Manual

Security Options for MOVI-C® CONTROLLER

Firmware V08.01 or Later (MOVISUITE® V2.40)

Edition 04/2024

31558119/EN

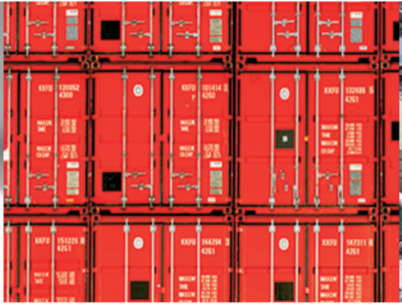


Table of Contents

1 General information

1.1 About this documentation

This documentation is an integral part of the product. The documentation is intended for all employees who perform work on the product.

Make sure that this documentation is accessible and legible. Ensure that persons responsible for the systems and their operation as well as persons who work with the product independently have read through the documentation carefully and understood it. If you are unclear about any of the information in this documentation, or if you require further information, contact SEW-EURODRIVE.

1.2 Content of the documentation

The descriptions in this documentation refer to the software and firmware versions at the time of publication. These descriptions might differ if you install later software or firmware versions. In this case, contact SEW-EURODRIVE.

The latest edition of the documentation is also always available in Online Support on the website of SEW-EURODRIVE.

1.3 Applicable documentation

For all other components, refer to the corresponding documentation.

Always use the latest edition of the documentation and the software.

The SEW-EURODRIVE website (www.sew-eurodrive.com) provides a wide selection of documents for download in various languages. If required, you can also order printed and bound copies of the documentation from SEW-EURODRIVE.

1.4 Structure of the safety notes

1.4.1 Meaning of signal words

The following table shows the graduation and meaning of the signal words in the safety notes.

Signal word	Meaning	Consequences if not observed
⚠ DANGER	Imminent danger	Death or severe injuries
⚠ WARNING	Possibly dangerous situation	Death or severe injuries
⚠ CAUTION	Possibly dangerous situation	Minor injuries
NOTICE	Possible damage to property	Damage to the product or its environment
INFORMATION	Useful information or tip: Simplifies handling of the product.	

1.4.2 Structure of section-related safety notes

Section-related safety notes do not apply to a specific action but to several actions pertaining to one subject. The hazard symbols used either indicate a general hazard or a specific hazard.

This is the formal structure of a safety note for a specific section:

SIGNAL WORD

Type and source of hazard.

Possible consequence(s) if disregarded.

- Measure(s) to prevent the hazard.

1.4.3 Structure of embedded safety notes

Embedded safety notes are directly integrated into the instructions just before the description of the dangerous step.

This is the formal structure of an embedded safety note:

⚠ **SIGNAL WORD!** Type and source of danger. Possible consequence(s) if disregarded. Measure(s) to prevent danger.

1.5 Decimal separator in numerical values

In this document, a period is used to indicate the decimal separator.

Example: 30.5 kg

1.6 Rights to claim under limited warranty

Read the information in this documentation. This is essential for fault-free operation and fulfillment of any rights to claim under limited warranty. Read the documentation before you start working with the product.

1.7 Product names and trademarks

The product names mentioned in this documentation are trademarks or registered trademarks of the respective titleholders.

1.8 Copyright notice

2 Safety notes

2.1 Preliminary information

The following general safety notes serve the purpose of preventing injury to persons and damage to property. They primarily apply to the use of products described in this documentation. If you use additional components, also observe the relevant warning and safety notes.

2.2 Target group

Specialist for working with software

Any work with the software may only be performed by a specialist with suitable training. A specialist in the context of this documentation is someone who has the following qualifications:

- Appropriate instruction
- Knowledge of this documentation and other applicable documentation
- SEW-EURODRIVE recommends additional training for products that are operated using this software.

2.3 IT security

If you need support with the configuration, contact SEW-EURODRIVE Service. You can obtain information about current security-related issues by e-mail or on the Product Security Management website. There you will find various contact options for reporting security-related problems.

For detailed information on the IT security of the products used, refer to the respective documentation.

3 Overview

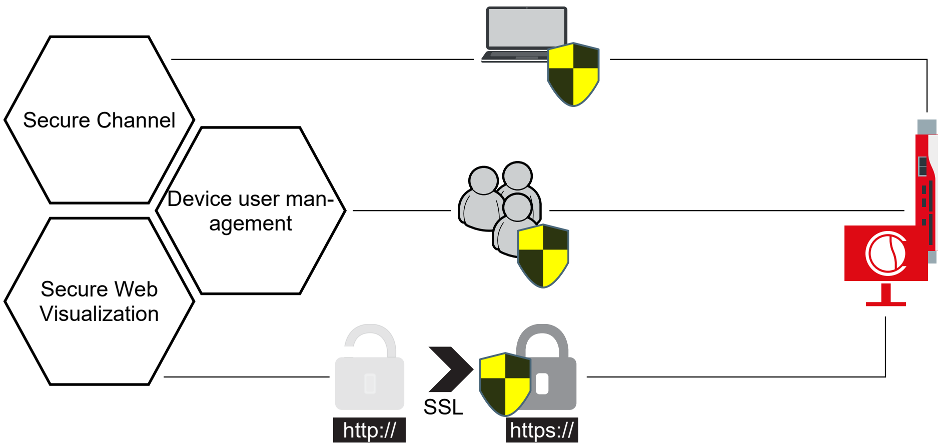
3.1 Prerequisites

The following prerequisites must be met for the security screen to be available and full access to the security functions to be possible:

- MOVI-C CONTROLLER® with firmware V08.01 or later
- MOVISUITE® V2.40 or later
- Access to the `root/APP` directory of the MOVI-C® CONTROLLER, for example via the "Files" tab of the IEC Editor.
- To ensure the validity of certificates, the time and date of the MOVI-C® CONTROLLER must be current and synchronous. To this end, click the [Apply PC system time] button in the "Date and time" parameter group in the configuration of the MOVI-C® CONTROLLER.

3.2 Available security options

The following graphic provides an overview of the available security options:



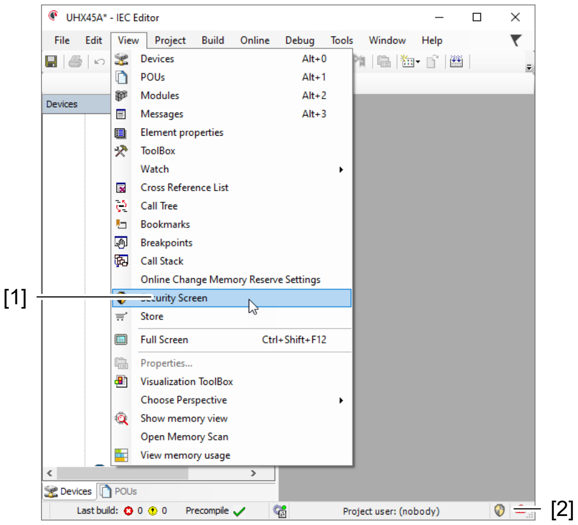
18014447434028555

For further information, refer to the following chapters:

- "Secure Channel" (→ 🗎 10)
- "Device user management" (→ 🗎 12)
- "Secure Web Visualization" (→ 🗎 16)

3.3 Opening the security screen

To open the security screen, select the menu command "View" > "Security Screen" [1] or double click the icon [2] in the status bar of the IEC Editor.



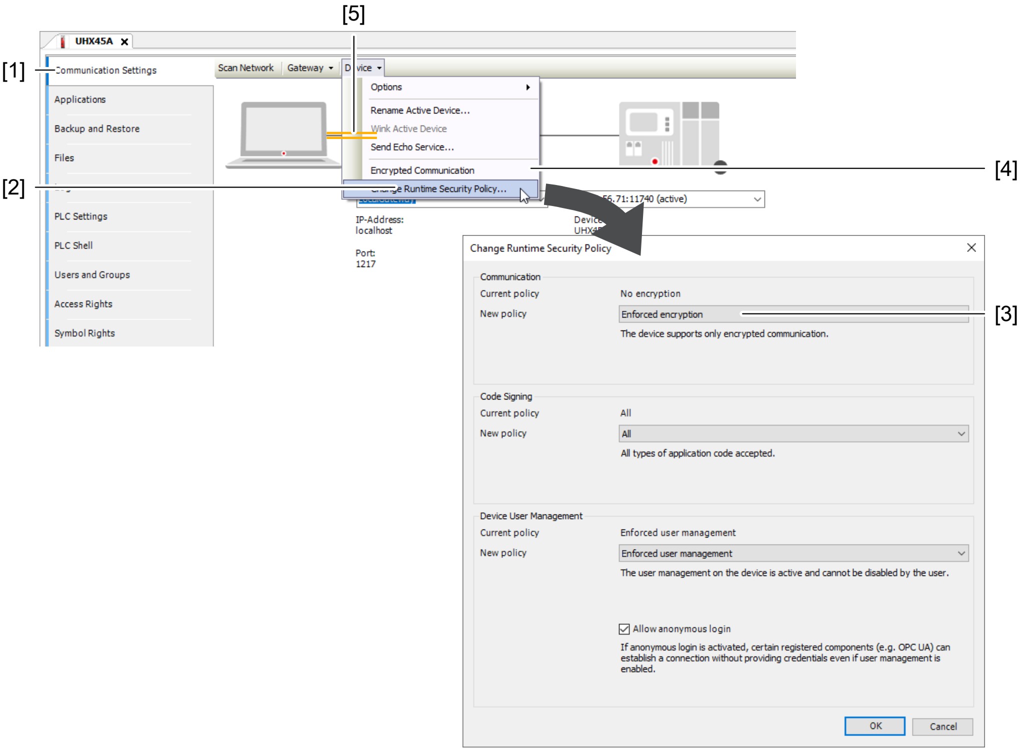
49227683083

4 Secure Channel

The Secure Channel allows certificate-based encrypted communication. For this purpose, you can either import an external certificate or have a self-signed certificate generated by the MOVI-C® CONTROLLER. For further information, refer to chapter "Certificates" (→ 🗎 18).

INFORMATION

If there is no certificate available on the MOVI-C® CONTROLLER for communication with a component, it generates a self-signed certificate with default values and uses this for encrypted communication.



Change Runtime Security Policy

Communication
Current policy: No encryption
New policy: Enforced encryption
The device supports only encrypted communication.

Code Signing
Current policy: All
New policy: All
All types of application code accepted.

Device User Management
Current policy: Enforced user management
New policy: Enforced user management
The user management on the device is active and cannot be disabled by the user.

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

18014447442763531

To activate the encrypted communication, proceed as follows:

✓ The IEC Editor is open.

✓ The connection to the MOVI-C® CONTROLLER is established.

✓ The device tree is open.

1. Double click the MOVI-C® CONTROLLER in the device tree.
2. On the "Communication Settings" tab [1], select the menu item [Device] > [Change Runtime Security Policy…] [2].

   ⇨ The "Change Runtime Security Policy" window is displayed.
3. In the "Communication" group, select [Enforced encryption] [3] from the "New policy" choice box.
4. Click [OK].

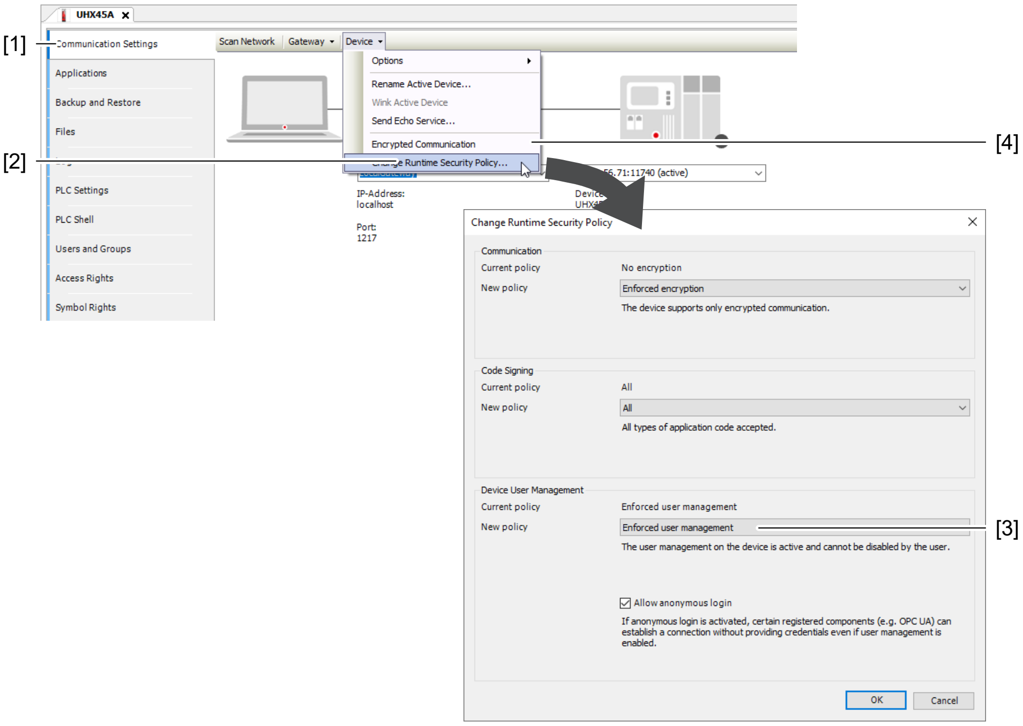
   ⇨ The MOVI-C® CONTROLLER now only supports encrypted communication.

5. On the "Communication Settings" tab [1], select the menu item [Device] > [Encrypted Communication] [4].

⇨ Encrypted communication is shown with a yellow connection line [5].

5 Device user management

5.1 Setting up device user management



Change Runtime Security Policy

Communication
Current policy: No encryption
New policy: Enforced encryption
The device supports only encrypted communication.

Code Signing
Current policy: All
New policy: All
All types of application code accepted.

Device User Management
Current policy: Enforced user management
New policy: Enforced user management
The user management on the device is active and cannot be disabled by the user.

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

49230031755

To set up the device user management of the MOVI-C® CONTROLLER, proceed as follows:

✓ The IEC Editor is open.

✓ The connection to the MOVI-C® CONTROLLER is established.

1. Double click the MOVI-C® CONTROLLER in the device tree.
2. On the "Communication Settings" tab [1], select the menu item "Device" > "Change Runtime Security Policy…" [2].
3. The "Change Runtime Security Policy" window is displayed.
4. In the "Device User Management" group, select "Enforced user management" [3] from the "New policy" choice box.
5. Click [OK].

   ⇨ The MOVI-C® CONTROLLER now requires a user login when establishing a connection.
6. Connect to the device.

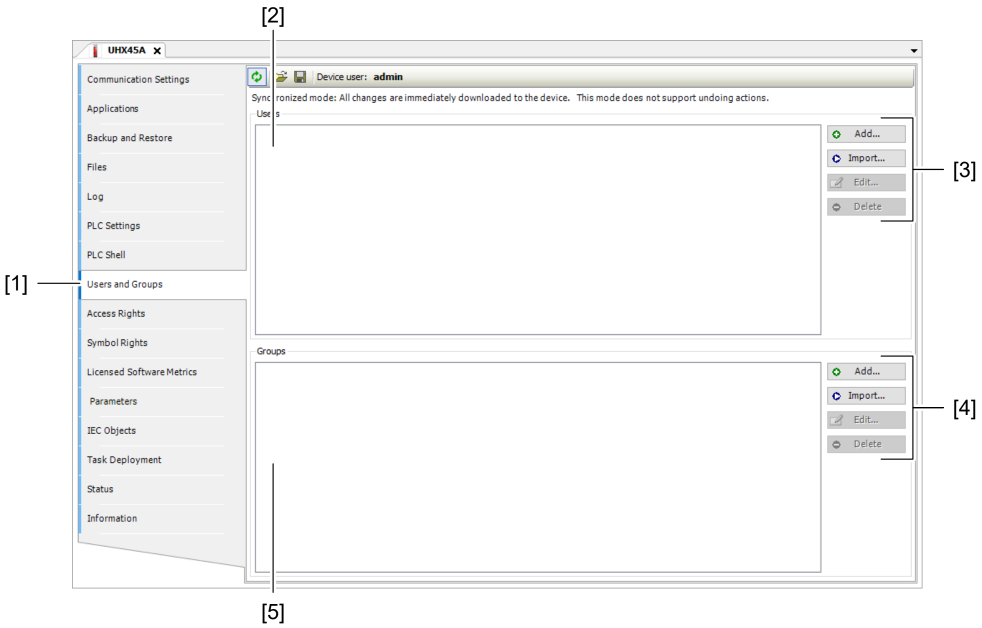
   ⇨ The "Activate device user management" prompt is displayed.
7. Confirm the prompt asking whether you want to activate device user management on the device.

   ⇨ When setting up for the first time, you will be asked to create an administrator user: The "Add device user" window is displayed.
8. Create the administrator user.

⇨ Device user management is active and an administrator user is set up.

5.2 Managing users and groups

To edit users and groups, you must have the appropriate authorizations. To perform editing, use the corresponding buttons on the "Users and Groups" tab. Users can only be assigned to existing groups.



Synchronized mode: All changes are immediately downloaded to the device. This mode does not support undoing actions.

48596892043

[1] "Users and Groups" tab
[2] List of users
[3] Buttons for editing users
[4] Buttons for editing groups
[5] List of groups

5.3 Resetting the password

To reset a user's password, proceed as follows:

✓ You have the appropriate authorizations.

1. Double click the user whose password you want to reset.

   ⇨ The "Edit user …" window opens.

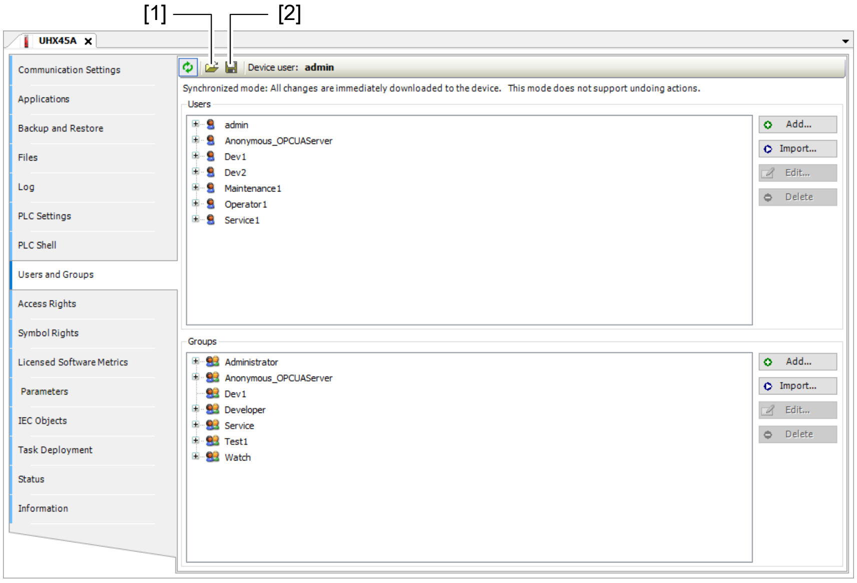
2. Enter a new password in the "Password" and "Confirm password" edit boxes.
3. Click [OK].

5.4 Deactivating users

To deactivate a user, you must have the appropriate authorizations. Remove the user from all available groups. Without an assigned group, a user does not fulfill a role and loses all associated access rights.

5.5 Transferring user management

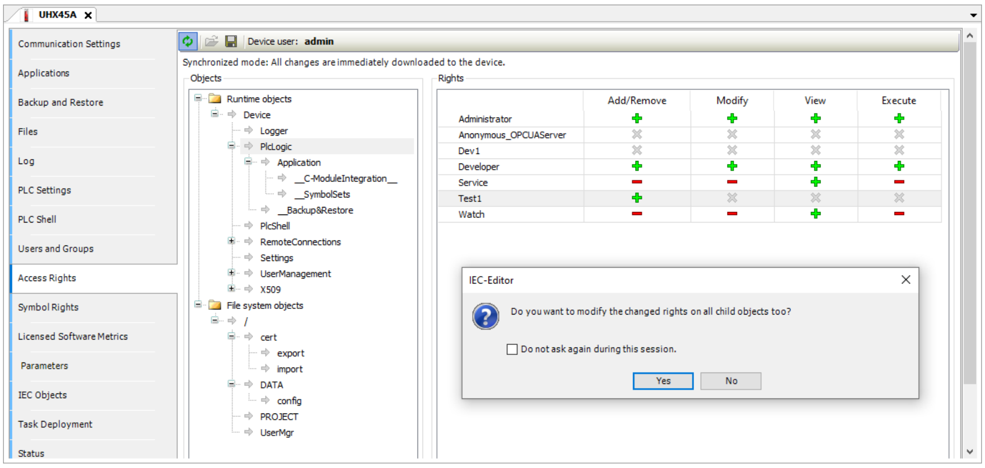
User management is transferred using a `.dum2` file. This allows users and groups to be backed up, restored and transferred to other MOVI-C® CONTROLLERs. Use the corresponding buttons for import [1] and export [2] and optionally assign a password for the file.



Synchronized mode: All changes are immediately downloaded to the device. This mode does not support undoing actions.

49230292747

5.6 Access rights



Synchronized mode: All changes are immediately downloaded to the device.

	Add/Remove	Modify	View	Execute
Administrator	✚	✚	✚	✚
Anonymous_OPCUAServer	✕	✕	✕	✕
Dev1	✕	✕	✕	✕
Developer	✚	✚	✚	✚
Service	−	−	✚	−
Test1	✚	✕	✕	✕
Watch	−	−	✚	−

Do you want to modify the changed rights on all child objects too?

☐ Do not ask again during this session.

9007248620625163

To change the access rights to an object, proceed as follows:

✓ You have the appropriate authorizations.

1. Click the object for which you want to change the access rights.
2. Double click the access right.

   ⇨ A query is displayed asking whether the new rights should be inherited.
3. Click the corresponding button.

⇨ The access right has been changed.

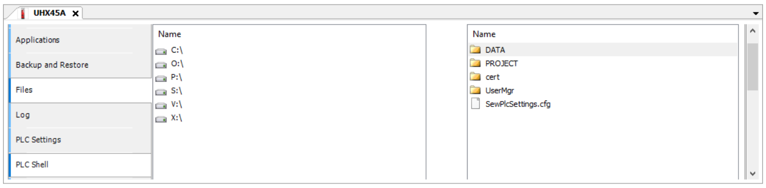
Possible access rights

Symbol	Meaning
✚	Access right explicitly granted
━	Access right explicitly denied
✛	Access right neutral, granted through inheritance
▭	Access right neutral, denied through inheritance
✖	The access right was not explicitly set or denied, not even in the parent object. Access is not possible.
None	Several objects are selected that do not have uniform access rights.

6 Secure Web Visualization

SEW-EURODRIVE recommends encrypting communication with the browser-based web visualization tool. Depending on the options set, parallel operation of encrypted and unencrypted communication is possible.

Setup is performed using the configuration file `SewPlcSettings.cfg` in the directory `root/APP/` of the MOVI-C® CONTROLLER. Create it with a text editor during the initial startup phase and save it in the directory. Use the "Files" tab of the MOVI-C® CONTROLLER for this purpose:



49289758347

6.1 Keys and values

`SECURITY.CommunicationMode`	
Meaning	**Possible values**
Use this key to specify the connection type between the browser and web visualization tool.	• HTTPS • REDIRECT_HTTP_TO_HTTPS • HTTP, HTTPS • HTTP

`SECURITY.CreateSelfSignedCert`	
Meaning	**Possible values**
Use this key to specify whether the MOVI-C® CONTROLLER generates a self-signed certificate if one is not stored.	• Yes • No

`WebServerSecurePortNr`
Meaning
Use this key to specify the port via which the browser and web visualization tool communicate.

6.2 Example of a configuration file

```
[CmpWebServer]
SECURITY.CommunicationMode=REDIRECT_HTTP_TO_HTTPS
SECURITY.CreateSelfSignedCert=YES
WebServerSecurePortNr=8443
```

This redirects the URL `http://<eigene_ip>:8080/webvisu.htm` to `https://<eigene_ip>:8443/webvisu.htm`.

6.3 Warning of an invalid certificate

When calling up the web visualization tool in the browser, a warning may be displayed indicating that the certificate used is invalid. The following cases are possible:

- Self-signed certificates

  A warning may appear when calling up the web visualization tool. In this case, an exception rule can be stored in the browser to prevent further warnings from being displayed.

- Certificates from a certification authority

  To avoid receiving warnings, install the root certificate of the certification authority on the device that is used to call up the web visualization tool.

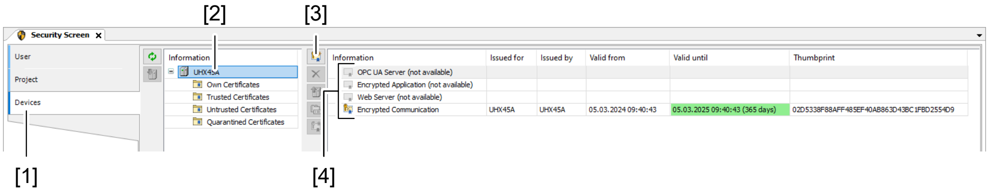
7 Certificates

7.1 Self-signed certificates

7.1.1 Generating a certificate

You can generate self-signed certificates directly on the MOVI-C® CONTROLLER for the following components:

- OPC UA server
- Web server
- Encrypted communication



Information	Issued for	Issued by	Valid from	Valid until	Thumbprint
OPC UA Server (not available)					
Encrypted Application (not available)					
Web Server (not available)					
Encrypted Communication	UHX45A	UHX45A	05.03.2024 09:40:43	05.03.2025 09:40:43 (365 days)	02D5338F88AFF485EF40AB863D43BC1FBD2554D9

49184615947

Proceed as follows:

✓ The IEC Editor is open.

✓ The connection to the MOVI-C® CONTROLLER is established.

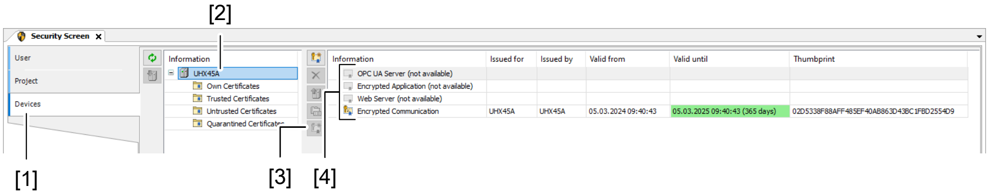
✓ The security screen is open.

1. Open the "Devices" tab [1].
2. Click the MOVI-C® CONTROLLER [2].
3. Click the component [4] for which you want to create a certificate.
4. Click the [Generate new certificate on the device] button [3].

   ⇨ The "Certificate settings" window opens.
5. Select the key length from the "Key length (bit)" drop-down list.
6. Enter the validity period of the certificate in the "Validity period (days)" edit box.
7. Click [OK].

⇨ The certificate is generated.

7.1.2 Renewing a certificate



Information	Issued for	Issued by	Valid from	Valid until	Thumbprint
OPC UA Server (not available)					
Encrypted Application (not available)					
Web Server (not available)					
Encrypted Communication	UHX45A	UHX45A	05.03.2024 09:40:43	05.03.2025 09:40:43 (365 days)	02D5338F88AFF485EF40AB863D43BC1FBD2554D9

49725424395

To renew a certificate, proceed as follows:

✓ The IEC Editor is open.

✓ The connection to the MOVI-C® CONTROLLER is established.

✓ The security screen is open.

1. Open the "Devices" tab [1].

2. Click the MOVI-C® CONTROLLER [2].
3. Click the component [4] whose certificate you want to renew.
4. Click the [Renew the selected certificate] button [3].
   ⇨ The "Certificate settings" window opens.
5. Select the key length from the "Key length (bit)" drop-down list.
6. Enter the validity period of the certificate in the "Validity period (days)" edit box.
7. Click [OK].

⇨ The certificate is generated.

7.2 Certificates from a certification authority

7.2.1 Creating CSR files

For all components

To create the CSR files for all components, proceed as follows:

✓ The IEC Editor is open.

✓ The connection to the MOVI-C® CONTROLLER is established.

1. In the IEC Editor, open the "PLC shell" tab.
2. Enter the command `cert-createcsr` in the command line.
3. Press the enter key.
   ⇨ The CSR files for all components are created and stored in the file system of the MOVI-C® CONTROLLER in the directory `root/APP/cert/export`.
4. To copy the CSR files from the MOVI-C® CONTROLLER to the engineering PC, use the "Files" tab.

For one component

To create the CSR file for a specific component, proceed as follows:

✓ The IEC Editor is open.

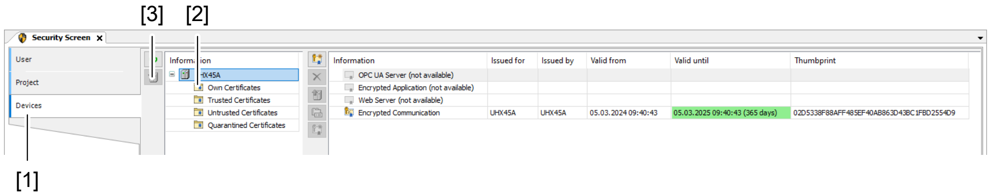
✓ The connection to the MOVI-C® CONTROLLER is established.

1. In the IEC Editor, open the "PLC shell" tab.
2. Enter the command `cert-getapplist` in the command line.
3. Press the enter key.
   ⇨ The available components are listed.
4. Enter the command `cert-createcsr` followed by the component number in the command line.
5. Press the enter key.
   ⇨ The CSR file for the selected component is created and stored in the file system of the MOVI-C® CONTROLLER in the directory `root/APP/cert/export`.
6. To copy the CSR file from the MOVI-C® CONTROLLER to the engineering PC, use the "Files" tab.

7.2.2 Using a certificate

INFORMATION

Delete existing certificates for a component before using a new certificate.



Information	Issued for	Issued by	Valid from	Valid until	Thumbprint
OPC UA Server (not available)					
Encrypted Application (not available)					
Web Server (not available)					
Encrypted Communication	UHX45A	UHX45A	05.03.2024 09:40:43	05.03.2025 09:40:43 (365 days)	02D5338F88AFF485EF40AB863D43BC1FBD2554D9

49219074059

To use a certificate from a certification authority, proceed as follows:

✓ You have a digital certificate from a certification authority for a component of the MOVI-C® CONTROLLER on the engineering PC.

✓ The IEC Editor is open.

✓ The connection to the MOVI-C® CONTROLLER is established.

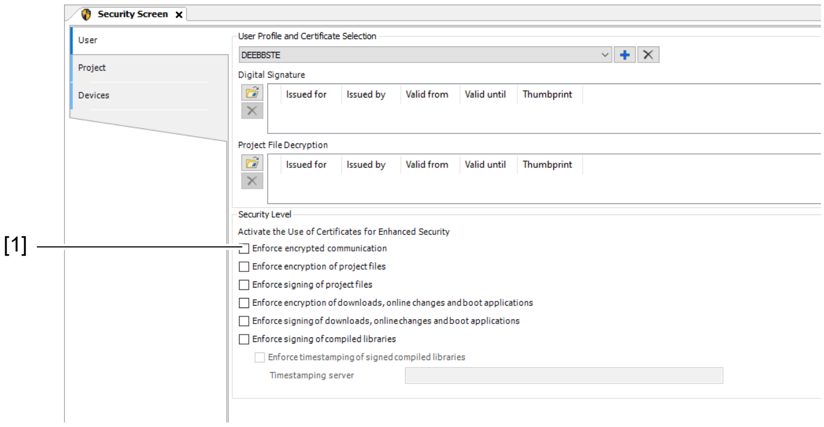
1. Open the "Devices" tab [1].
2. Click the "Own Certificates" certificate store [2].
3. Click the [Download] button [3].
4. Select the digital certificate on your engineering PC.
5. Click the [Open] button.

   ⇨ The imported certificate for the associated component is displayed in the list.
6. Restart the MOVI-C® CONTROLLER.

8 Additional information

8.1 Enforcing encrypted communication in the IEC project

The "Enforce encrypted communication" option applies to the entire IEC project. Communication is then only possible with devices that communicate in encrypted form.



User Profile and Certificate Selection

DEEBBSTE

Digital Signature

Issued for	Issued by	Valid from	Valid until	Thumbprint

Project File Decryption

Issued for	Issued by	Valid from	Valid until	Thumbprint

Security Level

Activate the Use of Certificates for Enhanced Security

□ Enforce encrypted communication
□ Enforce encryption of project files
□ Enforce signing of project files
□ Enforce encryption of downloads, online changes and boot applications
□ Enforce signing of downloads, online changes and boot applications
□ Enforce signing of compiled libraries
□ Enforce timestamping of signed compiled libraries
Timestamping server

48605803915

To enforce encrypted communication, proceed as follows:

✓ The IEC Editor is open.

✓ The connection to the MOVI-C® CONTROLLER is established.

✓ The security screen is open.

1. Open the "User" tab.
2. Activate the "Enforce encrypted communication" check box [1].

8.2 Certificates in the NBS library

When you use the NBS library, you exchange the certificates of the communication partners with each other.

8.3 Using a configuration file

You can either carry out the configuration via the IEC Editor or by using the configuration file `SewPlcSettings.cfg`. The configuration file is loaded when the MOVI-C® CONTROLLER is started. If you have set security-relevant device options in the IEC Editor that are also contained in the configuration file, these will be overwritten.

8.4 MOVIKIT® OPC-UA

8.4.1 Encryption

The MOVIKIT® OPC-UA software module supports certificate-based encryption. For more information, refer to the manual "MOVIKIT® OPC-UA, MOVIKIT® OPC-UA addon SensorInterface".

8.4.2 Port 4840

Port 4840 is closed if a license for the MOVIKIT® OPC-UA software module is not activated on the MOVI-C® CONTROLLER (test license or full version), as the OPC-UA server is not started. If a license is active, the OPC-UA server starts automatically together with the MOVI-C® CONTROLLER and port 4840 is opened.

Close permanently

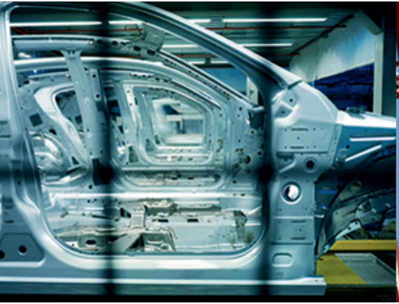
You can permanently close the port via the configuration file `SewPlcSettings.cfg`. If this setting is active, the OPC-UA server will not be started when the controller is booted up, despite an active license, and it also cannot be activated subsequently at runtime. To this end, use the following entry in the configuration file:

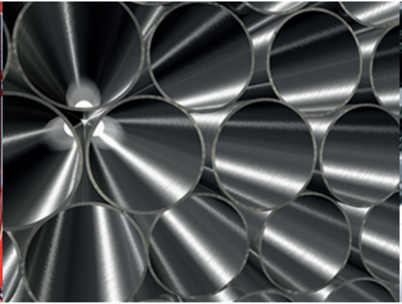
```
[CmpOPCUAServer]
SECURITY.Activation=DEACTIVATED
```

8.5 MOVIKIT® Visualization

The MOVIKIT® Visualization software module does not currently support the Secure-Channel function.

Index





SEW-EURODRIVE GmbH & Co KG
Ernst-Blickle-Str. 42
76646 BRUCHSAL
GERMANY
Tel. +49 7251 75-0
Fax +49 7251 75-1970
sew@sew-eurodrive.com
→ www.sew-eurodrive.com