EcoStruxure Control Expert

Security Editor

Operation Guide

Original instructions

EIO0000004105.05
07/2026

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric and its subsidiaries referred to in this document are the property of Schneider Electric or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Table of Contents 3
Safety Information 4
Before You Begin 4
Start-up and Test 5
Operation and Adjustments 6
About the Document 7
Access Security Management 12
Standard mode Tabs 16
Standard mode 16
Server Group Box 16
Client-Server Architecture 17
User Information Tab 18
Users Tab 19
Profiles Tab 22
Policies Tab 25
Login Policies Tab 27
Event Logging Tab 30
Certificate Actions Tab 31
Certificate whitelist Tab 33
Secured mode Tabs 36
Secured mode 36
Certificate Actions Tab 38
Users Tab 38
Profiles Tab 39
Security Policy Tab 39
Login Policies Tab 39
Certificate whitelist Tab 39
Configure a Controller Through the Enforced Engineering Link 40
Syslog Events 42
Recovery Procedure with a Detected Error 43
EcoStruxure Control Expert Predefined Profiles 44
EcoStruxure Control Expert Classic Access Rights 46
EcoStruxure Control Expert Classic Access Rights Assigned to Predefined Profiles 51
OS Loader Access Rights 57
Assigned OS Loader Access Rights to Predefined Profiles 58
Security Database Migration Tool 59
Index 60

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

Before You Begin

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions, government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point-of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

Start-up and Test

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check are made and that enough time is allowed to perform complete and satisfactory testing.

⚠WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995:

(In case of divergence or contradiction between any translation and the English original, the original text in the English language will prevail.)

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer’s instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer’s instructions and the machinery used with the electrical equipment.
- Only those operational adjustments required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

About the Document

Document Scope

This document describes how to use the Security Editor to manage access control, users, profiles, policies, certificates, and authentication mechanisms for EcoStruxure Control Expert and related tools.

It explains **Standard mode** and **Secured mode**, integration with EcoStruxure Cybersecurity Admin Expert 4.2.1 and any subsequent supporting version(s), client–server architectures, centralized and local databases, LDAP and Active Directory authentication, certificate handling, event logging, and syslog integration.

The guide details configuration workflows, predefined profiles and access rights, recovery procedures, database migration, and controller configuration to help enforce controlled engineering access.

Validity Note

This document has been updated for the release of EcoStruxure Control Expert 16.4.

Product Related Information

⚠WARNING

LOSS OF CONTROL

- Perform a Failure Mode and Effects Analysis (FMEA), or equivalent risk analysis, of your application, and apply preventive and detective controls before implementation.
- Provide a fallback state for undesired control events or sequences.
- Provide separate or redundant control paths wherever required.
- Supply appropriate parameters, particularly for limits.
- Review the implications of transmission delays and take actions to mitigate them.
- Review the implications of communication link interruptions and take actions to mitigate them.
- Provide independent paths for control functions (for example, emergency stop, over-limit conditions, and error conditions) according to your risk assessment, and applicable codes and regulations.
- Apply local accident prevention and safety regulations and guidelines.[1]
- Test each implementation of a system for proper operation before placing it into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[1] For additional information, refer to NEMA ICS 1.1 (latest edition), *Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control* and to NEMA ICS 7.1 (latest edition), *Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems* or their equivalent governing your particular location.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Only use software approved by Schneider Electric for use with this equipment.
- Update your application program every time you change the physical hardware configuration.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The examples in this manual are given for information only.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

Adapt examples given herein to the specific functions and requirements of your industrial application before you implement them.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the Cybersecurity Best Practices document.

Schneider Electric provides additional information and assistance:

- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity posture.
  - Learn more about cybersecurity in the cybersecurity academy.
  - Explore the cybersecurity services from Schneider Electric.

Product Related Cybersecurity Information

Refer to *Modicon Controller Platform Cybersecurity, User Guide*.

Available Languages of the Document

This document is available in these languages:

- English (EIO0000004105 (ENG))

- French (EIO0000004106 (FRE))
- German (EIO0000004107 (GER))
- Spanish (EIO0000004109 (SPA))
- Italian (EIO0000004108 (ITA))
- Chinese (EIO0000004110 (CHS))

Related Documents

Title of documentation	Reference number
EcoStruxure™ Control Expert, Installation Manual	35014793 (ENG) 35014792 (FRE) 35014794 (GER) 35014795 (SPA) 35014796 (ITA) 35012191 (CHS)
Modicon M580, Hardware, Reference Manual	EIO0000001578 (ENG) EIO0000001579 (FRE) EIO0000001580 (GER) EIO0000001581 (SPA) EIO0000001582 (ITA) EIO0000001583 (CHS)
EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual	CAE/EN UM/ (ENG)

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Terminology Derived from Standards

The technical terms, terminology, symbols and the corresponding descriptions in the information contained herein, or that appear in or on the products themselves, are generally derived from the terms or definitions of international standards.

In the area of functional safety systems, drives, and general automation, this may include, but is not limited to, terms such as *safety*, *safety function*, *safe state*, *fault*, *fault reset*, *malfunction*, *failure*, *error*, *error message*, *dangerous*, etc.

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers, part 2: Equipment requirements and tests.
ISO 13849-1:2023	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2013	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design
IEC 62061:2021	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software requirements.
IEC 61784-3:2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.
2006/42/EC	Machinery Directive
2014/30/EU	Electromagnetic Compatibility Directive
2014/35/EU	Low Voltage Directive

In addition, terms used in the information contained herein may tangentially be used as they are derived from other standards such as:

Standard	Description
IEC 60034 series	Rotating electrical machines
IEC 61800 series	Adjustable speed electrical power drive systems
IEC 61158 series	Digital data communications for measurement and control – Fieldbus for use in industrial control systems

Finally, the term *zone of operation* may be used in conjunction with the description of specific hazards, and is defined as it is for a hazard zone or danger zone in the Machinery Directive (2006/42/EC) and ISO 12100:2010.

NOTE: The aforementioned standards may or may not apply to the specific products cited in the present documentation. For more information concerning the individual standards applicable to the products described herein, see the characteristics tables for those product references.

Trademarks

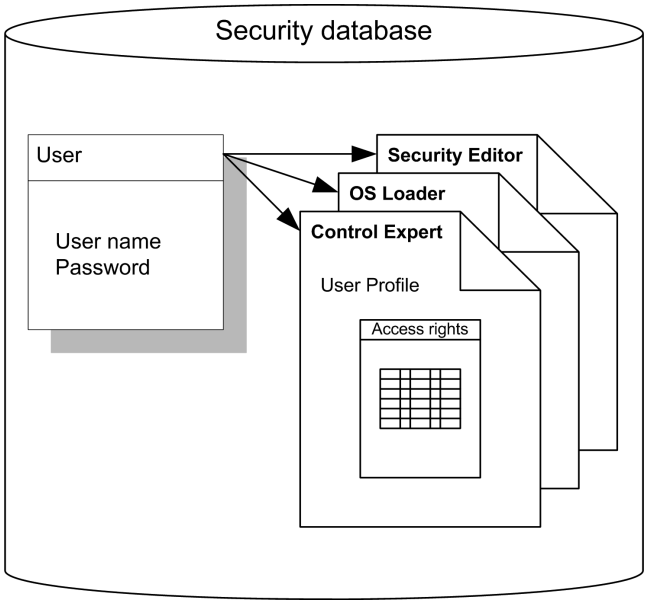
Microsoft, Windows, Windows Server, and Windows Defender are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Access Security Management

Conceptual Diagram

Launch and use the Security Editor tool to control access to the different functionalities of EcoStruxure Control Expert and the associated loader management software.

When you install and set up the Security Editor tool, a security database is automatically created with one administrative user (*SecurityAdmin*). The database contains definitions for users, user profiles, and user-access rights:



NOTE: Protected access to the EcoStruxure Control Expert and loader management software is optional, the **Security** option of the protected access is set to **OFF** by default.

Access to EcoStruxure Control Expert is applicable to the terminal on which the software (not the project) is installed. The project has its own protection system.

A log file can contain a chronological record of the various operations carried out by users with access to the software.

SecurityAdmin User

The *SecurityAdmin* user is reserved for the administrator of the Security Editor tool.

NOTE: The *SecurityAdmin* user performs the administrative role that was handled by the *Supervisor (super user)* in legacy versions of EcoStruxure Control Expert (those that predate version 15.3).

After the EcoStruxure Control Expert software is installed on a workstation, only the predefined *SecurityAdmin* user can launch the Security Editor and modify the security configurations after the authentication.

The first time you launch the Security Editor tool, you are prompted to create a password for the *SecurityAdmin* user. Change the *SecurityAdmin* password in the **User Information** tab, page 18.

The *SecurityAdmin* user has a unique profile within the Security Editor. Only this user has the administrative rights to manage the security database and define a list of user names and their respective access rights to the software.

The *SecurityAdmin* user can perform these tasks:

- Create or modify the user list.
- Create or modify user profiles.
- Deactivate one or more users.
- Modify the rules for software access.
- Modify the *SecurityAdmin* user password.
- Reset user passwords.
- Configure the authentication mechanism for a local or centralized database of users and their associated access rights.
- Generate, use, and manage certificates and create a list of certificates for the authentication of trusted computers.
- Launch the Security Editor in **Secured mode**.
- Import an EcoStruxure Cybersecurity Admin Expert cybersecurity configuration file to help secure EcoStruxure Control Expert.

Security Database Migration

During the migration of the security database, the database is automatically re-created with only one administrative user.

At that time, it is possible to recover security databases that were created with earlier versions of EcoStruxure Control Expert if you follow the prompts during the migration.

The authorization associated with the former administrator role (*Supervisor*) are automatically transferred to the new role of the *SecurityAdmin* user. Therefore, during the migration of the security database, the existing password is replaced by the password that was defined by the *SecurityAdmin* user.

User Profile

A user profile includes the defined access rights for a user. It is defined by a name, an optional comment (maximum of 256 characters), and a list of access rights. Security Editor provides 10 preconfigured profiles that cannot be modified. To complete this list, the *SecurityAdmin* user can create personalized profiles.

Predefined Users and User Profiles

The Security Editor provides 10 predefined users and 10 predefined profiles. The profiles are read-only. The predefined users can be activated or deactivated by the *SecurityAdmin* user.

These are the predefined users and the corresponding predefined profiles (according to the selected product):

Predefined User	Predefined Product Profile		
	Security Editor	EcoStruxure Control Expert	Loader management software
safety_user_Adjust	ReadOnly	Safety_Adjust	—
safety_user_Debug	ReadOnly	Safety_Debug	—
safety_user_Operate	ReadOnly	Safety_Operate	—
safety_user_Program	ReadOnly	Safety_Program	—
SecurityAdmin	SecurityAdmin	—	—
user_Adjust	ReadOnly	Adjust	—
user_Debug	ReadOnly	Debug	—
user_Operate	ReadOnly	Operate	—
user_Program	ReadOnly	Program	Program
user_ReadOnly	ReadOnly	ReadOnly	ReadOnly
NOTE: By default, the predefined users are deactivated.			

Default User Profile

When the software access security is active, the *SecurityAdmin* user can authorize these types of access for specific users while retaining control of the environment.

- **Security on, no login:** Open a software instance without entering a user name and password.
- **Security on, avoidable login:** Enter a user name without a password.

  NOTE: In these cases, the user has a default profile by way of your selection for the **Fixed profile** under the **Policies** tab. (Refer to the description of login parameters on the **Policies** tab, page 26).

Multiple Instancing

When EcoStruxure Control Expert executes multiple instances concurrently on the same terminal, each instance grants access to the functions that were defined by the rights of the user who created this instance.

Centralized Security Database

The *SecurityAdmin* user performs the following tasks to administer a centralized security database:

- Define users, user profiles, and user access rights on the remote server.
- Deploy the centralized security database to client workstations.

The Security Editor tool, which is automatically installed with EcoStruxure Control Expert, administers its own local security database.

Standard mode Tabs

Standard mode

In **Standard mode**, you can modify all the security configurations present in EcoStruxure Control Expert Classic.

It corresponds to the basic behavior of the Security Editor up to EcoStruxure Control Expert 16.2.

Server Group Box

Introduction

Use the configuration settings in the **Server** group box to configure the local security service to run as a server that receives authentication requests from other computers on the network. Those other computers, therefore, function as clients in a client-server architecture.

> **NOTE:** This guide includes a use-case example that shows the functionality of Security Editor in a client-server relationship, page 17.

A user in the SecurityAdmin role can perform a customized installation of EcoStruxure Control Expert Classic to install the Security Editor as a server in the absence of a complete installation of EcoStruxure Control Expert Classic. For more information, refer to the *EcoStruxure™ Control Expert, Installation Manual*.

Server Parameters

These are the configuration settings in the **Server** group box:

Parameter	Description
SecurityService as server	Select this checkbox to configure a computer to run Security Editor as a server that allows access to its configuration data and user profiles by authorized clients. In this case, Security Editor that runs on a client computer can target the server computer using the **Network** protocol from the **Centralized Protocol** menu on the **Login Policies** tab. **NOTE:** The server requires a valid **SecurityService** certificate to start. It is therefore possible that a server does not run even when the **SecurityService as server** parameter is selected. In this case, the *SecurityAdmin* user uses the instructions to generate a certificate on the **Certificate Actions** tab, page 32.
Port nb	Enter the port number that Security Editor uses to connect to a client computer.
Server State	This field reports the availability of the server: • **Available after Security Editor restart**: The parameters **SecurityService as server** and **Port nb** are not dynamically processed. The **SecurityService** server restarts with the new settings only after Security Editor closes. • **Running**: The **SecurityService** server is running. • **Stopped**: The **SecurityService** server is not running.

Restart Security Editor to implement the modified **Port nb** and **Server State** parameters:

Step	Action
1	Select **OK** to close the Security Editor tool.
2	Reopen the Security Editor tool to confirm that the server runs with the modified parameters.

Client-Server Architecture

Introduction

Use the Security Editor to establish a client-server architecture:

- *client:* The client computer runs Security Editor and requires access to configuration information on a server computer.
- *server:* The server computer runs the SecurityService of the Security Editor.

This architecture allows the client to use the configuration of the server. For example, you can start EcoStruxure Control Expert Classic on a client computer with credentials (username and password) that exist only on the server. The client also imports the certificate whitelist from the server.

Use the directions below to create an example of a client-server relationship with Security Editor.

NOTE: For a robust client-server architecture, follow the instructions to help enforce security for the EcoStruxure Control Expert project., page 40.

Configure the Server

Set up a remote computer to run Security Editor as a server.

Step	Action
1	Launch Security Editor to display the **Server** group box.
2	Confirm that the certificate for the selected product is valid by hovering the mouse over the certificate icon on the **Certificate Actions** tab, page 31.
3	Select the **SecurityService as server** checkbox to run as a server.
4	Select **OK** to apply your modifications and to close Security Editor.

Configure a Client to Connect to a Server

Configure a client for the Security Editor *SecurityService* to connect to the Security Editor *SecurityService* that runs on a remote server.

Step	Action
1	Select the **Login Policies** tab in the Security Editor.
2	Select a **Centralized** option from the **Authentication Mode** menu.
3	Select **Network** from the **Centralized Protocol** drop-down menu. **NOTE:** The selection of a **Centralized** server automatically sets the **Login** option on the **Policies** tab to **Security on, mandatory login**. In this case, other **Login** options on the **Policies** tab are deactivated.
4	In the **Server Address** group box, select the radio button that corresponds to your desired addressing method: • **Host IP:** Enter the IP address of the server. • **Host Name/DNS:** Enter the host name of the server. **NOTE:** • You can configure only one of these addressing methods. • You can establish this connection when the *SecurityService* client and the *SecurityService* server are on the same network.
5	In the **Port** field, enter the port number of the server computer.
6	Select **Apply**.

NOTE: On the *SecurityService* client side, whitelist the *SecurityService* certificate from the server to support the connection to the server. (Refer to the description of the **Certificates whitelist** tab, page 35.)

User Information Tab

Introduction

This topic describes the parameters and functions that are available when you select the **User Information** tab in the Security Editor tool.

Only the *SecurityAdmin* user can perform these actions:

- Access all user profiles.
- View the access rights for all users.
- Modify the passwords for all users.

Parameter Descriptions

The **User Information** tab indicates the name of the user and some corresponding parameters.

Field	Description
Name	Select the name of the applicable user from this drop-down menu.
Status	This read-only field displays one of these status for the selected user: • **Expired:** The password is expired. • **Valid until the <*Expiration Date*>:** The password is active until the displayed expiration date. • **Valid:** The password is active without a time limit.

Configure these parameters for the selected user:

Group Box	Component	Description
Password	**New password**	Enter the new password in this field. See important Safety and Security Information found at the end of this table.
	Confirm the new password	Reenter the new password in this field.
	Apply	Select **Apply** to save and apply the new password. Select **OK** to save the new password.
Profile(s)	**Product**	From this drop-down menu, select the product for which you want to display the user profile.
	Profile	When you make a selection in the **Name** drop-down menu on this tab, the name of the corresponding profile appears in this field.
	View profile	Select **View profile** to open the **View profile** dialog box, which displays the access rights in the user profile. **NOTE:** For users with multiple profiles, the **Access rights list** in the **View profile** dialog box shows the modified access rights. These access rights are present when at least one of the profiles of the multiple profiles contains that right.

If you implement password requirements, establish strong passwords for all users. If you implement security, define passwords for all users.

Users Tab

Introduction

This topic describes the parameters and functions that are available when you select the **Users** tab in the Security Editor tool.

Activate a user on the **Users** tab if you set the security access rules on the **Polices** tab to **Security on, mandatory login**. For other **Login** setting values, an activated user is not required.

NOTE: Refer to the selection of the security level in the **Login** group box on the **Policies** tab, page 25.

Only the *SecurityAdmin* user can access the **Users** tab and activate the execution of these functions:

- Modify the user list.
- Assign a profile to each user.
- Import and export information for one or more users.
- Deactivate one or more users.
- Delete passwords for one or more users.

Element Descriptions

These elements appear in the **User(s)** group box on the **Users** tab:

Element	Description
(list)	The list displays the users that are declared in the security database (including Predefined users, page 14).
Add	Select **Add** to add a new user to the **User(s)** list, page 21.
Delete	Select **Delete** to delete the selected user(s) from the list. **NOTE:** You cannot delete a predefined user.
Export(1)	Select **Export** to save the database (name and profiles) for the selected user(s) to a file. • An exported file includes encrypted passwords. • Refer to the description of database recovery, page 21.
Import(1)	Select **Import** to recover the database (name and profiles) of the selected user(s) from a file. **NOTE:** Refer to the description of database recovery, page 21.
Enable/ **Disable**	Toggle this button to switch between activating and deactivating access for a selected user: • **Enable**: Select **Enable** to activate access for the user that is selected in the **User(s)** list. • **Disable**: Select **Disable** to deactivate access for the user or users that are selected in the **User(s)** list. **NOTE:** ◦ A deactivated user is blocked at user authentication when **Security on, mandatory login** is on, page 25. Otherwise, a message informing you that your access has been deactivated is displayed. ◦ The name of a deactivated user ends with the **--disabled--** suffix in the list. ◦ You cannot deactivate a *SecurityAdmin* user.
Clear Password	Select **Clear Password** to set the password value to an empty string.
(1) The Security Editor runs under the *SecurityAdmin* user. It is not possible to access personal folders for the user such as the folders under `C:\users\current_user_name`. You cannot export or import a file to that location.	

These elements appear in the **Profile(s)** group box on the **Users** tab:

Element	Description
Product	In this drop-down menu, select the product for which you want to define a user profile.
Profile(s)	A *SecurityAdmin* user can select the boxes of available options in this list to select the profile or profiles to be associated with each selected user and mapped product. **NOTE:** Refer to the details below to associate profiles with Multiple Profiles, page 21.
Apply	Click **Apply** to apply each profile assignment. **NOTE:** This button is active when a change is made to the selections in the Profile(s) list.
OK	Select **OK** to acknowledge and validate each set of changes.

Add a User

Select **Add** to access these parameters:

Parameter	Description
User name	Enter the name of the new user in this field.
Password	Enter a password for the new user in this field.
Confirm the password	Reenter the password for the new user in this field.
With the following attributes	Select the attributes that correspond to the new user.
OK	Select **OK** to save and implement the parameters of the new user.

Multiple Profiles

Only a *SecurityAdmin* user can associate multiple profiles with a single user for each mapped product by selecting multiple items in the **Profile(s)** list.

This allows a user to log in with multiple profiles and products in the same or different software contexts. The resulting profile is a fusion of the selected profiles.

You cannot modify the predefined users, products, and profiles that appear in the **Profile(s)** list.

Database Recovery

You can recover the contents of the security database if you first export the **User** and **Profiles** information to backup files.

To backup users and profiles, create two exchange files with the appropriate file extensions:

- users backup file (.XSU.ENC)
- profiles backup file (.XSP.ENC)

These files are password-encrypted.

NOTE: Store the password in a known location to retrieve it later to restore the database content.

Restore the backup files in this order:

1. Import the profiles backup file.
2. Import the users backup file.

NOTE: The Security Editor runs under the *SecurityAdmin* user. It is not possible to access personal folders for the user such as the folders under `C:\users\current_user_name`. You cannot import or export a file to that location.

Save and Apply Changes

Apply and save the changes for each new user assignment.

Profiles Tab

Introduction

This topic describes the elements and functions that are available when you select the **Profiles** tab in the Security Editor tool.

Perform these functions on the **Profiles** tab:

- Add or delete a profile in the list.
- Read or modify the access rights associated with a profile.
- Import or export information for one or more user profiles.

Only the *SecurityAdmin* user can access the **Profiles** tab.

Element Descriptions

These are the elements on the **Profiles** tab:

Element		Description
Product (drop-down menu)	—	Select the product that corresponds to the user profile you want to access. **NOTE:** This document applies to EcoStruxure Control Expert Classic. Therefore, only the **Control Expert** selection from this menu is applicable to this guide.
Profiles (group box)	(list)	The user profiles in this list are associated with the selected product.
	Add	Select **Add** to add a user profile on the **Profiles** tab. **NOTE:** Refer to the directions to *Add a User Profile*, below.
	Delete	Select **Delete** to delete one or more selected user profiles from the list.
	Edit	Select **Edit** to modify the access rights associated with the selected and modify the user profile. **NOTE:** You cannot modify predefined user profiles. Refer to the directions to *Modify a User Profile*, below.
	Export(1)	Export the information (name and profiles) of the selected user profile(s) to a file by selecting **Export**.
	Import(1)	Import the information (name and profiles) of the selected user profile(s) from a file by selecting **Import**.
(1) The Security Editor runs under the *SecurityAdmin* user. It is not possible to access personal folders for the user such as the folders under `C:\users\current_user_name`. You cannot export or import a file to that location.		

Add a User Profile

Select **Add** to open the **Add a profile** dialog box and access these configuration parameters:

Parameter	Description
Add the profile	Enter the name of the new user profile.
With the following	From this drop-down menu, select the user profile that has the access rights you want to attribute to the user profile.
OK	Select **OK** to create the new profile and add it to the **Profiles** list.

Modify a User Profile

Select **Edit** to open the **Edit profile** dialog box.

Access these text fields:

Field	Description
Tool	This field contains the name of the selected product.
Profile	This field contains the name of the selected user profile.
Description	Comments associated with the user profile (optional).

The **Access rights list** table includes these columns:

Column	Description
Access right	This column is a list of product access rights that are associated with the user profile. Select or clear **Display Safety rights** checkbox to show or hide safety-related access rights. **NOTE:** There are no access rights for safety-related controllers for the loader management software or Security Editor.
Audit	This column shows the audit state for each access right. **Yes** activates audit logging of the access right to the Windows Event Viewer log file; **No** deactivates it. Set the value using **Audit Yes/No**.
Confirm	This column shows the confirmation state for each access right. **Yes** requires that you confirm the operation before it executes; No does not require confirmation. Set the value using **Confirm Yes/No**.

Select a role from the **DTM access rights** drop-down menu:

Parameter	Description
DTM access rights	Select a user: • **Administrator** • **MaintenanceEngineer** • **PlanningEngineer** • **SystemObserver** • **SystemOperator** **NOTE:** You can view the access rights and the DTM access rights associated with a preconfigured profile, but you cannot *modify* them. DTM access rights for EcoStruxure Control Expert. Select the **PlanningEngineer** or **Administrator** role if one of these user access right is activatedd: • **create a new project** • **build off-line** • **build on-line stop** • **build on-line run** • **Modify Project settings** • **Variable Add Remove** • **DDT Add Remove**

To change EcoStruxure Control Expert access rights:

Step	Action
1	Create a new profile based on an existing profile (the DTM role and DTM access rights for predefined profiles are read-only).
2	Select one or more access rights to modify.
3	Click **State On/Off** to activate or deactivate each selected right.
4	Check the status of the rights: • A blue checkmark indicates that the right is active • The absence of a blue checkmark indicates that the right is inactive
5	For an inherited profile, you can also change the default DTM role from the drop-down menu in the **Edit Profile** dialog box. If you select a DTM role with access rights incompatible with the current profile, the Security Editor displays a confirmation dialog.
6	Close the confirmation dialog.
7	Review the incompatible access rights highlighted in the **Edit Profile** dialog box.
8	Click **State On/Off** to deactivate the incompatible access rights.
9	Click **OK**.
10	Click **Apply** to save the changes.

NOTE: Regardless of the DTM role you select for a profile, EcoStruxure Control Expert applies the **PlanningEngineer** DTM role to all DTM applications. The DTM role selection in the **Edit Profile** dialog does not affect DTM application access.

Select these buttons to effect the corresponding action:

Button	Description
State On/Off	Activate or deactivate a selected access right for the selected profile: 1. Select an item in the **Access right** column. 2. Select **State On/Off** to toggle the selection mark for the selected item.
Audit Yes/No	Change the value in the **Audit** column to **Yes** to activate the selected **Access right**: 1. Select an item in the **Access right** column. 2. Select **Audit Yes/No** to toggle the value to **Yes** or **No**.
Confirm Yes/No	Change the value in the **Confirm** column to **Yes** to require confirmation for an operation: 1. Select an item in the **Access right** column. 2. Select **Confirm Yes/No** to toggle the value to **Yes** or **No**.
OK	Apply the changes you made.

Syslog Server Events

To capture access-right events for forwarding to a syslog server, create a profile on the **Profiles** tab with audit logging activated for every access right.

Step	Action
1	On the **Profiles** tab, click **Add** to open the **Add a profile** dialog box.
2	Add this profile name in the **Add a profile** field: *SYSLOG_Profile*
3	Make this selection from the **With the following** drop-down menu: *Program*
4	Click **OK** to close the **Add a profile** dialog box. **NOTE:** The new profile name appears in the **Profiles** group box on the **Profiles** tab.
5	Select the new profile name (*SYSLOG_Profile*) in the **Profiles** group box.
6	Click **Edit** to open the **Edit** profile dialog box.
7	Select every item in the **Access rights** list.
8	Click **Audit Yes/No** and set the value to **Yes**.
9	Click **OK** to close the **Edit profile** dialog box.

Policies Tab

Introduction

This topic describes the parameters and functions that are available when you select the **Policies** tab in the Security Editor tool.

Only the *SecurityAdmin* user can configure the parameters on the **Policies** tab to execute these functions:

- Determine the guidelines that are associated with a product.
- Define the default profile.
- Activate or deactivate the **Audit** option.
- Activate or deactivate the **Confirm** option.
- Configure the duration (in days) of the password validity.

Product Selection

Select **Control Expert** from the product drop-down menu.

NOTE: This document describes the Security Editor with respect to EcoStruxure Control Expert Classic. Therefore, only the **Control Expert** selection from this menu is applicable to the information in this guide.

Login Parameters

Use these selections in the **Login** group box to define security access rules per user account:

Security off	Select this radio button to deactivate security and allow complete access to the product.
Security on, mandatory login	Select this radio button to activate security and require both the user name and password. The defined profile for that user name is enforced.
Security on, avoidable login	Select this radio button to activate security. If you do not enter your user name and password, you can access the product, but confined to the default user profile defined by the **Fixed profile** selection. If you also enter your user name and password, you can access the product with the profile associated with your user name.
Security on, no login	Select this radio button to allow access directly to the product without a prompt for user name and password. However, security is activated in the sense that you are confined to the default profile defined by the **Fixed profile** selection.
Fixed profile	Use this drop-down menu to select a default user profile. This is the profile used when the **Login** access rule is set to **Security on, no login**.

Checkboxes: Select or clear these checkboxes:

Audit	Select this checkbox to create a log file that stores user events for EcoStruxure Control Expert and loader management software. **NOTE:** Display the log file with the Windows command (**Start > Programs > Windows Administrative Tools > Event Viewer**.)
Confirm	When you select this checkbox, enter your name and password each time you define secure access for a user action, page 22. **NOTE:** If you select **Confirm**, carefully select access rights when you create a new profile because many user actions will require multiple confirmations.

NOTE:

- The **Audit** and **Confirm** options are not assigned to a single user. They apply globally to users that have authorized access to the product.
- When you use the **Security off** option, the functionalities of the **Audit** and **Confirm** checkboxes are unavailable.

User Account Password Validity

Define a validity period for the password for in the **User Accounts** group box on the **Policies** tab:

Password validity period	Select this checkbox to reject login attempts that use an expired password (as defined by the **Period in days** value and the age in days of the latest password). **NOTE:** • You can implement the **Password validity period** only when you select **Security on, mandatory login** from the **Login** group box. • When the **Password validity period** checbox is not selected, the password does not expire. The value in the **Period in days** field is therefore ignored.
Period in days	Enter the number of days for which the password is valid when you select **Password validity**.
Apply	Select **Apply** to save and implement the value in the **Period in days** field.

NOTE: After you define a validity period for at least one user, you can verify the validity period. Select the user in the **Name** field on the **User information** tab and read the information associated with the **Status** field.

Syslog Server Events

To add all required syslog events to the syslog server, create a **SYSLOG_Profile** as described in *Syslog Server Events*, page 25 and configure the relevant options in the **Policies** tab:

Step	Action
1	On the **Policies** tab, select **Control Expert** from the product drop-down menu.
2	From the **Login** group box, select **Security on, no login**.
3	Select **SYSLOG_Profile** from the **Fixed profile** drop-down menu.
4	Select the **Audit** checkbox.
5	Click **Apply** or **OK** to apply the changes.

Login Policies Tab

Introduction

This topic describes the parameters and functions that are available on the **Login Policies** tab in the Security Editor. Use this tab to configure the authentication mechanism for a local or centralized database of users and their associated access rights.

These database types are available in the **Authentication Mode** drop-down menu:

- *local:* For a local database, the computer accesses a local database. In this case, select the **Local** database.
- *centralized:* For centralized databases, a client computer accesses a remote computer to use its database by selecting one of several centralized database types.

  NOTE: This guide includes a use-case example that shows the use of Security Editor in a client-server relationship, page 17.

Local Database

On the **Login Policies** tab, choose **Local** from the **Authentication Mode** drop-down menu to configure an authentication database in the local computer.

Use the **Local** mode to define users and their corresponding Role Based Access Control (RBAC) settings in the Security Editor database on the same local computer that is used for authentication.

When you select (and apply) a local database, you can change and update the login behavior on the **Policies** tab, page 25.

NOTE: The functionality with a local database matches the functionality of the authentication mode in legacy releases of the tool that predate EcoStruxure Control Expert version 15.3.

Centralized Database

On the **Login Policies** tab, choose one of these **Centralized** options from the **Authentication Mode** drop-down menu to configure a database on a remote server to authenticate one or more EcoStruxure Control Expert clients.

Authentication Mode	Description
Centralized,Local	An attempt is made to authenticate users against a remote *centralized* database. If that is not successful, a subsequent attempt is made to authenticate users against a *local* database.
Local,Centralized	An attempt is made to authenticate users against a *local* database. If that is not successful, a subsequent attempt is made to authenticate users against a remote *centralized* database.
Centralized	Attempts are made to authenticate users against a remote centralized database. (There is no attempt to authenticate locally.)

NOTE: The **Authentication Mode** options that include a comma indicate the sequence of attempts to access the server:

- **Centralized,Local:** Attempt to access a *centralized* server first and a *local* server second.
- **Local,Centralized:** Attempt to access a *local* server first and a *centralized* server second.

To use any of these **Centralized** authentication modes, be aware of the configuration distinctions for the client and server workstations:

- *client:*
  - Enter the IP address of the remote server in the **Host IP** text field in the **Server Address** group box.

    NOTE: Refer to the **Server Address** parameters in the *Element Descriptions* table (below).
  - The status of the **SecurityService as server** checkbox in the **Server** group box (at the top of the Security Editor window) is not relevant to the role of the client workstation.
- *server:*
  - Verify that the address of this remote server corresponds to the **Host IP** address in the client configuration (above).
  - Select the **SecurityService as server** check box in the **Server** group box (at the top of the Security Editor window).
  - The remote server can potentially be behind the firewalls that surround different security zones. Configure the server to activate access for the authentication policies. You can also configure the policies to redirect requests among the zones of security.

Consider these points when you select and apply a **Centralized** option from the **Authentication Mode** menu:

- Confirm that the firewall on the server authorizes access for the port.
- You cannot configure a **Login** type on the **Policies** tab, page 25. **Security on, mandatory login** is selected, other **Login** options are deactivated.
- You can configure the Windows Active Directory, page 30.

Element Descriptions

These elements are also in the **Network Security Service** group box on the **Login Policies** tab.

Element		Description
Centralized Protocol(1) (drop-down menu)	**Network**	Register the authentication for a server that is not on the local computer that makes the authentication request. This authentication allows local computers to use the centralized configuration of a remote server on which Security Editor is installed. **NOTE:** • To connect to the remote server or to use **LDAP**, whitelist the certificate. Refer to **Certificate whitelist**, page 33. • Regardless of the selection in the **Centralized Protocol** drop-down menu, connect the Security Service client to the same network as the **Network Security Service** server to establish a connection.
	LDAP	Implement the Lightweight Directory Access Protocol (LDAP) for user authentication through an LDAP server that supports TLS connection. **NOTE:** • The **LDAP** protocol is available in the **Centralized Protocol** menu only when you select a *Centralized* option from the **Authentication Mode** menu. • To connect to the remote server or to use LDAP, whitelist the certificate. Refer to **Certificate whitelist**, page 33. • The maximum length of LDAP credentials is 56 characters.
Server Address(1)	**Host IP**	Enter the IP address of the remote server to be used for authentication.
	Host Name/DNS	Enter the name of a remote server to be used for authentication.
	Port	Enter the port number of the remote server to be configured for security authentication. By default, these port numbers are associated with the selected protocol: • `50051`: **Network** is selected in the **Centralized Protocol** menu. • `389`: **LDAP** is selected in the **Centralized Protocol** menu. **NOTE:** You can establish this connection when the Security Service client and the Security Service server are on the same network.
LDAP Protocol Details(2)	**LDAP group(s)**(3)	Configure **LDAP group(s)** manually to authenticate the users in these **LDAP group(s)**.
Profile(s)(3) (4)	—	Select the profiles in this list to associate them with the selected group(s).
Base DN(2)	—	When active, this field contains the distinguished name that is created from the path to the user. **NOTE:** Refer to the description of **Base DN** below.
Export(5)	—	Export the information (**Login Policies**) to a file by selecting **Export**.
Import(5)	—	Import the information (**Login Policies**) from a file by selecting **Import**.
Apply	—	Select **Apply** to confirm and apply the changes.

(1) These elements are available when you select one of the *Centralized* options from the **Authentication Mode** menu.

(2) These elements are available when you select **LDAP** from the **Centralized Protocol** menu.

(3) When a user is successfully authenticated using an LDAP server, groups in the **LDAP group(s)** drop-down menu are queried and matched with this authenticated username. In this case, the corresponding profiles (roles) are assigned to the user profile. If multiple LDAP groups are configured, or if more than one profile is mapped to the LDAP group, multiple profiles are associated with the user. The following actions are available for LDAP groups:

- *Create a new LDAP group:* Enter the new group name and press **Enter**
- *Delete an LDAP group:* Select the group and the trash icon on the left.
- *Select an existing LDAP group:* Use the drop-down menu.

(4) When you select and apply a centralized **LDAP** protocol, the **LDAP group(s)** drop-down menu is active. Make a selection in this menu to activate the **Profile(s)** checkboxes and select profiles for single or multiple **LDAP group(s)** before you select **Apply** to implement your changes.

(5) The Security Editor runs under the *SecurityAdmin* user. It is not possible to access personal folders for that user such as the folders under `C:\users\current_user_name`. You cannot import or export a file to that location.

Base DN

The **Base DN** field is active when **LDAP** is selected in the **Centralized Protocol** menu.

In a non-Windows LDAP server, the **Base DN** field is mandatory. The **Base DN** contains the location at which you can find the user to be authenticated.

You can enter the common name (CN) or user identifier (UID) to log in to the software. In this case, the path to the user in the **Base DN** field is used to create a distinguished name (DN) for the logged-in user.

Active Directory Configuration

When a valid certificate appears on the **Certificate Actions** tab, you can configure the Windows Active Directory on the **Login Policies** tab.

Step	Action
1	Select the **Login Policies** tab.
2	Make these selections: • **Authentication Mode:** Choose one of the **Centralized** options. • **Centralized Protocol: LDAP**
3	Enter the appropriate information for these parameters: • **Host Name/DNS:** Enter a name for the remote server to be used for authentication. • **Port:** Enter the port number for the remote server to be configured for authentication. • **LDAP group(s):** Enter the name of an LDAP group of users to authenticate and press **Enter**. **NOTE:** • If necessary, request this information from the *SecurityAdmin* user. • Repeat this step to create additional LDAP groups.
4	Select a group from the **LDAP group(s)** drop-down menu and select names of profiles from the **Profile(s)** list to associate with that group. **NOTE:** Repeat this step to associate profiles with all items in the **LDAP group(s)** drop-down menu.
5	Select **Apply** at any time to apply and save the configuration.

NOTE: To confirm the configuration of the Active Directory, open EcoStruxure Control Expert Classic to confirm that the user name and associated profile for the Active Directory configuration appear in the title bar.

Event Logging Tab

Introduction

This topic describes the parameters and functions that are available on the **Event Logging** tab in the Security Editor.

Consider these points when you configure **Event Logging**:

- Logged events indicate a change in the LDAP configuration
- Event timestamps conform to the UTC standard.

Parameter Descriptions

Define the **Event Logging** behavior with the parameters on this tab:

- **Enable Syslog:** Select this box to send events to a syslog server that corresponds to the **Server Address**, **Server Port**, and **Protocol** values (below).
- **Server Address:** Enter the IP address of the syslog server.
- **Server Port:** Enter the port number of the syslog server.
- **Protocol:** TCP

NOTE: The **Event Logging** tab contains buttons that correspond to Windows commands (**OK**, **Apply**, **Cancel**, **Help**).

Event List

This table displays the logged event messages (in English only):

Event Message	Description
Successful login for SecurityAdmin	The *SecurityAdmin* user signed in successfully.
Failed login for SecurityAdmin	The *SecurityAdmin* user sign-in attempt was not successful.
Password changed for SecurityAdmin user	The *SecurityAdmin* user password changed.
Password changing failed for SecurityAdmin user	The *SecurityAdmin* user attempt to change a password was not successful.
LDAP group changed: <details>	This name (<*details*>) is a placeholder. It is replaced at runtime by the LDAP group name and the profiles used by that specific LDAP group.
Profile edited: <profile_name>	This name (<*profile_name*>) is a placeholder. It is replaced at runtime by the name of the profile being modified.
Logout	The *SecurityAdmin* user logged out successfully.
Security Database saved	All updates performed since the last successful login by the *SecurityAdmin* user are saved in the security database. Only updates saved in the security database are used at runtime for LDAP authentication processing.
Cybersecurity Configuration change	A new cybersecurity configuration has been successfully imported. It includes standardized objects such as: • UserAccount: Defines users and credentials. • RBAC: Manages access by roles. • SecurityPolicy: Sets system security rules. • Root Of Trust: Ensures authenticity of system components.
Product certificate (and/or keys) expired	An action has been performed on product certificate manually or through enrolment protocol. Standardized actions are specified in event result message.

Certificate Actions Tab

About EcoStruxure Control Expert Certificates

This topic describes the parameters and functions that are available in the **Certificate Actions** tab in the Security Editor tool. Access this tab to generate and share EcoStruxure Control Expert certificates. In a client/server relationship, these certificates are added to the **Certificate whitelist**, page 33 to help enforce security among the exchanges.

Create certificates:

- *automatically:* The **SecurityService** and **ControlExpert** certificates are generated automatically when you launch Security Editor for the first time.
- *manually:* Create a self-signed certificate in the **Certificate Actions** tab. The parameters for this tab are described below.

NOTE: This guide includes a use-case example that shows the functionality of Security Editor in a client-server relationship, page 17.

Element Descriptions

The commands on the **Certificate Actions** tab are applied to the manual creation of certificates:

Element	Description
Product (drop-down menu)	This document describes the Security Editor with respect to EcoStruxure Control Expert Classic.
General Self Signed Certificate (button)	Select **General Self Signed Certificate** to generate a self-signed certificate for products that require secure communications.
Export Certificate (button)	Select **Export Certificate** to export an existing certificate that is saved locally. **NOTE:** You can export a certificate only after you generate a certificate for a selection in the **Product** drop-down menu and select **General Self Signed Certificate**.
Certificate Properties (button)	Select **Certificate Properties** to open the **Certificate** dialog box. It contains detailed information about the certificate.

Generate a Self Signed Certificate

Generate certificates for **ControlExpert** or **SecurityService**:

Step	Action
1	On the server computer, select the **Certificate Actions** tab.
2	Make a selection in the from the **Product** drop-down menu: • **ControlExpert**: Generate a certificate for EcoStruxure Control Expert. • **SecurityService**: Generate a certificate for the security service when you run the service as a server. **NOTE:** A server requires a valid security service certificate to start. It is therefore possible that a server does not run even when the **SecurityService as server** parameter is selected. In this case, the *SecurityAdmin* user generates the certificate for the security service.
3	Select **Generate Self Signed Certificate** to generate and install the **ControlExpert** or **SecurityService** certificates in the local Windows certificate store.
4	Select **OK** to apply the modifications and close the Security Editor.
5	Optional: Hover the cursor over the icon to verify that the self-signed certificate was generated and saved to the certificate store.

Export a Certificate

From within the Security Editor, you can use one of these tools to export the certificate that you generated above:

- **Export Certificate** (in Security Editor)
- **Certificate Export Wizard:** (Windows tool)

Both procedures are described below.

Export Certificate:

Use **Export Certificate** to export a generated certificate from the local Windows certificate store:

Step	Action
1	Select **Export Certificate** to open a **Save As ...** dialog box.
2	Select a location and save the certificate.

Certificate Export Wizard:

Export a generated certificate with the Windows **Certificate Export Wizard:**

Step	Action
1	Select **Certificate Properties** to open the Windows **Certificate** properties dialog box.
2	Select the **Details** tab.
3	Select **Copy to File…** to open the home page for the Windows **Certificate Export Wizard**.
4	Click **Next** to go to the **Export Private Key** page.
5	Select **No, do not export the private key** and click **Next** to access the **Export File Format** page. **NOTE:** The Security Editor uses a Trusted Platform Module (TPM) to generate and store private keys and cannot export the private key with the certificate. Selecting **Yes** exports the private key results in an error on the final wizard page.
6	Select a file format and click **Next** to access the **File to Export** page.
7	Name the file and save it to an appropriate local location.
8	Click **Next** to go to the completion page and click **Finish** to complete the export.

NOTE: The **Certificate Properties** in the Security Editor tool opens the same *Certificate* (properties) dialog box for Windows that you open when you double-click a certificate in the *Microsoft Management Console*. Similarly, the **Copy to File** in the Security Editor tool opens the same *Certificate Export Wizard* for Windows that you open when you right-click a certificate in the *Microsoft Management Console* and scroll to *All Tasks* > *Export*.

Certificate whitelist Tab

Introduction

The **Certificate whitelist** tab in Security Editor displays a list of connections to remote servers that are trusted by personnel in the *SecurityAdmin* role.

Use the parameters on this tab to add trusted servers to the table.

NOTE:

- The use of bypass firewalls may be required to create a successful connection to the remote IP port of the server.
- This guide includes a use-case example that shows the functionality of Security Editor in a client-server relationship, page 17.
- To use the **Certificate whitelist** with Windows Server, activate **Network Discovery**.

EcoStruxure Control Expert Tasks

The **Certificate whitelist** requires a known IP address for a controller to connect to a remote server:

Step	Action
1	Open the **Set Address** dialog box in EcoStruxure Control Expert (**PLC > Set Address**) and make these selections in the **PLC** group box: • **Address: SYS** • **Communication Protocol: HTTPS via USB** Select **OK** to close the dialog box.
2	Connect to the controller (**PLC > Connect**).

Step	Action
3	Select **Upload Project** to open the **Transfer Project from PLC** dialog box.
4	Select **Transfer Project from PLC** and monitor the progress bar in the **Project transfer** pop-up window.
5	Open the **PLCScreen** window (**Tools > PLC Screen**) and select the **Information** tab to verify that the **NETWORK ADDRESS** is a USB connection.
6	Select **Disconnect**.
7	Launch the Security Editor and select the **Certificate whitelist** tab.

Select the ellipses (**...**) from any row in the whitelist to open the **Certificate** dialog box, access the **Details** tab, and view the properties and status of the certificate.

Add a Trusted Device

Before you retrieve the controller certificate, confirm that the endpoint security tool on your local computer is activated to allow groups to access the server for a set period of time.

Create a security service certificate and add it to the **Certificates whitelist** for a connection to a controller:

Step	Action
1	On the **Certificate whitelist** tab, select **Add** to open the **Add Server Address** dialog box.
2	Make a selection in the **Communication Protocol** drop-down menu: • **HTTPS** or **HTTPS via USB:** Use these protocols to add a controller to the **Certificate whitelist** table (through default port 443). • **TCPIP:** Use this protocol to add these devices to the **Certificate whitelist** table: ◦ another computer that runs Security Editor (default port: 50051) ◦ LDAP server (default port: 389) **NOTE:** • To approve a remote **SecurityService as server**, the Security Service client must be on the same network as the Security Service server. • You can whitelist a remote Security Server that runs as a server when the server is on the same network as the Security Service client.
3	Enter a port number (**Port**) that supports traffic from the server.
4	Select the plus sign (**+**) to display the connection in the table and reset the IP address to *0.0.0.0*.
5	Click **OK** to confirm that the new connection appears in the list of trusted remote servers and close the **Add Server Address** dialog box. **NOTE:** • Repeat these steps to create additional connections • When EcoStruxure Control Expert connects to a remote server, the implemented security database is that of the server. The selections in the **Authentication Mode** and **Centralized Protocol** drop-down menus on the **Login Policies** tab are therefore ignored, except when **LDAP** is selected from the **Centralized Protocol** menu.
6	Select the appropriate checkboxes for the new connections and select **Trust Certificates** to add the certificates to the security database and complete the whitelisting operation.

Management Buttons

Select these buttons in the **Connections** group box to manage items in the whitelist:

- **Add:** Open the **Add Server Address** dialog box.
- **Select All:** Select all items before you remove them from the table or to confirm their trusted status with **Trust Certificate**.
- **Unselect All:** Deselect all items in the table.
- **Remove:** Remove the selected item or items from the whitelist table.

After the certificate is obtained, the status of each connection is automatically updated.

Secured mode Tabs

Secured mode

Introduction

Secured mode is a read-only operational mode in which security configurations are managed through EcoStruxure Cybersecurity Admin Expert (CAE) and saved in the EcoStruxure Control Expert database.

This topic explains how to activate the **Secured mode**, create and import the security configuration from EcoStruxure Cybersecurity Admin Expert to EcoStruxure Control Expert on Modicon M580 controllers version 04.50 and any subsequent supporting version(s).

Installing EcoStruxure Cybersecurity Admin Expert

To install EcoStruxure Cybersecurity Admin Expert, refer to EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.

Creating and Exporting a Cybersecurity Configuration File

To create a security configuration file on EcoStruxure Cybersecurity Admin Expert, follow the steps below:

Step	Action
1	Open EcoStruxure Cybersecurity Admin Expert using credentials specified in the *Accessing CAE* section of EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.
2	Click ☰ to open the menu of EcoStruxure Cybersecurity Admin Expert.
3	Click **Projects** > **Create Project** to create a new project.
4	Type a name for the new project and set its **Architecture** to **Plant Automation**. Click **Save** to confirm. For more information, refer to *How to Manage Projects* in EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.
5	Click the book icon 📖 and select **Create User Account** to create a *SecurityAdmin* user account. Set the **Role(s)** of this new user to **SECADM**. This step is necessary to import the Cybersecurity Configuration file associated with the project to the Security Editor tool.
6	Set the **Role(s)** of this new user to **SECADM**. This step is necessary to import the Cybersecurity Configuration file associated with the project to the Security Editor tool. For more information, refer to *How to Manage Projects* in EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual and the *SecurityAdmin* User section, page 12.
7	Configure your project. For information on how to configure your project, refer to *How to Manage Projects* in EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.
8	Create at least one additional user account with an **ENGINEER**, **OPERATOR** or **VIEWER Role(s)**. By default, each role includes credentials that grant access to the **Secured mode** of EcoStruxure Control Expert. You can customize each Role, and you can also create new Roles. For more information, refer to *Roles Management* in EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.

Step	Action
9	Click ☰ to open the menu of EcoStruxure Cybersecurity Admin Expert.
10	Click the export project icon associated with your project.
11	Set a password to encrypt the exported file and click **Export**.
12	Click **Save** to confirm filename and location. For more information, refer to *How to Manage Projects* in EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.

Importing the Cybersecurity Configuration File

To activate the **Secured mode**, import the Cybersecurity Configuration file into the Security Editor tool:

Step	Action
1	Login to the Security Editor tool and select **Secured mode** from the box on the top-left of the interface.
2	Click **Yes** to confirm. **Result:** The login page of the Security Editor tool opens.
3	Login to the Security Editor tool again. **Result:** The drop-down menu displays **Secured mode**.
4	Click **Import and Apply CS Configuration**.
5	Select the configuration file and click **Open**.
6	In the **CS Configuration Password** window, enter the password created to decrypt the file and click **OK**. **Result:** The login page of the Security Editor tool opens.
7	Login to the Security Editor tool again, using the *SecurityAdmin* credentials created in EcoStruxure Cybersecurity Admin Expert. **Result:** The interface displays the Cybersecurity Configuration filename under **Current cs config filename :**.

NOTE: With a Cybersecurity Configuration file imported to the Security Editor tool, EcoStruxure Control Expert can only be launched in **Secured mode**, with a user profile and associated password defined in CAE. For additional information, refer to the Creating and Exporting a Cybersecurity Configuration File, page 36.

Activating Secure Configuration

Secure Configuration can only be activated in **Secured mode**.

To activate the **Secure Configuration** in EcoStruxure Control Expert, follow the steps below:

Step	Action
1	Login to EcoStruxure Control Expert software with an **ENGINEER**, **OPERATOR** or **VIEWER** user profile. For additional information, refer to the Creating and Exporting a Cybersecurity Configuration File, page 36.
2	Navigate to **Project Browser**.

Step	Action
3	Select **Project** > **Configuration** > expand the rack > expand the module > expand the controller > double click **EIO**. **Result:** The **EIO** window is displayed.
4	In the **Security** tab, inside the **Global policy** group, click the checkbox to select **Secure Configuration**.

Reverting to Standard mode

To deactivate the **Secured mode** and revert EcoStruxure Control Expert to **Standard mode**, follow the steps below:

Step	Action
1	Login to the Security Editor tool and select **Standard mode** from the box on the top-left of the interface.
2	Click **Yes** to confirm. **Result:** The login page of the Security Editor tool opens.
3	Login to the Security Editor tool again. **Result:** The drop-down menu displays **Standard mode**.
4	Launch EcoStruxure Control Expert.

Certificate Actions Tab

The **Certificate Actions** tab displays the status of the certificate associated with the cybersecurity configuration set up in EcoStruxure Cybersecurity Admin Expert for the EcoStruxure Control Expert Classic product.

The certificate icon on the left indicates if a self signed certificate is available or missing in the certificate store.

The certificate icon on the right presents the status of the cybersecurity configuration.

Use the available buttons to **Generate Self Signed Certificate**, **Export Certificate** (in .CER format), and display **Certificate Properties**.

For more information, refer to *Certificate Policy* in EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.

Users Tab

The **Users** tab presents the list of **Users** configured in EcoStruxure Cybersecurity Admin Expert for the EcoStruxure Control Expert Classic product.

For each **User**, **User Name** and **Role** are displayed, as well as a reminder of the **Password maximum duration**, expressed in days.

For more information, refer to *User Accounts* and *Roles Management* in EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.

Profiles Tab

The **Profiles** tab displays the profiles set up in EcoStruxure Cybersecurity Admin Expert for the EcoStruxure Control Expert Classic product.

By default, **ENGINEER**, **OPERATOR** and **VIEWER Profiles** are available.

Select one of the **Profiles** and click **View** to display the **Access right list** associated to the selected profile.

For more information, refer to *Roles Management* in EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.

Security Policy Tab

The **Security Policy** summarizes as a read-only table the elements associated with the cybersecurity configuration set up in the **SECURITY SETTINGS** menu of EcoStruxure Cybersecurity Admin Expert.

For more information, refer to *Security Configuration* in EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.

Login Policies Tab

The **Login Policies** tab displays the status of **Network SecurityService** associated with the cybersecurity configuration set up in EcoStruxure Cybersecurity Admin Expert.

It summarizes as read-only data **Authentication Mode**, **Centralized Protocol**, **LDAP Protocol Details** and **LDAP group(s)**, if applicable, as well as active **Profiles** and **Base DN**.

For more information, refer to *Security Configuration* in EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.

Certificate whitelist Tab

The **Certificate whitelist** tab displays the list of certificates associated with the cybersecurity configuration set up in EcoStruxure Cybersecurity Admin Expert.

For each available certificate, the table displays its **Issuer name**, **Expiration date**, **Distinguished Name**, **Property**, **Status** and **Thumbprint**.

For more information, refer to *Certificates Management* in EcoStruxure™ Cybersecurity Solution – Cybersecurity Admin Expert, User Manual.

Configure a Controller Through the Enforced Engineering Link

Introduction

When the *SecurityService* of the Security Editor runs on a server, it can establish secure connections to authorized clients only when the EcoStruxure Control Expert Classic project is configured for an application password. Follow the instructions below to create an application that is conducive to the client-server functionality of the Security Editor.

Configure a Controller Project

Use the instructions below when you have local computer that runs an EcoStruxure Control Expert Classic project that includes a single controller module:

Step	Action
1	In EcoStruxure Control Expert Classic, create a new project (**File > New**) to open the **New Project** dialog box.
2	Select a controller for the application and select **OK** to open the **Security enforcement** dialog box.
3	When prompted, create an **Application password** for the project and select **OK** to close the **Security enforcement** dialog box.
4	In the **PLC bus**, double-click the ports on the controller to open the submodule parameters.
5	Select the **Security** tab and select **Unlock Security** to activate all services.
6	Select **Enforced** from the **Engineering Link Mode** drop-down menu.
7	Configure an IP address for the project controller: **a.** Open the **Set Address** dialog box (**PLC > Set Address**). **b.** Select **MODBUS TCP** from the **Communication Protocol** drop-down menu. **c.** Select **OK** to close the **Set Address** dialog box.
8	Rebuild the project (**Build > Rebuild All Project**) and save the application (**File > Save**).
9	Download the project to the controller (**PLC > Transfer Project to PLC**).

When you open the EcoStruxure Control Expert Classic project in the future, you are prompted for the application password.

Change the Password: Change the password for a project or add a password to an existing (password-less) project:

Step	Action
1	Open an EcoStruxure Control Expert Classic project.
2	In the **Project Browser**, right-click **Project** and select **Properties** to open the **Properties of Project** dialog box.
3	Select the **Projects & Controller Protection** tab and select **Change password...** to open the **Modify Password** dialog box for the applicable password (**Application**, **Firmware**, **Web Diagnostic/Data Storage**).
4	Enter the password in the **New password** group box. **NOTE:** To change the password for a password-protected application, first enter the existing password in the **Old password** field.

Step	Action
5	Rebuild the project (**Build > Rebuild All Project**) and save the application (**File > Save**).
6	Select **OK** to apply the passwords and close the **Modify Password** dialog box.

Whitelist the Controller in Security Editor

With a configured Ethernet address, the controller automatically generates a certificate.

To configure EcoStruxure Control Expert Classic to communicate with the controller through an HTTPS connection, add the controller's certificate to the list of trusted devices on the **Certificates whitelist** tab, page 35.

Generate a Certificate for the Local Computer

The Security Editor can add another software program or device (for example, the *SecurityService* running on a remote computer, controller, LDAP server, etc.) to a whitelist only when it is identified by its unique certificate.

Generate the unique certificate for EcoStruxure Control Expert and the *SecurityService* with the Security Editor:

Step	Action
1	Using the Security Editor that runs on a local computer, select the **Certificate Actions** tab, page 31..
2	Select **SecurityService** (or **Control Expert**) from the **Product** drop-down menu.
3	Select **Generate Self Signed Certificate**, page 32.

NOTE: The certificates are generated at the first launch of the Security Editor. If necessary, you can manually generate a certificate. (Refer to the instruction to generate a certificate on the **Certificate Actions** tab, page 32.

Syslog Events

Activate Tracking

The Security Editor tool can use and manage syslog events.

activate the syslog service to track syslog events in the syslog server:

Step	Action
1	In the **Profile** tab, create a new profile for each applicable audit case.
2	In the **Policies** tab, select **Security on, no login** for the minimum amount of required security.
3	In the **Policies** tab, select the new profiles for the audit cases you want to monitor.
4	In the **Policies** tab, activate the **Audit** option to obtain the syslog messages for the activated events.

Recovery Procedure with a Detected Error

Introduction

Use the Security Editor tool to control access to EcoStruxure Control Expert and the loader management software. If an error occurs (for example, incorrect passwords or unauthorized access attempts), follow the appropriate recovery procedure for the situation.

Undefined User Access

These types of access are available when a user is not defined in the security database while security is activated:

Configuration	Access
Access is configured with an avoidable login (**Security On, avoidable login**).	The undefined user can access EcoStruxure Control Expert or the loader management software with the default profile.
Access is configured with a mandatory login (**Security On, mandatory login**).	The undefined user cannot access EcoStruxure Control Expert or the loader management software.

For Security Editor, access is set to a mandatory login (**Security On, mandatory login**) and cannot be modified. An undefined user cannot access Security Editor.

NOTE: If the database of the Security Editor is damaged or if it was deleted, access to EcoStruxure Control Expert or the loader management software is not possible, even with **Security Off**.

Availability of Security Components After Installing EcoStruxure Control Expert

The manner in which you install EcoStruxure Control Expert has an impact on the availability of the security components:

Installation Type	Results
Install	There is no action relative to the security components.
Repair	There is no action relative to the security components.
Upgrade	Moves the security database files to a backup folder to support a later migration of the database.
	Removes all other security components.
Remove	Removes all security components.

NOTE: The security components are created the first time you launch the Security Editor.

Lost Password

If you lose the password for the *SecurityAdmin* user, contact your Schneider Electric support representative.

EcoStruxure Control Expert Predefined Profiles

Introduction

This topic presents the available predefined profiles you can use to associate at user creation.

Predefined User Profiles

EcoStruxure Control Expert provides these user profiles:

Predefined Profile	Applicable Program Type	Description
ReadOnly	**Programs**	The user can only access the project in read mode, except for the controller address, which can be modified. The user can also copy or download the project.
	Programs-PROCESS	
	Program-SAFE	
Operate	**Programs**	The user has the same rights as with a **ReadOnly** profile, with the added possibility of modifying execution parameters (constants, initial values, task cycle times, etc.).
	Programs-PROCESS	
Safety_Operate	**Programs**	The user has similar rights as with the **Operate** profile, but with respect to the safety-related program, except that: • Transferring data values to the non-safety-related controller is not permitted. • Commanding the safety-related program to enter maintenance mode is permitted.
	Programs-PROCESS	
	Program-SAFE	
Adjust	**Programs**	The user has the same rights as with an **Operate** profile, with the added possibility of uploading a project (transfer to the controller) and modifying the controller operating mode (**Run**, **Stop**, ...).
	Programs-PROCESS	
Safety_Adjust	**Programs**	The user has similar rights as with the **Adjust** profile, but with respect to the safety-related program, except that: • Transferring data values to the non-safety-related controller is not permitted. • Commanding the safety-related program to enter maintenance mode is permitted.
	Programs-PROCESS	
	Program-SAFE	
Debug	**Programs**	The user has the same rights as with an **Adjust** profile, with the added possibility of using the debugging tools.
	Programs-PROCESS	
Safety_Debug	**Programs**	The user has similar rights as with the **Debug** profile with respect to the safety-related program, with these exceptions: • Stopping or starting the program is not permitted. • Updating initialization values is not permitted. • Transferring data values to the non-safety-related controller is not permitted. • Forcing inputs, outputs or internal bits is not permitted. • Commanding the safety-related program to enter maintenance mode is permitted.
	Programs-PROCESS	
	Program-SAFE	
Program	**Programs**	The user has the same rights as with a **Debug** profile, with the added possibility of modifying the program.
	Programs-PROCESS	
Safety_Program	**Programs**	The user has similar rights as with the **Program** profile, but with respect to the safety-related program, except that: • Stopping or starting the program is not permitted. • Updating initialization values is not permitted. • Transferring data values to the non-safety-related controller is not permitted. • Forcing inputs, outputs or internal bits is not permitted. • Commanding the safety-related program to enter maintenance mode is permitted.
	Programs-PROCESS	
	Program-SAFE	

Predefined DTM roles (access rights to modify DTMs) are associated with the user profiles. Preconfigured user profiles are associated with specific DTM roles, and a new user profile is associated with a selected DTM role. This table shows the correspondence between profile names and DTM roles:

User Profile	DTM Role
SecurityAdmin	**Administrator**
Adjust	**SystemOperator**
Debug	**MaintenanceEngineer**
Operate	**SystemOperator**
Program	**PlanningEngineer**
ReadOnly	**SystemObserver**
Safety_Adjust	**SystemOperator**
Safety_Debug	**MaintenanceEngineer**
Safety_Operate	**SystemOperator**
Safety_Program	**PlanningEngineer**

NOTE:

- Refer to the directions for creating a new user profile, page 22.
- When you map a DTM role to a user profile, choose the role that best corresponds to the access rights for that profile.

EcoStruxure Control Expert Classic Access Rights

Project Services

These access rights define the actions that users can perform for project services:

Access right	Description
create a new project	Create a new project.
open an existing project	Open an existing project.
save a project	Save the open project.
save as a project	Save the project with a new name or to a new location.
import a project	Import a project. (A partial import is considered a program modification.)
build off-line	Launch a generation of the executable in offline mode.
build on-line stop	Launch a generation of the executable in online mode when the controllers are de-energized.
build on-line run	Launch a generation of the executable in online mode when the controllers energized.
start stop or initialize the PLC	Command the controller to energize, de-energize, or initialize. **NOTE:** Only process tasks are started or stopped: • For a non-safety-related controller, controller starts or stops. • For a Modicon M580 Safety controller, tasks other than the SAFE task start or stop.
Update init values with current values	Update the initial values with the latest values (only non-safety-related data).
transfer project from PLC	Transfer the executable program from the controller to the terminal.
transfer project to PLC	Transfer the executable program from the terminal to the controller.
transfer data values from file to PLC	Transfer data from a file to the controller (non-safety-related data only).
restore project backup in PLC	Restore the contents of backup memory (Modicon Premium) or the memory card (Modicon M340 and Modicon M580) in the controller executable area. **NOTE:** On Modicon M580, you can save to flash memory if no memory card is inserted.
save to project backup in PLC	Save the project program in the backup memory (Modicon Premium) or the memory card (Modicon M340 and Modicon M580). **NOTE:** On Modicon M580, restore from flash memory if no memory card is inserted.
Set address	Access a controller through the network.
Modify options	Modify project attributes.

Adjustment/Debugging

These access rights define actions that users can perform for adjustments and debugging:

Access right	Description
Modify variable values	Modify the value of the variables (non-safety-related variables only).
Modify safety variable values	Modify the value of the safety-related variables.
Force internal bits	Force internal bits.
Force outputs	Force outputs.
Force inputs	Force inputs.
Task management	Command the execution of project program tasks (energize, de-energize; initialization).

Access right	Description
SAFE task management	Command the execution of safety project program SAFE tasks (energize, de-energize, initialization).
Task cycle time modification	Modify cycle times for cyclical tasks.
SAFE task cycle time modification	Modify cycle times for cyclical SAFE tasks.
Suppress message in diag viewer	Delete the message displayed in the viewer.
Debug executable	Debug the executable program.
Replace project variable	Replace all occurrences of a variable in the program with another variable (non-safety-related variables only).
Replace safety project variable	Replace all occurrences of a safety-related variable in the program with another.

Libraries

These access rights define actions that users can perform for libraries:

Access right	Description
Create libraries or families	Create libraries or families of user functions.
Create safety libraries or families	Create safety-related libraries or families of user functions.
Delete libraries or families	Delete libraries or families of user functions.
Delete safety libraries or families	Delete safety-related libraries or families of user functions.
Put object into library	Insert an object in a library.
Put an object from the safety library	Insert an object in a safety-related library.
Delete object from library	Delete an object from a library.
Delete an object from safety library	Delete an object from a safety-related library.
Get object from library	Import an object from a library to the project.
Get an object from the safety library	Import an object from a safety-related library to the project.

Global Modification

These access rights define actions that users can perform for global modifications:

Access right	Description
Modify documentation	Modify the documentation.
Modify functional view	Create, delete, or modify a functional module.
Modify animation tables	Modify the structure (not the values) of animation tables.
Modify constant values	Modify the value of the project constants.
Modify safety constant values	Modify the value of the safety project constants.
Modify the program structure	Modify the executable code structure (add/delete a section; modify the activation conditions for a section; modify section order.)
Modify the safety program structure	Modify the safety executable code structure (add/delete a section; modify the activation conditions for a section; modify section order.)
Modify program sections	Modify the executable code for a section.
Modify safety program sections	Modify the executable code for a section in the safety program.
Modify Project settings	Modify the generation options.
Modify safety project settings	Modify the safety project settings.

Elementary Modification of Variables

These access rights define actions that users can perform for elementary modifications of variables:

Access right	Description
Variable Add Remove	Add or delete a variable.
Safety Variables add remove	Add or delete a safety-related variable.
Variable Main Attributes modification	Modify a variable's name, type, and address.
Safety Variables Main Attributes Modification	Modify a safety-related variable's name, type, and address.
Variable Minor Attributes modification	Modify the comment and the initial value for a variable.
Safety Variables Minor Attributes Modification	Modify the comment and the initial value for a safety-related variable.

Elementary Modification of Device DDT Compound Data

These access rights define actions that users can perform for elementary modifications of a device DDT compound data:

Access right	Description
DDT Add Remove	Add or delete a compound data item.
DDT modification	Modify the structure, comment, and initial value of a compound data item.
Safety DDT modifications	Modify the structure, comment, and initial value of a safety compound data item.

Elementary Modification of a DFB Type

These access rights define actions that users can perform for elementary modifications of DFB variables:

Access right	Description
DFB type Add Remove	Add or delete a DFB type.
Safety DFB Type add remove	Add or delete a safety DFB type.
DFB type structure modification	Modify the structure of a DFB type.
Safety DFB Type structure modification	Modify the structure of a safety DFB type.
DFB type sections modification	Modify the code section of a DFB type.
Safety DFB type section modification	Modify the code section of a safety DFB type.

Elementary Modification of a DFB Type Instance

These access rights define actions that users can perform for elementary modifications of DFB type instances:

Access right	Description
DFB instance Modification	Add, delete, or modify (name and type) a DFB instance.
Safety DFB Type instance modification	Add, delete, or modify (name and type) a safety DFB instance.
DFB instance Minor Attributes modification	Modify the comment and the initial value for a DFB instance.
Safety DFB Type Minor Attributes modification	Modify the comment and the initial value for a safety DFB instance.

Bus Configuration Editor

These access rights define actions that users can perform in the bus configuration:

Access right	Description
Modify configuration	Modify the configuration.
Modify safety configuration	Modify the safety configuration.
IO sniffing	Execute bus configuration sniffing.

Input/Output Configuration Editor

These access rights define the actions that users can perform in the input/output configuration:

Access right	Description
Modify the IO configuration	Modify the input/output configuration.
Modify the safety I/O configuration	Modify the safety input/output configuration.
Adjust the IO	Adjust inputs/outputs.
Adjust the safety I/O	Adjust safety inputs/outputs.
Save param	Save the module input/output parameters explicitly. (The initial parameter values are replaced by the latest values).
Restore param	Restore the module input/output parameters explicitly. (The initial parameter values are replaced by the latest values).

Runtime Screens

These access rights define the actions that users can perform on runtime screens:

Access right	Description
Modify screens	Modify runtime screens.
Modify messages	Modify runtime messages.
Add/Remove screens or families	Add or delete a runtime screen.

Cybersecurity

These access rights define the actions that users can perform for cybersecurity functions:

Access right	Description
Create or modify application password	Create and modify the application password.
Enter Maintenance mode	Enter maintenance mode.
Adapt Auto-Lock timeout	Adapt the Auto-Lock timeout.

EcoStruxure Control Expert Classic Access Rights Assigned to Predefined Profiles

Project Services

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
create a new project	–	–	–	–	–	–	–	✓	✓
open an existing project	✓	✓	✓	✓	✓	✓	✓	✓	✓
save a project	–	–	–	–	–	–	–	✓	✓
save as a project	✓	✓	✓	✓	✓	✓	✓	✓	✓
import a project	–	–	–	–	–	–	–	✓	✓
build off-line	–	–	–	–	–	–	–	✓	✓
build on-line stop	–	–	–	–	–	–	–	✓	✓
build on-line run	–	–	–	–	–	–	–	✓	✓
start stop or initialize the PLC	–	✓	–	✓	–	–	–	✓	✓
Update init values with current values	–	–	–	✓	–	–	–	✓	✓
transfer project from PLC	✓	✓	✓	✓	✓	✓	✓	✓	✓
transfer project to PLC	–	✓	✓	✓	✓	–	–	✓	✓
transfer data values from file to PLC	–	✓	–	✓	–	✓	–	✓	✓
restore project backup in PLC	–	–	–	–	–	–	–	✓	✓
save to project backup in PLC	–	–	–	–	–	–	–	✓	✓
Set address	✓	✓	✓	✓	✓	✓	✓	✓	✓
Modify options	–	✓	✓	✓	✓	✓	✓	✓	✓

✓ Included

– not included

Adjustment/Debugging

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
Modify variable values	–	✓	–	✓	–	✓	–	✓	✓
Modify safety variable values	–	–	✓	–	✓	–	✓	–	✓
Force internal bits	–	–	–	✓	–	–	–	✓	✓
Force outputs	–	–	–	✓	–	–	–	✓	✓
Force inputs	–	–	–	✓	–	–	–	✓	✓
Task management	–	–	–	✓	–	–	–	✓	✓
SAFE task management	–	–	–	–	✓	–	–	–	✓
Task cycle time modification	–	✓	–	✓	–	✓	–	✓	✓
SAFE task cycle time modification	–	–	✓	–	✓	–	✓	–	✓
Suppress message in diag viewer	–	✓	✓	✓	✓	✓	✓	✓	✓
Debug executable	–	–	–	✓	✓	–	–	✓	✓
Replace project variable	–	–	–	–	–	–	–	✓	✓
Replace safety project variable	–	–	–	–	–	–	–	–	✓
✓ Included – not included									

Libraries

The access rights for this category are as follows:

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
Create libraries or families	–	–	–	–	–	–	–	✓	✓
Create safety libraries or families	–	–	–	–	–	–	–	–	✓
Delete libraries or families	–	–	–	–	–	–	–	✓	✓
Delete safety libraries or families	–	–	–	–	–	–	–	–	✓
Put object into library	–	–	–	–	–	–	–	✓	✓
Put an object from the safety library	–	–	–	–	–	–	–	–	✓
Delete object from library	–	–	–	–	–	–	–	✓	✓
Delete an object from safety library	–	–	–	–	–	–	–	–	✓
Get object from library	–	–	–	–	–	–	–	✓	✓
Get an object from the safety library	–	–	–	–	–	–	–	–	✓
✓ Included – not included									

Global Modification

The access rights for this category are as follows:

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
Modify documentation	–	✓	✓	✓	✓	✓	✓	✓	✓
Modify functional view	–	–	–	–	–	–	–	✓	✓
Modify animation tables	✓	✓	✓	✓	✓	✓	✓	✓	✓
Modify constant values	–	✓	–	✓	–	✓	–	✓	✓
Modify safety constant values	–	–	✓	–	✓	–	✓	–	✓
Modify the program structure	–	–	–	–	–	–	–	✓	✓
Modify the safety program structure	–	–	–	–	–	–	–	–	✓
Modify program sections	–	–	–	–	–	–	–	✓	✓
Modify safety program sections	–	–	–	–	–	–	–	–	✓
Modify Project settings	–	–	–	–	–	–	–	✓	✓
✓ Included **–** not included									

Elementary Modification of a Variable

The access rights for this category are as follows:

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
Variable Add Remove	–	–	–	–	–	–	–	✓	✓
Safety Variables add remove	–	–	–	–	–	–	–	–	✓
Variable Main Attributes modification	–	–	–	–	–	–	–	✓	✓
Safety Variables Main Attributes Modification	–	–	–	–	–	–	–	–	✓
Variable Minor Attributes modification	–	✓	–	✓	–	✓	–	✓	✓
Safety Variables Minor Attributes Modification	–	–	✓	–	✓	–	✓	–	✓
✓ Included **–** Not included									

Elementary Modification of Device DDT Compound Data

The access rights for this category are as follows:

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
DDT Add Remove	–	–	–	–	–	–	–	✓	✓
DDT modification	–	–	–	–	–	–	–	✓	✓

✓ Included

– not included

Elementary Modification of a DFB Type

The access rights for this category are as follows:

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
DFB type Add Remove	–	–	–	–	–	–	–	✓	✓
Safety DFB Type add remove	–	–	–	–	–	–	–	–	✓
DFB type structure modification	–	–	–	–	–	–	–	✓	✓
Safety DFB Type structure modification	–	–	–	–	–	–	–	–	✓
DFB type sections modification	–	–	–	–	–	–	–	✓	✓
Safety DFB type section modification	–	–	–	–	–	–	–	–	✓

✓ Included

– not included

Elementary Modification of a DFB Instance

The access rights for this category are as follows:

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
DFB instance Modification	–	–	–	–	–	–	–	✓	✓
Safety DFB Type instance modification	–	–	–	–	–	–	–	–	✓
DFB instance Minor Attributes modification	–	✓	–	✓	–	✓	–	✓	✓
Safety DFB Type Minor Attributes modification	–	–	✓	–	✓	–	✓	–	✓

✓ Included

– not included

Bus Configuration Editor

The access rights for this category are as follows:

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
Modify configuration	–	–	–	–	–	–	–	✓	✓
Modify safety configuration	–	–	–	–	–	–	–	–	✓
IO sniffing	–	–	–	–	–	–	–	✓	✓
✓ Included – not included									

Input/Output Configuration Editor

The access rights for this category are as follows:

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
Modify the IO configuration	–	–	–	–	–	–	–	✓	✓
Modify the safety I/O configuration	–	–	–	–	–	–	–	–	✓
Adjust the IO	–	✓	–	✓	–	✓	–	✓	✓
Adjust the safety I/O	–	–	✓	–	✓	–	✓	–	✓
Save param	–	–	–	✓	–	–	–	✓	✓
Restore param	–	–	–	✓	–	–	–	✓	✓
✓ Included – not included									

Runtime Screens

The access rights for this category are as follows:

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
Modify screens	–	–	–	–	–	–	–	✓	✓
Modify messages	–	–	–	–	–	–	–	✓	✓
Add/Remove screens or families	–	–	–	–	–	–	–	✓	✓
✓ Included – not included									

Cybersecurity

The access rights for this category are as follows:

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
Create or modify application password	–	–	–	–	–	–	–	✓	✓
Enter Maintenance mode	–	–	✓	–	✓	–	✓	–	✓
Adapt Auto-Lock timeout	–	✓	✓	✓	✓	✓	✓	✓	✓

✓ Included

– not included

OS Loader Access Rights

Introduction

This topic presents the available access rights for OS Loader product.

Description

The OS Loader access rights are as follows:

Access right	Description
Sniffing	You can launch a sniffing program on the network.
Connect/disconnect	You can connect/disconnect OS Loader to a device.
Read Device Properties	You have access to the device properties.
Read Executive Properties	You have access to the OS properties
Start/Stop	You can start/stop controller.
Upload executive	You can upload OS from device
Download executive	You can download OS to device

Assigned OS Loader Access Rights to Predefined Profiles

Introduction

This topic presents the access rights assigned to the predefined profiles.

Project services

Access right	ReadOnly			Program		
	State	Audit	Confirm	State	Audit	Confirm
Sniffing	✓	Yes	No	✓	No	No
Connect/disconnect	✓	Yes	No	✓	No	No
Read Device Properties	✓	Yes	No	✓	No	No
Read Executive Properties	✓	Yes	No	✓	No	No
Start/Stop	–	Yes	No	✓	No	No
Upload executive	✓	Yes	No	✓	No	No
Download executive	–	Yes	No	✓	No	No
✓ Included – not included						

Security Database Migration Tool

Migration Procedure

The first time you launch the Security Editor, you are prompted to migrate an existing security database. You can follow the prompts or choose to migrate an existing database during a subsequent login.

Throughout the procedure below, accept the on-screen prompts to proceed with the migration.

Migrate a security database:

Step	Action
1	Launch the tool with one of these methods: • Type *Security Database Migration Tool* in the Windows search box. • Double-click the executable file for the tool (SecDBConv.exe) in your downloaded EcoStruxure Control Expert program folder.
2	When prompted, log in to the previous database by entering the access credentials for the *SecurityAdmin* account, page 12 on the Security Database Migration Tool login page. **NOTE:** In legacy versions of EcoStruxure Control Expert (earlier than version 15.3), use the credentials for the Supervisor (*super user*) account, as discussed in the description of the migration of the administrator role.
3	Select **Login** and accept any prompt to log in to the active database.
4	Enter the access credentials for the same administrative user as above on the Security Database Migration Tool login page.
5	Select **Login** and wait for confirmation that the previous data are migrated to the active database.

NOTE: You can confirm that the database is migrated by verifying that the appropriate data appears on the tabs in the Security Editor.

Index

C

Control Expert
access rights 46
Security Editor 46

O

OS Loader
access rights 57
security editor 57
OS Loader
predefined user profiles 58

Schneider Electric
1884 Boulevard de la Défense
92000 Nanterre
France

www.se.com

© 2026 Schneider Electric. All rights reserved.

EIO0000004105.05