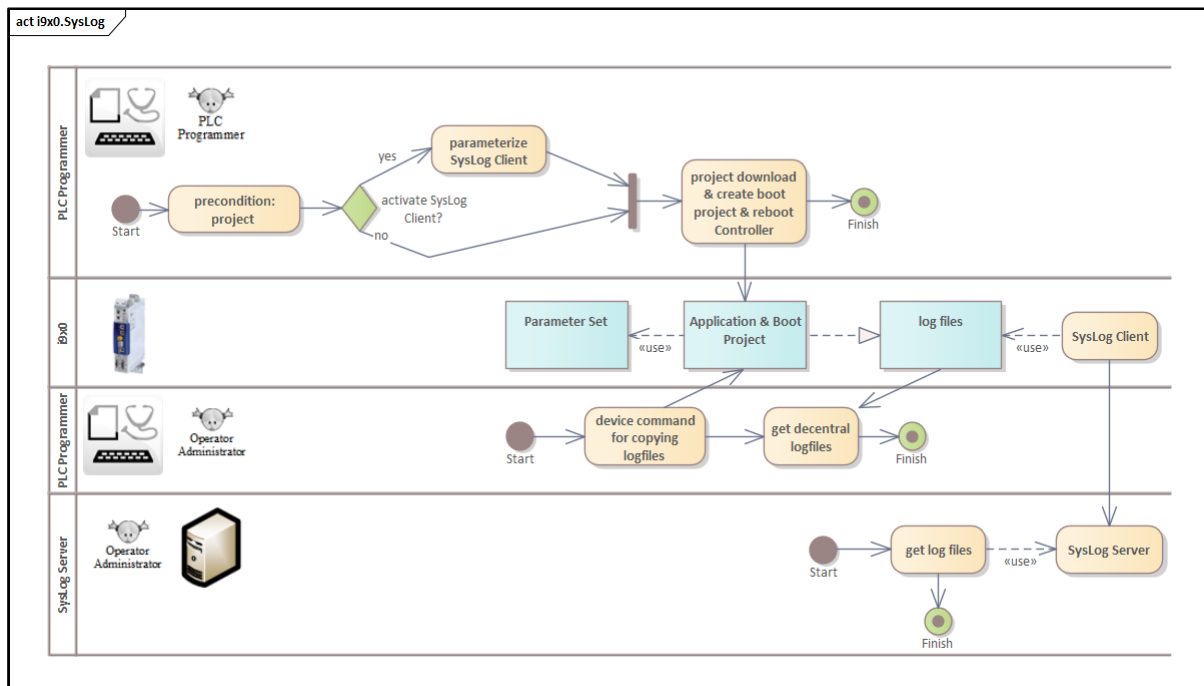
i9x0.DeviceReplacement



For more information about upgrade and downgrade between firmware version V1.x and version V2.x please refer to chapter [i9x0.SecurityMechanisms:DeviceReplacement](#),

## i9x0.SysLog

The SysLog (System Logging Protocol) function enables the controller to log its important activities in local log files and optionally send them to a central SysLog server via a SysLog protocol. This enables the end user to monitor their infrastructure. This functionality is available from firmware version 2.0.0 on.



Activity Diagram

1. Activate and parameterize the SysLog Client
2. Prepare the i950 Servo Inverter to access the local logfiles
3. Get local logfiles
4. Get logfiles from SysLog Server



In the event of a power failure, the local log file messages and messages sent via the syslog client are not guaranteed. Messages are not saved in the i950. One solution could be to use a UPS.

### Activate and parameterize the SysLog Client

The function can be parameterized using the following parameters. Please note that these parameters must be saved persistently in the parameter set and the i950 Servo Inverter must be restarted for the parameters to become valid.

### Activate SysLog Client

The i950 Servo Inverter has two logging options:

- Internal logging into local log files
- Sending of logging messages via the SysLog protocol to a SysLog Server

The local logging is always active, but the sending of logging messages can be activated with the following parameter.

Parameter for SysLog Client activation

| Address    | Name                                   |                       | Info                         |
|------------|----------------------------------------|-----------------------|------------------------------|
| 0x5914:001 | SysLog Client: SysLogClient activation |                       | SysLog Client activation     |
|            | enum 0                                 | Deactivated (default) | SysLog Client is deactivated |
|            | enum 1                                 | Activated             | SysLog Client is activated   |

### SysLog Server IP address.

This is the IP v4 address of the SysLog Server.

Parameter for SysLog Server IP address

| Address    | Name                                                                                              | Info                        |
|------------|---------------------------------------------------------------------------------------------------|-----------------------------|
| 0x5914:002 | SysLog Client: IP address of SysLog Server<br>UDINT 4 bytes<br>0.0.0.0 (default) –255.255.255.255 | IP address of SysLog Server |

### SysLog Server Port

This is the parameter for the port of the SysLog Server. This setting is independent of whether a protocol udp or tcp is selected.

Parameter for SysLog Server Port

| Address    | Name                                                                         | Info                  |
|------------|------------------------------------------------------------------------------|-----------------------|
| 0x5914:003 | SysLog Client: Port of SysLog Server<br>UDINT 2 bytes<br>0 (default) - 65535 | Port of SysLog Server |

### SysLog Protocol Type

This is the parameter for the protocol of the SysLog Messages and for the setting of the optional encryption.

Parameter for SysLog Protocol Type and SysLog Encryption

# i9x0 servo inverters

i9x0.DeviceReplacement

| Address | Name                               |                    | Info                                       |
|---------|------------------------------------|--------------------|--------------------------------------------|
|         | SysLog Client: SysLog ProtocolType |                    | SysLog Client Protocol Type                |
|         | enum 0                             | UDP (default)      | SysLog Messages via UDP                    |
|         | enum 1                             | TCP                | SysLog Messages via TCP                    |
|         | enum2                              | TCP /TLS encrypted | SysLog Messages via TCP with TLS encrypted |

## SysLog Message Severity Filter

These are the parameters for filtering the SysLog Messages via Severity.

Parameter for filtering the SysLog severities

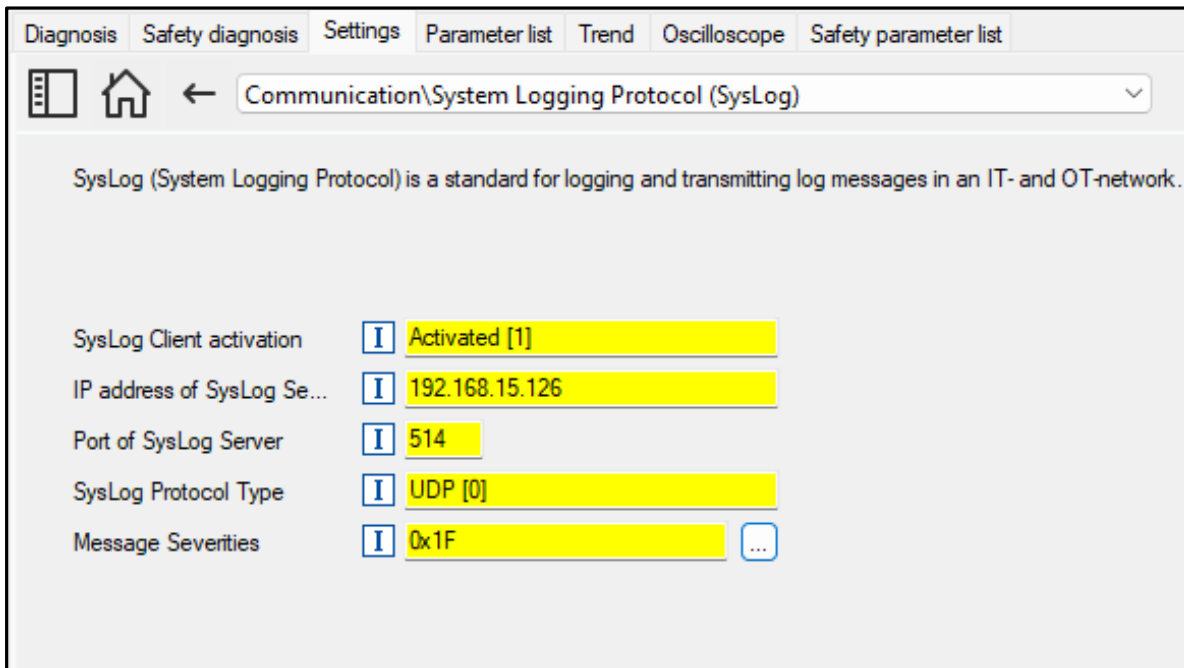
| Address    | Name                              |                                 | Info                                                     |
|------------|-----------------------------------|---------------------------------|----------------------------------------------------------|
| 0x5914:006 | SysLog Client: Message Severities |                                 | Filter for SysLog Message Severities                     |
|            | bit 0                             | emerg (default = activated)     | Severity Emergencies "System unusable"                   |
|            | bit 1                             | alert (default = activated)     | Severity Alerts "Immediate action needed"                |
|            | bit 2                             | crit (default = activated)      | Severity Severity Critical "Critical conditions"         |
|            | bit 3                             | err (default = activated)       | Severity Severity Error "Error conditions"               |
|            | bit 4                             | warning (default = deactivated) | Severity Warning "Warning conditions"                    |
|            | bit 5                             | notice (default = deactivated)  | Severity Notification "Normal but significant condition" |
|            | bit 6                             | info (default = deactivated)    | Severity Information "Informational messages only"       |
|            | bit 7                             | debug (default = deactivated)   | Severity Debugging "Debugging messages"                  |



The parameter 0x5914:006 for filtering the Severities is working for the SysLog-Client functionality and the local logfiles on the i950 Servo Inverter. The filter works on local log files even if the SysLog Client is deactivated.

These parameters can be modified for example via the parameter list or the user dialog via Settings \ Communication \ System Logging Protocol (SysLog).



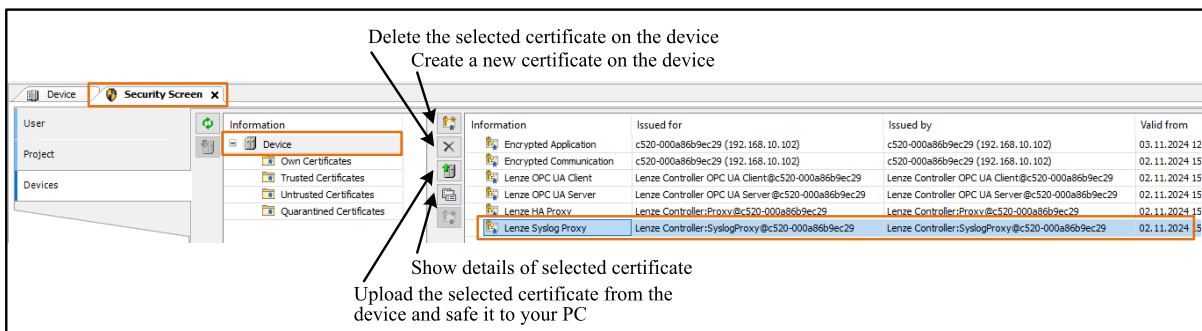


Settings Dialog

### Certificate Handling for encrypted SysLog

If the user wants to secure remote logging on syslog servers, the user can activate encrypting the protocol with TLS.

When setting the encrypted SysLog protocol with parameter 0x5914:004 to enumeration 2, a certificate is needed for the encryption. The user can handle this certificate via the Security Screen of the PLC Designer via the menu View / Security Screen. When choosing the Device tab and the Device itself, the actual certificates are shown after 'Refresh the list of available devices and their certificate stores'.



Certificate for SysLog

The user can use the auto-generated certificate for 'Lenze Syslog Proxy', or delete this and create a new one. The user can also upload this certificate to the user computer or show the details.

Details of this automatically generated certificate can be found in this documentation, ([i9x0.CertificateStore.SysLogProxy:Certificate](#))



A certificate is mandatory for a secure SysLog connection. If the user manually deletes the SysLog Proxy Certificate during operation, the SysLog Client of the controller will send information about missing certificates to the SysLog Server. Therefore the Client will use the `deleted` certificate until rebooting.



A certificate is mandatory for a secure SysLog connection. If the user manually generate a new SysLog Proxy Certificate during operation, the SysLog Client will terminate the TLS connection based on the old certificate and will start a new TLS connection based on the new certificate.



If the SysLog connection is used in an encrypted manner and the certificate expires during operation, communication continues based on the then invalid certificate. If the controller is restarted, a new valid certificate is automatically generated and the SysLog connection is opened based on the new valid certificate.

### Behavior when SysLog Proxy Certificate is deleted after different reset levels

| Reset Level                                   | Behavior                                                     |
|-----------------------------------------------|--------------------------------------------------------------|
| Manually stop and start the application       | The SysLog Proxy Certificate is still deleted.               |
| Reset Warm                                    | The SysLog Proxy Certificate is still deleted.               |
| Reset Cold                                    | The SysLog Proxy Certificate is still deleted.               |
| Reset Origin and create the application again | The SysLog Proxy Certificate is still deleted.               |
| Boot the Controller                           | The SysLog Proxy Certificate is automatically generated new. |

### File Monitoring

In addition to the SysLog, a file monitoring was initialized to log information about configuration changes.



This file monitoring is only available at runtime, i.e. changes to the file system when the system is turned off are not logged. The SD Card must therefore be protected against unauthorized removal and modification.



The focus of this file monitoring is on static files that change frequently during commissioning, but should not or rarely change during machine runtime ([i9x0.SysLog:MonitoredFilesAndDirectories](#)). The focus is not on files that are subject to permanent change, e.g. an application logbook.

The type of monitoring and the response in the log lines can be seen in the following two tables.

#### Monitoring of Files

| File Monitoring                          | Example Log Line<br>(Log lines may vary depending on the tool used) |
|------------------------------------------|---------------------------------------------------------------------|
| Create file if it does not exists        | /<path>/<file>: CREATE<br>/<path>/<file>: CLOSE_WRITE               |
| Delete existing file                     | /<path>/<file>: DELETE                                              |
| Change and safe content of existing file | /<path>/<file>: CLOSE_WRITE                                         |
| Change rights of existing file           | /<path>/<file>: ATTRIB                                              |

#### Monitoring of Directories

| Directory Monitoring                         | Example Log Line<br>(Log lines may vary depending on the tool used) |
|----------------------------------------------|---------------------------------------------------------------------|
| Rename existing file in directory            | /<path>/<oldfile>: MOVED_FROM                                       |
| Change content of existing file in directory | /<path>/<file>: CLOSE_WRITE                                         |
| Change rights of existing file in directory  | /<path>/<file>: ATTRIB                                              |
| Delete existing file in directory            | /<path>/<file>: DELETE                                              |



This file and directory monitoring procedure cannot process files or directories with the special character “;” (semicolon). The Lenze Tools do not create files or directories with this character. This means that the user may not use customized files or directories with this special character.

If a file or directory with this special character exists and this file or directory is being monitored, the application will not start for security reasons.

#### Application Logging via FB AddSysLog

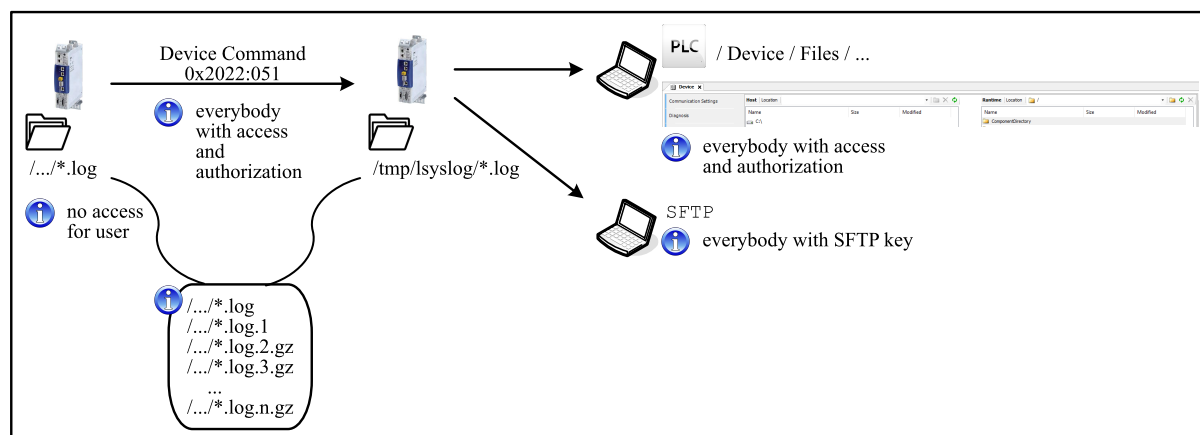
Please refer to chapter [SysLog](#) to get more information about this function block.

#### i9x0.SysLog.Get logfiles from i9x0

To a limited extent, the controller records the SysLog data and can make it available via a defined path, as shown in the following image. This functionality is available from firmware version 2.0.0 on.

# i9x0 servo inverters

i9x0.DeviceReplacement



Get local Logfiles

- All Logfiles are stored on the i9x0 Servo Inverter in a protected inaccessible area.
- Users with access to the i950 Servo Inverter's parameter set can execute the device command to copy log files to the `/tmp/lsyslog` directory.
- Users with a PLC Designer and access to the i9x0 Servo Inverter can retrieve these files via the Files tab.
- If the user has an SFTP client and an SFTP key, they can access the files via SFTP.

The structure of the log files is shown in the figure before.

- The first logfile is written without compression.
- After reaching a file size, a new log file will be generated with `.1`-extension.
- After reaching the file size again, a new log file will be generated and compressed with a `.2.gz`-extension.
- After reaching the maximum number of log files, the oldest file will be dropped.

Log files with their focus and an example of content

| Log file | Example of content                                                                                                                       |
|----------|------------------------------------------------------------------------------------------------------------------------------------------|
| kern     | e.g. `mmc0: card 5048 removed` -> SD card was removed                                                                                    |
| user     | e.g. ` <user message="">` -&gt; User messages, generated by the FB</user>                                                                |
| daemon   | e.g. `check-and-mount@mmcbk0p1.service: Succeeded<br>finished check and mount device mmcbk0p1` -> a new SD card was detected.            |
| auth     | e.g. `session opened for local user customer from [192.168.10.201]<br>realpath"/sdcard" ` -> SFTP Session opened and path set to /sdcard |
| authpriv | e.g. `child connection from 192.168.10.201:63287` -> SFTP-Child connection from given IP address                                         |
| local0   | e.g. `Sessioninfo: client: 'PLC Designer 4.0.0', host: '<hostname>'` -> PLC Designer logged into the Controller                          |
| local1   | Reserved for EtherCAT-Master-Debugging (only for Lenze developer)                                                                        |
| local2   | e.g. `ViwiWin7.Server.Manager: WebGateway Server WebGateway:WebGateway Server started`                                                   |

## Persistence of local stored log files

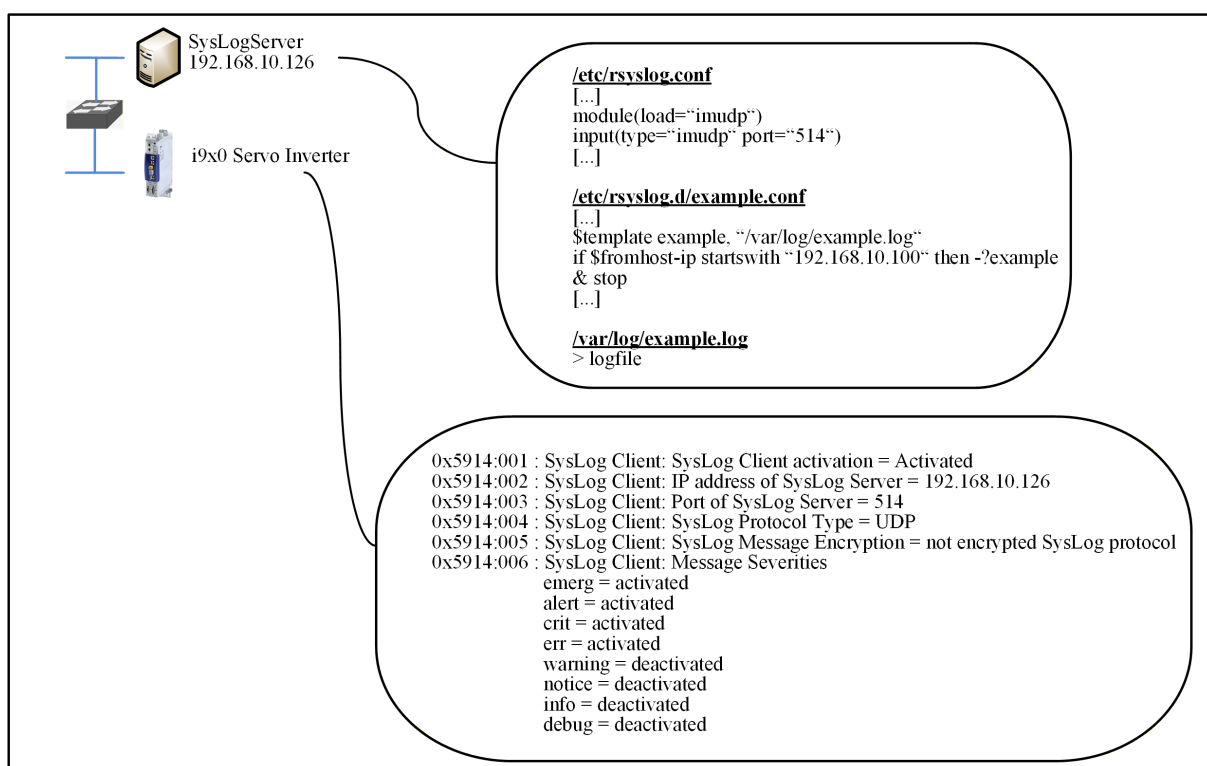
This chapter describes some use cases related to the persistence of log files.

Persistence of SysLog log files

| Use Case                                    | Persistence of log files                                                                                                 |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Reboot or Shutdown the i9x0 Servo Inverter. | The log files are not persists. After starting the i9x0 Servo Inverter the logging mechanism starts with empty logfiles. |
| Firmware Up- or Downgrade.                  | The log files are not persists. After starting the i9x0 Servo Inverter the logging mechanism starts with empty logfiles. |

### Get logfiles from SysLog Server

There are a lot of different ways to setup a SysLog Server. In this example, a SysLog Server based on an Ubuntu Linux system with the functionality of the rsyslog service is described and shown in the following figure.



Get Lofile from SysLog Server

Set up the i9x0 Servo Inverter:

- In this example, the i9x0 Servo Inverter has the IP address of 192.168.10.100.
- Set the parameter 0x5914:001 to `activated` to activate the SysLog Client of the i9x0.
- Set the parameter 0x5914:002 to the IP address of the SysLog Server.
- Set the parameter 0x5914:003 to the Port of the SysLog Server.
- Set the parameter 0x5914:004 to the Protocol Type UDP.
- Set the flags of parameter 0x5914:006 of the wanted severities.

Setup the SysLog Server:

- Use the Ubuntu Linux Distribution and install the `rsyslog` service.
- Configuration `/etc/rsyslog.conf` and activate the syslog reception via hdp/514 with the following lines:  
module(load="imudp")

# i9x0 servo inverters

i9x0.DeviceReplacement

```
input(type="imudp" port="514")
```

- Generate a template file `/etc/rsyslog.d/example.conf`:`  
\$template example, "/var/log/example.log"  
if \$fromhost-ip startswith "192.168.10.100" then -?example  
& stop
- Restart the Service: `systemctl restart rsyslog`
- When using the Controller in this settings, the SysLog Messages will be found in the SysLog Server in the `/var/log/example.log`.



To ensure that the time stamps in the logbooks on the i950 Servo Inverter and the higher-level SysLog server match and that the logs in the SysLog server also match those of other devices in the system, it is recommended that the SysLog server, the i950 and all other devices that use this service be connected to a central time source via NTP and synchronized.

## i9x0.WebVisu.Activation

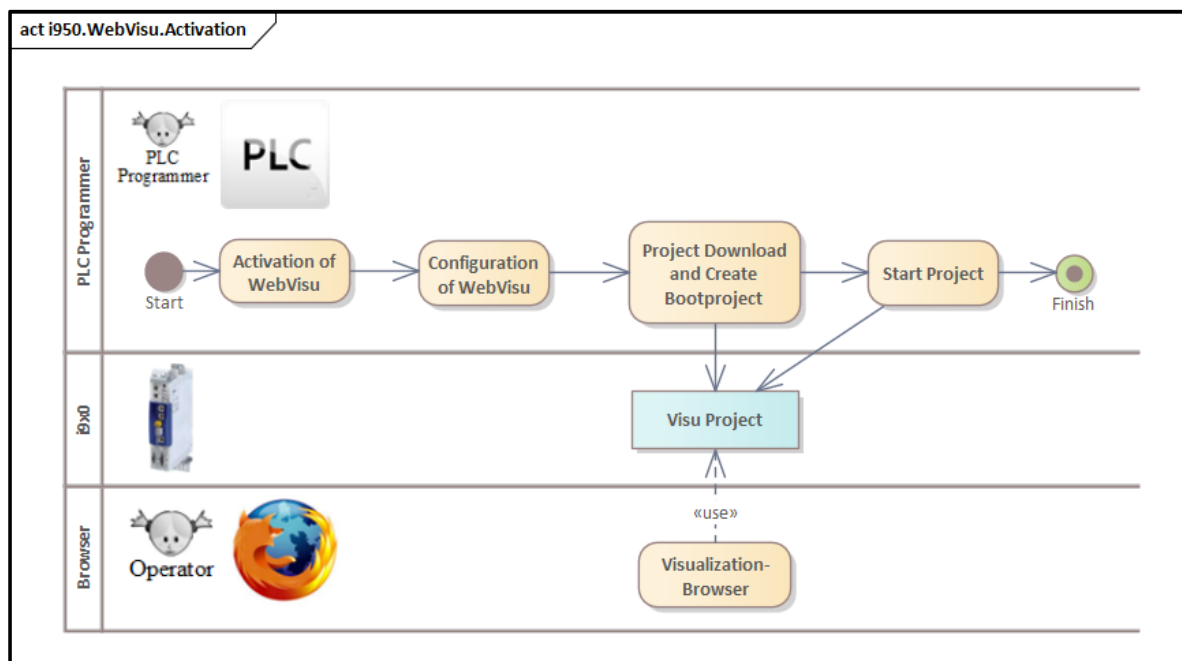
The i9x0.WebVisu is only available with the customer-specific type of the i950 Servo Inverter and from the firmware version 01.07.04 on.



Be sure to use a target device in the PLC Designer with the name of the i9x0 and the added note "Extended for customer specific devices only".

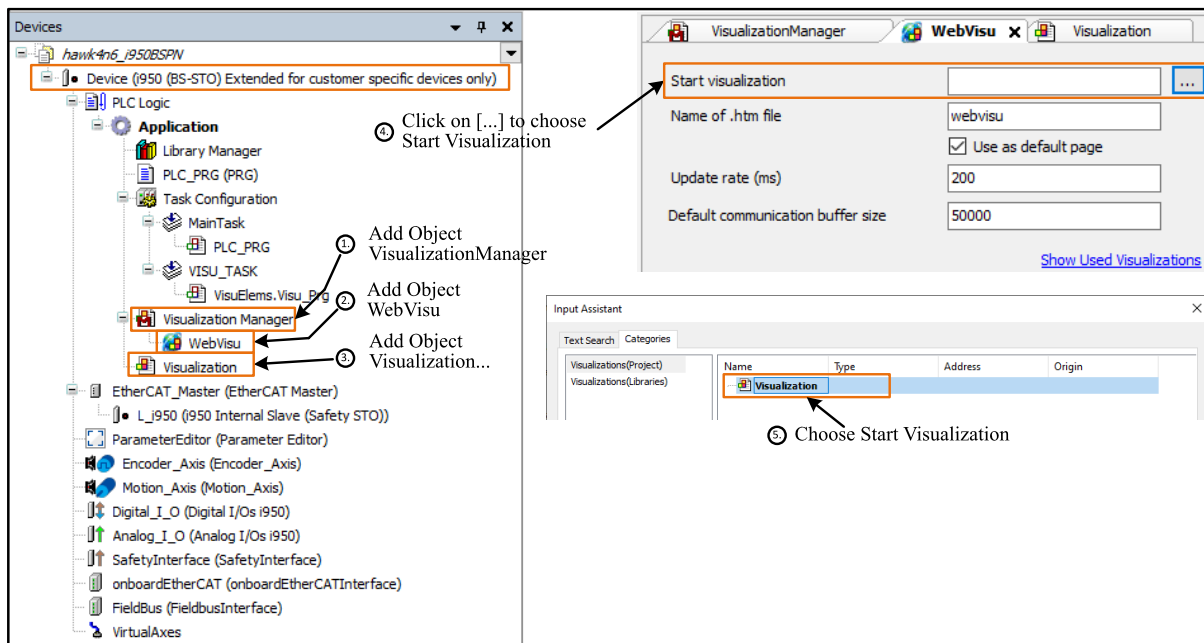
\* The product ID is I95xxxxxxxxxxWxxxx or I95xxxxxxxxxxVxxxx.

\* The parameter 0x2012:007 has the value 'enabled [1]'.



Activity Diagram

To activate WebVisu, please follow these steps:



Activation of the WebVisu in the PLC Designer

1. After adding a i950 device with the "Extended for customer specific devices only" extension, add an object called "VisualizationManager" as a child of the application. During this procedure, activate the "VisuSymbols (System)" symbol library.
2. Add an object called "WebVisu" as a child of the VisualizationManager.
3. Add an object called "Visualization..." as a child of the application.
4. Open the tab for WebVisu and start the input assistant for the start visualization by clicking the [...] button.
5. Select Start Visualization.

Afterwards, build and download the project to the i950. Finish by creating the boot application.



Please check the firewall settings, and if necessary open the port 8080 via the application ports.

The visualization can be shown in a browser of a panel when connecting to the IP address, the port 8080 and the name of the htm file (shown in the WebVisu-Tab), e.g.:

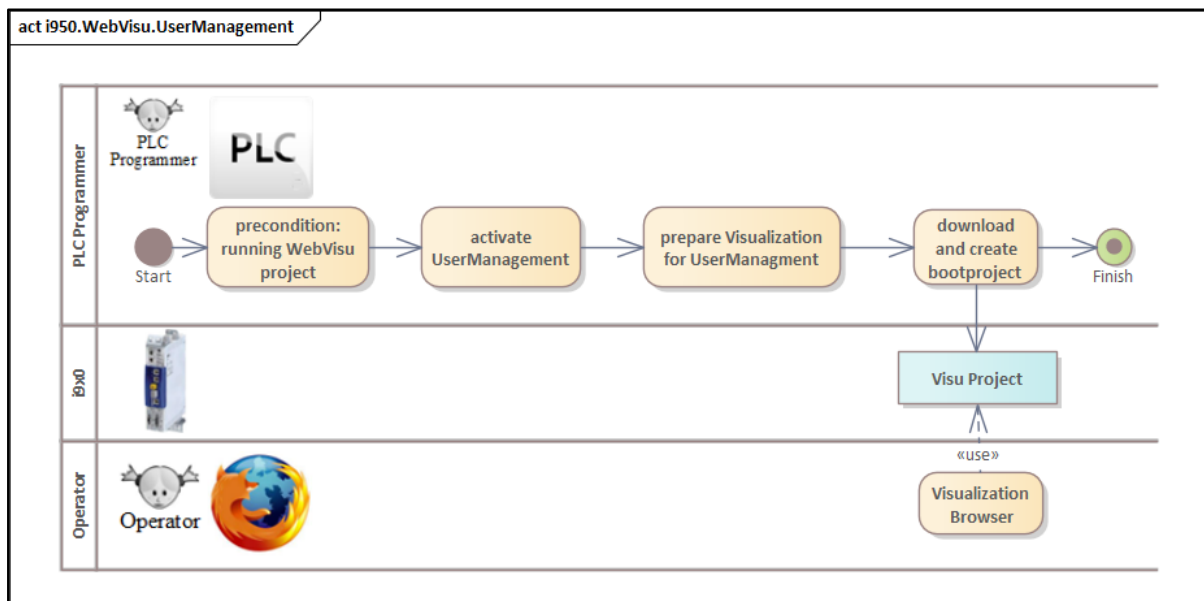
<http://192.168.10.102:8080/webvisu.htm>

## i9x0.WebVisu.UserManagement

It is strongly recommended to activate the User Management for the WebVisu, of the Customer-Variant of these i9x0 servo inverter. This functionality is available from version V2.0.0 on.

# i9x0 servo inverters

i9x0.DeviceReplacement



Activity Diagram

To activate the User Management for the WebVisu please follow the steps:



activate i9x0.UserManagement

The screenshot shows the 'VisualizationManager' window with the 'User Management' tab selected. The 'Create User Management with Default Groups and Users' button is highlighted with an orange box and labeled with a circled 2. Below this, the 'Groups' tab shows a table of default groups, and the 'Users' tab shows a table of default users. The 'Settings' tab is also visible, with the 'Allow decision on every download' option selected under 'Settings for Download of User Data'. A red arrow points from this option to a dialog box that appears during login, asking if the user wants to download user data.

**Groups Tab:**

| Group Name          | Automatic Logout                    | Logout Time | Permission to Change User Da...     | Description | Id |
|---------------------|-------------------------------------|-------------|-------------------------------------|-------------|----|
| Admin               | <input checked="" type="checkbox"/> | 1 minute(s) | <input checked="" type="checkbox"/> |             | 1  |
| has user 'Admin'    |                                     |             |                                     |             |    |
| Service             | <input type="checkbox"/>            | 1 minute(s) | <input type="checkbox"/>            |             | 2  |
| has user 'Service'  |                                     |             |                                     |             |    |
| Operator            | <input type="checkbox"/>            | 1 minute(s) | <input type="checkbox"/>            |             | 3  |
| has user 'Operator' |                                     |             |                                     |             |    |
| None                | <input type="checkbox"/>            | 1 minute(s) | <input type="checkbox"/>            |             |    |

**Users Tab:**

| Login Name | Full Name     | Password | User Group | Deactivate               | Description |
|------------|---------------|----------|------------|--------------------------|-------------|
| Admin      | Administrator | *****    | Admin      | <input type="checkbox"/> |             |
| Service    | Service       | *****    | Service    | <input type="checkbox"/> |             |
| Operator   | Operator      | *****    | Operator   | <input type="checkbox"/> |             |

**Settings Tab:**

**Settings for Download of User Data:**

- ☐ Download user data on every login
- ☐ Never download user data on login
- ☒ Allow decision on every download

**Access Rights for Elements:**

- ☐ Use group hierarchy

**Logout Behaviour:**

- ☐ Change to start visualization when logout

**Login Settings:**

- ☐ Apply login restrictions
- Maximum number of authentication attempts: 1
- User Lockout:
  - ☒ Permanent lockout
  - ☐ Temporary lockout time: 1 minute(s)

**Dialog Box:**

PLC Designer 3.28.0 (Manufacturer license)

A visu user management is available. Do you want to download the user data? If a user data file already exists on the device, it will be overwritten.

Yes No

Activate User Management

1. Double click the component "VisualizationManager". Choose the "User Management" Tab.
2. Click the "Create User Management with Default Groups and Users" button. User management will now activate.
3. After activation, you can view more information about the groups in the Groups tab.
4. After activation, you can view more information about users in the "Users" tab. It is strongly recommended that you change all Usernames and Passwords from the default settings to personalized ones.
5. After activation, you can view more information about the security settings in the "Settings" tab.
6. Pay special attention to the "Settings for Download of User Data" option. The "Allow decision on every download" setting is recommended. With this setting, a pop-up menu will appear when logging in, which allows the user to make a decision based on the situation.

# i9x0 servo inverters

i9x0.DeviceReplacement



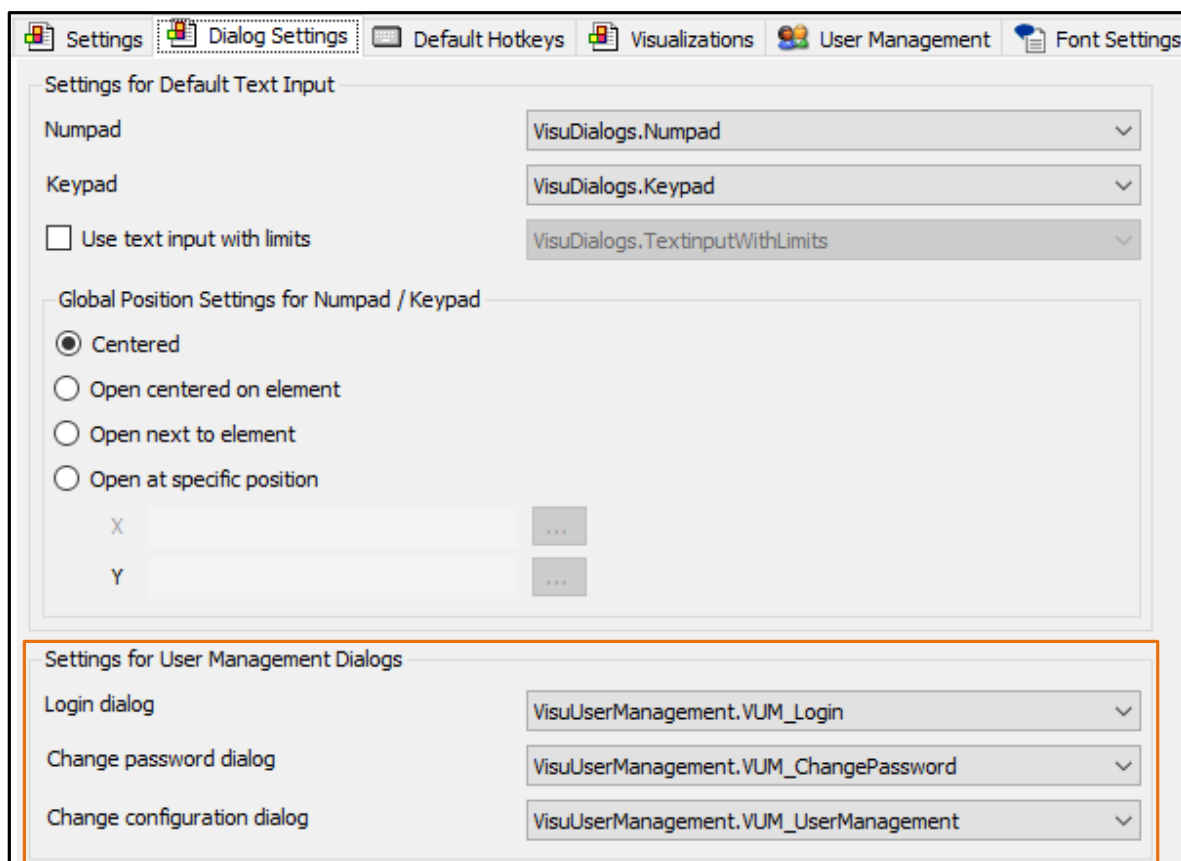
The default settings for the default user are:

User Admin / Password Admin

User Service / Password Service

User Operator / Password Operator

After setting up the User Management, please check the settings of the dialogs and design the wanted layout for the visualization components:



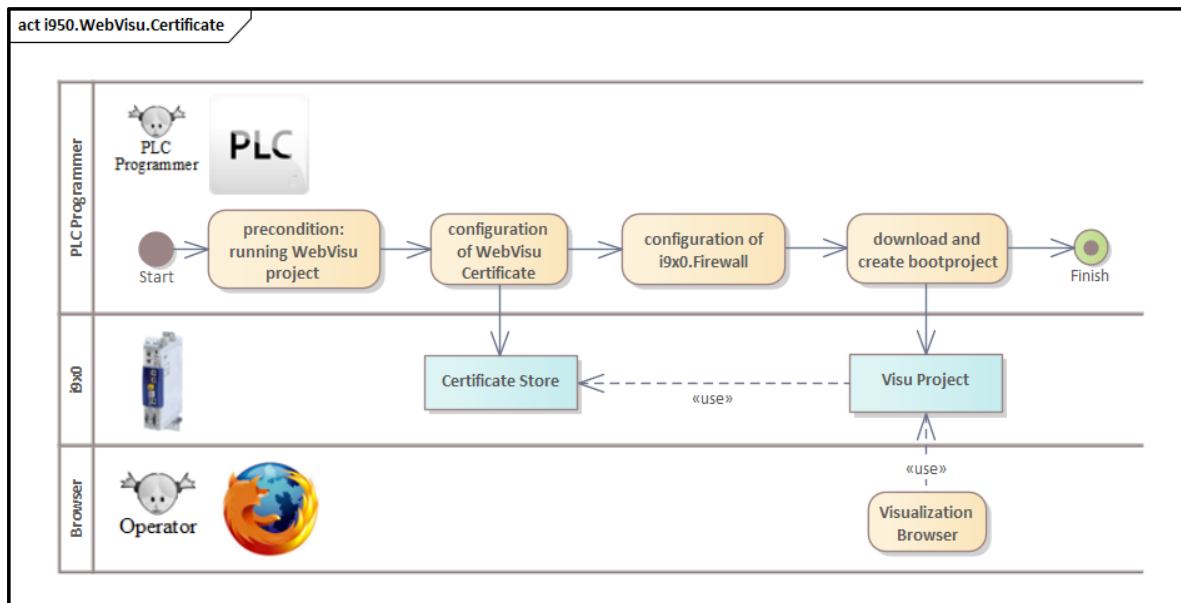
Prepare Visualization for User Management



If the "User Management" tab is not visible, please click on the "Convert to Legacy" button.

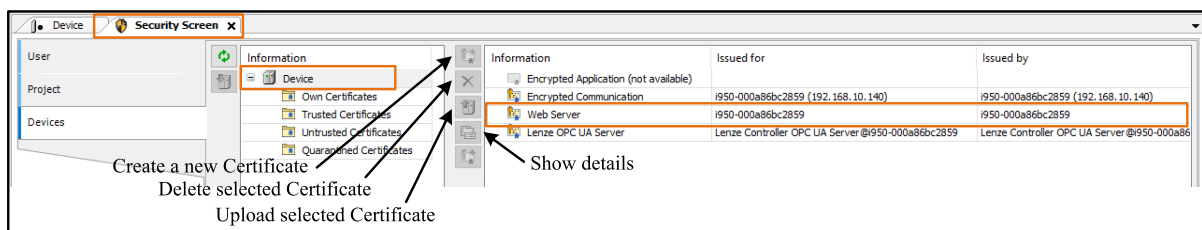
## i9x0.WebVisu.Certificate

For using the http security protocol, WebVisu also has the option to communicate via https. This functionality is available from version V2.0.0 on.



Activity Diagram

To use this communication, please follow these steps:



Handling the Certificate for the WebServer

1. Open the Security Screen via the security icon on the bottom right corner, or via the PLC Designer Menu / View / Security Screen.
2. Select the Devices tab and click Devices
3. Refresh the Certificate Store.
4. The used certificate is located in the placeholder with the name "Web Server".
5. After selecting this "Web Server" certificate, the user can delete this certificate and generate a new one. The user can upload the public certificate or can show the details of it.
6. When changing the certificate, please stop and start the i9x0, to activate the changes.



It is strongly recommended to activate the i9x0.Firewall (refer to chapter /Security Functions/i9x0.Firewall). The activation of the Firewall will block the port 8080, so that the browser cannot connect to the port 8080 via http anymore.

Now, the visualization can be shown in a browser of a panel when connecting to the IP address, the port 443 and the name of the htm file (shown in the WebVisu-Tab), e.g.:

<https://192.168.10.140:443/webvisu.htm>

## i9x0 servo inverters

i9x0.DeviceReplacement

---



On some browsers, a warning message appears that the https connection is based on a self-signed certificate and therefore cannot be checked in a PKI structure. This warning message must be acknowledged so that the visualization can be displayed.

## Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

### i9x0.AccountManagementGuidelines

The Account Management Guidelines of the i9x0 servo inverter are described below. The focus here is on i9x0.UserManagement and the SSH / SFTP access.

#### i9x0.AccountManagementGuidelines :: i9x0.UserManagement

##### Default / Factory Settings:

The User Management of the i9x0 servo inverter is deactivated and must be activated via the PLC Designer. If this is done, the following accounts are automatically created by default:

- <name> (user) | "Administrator" (group) | <password> (password)  
 <name> and <password> must be assigned upon activation of the User Management.
- "Anonymous\_OPCUAServer" (user) | "Anonymous\_OPCUAServer" (group) | "" (password)  
 The empty string password is not relevant, as this user is intended exclusively for anonymous use of the OPC UA server, and it is precisely this anonymous use that does not require a password.
- "EngineeringItf" (user) | "Engineering" (group) | DefaultPassword (password)  
 For reasons of compatibility with older firmware versions, this default user is provided with a default password.

##### Account Handling:

- It is recommended to remove the "EngineeringItf" (user), which is included due to compatibility with older firmware versions, when reconfiguring or to individualize its password.
- New users and groups can be defined using the PLC Designer.

##### Policies:

The Runtime Password Policy is deactivated by default. It is recommended to activate it and adapt it to the current password strength requirements. Current default settings after activation are:

- Minimum length = 8
- Number of unique characters = 4
- Requires lowercase letter = activated
- Requires uppercase letter = activated
- Requires digit = activated
- Requires special character = activated
- Must not contain username = activated

#### Controller.AccountManagementGuidelines :: SFTP

##### Default / Factory Settings:

By default, no customer keys are present in the delivery state.

# i9x0 servo inverters

## Security data

### Key Handling:

- The customer can store their own customer key.

### Policies:

The customer.pkk customer key has the following requirements:

- RSA
- min. 2048 Bits

## i9x0.Firewall : PortList with deactive firewall

### Port List with deactivated firewall

The following table shows the ports, scanned with nmap -sT (TCP connect scan) without activated i9x0.Firewall.

Open TCP Ports with deactivated i9x0.Firewall

| Port      | Engineering Port X16                        | PROFINET Module X256/X257                | Ethernet/IP Module X266/X267             | EoE via onboard EtherCAT X236/X237          | Protocol                                                                             |
|-----------|---------------------------------------------|------------------------------------------|------------------------------------------|---------------------------------------------|--------------------------------------------------------------------------------------|
| 22/tcp    | <input checked="" type="checkbox"/> open*1) | <input type="checkbox"/> filtered        | <input type="checkbox"/> filtered        | <input checked="" type="checkbox"/> open*1) | <a href="#">Secure Shell (SSH)</a>                                                   |
| 80/tcp    | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered        | <input type="checkbox"/> filtered        | <input checked="" type="checkbox"/> open    | <a href="#">Hypertext Transfer Protocol (HTTP)</a>                                   |
| 443/tcp   | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open | <input checked="" type="checkbox"/> open | <input checked="" type="checkbox"/> open*3) | <a href="#">Secure Hypertext Transfer Protocol (HTTPS)</a>                           |
| 1217/tcp  | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered        | <input type="checkbox"/> filtered        | <input checked="" type="checkbox"/> open    | <a href="#">PLC-Designer Gateway-Search</a>                                          |
| 4840/tcp  | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open | <input checked="" type="checkbox"/> open | <input checked="" type="checkbox"/> open    | <a href="#">(OPC UA) OPC Unified Architecture</a>                                    |
| 6000/tcp  | <input checked="" type="checkbox"/> open*2) | <input type="checkbox"/> filtered        | <input type="checkbox"/> filtered        | <input checked="" type="checkbox"/> open*2) | <a href="#">EtherCAT Master Diagnosis</a>                                            |
| 8080/tcp  | <input checked="" type="checkbox"/> open*3) | <input type="checkbox"/> filtered        | <input type="checkbox"/> filtered        | <input checked="" type="checkbox"/> open*3) | <a href="#">Web Visu Server (only available for the extended Controller variant)</a> |
| 9410/tcp  | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open | <input checked="" type="checkbox"/> open | <input checked="" type="checkbox"/> open    | <a href="#">GCI</a>                                                                  |
| 11740/tcp | <input checked="" type="checkbox"/> open    | <input checked="" type="checkbox"/> open | <input checked="" type="checkbox"/> open | <input checked="" type="checkbox"/> open    | <a href="#">PLC-Designer Gateway</a>                                                 |
| 44818/tcp | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered        | <input checked="" type="checkbox"/> open | <input type="checkbox"/> filtered           | <a href="#">EtherNET/IP Messaging'</a>                                               |
| 47877/tcp | <input checked="" type="checkbox"/> open*1) | <input type="checkbox"/> filtered        | <input type="checkbox"/> filtered        | <input checked="" type="checkbox"/> open*1) | <a href="#">SFTP (SSH File Transfer Protocol)</a>                                    |

\*1) For more information, please refer chapter [i9x0.SSHServer](#): Combination of SSH and SFTP via Ports and Networks'

\*2) Port 6000/tcp is only open, if the application contains an EtherCAT master object. For example, if 0x4000 is set to 'CIA 402 [0]', there is no EtherCAT master object available, and therefore the port 6000/tcp is closed. On the other hand, if 0x4000 is set to 'TA Table Positioning [20]' and 0x2371:009 is set to 'Master [1]', there is an EtherCAT master object available, and therefore the port 6000/tcp is open.

\*3) Port 8080/tcp is only open, if the 'Extended for customer specific devices only' variant of i950 is used.

The following table shows the ports, scanned with nmap -sU (UDP scan) without activated i9x0.Firewall.

Open UDP ports with deactivated i9x0.Firewall

| Port                                         | Engineering Port X16                                   | PROFINET Module X256/X257                   | Ethernet/IP Module X266/X267                | EoE via onboard EtherCAT X236/X237                     | Protocol                                       |
|----------------------------------------------|--------------------------------------------------------|---------------------------------------------|---------------------------------------------|--------------------------------------------------------|------------------------------------------------|
| 68/udp                                       | <input type="checkbox"/> closed                        | <input type="checkbox"/> open   filtered    | <input type="checkbox"/> open   filtered    | <input type="checkbox"/> open   filtered               | DHCP Client                                    |
| 123/udp                                      | <input type="checkbox"/> closed                        | <input type="checkbox"/> open   filtered    | <input type="checkbox"/> open   filtered    | <input type="checkbox"/> open   filtered               | <a href="#">NTP Client</a>                     |
| 161/udp                                      | <input type="checkbox"/> closed                        | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> open   filtered    | <input type="checkbox"/> open   filtered               | SNMP Client                                    |
| 1740/udp<br>1741/udp<br>1742/udp<br>1743/udp | <input checked="" type="checkbox"/> open   filtered*1) | <input type="checkbox"/> open   filtered*1) | <input type="checkbox"/> open   filtered*1) | <input checked="" type="checkbox"/> open   filtered*1) | <a href="#">PLC-Designer UDP Communication</a> |
| 3677/udp                                     | <input type="checkbox"/> closed                        | <input type="checkbox"/> open   filtered    | <input type="checkbox"/> open   filtered    | <input type="checkbox"/> open   filtered               | ESDCP                                          |

\*1) Due to the scanning properties of nmap for UDP ports, these udp ports are displayed as 'open | filtered'. However, UDP communication can only take place via the engineering port and not via PROFINET or EtherNET/IP.

### i9x0.Firewall : PortList with activated firewall and default parameter set

The following table shows the ports, scanned with nmap -sT (TCP connect scan) with activated i9x0.Firewall and a default parameter set.

Open TCP ports with activated i9x0.Firewall and default parameter set

| Port      | Engineering Port X16                        | PROFINET Module X256/X257         | Ethernet/IP Module X266/X267                | EoE via onboard EtherCAT X236/X237       | Protocol                                                   |
|-----------|---------------------------------------------|-----------------------------------|---------------------------------------------|------------------------------------------|------------------------------------------------------------|
| 22/tcp    | <input checked="" type="checkbox"/> open*1) | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered        | <a href="#">Secure Shell (SSH)</a>                         |
| 80/tcp    | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered        | <a href="#">Hypertext Transfer Protocol (HTTP)</a>         |
| 443/tcp   | <input checked="" type="checkbox"/> open*3) | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered        | <a href="#">Secure Hypertext Transfer Protocol (HTTPS)</a> |
| 1217/tcp  | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered        | <a href="#">PLC-Designer Gateway-Search</a>                |
| 4840/tcp  | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered           | <input checked="" type="checkbox"/> open | <a href="#">Lenze OPC-UA Server</a>                        |
| 6000/tcp  | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered        | <a href="#">EtherCAT Master Diagnosis</a>                  |
| 8080/tcp  | <input type="checkbox"/> filtered*3)        | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered        | <a href="#">Web Visu Server</a>                            |
| 9410/tcp  | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered        | <a href="#">Parameter Communication GCI</a>                |
| 11740/tcp | <input checked="" type="checkbox"/> open    | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered        | <a href="#">PLC-Designer Gateway</a>                       |
| 44818/tcp | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered | <input checked="" type="checkbox"/> open*2) | <input type="checkbox"/> filtered        | <a href="#">EtherNET/IP Messaging</a>                      |
| 47877/tcp | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered | <input type="checkbox"/> filtered           | <input type="checkbox"/> filtered        | <a href="#">SFTP (SSH File Transfer Protocol)</a>          |

# i9x0 servo inverters

## Security data

\*1) For more information, please refer chapter [i9x0.SSHServer](#): Combination of SSH and SFTP via Ports and Networks'

\*2) Port 44818/tcp is always open and cannot closed via the i9x0.Firewall, because it is a mandatory port for EtherNET/IP.

\*3) Port 8080/tcp is only open, if the 'Extended for customer specific devices only' variant of i950 is used and will be filtered if the firewall with default parameter set is activated.

The following table shows the ports, scanned with nmap -sU (UDP scan) with activated i9x0.Firewall and default parameter set.

Open UDP ports with activated i9x0.Firewall and default parameter set

| Port                                         | Engineering Port X16                              | PROFINET Module X256/X257                            | Ethernet/IP Module X266/X267                         | EoE via onboard EtherCAT X236/X237        | Protocol                                       |
|----------------------------------------------|---------------------------------------------------|------------------------------------------------------|------------------------------------------------------|-------------------------------------------|------------------------------------------------|
| 68/udp                                       | <input type="checkbox"/> open filtered            | <input type="checkbox"/> open filtered               | <input type="checkbox"/> open filtered               | <input type="checkbox"/> open filtered    | DHCP Client                                    |
| 123/udp                                      | <input type="checkbox"/> open filtered            | <input type="checkbox"/> open filtered               | <input type="checkbox"/> open filtered               | <input type="checkbox"/> open filtered    | <a href="#">NTP Client</a>                     |
| 161/udp                                      | <input type="checkbox"/> open filtered            | <input checked="" type="checkbox"/> open             | <input type="checkbox"/> open filtered               | <input type="checkbox"/> open filtered    | SNMP                                           |
| 1740/udp<br>1741/udp<br>1742/udp<br>1743/udp | <input checked="" type="checkbox"/> open filtered | <input checked="" type="checkbox"/> open filtered*1) | <input checked="" type="checkbox"/> open filtered*1) | <input type="checkbox"/> open filtered*1) | <a href="#">PLC-Designer UDP Communication</a> |
| 3677/udp                                     | <input type="checkbox"/> open filtered            | <input type="checkbox"/> open filtered               | <input type="checkbox"/> open filtered               | <input type="checkbox"/> open filtered    | ESDCP                                          |

\*1) Due to the scanning properties of nmap for UDP ports, these udp ports are displayed as 'open|filtered'. However, UDP communication can only take place via the engineering port and not via PROFINET or EtherNET/IP.



### i9x0.EncryptedCommunication.PLCDesigner : Certificate

The automatically created certificate for Encrypted Communication has the following identifiers:

Fields of the Certificate for the Encrypted Communication

| Field                     | Description and Value                                                                                     |
|---------------------------|-----------------------------------------------------------------------------------------------------------|
| Issuer, SERIALNUMBER      | The serial number is the MAC Address of the X16 network, the Engineering Port, of the i9x0 servo inverter |
| Issuer, Unstructured Name | Device: Controller,<br>e.g. Device: i950 (BS-STO)                                                         |
| Issuer, Unstructured Name | Vendor: Lenze                                                                                             |
| Issuer, CN                | Combination off device type, device MAC address and device IP address,<br>e.g. i950-MAC (192.168.10.140)  |
| Valid from<br>Valid to    | The automatically created certificate is valid for 30 days.                                               |

### i9x0.CertificateStore.SysLogProxy : Certificate

The automatically created certificate for the SysLog Proxy has the following identifiers:

Fields of the Certificate for the SysLog Proxy

| Field                  | Description and Value                                                                                                                                                                                                                                                   |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Issuer                 | CN = Lenze Controller:SysLogProxy@c550-000a86b9ec22<br>The CN is 'Lenze Controller:SysLogProxy@' with the controller type and the MAC address of the X16 engineering port of the controller.<br>OU = Controls<br>O = Lenze<br>L = Aerzen<br>S = Niedersachsen<br>C = DE |
| Valid from<br>Valid to | The automatically created certificate is valid for 60 year.                                                                                                                                                                                                             |

### i9x0.SysLog : MonitoredFilesAndDirectories

This chapter lists the files and directories that are monitored in the file monitoring. For more information, refer to chapter [i9x0.SysLog](#)

The recursion depth is specified for directories being monitored. The recursion depth of the monitoring is also specified here. A recursion depth of 0 means that only the directory and its files are monitored. A recursion depth of 1 means that the directory and its subdirectories are monitored. A recursion depth of \* means that all subdirectories and their files are monitored.

#### Static monitoring of files:

- /sdcard/Licenses\_do\_not\_delete/LicenseFile.lic
- /sdcard/Licenses\_do\_not\_delete/VerificationFile.lic

# i9x0 servo inverters

## Security data

---

- /data\_usr/LicenseFile.lic
- /sdcard/.enable-ssh
- /sdcard/ip.txt
- /sdcard/ip\_old.txt
- /sdcard/plc/CODESYSControl\_User.cfg
- /sdcard/plc/CODESYSControl\_UserSec.cfg
- /sdcard/plc/SysFileMap.cfg
- /sdcard/plc/prg/pta1/.UserDatabase.csv
- /sdcard/plc/prg/pta1/.GroupDatabase.csv
- /sdcard/plc/prg/pta1/.UserMgmtRightsDB.lcsv
- /sdcard/plc/prg/pta1/.UserMgmtExt.csv
- /sdcard/plc/prg/pta1/.PswDB.csv
- /sdcard/plc/prg/pta1/ecat\_master\_0.xml
- /sdcard/plc/prg/pta1/ecat\_master\_0\_boot.xml
- /sdcard/plc/prg/pta1/ParameterSets/ParSetConfig.cprm
- /sdcard/public-key/customer.key
- /sdcard/update.fw
- /data\_usr/dhcpd.conf
- /data\_usr/dhcpd.conf.md5sum

### Static monitoring of directories:

- /sdcard/plc/.pki/ (recursiv \*)
- /sdcard/plc/prg/PlcParameterSet/ (recursiv \*)
- /sdcard/plc/prg/pta1/Recipes/ (recursiv \*)
- /sdcard/firmware/ (recursiv \*)

### Dynamic monitoring of files:

- /sdcard/plc/prg/pta1/\*.app
- /sdcard/plc/prg/pta1/\*.crc
- /sdcard/\*.lpk

### Dynamic monitoring of directories:

- n.r.

## o450 Motor Driven Roller

The Motor Driven Roller is referred to as the o450 and is designed as a single roller in applications.

## Product description

## Product identification

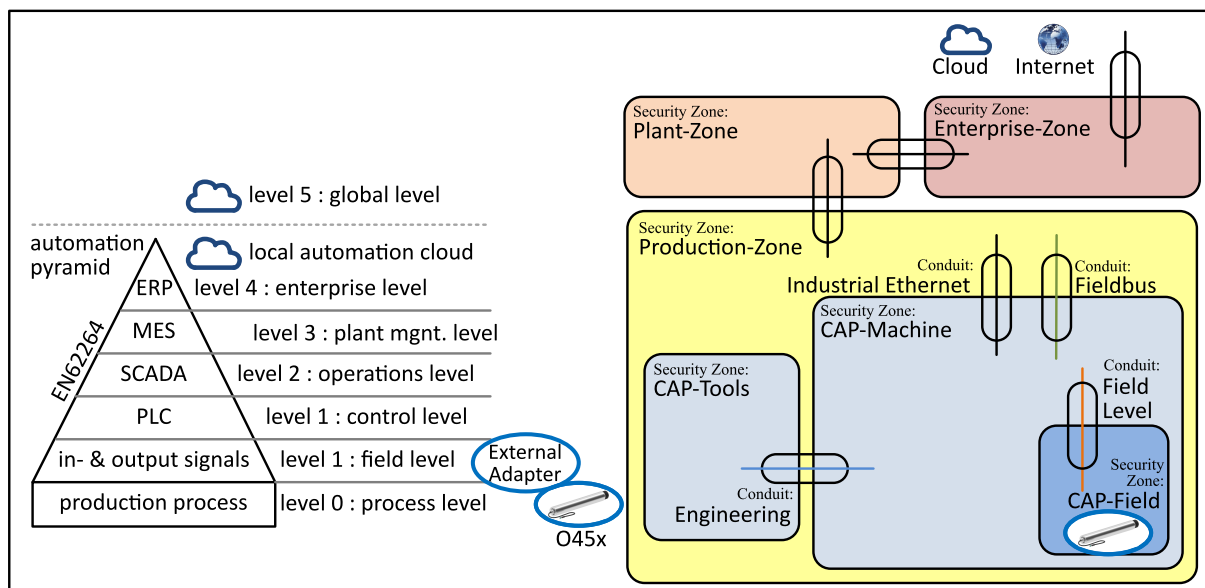
This documentation applies to the "Motor Driven Roller" product family, which consists of the following components and their identification:

Name of product and product ID

| Name of product     | Product ID         |
|---------------------|--------------------|
| Motor Driven Roller | O45ASxxxxxxxxxxxxx |

### Location in the network

These components are located in the automation pyramid at the control level. Furthermore, they are located in the security zone "CAP-Field" ([Zones and conduits](#)).



### Location in the Network

The components addressed here have one relevant interfaces:

- Conduit: Field Level

The Motor Driven Rollers are located in the process level and have only one interface for the external adapter which is located at the field level-This adapter realizes the conduit field level. The Motor Driven Roller interface is not designed as a data fieldbus, but as a dedicated I/O interface. The limited data-related functions are described below.

### Intended purpose

The intended use of these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding cyber security are discussed.

# o450 Motor Driven Roller

## Security mechanisms

- 
- These components are professional equipment and may only be commissioned and decommissioned by specialists.
  - These components also require maintenance during their life cycle, which must be carried out by the operator.
  - Modifications to the firmware or hardware of the component are not permitted.
  - If these components are taken out of operation or disposed of, the instructions here in the documentation must be observed.

### Intended environment

The intended environment for these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding cyber security are discussed.

- As these components are decentralized, a closed control cabinet is out of the question. Therefore, physical access protection is required.
- The components are not operated directly on the open Internet, but must also be operated by the operator via protection systems such as firewall, IDS, IPS, ...
- Deactivate all unused interfaces and/or protocols, both for the components mentioned here and for all components that are connected to the network.
- The more security-critical an application is, the more systems should be separated. Only combine tasks on one component if they are in the same risk classification.
- Wherever possible, use a Defense-in-Depth Concept in the environment of this component.
- Use appropriate authentication mechanisms. This applies, for example, to passwords that have the necessary complexity and an appropriate life cycle. The current state of the art must be taken into account here.
- Handle secrets, such as passwords, appropriately. The focus here is on the handling of secrets on the components noted here, but also on the data stored in the environment of these components.
- Validate all input options for validity. Pay attention to all human user interfaces as well as the machine software interfaces.
- Evaluate the environment, the technical task to be performed and the existing component security in a security-critical consideration and assess whether additional protective measures are necessary for your application.

### Security key indicators

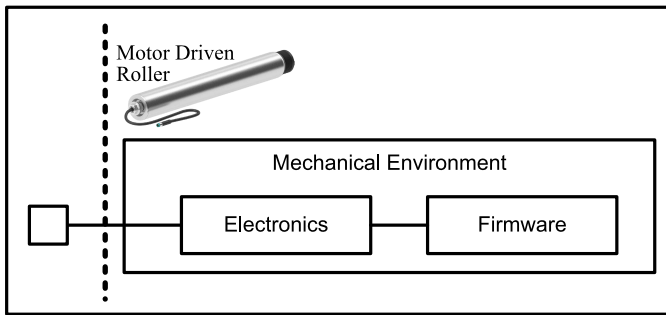
Security key indicator (in accordance with IEC 62443-4-2):

- These components are considered embedded devices (EDR).
- These components have a security level of SL-C 0, because no certification was carried out.
- These components have the technical functionality to enable an SL-vector from SL-C (MotorDrivenRoller)={ IAC=n.a.; UC=1; SI=1; DC=n.a.; RDF=n.a.; TRE=n.a.; RA=1 }.

## Security mechanisms

### Product Defense in Depth

The following image shows the Defense in Depth product concept. For the sake of clarity, some details have been deliberately omitted.



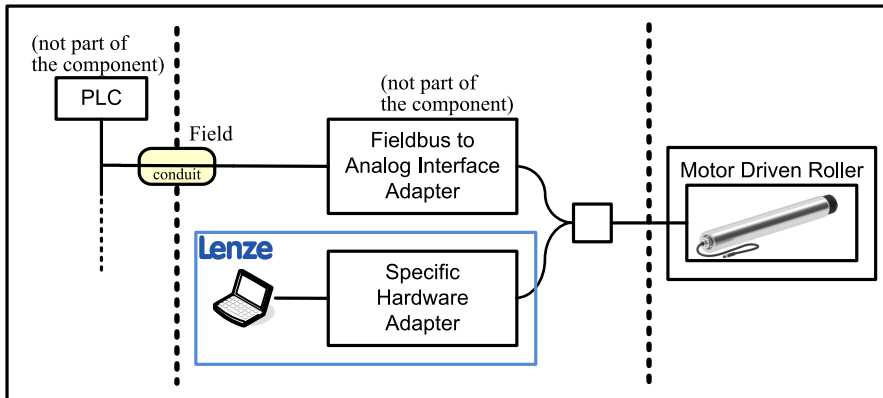
Product Defense in Depth

The core concept of the Motor Driven Roller is a mechanical encapsulation of all relevant electronic parts and the firmware running on them. Here, the firmware is imprinted on electronics by the manufacturer and these electronics are pressed into a mechanical environment of the Motor Driven Roller itself. Once assembled, this connection can no longer be separated non-destructively.

As this component is part of the Security Zone Field and cannot be used independently, requiring upstream electronics in order to be operated on a network, it is not necessary to provide user management or other access authorizations. These must be realized in the upstream electronics.

### Expected Defense in Depth in the environment

The following image shows the Expected Defense in Depth in the environment of the Motor Driven Roller.



Expected Defense in Depth in the environment

#### Conduit Field:

- It is not possible to operate the Motor Driven Roller directly on the Conduit Field, as it only has an analog interface and no fieldbuses on board.
- Additional components are required to use a Motor Driven Roller on a fieldbus. These are not sold by Lenze, but components that are freely available on the market can be used for this purpose (e.g. the AS-Interface-Module G20 from PEPPERL+FUCHS).
- All cyber security protection mechanisms required for the customer's application must be implemented here or in a higher-level logic.

#### General Environment:

- General physical access protection must be provided for the components.

# o450 Motor Driven Roller

Commissioning and hardening notes and organizational measures

---

## Security mechanisms:

The following security functions are included in the listed components:

- MotorDrivenRoller.FirmwareUpdate

## Commissioning and hardening notes and organizational measures

The following commissioning instructions must be followed:

### General instructions:

- As far as possible, avoid connecting the Motor Driven Roller (and the upstream electronics required for operation) to open networks or the internet. We recommend organizational and technical actions for the Motor Driven Roller and the required upstream electronics.
- For protection, additionally use data link layers such as a VPN for remote access.
- Install Firewall mechanisms, IPS (Intrusion Protection Systems) and IDS (Intrusion Detection Systems).
- Connect external devices upstream to provide protection against DoS (Denial of Service) or DDoS (Distributed Denial of Service).
- Restrict physical access to authorized persons only.

### Commissioning and hardening instructions:

- Check the security maintenance instructions in the documentation of the upstream electronics to plan the commissioning and hardening procedure.
- This component, considered on its own, does not require special commissioning and hardening procedures.

### Periodic Security Maintenance:

- Check the security maintenance instructions in the documentation of the upstream electronics to plan the periodic security maintenance.
- This component, considered on its own, does not require periodic security maintenance.

### Decommissioning Instructions:

- Check the security maintenance instructions in the documentation of the upstream electronics to plan the decommissioning.
- This component, considered on its own, does not require any decommissioning procedures.

### Removal of product from environment:

- Check the security maintenance instructions in the documentation of the upstream electronics to plan the decommissioning.
- This component, considered on its own, does not require any removal procedures from the environment.

## Security functions

This chapter describes the individual supported cyber security-relevant functions and their application.

---

## MotorDrivenRoller.FirmwareUpdate

This functionality has been available since the release of Motor Driven Roller Generation A (product ID: O45Axxxxxxxxxxxxxx).

The following requirements are necessary to carry out a firmware update:

- Only the manufacturer Lenze is able to update the firmware.
- Since the firmware does not have any security-relevant functions, it is not necessary to install cyclical updates from a cyber security perspective.
- To install a firmware, the functionality of the digital and analog inputs and outputs are used as well as special hardware and software and procedures are required.

## Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

## MotorDrivenRoller.AccountManagementGuidelines

Since the Motor Driven Roller has no user management, there are no account management guidelines. The Account Management Guidelines described by the external component must be applied to the upstream component required for operation on a fieldbus.

# m300 Lenze Smart Motor

Product description

---

## m300 Lenze Smart Motor

The Lenze Smart Motor reduces the number of different drive versions by up to 70%. Converter and starter do not feature, fixed speeds can be set at will and there are numerous integrated functions for materials handling applications. The Lenze Smart Motor also complies with the highest energy efficiency requirements and can be very conveniently operated using a smartphone.

## Product description

### Product identification

This documentation applies to the m300 Lenze Smart Motor product family consists of the following components and their identification:

Name of product and product ID

| Name of product        | Product ID    |
|------------------------|---------------|
| m300 Lenze Smart Motor | MSEMAxxxxx-xx |

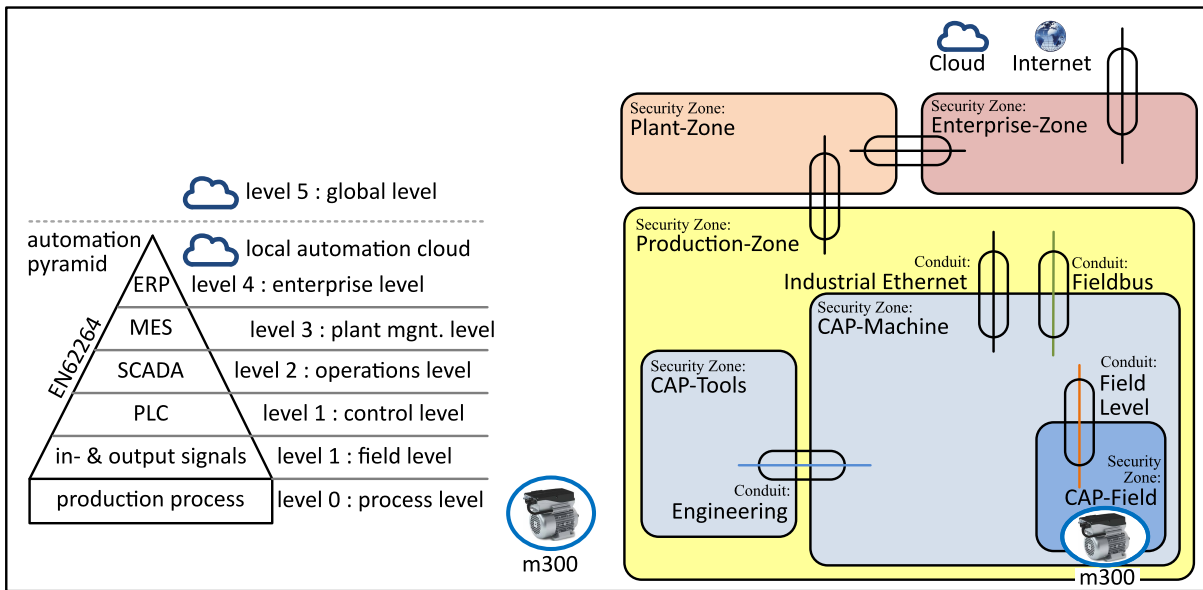
Name of accessories

| Name of accessory     | Product ID                                    |
|-----------------------|-----------------------------------------------|
| Lenze Smart Motor App | Android Play Store / Lenze Smart Motor        |
| EASY Starter          | refer to chapter <a href="#">EASY Starter</a> |
| Conoverter USB -> NFC | EZAETF001                                     |

### Location in the network

These components are located in the automation pyramid at the control level. Furthermore, they are located in the security zone "CAP-Field" ([Zones and conduits](#)).





Location in the Network

The components addressed here have two relevant interfaces:

- Conduit: Field Level

The Field Level interface refers to the three digital inputs and one digital output. With the help of the inputs, the user can specify the defined speeds and receive information about an existing error via the output. These interfaces are negligible from a cyber security point of view as they do not support any data protocols.

- Conduit: Engineering

The m300 Lenze Smart Motor has a smart interface via NFC (near field communication) to carry out parameterization in two ways. Way (a) refers to the use of a Smart Motor App and the NFC function of a smartphone, way (b) refers to the use of an EASY Engineering Tools Starter and simultaneous use of a USB -> NFC adapter.

## Intended purpose

The intended use of these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding Cyber Security are discussed.

- These components are professional equipment and may only be commissioned and decommissioned by specialists.
- These components also require maintenance during their life cycle, which must be carried out by the operator.
- Modifications to the firmware, software or hardware of the components are not permitted.
- If these components are taken out of operation or disposed of, the instructions here in the documentation must be observed.

## Intended environment

The intended environment for these components is described in the application as directed and can be found in the operating instructions for the respective component. In the following, some specifics regarding Cyber Security are discussed.

# m300 Lenze Smart Motor

## Security mechanisms

- 
- As these components are decentralized, a closed control cabinet is out of the question. Therefore, physical access protection is required.
  - The components are not operated directly on the open Internet, but must also be operated by the operator via protection systems such as firewall, IDS, IPS, ... .
  - Deactivate all unused interfaces and/or protocols, both for the components mentioned here and for all components that are connected to the network.
  - The more security-critical an application is, the more systems should be separated. Only combine tasks on one component if they are in the same risk classification.
  - Wherever possible, use a Defense-in-Depth Concept in the environment of this component.
  - Use appropriate authentication mechanisms. This applies, for example, to passwords that have the necessary complexity and an appropriate life cycle. The current state of the art must be taken into account here.
  - Handle secrets, such as passwords, appropriately. The focus here is on the handling of secrets on the components noted here, but also on the data stored in the environment of these components.
  - Validate all input options for validity. Pay attention to all human user interfaces as well as the machine software interfaces.
  - Evaluate the environment, the technical task to be performed and the existing component security in a security-critical consideration and assess whether additional protective measures are necessary for your application.

### Security key indicators

Security key indicator (in accordance with IEC 62443-4-2):

- These components are considered embedded devices (EDR).
- These components have a security level of SL-C 0, because no certification was carried out.
- These components have the technical functionality to enable an SL-vector from SL-C (m300)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

## Security mechanisms

### Product Defense in Depth

The customer interface to the m300 Smart Motor is the NFC. The parameters can be set via this interface if the m300 is not connected to main voltage supply.

In rare cases, the housing of the m300 Smart Motor must be opened by the customer in order to connect the m300 electrically.

Depending on the machine risk analysis (and the criticality of the corresponding assessment), the customer must affix a security seal to the housing. However, this will not be necessary due to the simple application and in most cases uncritical use and should only be implemented in exceptional cases.

### Expected Defense in Depth in the environment

The interface for operation are the three digital inputs and the digital output.

If the Smart Motor app is installed on a smartphone by the customer, it must be ensured that this app is protected by current IT protection measures on the smartphone.

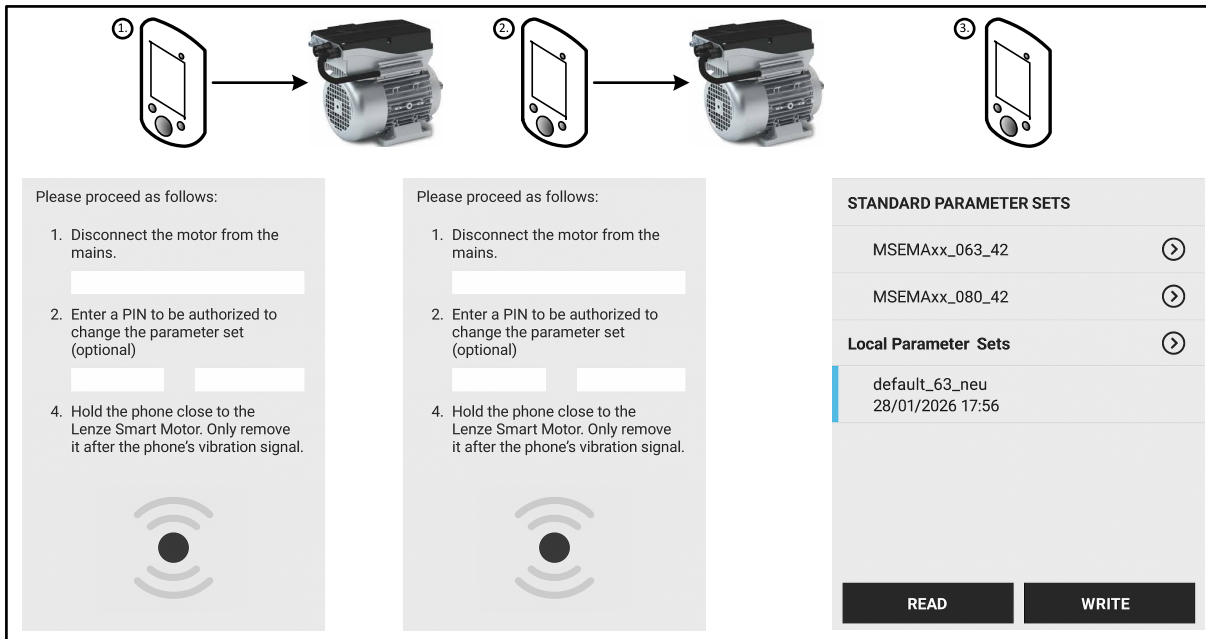
### Security mechanisms:

The following security functions are included in the listed components:

- m300.FirmwareUpdate
- m300.AccessProtection

## Security mechanisms :: Decommissioning

If the m300 Smart Motor is to be taken out of operation, the following steps must be carried out.



m300 Decommissioning

If a pin is set in the m300, it is recommended to remove this pin before decommissioning:

- ( 1 ) Connect Smart Motor App to the m300 Smart Motor  
If a pin is set, this must be taken into account when establishing the connection.
- ( 2 ) Enter an empty pin  
Change the existing pin so that an empty pin is entered and transferred to the m300.
- ( 3 ) Delete parameterset in app  
Select and delete the parameter set in the Smart Motor app.

## Commissioning and hardening notes and organizational measures

The following commissioning instructions must be followed:

### General instructions:

- As far as possible, avoid connecting the m300 Smart Motor (and the upstream electronics, e.g. the Converter USB->NFC required for operation) to open networks or the internet. We recommend organizational and technical actions for the m300 Smart Motor and the required upstream electronics.
- For protection, additionally use data link layers such as a VPN for remote access.
- Install Firewall mechanisms, IPS (Intrusion Protection Systems) and IDS (Intrusion Detection Systems).

# m300 Lenze Smart Motor

## Security functions

---

- Connect external devices upstream to provide protection against DoS (Denial of Service) or DDoS (Distributed Denial of Service).
- Restrict physical access to authorized persons only.

### Commissioning and hardening instructions:

- Check the security maintenance instructions in the documentation of the upstream electronics to plan the commissioning and hardening procedure.
- This component, considered on its own, does not require special commissioning and hardening procedures.
- In most cases, the access authorization described here will be sufficient to cover the typical use case within a machine. However, if the machine risk analysis reveals that there is a particular risk if the housing of the m300 is opened during the life cycle, it is recommended to protect the housing with an appropriate security seal after commissioning. Since in a few cases the housing has to be opened during the installation of the m300, it is not possible to set this seal ex works, but it must be set by the customer (if necessary) after the electrical installation. If there is a corresponding risk within a machine, the manufacturer of the machine will have a corresponding process through its own machine manufacturer seal. This machine manufacturer's seal must then be affixed to the edge of the m300 housing.
- Setting the pin for access protection, refer to chapter [m300.AccessProtection](#).
- If necessary, create a backup for a later restore, refer to chapter [m300.BackupAndRestore](#).

### Periodic Security Maintenance:

- Check the security maintenance instructions in the documentation of the upstream electronics to plan the periodic security maintenance.
- This component, considered on its own, does not require periodic security maintenance.

### Decommissioning Instructions:

- Check the security maintenance instructions in the documentation of the upstream electronics to plan the decommissioning.
- When decommissioning, the instruction refer to chapter [m300.Decommissioning](#) must be observed.

### Removal of product from environment:

- Check the security maintenance instructions in the documentation of the upstream electronics to plan the decommissioning.
- When decommissioning, the instruction refer to chapter [m300.Decommissioning](#) must be observed.

## Security functions

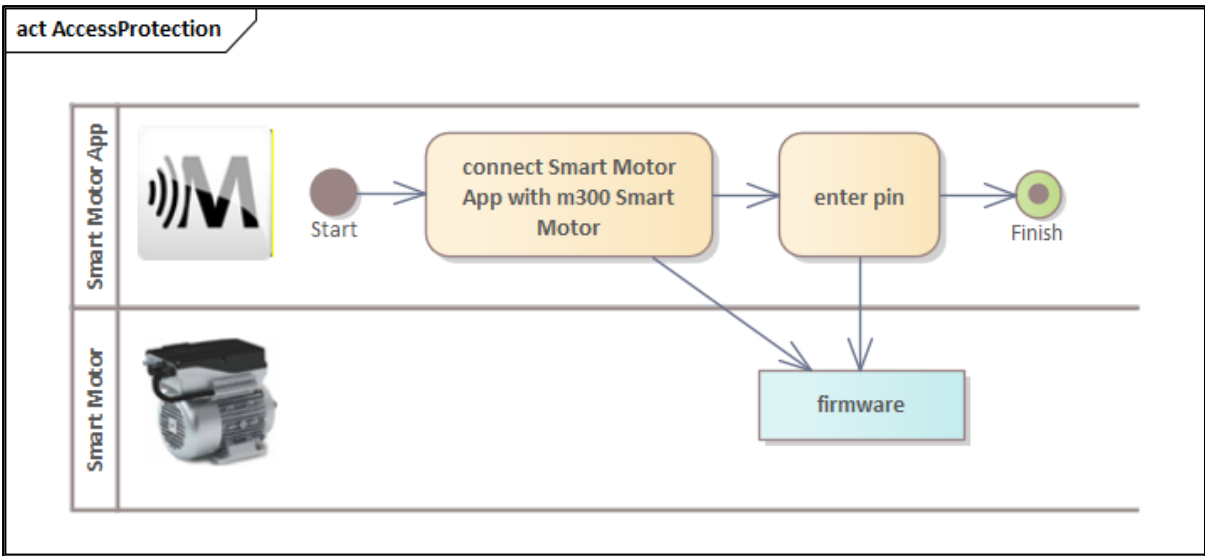
This chapter describes the individual supported cyber security-relevant functions and their application.

### m300.FirmwareUpdate

The m300 does not have a firmware upload that can be carried out by the customer. If a firmware upload is necessary, this must be carried out by Lenze. Any manipulation of the firmware by the user is not permitted. If required, please contact the manufacturer Lenze.

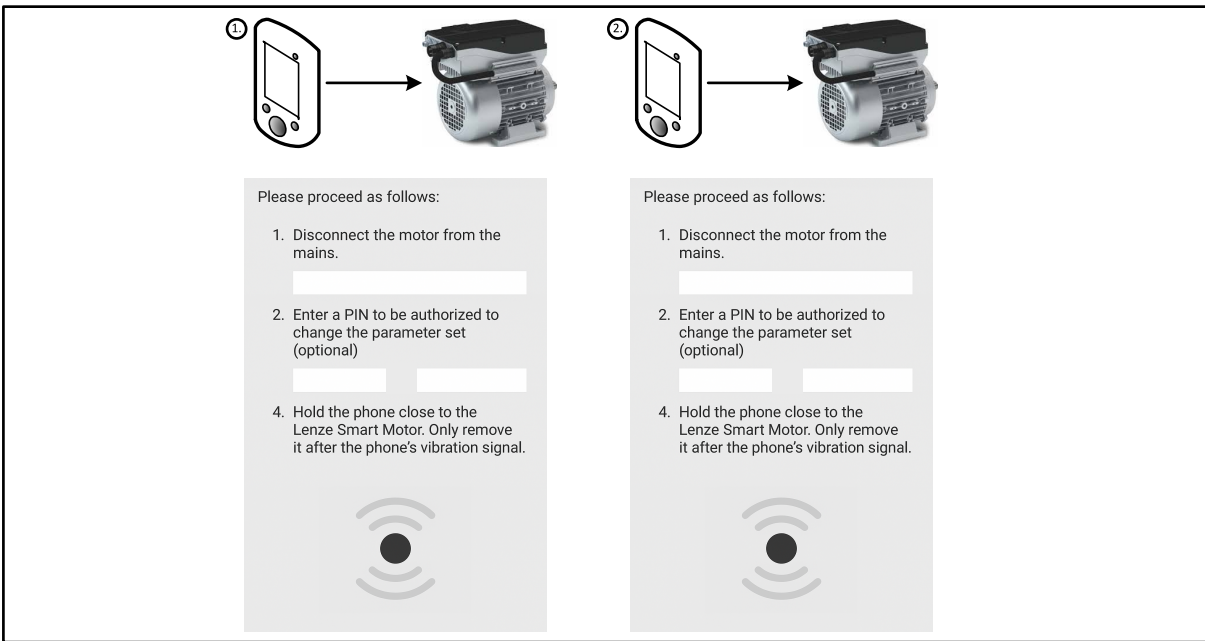
### m300.AccessProtection

The m300 has access protection that can be used by the user.



m300 Access Protection

The procedure is shown in the following figure.



m300 Access Protection

- ( 1 ) Set Pin  
The Smart Motor app must be connected to the m300 Smart Motor. Based on this connection, the access protection (implemented as a pin) can be set.
- ( 2 ) Verify Pin  
To check whether the pin has been set correctly, disconnect the smartphone from the

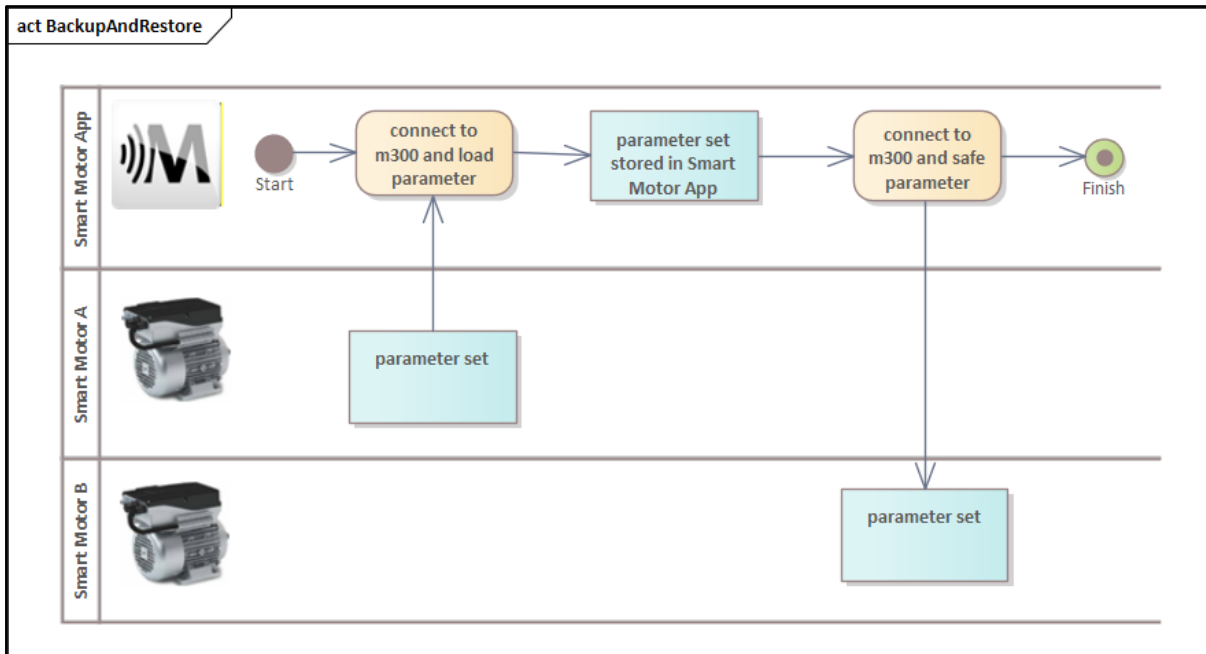
# m300 Lenze Smart Motor

## Security data

m300 and reconnect via NFC. An attempt without a pin must fail and an attempt with a pin must be successful.

### m300.BackupAndRestore

The backup and restore mechanism is shown in the following image.



m300 Backup and Restore

To perform a backup and restore, the following steps must be carried out

- Connect the Smart Motor App to the existing m300 Smart Motor and load the parameter set into the Smart Motor App. If necessary, enter the m300 pin beforehand.
- Replace the m300 Smart Motor.
- Connect the Smart Motor App to the new m300 Smart Motor and save the parameter set in the m300 Smart Motor. If necessary, set the m300 pin.

## Security data

This chapter describes the Account Management Guidelines and provides further information on security-relevant data as required.

### m300.AccountManagementGuidelines

The m300 has access protection with the aid of a pin.

#### m300.AccountManagementGuidelines :: m300.AccessProtection

##### Default / Factory Settings:

The access protection of this pin is not set and has to be activated from the customer.

- Default pin = ""

## Account Handling:

- Changing the pin is possible via the Smart Motor App.

## Policies:

The Pin Policy is:

- Maximum length of digits = 4

