

Table of contents

- Command 'Security Screen'



Command 'Security Screen'

Command 'Security Screen'

Symbol: 

Function: The command opens the *“Security Screen”* view.

Call:

- *“View”* menu
 -  icon or  in the status bar
- The icon is displayed in blue when a valid certificate is specified for the digital signature. When only one client certificate is specified for the encrypted communication, the icon remains gray, resulting in the client certificate providing no increased security for the user.

The following security features of PLC Engineering are configured and displayed in the view:

- Personal user certificate
- Encrypted communication
- Encryption and signatures of IEC projects
- Encryption and signature of download, online change, and boot application
- Security level



NOTICE!

When the *“Security Screen”* is opened and closed, the current settings are applied in the user options, even when no active changes have been made.



If the CODESYS Security Agent add-on product is installed, then the *“Security Screen”* view provides an additional *“Devices”* tab. This allows for the configuration of certificates for the encrypted communication with controllers.


Tab 'User'


On this tab, certificates are configured that are required for the encrypted communication and the digital signature of the user. Only certificates with private keys can be specified here. The user profile is saved as an XML file in the user options.

“User Profile and Certificate Selection”

By default, the login name for Windows is specified as the user profile.

List box with existing user profiles

: Opens the *“User Profiles”* dialog. Here you specify the name for a new user profile.

: Deletes the selected user profile. This user profile is no longer displayed in the list box.

“Digital Signature”

: Opens the *“Certificate Selection”* dialog for selecting the certificate for the digital signature.

One certificate can be selected. The certificate has to have a private key.

: Deletes the displayed certificate.

One certificate can be selected. The certificate has to have a private key.

“Project File Decryption”

: Opens the *“Certificate Selection”* dialog for selecting the certificate for decrypting project files.

One certificate can be selected. The certificate has to have a private key.

: Deletes the displayed certificate.


See also

- \ “Certificate selection” dialog”


“Security Level”

“Activate the Use of Certificates for Enhanced Security”

“Enforce encrypted communication”

: When the user communicates with the controller, the server certificate of the controller is used for establishing an encrypted connection. Then the entire communication is encrypted.

“Enforce encryption of project files”

: All project files of the user are encrypted with a certificate. When the project is saved, it is encrypted with the certificate specified in the project settings (*Project Settings* → *Security* dialog). The selected certificate is displayed on the *“Project”* tab in the *“Project file encryption”* group.

To open this project, the certificate to be encrypted has to be specified in *“Project file decryption”* with a private key.

“Enforce signing of project files”

☒: All project files of the user are signed with a certificate. In *“Digital Signature”*, a certificate has to be specified with a private key.

When a project is saved, a signature file <project name>.project.p7s is generated in the project directory containing the signature.

“Enforce encryption of downloads, online changes and boot applications”

☒: The data that is downloaded to the controller has to be encrypted with a controller certificate.

This certificate is defined directly either in the properties dialog of the application on the *“Encryption”* tab, or in the security screen, on the *“Project”* tab, in the *“Encryption of Boot Application, Download and Online Change”* group.

Controller certificates are located in the local Windows Certificate Store in the *“PLC Certificates”* directory. If the certificates of your controller are not available in the directory, then they first have to be loaded from the controller and installed to the directory. For instructions, see the *“Controller Certificates”* chapter.

“Enforce signing of downloads, online changes and boot applications”

☒: The online code (downloads, online changes, and boot applications) have to be signed with a certificate with a personal key. The certificate is selected from the *“Digital Signature”* area.

Requirement: The *“Encryption of boot application, download and online change”* option is selected.

“Enforce signing of compiled libraries”

☒: The *File → Save Project as Compiled Library* command generates a signed library <library name>.compiled-library-v3.

Requirements

- A certificate with a private key that supports code signing is available.
- A library compatibility >= PLC Engineering V3 SP15 is set in the project information.

“Enforce timestamping of signed compiled libraries”: ☒: The URL of the time stamp server which created the time stamp has to be entered in the *“Timestamping server”* field. Example: timestamp.comodoca.com/rfc3161.

See also


- ↘ *“Command 'Save Project as Compiled Library'”*
- ↘ *“Information for library developers”*

Tab 'Project'

All project-specific settings are configured on this tab. These elements are active only when a primary project is loaded.

"Project file encryption"

"Technology" : Opens the *Project Settings → Security* dialog


When you select the *"Encryption"* project setting and then *"Certificates"* in the dialog, you can choose a corresponding certificate by clicking . For more information, see the description of the "Project Settings: Security" dialog.

"Certificates of Users Sharing this Project" Area for listing the certificates that encrypt the project file.

"Encryption of Boot Application, Download and Online Change"

List of the applications of the controller Double-clicking an application in the list opens the *Properties → Encryption* dialog. Depending on the settings of the *"Security Level"* on the *"User"* tab of the *"Security Screen"*, the following fields are available in the open properties dialog:

- *"Encryption"* tab with active *"Certificates"* area
- *"Encryption"* tab with *"Encryption Technology"* list box.

In the *Properties → Encryption* dialog, click the  button to select the controller certificate for *"Encryption of Boot Application, Download and Online Change"*. For more information, see the description of the "Properties: Encryption" dialog.

Controller certificates are located in the local Windows Certificate Store in the *"PLC Certificates"* directory. If the certificates of your controller are not available in the directory, then they first have to be loaded from the controller and installed to the directory. For instructions, see the "Protecting and Saving a Project" - "Encryption with Certificates" chapter.

See also

- \ "Project settings' dialog - 'Security'"
- \ "Dialog 'Properties' - 'Encryption'"
- \ "Encrypting the project with a certificate"

Tab 'Devices'



This tab is available only after you have installed the CODESYS Security Agent add-on.
For a description of this tab, see the help for the CODESYS Security Agent.