Software manual | EN

Cyber Security

Content

Content

Content

About this documentation

Version	Date
1.0	2023-10-31

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.

Conventions used

This documentation uses the following conventions to distinguish between different types of information:

Type of information	Highlighting	Examples/notes
Numeric notation		
Decimal separator	Point	The decimal point is always used. For example: 1234.56
Hexadecimal number	0x	For hexadecimal numbers, the "0x" prefix is used. Example: 0x60F4
Text		
Program name	» «	»PLC Designer« ...
Variable names	*italics*	By setting *bEnable* to TRUE...
Function blocks	**Bold**	The **L_MC1P_AxisBasicControl** function block ...
Function libraries		The **L_TT1P_TechnologyModules** function library...

Source code	Font
	`"Courier new"`
		...
		dwNumerator := 1;
		dwDenominator := 1;
		...

Hyperlink	underlined	Optically highlighted reference to another topic. It is activated with a mouse-click in this online documentation.
Symbols		
Step-by-step instructions		Step-by-step instructions are indicated by a pictograph.

Variable names

The conventions used by Lenze for the variable names of Lenze system blocks, function blocks, and functions are based on the "Hungarian Notation". This notation makes it possible to identify the most important properties (e.g. the data type) of the corresponding variable by means of its name, e.g. *xAxisEnabled*.

Introduction

To the main product lines of Lenze, Lenze discusses here, without guarantee of completeness or correctness, selected technical issues from our ongoing product development and support. The cyber security documentation informs about typical

- Functional enhancements,
- remedied functional limitations and
- 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 on your own responsibility.

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 only for qualified technical personnel of a business user of Lenze products.
The cyber security documentation is a self-help tool which the user of the cyber security documentation may use exclusively under his own responsibility and to the exclusion of any liability on the part of Lenze.

Disclaimer of liability

Lenze shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the security documentation as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Lenze against existing or future claims of third parties in this connection except where Lenze is mandatorily liable. By using the security documentation you acknowledge that Lenze cannot be held liable for any damage beyond the liability provisions described.

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.

Security information

Lenze provides products and solutions with Industrial Security functions that support the secure operation of systems, machines and networks. In order to protect systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Lenze products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

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

Type of documentation

The strategy regarding cyber security first provides for a description of the status quo and on this basis 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 complete and therefore does not yet reflect the complete picture of the components.

Security strategy

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 personal for security

These three aspects are part of the cyber security consideration in the following standard. The standard IEC 62443 focused 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 goals:

1. Confidentiality
2. Integrity
3. Availability

Cyber security focuses on the assets in the automation system. 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 goals are realized through a combination of security functions in the assets, but also through organizational measures and requirements for the environment of the assets. Only a complete view ensures the necessary protection goals.

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 have a certain influence. However, as long as they run in a time window that does not impair the promised availability, they are considered legitimate. Only when the retroactive effect affects the assigned availabilities are they interpreted as harmful. This can occur, for example, due to excessive load on a processor.

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 whether an unauthorized change of the data has taken place. This can be done on the basis of communicated data (e.g. via Ethernet) or data at rest (e.g. stored files).

Integrity is between a manipulation protection, i.e. a mechanism that securely prevents the change and a manipulation detection, i.e. a mechanism that reliably detects an unauthorized change.

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. This determines which subject is allowed to access which object. The goal is that unauthorized subjects do not get access to the objects. Even with this protection goal, a distinction can be made between confidentiality of moving data (e.g. via Ethernet) or data at rest (e.g. stored files).

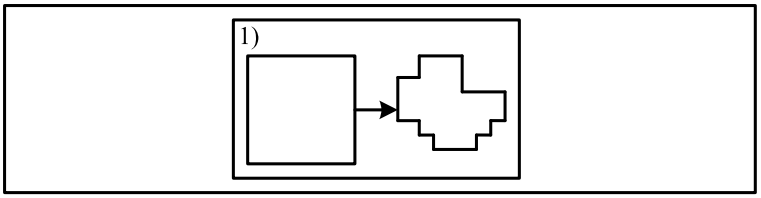
Golden rules for secure systems

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

Due to 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 with 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

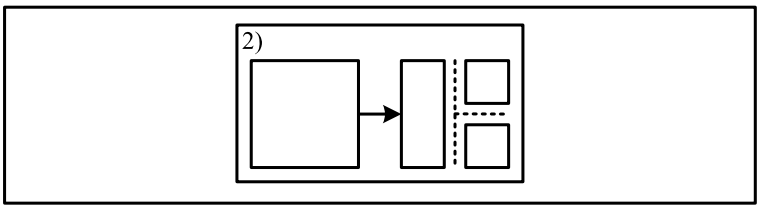
Every used area of a system represents a potential attack surface. The goal is therefore to keep this attack surface as small as possible and thus minimize it. For this purpose, only the functions in the system that are necessary for essential operation should be usable. This applies not only to functions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

The following points need to be optimized:

- Uninstalling or deactivating software packages that are not necessary
- Disable unnecessary services or features
- Check factory settings and restrict them restrictively if necessary
- Restrict user privileges and access rights
- Limitation of 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 principle is a concept for cyber security in which a user is granted only the minimum level of access or authorization required for his or her activity.

Separate Systems



Golden Rule: Separate Systems

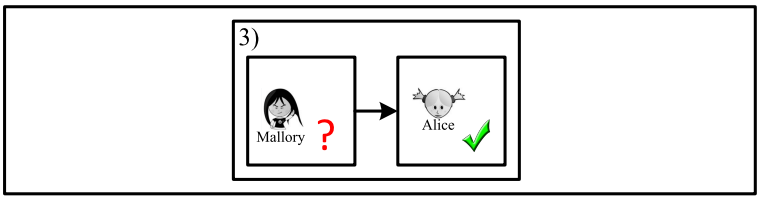
An effective mechanism for security resilience is the defense-in-depth concept. This describes a shell-like structure of the security structure with the background of the cascaded protection mechanisms. Several shells act on different protective mechanisms.

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



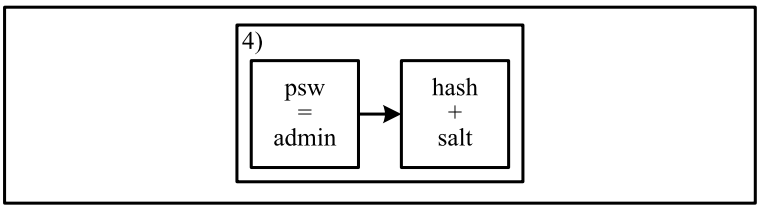
Golden Rule: Appropriate Authentication

As soon as a communication is confidential (at the latest when it crosses a security zone), it must be authenticated. It is independent of whether it is a human communication or a communication of 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 secrecy
- Consideration of the storage of authentication secrecy
- Establishment of a role-based access system and the need-to-have principle (knowledge only if necessary) to be used
- Consistent withdrawal of authorization without necessity
- etc.

Confidential encryption



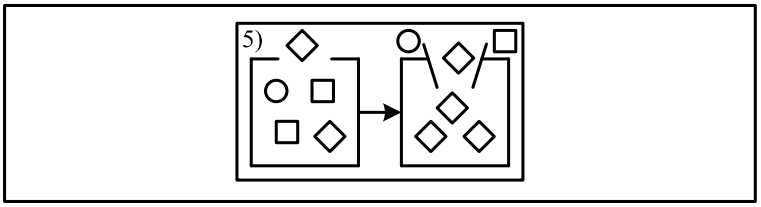
Golden Rule: Confidential encryption

The establishment of this requirement starts with the identification of the trustworthy information. These must be encrypted due to their content that is worthy of protection. Here, the consideration refers to transmitted information, as well as to the dormant 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

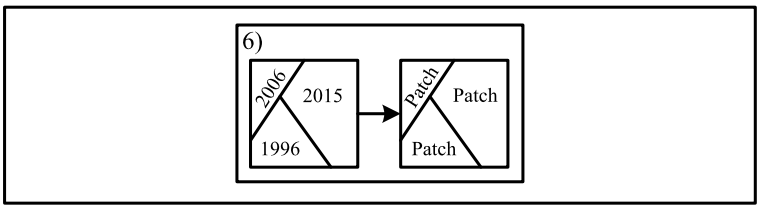
Any input submitted from the outside must be validated for validity. It is irrelevant whether this input is inputted by a human user, a software interface or a device.

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 at an interface for human users is conspicuous)
- Checking the content (e.g. February 31 is not a valid date)
- etc.

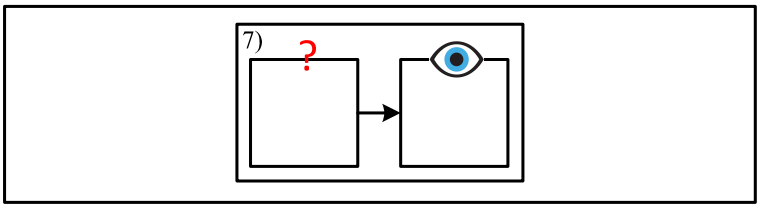
Update regularly



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 mentioned that patches can be introduced by the manufacturer of the components, but also corrective measures can 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 permanently improved.

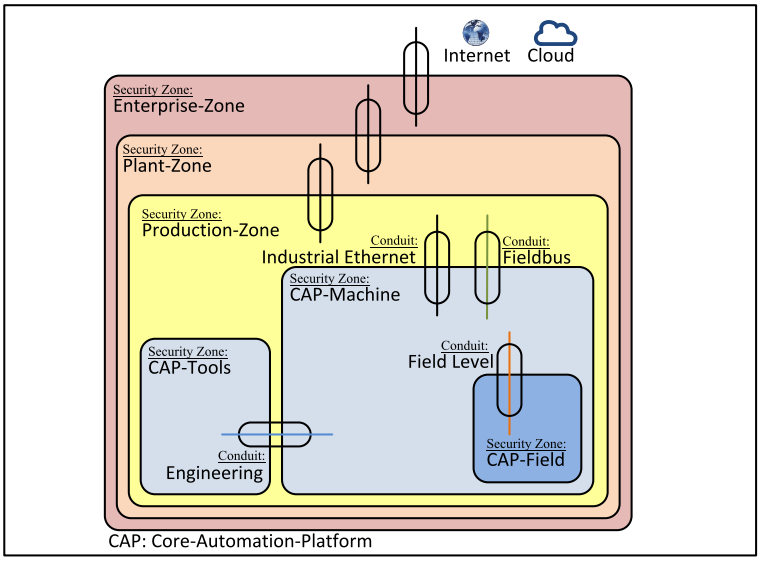
System monitoring must be used. These are advanced firewall systems IPS (Intrusion Prevention Systems) or IDS (Intrusion Detection Systems). As a result, the field of application is observed and measures can be derived directly from it.

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 can be found in the following picture.



Defense in Depth Concept

Here, the protection mechanisms on the operator of a plant fall on Enterprise-, Plant- and Production-Zone. A consideration in accordance with IEC 62443-3-x is recommended here.

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

- Minimize 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 transfer and in rest.
- Risk appropriate authentication methods.
- Organizational measures for protection, when handling with removable data carriers.
- …

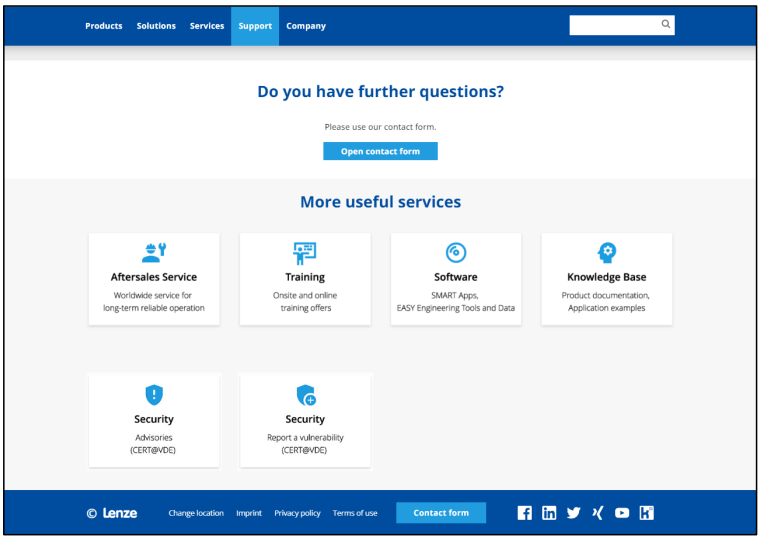
Within the Production-Zone, a security zone "CAP-Machine" is defined. Components in this security zone are permanently active in the machine and must have the same level of protection. In addition, there is a security zone "CAP-Tools", in which all commissioning and maintenance tools are located. This is characterized by the fact that they are not permanently active, but only when necessary. Within the security zone "CAP-Machine" there is a subordinate security zone "CAP-Field". This is characterized by the fact that the components are permanently active in the machine, but they must be protected by organizational measures.

Security management

A Product Security Incident Response Team (PSIRT) is currently being established at Lenze SE. For this purpose, a communication channel has already been made possible via the homepage. Contact us 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://cert.vde.com/de/advisories/vendor/lenze/
  The security Advisories are published here.
- Security Report a vulnerability (link to the CERT@VDE)
  https://cert.vde.com/de/more/report-a-vulnerability/
  Here is the possibility to report a vulnerability.

Basics of security

IEC 62443 terms

Types of Component

IEC 62443-4-2 describes the security requirements for the components. These requirements are divided into foundational requirements (FRs). These are 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 that has a specific purpose with a specific software in 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 to HDR.

Host device requirements (HDR)

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

Network device requirements (NDR)

A device that focuses on network traffic. Here are switches, routers but also firewalls to mention. NDR often combine different network segments. Therefore, the focus here is to be placed on physical and logical network separation.

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 threat e.g. through negligent application of the IT security guideline
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 (which, however, target a wide area and not the 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 with SL-3, also more motivated, has even 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 AL): Currently achievable security level in the target application
- SL-C (Capability SL): Currently achievable security level regardless of the target application

Security Vector

In order to further specify the key figure of the security level, the Security Vector was introduced. Here, the perspective is shifted away from the component towards the foundational requirements (FRs). Each foundational requirement is sorted into the Security Level (SL) and evaluated. This allows different details about the component to be displayed.

The Security Vector is specified in the form:

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

Here, the reference to the component under consideration is given in parentheses and the respective key figures 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) Restrocted Data Flow
- FR6: (TRE) Timely Response to Eventy
- FR7: (RA) Resource Availability

Secure communication

Secure communication serves the purpose of protecting information of data from unauthorized access or transmitting it confidentially. 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 refers to a cryptographic protocol for secure communication over unsecured networks. A common use is the use of a remote command line. On this basis, other protocols can be set up, such as the SFTP (Secure File Transfer Protocol). SSH replace TELNET and other remote logon schemes that provide no security.

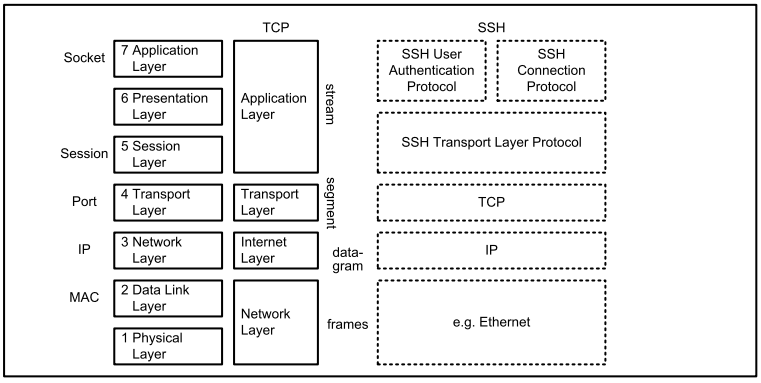
Ports

tcp/22

Architecture

SSH applications are based on a client-server architecture and can be used for network functions as file transfer. SSH User Authentication Protocol is used to authenticate the client-user to the server. SSH Connection Protocol is used to provide logical channels. SSH Transport Layer Protocol is responsible for the server authentication, the 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 provide secure file transfer capabilities. This protocol assues that it runs over a secure channel, like SSH. This is necessary because SFTP assues, that there is already an authenticated client and server. Not to 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/).

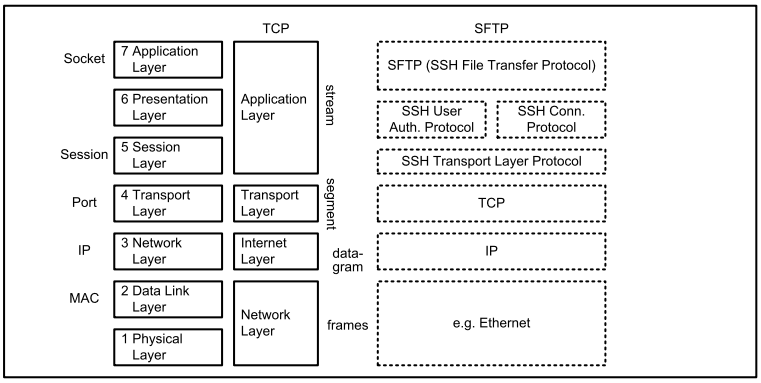
Ports

tcp/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

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.

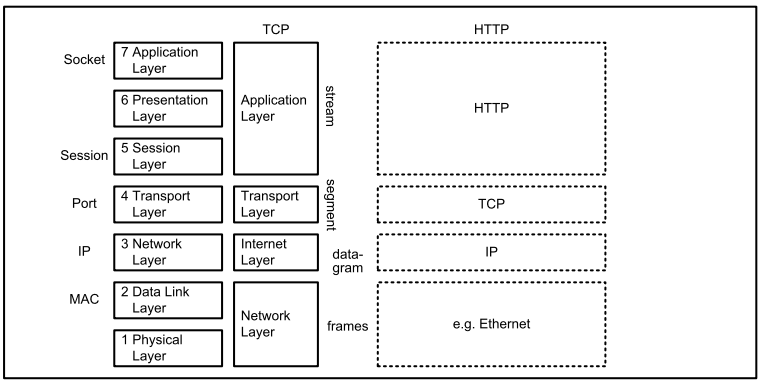
Ports

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 more eavesdropping transmission. It focuses on transport encryption. The protection goal is secure encryption and authentication. Use is found in the focus between web browser (client) and web server (server).

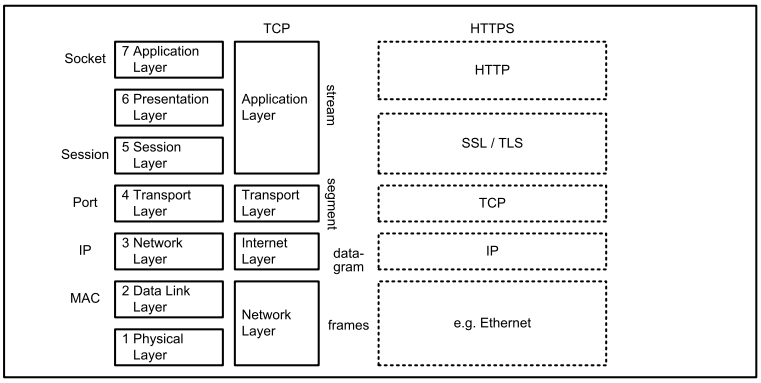
Ports

tcp/443

Architecture

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

ISO/OSI-Model



HTTPS in the ISO/OSI Model

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.

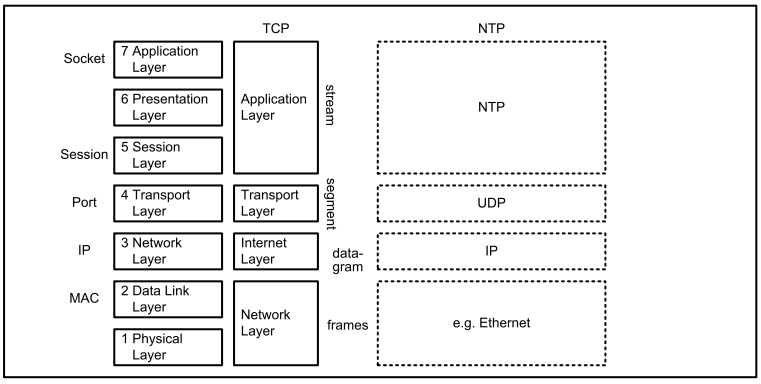
Ports

udp/123

Architecture

The NTP protocol is usually based on the UDP packet.

ISO/OSI-Model



NTP in the ISO/OSI Model

PLC-Designer 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.

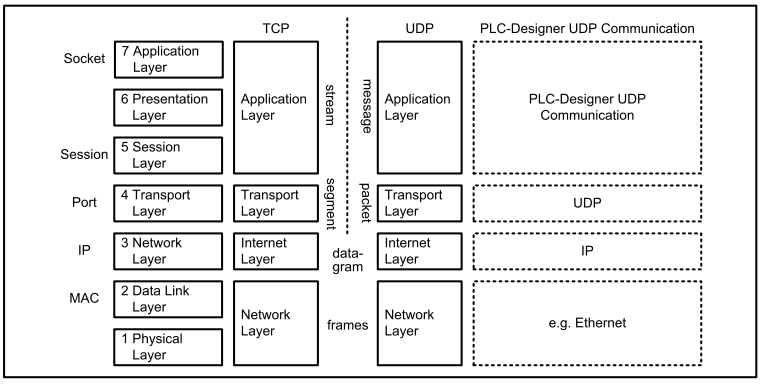
Ports

udp/1740 … 1743

Architecture

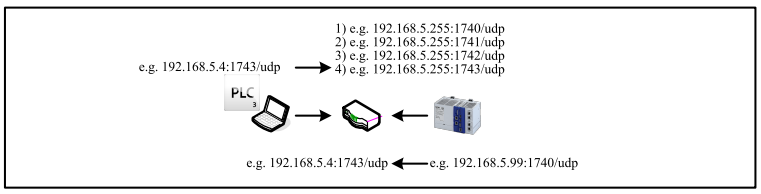
These communication is based on the udp-communication.

ISO/OSI-Model



PLC Designer UDP Communication in the ISO/OSI Model

Scan Network

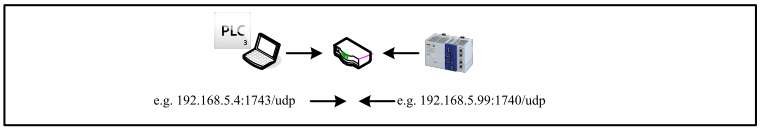


Scan Network

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

Communication

After a network scan, you can go online to the controller. Here we use the previously scanned udp connection.



UDP Communication

OPC UA (OPC Unified Architecture)

Name of Protocol

OPC Unified Architecture (OPC-UA)

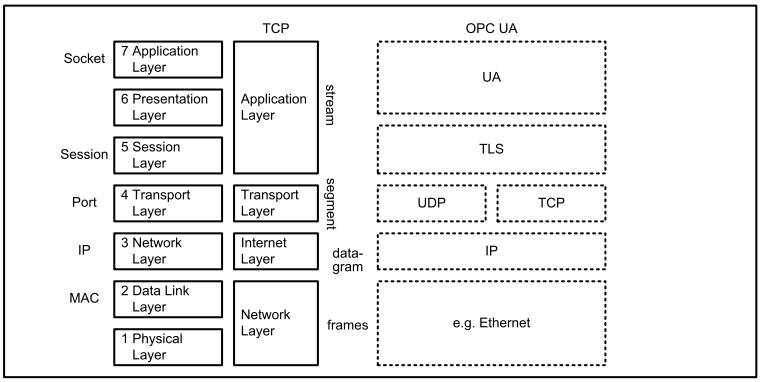
Purpose

The OPC UA protocol is a platform-independent architectural approach. In this context, this is mainly 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. With this diagnostic tool, a diagnosis can be carried out, but also active access to the EtherCAT master.

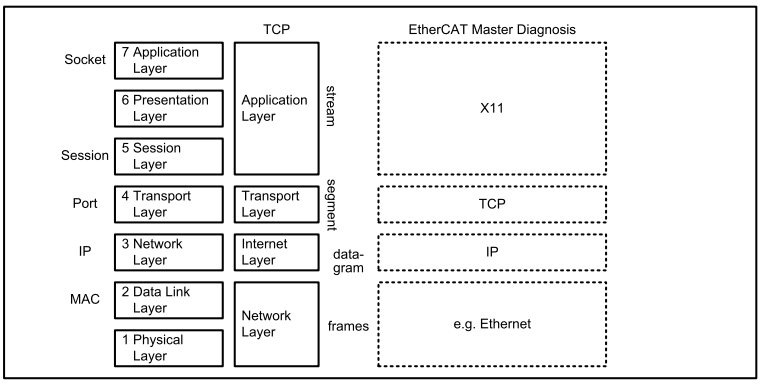
Ports

tcp/6000

Architecture

The protocol used here is based on TCP.

ISO/OSI-Model



EtherCAT Master Diagnosis in the ISO/OSI Model

UI Designer

Name of Protocol

UI Designer

Purpose

The »EASY UI Designer« uses the standard TCP IP Communication via the Port 7100.

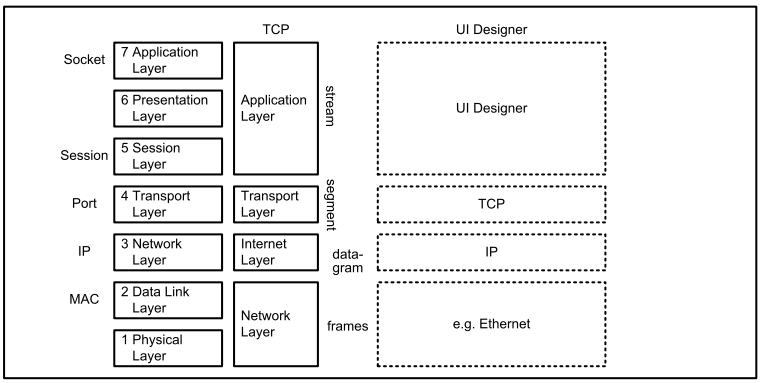
Ports

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 the Port 7200.

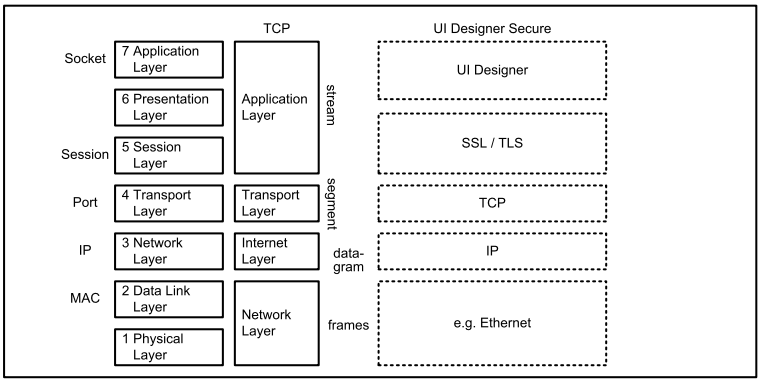
Ports

tcp/7200

Architecture

The protocol used here is based on TCP.

ISO/OSI-Model



UI Designer Secure in the ISO/OSI Model

GCI

Name of Protocol

GCI

Purpose

GCI is a proprietary protocol for communication between engineering tools and devices. This is developed in such a way that it can be embedded in various communication protocols. If a GCI is transmitted via an Ethernet protocol, port tcp/9410 is used in focus. 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.

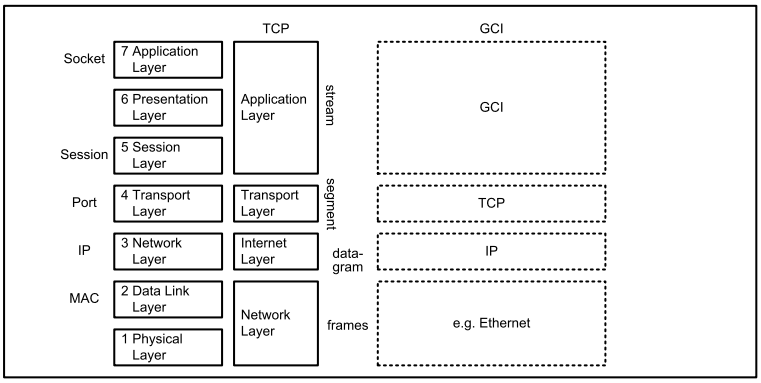
Ports

tcp/9410

Architecture

The protocol used here is based on TCP.

ISO/OSI-Model



GCI in the ISO/OSI Model

Integrity

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

In most cases, this is done by using hash functions. These map any input data via the hash function to a hash value with a fixed size. This hash function is based on the requirement of the one-way function, which means that it should be possible to calculate a hash value from input data using simple means, but that there should be no conclusions from the hash value about the input data entered. Even small changes in the input data should be clearly visible in the hash value. In addition, there is a requirement for freedom from collisions, i.g. 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 024348b5fe28136bbe798f095be5d121edea86dfea2067e1ab0a1c7b8fe79abf is specified on the website. In addition, there is a note that the hash procedure SHA256 was used.

Example Solution

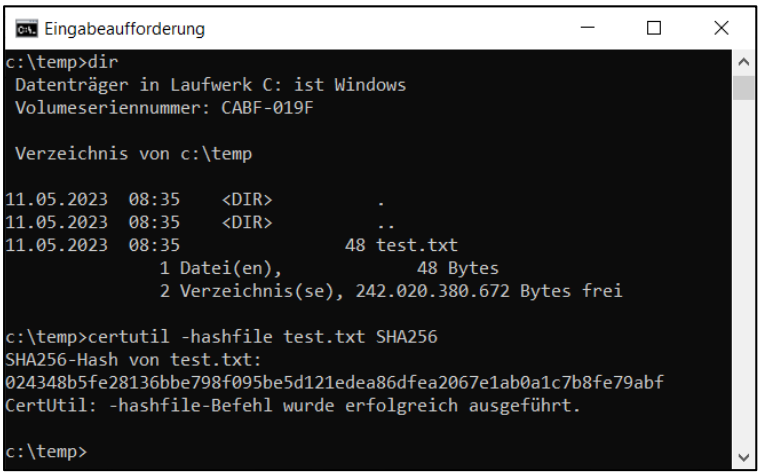
The file test.txt is saved to the hard disk under "c:\temp\". The command line is called with the command "cmd". It is changed with "cd c:\temp\" into the desired directory. With the command dir the directory content can be displayed and the file "test.txt" appears. With the following syntax the integrity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

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

In this example, the command line is thus:

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

And the output looks like this:



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

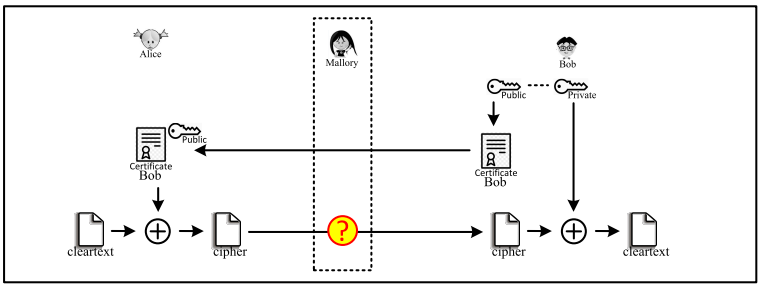
Certificates are based on the ISO/IEC 9594-8:2020 standard, the so-called X.509 standard.

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	

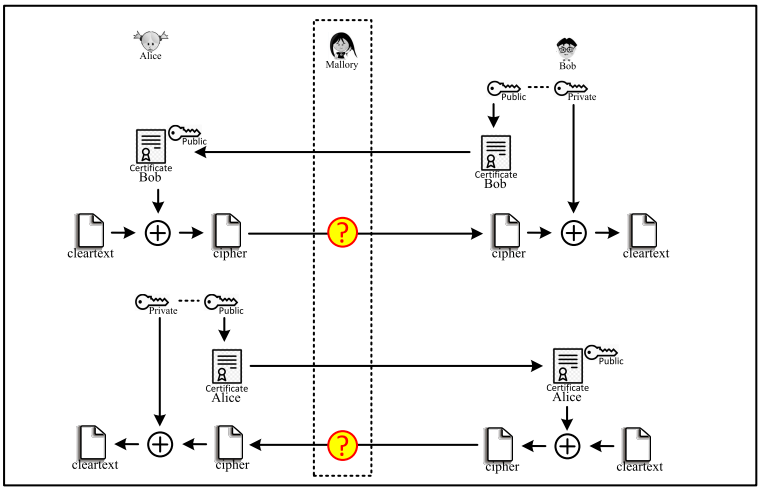
Examples of use cases for certificates for the use case encryption

A simple example of using certificates is outlined here to illustrate the principle. The task is for Alice to send a file to Bob without Mallory, if she intercepts the file, being able to read 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.

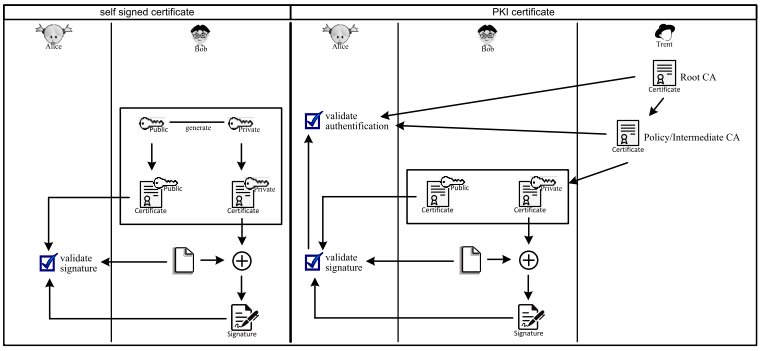


Example for encryption in both ways (asymmetric encryption)

First, Alice generates a pair of keys and puts the public key in a certificate. Bob requests Alice's certificate and can use the key it contains to encrypt the file. In transit, Mallory cannot read the file even in possession of Alice's public key. However, Alice herself can use the private key to decrypt the file and then read it in plain text.

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:

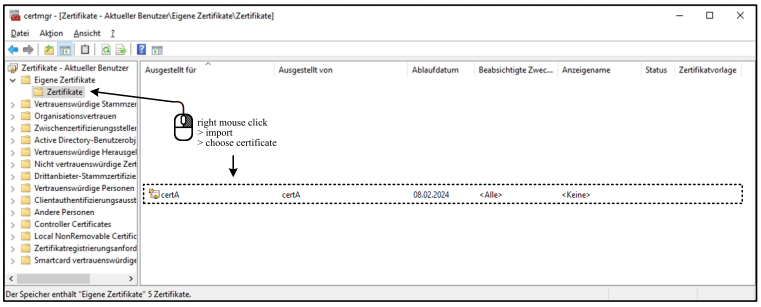
```
openssl x509 -outform der -in cert.pem -out certificate.cer
```

3. Change format of certificate inclusive private key:

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

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 with ‘certmgr.msc’.
2. Open the own certificate folder and right click on import.
3. Choose a certificate.
4. The certificate will integrate and viewed in the table on the right side.

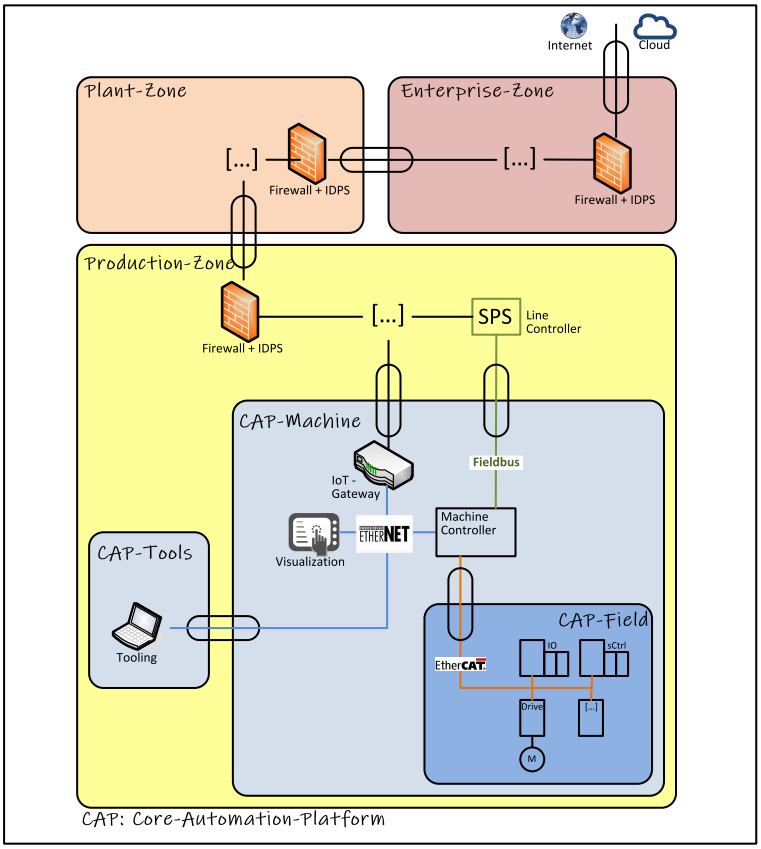
Core Automation Platform

The consideration of cyber security in industrial automation systems is based on IEC 62443. This 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 presents a presentation at system level. However, this must be adapted by each system integrator or machine builder to his own environment and his own system composition and is his responsibility. Only a reference architecture is discussed in order to sort the relationships and to specify a required system environment for the components.

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



Zones and Conduits

Zones and conduits

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

These zones depending on the operator and is responsible for its structuring and organization. These zones are listed here for one reason and that states that the components mentioned here may not be operated directly on the open Internet, but require an additional level of protection in the sense of the "Defence-in-Depth" concept. The design of these protection levels must be considered and responsible for by the operator.

Zone "CAP-Machine"

The abbreviation CAP-Machine means "Core Automation Platform – Machine". In this zone there are 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 into the machine 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.

Conduit "IoT-Gateway"

This conduit connects the Security Zone "CAP Machine" with the "Production-Zone". When integrating the machine into production, special attention is paid to this interface, as it represents an important level in the defense-in-depth concept from a cyber security point of view. Here reference is made to the possibilities in the chapter of the component x5x0.

Conduit "Fieldbus"

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 in system design.

Secondly, the standardized Ethernet TCP/UDP channel is possible here in parallel to some proprietary fieldbus systems. This must be considered separately and taken into account in the cyber security risk assessment in system design.

Conduit "Tools"

This conduit connects the security zone "CAP Machine" with the "CAP Tools". 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 be taken 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 cybersecurity requirements and correspond to the state of cybersecurity.

Conduit "Field"

This conduit connects the security zone "CAP Machine" with the "CAP Field". The special feature here lies 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.

Zone "CAP-Field"

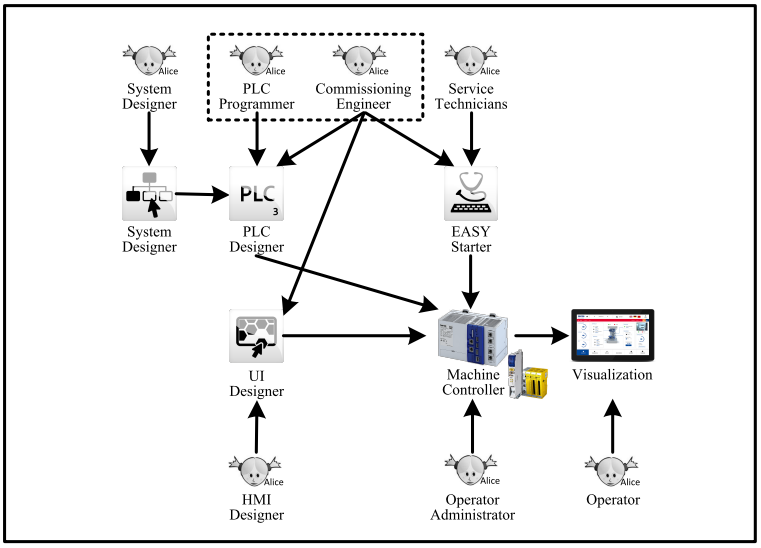
The abbreviation CAP-Field means "Core Automation Platform – Field". These are connected via the communication medium EtherCAT and thus represent only a low level of protection in terms of cyber security. The operator must therefore ensure that no unauthorized access to the components can take place.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

Zone "CAP-Tools"

The abbreviation CAP-Tools means "Core Automation Platform – Tools". The user of the tools installs them on a self-responsible computer hardware. The responsibility for the correct use, the cyber security of the computer and the updating via patch management lies with the user. 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 chapters of the tools, but these are only one possibility of cyber security functions.

Roles

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



Roles in the System

Role "System Designer"

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

Role "PLC Programmer"

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

Role "HMI Designer"

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.

Role "Commissioning Engineer"

The Commissioning Engineer sets up a machine with the PLC and visualization projects. Here he can (depending on how many rights he has received from the PLC programmer) also edit the application of the controller. In addition, he can import and parameterize the prepared visualization for the machine programming.

Role "Service Technicians"

The Service Technicians provides support with problems during commissioning and the service life of a machine and carries out maintenance work if necessary.

Role "Operator"

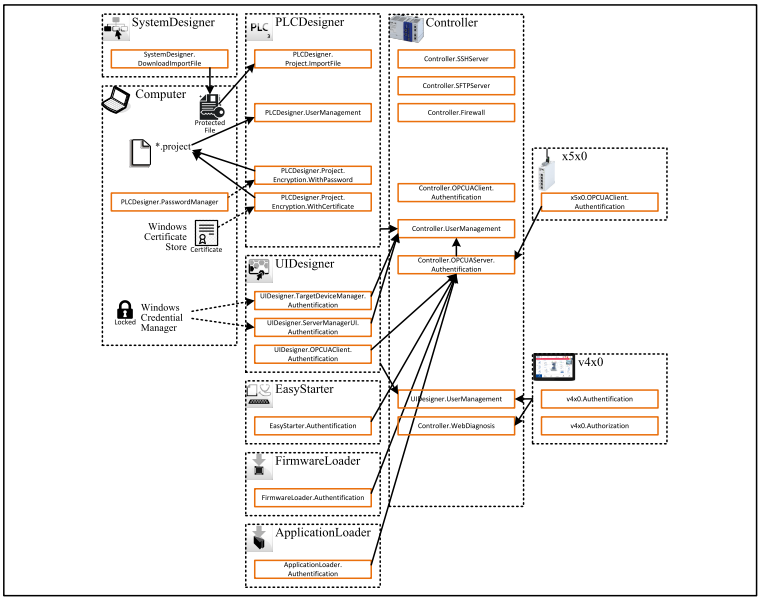
The Operator controls the machine at runtime, usually via an HMI with the configured visualization.

Role "Operator Administrator"

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.

Overview

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



Identification, Authentication and Authorization in the Core Automation Platform

x5x0 IoT-Gateway

The x5x0 components are configured from the x4portal and span a VPN tunnel between both. The component itself has no identification or authentication of human users.

Drives DataHub

The Drives DataHub has its own user administration and can therefore identify and authenticate human users. A corresponding rights management then takes over the authorization. The mechanisms for this are described in the corresponding chapter.

Brownfield and drive based

Is not in focus of this documentation, now.

»EASY System Designer«

This cloud service has its own user management and can identify, authenticate and give human users the necessary rights via an authorization. The mechanisms for this are described in the corresponding chapter.

»PLC Designer«

The »PLC Designer« does have its own user management and provides functions in this sense. On the one hand, the projects can be stored protected and on the other hand, the users and their passwords for the projects can be managed centrally in a password manager. The mechanisms for this are described in the corresponding chapter.

»EASY UI Designer«

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

Controller

The Controller contains two user administrations. On the one hand the user management of the controller accesses: here, users and their passwords are managed with the help of the »PLC Designer« and stored on the controller in the user administration. Any access to the Controller is via this mechanism. On the other hand, the user administration for the operators on the v450 is on the Controller. These can initially be created via the »EASY UI Designer« but can also be changed at runtime on the v4x0 web panel. Both mechanisms are described in the corresponding chapters.

v4x0 web panel

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

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

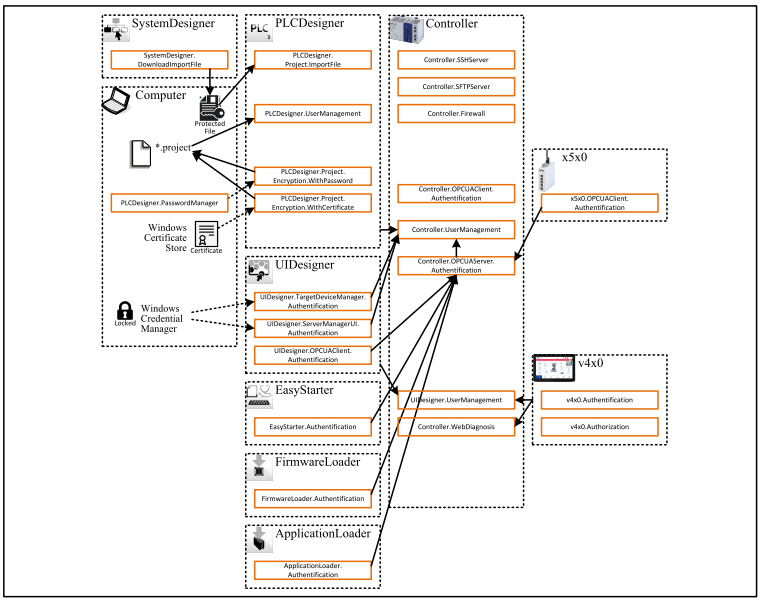
These three auxiliary tools do not have their own user management but must identify and authenticate themselves on the controller before they can establish a connection.

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.

Authentication, identification and authorization

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



Identification, authentication and authorization

In the following, 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

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

Identification, authentication and authorization within the PLC Project

- PLCDesigner.Project.UserManagement

Setup different users and authorization 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 device "Controller"

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

This is the user management of the controller. This is set via the settings in the »PLC Designer« and forms the basis for all identification and authorization mechanisms on the controller. All elements to be authenticated to the controller, such as the »EASY Starter«, the »EASY UI Designer«, the x5x0 IoT Gateway, the UA Expert, the »EASY Firmware Loader« and the »EASY Application Loader«, use this mechanism.

User management for the visualization representations

- UIDesigner.UserManagment
- Controller.WebDiagnosis

The user management of the visualization display is set via the »EASY UI Designer«. Here the users, their authentication and authorizations can be regulated. These apply on the one hand to process visualization but also to diagnostic visualization.

User management of the visualization component

- v4x0.Authentification
- v4x0.Authorization

The component v4x0 web panel has its own user management with the help of which the rights can be set for the two users admin and user. This regulates the different access authorizations for the different access paths.

Controller firewall

- Controller.Firewall

The controller firewall is used to minimizes the attack surface and close all ports on different networks.

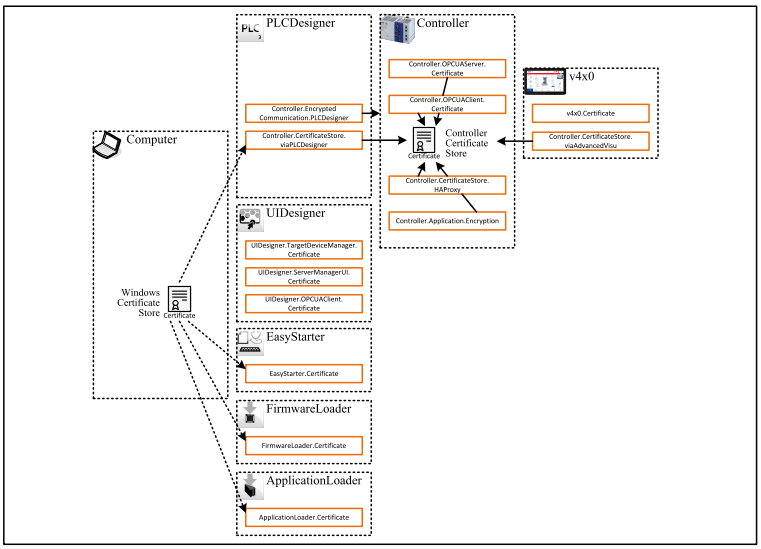
Service access to the controller

- Controller.SSHServer
- Controller.SFTPServer

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

Certificate handling

The following image shows an overview of the certificate handling.



Certificate Handling

Controller Certificate Store

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

The Controller Certificate Store can handle all own or other Certificates for the device Controller. These Certificates can handled via the »PLC Designer«.

Handling Controller Certificates via the Visualization

- v4x0.Certificate
- Controller.CertificateStore.viaAdvancedVisu

With the functionality Controller.CertificateStore.viaAdvancedVisu the user can handle the certificates via the Visualization.

Encryption of Application

- Controller.Application.Encryption

With this functionality the user can encrypt the application and handle the needed certificate in the Controller Certificate Store.

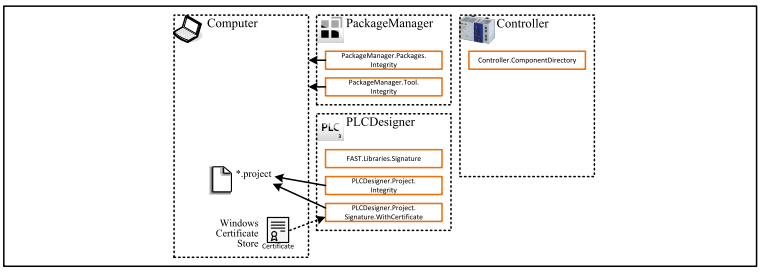
Encrypted Communication Controller

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

Encrypted connection between the tools »PLC Designer«, »EASY Starter«, »Firmware Loader«, »Application Loader« and »EASY UI Designer« and the Device Controller and protect 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 authenticy

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

Check the Integrity Values before installation the packages or the tools.

Signature for Libraries

- FAST.Libraries.Signature

Check the Signature before integrate Libraries in the Project.

Integrity and Signature for PLC Projects

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

Protect the PLC project with integrity or signature.

Component Directory

- Controller.ComponentDirectory

Use the Component Directory to get the needed information for the Security Board of the operator.

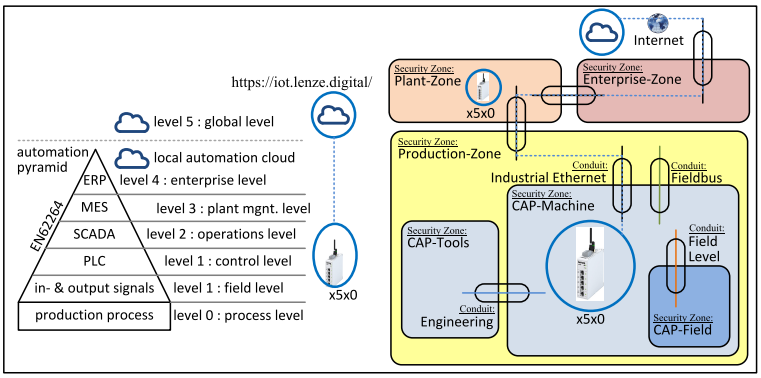
x5x0 IoT Gateway

Product description

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

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

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" (Zone "CAP-Machine" (📖 42)) 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 generated to the x4remote 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 environment:

- The component must be mechanically protected against unauthorized use. This can be achieved, for example, via access control systems or lockable control cabinets.
- In particular, the handling of the USB Stick 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, e.g. be protected.

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 }.

Security mechanisms

The following security functions are included in the listed service:

Security mechanisms

- x5x0.OPCUAClient.Authentification

Commissioning and hardening instructions

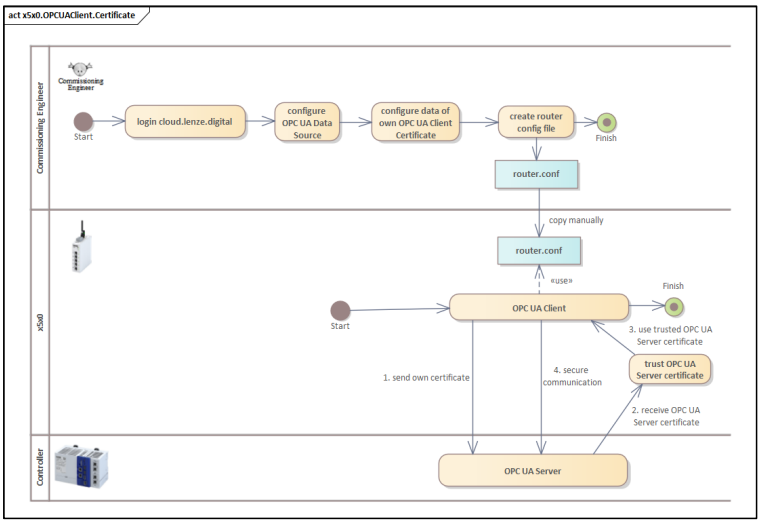
The following commissioning instructions must be followed.

- 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.

Security functions

x5x0.OPCUAClient.Authentification

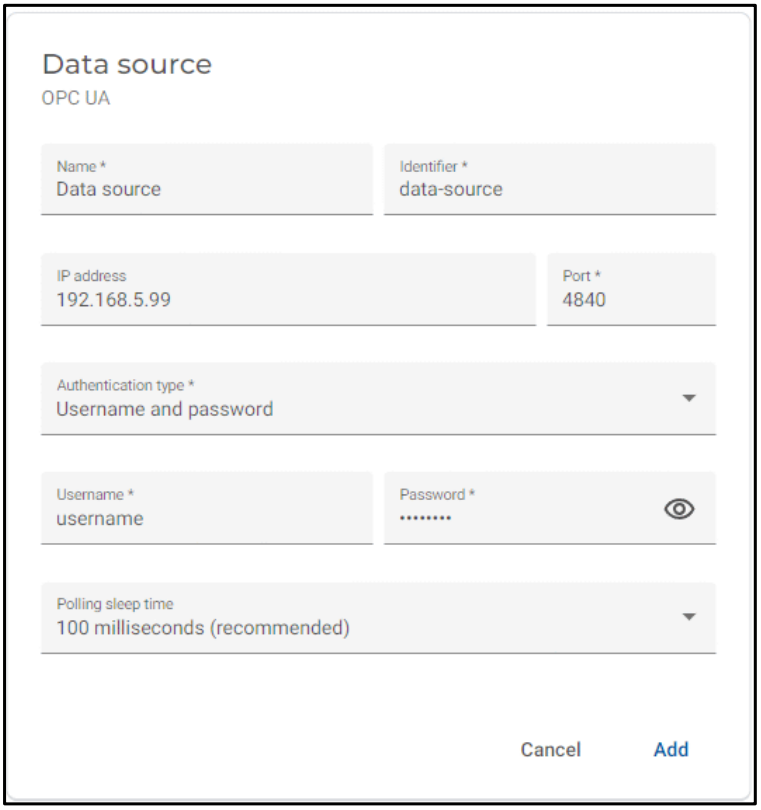
The x5x0 has an OPC UA client, which can be parameterized via a cloud configuration.



Activity Diagram

To connect the x5x0 to an OPC-UA-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 choose Authentication type = Username and password
- Type in the Username and Password



Data Sources

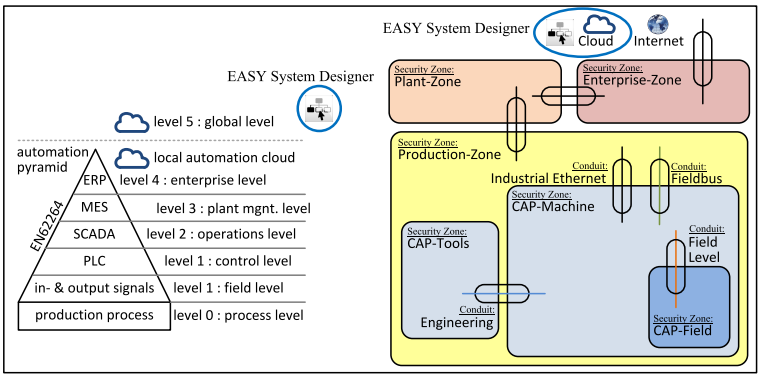
»EASY System Designer«

Description

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

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

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 (📖 42)).



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.

Security mechanisms

The following security functions are included in the listed service:

Security mechanisms

- SystemDesigner.DownloadImportFile

Security data

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 ?=.*[!@#$%^&*]

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 (is not part of this documentation).

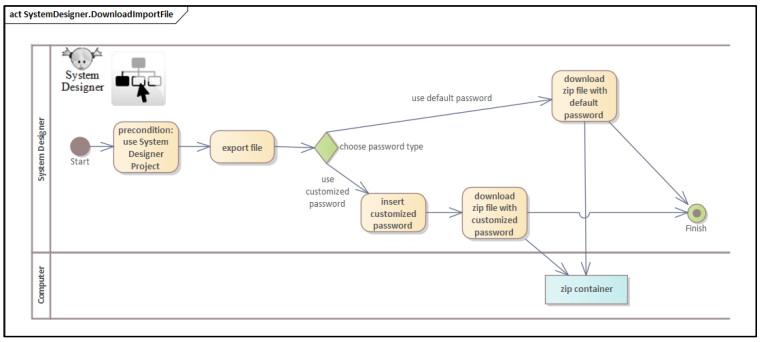
Commissioning and hardening instructions

- If downloading a project for using in the »PLC Designer«, use the user defined password (SystemDesigner.DownloadImportFile (📖 61)), to protect the import file for unauthorized usage.

Security functions

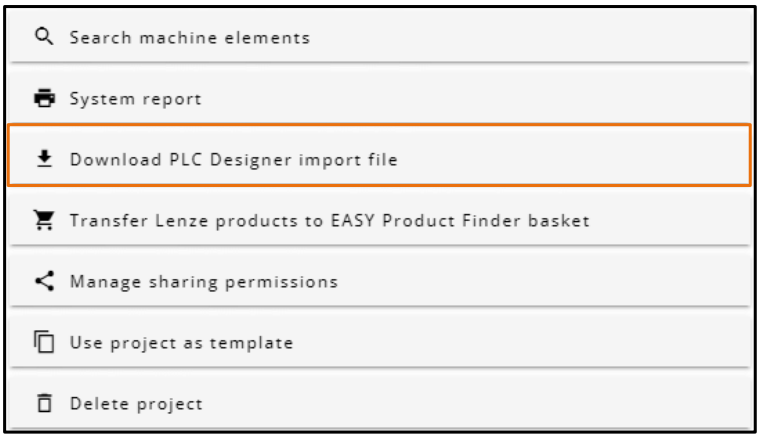
SystemDesigner.DownloadImportFile

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



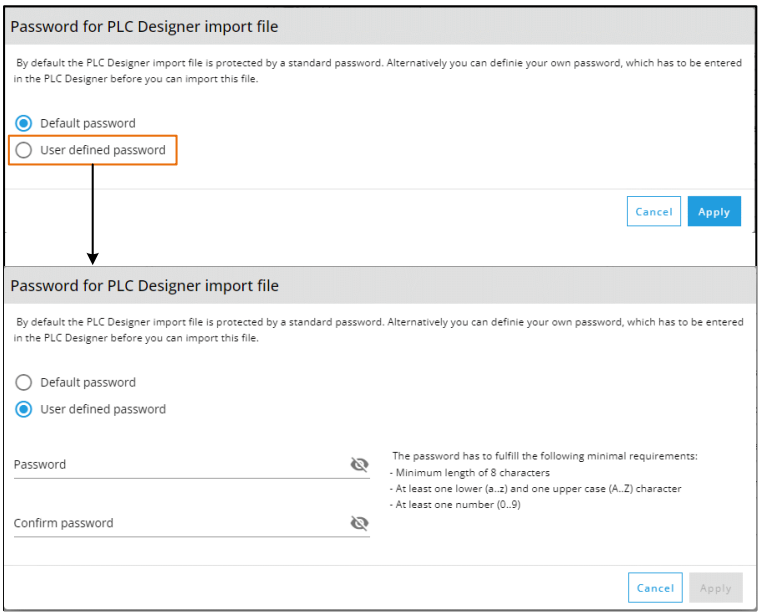
Activity Diagram

In the »EASY System Designer« a function is available to create the »PLC Designer« import file and to download it. The following image shows the button "Download »PLC Designer« import file" for this:



Download »PLC Designer« import file

This is followed by a question as to whether the default password should be used to protect the zip container, or whether a personalized password should be used.



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 with *.plcExportFile. To import this file into the »PLC Designer« see PLCDesigner.Project.ImportFile (📖 66).

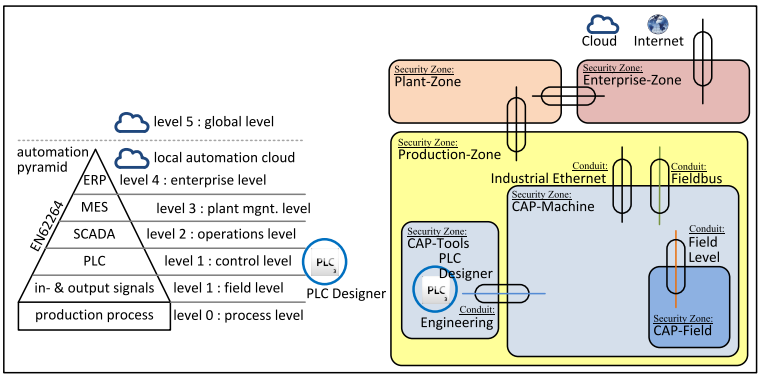
»PLC Designer«

Product description

This documentation is applicable to the following component with its identification:

Name of product	Product ID
»PLC Designer«	n.a.

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 (📖 42)).



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 environment:

- The 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.

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

- This software is considered 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

The following security functions are included in the described product:

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

Security data

PLCDesigner.PasswordManager

The Password Manager Files are located on user"s computer in following directory:

c:\ProgramData\PlcDesigner\Options\LiveOptions\

The relevant files are:

LIVE_UserRoot_{<ID>}.opt

After deinstalling the »PLC Designer«, these data has to remove manually from the user.

Controller.EncryptedCommunication.PLCDesigner

If storing the Controller Certificates for the Encrypted Communication in the Windows Certificate Store in the directory "Controller Certificates/Certificates", these Certificates will not be deleted during deinstalltion. After deinstallation of the »PLC Designer«, these data has to remove manually from the user.

For more information see Integrate a certificate in the windows certificate store (📖 40).

Commissioning, hardening and decommissioning notes and organizational measures

The following commissioning instructions must be followed:

General instructions

- Installation and operation only on current and security-maintained computers.
- Restrict access to authorized persons.

Commissioning and hardening instructions

- Using the PLCDesigner.ImportFile to import project data from the »EASY System Designer« (PLCDesigner.Project.ImportFile (📖 66))
- Use the user management for the »PLC Designer« Project (PLCDesigner.Project.UserManagement (📖 68)).
- Optional the password manager can be used PLCDesigner.PasswordManager (📖 70)).
- Activate the »PLC Designer« Project-Encryption with password (PLCDesigner.Project.Encryption.WithPassword (📖 74)) to protect the secure project from unauthorized access.
- Activate the »PLC Designer« Project-Encryption with certificate (PLCDesigner.Project.Encryption.WithCertificate (📖 77)) to protect the secure project from unauthorized access.
- Activate the »PLC Designer« Project-Signature (PLCDesigner.Project.Signature.WithCertificate (📖 80)) to sign the project.

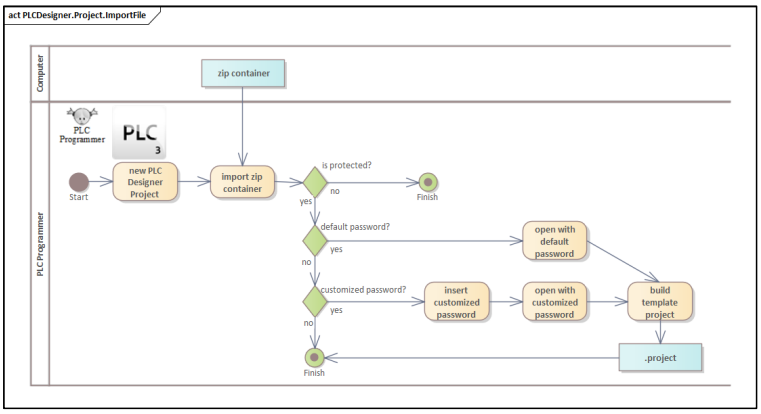
Decommissioning instructions

- After uninstallation the »PLC Designer«, please remove the Data from the PLCDesigner.PasswordManager manually (PLCDesigner.PasswordManager (📖 70)).
- After uninstallation the »PLC Designer«, please remove the Certificates from the controller manually (Controller.EncryptedCommunication.PLCDesigner (📖 64)).

Security functions

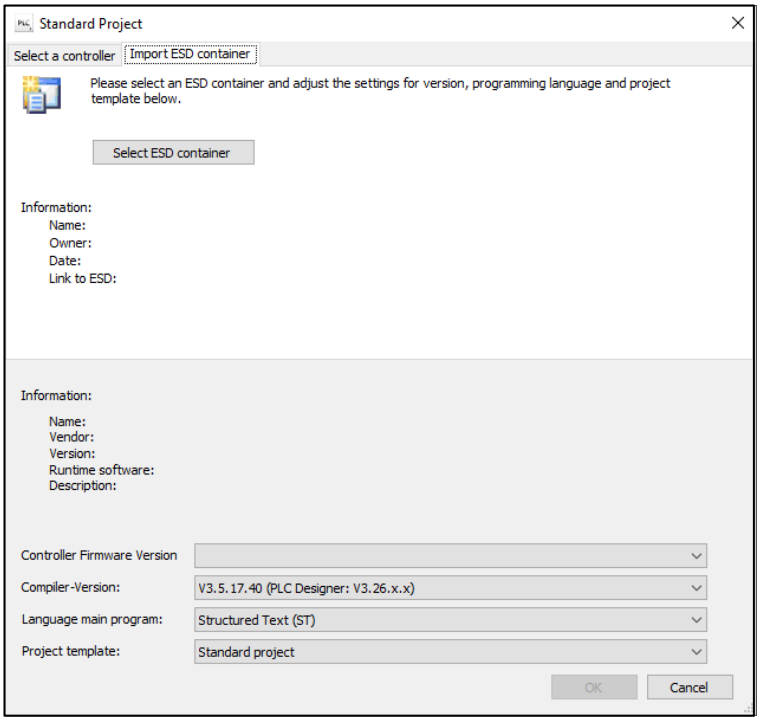
PLCDesigner.Project.ImportFile

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



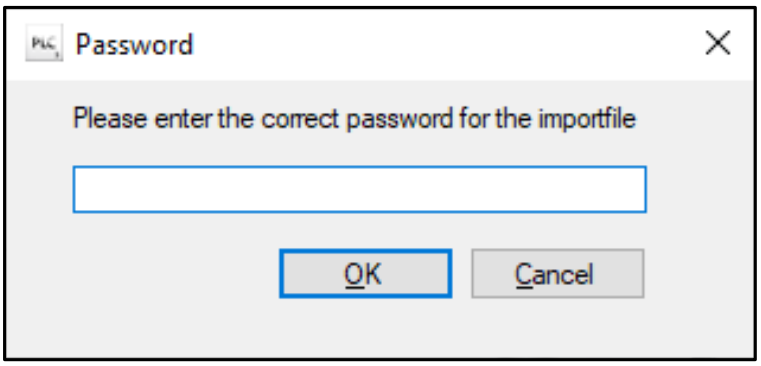
Activity Diagram

After downloading the import file from the »EASY System Designer« SystemDesigner.DownloadImportFile (📖 61)) it can be integrated into the PLC project. If the »PLC Designer« is started, an ESD container can be selected via the call "PLC Designer➞new project➞Import ESD container", see next figure.



Import ESD container

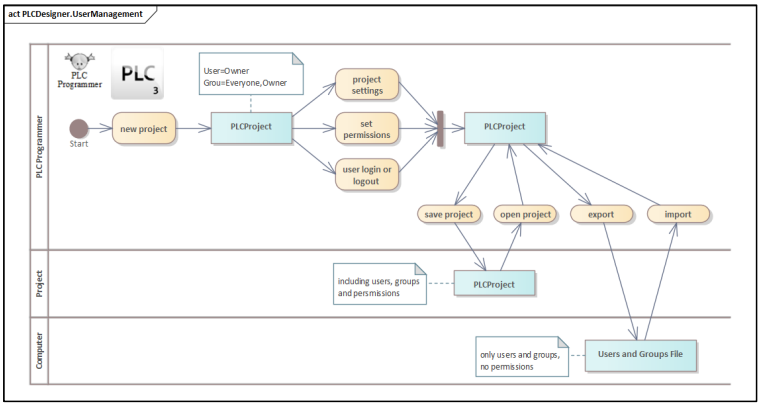
If the zip container is protected with the default password, it is imported. If it is protected via user defined password, a dialog opens to enter this password.



Enter Password Dialog

PLCDesigner.Project.UserManagement

This chapter describes the functionality of an 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. With this function the user can protect individual objects with read/write protection. 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 group "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, a login to the default user "Owner" with the default password <empty> must first be made. 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 a larger number of incorrect passwords than under maximum number of login attempts, he will be blocked and can no longer log in with the correct password. Under "Project/Project Settings/Users and Groups" it is displayed with a red cross. To activate the user again, set the property "Active" again via "Edit". Only the users of the group "Owner" may 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 and the colored settings in red and green in changed properties.

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

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

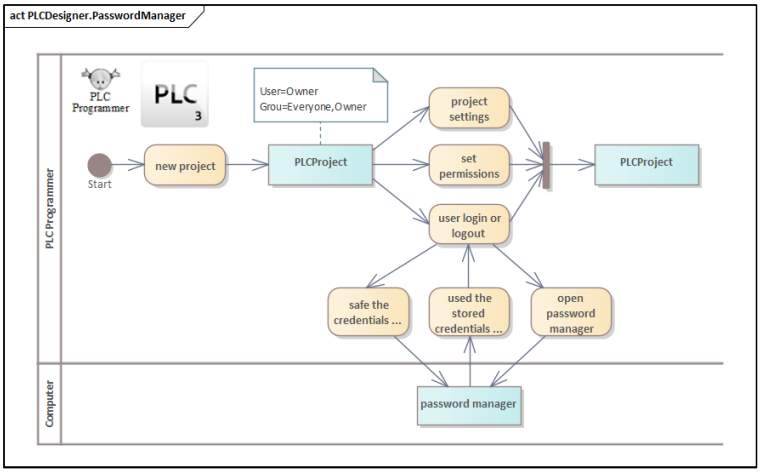
Export and import

Via export and import, the Users and Groups and their relationship can be exported or imported into a file (*.user). The respective permission settings are not included here.

If the Users and Groups are to be transferred from one PLC project to another, there is also the option of doing this using the CODESYS export/import (to be found in the »PLC Designer« menu under the topic Project). When exporting, select the second POUs tab and activate the project settings here. A file with extension *.export will be created. These can then be integrated in 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>

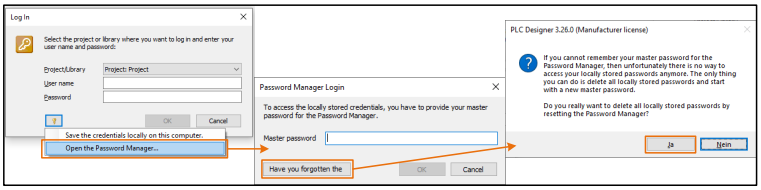
This function can be used to load passwords stored in the password manager.

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.

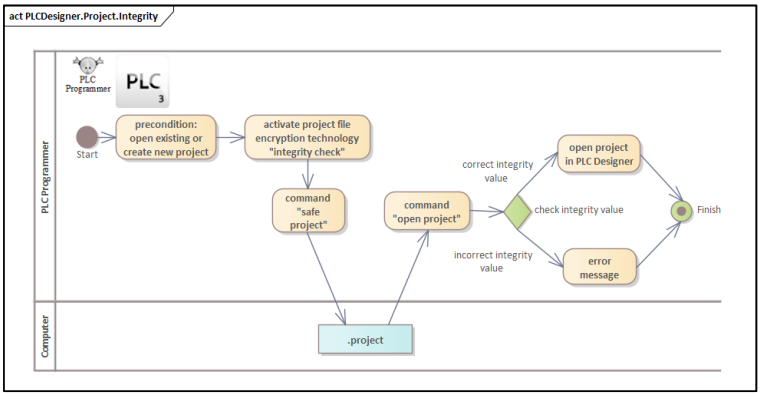


Forgotten Password

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

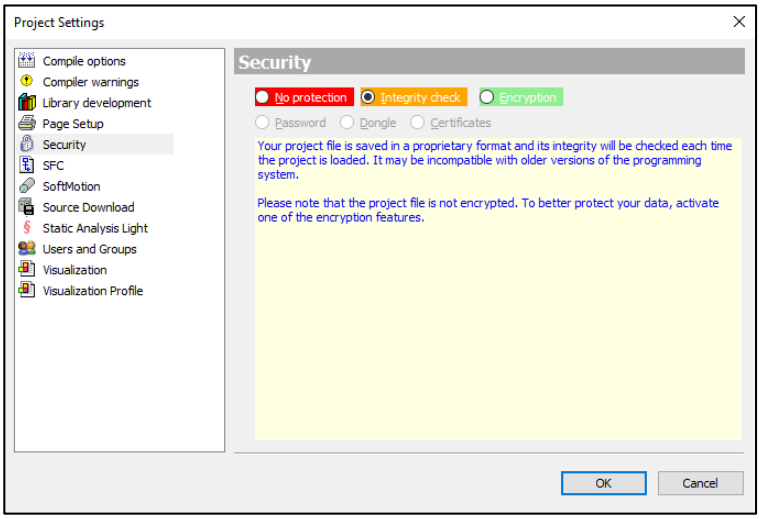
PLCDesigner.Project.Integrity

This functionality generate and verify a integrity value of 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, which is checked when opened. This function only checks integrity. The proprietary format does not represent encryption or confidentiality.



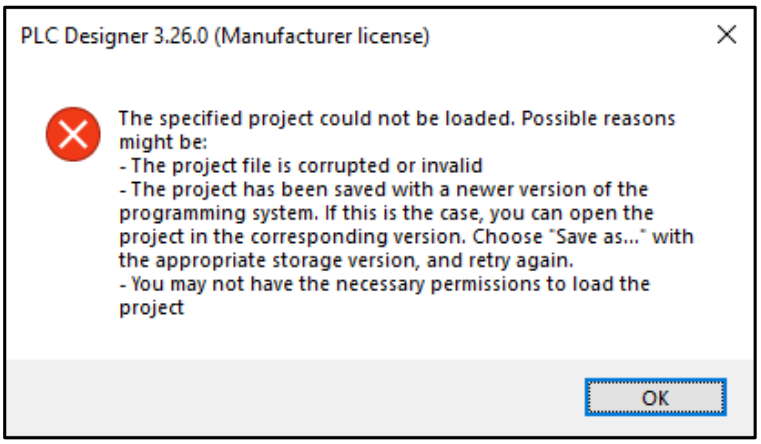
Activity Diagram

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

When a PLC project is opened, the project is checked for integrity. If integrity is given, the project is opened without a message. If the integrity is changed, an error message is displayed and the project is not opened.

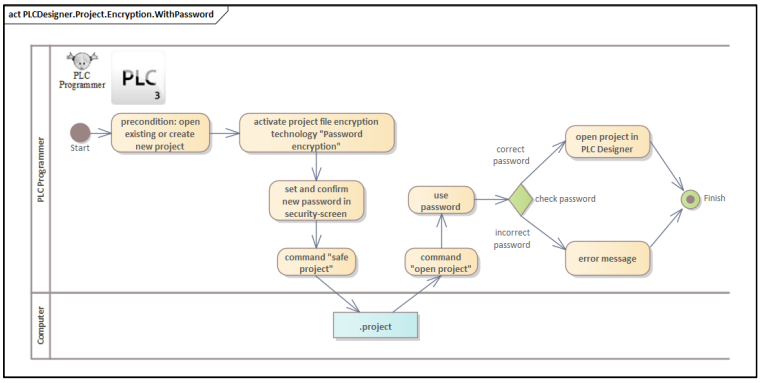


Error Message

This function applies only to the base project file "*.project". When saving the PLC project, additional data is stored. An example are the xml files for nodesets for the OPC-UA model. These additional files are not protected in their integrity with this function and must be protected organizationally by the user if necessary.

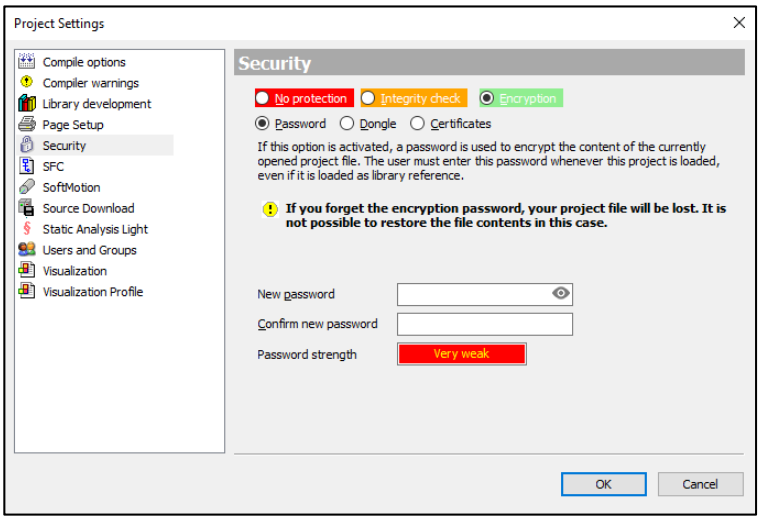
PLCDesigner.Project.Encryption.WithPassword

This functionality encrypt and decrypt the PLC project with an password.



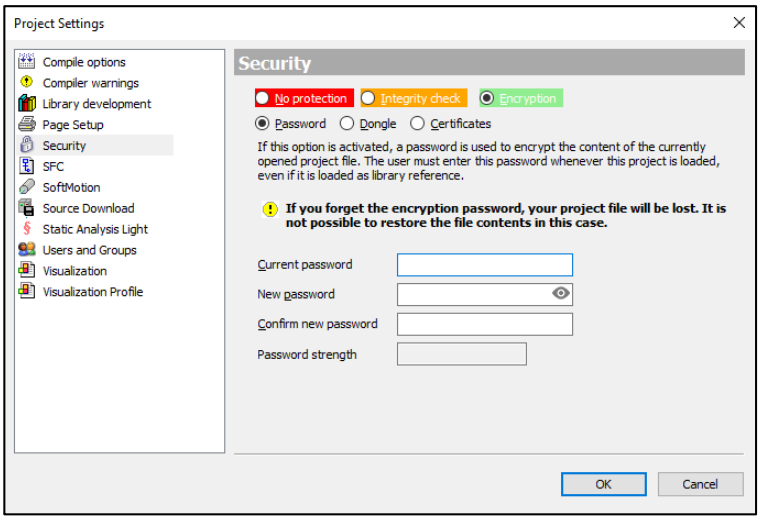
Activity Diagram

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 choosen, the function is activated. At this point, a new password must be assigned and confirmed.



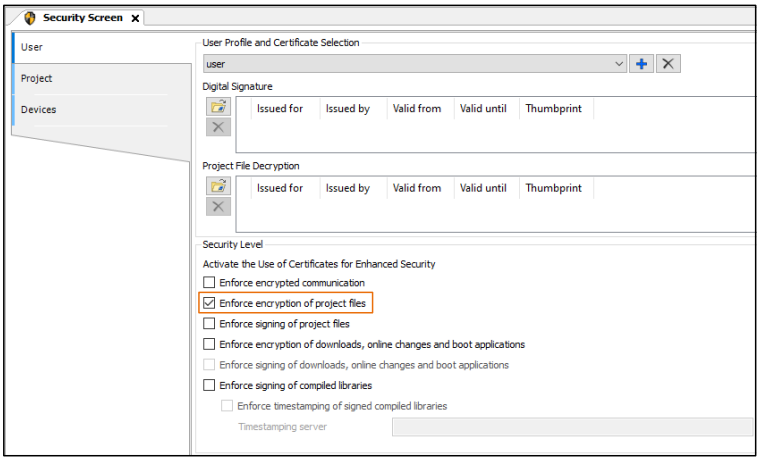
Project Settings

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



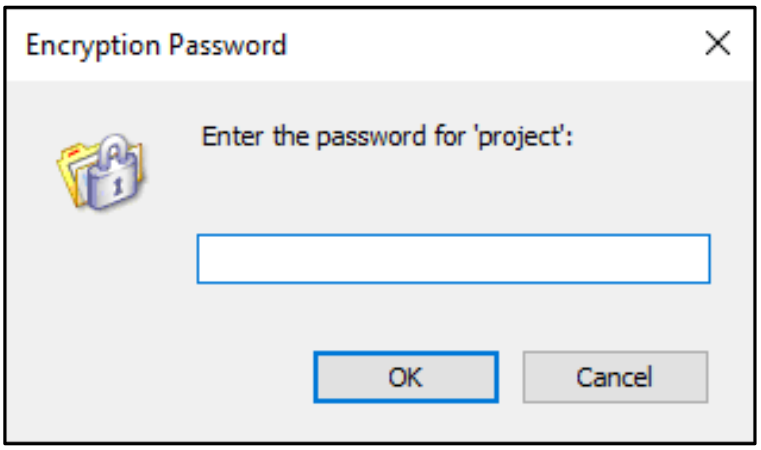
Project Settings for New Password

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



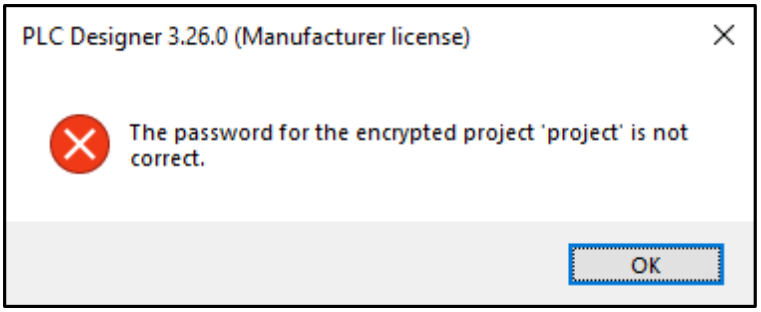
Enforce encryption of project files

When a PLC project is opened, the user has to enter the password.



Enter Encryption Password

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

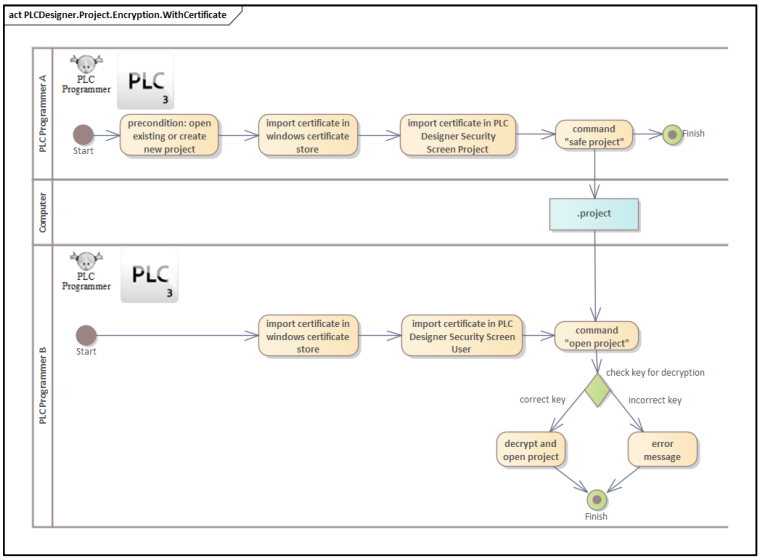


Password not correct

This function applies only to the base project file "*.project". When saving the PLC project, additional data is stored. An example are the xml files for nodesets for the OPC-UA model. These additional files are not encrypted with this function and must be protected organizationally by the user if necessary.

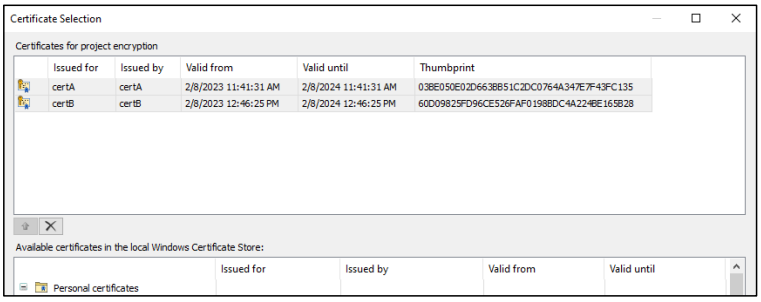
PLCDesigner.Project.Encryption.WithCertificate

This functionality encrypt and decrypt the PLC project with a key out of 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 choosen, 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).

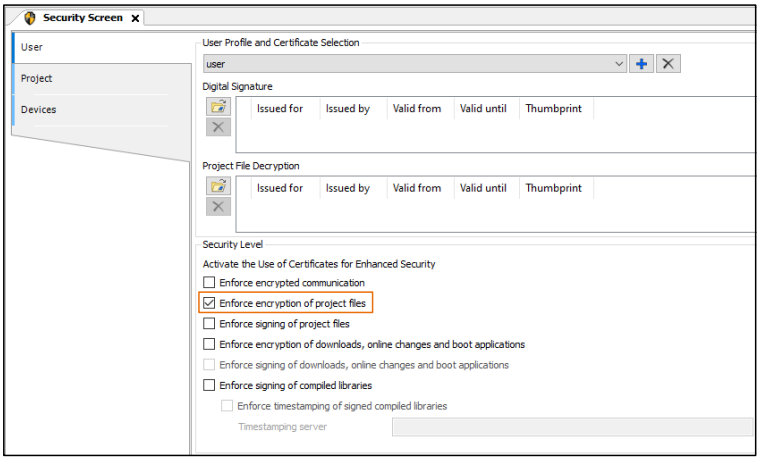


Certificate selection for encryption

If a certificate is imported into the »PLC Designer« "\Security Screen\Project\Project File Encryption", which does not contain a private key, the following warning message appears "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 is information because the public key is needed to encrypt and the private key to decrypt.

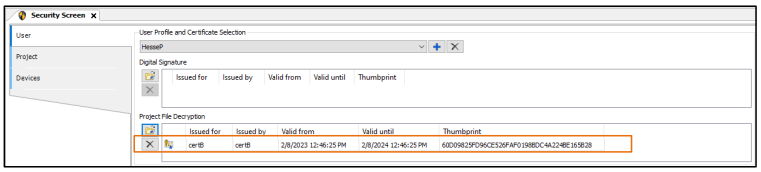
After selecting the certificates, the project can be safed encrypted.

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



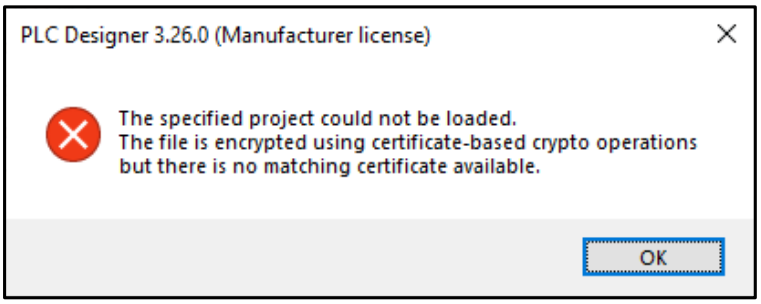
Enforce encryption of project files

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



Certificate for Project File decryption

If the private key is correct, the project is opened, if not a following error message appears.



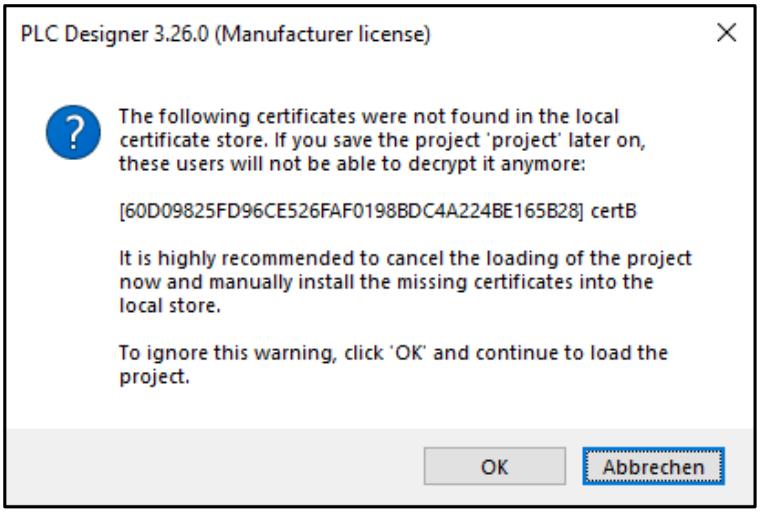
No matching Certificate available

Above it was described that it is possible to encrypt the project with several public keys and open it only with 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 this key is used when saving again.

Example:

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

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

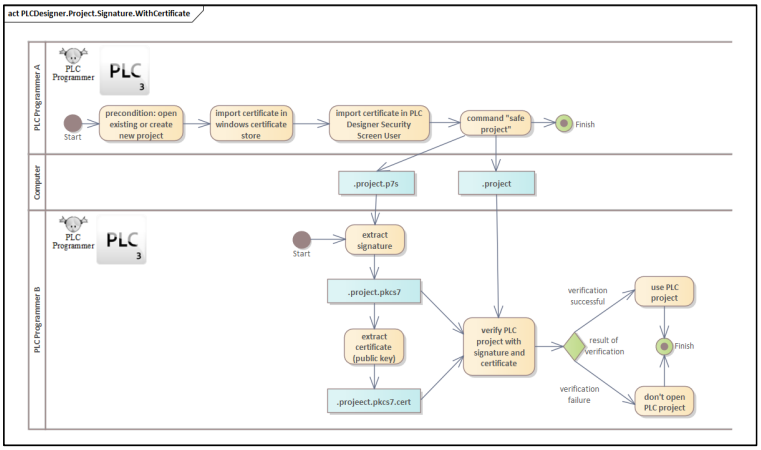


Missing certificates were not found

This function applies only to the base project file "*.project". When saving the PLC project, additional data is stored. An example are the xml files for nodesets for the OPC-UA model. These additional files are not encrypted with this function and must be protected organizationally by the user if necessary.

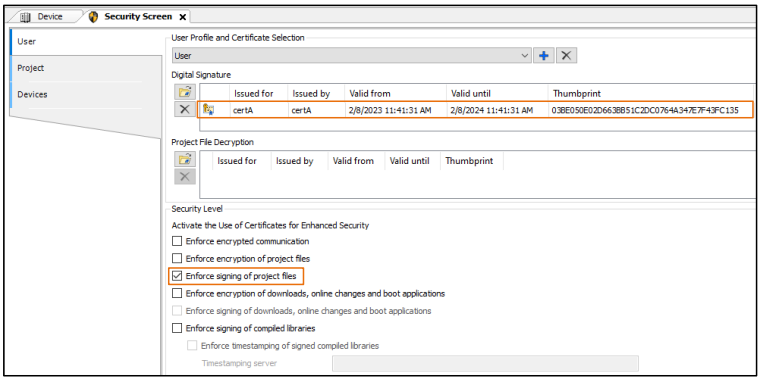
PLCDesigner.Project.Signature.WithCertificate

This functionality sign the PLC project with a key out of a certificate, so that the PLC project creator can send the project to a second person and check that the PLC project comes from the project creator.



Activity Diagram

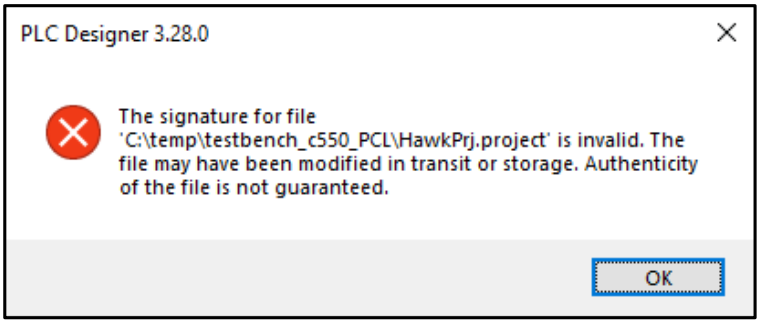
In order to provide a PLC project with a signature, a certificate must be selected in the area of the Digital Signature in the Security Screen in the User area in the »PLC Designer«. This certificate must contain a private key. In addition, select the item "Enforce signing of project files".



Enforce signing of project files

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

When the project is opened in the »PLC Designer«, the signature is checked. If this is not valid 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 applies only to the base project file "*.project". When saving the PLC project, additional data is stored. An example are the xml files for nodesets for the OPC-UA model. These additional files are not signed with this function and must be protected organizationally by the user if necessary.

Controller

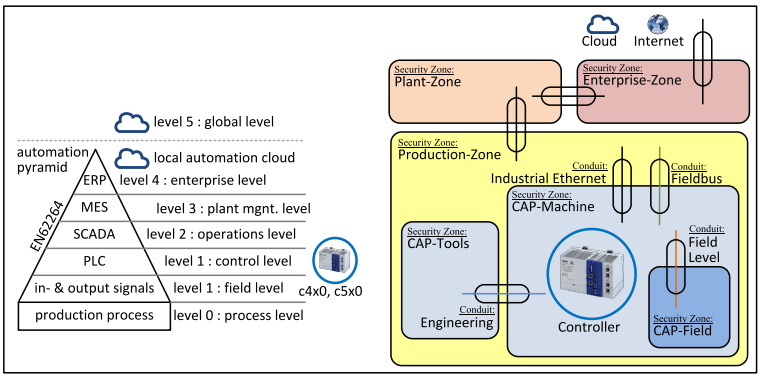
Product description

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

Name of product	Product ID
c430 controller	C43AE50xxxAxxxxxxx
c520 controller	C52AE10xxxAxxxxxxx
c550 controller	C55AE40xxxAxxxxxxx

The functions described in this chapter concern the standard device (product ID CxxxxxxxxxAxxxxxxx) and not the customer-specific variants (product IDs CxxxxxxxxxBxxxxxxx and CxxxxxxxxxCxxxxxxx). This is shown under "Controller c5x0 + extended functionality for customer specific devices only" in engineering and is explicitly excluded here.

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 (📖 42)).



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. This has the task of enabling 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 security zone "CAP Machine" with the "CAP Field". The special feature here lies 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 zoZone.

Intended environment:

- The component must be mechanically protected against unauthorized use. This can be achieved, for example, via access control systems or lockable control cabinets.
- 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, … be protected.

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

The following security functions are included in the listed components:

Security mechanisms:

- 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.Authentification
- Controller.OPCUAServer.Certificate
- Controller.OPCUAClient.Authentification
- Controller.OPCUAClient.Certificate
- Controller.ComponentDirectory

Security data

Controller.SFTP:KeyRequirements

The customer.ppk customer key has the requirements:

- RSA
- min. 2048 Bits

Controller.Firewall:PortList

The default-ports can be used in the components at the specified interfaces with an empty default PLC-Project.

The following table shows the open ports, scanned with nmap without activated Controller.Firewall

Port	Engineering Port X16	PROFINET Device X257/X258	Dual Network	Protocol
22/tcp	open	closed	open	SSH (Secure Shell) (📖 22)
80/tcp	open	closed	open	HTTP (Hypertext Transfer Protocol) (📖 24)
443/tcp	open	closed	open	HTTPS (Hypertext Transfer Protocol Secure) (📖 25)
1217/tcp	open	closed	open	PLC-Designer TCP Gateway-Search
4840/tcp	open	open	open	Lenze OPC-UA Server OPC UA (OPC Unified Architecture) (📖 29)
4840/udp	open	open	open	Lenze OPC-UA PubSub OPC UA (OPC Unified Architecture) (📖 29)
6000/tcp	open	closed	open	EtherCAT Master Diagnosis (📖 30)
7100/tcp	open	closed	open	UI-Designer RAW
7200/tcp	closed	closed	open	UI-Designer secure-RAW
9410/tcp	closed	closed	closed	Parameter Communication GCI
11740/tcp	open	open	open	PLC-Designer Gateway
31855/tcp	open	closed	open	SFTP (SSH File Transfer Protocol) (📖 23)
47877/tcp	open	open	open	SFTP for customer and Lenze-production SFTP (SSH File Transfer Protocol) (📖 23)

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 Adress of the X16 network, the Engineering Port, of the Controller.
Issuer, Unstructured Name	Device: Controller, e.g. Device: c500
Issuer, Unstructured Name	Vendor: Lenze
Issuer, CN	Combination of Controller Type and IP Address, e.g. c550 (192.168.10.100)
Valid from 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 The CN is "Lenze Controller:Proxy@" with the Controller-Type and the MAC Adress of the X16 network, the Engineering Port, of the Controller. OU = Controls O = Lenze L = Aerzen S = Niedersachsen C = DE
Valid from Valid to	The automatically created certificate is valid for 60 year.

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 Crotection Systems) and IDS (Intrustion Detection Systems).
- Restrict access to authorized persons only.
- Change existing default passwords after the first start-up and also 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.

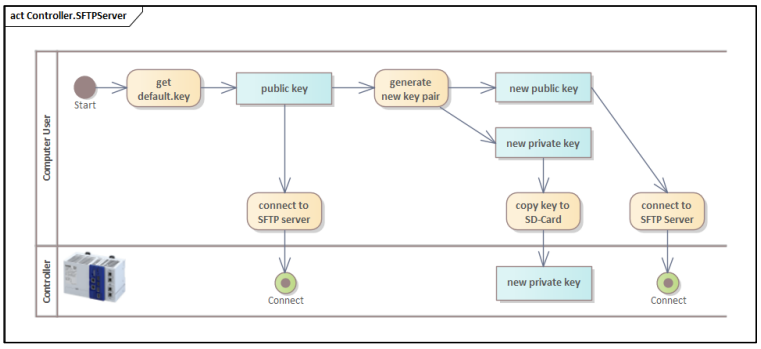
Commissioning and hardening instructions

- Change the Key for SFTP-Server-Communication (Controller.SFTPServer (📖 89)).
- Be sure, that there is no ".enable-ssh" file on the SD-Card for SSH-Access (Controller.SSHServer (📖 95)).
- Change the settings of the Controller Firewall for Hardening the Component (Controller.Firewall (📖 98)).
- Activate and use the user management (Controller.UserManagement (📖 107)).
- Change the standard EngineeringItf-User-Password (Controller.UserManagement: EngineeringItf (📖 112)) or delete this standard user.
- Prevent the deletion of the user management on the SD-Card via an organizational measure (Controller.UserManagement (📖 107)).
- Activate the function "Encrypted Communication" (Controller.EncryptedCommunication.PLCDesigner (📖 115)).
- Activate encrypted Application to secure the Application on the Controller (Controller.Application.Encryption (📖 122)).
- Handle the certificates in the programming phase of the machine with the »PLC Designer« (Controller.CertificateStore.viaPLCDesigner (📖 131)).
- Handle the certificates in the production phase via the Diagnosis Visu (Controller.CertificateStore.viaAdvancedVisu (📖 133)).
- Change the credentials for the WebDiagnosis Controller.WebDiagnosis (📖 141)).
- Change the communication to the web-visualization to https (Controller.CertificateStore.HAProxy (📖 136)).
- If using the OPC-UA Server, please use the Authentication (Controller.OPCUAServer.Authentification (📖 144)) and the Certificatehandling (Controller.OPCUAServer.Certificate (📖 148)).
- If using the OPC-UA Client, please use the Authentication Controller.OPCUAClient.Authentificate (📖 150)) and the Certificatehandling (Controller.OPCUAClient.Certificate (📖 153)).
- Activate and test the Component Directory at the Controller (Controller.ComponentDirectory (📖 155)).

Security functions

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

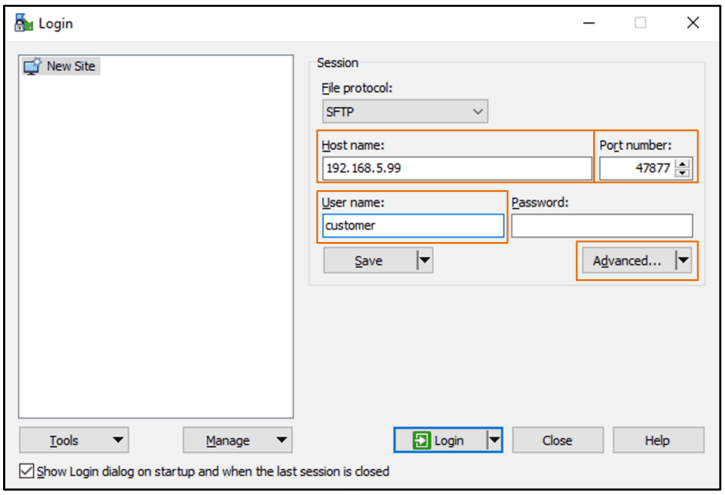
- Connector X16 (Engineering Access)
- Connector X256/X257 (Fieldbus-Device)
  Only if a fieldbus (e.g. PROFINET Device) is included in the device tree of the controller in the »PLC Designer« and the IP-Configuration 0x2381 is set in the parameter set.
- Used Port for SFTP is 47877/tcp

Controller.SFTPServer: Access to the SD-Card

Access the File System via SFTP is available since FW Version 01.03.00.

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

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

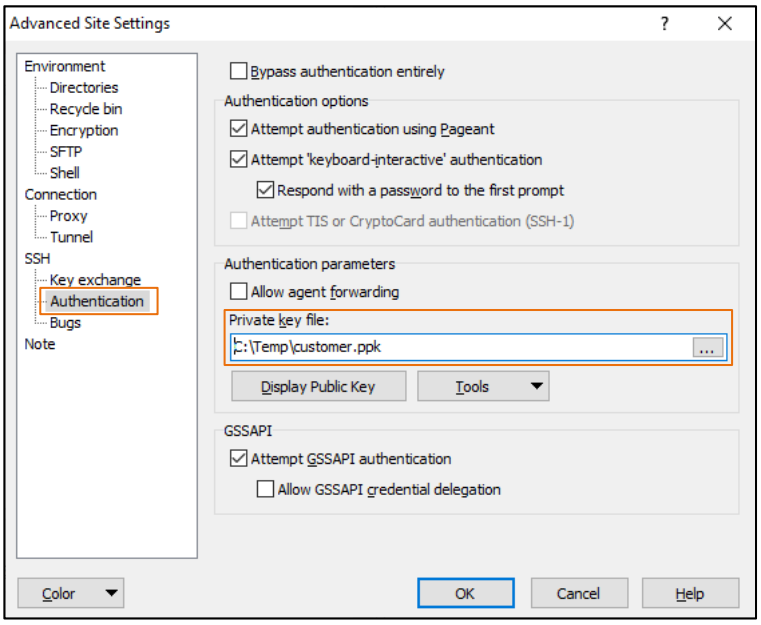


WinSCP Login

Insert the following data

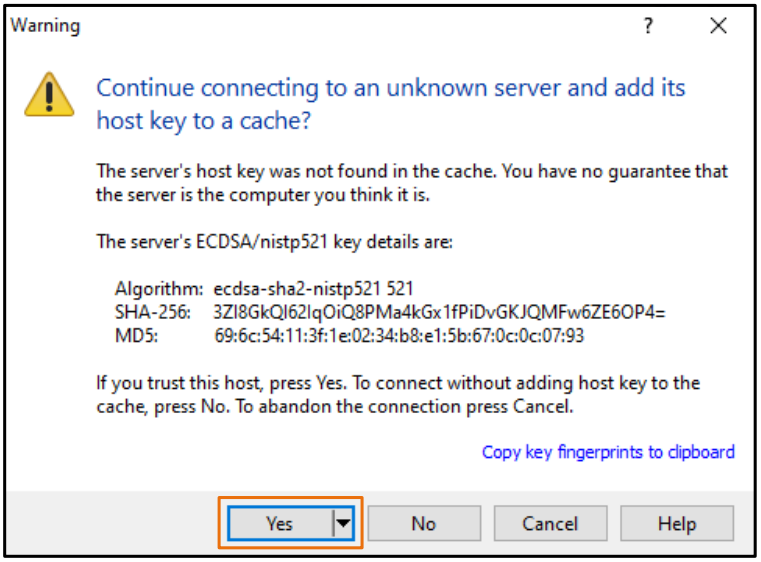
- File protocol: SFTP (communication protocol)
- Host Name: IP-Adress of the Controller
- Port Number: SFTP-Portnumber of the controller (c4x0 and c5x0 uses Port 47877)
- User Name: customer
- Password: keep this password empty

In the next step the advanced dialog has to be used. A *.ppk-file is needed to insert the private key file in the Menu/Authentification-Window. You will get the file from the Lenze-Intern AKB (Dokument ID 201800294). Please ask the Lenze-Support.



Insert customer.pkk key-file

After agreeing the following warning, the /userData path can accessed at the Controller.



Agree Warning

Controller.SFTPServer: Changing the customer.ppk

Changing the customer.ppk is available since FW Version 01.04.00.

This description is required if the access key (customer.ppk) for SFTP access to the controllers is to be individualized. To do this, a separate key must be generated.

In general, it should be noted that the resetting of a key in the Controller once changed can only be carried out by the Lenze service. In this respect, great care must be taken when storing and archiving a new key.

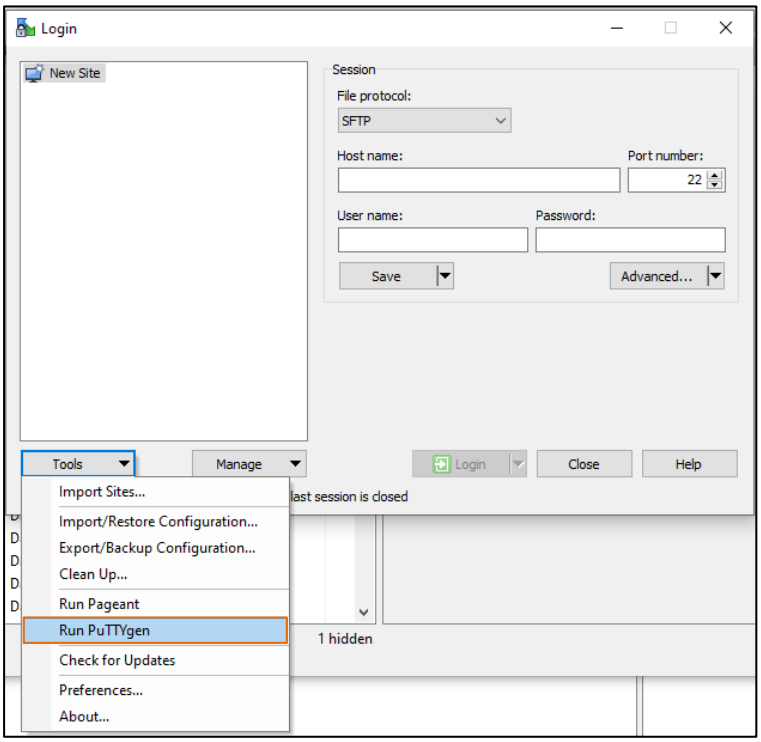
A private key once changed can also be found in a backup of a controller and thus automatically becomes active during a restore on a new device.

Constraints on the key

- RSA
- minimal length of 2048 Bits

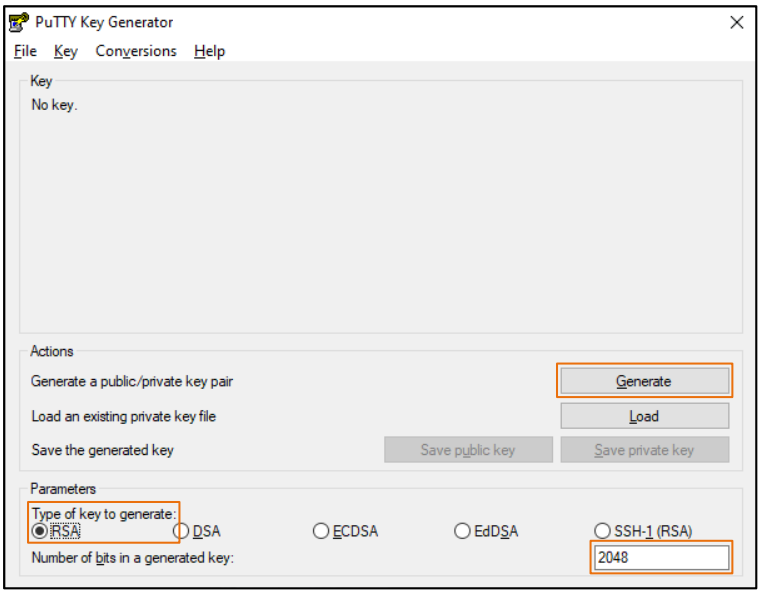
Generate a new key

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



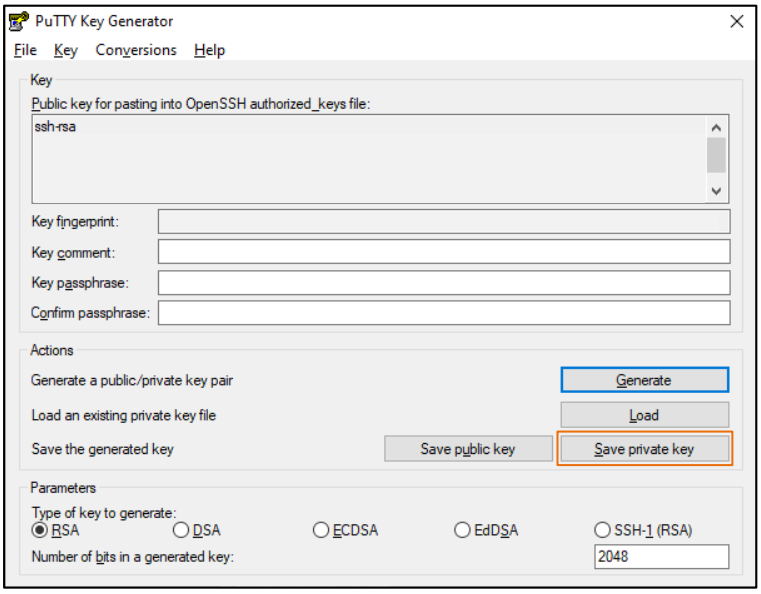
WinSCP using Tools / Run PuTTYgen

2. In PuTTYgen, the key type to be generated (RSA) is set and the length of the Keys specified in bits (minimum 2048 bits). By pressing the "Generate" button the new key pair is generated.



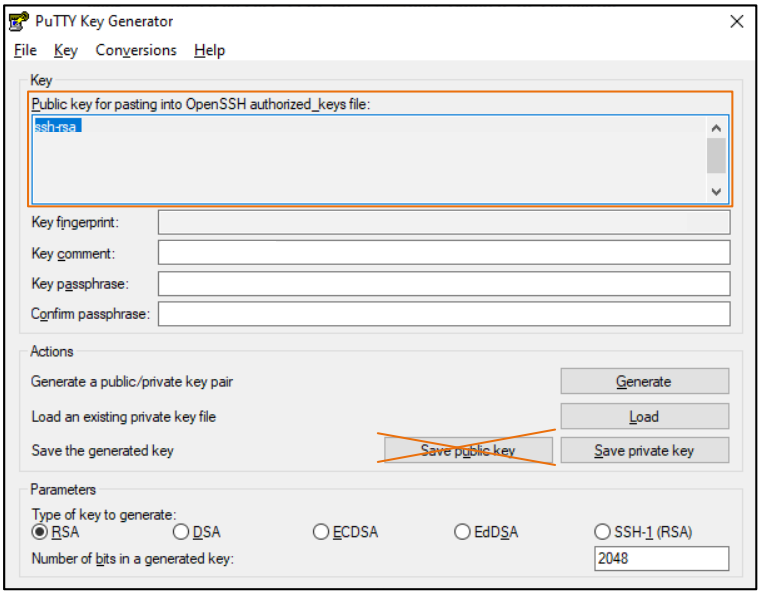
PuTTY Key Generator

3. After creation, a comment on the key can be entered 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: Safe Private Key

4. In order to make this private key known to a device, the contents of the text box "Public key for pasting into OpenSSH authorized_keys file" must be copied and saved in an ASCII text file with the name "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 Controller

1. The file "customer.key" must be on the SD Card of the device in the already existing directory "public-key". For security reasons, the directory "/sdcard/public-key" can only be accessed using SFTP be accessed read; 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" stored.
4. The storage process is registered by the device; as a result, the transferred file is stored on correctness checked:
   - On the SD Card, an identical file must be .key under "public-key/customer.key exist.
   - The file may contain only one line with an RSA key (empty lines become 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" automatically deleted from the device.
     If a check is not successful, the directory "/tmp/user_data" as result generates a file "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 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 in the future can be used.

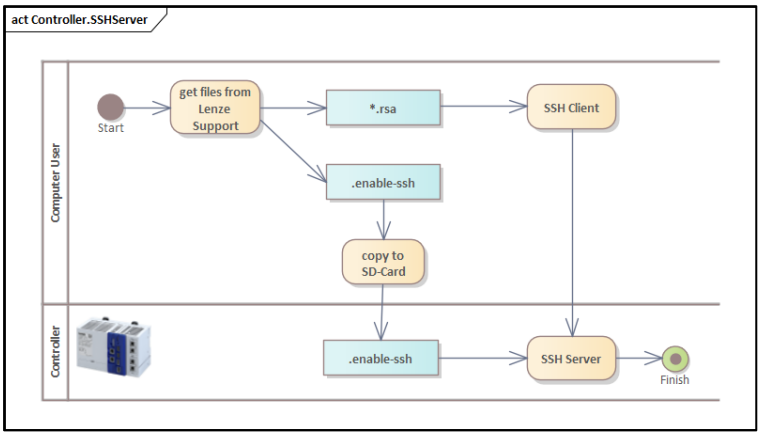
Information on handling

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

Controller.SSHServer

Access the File System via SSH is available since FW Version 01.04.00.

With this functionality, the file system can be accessed via Ethernet. To access the device, a ssh-key is needed. This key is generated by Lenze-Support only in special support cases and not to be used during normal operation.



Activity Diagram

You will receive two files from Lenze Support.

- .enable-ssh
- *.rsa

Both files are personalized to 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. This key is generated by Lenze-Support only in special support cases and not to be used during normal operation.
- The .enable-ssh file must be copied to the controller'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 to 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 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 file from Controller"s SD Card.

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 c550: X16 onboard c520: X16 onboard c430: X16 onboard	22	☑ SSH ☑ SFTP	☑ SSH ☑ SFTP	☑ SSH ☑ SFTP	☐SSH ☐SFTP	☐SSH ☐SFTP	☐SSH ☐SFTP
	31855	☑ SSH ☑ SFTP	☑ SSH ☑ SFTP	☑ SSH ☑ SFTP	☐SSH ☐SFTP	☐SSH ☐SFTP	☐SSH ☐SFTP
	47877	☑ SSH ☑ SFTP	☑ SSH ☑ SFTP	☑ SSH ☑ SFTP	☐SSH ☑ SFTP	☐SSH ☑ SFTP	☐SSH ☑ SFTP
PROFINET Device c550: X257/X258 in E1 c520: X257/X258 in E1 c430: X396/X397 onboard	22	☐ SSH ☐SFTP	☐ SSH ☐SFTP	☐ SSH ☐SFTP	☐SSH ☐SFTP	☐SSH ☐SFTP	☐SSH ☐SFTP
	31855	☐SSH ☐SFTP	☐SSH ☐FTP	☐SSH ☐SFTP	☐SSH ☐SFTP	☐SSH ☐SFTP	☐SSH ☐SFTP
	47877	☑ SSH ☑ SFTP	☑ SSH ☑ SFTP	☑ SSH ☑ SFTP	☐SSH ☑ SFTP	☐SSH ☑ SFTP	☐SSH ☑ SFTP
Switch c550: x257/x258 in E1 c520: x257/x258 in E1 c430: X396/X397 onboard	22	n.a.	n.a.	☑ SSH ☑ SFTP	n.a.	n.a.	☐SSH ☐SFTP
	31855	n.a.	n.a.	☑ SSH ☑ SFTP	n.a.	n.a.	☐SSH ☐SFTP
	47877	n.a.	n.a.	☑ SSH ☑ SFTP	n.a.	n.a.	☐SSH ☑ SFTP

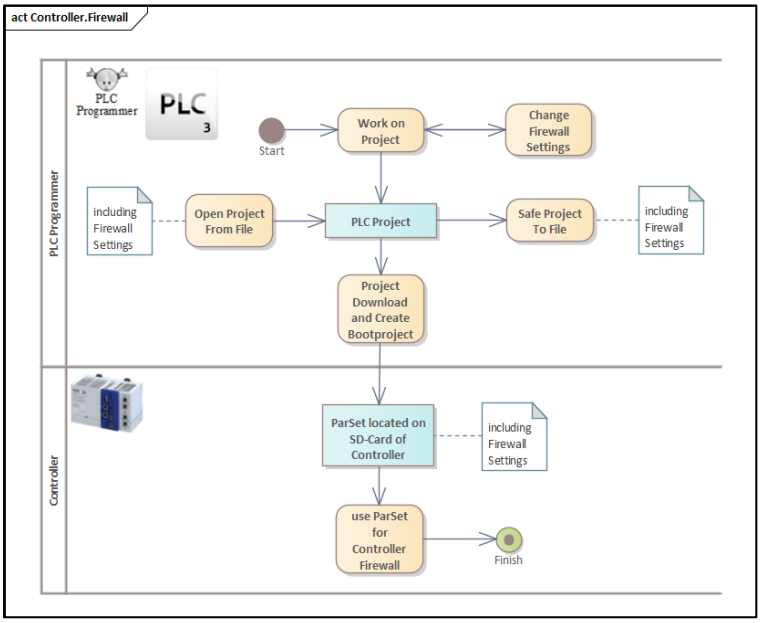
.enable-ssh	Mechanism as described in chapter Controller.SSHServer: Enable SSH-Access (📖 96)
☑	Possible
☐	Not possible

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

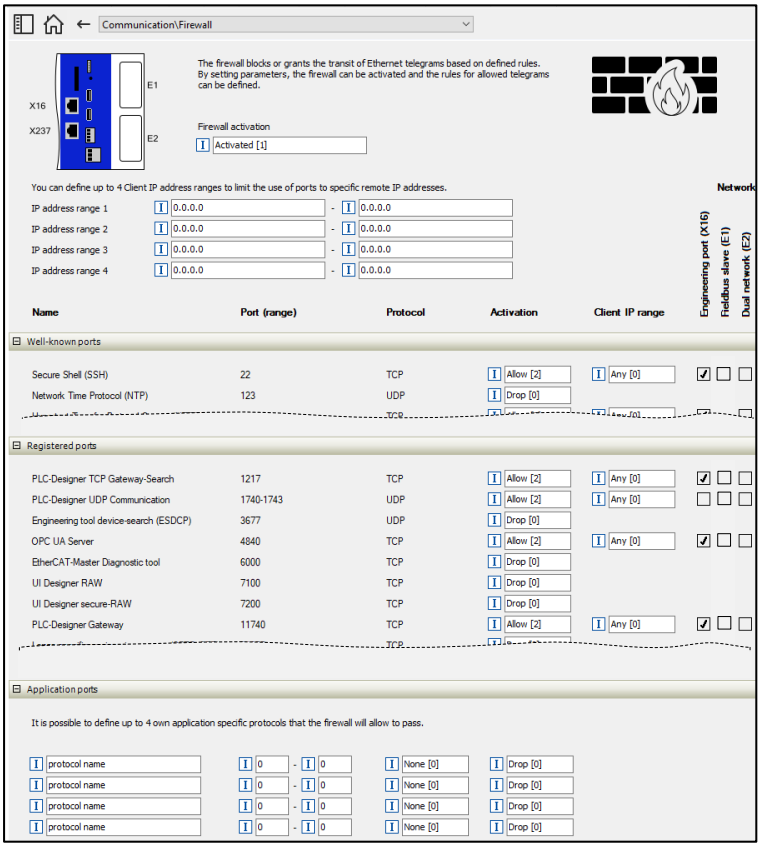
Controller.Firewall: Configuration

This chapter describes the configuration regarding parameterization 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 then finally on the SD Card of the Controller.

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 are some (not completely) listed: (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 Controller.Firewall

Parameter 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. The activation is possible 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=192.168.5.100 and 0x5910:003=192.168.5.120 are parameterized, the range of IP addresses is allowed, i.e. a client with the IP address of 192.168.5.110 may access, 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 0x5910:004 0x5910:006 0x5910:008	Firewall IP Range: IP Range Start	Start of IP-Range for the IP-Clients Range 1 Range 2 Range 3 Range 4
0x5910:003 0x5910:005 0x5910:007 0x5910:009	Firewall IP Range: IP Range End	End of IP-Range for the IP-Clients Range 1 Range 2 Range 3 Range 4

Please remember, 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.

The setting of the IP-Ranges of the Clients only affects the Engineering Port and the Switch as a network. The Clients on the Fieldbus are not considered in terms of their IP addresses.

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. In each block of 10 are 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	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 choices 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. In each block of 10 are 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 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 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, i.e. 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		Start Port Address
0x5911:xx9	Firewall: Port Range End		End Port Address
0x5910:x10	Firewall: Protocol Name		Help note for the protocol name

With these parameters, the user can open an application port with these parameters:

0x5910:x10 Protocol Name

This parameter is only available so that the firewall rule can be given a name. Here the customer has the possibility to assign a name, which is stored in the parameter set and then also 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, only a single port is addressed. By default, the port range 49,152 to 65,535 is set here. This is the area where customers should put 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 areas 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, which is already listed under well-known or registered ports. If the rules between the application port and well-known or registered ports contradict each other, the rule of well-known or registered ports leads.

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 UDP and TCP protocols together.

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. Using the command "Save parameter sets..." these changes can then be persisted 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, 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 only then the lower value.

Exclude from the Controller

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 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:

Because 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 they are part of 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 that are required within the production for the production of the components.

This results in the following default settings for the activation parameters.

Protocol	Port	Default Value for Activation
Secure Shell (SSH)	tcp/22	Allow
Network Time Protocol (NTP)	udp/123	Drop
Hypertext Transfer Protocol Secure (HTTPS)	tcp/443	Allow
PLC-Designer TCP Gateway-Search	tcp/1217	Allow
PLC-Designer UDP Communication	udp/1740-1743	Allow
Engineering tool device-search (ESDCP)	udp/3677	Drop
OPC UA Server	tcp/4840	Allow
EtherCAT-Master Diagnostic tool	tcp/6000	Drop
UI Designer RAW	tcp/7100	Drop
UI Designer secure-RAW	tcp/7200	Drop
PLC-Designer Gateway	tcp/11740	Allow
Lenze specific engineering access (SFTP/SCP)	tcp/31855	Drop
SFTP/SCP	tcp/47877	Drop

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 each other with the application area, the rule of the first two areas counts.

Using http via Port 80

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

- Applications must be switched from http with port 80 to https with port 443. An example is the connection of the visualization. For a corresponding description see UIDesigner.TargetDeviceManager.Certificate (📖 176).
- The http port 80 must be added to the scope of the Application Port Settings and opened explicitly.
- Deactivate the Controller Firewall (not recommended).

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 and not outgoing connections. However, if an outgoing connection is established, in most cases a response is made, which in turn must be taken into account in the firewall. As an 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.
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 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.

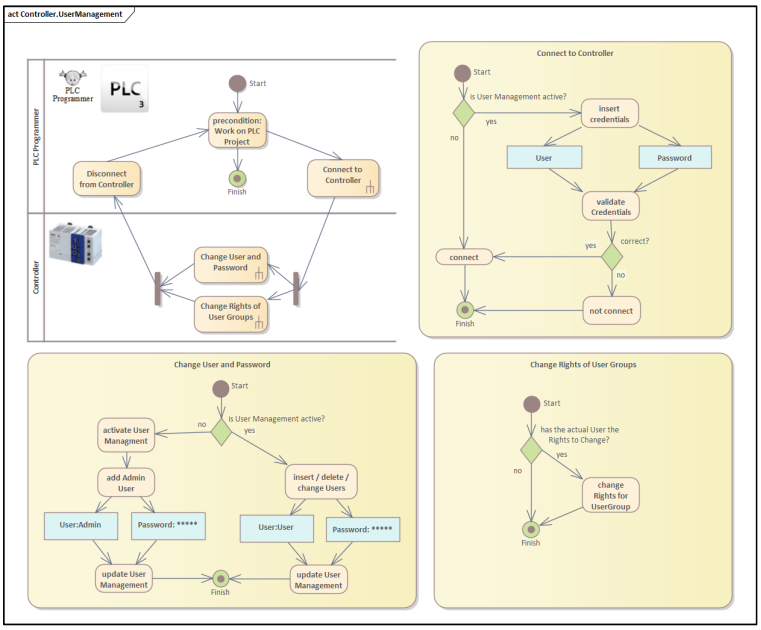
A Controller.Firewall rule for the Controller A might look like this:

- 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.UserManagement

Controller.UserManagement is 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.

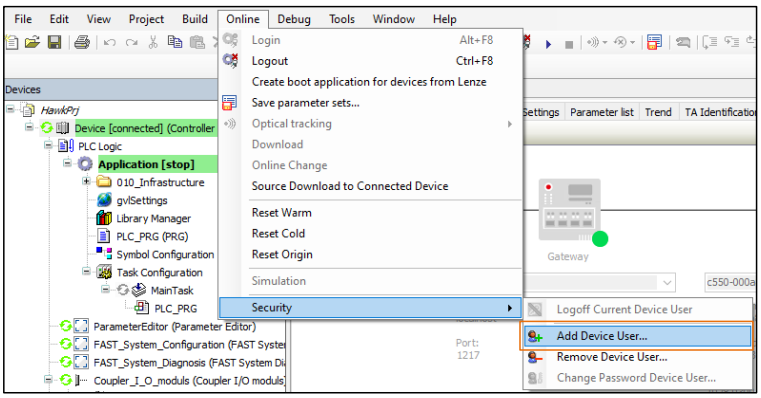


Activity Diagram

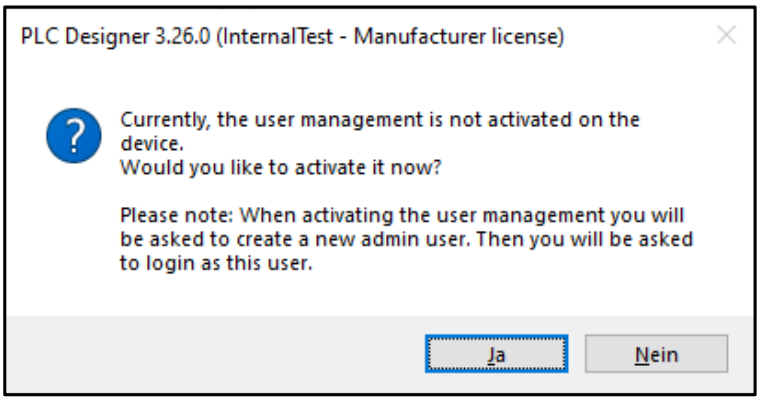
Controller.UserManagement: Activating

To activate user management, the »PLC Designer« must be connected online to the Controller. With the setting

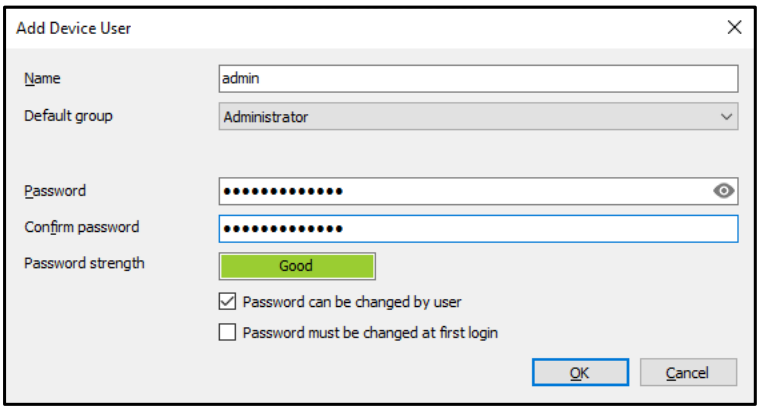
Menu / Online / Security / User Login ...



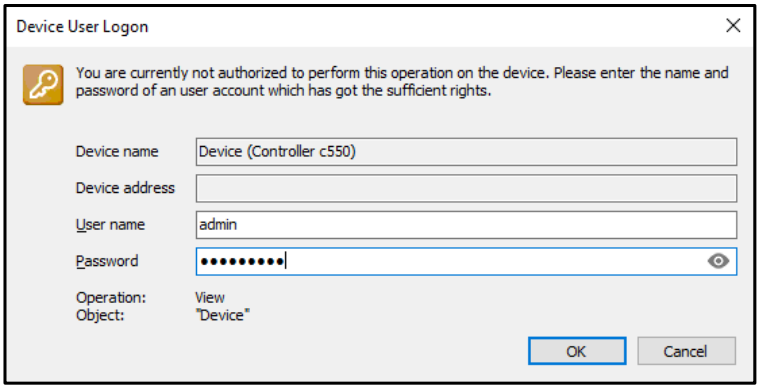
Add Device User



Activate user management



Add Device User Dialog

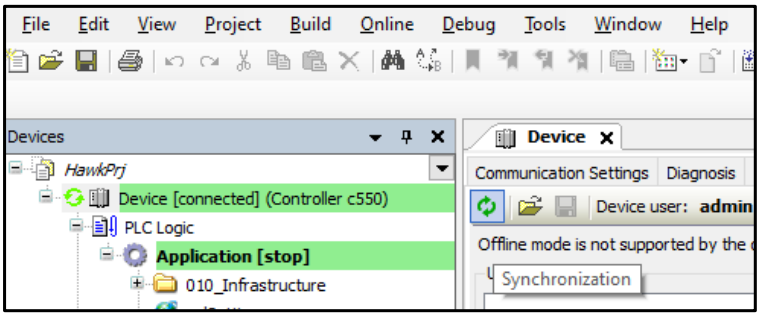


Device User Logon

Controller.UserManagement: Change Users and Groups

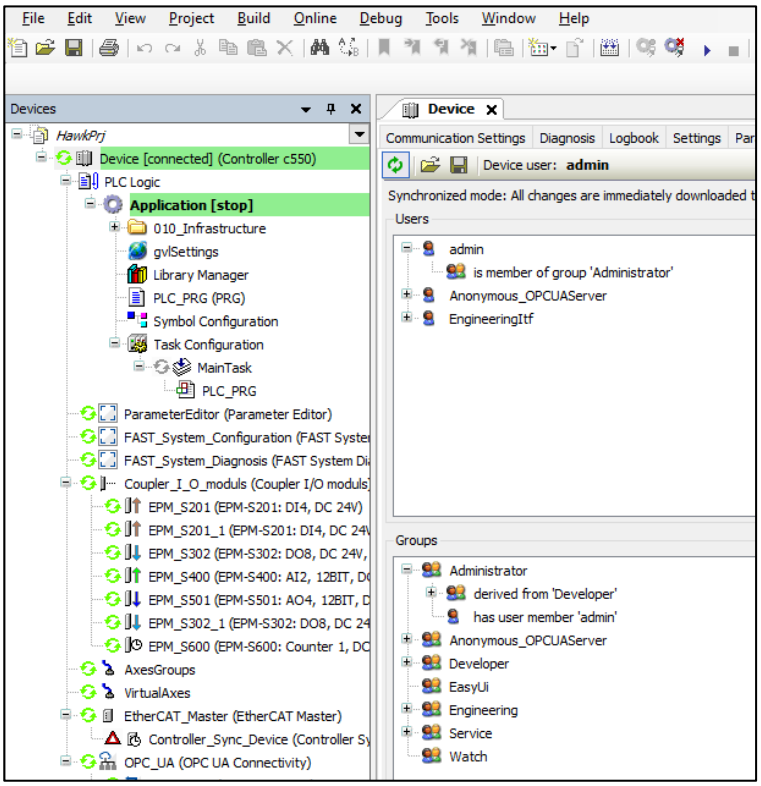
To manage the users, first synchronize the user management, with:

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



Synchronization

Adding a user is accessed via the Add... realized. 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.

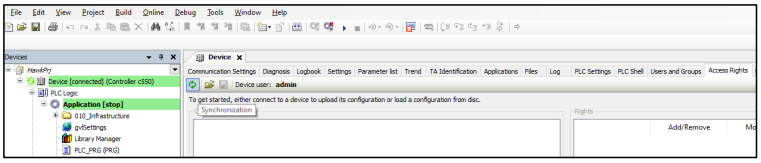


Set Users and Groups

Controller.UserManagement: Change Access Rights

To manage the Access Rights, first synchronize the user management, with:

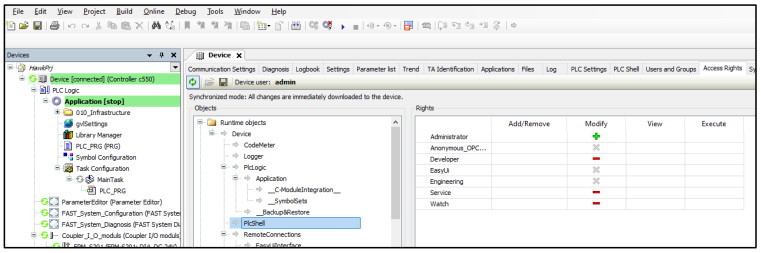
Device-Tree / Project / double-click on Device / Menu Access Rights / Synchronization



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



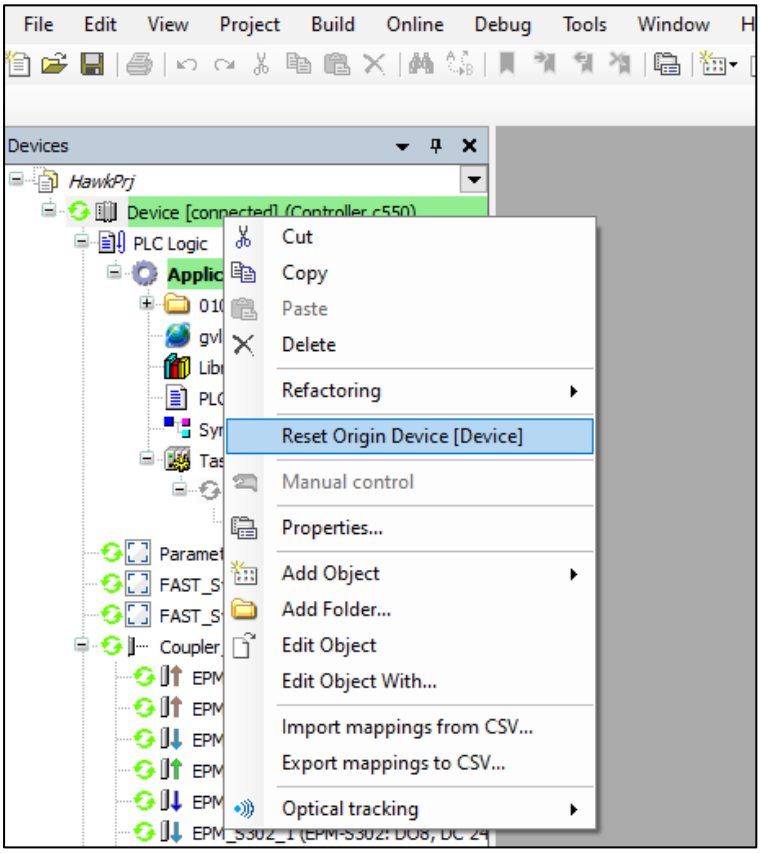
Setting the Access Rights

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

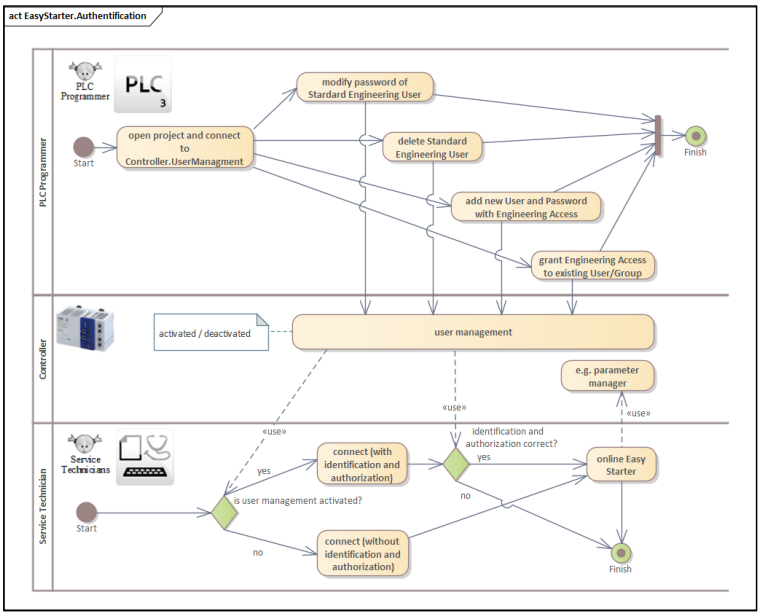
To remove the user management (Attention: All users, groups and access rights will be removed) right-click on the Controller device in the device tree of the PLC project and execute the "Reset Orogin Device" for the user management.



Reset Origin Device [Device]

Controller.UserManagement: EngineeringItf

User management is not activated in the delivery state. In this respect, 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 (📖 107)), these tools must identify and authenticate themselves before they can go online. The activation of the user management, as well as the settings of it, is 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 thus personalize it. In addition, there is an entry '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 authentification.

Add new User and Password with Engineering Access

The programmer can add a new or an existing user to the "Engineering" group. Through this mechanism, it can give 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 object "Runtime objects / Device / RemoteConnections / EngineeringInterface" can be set under the tab "Access Rights". Only the rights "Modify" can be set here. With this setting, the above access can be consented to or not.

Anonymous login

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

In the settings under "Communication Settings / Device / Change Communiation Policy" there is a selection in the category "Device User Management", 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 in the Group "Anonymous_OPCUAServer".
If anonymous login is prohibited, the user "Anonymous_OPCUAServer" and the group "Anonymous_OPCUAServer" will be delete. 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". There is no Users in this Group.
- By adding a new User to the group "EasyUI", this created user can later authenticate to the controller with the name and password assigned here with the »EASY UI Designer«.
- Existing users can be added to the "EasyUI" group. This also gives you permission.
- Furthermore, complete other groups can be inherited into the group "EasyUI" and thus complete groups get the right.

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 group "EasyUI" 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«

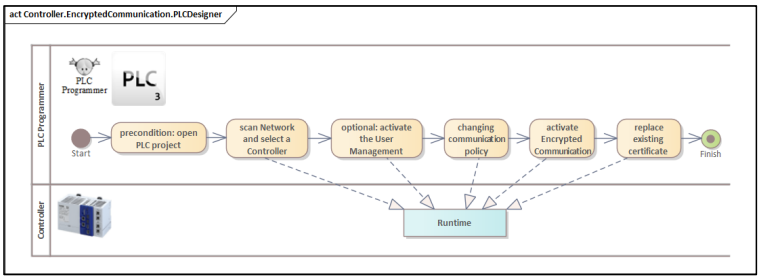
After the configuration of the user management described above, the rights for the group "EasyUI" can be restricted. This is done via the "Access Rights" tab. The setting can be found under "Runtime objects / Device / RemoteConnections / EasyUiInterface". With the settings Modify, View and Execute, the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

All users in the group have the same rights.

Controller.EncryptedCommunication.PLCDesigner

This functionality is available sind Controller Firmeware 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:

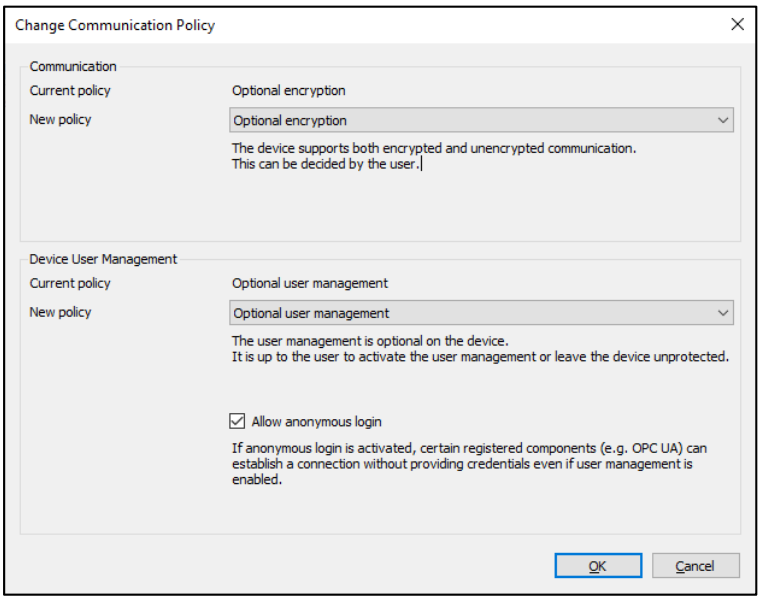
- Open the »PLC Designer« project or generate a new project in the »PLC Designer«.
- In the Device Tree double-click the Device, e.g. Controller c550.
- Open the Communication Settings tab.
- Scan Network and select the Controller.

Optional: Activate the user management

Activate the user management (Controller.UserManagement (📖 107)).

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 ...".



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 accepts only not encrypted communications. In this case the »PLC Designer« has to communicate in cleartext.
- "Optional encryption"
  Then the Controller accepts both, encrypted or unencrypted communications. In this case the User of the »PLC Designer« can deside if the tool will communicate in cleartext or encrypted.
- "Enforced encryption"
  Then the Controller 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:

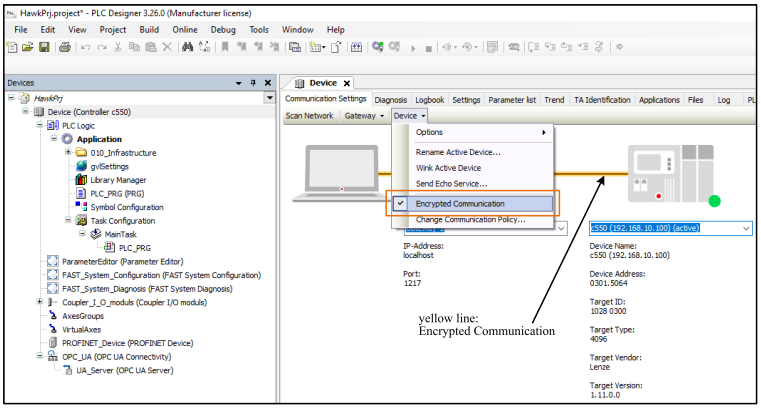
- "Optional user management"
  If a new project is generated the user management is deactivated. The user management can be activated by the user (Controller.UserManagement (📖 107)).
- Enforced user management
  If a new project is generated the user management is active. When using it for the first time, an administrator-user must set up.

With the setting "Allow anonymous login" the anonymous login can be prevented. For more details see Controller.UserManagement (📖 107).

Activate Encrypted Communication

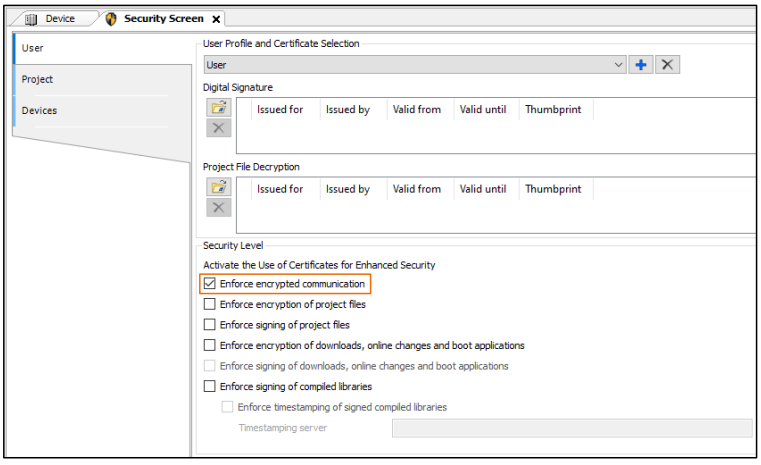
There are two ways to activate the encrypted communication:

- The menu item to activate the encrypted communication is located in the "Communication Settings" tab within 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

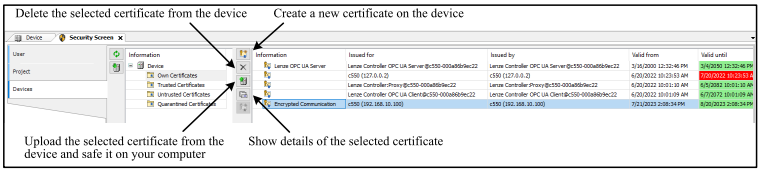
- The second way is to use the Security Screen. The Security Screen is located in the »PLC Designer« Menu "View / Security Screen". Within the tab "User" the checkbox "Enforce encrypted communication" can be found.



Enforce Encrypted Communication

Using Encrypted Communication

After activating the "encrypted communication" there will be a certiciate 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".



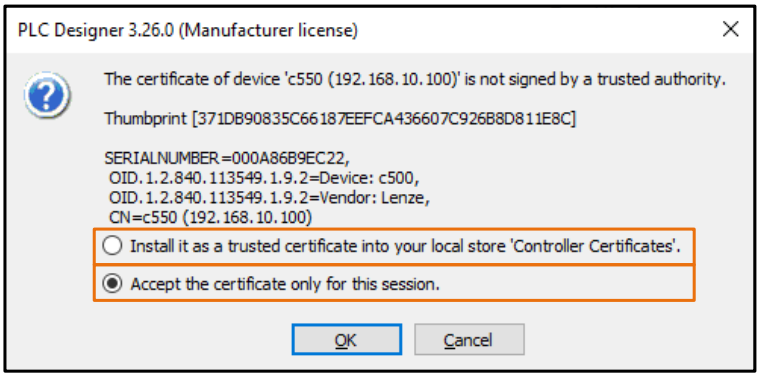
Certificate for Encrypted Communication

Details of this automatic generated certificate can be found in this documentation: Controller.EncryptedCommunication.PLCDesigner:Certificate (📖 86)

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 Controller the »PLC Designer« has to trust the Certificate of the Controller. There are two ways to do this:

The first way is to login the »PLC Designer« to the Controller with activated "Encrypted Communication". The following message box will appear and the user can decide, if the Certiciate is only used 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 connection and for all subsequent connections as long as the Fingerprint of the Certificate matches.

More information about the Windows Certificate Store:

- Security strategy (📖 11)
- Integrate a certificate in the windows certificate store (📖 40)

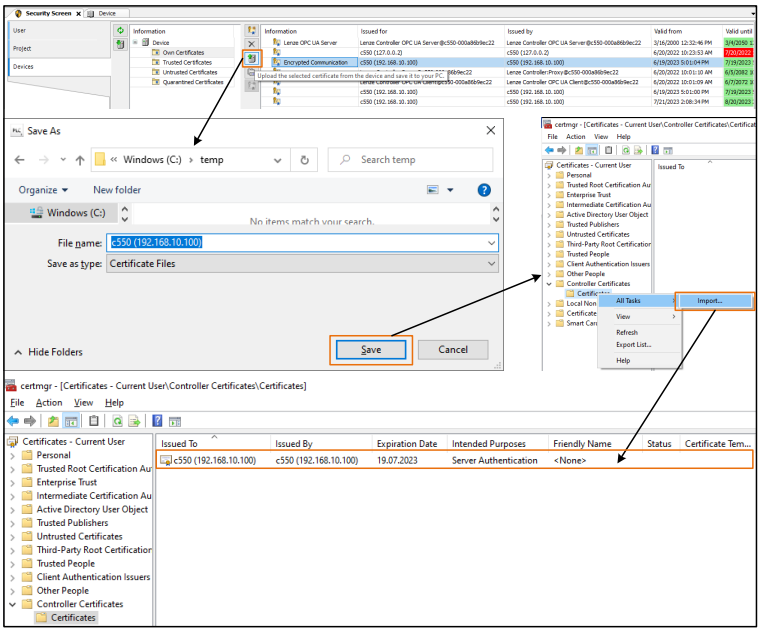
The second way is using the Security Screen with a logged in »PLC Designer« to the Controller. To do this, follow the steps below:

1. Open the Security Screen in the »PLC Designer« Menu "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 safe it on your PC". Choose an Directory and safe 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 format of the file 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 (📖 36).

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

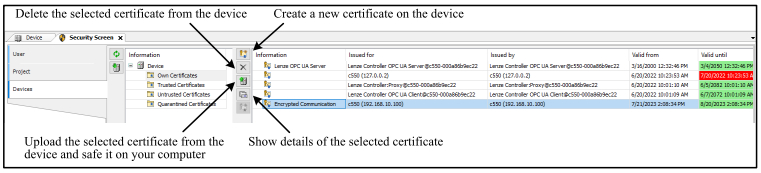
4. After the import, the Certificate is shown in this directory and the »PLC Designer« will use it for every connection to this Controller without asking for trust.



Upload and Import Certificate

Replace existing Certificate

For replacing the existing Certificate, for example to extend the valid dates, the Certificate can 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:

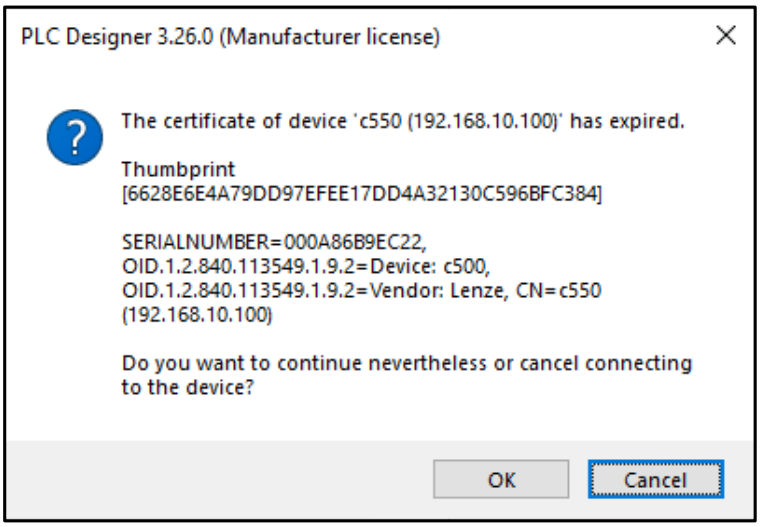
If deleting the Certificate of the "Encrypted Communication" it will automatically generate new with the default values (Controller.EncryptedCommunication.PLCDesigner:Certificate (📖 86)).

Create a new certificate on the device:

With using the button "Create a new certificate on the device", the user is able to generate a new certificate and input the wanted Key Length and the Validty Period.

Expired certificate

If the certificate of the "Encrypted Communication" is not valid anymore, and the »PLC Designer« logged into the Controller a warning will appear:



Valid Warning

The user can decide if he like to cancel or using the expired certificate.

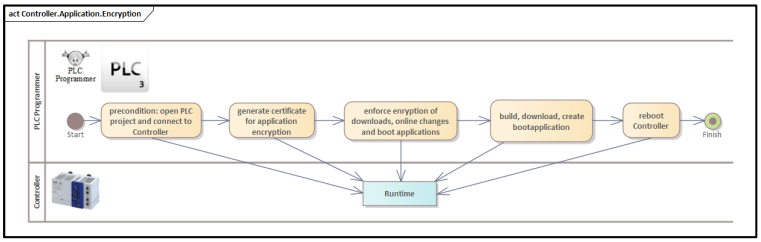
Controller.Application.Encryption

This functionallity is available since Controller Firmware version 01.11.00.

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

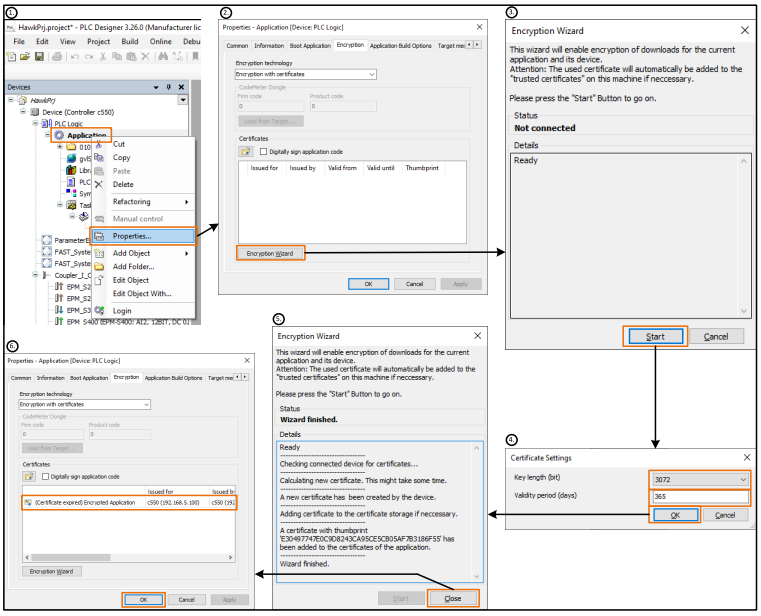
- the application itself
- the online change
- the boot application.

The system integrator can use this functionality to protect its intellectual property and thus the 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.

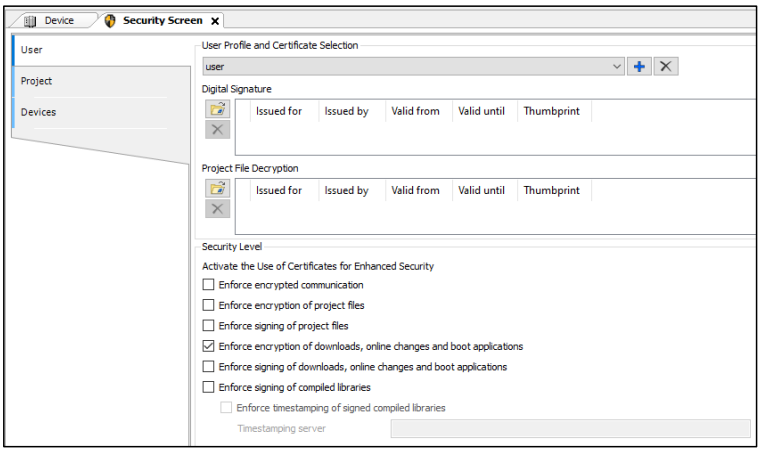


Encryption Wizzard

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

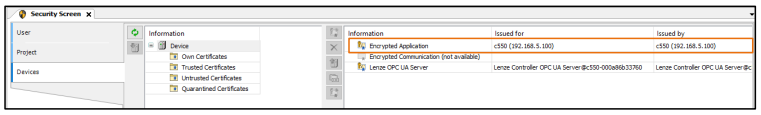
- Open the »PLC Designer« project and select the item Application in the Devices Tree and call up the entry "Properties...".
- Call the Encryption Wizard in the following dialog. Please choose the Encryption technology "Encryption with certificates".
- Start the Encryption Wizard.
- Enter the key length 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

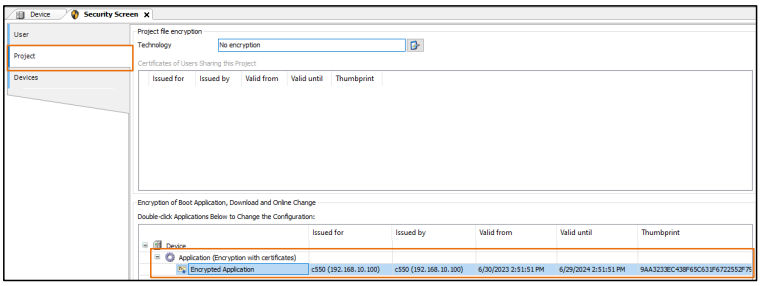
The generated certificate for the Encrypted Application can be found in the Security Screen in the Devices tab. As long as the certificate is not generated, a placeholder labeled "Encrypted Application (not available)" is displayed here.



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 (📖 131)).

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



Security Screen Project

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

1. Use the »PLC Designer« to build the project again.
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 behavior of the Controller is described below if an Encrypted Application was stored as a boot project and the certificate is then deleted.

Pre-Condition

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

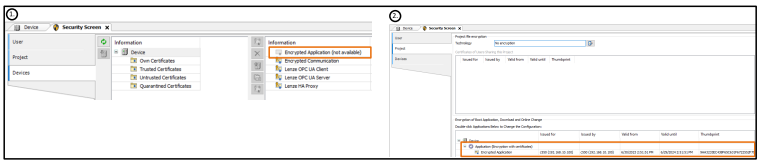
Delete the Own Certificate "Encypted Application" on the Controller

Next step is manually delete the certificate "Encrypted Application" on the Controller, 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 Screen→Devices" is shown as deleted, i.e. with the placeholder "Encrypted Application (not available)" (see (1.) in the follwing figure). Unter "Security Screen→Project" the certificate for the Encryption of the Application is still shown, because the Application of the Controller still needs this Certificate (see (2.) in the follwing figure).

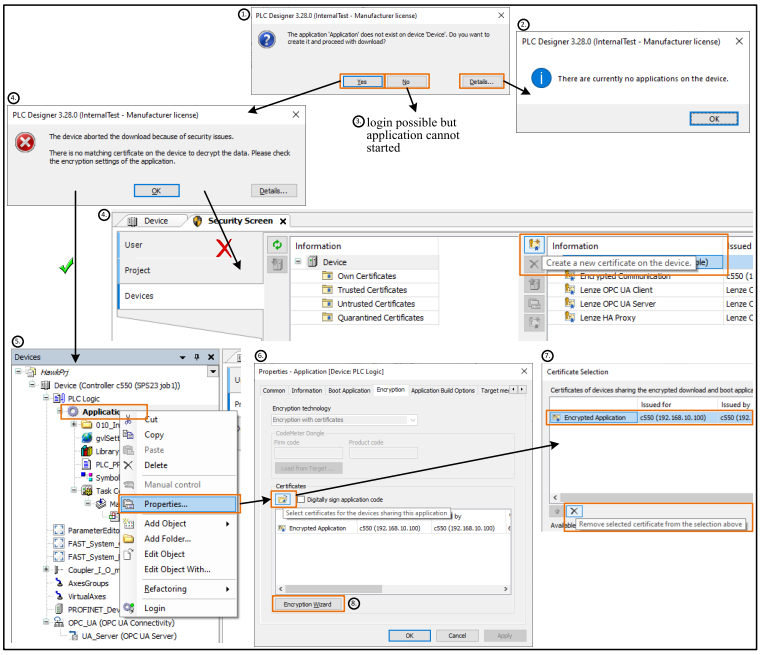


Certificate Encrypted Application Deleted

If the certificate is deleted and the user wants to go online on the Controller with the »PLC Designer«, this is not possible. An online change or a create boot application is also not possible. The deletion has an immediate effect.

Replace the Own Certificate "Encypted Application" on the Controller

After "Log Off Current Device User" and "Login" again, the message "The application does not exist" appears (see (1.) in the following figure).



Certificae Encrypted Application Renew

The existing application cannot downloaded to the Controller, because there is no matching certificate on the Controller 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 solv 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 Wizzard. After these steps, build, download the application, generate the boot application and restart the Controller, the application is 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 a create 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.

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

The behavior of the Controller is described below if an Encrypted Application was stored as a boot project and the Controller has to replace.

Pre-Condition

The Controller.Encrypted.Application with a Certificate is activated, 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, create boot project and restart 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.

Pre Condition

The Controller.Encrypted.Application with a Certificate is activated, 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, refer to Parameter 0x2022:040, the runtime system (firmware) and the project data on the SD Card is copyed to the plugged USB stick.

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, a restore to the original state should be restored. With the help of the Restore mechanism, refer to Parameter 0x2022:043, the runtime system (firmware) and the project data on the SD Card is copyed from the plugged USB stick.

Depending on the condition, the behavior may differ.

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

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

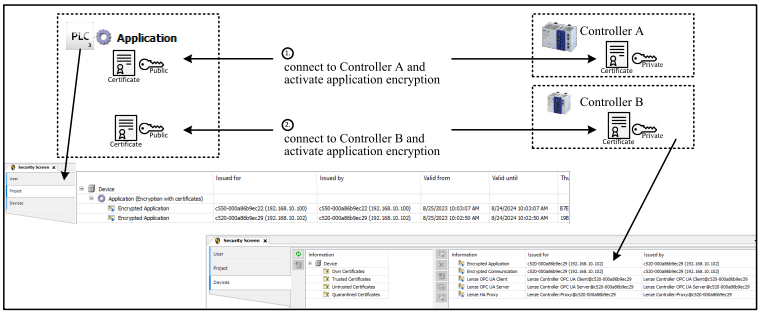
The Backup and Restore Tool saves the data of the firmware and the application on the USB stick. However, for security reasons, the private keys and certificates are not saved. For this reason, series commissioning cannot be used with this mechanism, since the pair of keys does not exist on the target 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 offline-"create boot application" function from the »PLC Designer« does not work with the Controller.Application.Encryption. Therefore, an *.lda cannot be created in this way.

Use Case: Handling one project with Controller.Application.Encryption for more Controller

The use case here describes the behavior of a »PLC Designer« project that is to be used for several controllers. The process is shown in the following figure.

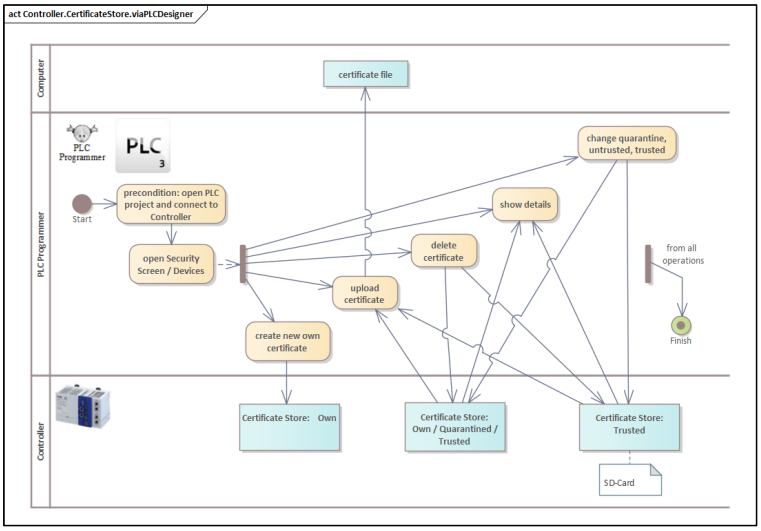


Project for multible Controllers

1. Connecting the »PLC Designer« to Controller A and activate the application encryption using the Encryption Wizard of the Application.
2. The Controller A will create an Certificate including the private key and it will be available in the Certificate Store of Controller A as ‚Encrypted Application" certificate.
3. On 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. Connecting the »PLC Designer« to Controller B and activate the application encryption using the Encryption Wizard of the Application.
5. The Controller B will create an Certificate including the private key and it will be available in the Certificate Store of Controller B as ‚Encrypted Application" certificate.
6. On 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 result, the Application for the PLC Project will have included both certificates. Depending on the active application, the corresponding certificate is then used for encryption.

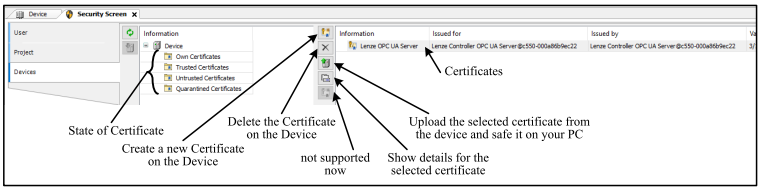
Controller.CertificateStore.viaPLCDesigner

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 with the tab "Devices".



Security Screen Devices

In the middle window, the respective status of the certificates can be selected under Information. The following four statis are available:

- Own Certificates:
  Own certificates of the Controller
- Trusted Certificates:
  Certificates from communication partners who are trusted
- Untrusted Certificates:
  Certificates from communication partners who are untrusted
- Quarantied Certificates:
  Certificates from communication partners who are 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:

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.

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".

Upload the selected certificate from the device and safe it on your PC

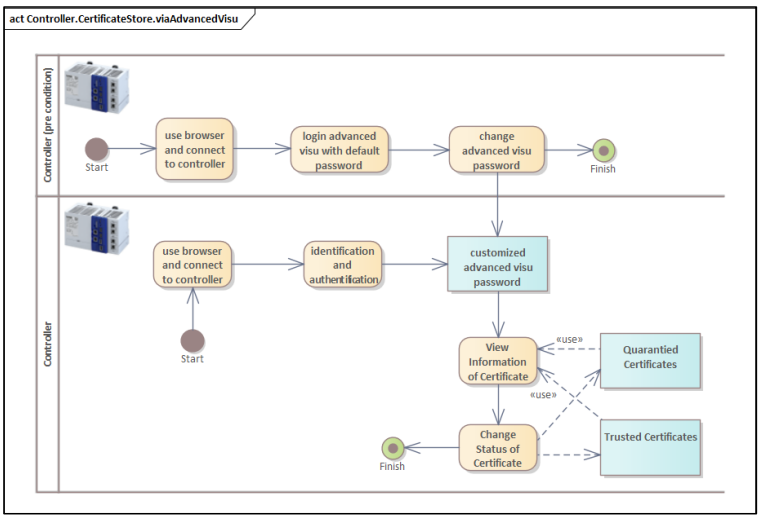
For this purpose, a certificate must be selected and the button must be pressed. It is important that the respective certificates are loaded onto the PC with the public key. The private key remains on the controller.

Show details for the selcted 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.

Controller.CertificateStore.viaAdvancedVisu

The functionality to change the status of certificates (Controller.CertificateStore.viaPLCDesigner (📖 131)) allows the machine programmer to manage the certificates on the controller. If the machine is delivered to the end customer and operated, this end customer also needs the possibility to manage new certificates on the controller. In most cases, however, the »PLC Designer« is not available for this purpose, as the PLC project remains with the machine programmer in most cases. For these reasons, a function is 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.

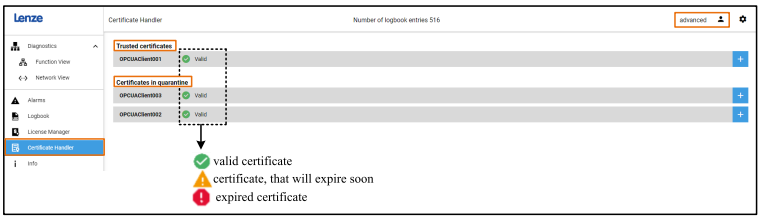


Activity Diagram

In order for the end customer to use this feature, the user must go through the following steps. First the user has to connect a browser with the diagnostic visualization of the Controller by using the IP address. In the next step the user has to identify and authenticate as a human user during diagnostics visualization with the "Advanced" user (Controller.WebDiagnosis (📖 141)).

Authentificate as Advanced User

After completing authentication the advanced diagnosis visualization is visible and the menu item "Certificate Handler" can be selected.

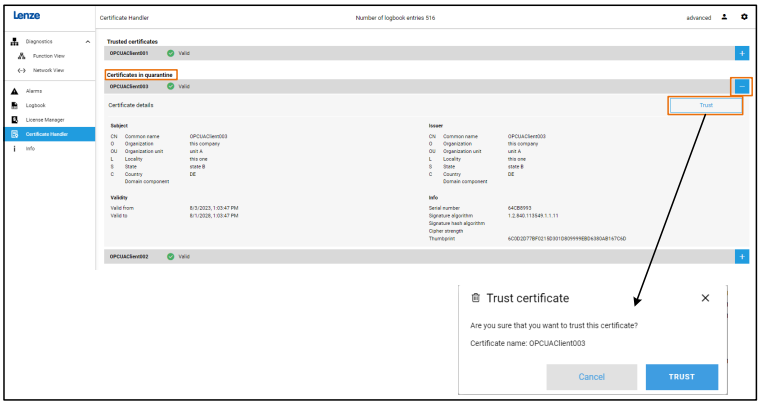


Overview

When choosing the "Certificate Handler" item, the trusted certificates and the certificates in quarantine are visible. A symbol shows the status of the validity.

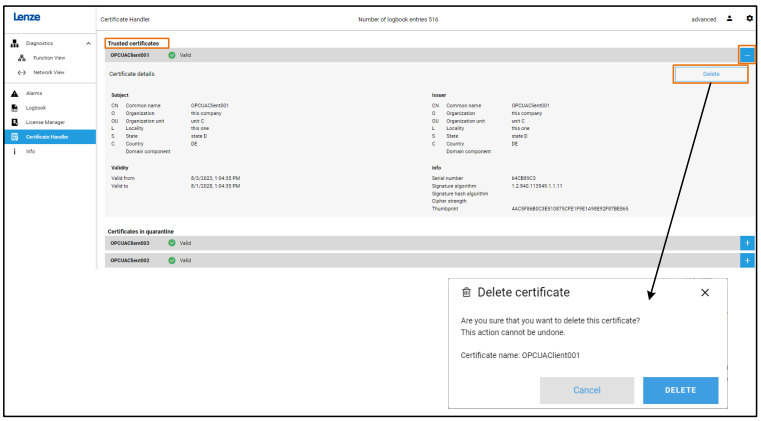
Symbol	Legend
green hook	**valid certificate** The certificate is valid.
yellow exclamation mark	**certificate, that will expire soon** The certificate is valid, but it will expire <= 27 months.
red exclamation mark	**expired certificate** The certificate in not valid (Either it is not yet valid or it is expired).

When unfold the detail view of one certificate in the quarantine, some detailed information will be shown. If selecting the Trust-button, an dialog will appear, where the user can trust this choosen certificate.



Trust Certificate

On the other hand, when unfold the detail view of one certificate in trusted certificates, some detailed information will be shown. If selecting the Delete-button, a dialog will appear, where the user can delete this choosen certificate.



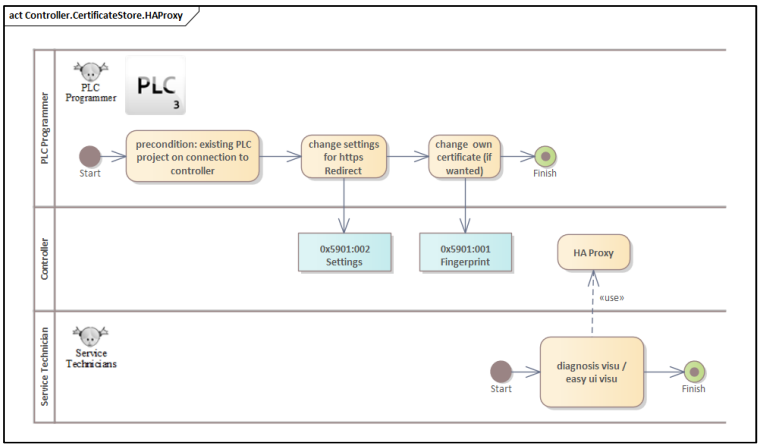
Delete Certificate

If a certificate is trusted or deleted by the user of the visualization, the visualization is automatically updated. If a certificate is created in parallel by another participant or the status is changed, the changes are not automatically visible, but a refresh must be carried out via the browser to see the changes.

Controller.CertificateStore.HAProxy

Secure Communication is available since FW Version 01.04.00.

Handling the Certificate for the Secure Communication in the Controller.CertificateStore is available since FW Version 01.11.00.



Activity Diagram

The Controller supports communication via the http and https protocols. The use of https instead of http offers your data additional protection against unauthorized access. The protection is increased, as the transmission is encrypted and there are possibilities for authentication. However, these additional functionalities can only be achieved through increased resource consumption and organizational effort.

For the selection of the communication protocol, at least the given network structure, the security needs, the capabilities of the web application and the effort (administrative and resource-related) should be considered.

Delivery Condition

From the factory, the controller offers both http and https as a protocol for various services. It is therefore a decision of the clients 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. A client 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 clients must therefore trust the new certificate.

Parameters for Displaying the Certificate Fingerprint

The parameter 0x5901:001 displays the Fingerprint of the Certificate that the Controller uses as part of an https connection to identify itself to the client. The string displayed here must exactly match the fingerprint of the server certificate displayed in the web client (e.g., web browser) to authenticate the server.

Address	Name / Setting Range / [Default]	Info
0x5901:001	Certificate fingerprint Display only	Fingerprint of Certificate for https/wss communication

Visualization

The Controllers provides a visualization system with a built-in user management. The login data is to be understood as particularly sensitive information. For this reason, it is recommended to use an https connection for visualization with configured user management.

To avoid the unwanted use of http in the context of the visualization, the controller offers the possibility to redirect client requests of visualization content to https. Redirection is to be understood as an instruction to the client to change its connection to https. A client is not forced to follow this instruction, but this should be fulfilled by all current browser versions.

Parameters for Configuring the https Forwarding of the Visualization

In the factory state, the forwarding of 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«. A change of the parameter value can only be made by the application program by appropriate control of 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 allows to change 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 reasons, it is recommended to write the parameter value only if a new setting is to be made.

The parameter setting is persisted on the device. A transfer of the setting during a device replacement / backup is not carried out. In the case of new hardware, the parameter must therefore be set anew 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, the redirect also applies to the actual landing page of the Controller and 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

The Controller uses self-signed certificates, so a client such as a web browser cannot automatically authenticate the server (the controller point). This is because the clients determine the authenticity of a certificate and thus the authenticity of a server by checking the certificate signature. This check fails for self-signed certificates because the certificate was issued by a certification authority unknown to the client and therefore not trustworthy.

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. An installation of the certificate, so that it can be used to authenticate other addresses, may not take place for security reasons.

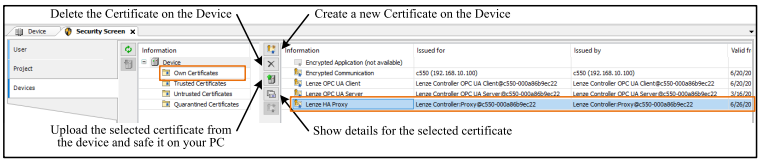
Website not working correctly with https

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 other 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 another port as 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 a 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 "/Security Data / 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.

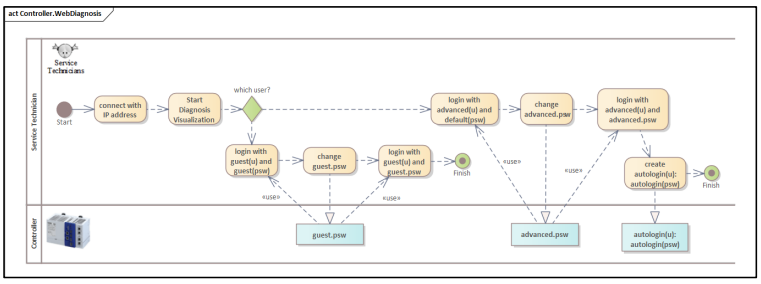
A Certificate is mandatory for a secure https connection. Existing connections are also terminated if the HA Proxy Certificate has been deleted and a new one has not yet been generated.
Example:
A web browser is connected via https to the Diagnosis Visualization of the Controller and the User has passed the authentification 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 in the browser appears "…Client cannot communicate. Socket is not available…". If now a new HA Proxy Certificate is generated with the »PLC Designer« and the user is push the Reload button on the Browser-Page, the https-connection will be established and the User has to authentificate 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.

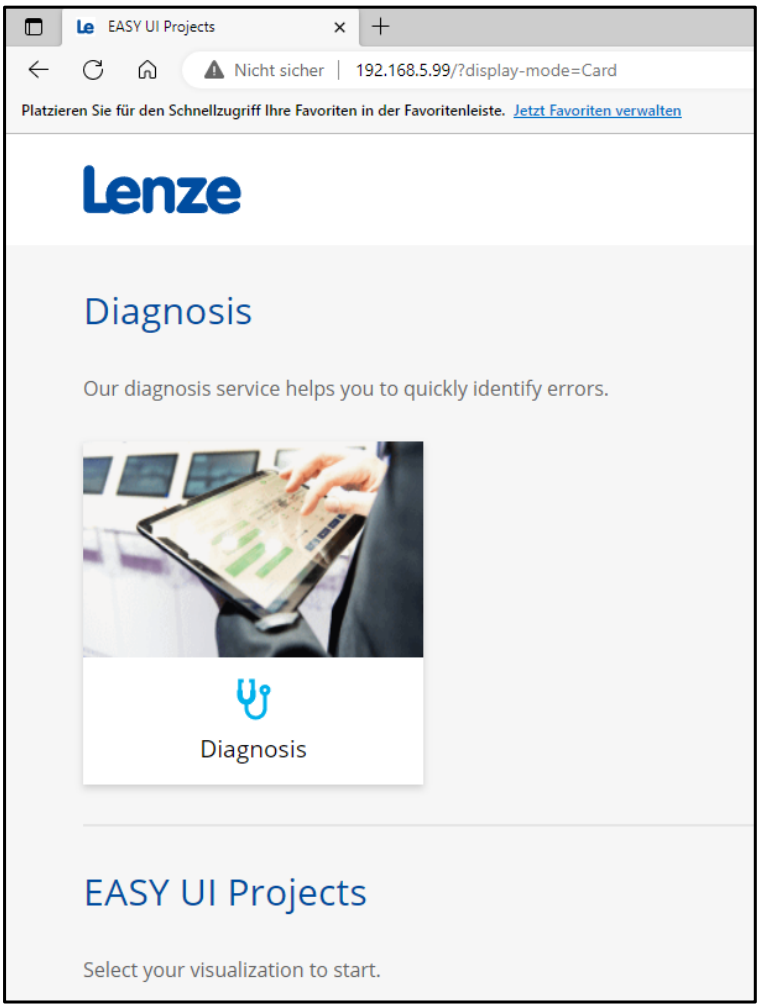
Controller.WebDiagnosis

The Controller provides diagnostics via web access since firmware version 01.09.00.



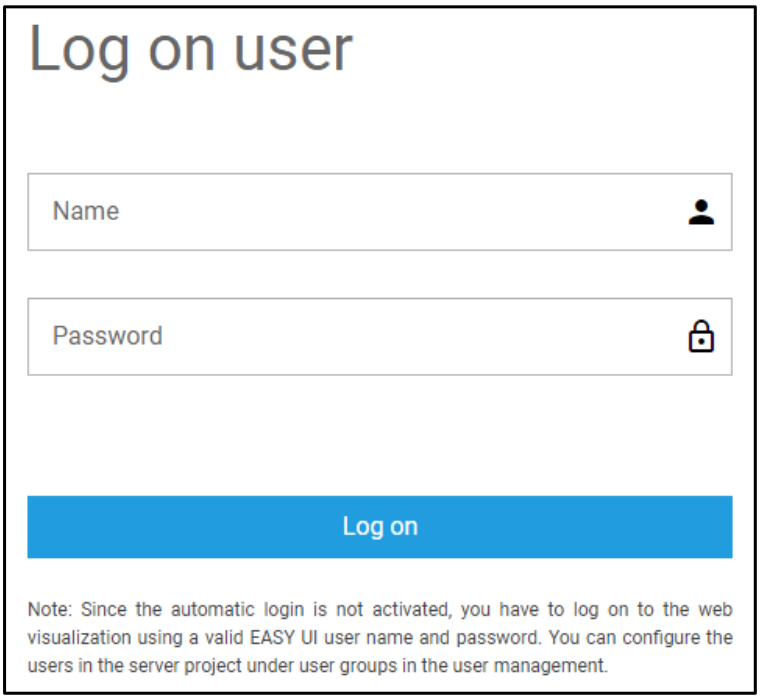
Activity Diagram

For this purpose, the web server can be addressed by entering the IP address in a browser.



Diagnosis Web-Server

After calling the web diagnostics, a login screen starts.



Log on Screen

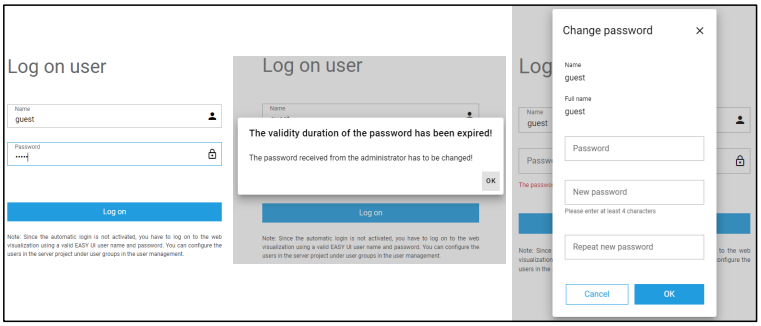
By default, two users / groups / passwords are created:

- 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 may not change any data in writing. The only exception is the function "global reset", 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 Groups Users and Advanced are called up for the first time, the respective password must be changed.



Change password procedure

Hardening of User guest and advanced

The users "guest" and "advanced" are created by default and their default password must be changed at the first use. With the exception mentioned above, this user "guest" has only read rights on the controller. The user is available by default and cannot be deleted. Use the "User settings" to change the password.

Activate Autologin

By default, the two user guest and advanced are created and their password must be changed at first use. If an uncomplicated call of the WebDiagnosis is desired and the customer waives the security function, he can perform the following steps:

- A login vom User advanced is the basic requirement, i.e. the user guest may not perform the following steps.
- A new user has to 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

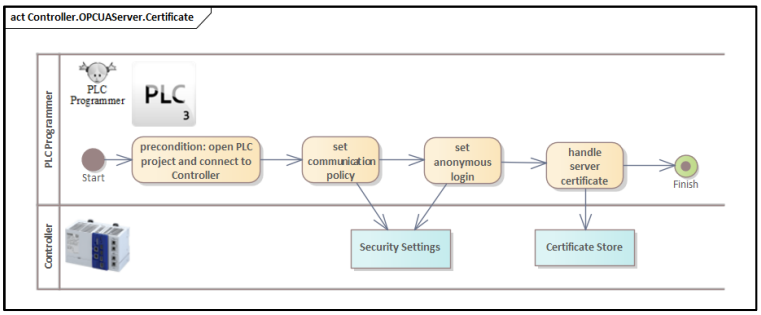
After activate autologin the user can deactivate it via the following steps:

- Automatically autologin with user "autologin".
- Choose "Logon user".
- Logon with user "advanced" and the advanced-password.
- Choose "Remove user".
- Remove User "autologon".

Controller.OPCUAServer.Authentification

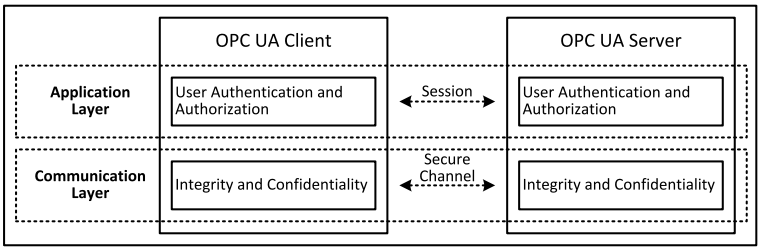
In order to be able to use the authentication of the OPC UA Server, the controller user management is required. The activation of this is described in chapter Controller.UserManagement (📖 107).

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 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 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 Controller. An OPC-UA Client can connect without having to authentificate the user.

In the »PLC Designer«, the following setting option exists for the device: Device > Communication Settings > Device > Change Runtime Security Policy ... > [Checkbox] 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 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

For 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 for deactivating 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 described for information, but 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.

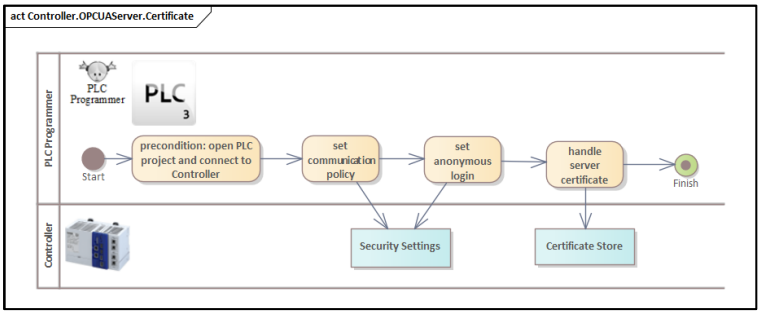
If you want to restore the user Anonymous_OPCUAServer after deletion, there are two possibilities. The first possibility is to delete the complete user management on the SD Card from the Controller. After removing user management, user management must be activated via the »PLC Designer«. This step restores 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.OPCUAServer.Certificate

The OPC UA Server offers the following message security modes:

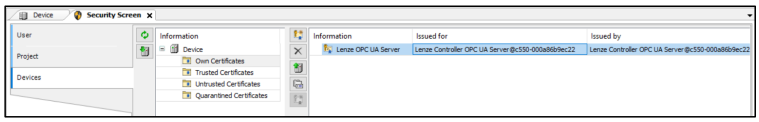
- None
  Does not include security mechanisms and should only be used for test facilities and therefore not for productive operation.
- Sign
  Includes security mechanisms to ensure integrity.
- Sign & Encrypt
  Includes security mechanism to ensure integrity and confidentiality.

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

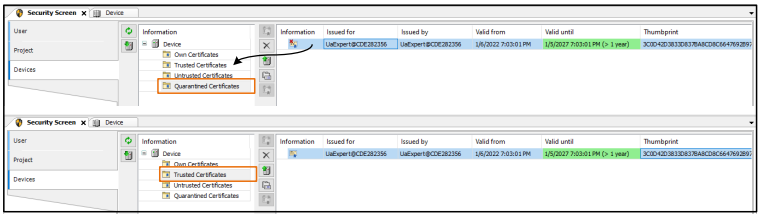
When the controller is started for the first time, a separate certificate is created for the OPC UA Server. This can be seen in the Security Screen under Devices in the "Own Certificates" section.



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 with the function "Create a new certificate on the device" (Controller.CertificateStore.viaPLCDesigner (📖 131)).

When connecting from an OPC UA Client 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 "Quarantied 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 (📖 131)) or the diagnostic visualization (Controller.CertificateStore.viaAdvancedVisu (📖 133)). After moving to the trusted area, the connection between client and server can be established.

Controller.OPCUAClient.Authentificate

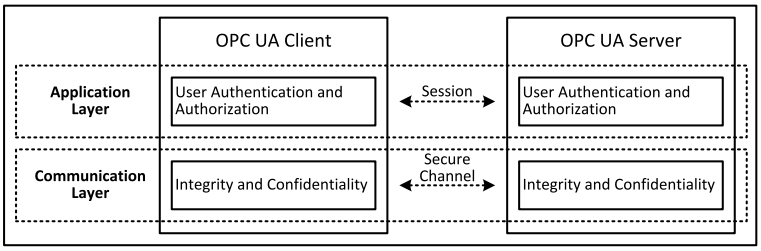
This function is available sind firmware version 01.09.00 of the Controller.

To be able to use a 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.

SecurityMsgMode

The variable is part of the structure "SessionConnectInfo". The following list shows the possibilities which could be chosen.

- 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 variable "SecurityPolicy" which is part of the structure "SessionConnectInfo".

The "SecurityPolicy" specifies the type of encryption of the transaction. Here the selection Best Available, None, Basic256Sha256 and Aes256Sha256RsaPss are offered.

- 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

UserIdentityToken

In "UserIdentityToken", the user is associated with the session. This is not for encryption of the transaction. This is used for identifying 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 ... > [Checkbox] 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.OPCUAClient.Certificate

This functionallity is available sind Controller firmware version 01.11.00.

Different to the server the OPC UA setting for the 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 certificate handling of the OPC UA client is done by the function block "UA_Connect". The certificate handling is done by the variable "SecurityMsgMode".

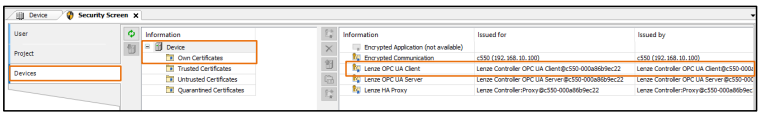
SecurityMsgMode

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.

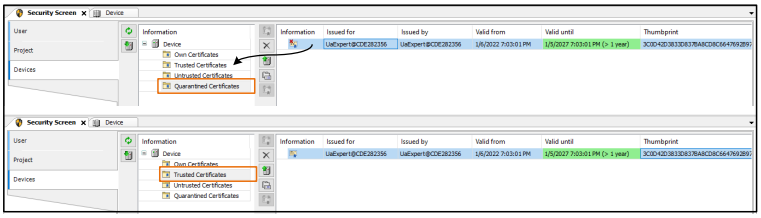
When the controller is started for the first time, a separate certificate is created for the OPC UA Client. This can be seen in the Security Screen under Devices in the "Own Certificates" section.



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 with the function "Create a new certificate on the device" (Controller.CertificateStore.viaPLCDesigner (📖 131)).

When connecting an OPC UA Client to an OPC UA Server, the respective own certificates are exchanged. With the OPC UA Client, the received server certificate will then be found under "Quarantied Certificates".



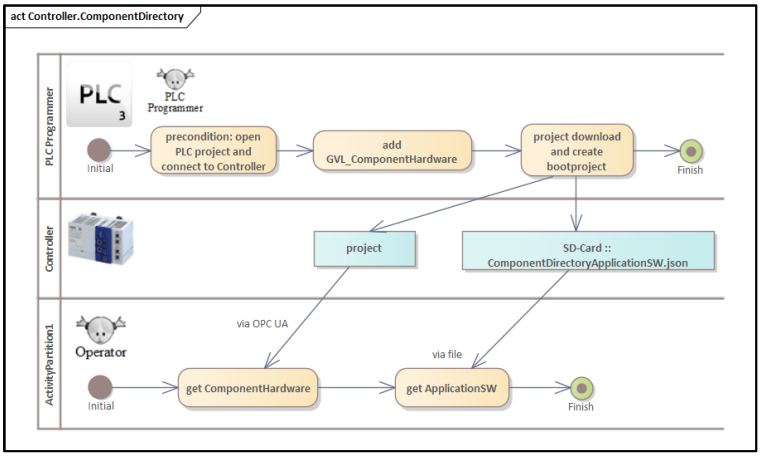
Handling Client Certificates

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 (📖 131)) or the diagnostic visualization (Controller.CertificateStore.viaAdvancedVisu (📖 133)). After moving to the trusted area, the connection between Client and Server can be established.

Controller.ComponentDirectory

This functionallity is available sind Controller firmware version 01.11.00.

An overview of the Component Directory can be found in the following figure:



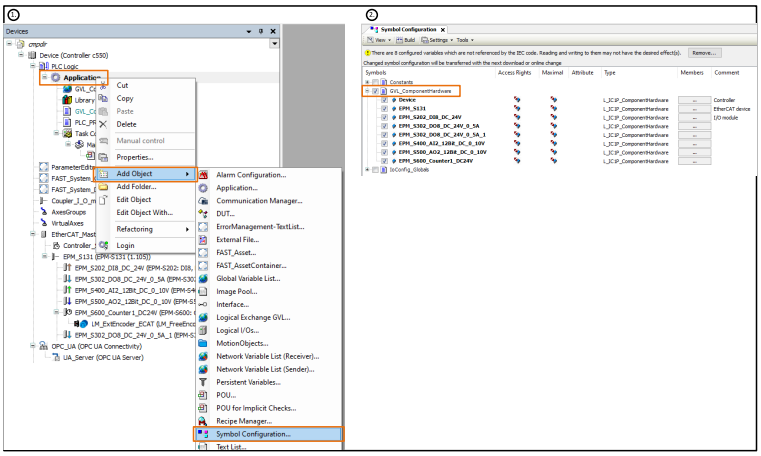
Activity Diagram

The following steps are relevant here:

- Add GVL_ComponentHardware
- Get ComponentHardware
- Get ApplicationSW

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".



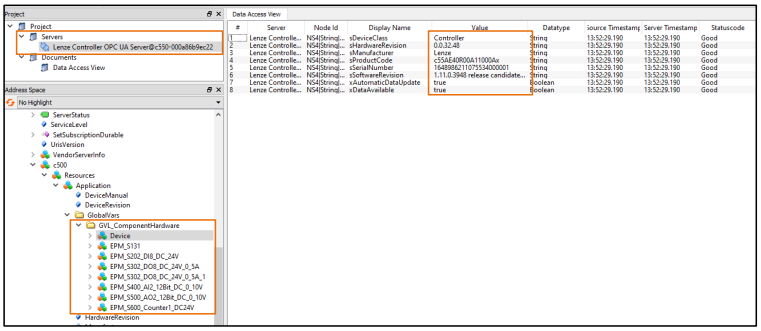
Add GVL_ComponentHardware

These are then available with a project download and subsequent create boot project. It is possible to limit data availability. Please refer to the documentation from 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



Get ComponentHardware

Get ApplicationSW

Information about the ApplicationSW are 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 from 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

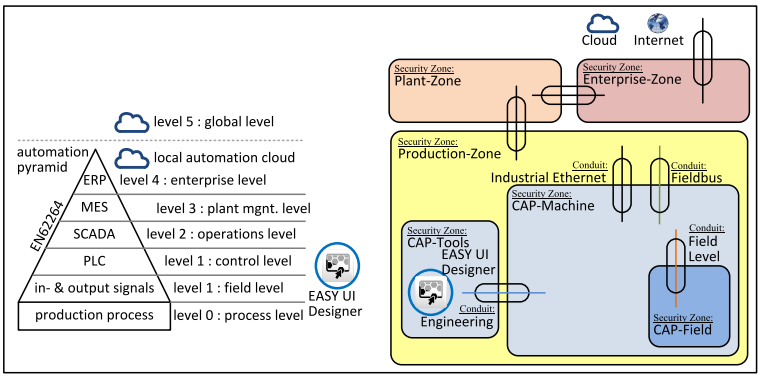
»EASY UI Designer«

Product description

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

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

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 (📖 42)).



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 environment:

- The 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.

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(UIDesigner)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }

Security mechanisms

The following security functions are included in the listed components:

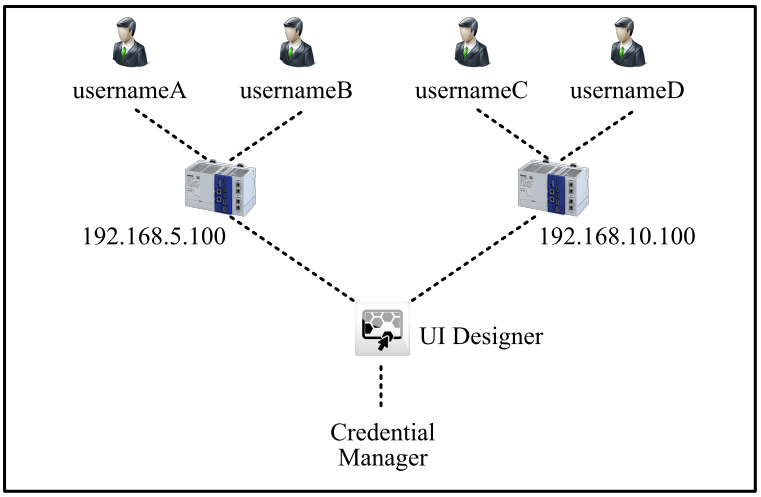
Security mechanisms

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

Security data

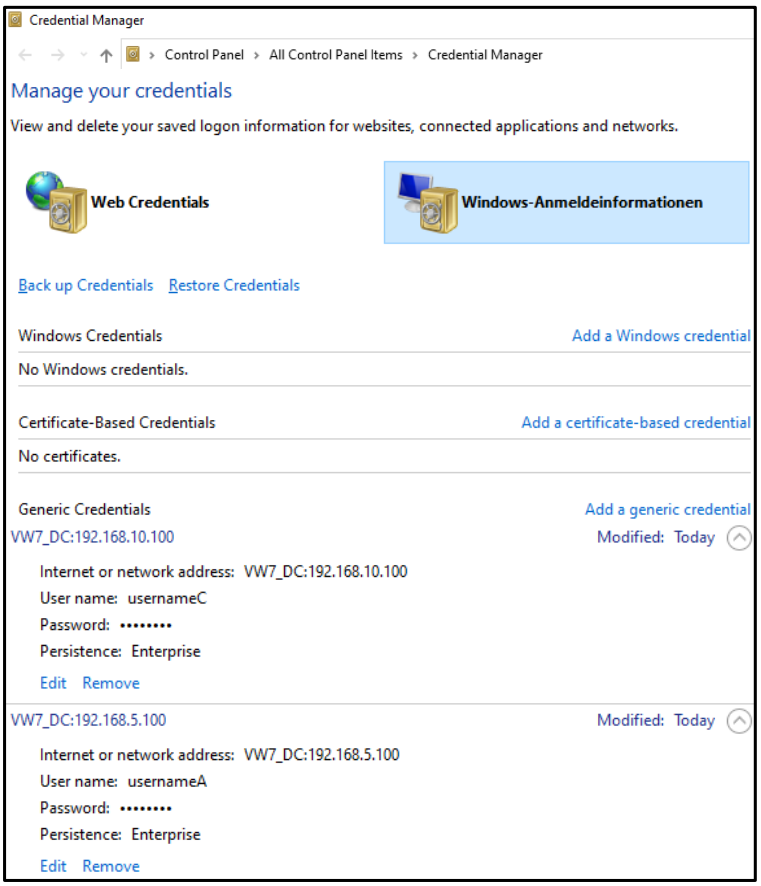
Storing credentials for authentication

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



Device User Handling

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 field "Stay logged in", two entries are created in the Credential Manager. This can be seen in the following image with 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 is 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 credential is 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:

- Calling 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-Informations".
- 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".

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 tool-access to authorized persons.
- Change existing default passwords after the first start-up and also regularly afterwards.

Commissioning and hardening instructions

- If the controller has an enabled user management, the OPC UA Client needs an authentication to access (UIDesigner.OPCUAClient.Authentification (📖 163)).
- If the controller forcing an encrypted communication the OPC UA Client needs an certificate handling for encryption (UIDesigner.OPCUAClient.Certificate (📖 165)).
- If the controller has an enabled user management, the Server Manager UI needs an authentication to access (UIDesigner.ServerManagerUI.Authentification (📖 168)).
- If the Controller forcing an encrypted communication the Server Manager UI needs an Certificate Handling for encryption (UIDesigner.ServerManagerUI.Certificate (📖 170)).
- If the Server Manager UI can only be executed with certain rights, these must be configured in the »PLC Designer« beforehand (UIDesigner.ServerManagerUI.Authorization (📖 172)).
- If the controller has an enabled user management, the Target Device Manager needs an authentication to access (refer to chapter "UIDesigner.TargetDeviceManager.Authentification (📖 173)).
- If the controller forcing an encrypted communication the Target Device Manager needs an certificate handling for encryption (UIDesigner.TargetDeviceManager.Certificate (📖 176)).
- If the Target Device Manager can only be executed with certain rights, these must be configured in the »PLC Designer« beforehand (UIDesigner.TargetDeviceManager.Authorization (📖 177)).
- Use the »EASY UI Designer« authorization concept via the user management (UIDesigner.UserManagement (📖 178)).

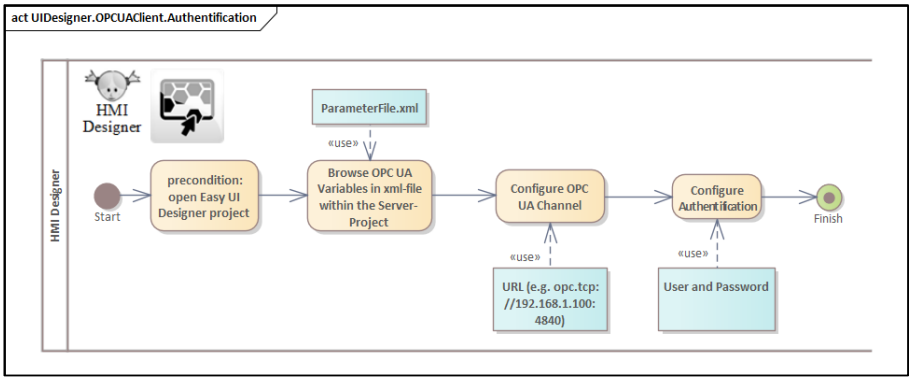
Decommissioning instructions

- After uninstalling the »EASY UI Designer«, the stored credentials must be manually removed from the Windows Credential Store (Storing credentials for authentication (📖 160)).

Security functions

UIDesigner.OPCUAClient.Authentification

The runtime of the »EASY UI Designer« executes on the Controller. This in turn has a controller-internal connection to the OPC UA Server to get the data to be displayed. This typically internal connection can also be switched externally from controller to controller, i.e. 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 (*.xlm)
- Namespace index: 4
- Device type: e.g. c500
- Device name: choose a typical name
- Choose parameter file in the PLC Projekt Directory
- Then browse through the variable tree an 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 tab Common 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.Brw.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 parametrized. If there is no active user management running on the controller (Controller.UserManagement (📖 107))

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

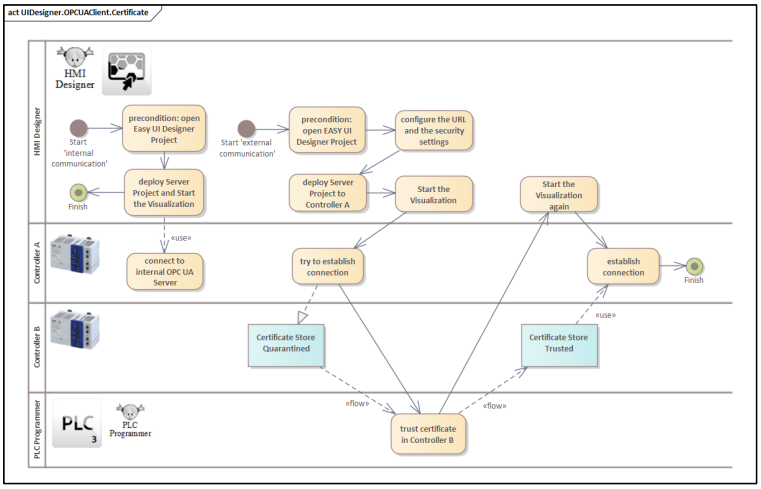
If there is an active user management running on the Controller

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

When entering the password, it should be noted that it can be read on the screen when entered in plain text. 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 forcing an encrypted communication the OPC UA Client needs an Certificate Handling for encryption.



Activity Diagram

Two different considerations or possible uses must be distinguished here.

Internal Communication

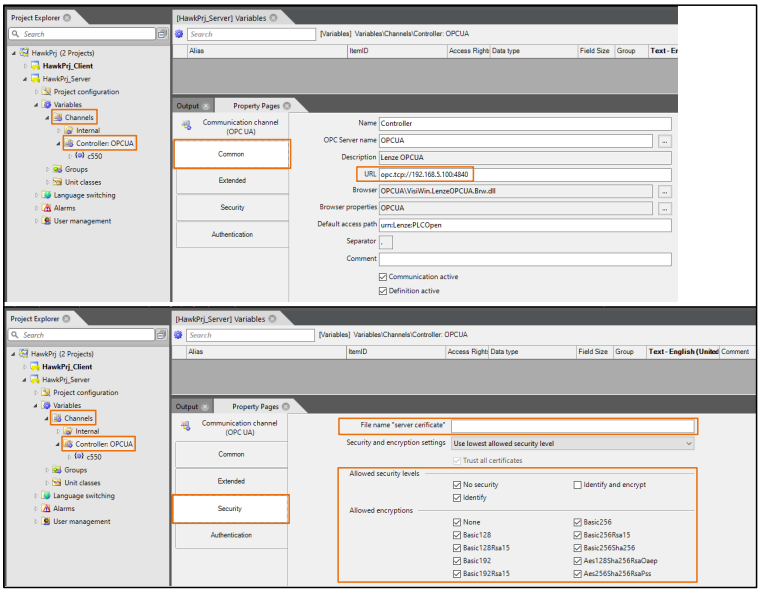
The UI Designer Runtime runs on the same Controller as the Application program. In this case, the UI Designer Runtime accesses the internal endpoint of the OPC UA Server via an OPC UA Client via internal communication. In this case, Authentication (UIDesigner.OPCUAClient.Authentification (📖 163)) is required, but no encrypted communication, since this takes place internally.

External Communication

The UI Designer runtime runs on a different Controller, as does 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.Authentification (📖 163)) is required, and encrypted communication if the other controller enforces it.

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. Please be clear to set the correct ip address with the Port of the OPC UA Server.



own “server certificate”

If changing to the Security tab, some configurations can be done, concerning the Server Certificate to connect to.

Security and encryption settings:

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

Allowed security levels:

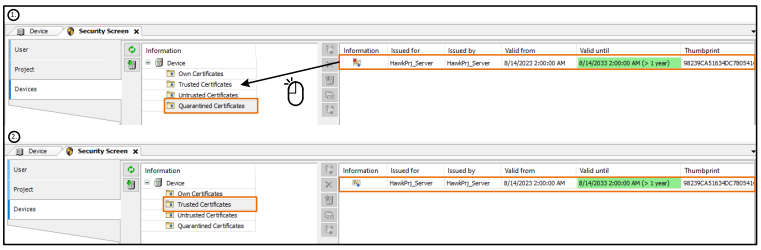
- No security
- Identify
- Identify and encrypt

Allowed encryptions:

- None
- Basic128
- Basic128Rsa15
- Basic192
- Basic192Rsa15
- Basic256
- Basic256Rsa15
- Basic256Sha256
- Aes128Sha256RsaOaep
- Aes256Sha256RsaPss

After configuration the encrypted communication, the Server Project has to deploy to the Controller A (refer to picture at the beginning of this chapter). When starting the Visualization on Controller A a connection to controller B is tried established and a certificate is quarantined here.

Now the PLC Programmer of Controller B has to trust the Certificate e.g. with the »PLC Designer«.



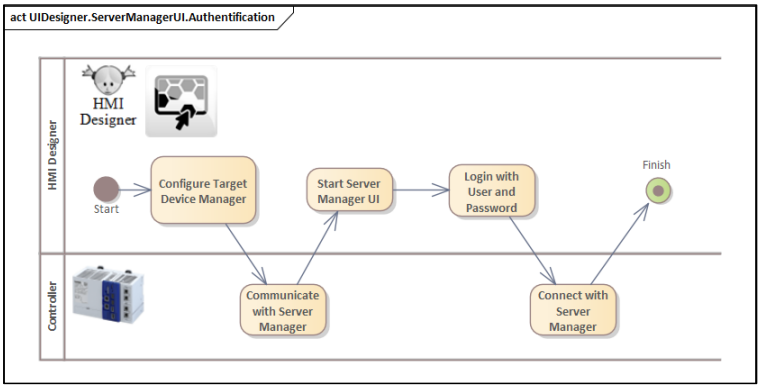
Trust Certificate

After trusting the Certificate on the Controller B the »EASY UI Designer« can start the Visualization.

Important:
This automatically generated own Certificate for the OPC UA Client is valid for 10 years and has to renew before expiration. If not, the connection from the OPC UA Client isn"t possible anymore.

UIDesigner.ServerManagerUI.Authentification

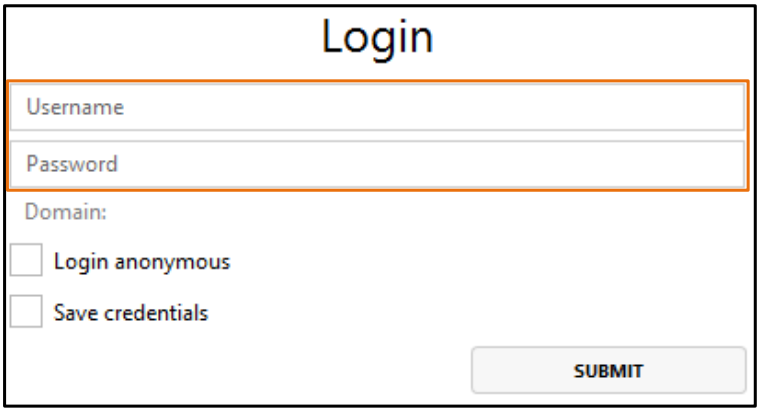
In order to be able to go online with the »EASY UI Designer« when user management of the Controller is activated, authentication must be enabled by the "Server Manager UI".



Activity Diagram

The settings for this are made with the following steps:

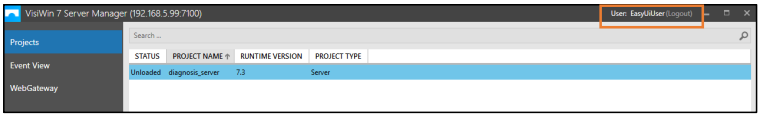
- Start the "Server Manager UI" with "UI Designer / Tools / Server Manager UI".
- Enter the username and password of an user in the controller user management group "EasyUi" (refer to chapter "Cyber Security\c5x0 controller\Security Functions\Controller.UserManagement\Controller.UserManagent: User for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



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.

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



Logout

The following characters are not supported within 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.

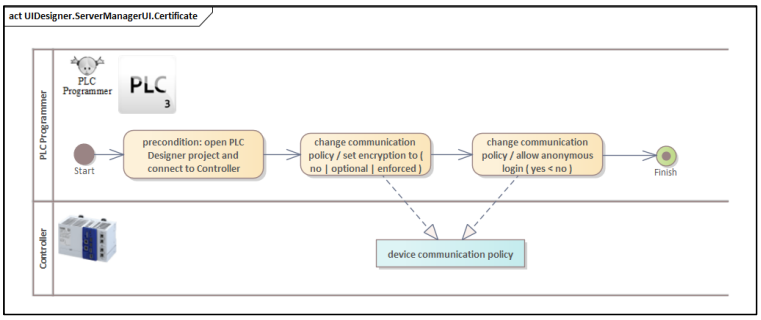
Save credentials

If the user activate the "Save credentials" flag, the Username and the Password will save in the Windows Credential Manager, (Storing credentials for authentication (📖 160)). At the next login the data will be used again.

UIDesigner.ServerManagerUI.Certificate

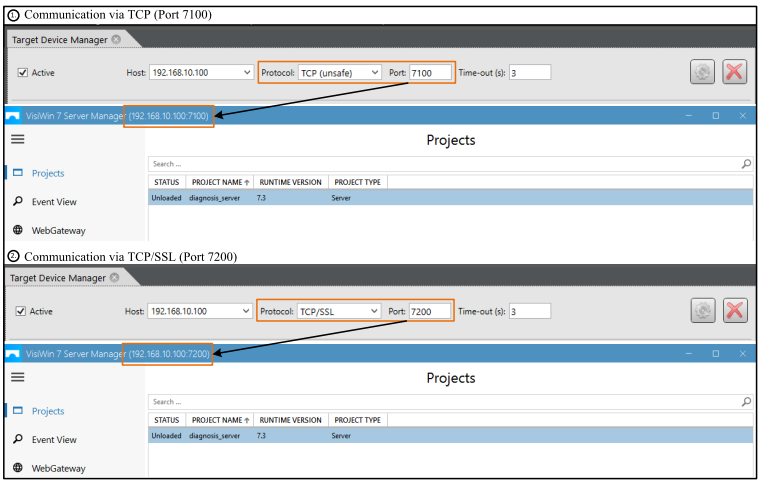
This functionallity is available sind »EASY UI Designer« version 01.05.00 and Controller firmware version 01.11.00.

If the Controller forcing an encrypted communication the Server Manager UI needs an Certificate Handling for encryption.



Activity Diagram

The »EASY UI Designer« can be operated with two protocols. On the one hand the unencrypted TCP protocol via port 7100 and the encrypted TCP/SSL protocol via port 7200. The »EASY UI Designer« operator can set this via the Target Device Manager.



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, i.e. the »EASY UI Designer« and the Runtime one the Controller, which is used for encryption. User interaction is not necessary.

UIDesigner.ServerManagerUI.Authorization

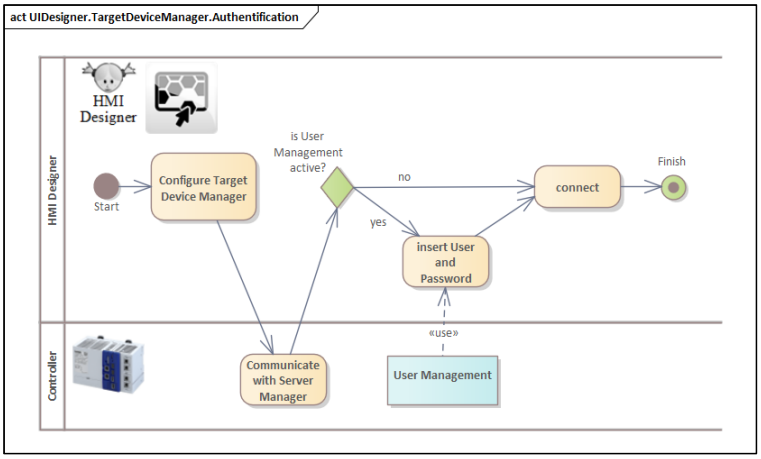
In order to configure the rights for authorization, the »PLC Designer« must be log in to the controller and the user management must be activated (Controller.UserManagement (📖 107)).

After activation the user can open the Device Window and choose the "Users and Groups" tab. Here the Group EasyUi is already existing. All Users in this Group can access the Controller via the »EASY UI Designer«. If choosing the "Access Rights" tab, the configurable Objects are shown. The Object "Runtime object\Device\RemoteConnections\EasyUiInterface" is intended for the allocation of Rights relevant here.

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 neeeded, that the Server Manager UI is able to start and stop processes and manage files.
Modify	Change	Modify-Rights are needed, that the Server Manager UI can change the configuration of projects and the Server Manager.
Add / Remove	Admin	Is not used.

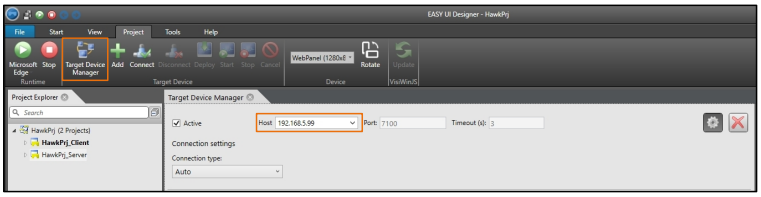
UIDesigner.TargetDeviceManager.Authentification

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



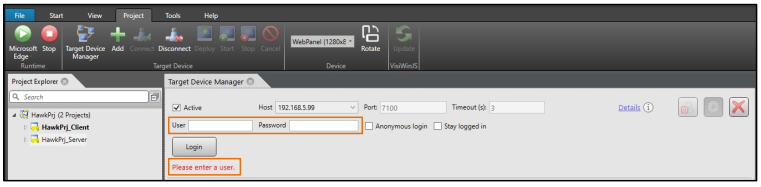
Activity Diagram

Integrate the Host-IP and connect to the controller.



Integrate Host-IP

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

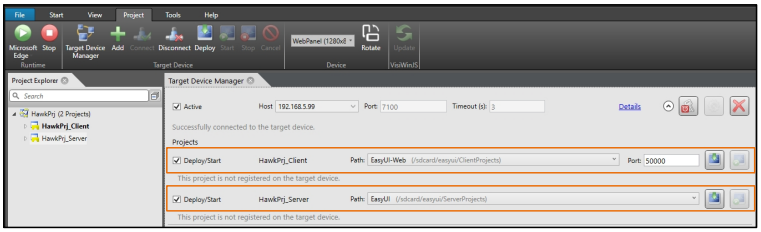


Enter a user

A user with password from an user, created in the Controller.UserManagement (Controller.UserManagement (📖 107)), must be specified.

What happens if authentication is correct?

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



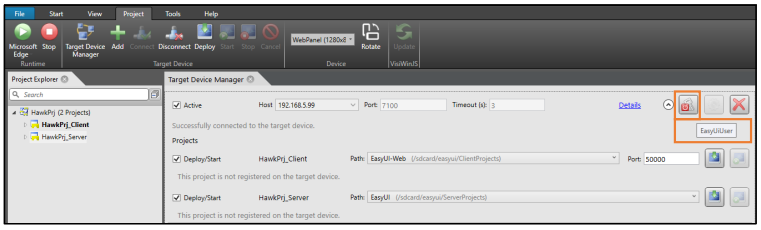
Deployment

What happens if I enter incorrectly?

If logged in with empty user " " and empty password " ", an error message "Please enter a user" appears. If you are logged in with the wrong user and/or password, an error message "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

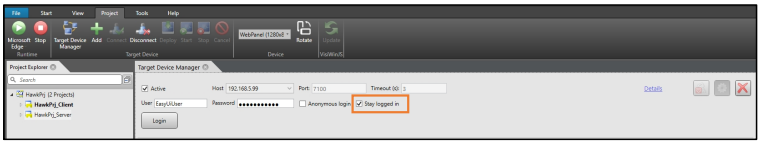
By clicking on the button, the log in authentication appears and another user can be entered and authenticated with his password.

What does "Anonymous login" mean?

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

Save credentials

With the check "Save credentials" the credentials of the user can be saved.



Stay logged in

Use case 1: Disconnect and connect from the target.

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

If the user activate the "Save credentials" flag, the username and the password will save in the Windows Credential Manager, (Storing credentials for authentication (📖 160)). At the next log in the data will be used again.

Behavior when Controller.UserManagement is not enabled

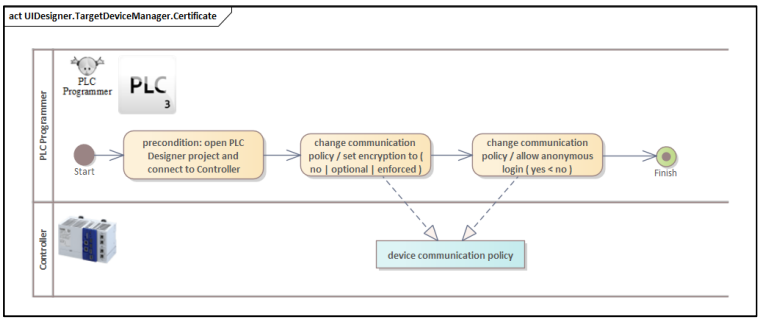
If user management is not enabled on the controller, the »EASY UI Designer« can go online without authentication. To go online to the IP address specified under host, press the button "Connect".

Connect without Controller.UserManagement

UIDesigner.TargetDeviceManager.Certificate

This functionallity is available sind »EASY UI Designer« version 01.05.00 and Controller firmware version 01.11.00.

If the Controller forcing an encrypted communication the Target Device Manager needs an Certificate Handling for encryption.



Activity Diagram

For more information see UIDesigner.ServerManagerUI.Certificate (📖 170).

UIDesigner.TargetDeviceManager.Authorization

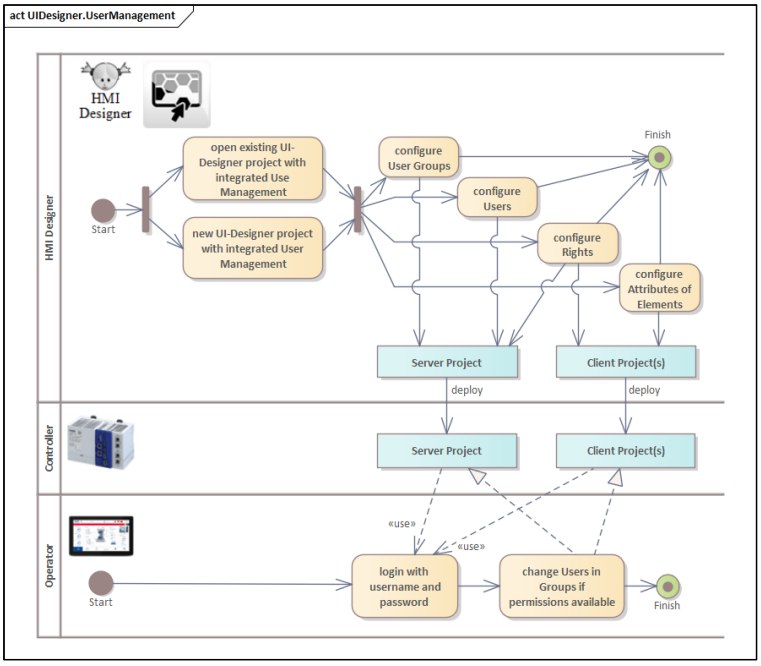
In order to configure the rights for authorization, the »PLC Designer« must be connected to the Controller and the user management must be activated (Controller.UserManagement (📖 107)).

After activation the User can open the Device Window and choose the "Users and Groups" tab. Here the Groupe EasyUi is already existing. All users in this group can access the controller via the »EASY UI Designer«. If choosing the "Access Rights" tab, the configurable objects are shown. The object "Runtime objects\Device\RemoteConnections\EasyUiInterface" is intended for the allocation of rights relevant here.

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, this can be created with the »EASY UI Designer« and adapted at runtime of the machine via the web panel (e.g. v450).

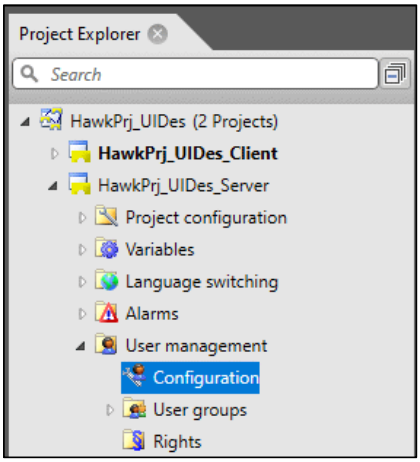


Activity Diagram

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

UIDesigner.UserManagement : Configuration

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



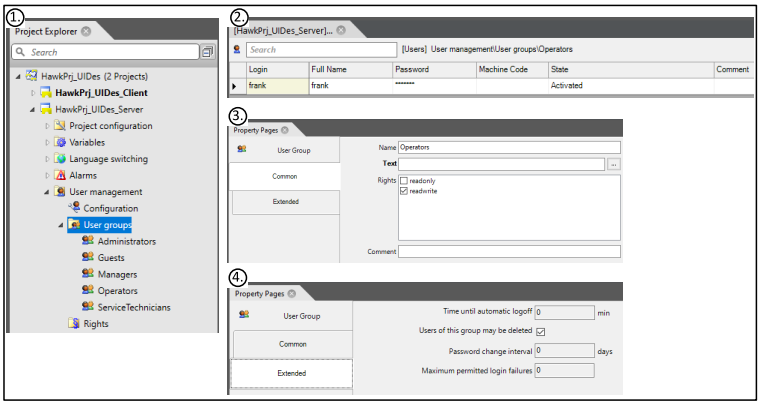
Configuration

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 Wizzard 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 result 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.

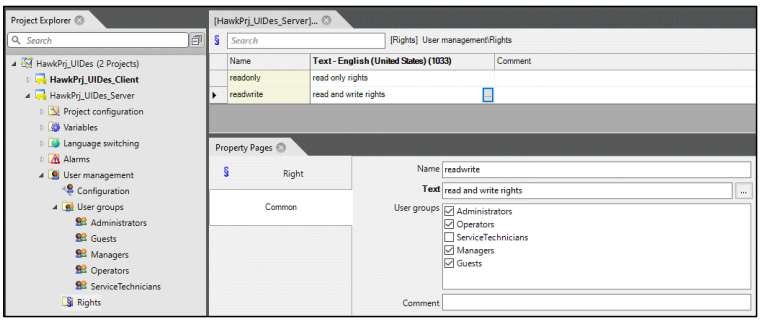
Rights

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

How to set these up, see UIDesigner.UserManagement : Rights (📖 180).

UIDesigner.UserManagement : Rights

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

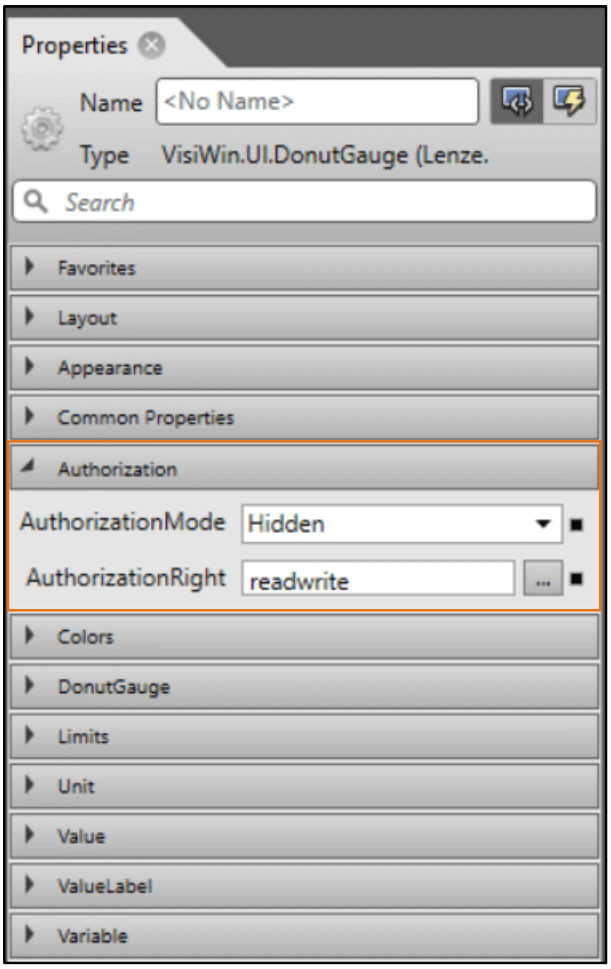


Rights

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.Authentification (📖 163).

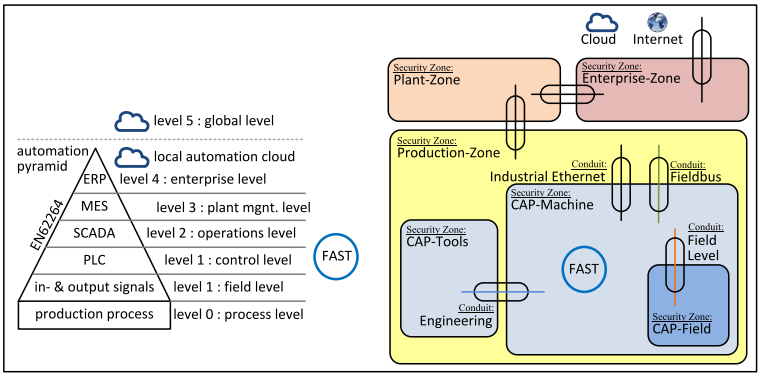
FAST

Product description

This documentation is applicable to the following software functionalities with their identification:

Name of software-functionalities	ID
FAST	n.a.

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 (📖 42)).



Product location in the network

This software functionality runs on the Controller (📖 82) and therefore has no hardware interfaces of its own.

Intended environment:

- The software functionality in the respective libraries is a product responsibility and is described here.
- The configuration of the functionalities, their parameterization and the additional programming of the application is the responsibility of the user.

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

- These components are considered 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

The following security functions are included in the listed components:

Security mechanisms

- FAST.Library.Signature

Security data

Commissioning and hardening instructions

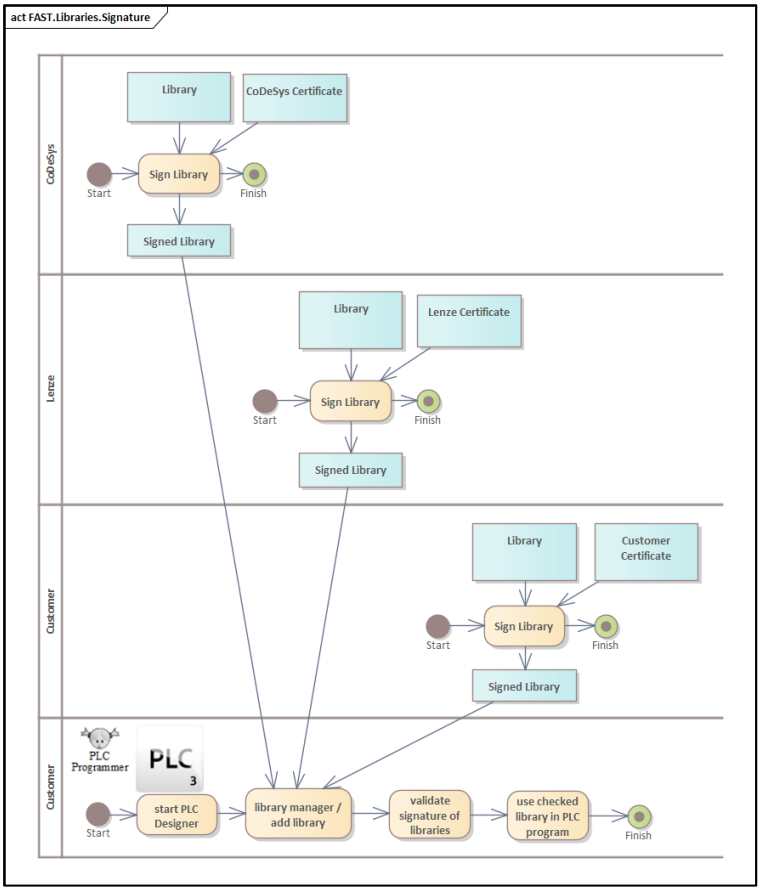
The following commissioning instructions must be followed:

- Before adding libraries in the library manager, validate the signature of the library (FAST.Library.Signature (📖 184)).

Security functions

FAST.Library.Signature

To make sure that the used libraries also come from the specified sender, so the libraries 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 activity on the part of the user is required.

Signed Libraries from LENZE

Some libraries of Lenze are already signed. No activity on the part of the user is required.

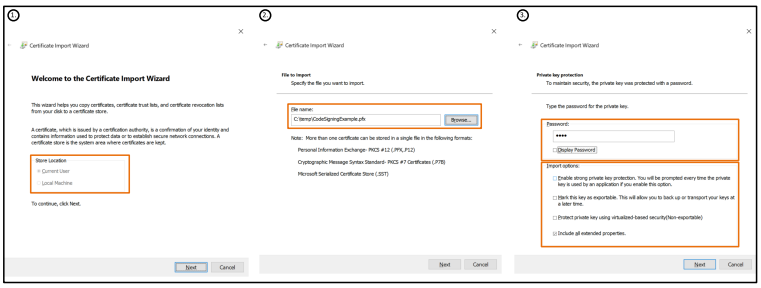
Signed Libraries from the User

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:

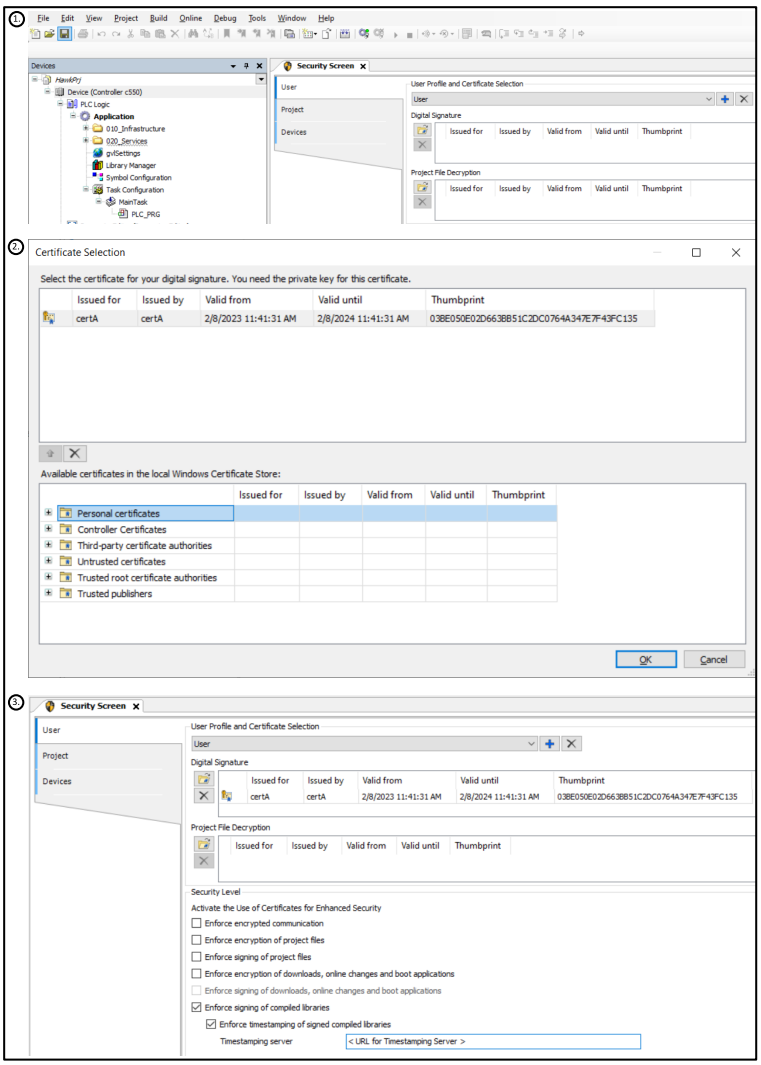
- »PLC Designer« with version > V3.22
- X509.Certificate for Code Signing (keyUsage = digitalSignatur) in *.pfx file.
- Extended-Validation-Certificate (EV-Certificate)
- Recommendation of an additional timestamping certificate to guarantee a forgery-proof time at the time of signing. Access to RFC-3161 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

Now, the »PLC Designer« must be started and a new project with the category "Libraries" and the template "Empty library" has to generate. The Security Screen must be opened with the Menu View / Security Screen. After selecting the tab "User" the Certificate for the Digital Signature can be selected.



Signing Libraries

The last activity is to save the library as a compiled library with the command "Save Project and Install into Librrary Repository". The library will be saved as a "COMPILED-LIBRARY-V3" format.

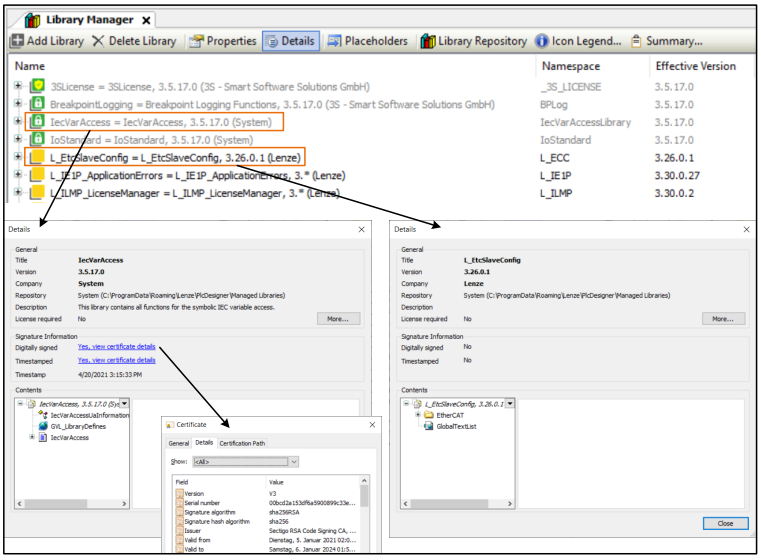
When the Library is signed, the Public Keys of the Signing Certificate and the Timestamping Certificate are integrated into the Library.

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 singed with a trusted certificate
- Yellow Box
  Library is not signed

If selecting the library, the button Details shows some information including the Certificates for Signing.



Verify Signature

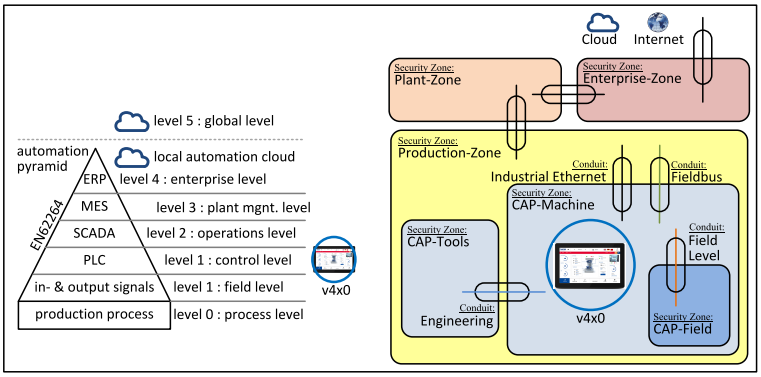
v4x0 web panel

Product description

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

Name of product	Product ID
v430 7in	V43AE70000000S
v430 10.1in	V43AEA0000000S
v430 15.6in	V43AEF0000000S
v450 7in	V45AP78000000S
v450 10.1in	V45APA8000000S
v450 15.6in	V45APF8000000S
v450 PoE-Injector	V4ZA0AP010000S

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 (📖 42)).



Location in the network

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.

Intended environment:

- 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 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

The following security functions are included in the listed components (except for the PoE-Injector):

Security mechanisms

- v4x0.Authentification
- v4x0.Certificate
- v4x0.Authorization

Security data

v4x0.Authentification : PasswortPolicy

Password-Policy for the user and admin password:

- 8 characters one lower and one upper case letter
- one numeric character
- one special character

Commissioning and hardening instructions

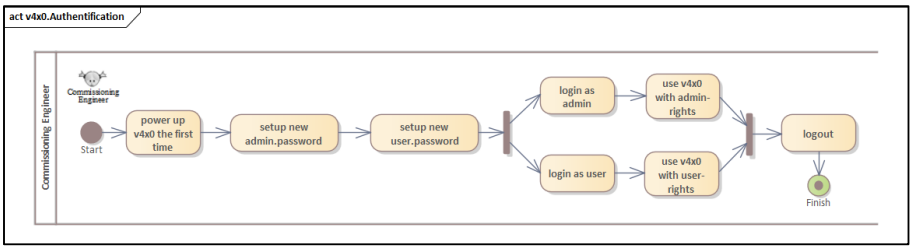
The following commissioning instructions must be followed.

- Set up the admin- and user-account (v4x0 Authentv4x0.Authentification (📖 191)).
- Create a certificate (v4x0.Certificate (📖 197)).
- Viewing the information about the authorization of the user and admin (v4x0.Authorization (📖 199)).

Security functions

v4x0 Authentv4x0.Authentification

The component v4x0 has a user management that allows users to authenticate themselves.



Activity Diagram

There are only the admin and the user account. This is delivered with

- admin-name = admin,
- admin-password = admin,
- user-name = user,
- user-password = user

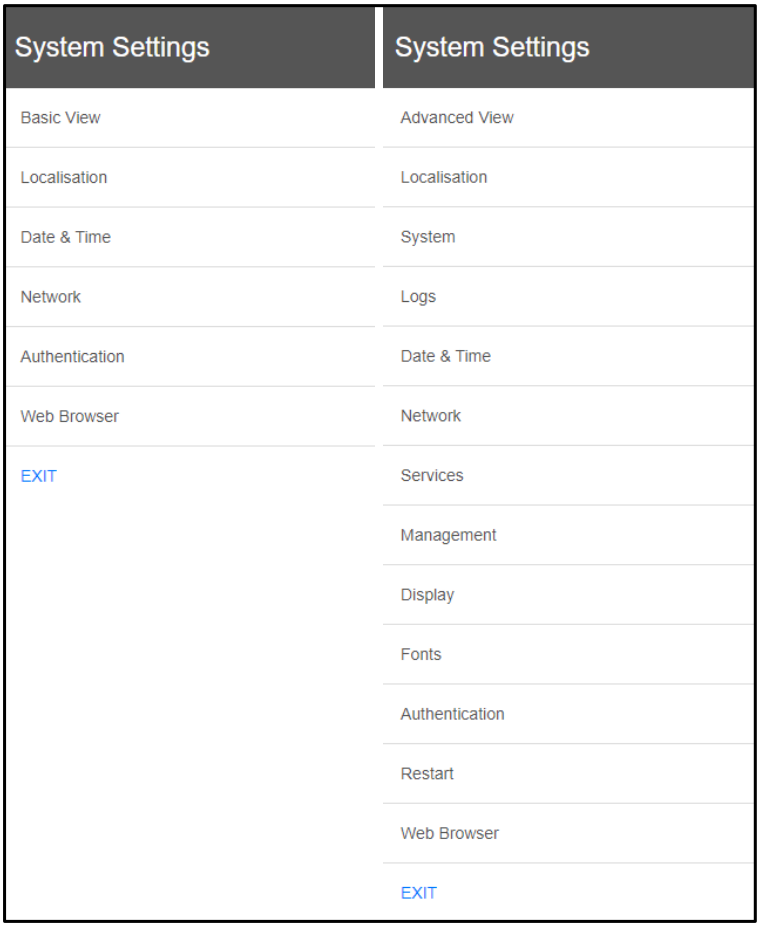
and must be changed when starting for the first time.

These accounts can be used on different ways.

Login to the Panel

These accounts are needed when directly login at the web-panel. There are two options:

- Tab-tab on the screen during startup
  Choose "System Settings"
  Enter Username and Password
- Long-hold on the left-upper corner for about 3 seconds
  Enter Username and Password

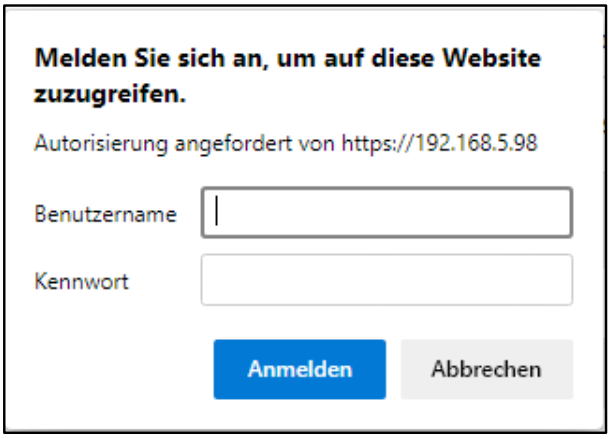


System Settings for user (Basic View) and admin (Advanced View)

Using a Web-Browser for Login

These accounts are also needed when connecting a device via webbrower to the web-panel:

- Open web browser
- Connect to IP-address of the web-panel
- Enter Username and Password

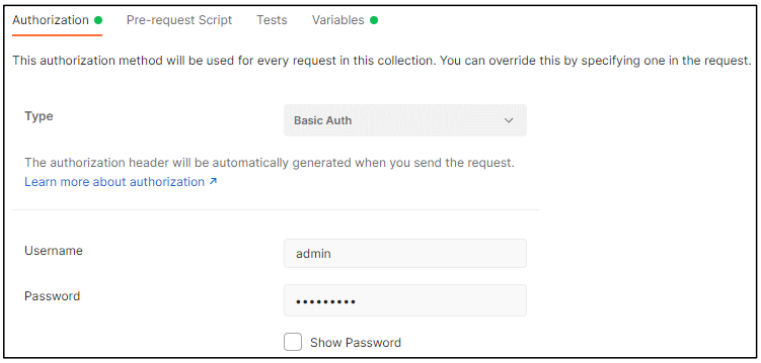


Authentification via Web-Brower

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"
- Type in the Username and Password
- Using url "https://<ip>/rest/api/v1"



authentification via postman

With a GET on the URL, all setting options are returned. A GET to the URL followed by a \< parameter> returns the value of the parameter.

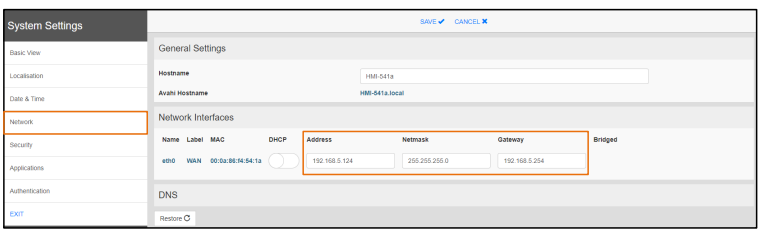
Reset authentification management

If the authentication features for the users "admin" or "user" have been lost, the components can be reset.

With this procedure, all settings (not only the authentication features) are lost.

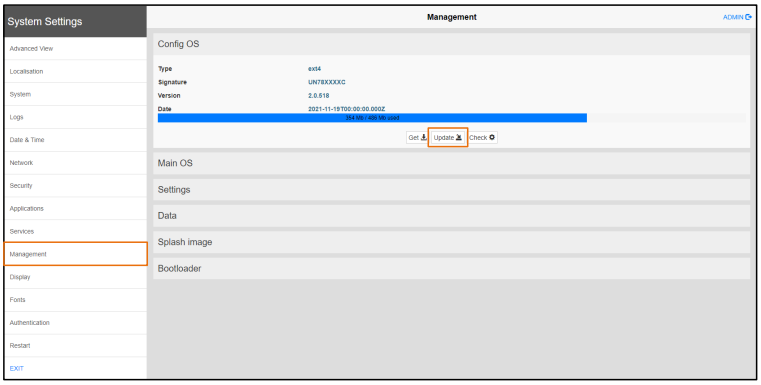
To reset the component follow the following instructions:

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 SETTINGS
3. choose "SYSTEM SETTINGS"
4. Another message will appear:
   - ENTERING SYSTEM SETTINGS
   - >> DEFAULT MODE
   - DEVICE RESTORE
5. choose "DEVICE RESTORE"
6. An information will appear:
   - Restoring device to defaults
     This operation could take few minutes, please wait
     ...
7. After some time the component will reboot automatically.
8. Now, the operator have to enter the credentials for the user.
9. After that, the operator have to enter the credentials for the administrator.
10. The component will reboot automatically with the network-settings:
    - IP Address: e.g. 192.168.10.126
    - Netmask: 255.255.255.0
    - Gateway: e.g. 192.168.10.120
    - DHCP: activated
11. A message will appear:
    - Empty boot sequence
12. On the display two button are located:
    - System Settings
    - Startup sequence
13. Start the System Settings and login with admin-user and admin-password
14. Change the IP Address in the System Settings Menu under the Network Tab:



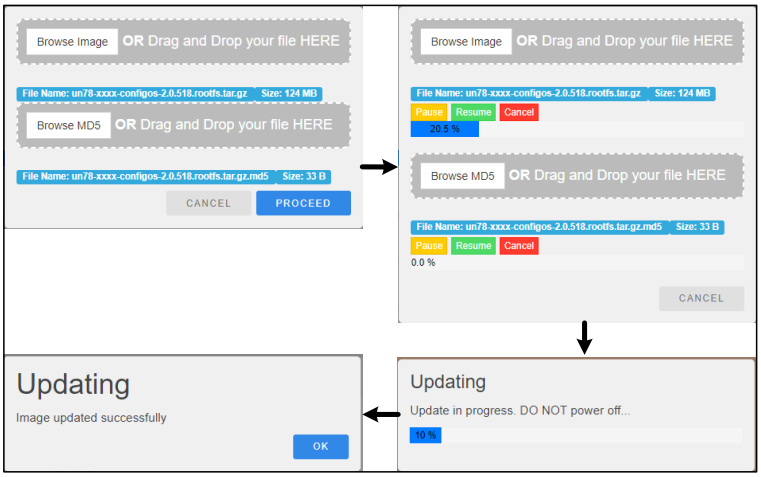
Change IP Address

15. Ask the Lenze Support for the needed files:
    - …configos….tar.gz
    - …configos….tar.gz.md5
    - …mainos….tar.gz
    - …mainos….tar.gz.md5
    - chromium….zip
16. There are two ways to transport these files to the v4x0 component:
    a) via USB-Stick to the USB-Cable
    b) via online Web-Browser
17. Update the "Config OS" via the System Settings and the Management Tab and choose Config OS and the Update Button:



Config OS

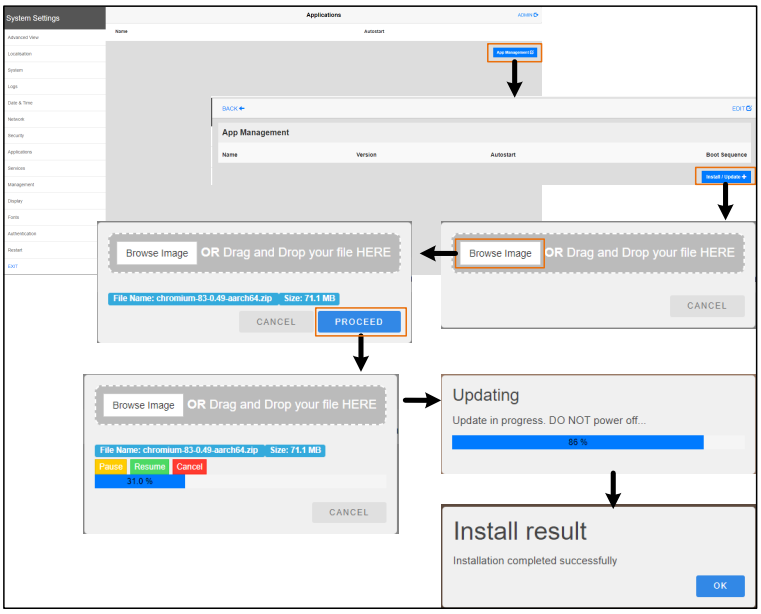
After that please choose the …configos….tar.gz and the …configos….tar.gz.md5 file, and proceed.



Config OS Status

18. Update the "Main OS" via the System Settings and the Management Tab and choose Main OS and the Update Button in similar way.

19. In the last step, the application Chromium must be loaded. For this purpose, the application must be added in the System Settings under the item Applications.

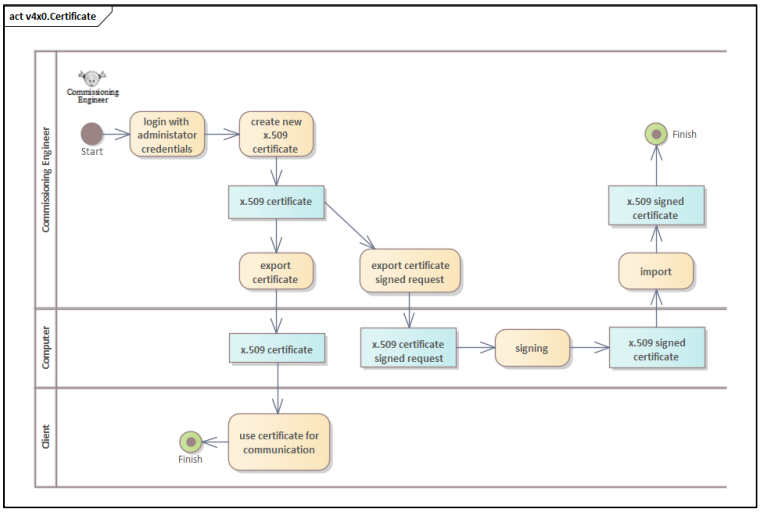


Applications

20. After a reboot, the System Settings contains an entry Web Browser. At this point, the homepage and the startup behavior can be entered.

v4x0.Certificate

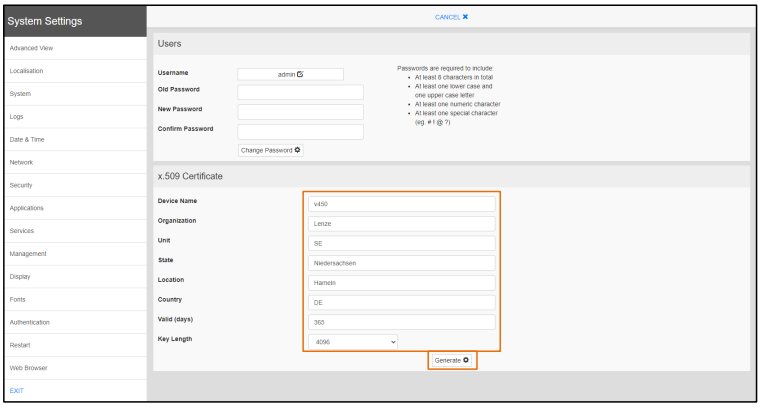
In order to use certificates, they must be created in advance on the component.



Activity Diagram

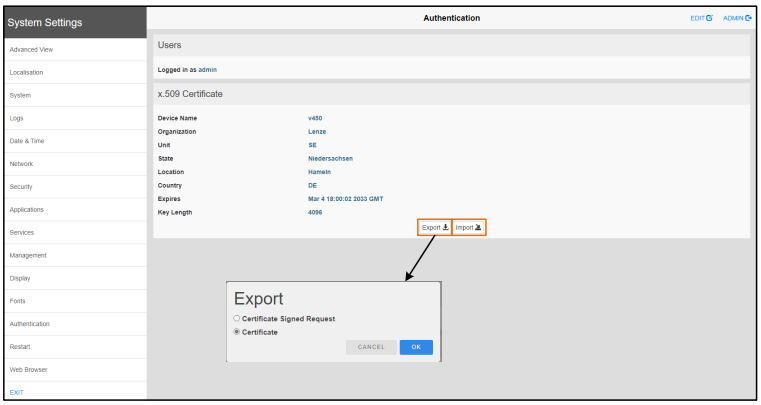
To do this, you must first create your own certificate on the component. This is done using the "System Settings" in the Authentication menu under the heading "x.509 Certificate". To create this you have to log in as admin.

At this point, the data for the certificate, the validity period in days and the key length can be defined. The certificate is then created with the Generate button.



System Settings

After generating the certificate and Export and an Import Button are available.

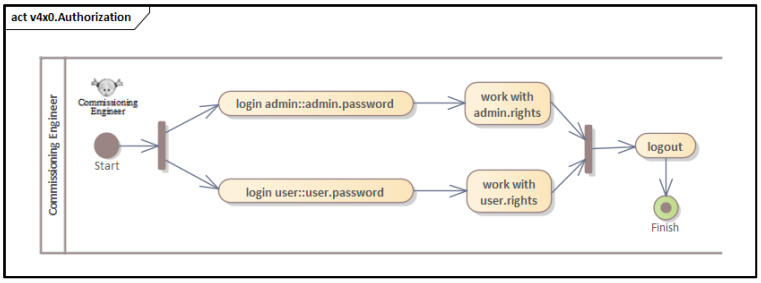


Export and Import of Certificates

At this point, there are two options. First, 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.Authorization

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

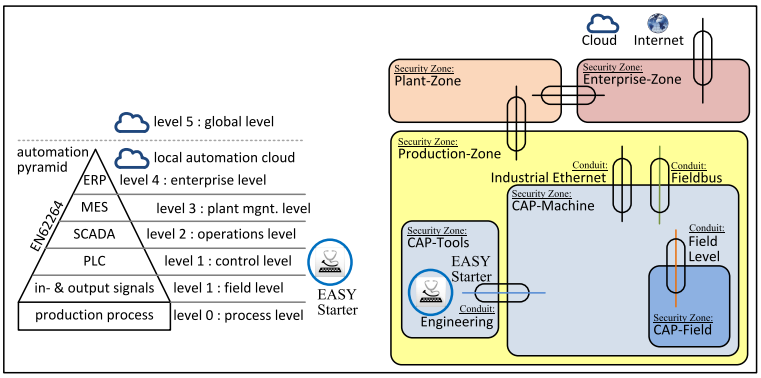
»EASY Starter«

Product description

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

Name of product	Product ID
»EASY Starter« (part of the »EASY Starter Suite«)	n.a.

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 (📖 42)).



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 environment:

- The 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.

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

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

Security data

EasyStarter.Certificate

If using an encrypted communication the »EASY Starter Suite« is storing the own certificate and the Controller Certificates for the Encrypted Communication in the Windows Certificate Store.

The own Certificate of the »EASY Starter Suite« is stored in the Windows Certificate Store in the directory "/Personal/Certificates" with the following information:

- Issuer and Subject
  CN = urn:<Device name>:Lenze:EASYStarter
  with <Device name> is the Device name of the Windows System.
- Valid from
  Today"s day minus 2 days. Therefore, so that the certificate is certainly valid in different time zones when maintenance or repair work is critical in terms of time.
- Valid to
  The Certificate is valid for 1 year.

The Controller Certificate will be stored also in the Windows Certificate Store in the directory "Controller Certificates/Certificates".

All these Certificates will not be deleted during deinstallation of the »EASY Starter Suite«. After deinstallation of the »EASY Starter Suite«, these data has to remove manually from the user. For more information, please have a look at Integrate a certificate in the windows certificate store (📖 40).

Security mechanisms

The following security functions are included in the listed components:

Security mechanisms

- EasyStarter.Authentification
- EasyStarter.Certificate

Commissioning, hardening and decommissioning notes

The following commissioning instructions must be followed:

Commissioning and hardening instructions

- If using the »EASY Starter« with a controller with activated user management, the human user authentication of the »EASY Starter« has to be use (EasyStarter.Authentification (📖 203)).
- If using the »EASY Starter« with a controller with forced encrypted communication the handling of the certificates are explained (EasyStarter.Certificate (📖 204)).

Decommissioning instructions

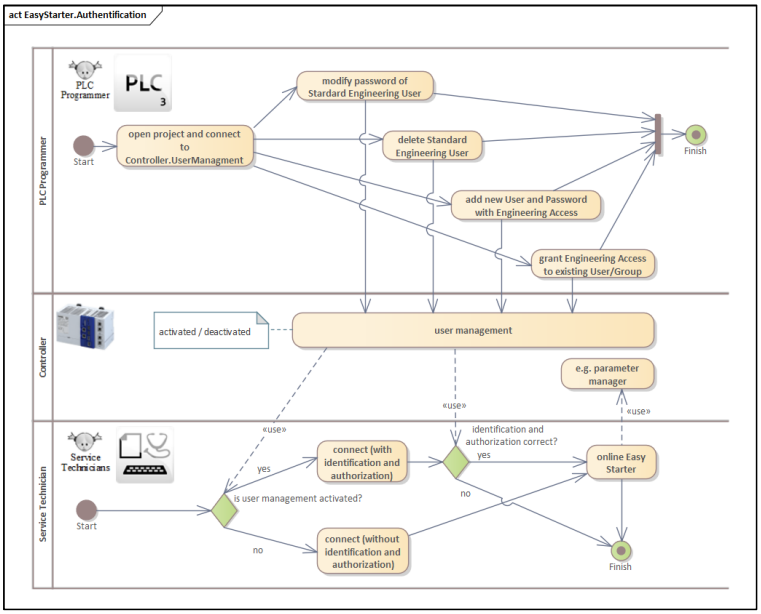
- After uninstallation the »EASY Starter Suite«, please remove the certificates manually from the Windows Certificate Store (EasyStarter.Certificate (📖 204)).

Security functions

EasyStarter.Authentification

This function is available sind version 01.24.00 of the EASY Starter.

This chapter describes the authentification from the »EASY Starter« while connecting the Controller. An overview is shown in the following figure.



EasyStarter.Authentification

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 is done when establishing a connection to the controller, but also when the controller establishes a connection to subordinate devices.

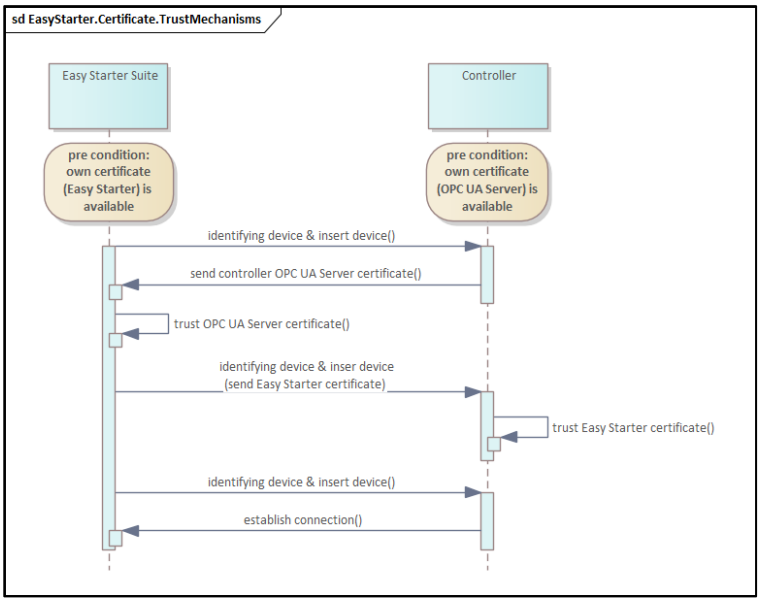
EasyStarter.Certificate

This function is available since version 01.25.00 of the »EASY Starter Suite«.

First we will describe when the »EASY Starter Suite« needs a certificate handling at all. This decision does not lie with the »EASY Starter Suite«, but 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 (Controller.UserManagement (📖 107))	The Certificate Handling is not dependent to the Controller.UserManagement activation.
EngineeringItf-User (Controller.UserManagement (📖 107))	The Certificate Handling is not dependent to the existence of the default Engineering User "EngineeringItf".
Anonymous Login (Controller.UserManagement (📖 107))	The Certificate Handling is not dependent to the existence of the activation of the Anonymous Login.
Encrypted Communication (Controller.EncryptedCommunication.PLCDesigner (📖 115))	The Certificate Handling is not dependent to the encrypted communication between »PLC Designer« and Controller.
User Enforced Encryption (Controller.EncryptedCommunication.PLCDesigner (📖 115))	The Certificate Handling is not dependent to the User "Enforced Encrypted Communication" in the Security Screen of »PLC Designer«.
Device Enforced Encryption (Controller.EncryptedCommunication.PLCDesigner (📖 115))	The Certificate Handling is only dependent to the Device "Enforced Encrypted Communication" in the Security Screen of »PLC Designer«. No encryption: The »EASY Starter Suite« will not handle certificates for communication. Optional encryption: The »EASY Starter Suite« will not handle certificates for communication. Enforced encryption: The »EASY Starter Suite« has to handle certificates for communication.

In the following, the procedure for mutual trussing is described using the example of a connection setup between the »EASY Starter« and the Controller.



Trust Mechanisms

Handling own certificates

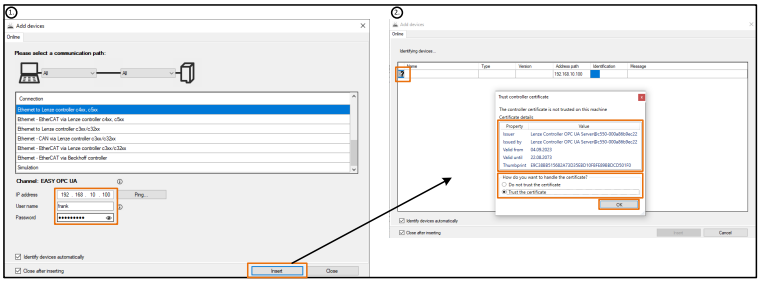
As a prerequisite, the »EASY Starter Suite« and the Controller must create their own Certificate.

- The »EASY Starter Suite« creates its own certificate automatically during first connection to the Controller. Fore more information see EasyStarter.Certificate (📖 201).
- The Controller creates its own certificate "Lenze OPC UA Server" automatically at the first boot. For more information see Controller.OPCUAServer.Certificate (📖 148).

For both, the user does not have to take any activity. This step does not require any interaction, but is only described to better understand the function.

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

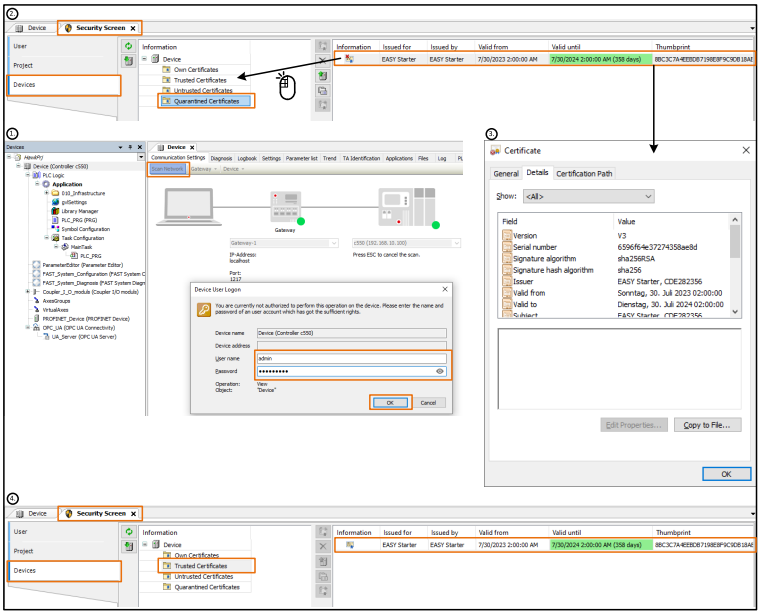
The Controller is displayed as a Device with its IP address and the connection setup is initialized. The Controller"s Certificate is sent to the »EASY Starter« and displayed in the window with some data for Identification.

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, the security screen must be opened and the "Devices" tab opened. 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 "Quarantied Certificates" to "Trusted Certificates" with a mouse drag and drop.

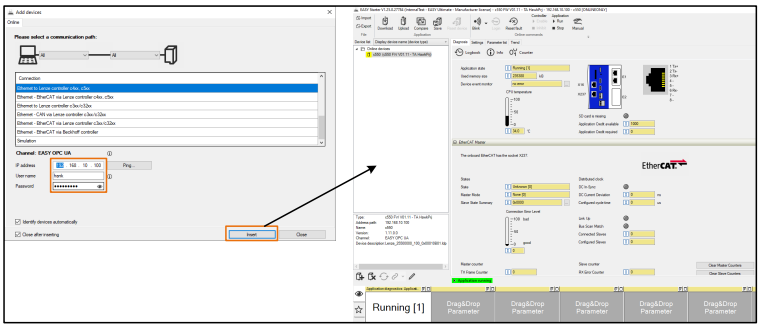
This completes the trust of the »EASY Starter« Certificate.

Trust »EASY Starter« Certificate in the Advanced Visualization (Production Use Case)

The connection of the »EASY Starter« in the Production is the same in the Production as in the 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 (📖 133)).

Establish Connection

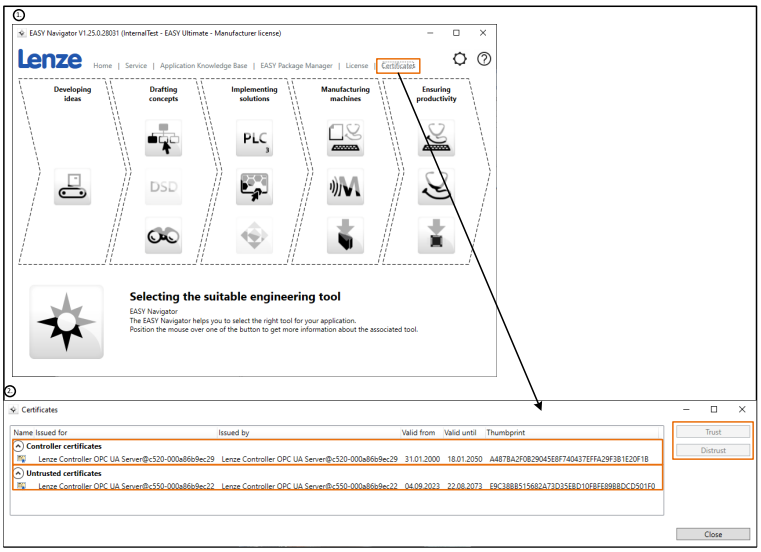
After trusting the Certificates on both sides, the User can insert the Controller in the »EASY Starter« and can go online.



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:

- If selecting an untrusted Certificate, the User can trust this Certificate.
- If selecting an trusted Certificate, the User can untrust this Certificate.

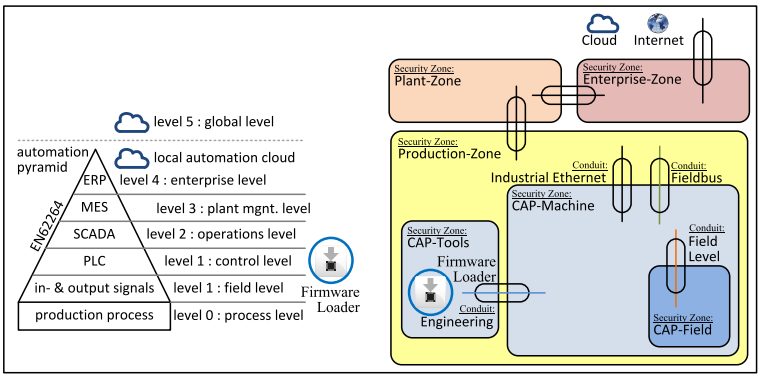
»EASY Firmware Loader«

Product description

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

Name of product	Product ID
»EASY Firmware Loader« (part of the »EASY Starter Suite«)	n.a.

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 (📖 42)).



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 environment:

- The 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.

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(FirmwareLoader)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

Security data

Security mechanisms

The following security functions are included in the listed components:

Security mechanisms

- FirmwareLoader.Authentification
- FirmwareLoader.Certificate

Commissioning and hardening instructions

The following commissioning instructions must be followed.

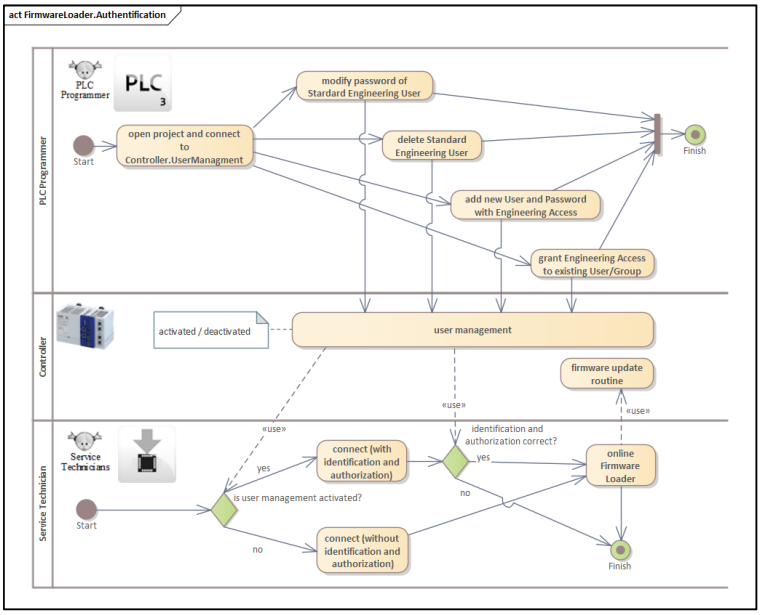
- If using the »EASY Firmware Loader« with a controller with activated user management, the human user authentication of the »EASY Firmware Loader« has to be use (FirmwareLoader.Authentification (📖 211)).
- If using the »EASY Firmware Loader« with a controller with forced encrypted communication the handling of the certificates are explained (FirmwareLoader.Certificate (📖 212)).

Security functions

FirmwareLoader.Authentification

This function is available since »EASY Firmware Loader« version 01.24.00.

This chapter describes the authentification 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 Fimware 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 is done when establishing a connection to the Controller, but also when the Controller establishes a connection to subordinate devices.

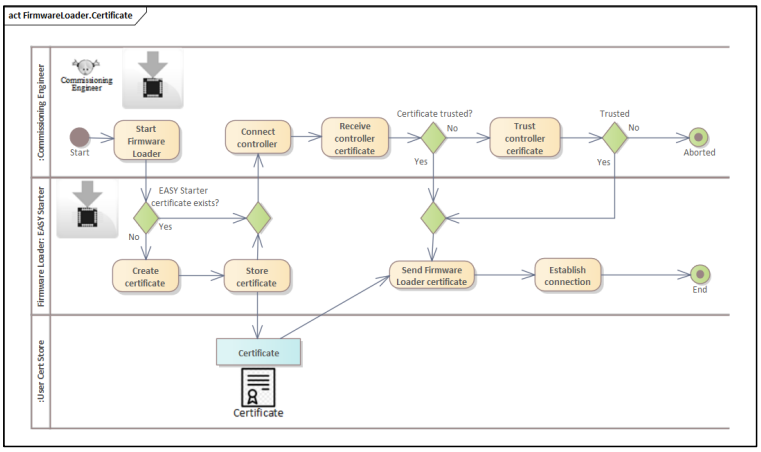
Using the firmware-loader in batchmode

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 is 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 (📖 204)).



Activity Diagram

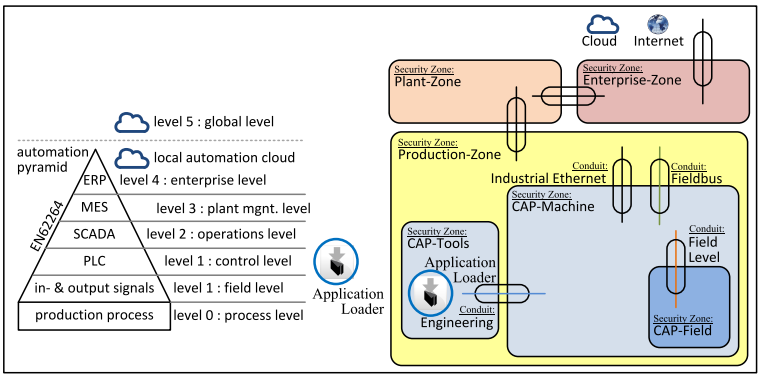
»EASY Application Loader«

Product description

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

Name of product	Product ID
»EASY Application Loader« (part of the »EASY Starter Suite«)	n.a.

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 (📖 42)).



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 environment:

- The 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.

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 data

Security mechanisms

The following security functions are included in the listed components.

Security mechanisms

- ApplicationLoader.Authentification
- ApplicationLoader.Certificate

Commissioning and hardening instructions

The following commissioning instructions must be followed.

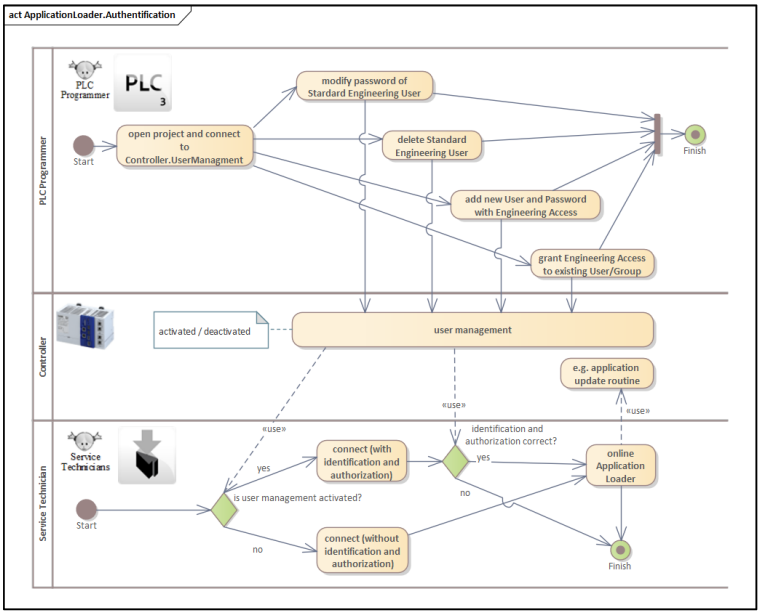
- If using the »EASY Application Loader« with a controller with activated user management, the human user authentication of the »EASY Application Loader« has to be use (ApplicationLoader.Authentification (📖 215)).
- If using the »EASY Application Loader« with a controller with forced encrypted communication the handling of the certificates are explained (ApplicationLoader.Certificate (📖 217)).
- If 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, there is increased attention to the procedure of these files and the confidentiality must be ensured organizationally by the user.
  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>
  - ApplicationFileSet=”C:\file.lfl”

Security functions

ApplicationLoader.Authentification

This function is available since »EASY Application Loader« version 01.24.00.

This chapter describes the authentification 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 Firmware Loader. This is done via username and password. This is done when establishing a connection to the controller, but also when the controller establishes a connection to subordinate devices.

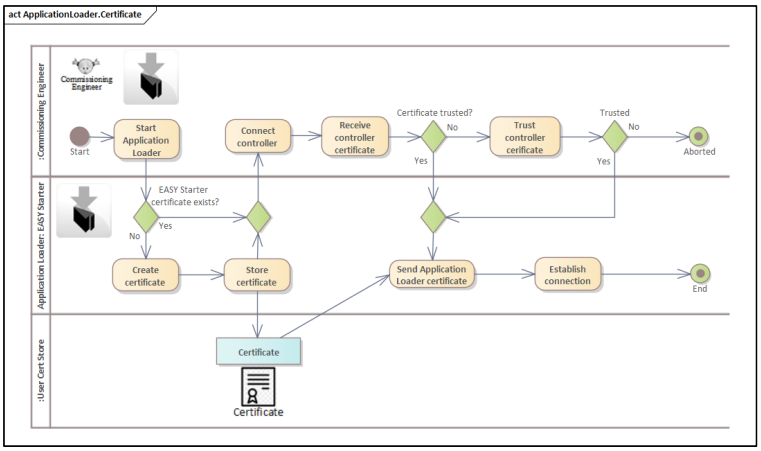
An application can be created with the help of the »PLC Designer«. For this purpose, the entry "EASY Export..." is displayed in the menu under "Project". and created a "Complete device application *.lda". It is important to know that the Controller.UserManagement is not part of dla. file. This has security-related 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 is 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 (📖 204)).



Activity Diagram

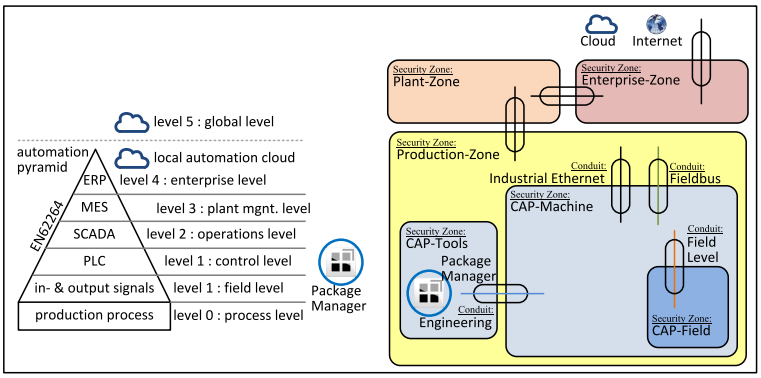
»EASY Package Manager«

Product description

This documentation is applicable to the following component with its identification:

Name of product	Product ID
»EASY Package Manager« (part of the »EASY Starter Suite«)	n.a.

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 (📖 42)).



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 environment:

- The 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.

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(PackageManager)={ IAC=0; UC=0; SI=0; DC=0; RDF=0; TRE=0; RA=0 }.

Security data

PackageManager.FirmwarePackage.Integrity: Hash Function

The method for calculating integrity is:

- SHA512

PackageManager.Tools.Integrity: Hash Function

The method for calculating integrity is:

- SHA512

Security mechanisms

The following security functions are included in the listed software:

Security mechanisms

- 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.

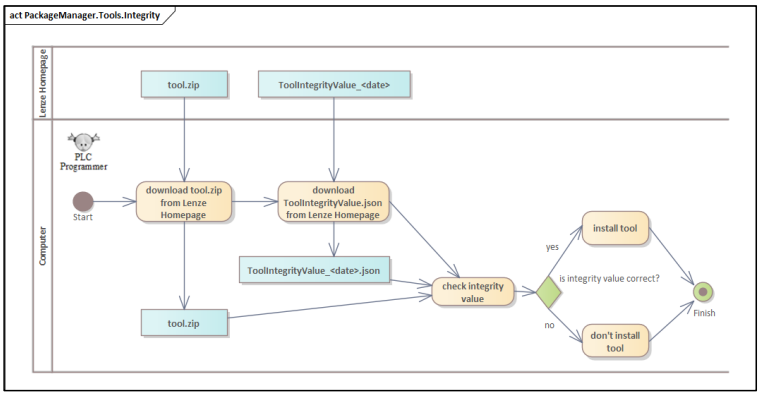
Commissioning and hardening instructions

- Before installing a tool, the hash value should be checked (PackageManager.Tool.Integrity (📖 220)).
- Before individual firmware packages are installed, they must be checked for integrity (PackageManager.Package.Integrity (📖 221)).

Security functions

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 exactly this version of this tool. This option is ideal for those who want to install a tool individually.
- Secondly, there is an integrity file of all tools in all versions released so far. This can be found under:
  https://www.lenze.com/de-de/service-und-support/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 automatisms. These people do not have to download various integrity files, but the latest version of the sum file is sufficient.

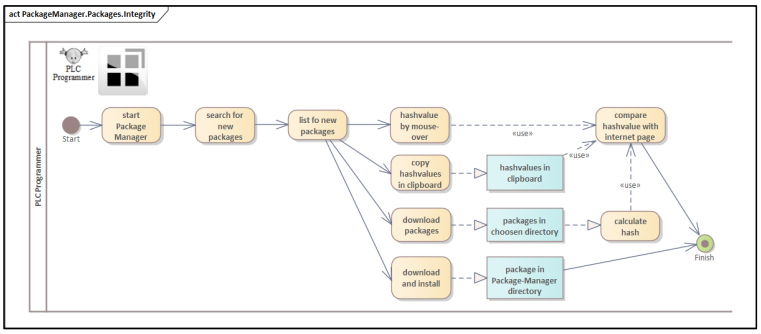
Regardless of whether the single file or the sum file was downloaded, there is a zip file. If this zip file is unpacked, there are three files as a result. This is a *.csv, a *.json, and a *.xml. All three files contain the same content, that is, the same integrity values, and only reflect different formats.

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 is 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/de-de/service-und-support/cyber-security

Hash value by mouse-over

On the list of packages, the hash value can be displayed with a mouse-over. This can be manually compared with the published hash values.

Copy hashvalues to clipboard

Via the button "Copy hashvalues to clipboard" the hash values of the selected packages can be transferred to the clipboard. These can then be manually compared with the published hash values.

Download packages

With this function, the selected packets are written to a directory to be selected. An installation does not yet take place. These loaded packages can be manually subjected to an integrity check by calculating the hash value and menu. This function installs the packages directly and comparing it with the published hash values.

Download in install

This function installs the packages directly.