EcoStruxure™ Control Expert

Security Editor Operation Guide

Original instructions

09/2020

EIO0000004105.00

www.schneider-electric.com

Schneider Electric

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

Table of Contents

Safety Information

Important Information

NOTICE

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.

About the Book

At a Glance

Document Scope

This manual describes the Security Editor tool implementation.

Validity Note

This documentation is valid for EcoStruxure™ Control Expert 15.0 or later.

Related Documents

Title of documentation	Reference number
EcoStruxure™ Control Expert, Installation Manual	35014792 (English), 35014793 (French), 35014794 (German), 35014795 (Spanish), 35014796 (Italian), 35012191 (Chinese)

You can download these technical publications and other technical information from our website at *www.schneider-electric.com/en/download*.

Product Related Information

⚠ **WARNING**

UNINTENDED EQUIPMENT OPERATION

The application of this product requires expertise in the design and programming of control systems. Only persons with such expertise are allowed to program, install, alter, and apply this product.

Follow all local and national safety codes and standards.

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

Chapter 1
Security Editor Tool Implementation

Subject of this chapter

This chapter describes the Security Editor tool implementation.

What Is in This Chapter?

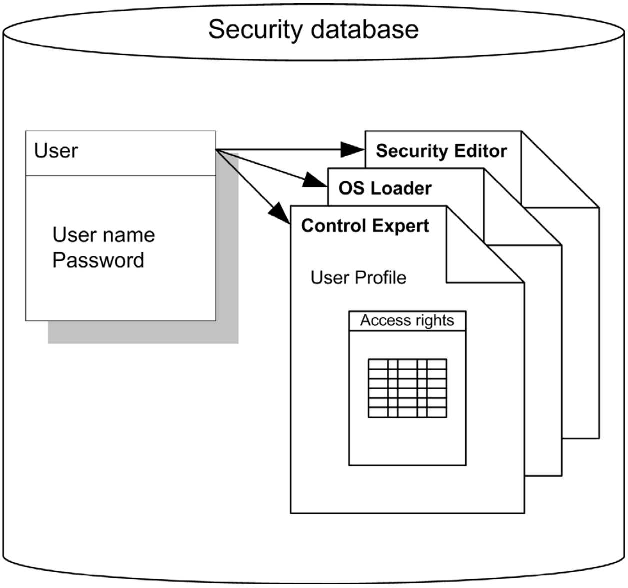
This chapter contains the following topics:

Access Security Management

At a Glance

Security Editor tool lets you limit and control access to the Control Expert and OS Loader software different functionalities.

The access security is managed by the security database which defines the users, user profiles, and user access rights:



NOTE: Protected access to the Control Expert and OS Loader software is optional.

Control Expert access security concerns the terminal on which the software is installed and not the project, which has its own protection system.

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

Supervisor (super user)

After installation of EcoStruxure Control Expert software on a workstation, only the predefined user name **supervisor** can access the security configuration without any limitation of rights (without a password).

⚠ **WARNING**

UNINTENDED EQUIPMENT OPERATION

Immediately define a secure password for user name **supervisor**.

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

A super user has a supervisor profile. The super user is the only person with rights to manage the access security database. The super user defines the list including the names of users who can access the software and their access rights.

NOTE: The user name reserved for the super user is Supervisor.

With access right **maintain product security** enabled, the super user can:

- create or modify the user list,
- create or modify user profiles,
- disable one or more users,
- modify the rules for software access security,
- modify his password,
- reset user passwords.

Users

Users are defined by the super user.

When access security is active and If your name is in the user list, you can access a software instance by entering your name (exactly as it appears on the list) and your password.

In Security Editor, a user has the following rights:

- access the rights defined by his profile in read mode,
- modify his password.

User Profile

The profile for a user comprises all of his access rights. It is defined by a name (2 to16 characters), 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 super user can create all the personalized profiles that he requires.

Predefined Users and User Profiles

Security Editor provides 10 predefined users and 10 predefined profiles that cannot be modified.

The following table gives the matrix predefined users / products / predefined profiles:

Predefined User	Product		
	Security Editor	Control Expert	OS Loader
safety_user_Adjust	ReadOnly	Safety_Adjust	—
safety_user_Debug	ReadOnly	Safety_Debug	—
safety_user_Operate	ReadOnly	Safety_Operate	—
safety_user_Program	ReadOnly	Safety_Program	—
supervisor	Supervisor	—	—
user_Adjust	ReadOnly	Adjust	—
user_Debug	ReadOnly	Debug	—
user_Operate	ReadOnly	Operate	—
user_Program	ReadOnly	Program	Program
user_ReadOnly	ReadOnly	ReadOnly	ReadOnly
— No access to the product for the predefined user when access security is active.			

Default User Profile

When the software access security is active, the super user can authorize a given user to open the software instance without having to enter his name and password. In this case, this user has a default profile.

Log Information Generated by the Security Editor

Security editor log information is managed by the Microsoft Windows **Event Viewer**. If you want to display the log information, launch the event viewer. Here you can filter according to all the **server sequential** events.

You can use all the Event viewer functions, like **sort**, **filter** etc.

Confirm

If this option is chosen by the super user, enter your name and password each time secure access is defined for a user action.

Multiple Instancing

When Control Expert executes multiple instances concurrently on the same terminal, each of these instances grants access to the functions that were defined by the rights of the user who created this instance. However, the Control Expert access method used (inactive security or type of active security) is identical for all the instances.

Centralized Security Database

EcoStruxure Control Expert is based on a client-server architecture. For more information on Control Expert client - server architecture, refer to *EcoStruxure™ Control Expert, Installation Manual*.

To administrate a centralized security database the super user (**supervisor**):

- defines users, user profiles, and user access rights on the remote Topology Manager server.
- deploys the centralized security database to the client workstations.

Security Editor tool automatically installed with Control Expert handle its own local security database.

To get the centralized security database on a local workstation you need to connect once to the remote topology manager server. When connected the centralized security database overwrites the local security database on the local workstation.

A backup of the local security database can be performed and restored when you connect back to the local topology server.

A popup window appears at connection to the remote topology manager and lets you choose to **perform the backup** of your local security database.

A popup window appears at connection back to the local topology manager and lets you choose to **restore your local backup** security database. To restore the local security database you must be identified as a the super user for the local security database.

NOTE: If the centralized security database is locked (update is in progress for example), the copy of the centralized security database is not performed.

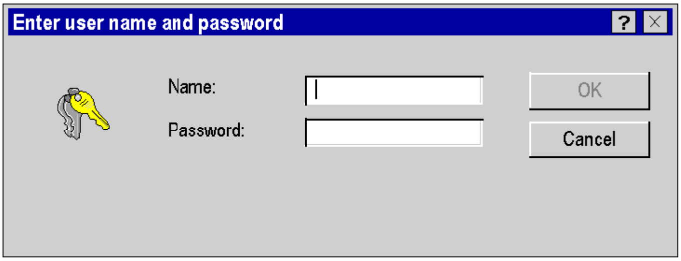
Security editor

At a Glance

The security editor is used to define software users and their access rights. It also allows you to define actions which are protected (user name and password) and which are stored in the log file.

Launching the security editor.

Execute the following commands to start security editor:

Step	Action
1	Open with **Start** → **Programs** → **EcoStruxure Control Expert** → **Security Editor**.The following dialog appears:  Enter user name and password Name: Password:
2	Enter your name and password.
3	Confirm with **OK**.
4	If you are a user *(see page 11)*, you can access the User information screen *(see page 15)* which allows you to consult your user profile or to modify your password.
5	If you are the Super User (Supervisor) *(see page 11)* the Security Editor *(see page 15)* will launch enabling administration of software access security.

NOTE: The user name reserved for the super user is Supervisor.

User Information

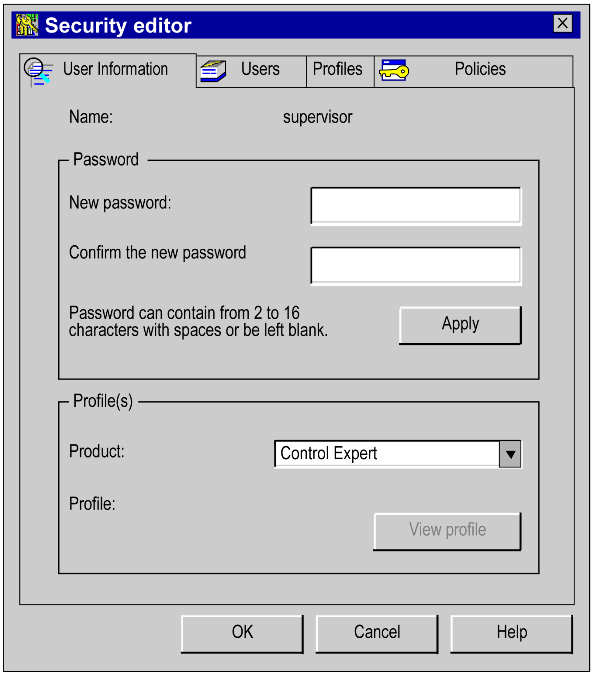
At a Glance

This tab in the security editor can be accessed by all users. It enables the execution of the following functions:

- modify a password. Users, including the super user, can only modify their own passwords,
- consult a profile and the associated user rights.

User information tab

The **User Information** looks as follows. It indicates the name of the user and contains the two sections **Password** and **Profile**:



Security editor

Name: supervisor

Password

New password:

Confirm the new password

Password can contain from 2 to 16 characters with spaces or be left blank.

Profile(s)

Product: Control Expert

Profile:

Description of the parameters

Password field,

Parameter	Description
New password	Data entry field for the new password: 2 to 16 characters. This field can be empty (no characters entered). **NOTE:** A password is mandatory for validating a user authentication in Control Expert Topology Manager *(see page 30)* when security is on.
Confirm the new password	Confirmation field for the new password. The contents of this field has to be identical to that of the **New password** field.
Apply	Command used to apply the new password. **Note**: The new password is entirely acknowledged only if it is validated with the **OK** command. Clicking **Cancel** cancels acknowledgment of the new password.

Profile(s) field

Parameter	Description
Product	Enables the selection of the product for which you want to display your user profile.
Profile	Shows the name of your user profile for the product.
View profile	Use this command to display all of the access rights included in your user profile.

User Functions

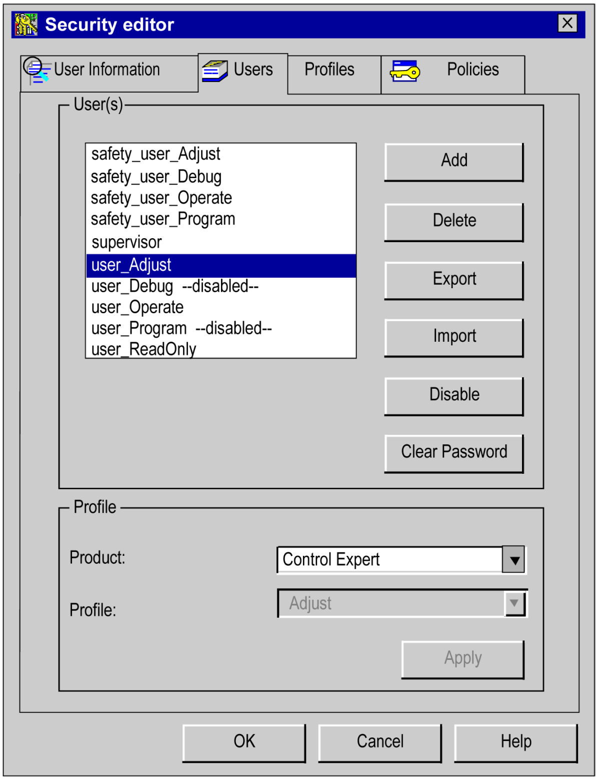
At a Glance

Only the super user *(see page 11)* (**supervisor**) can access this tab. It enables the execution of the following functions:

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

Users tab

The **User** tab looks like this. It contains the two areas **User(s)** and **Profile**:



safety_user_Adjust
safety_user_Debug
safety_user_Operate
safety_user_Program
supervisor
user_Adjust
user_Debug --disabled--
user_Operate
user_Program --disabled--
user_ReadOnly

Product: Control Expert

Profile: Adjust

Description of the parameters

Users field

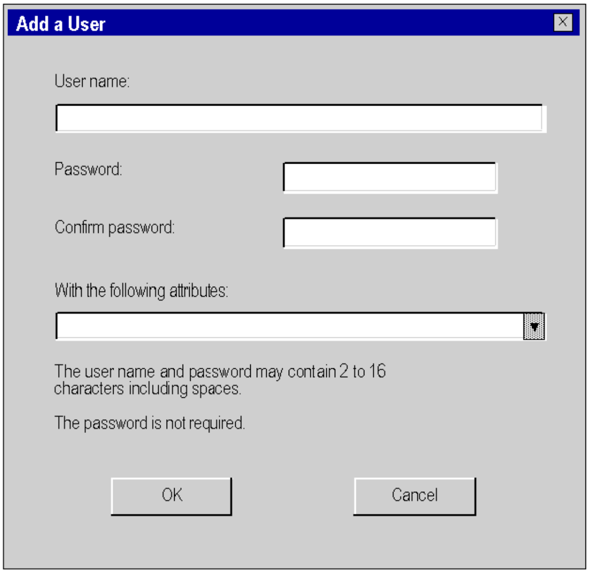
Parameter	Description
Users	List of users declared in the security database, including Predefined users *(see page 12)*.
Add	Command used to add a new user to the list.
Delete	Command used to delete the selected user(s) from the list. **NOTE:** Predefined users cannot be deleted.
Export	Command used to export the information (name and profiles) of the selected user(s) to a file. Passwords are not exported.
Import	Command used to import the information (name and profiles) of the selected user(s) from a file. If a user is already on the list, a warning message is displayed.
Disable/Enable	Command used to disable selected users. A disabled user is blocked at user authentication when security is on *(see page 25)*. One or more users can be selected. You are asked whether the user or users should really be disabled prior to disabling them. **Disable** is not possible for the user **supervisor**. If a user has been disabled, the user name is completed with **--disabled--** in user(s) list. If a disabled user attempts to start a software, the **User disabled** message appears.
Clear Password	Command used to delete passwords for selected users such as when a user forgot his password. **Clear Password** is not possible for predefined users.

Profiles field

Parameter	Description
Product	Used to choose the product whose user profile you would like to define.
Profile	Used to choose the profile that is assigned to the selected user and selected product. **NOTE:** The matrix predefined users / products / predefined profiles cannot be modified.
Apply	Command used to apply the profile assignment. The profile is entirely acknowledged only if it is validated with the **OK** command. Clicking **Cancel** cancels assignment of the profile.

Adding a user

Clicking **Add** displays the following dialog window:



The user name and password may contain 2 to 16 characters including spaces.

The password is not required.

2 data entry fields are provided:

Parameter	Description
User name	This field is used to enter the name of the new user (2 to 16 characters). If the name entered is not correct, or if it exists already, a warning message is displayed.
Password	Data entry field for the password: 2 to 16 characters. This field can be empty (no characters entered) at user creation.
Confirm password	Confirmation field for the password. The contents of this field has to be identical to that of the **Password** field.
With the following attributes	Field used to select the user whose attributes you would like to retrieve.

User Profiles

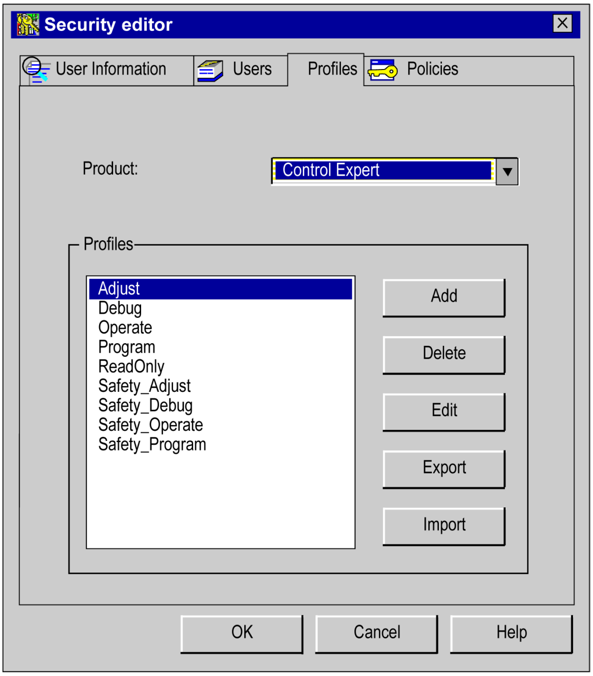
At a Glance

Only the super user *(see page 11)* (**supervisor**) can access this tab. It is used to perform the following functions:

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

“Profiles” Tab

The **Profiles** tab looks as follows. It features the **Product** and **Profiles** areas:



Product: Control Expert

Profiles

Adjust
Debug
Operate
Program
ReadOnly
Safety_Adjust
Safety_Debug
Safety_Operate
Safety_Program

Description of the parameters

Product area:

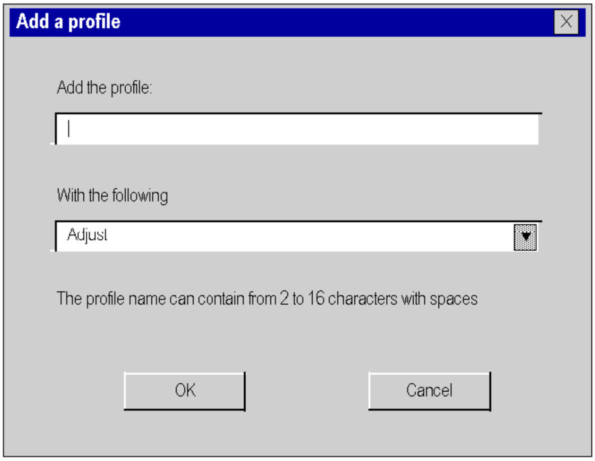
Parameter	Description
Product	Used to specify the product whose user profile you would like to access.

Profiles area:

Parameter	Description
Profiles	List of user profiles associated with the selected product.
Add	Command used to add a new user profile to the list.
Delete	Command used to delete one or more selected user profiles from the list. If you delete a profile from the list, users with this profile have the default profile. **NOTE:** Preconfigured user profiles cannot be deleted from the list.
Edit	Command used to modify access rights associated with the selected user profile. **NOTE:** Predefined user profiles cannot be modified.
Export	Command used for exporting to a file the information (name and profiles) of the selected user profile(s).
Import	Command used for importing from a file the information (name and profiles) of the selected user profile(s). If a user profile is already on the list, a warning message is displayed.

Adding a user profile

Use the **Add** command to display the following dialog box:



Add a profile

Add the profile:

With the following: Adjust

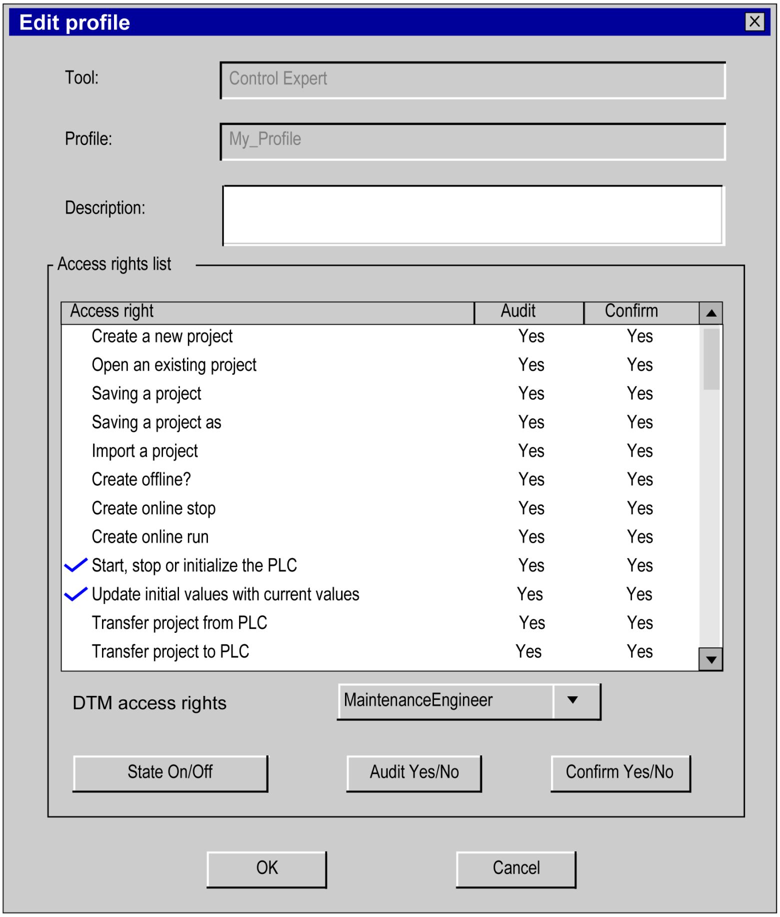
The profile name can contain from 2 to 16 characters with spaces

2 data entry fields are provided:

Parameter	Description
Add the profile	This field is used to enter the name of the new user profile (2 to16 characters). If the name entered is not correct, or if it exists already, a warning message is displayed.
With the following	Field used to choose the user profile whose attributes you would like to retrieve.

Modifying a user profile

Use the **Edit** command to display the following dialog box:



Tool: Control Expert

Profile: My_Profile

Description:

Access rights list

	Access right	Audit	Confirm
	Create a new project	Yes	Yes
	Open an existing project	Yes	Yes
	Saving a project	Yes	Yes
	Saving a project as	Yes	Yes
	Import a project	Yes	Yes
	Create offline?	Yes	Yes
	Create online stop	Yes	Yes
	Create online run	Yes	Yes
✓	Start, stop or initialize the PLC	Yes	Yes
✓	Update initial values with current values	Yes	Yes
	Transfer project from PLC	Yes	Yes
	Transfer project to PLC	Yes	Yes

DTM access rights: MaintenanceEngineer

4 areas are provided for display or data entry:

Parameter	Description
Tool	Shows the name of the product that you selected in the previous screen.
Profile	Shows the user profile name that you selected in the previous screen.
Description	This data entry field is used to associate a comment with the user profile modification.

Parameter	Description
Access rights list	This list displays the product access rights associated with the selected user profile. ● **Access right**: List of product access rights associated with the user profile. **NOTE:** The check box **Display Safety rights** allows to show or hide the safety access rights in the list of access rights displayed for Control Expert. There is no safety access rights for OS Loader nor Security Editor. ● **DTM access rights** (only for Control Expert product): Select the DTM access right role among the 5 following types: ○ **SystemObserver** ○ **SystemOperator** ○ **MaintenanceEngineer** ○ **PlanningEngineer** ○ **Administrator** ● **State On/Off**: This option is used to enable/disable a designated right for the current profile. To enable/disable the right: ○ Select **Access right** in the list. ○ Click **State On/Off**: the selection mark appears/disappears. ● **Audit Yes/No**: When this option is enabled, it enables an operation to be stored in the log file. To enable/disable the option for the corresponding access right: ○ Select **Access right** in the list. ○ Click **Audit Yes/No**. ● **Confirm Yes/No**: Enable this option to require a confirmation for an operation. To enable/disable the option for the corresponding access right: ○ Select **Access right** in the list. ○ Click **Confirm Yes/No**.

NOTE: You can view the access rights and DTM access rights associated with a preconfigured profile, but you cannot modify them.

DTM access rights for Control Expert. Select **PlanningEngineer** or **Administrator** role if one of the following user access right is enabled:

- **create a new project**
- **build off-line**
- **build on-line stop**
- **build on-line run**
- **Modify Project settings**
- **Variable Add Remove**
- **DDT Add Remove**

Policies

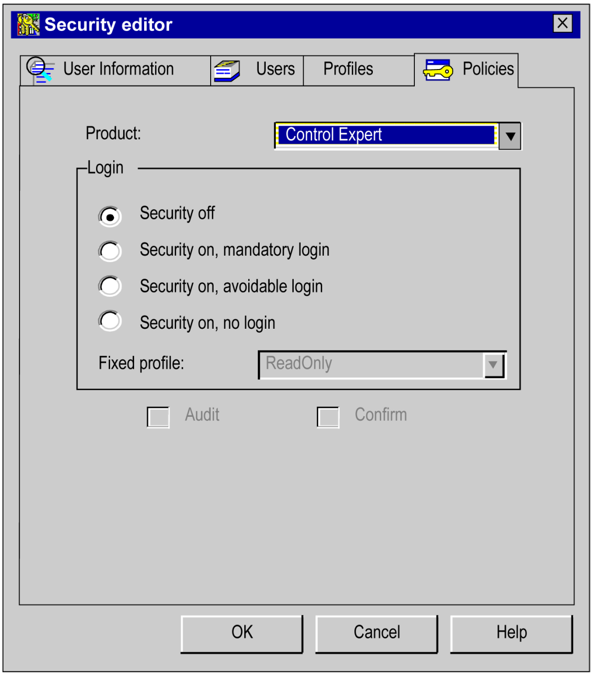
At a Glance

This tab in the security editor can be accessed only by the super user. It enables the execution of the following functions:

- Determine the guidelines associated with a product,
- define the default profile,
- Enable/disable the **Audit** option.
- Enable/disable the **Confirm** option.

Policies

The **Policies** tab of the security editor looks as follows:



Product: Control Expert

Login

● Security off

○ Security on, mandatory login

○ Security on, avoidable login

○ Security on, no login

Fixed profile: ReadOnly

□ Audit □ Confirm

Description of the parameters

The following table describes the screen parameters:

Parameter	Description
Product	Used to choose the product for which you would like to define guidelines. **NOTE:** The policy that applies to Securitor Editor (as a product) can not be modified.
Login	Used to define product access rules for the users: ● **Security off**: Security is disabled. You have direct access to the product. This is the default setting. ● **Security on, mandatory login**: Security is enabled. To access the product, it is mandatory that you enter your name and password, which will determine your profile. ● **Security on, avoidable login**: Security is enabled. To access the product, enter your name and password. In this case, you will have your user profile. You can also access the product without entering the password. In this case, you will have the default user profile. ● **Security on, no login** Security is enabled, but you have direct access to the product. The profile then is the default profile. When the security is disabled, the **Audit** and **Confirm** options will also be disabled.
Fixed profile	Used to define the default user profile.
Audit	Used to enable or disable the **Audit** option (this option is only available if security is enabled). If this check box is enabled, a log file will be created to store Control Expert and OS Loader user events. The log file is located at **Start** → **Programs** → **Windows Administrative Tools** → **Event Viewer** on your desktop.
Confirm	Used to enable or disable the **Confirm** option. If this box is checked, enter your name and password each time secure access is defined for a user action *(see page 20)*. **Note:** If you are using the **Confirm** option in the **Policies** tab of the security editor, carefully select access rights when creating a new profile. Otherwise, changes will require multiple confirmations in the program sections.

NOTE: The **Audit** and **Confirm** options are not assigned to one user but apply globally to all users with authorized access to the product.

Recovery procedure with an error

At a Glance

The security editor is used to control access to Control Expert and OS Loader. If a problem occurs, (access attempted by an illegal user, loss of password, etc.), follow the recovery procedure corresponding to the problem.

Access by an unknown user

If a user is not known to the security database, and security is enabled, there are two options:

- Access is configured with an **avoidable login** (**Security On, Password Optional**): in this case, the unknown user can access Control Expert/ OS Loader with the default profile,
- Access is configured with **mandatory login** (**Security On, Password Required**): in this case, the unknown user cannot access Control Expert / OS Loader.

For Security Editor access is set to **mandatory login** (**Security On, Password Required**) and cannot be modified. Unknown user cannot access Security Editor.

NOTE: If the database of the security editor is damaged or it was deleted, access to Control Expert / OS Loader is not possible, even if security is not active (**Security Off**).

Loss of password

If you have forgotten your password, the procedure to follow differs depending upon whether you are a user or a super user:

- if you are a user, contact the super user. He can reset your password. You can then enter a new password.
- If you are the super user, reinstall Control Expert, choosing a customized installation: Install only the security editor.

Database protection

To protect the database against possible damage, a backup file is created during installation. This hidden file can only be accessed in read mode. It enables the database to be restored when a fault occurs.

NOTE: The backup file is maintained and used if the database is damaged. If the automatic procedure fails, then repeat the installation procedure.

Control Expert Predefined Profiles

Introduction

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

Predefined User Profiles

Control Expert provides the following 9 user profiles:

Predefined Profile	Applicable program type	Description
ReadOnly	Program Program-PROCESS Program-SAFE	The user can only access the project in read mode, except for the PLC address, which can be modified. He can also copy or download the project.
Operate	Program Program-PROCESS	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.).
Safety_Operate	Program Program-PROCESS Program-SAFE	The user has similar rights as with the **Operate** profile, but with respect to the safety program, except that: ● Transferring data values to the PAC is not permitted. ● Commanding the safety program to enter maintenance mode is permitted.
Adjust	Program Program-PROCESS	The user has the same rights as with an **Operate** profile, with the added possibility of uploading a project (transfer to the PLC) and modifying the PLC operating mode (**Run**, **Stop**, ...).
Safety_Adjust	Program Program-PROCESS Program-SAFE	The user has similar rights as with the **Adjust** profile, but with respect to the safety program, except that: ● Transferring data values to the PAC is not permitted. ● Commanding the safety program to enter maintenance mode is permitted.
Debug	Program Program-PROCESS	The user has the same rights as with an **Adjust** profile, with the added possibility of using the debugging tools.
Safety_Debug	Program Program-PROCESS Program-SAFE	The user has similar rights as with the **Debug** profile, but with respect to the safety program, except that: ● Stopping or starting the program is not permitted. ● Updating initialization values is not permitted. ● Transferring data values to the PAC is not permitted. ● Forcing inputs, outputs or internal bits is not permitted. ● Commanding the safety program to enter maintenance mode is permitted.

Predefined Profile	Applicable program type	Description
Program	Program Program-PROCESS	The user has the same rights as with a **Debug** profile, with the added possibility of modifying the program.
Safety_Program	Program Program-PROCESS Program-SAFE	The user has similar rights as with the **Program** profile, but with respect to the safety program, except that: ● Stopping or starting the program is not permitted. ● Updating initialization values is not permitted. ● Transferring data values to the PAC is not permitted. ● Forcing inputs, outputs or internal bits is not permitted. ● Commanding the safety program to enter maintenance mode is permitted.

Predefined DTM roles (access rights to modify DTMs) are associated with the user profiles. Preconfigured user profiles are associated with specific DTM roles, and new user profiles are associated to a chosen DTM role. DTM roles are named and associated as follows:

User Profile	DTM Roles
Supervisor	Administrator
Adjust	SystemOperator
Debug	MaintenanceEngineer
Operate	SystemOperator
Program	PlanningEngineer
ReadOnly	SystemObserver
Safety_Adjust	SystemOperator
Safety_Debug	MaintenanceEngineer
Safety_Operate	SystemOperator
Safety_Program	PlanningEngineer
New user profile *(see page 22)*	Any right level among the 10 predefined roles. The DTM role needs to be chosen in accordance with the user access rights selected.

Control Expert Access Rights

Introduction

Control Expert access rights are classified in the following categories:

- project services
- adjustment/debugging
- libraries
- global modification
- elementary modification of a variable
- elementary modification of DDT compound data
- elementary modification of a DFB type
- elementary modification of a DFB instance
- bus configuration editor
- input/output configuration editor
- runtime screens
- cyber security

Topology Manager Access Rights

The table below present the the minimum access rights required to execute a command in Topology Manager when security is on:

Command	Access rights
Edit Control Project	● Create a new project ● Open an existing project ● Save a project ● Modify the configuration ● Modify the I/O configuration In addition to the above access rights, for M580 safety and safety redundant PAC, you must have the following access rights: ● Modify the safety configuration ● Modify the safety I/O configuration
Build	● Open an existing project ● Save a project ● Build off-line
Save Control Project as	● Save a project

Command	Access rights
Deploy → Control Project	● Transfer project to PLC
Deploy → IP Address	● Create a new project ● Modify the configuration ● Save a project ● Transfer project to PLC In addition to the above access rights, for M580 safety and safety redundant PAC, you must have the following access rights: ● Modify the safety configuration

Project services

The access rights for this category are as follows:

Access right	Description
Create a new project	You can create a new project.
Open an existing project	You can open an existing project.
Save a project	You can save the project.
SaveAs a project	You can copy the project.
Import a project	You can import a project. Partial import is considered to be a program modification.
Build off-line	You can launch generation of the executable in offline mode.
Build on-line STOP	You can launch generation of the executable in online mode, with the PLCs powered down.
Build on-line RUN	You can launch generation of the executable in online mode, with the PLCs powered up.
Start, stop or initialize the PLC	You can command the PLC (power up, power down, initialization). **NOTE:** Only process tasks are started or stopped. For a non-safety PLC, this means the PLC is started or stopped. For an M580 safety PAC, this means that tasks other than the SAFE task are started or stopped.
Update init values with current values	You can copy the current values to update the initial values (only non-safe data).
Transfer project from PLC	You can transfer the executable program from the PLC to the terminal.
Transfer project to PLC	You can transfer the executable program from the terminal to the PLC.
Transfer data values from file to PLC	You can transfer data from a file to the PLC (Only non-safe data)
Restore project backup in PLC	You can restore the contents of backup memory (Premium) or the memory card (Modicon M340 and Modicon M580) in the PLC executable area. **NOTE:** On Modicon M580, you can save to flash memory if no memory card is inserted.

Access right	Description
Save to project backup in PLC	You can save the project program in the backup memory (Premium) or the memory card (Modicon M340 and Modicon M580). **NOTE:** On Modicon M580, you can restore from flash memory if no memory card is inserted.
Set address	You can access a PLC via the network.
Modify options	You can modify project attributes.

Adjustment/Debugging

The access rights for this category are as follows:

Access right	Description
Modify variable values	You can modify the value of the variables (only non-safety variables).
Modify safety variable values	You can modify the value of the safety variables.
Force internal bits	You can force internal bits.
Force outputs	You can force outputs.
Force inputs	You can force inputs.
Task management	You can command execution of project program tasks (power up, power down; initialization).
SAFE Task management	You can command execution of safety project program SAFE tasks (power up, power down; initialization).
Task cycle time modification	You can modify cycle time for cyclical tasks.
SAFE Task cycle time modification	You can modify cycle time for cyclical SAFE tasks.
Suppress message in viewer	You can delete the message displayed in the viewer.
Debug the executable	You can debug the executable program.
Replace a project variable	You can replace all occurrences of one variable in the program by another (only non-safe variables).
Replace a safety project variable	You can replace all occurrences of one safety variable in the program by another.

Libraries

The access rights for this category are as follows:

Access right	Description
Create libraries or families	You can create libraries or families of user functions.
Create safety libraries or families	You can create safety libraries or families of user functions.
Delete libraries or families	You can delete libraries or families of user functions.
Delete safety libraries or families	You can delete safety libraries or families of user functions.

Access right	Description
Put an object into library	You can insert an object in a library.
Put an object into safety library	You can insert an object in a safety library.
Delete an object from library	You can delete an object from a library.
Delete an object from safety library	You can delete an object from a safety library.
Get an object from a library	You can import an object from a library to the project.
Get an object from the safety library	You can import an object from a safety library to the project.

Global modification

The access rights for this category are as follows:

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

Elementary modification of a variable

The access rights for this category are as follows:

Access right	Description
Variable add/remove	You can add or delete a variable.
Safety Variables add/remove	You can add or delete a safety variable.
Variable main attributes modifications	You can modify a variable's name, type, and address.
Safety Variables main attributes modifications	You can modify a safety variable's name, type, and address.
Variable minor attributes modifications	You can modify the comment and the initial value for a variable.
Safety Variables minor attributes modifications	You can modify the comment and the initial value for a safety variable.

Elementary modification of DDT compound data

The access rights for this category are as follows:

Access right	Description
DDT add/remove	You can add or delete a compound data item.
DDT modifications	You can modify the structure, comment and initial value for a compound data item.

Elementary modification of a DFB type

The access rights for this category are as follows:

Access right	Description
DFB type add/remove	You can add or delete a DFB type.
Safety DFB type add/remove	You can add or delete a safety DFB type.
DFB type structure modification	You can modify the structure of a DFB type.
Safety DFB type structure modification	You can modify the structure of a safety DFB type.
DFB type sections modification	You can modify the code section of a DFB type.
Safety DFB type sections modification	You can modify the code section of a safety DFB type.

Elementary modification of a DFB instance

The access rights for this category are as follows:

Access right	Description
DFB instance modification	You can add, delete, or modify (name and type) a DFB instance.
Safety DFB instance modification	You can add, delete, or modify (name and type) a safety DFB instance.
DFB instance minor attributes modification	You can modify the comment and the initial value for a DFB instance.
Safety DFB instance minor attributes modification	You can modify the comment and the initial value for a safety DFB instance.

Bus configuration editor

The access rights for this category are as follows:

Access right	Description
Modify the configuration	You can modify the configuration.
Modify the safety configuration	You can modify the safety configuration.
I/O sniffing	You can carry out bus configuration sniffing.

Input/output configuration editor

The access rights for this category are as follows:

Access right	Description
Modify the I/O configuration	You can modify the input/output configuration.
Modify the safety I/O configuration	You can modify the safety input/output configuration.
Adjust the I/O	You can adjust inputs/outputs.
Adjust the safety I/O	You can adjust safety inputs/outputs.
Save_param	You can save the module input/output parameters explicitly (initial parameter values are replaced by their current values).
Restore_param	You can restore the module input/output parameters explicitly (initial parameter values replace their current values).

Runtime screens

The access rights for this category are as follows:

Access right	Description
Modify screens	You can modify the runtime screens.
Modify messages	You can modify the runtime messages.
Add/remove screens or families	You can add or delete a runtime screen.

Cyber security

The access rights for this category are as follows:

Access right	Description
Create or modify application password	You can create and modify application password.
Enter Maintenance mode	You can enter in maintenance mode.
Adapt Auto-Lock timeout	You can adapt the Auto-lock timeout.

Assigned Control Expert Access Rights to Predefined Profiles

Introduction

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

Control Expert access rights are classified in the following categories:

- project services
- adjustment/debugging
- libraries
- global modification
- elementary modification of a variable
- elementary modification of DDT compound data
- elementary modification of a DFB type
- elementary modification of a DFB instance
- bus configuration editor
- input/output configuration editor
- runtime screens
- cyber security

NOTE: For predefined profiles, the **Audit** and **Confirm** options of all access rights are disable.

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	–	–	–	–	–	–	–	✓	✓
SaveAs 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	–	–	–	✓	–	–	–	✓	✓
✓ Included – not included									

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
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 viewer	–	✓	✓	✓	✓	✓	✓	✓	✓
Debug the executable	–	–	–	✓	✓	–	–	✓	✓
Replace a project variable	–	–	–	–	–	–	–	✓	✓
Replace a 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 an object into library	–	–	–	–	–	–	–	✓	✓
Put an object into safety library	–	–	–	–	–	–	–	–	✓
Delete an object from library	–	–	–	–	–	–	–	✓	✓
Delete an object from safety library	–	–	–	–	–	–	–	–	✓
Get an object from a 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 the documentation	–	✓	✓	✓	✓	✓	✓	✓	✓
Modify the functional view	–	–	–	–	–	–	–	✓	✓
Modify the animation tables	✓	✓	✓	✓	✓	✓	✓	✓	✓
Modify constants value	–	✓	–	✓	–	✓	–	✓	✓
Modify safety constants value	–	–	✓	–	✓	–	✓	–	✓
Modify the program structure	–	–	–	–	–	–	–	✓	✓
Modify the safety program structure	–	–	–	–	–	–	–	–	✓
✓ Included – not included									

Access right	ReadOnly	Adjust	Safety_Adjust	Debug	Safety_Debug	Operate	Safety_Operate	Program	Safety_Program
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 modifications	–	–	–	–	–	–	–	✓	✓
Safety Variables main attributes modifications	–	–	–	–	–	–	–	–	✓
Variable minor attributes modifications	–	✓	–	✓	–	✓	–	✓	✓
Safety Variables minor attributes modifications	–	–	✓	–	✓	–	✓	–	✓
✓ Included – not included									

Elementary modification of 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 modifications	–	–	–	–	–	–	–	✓	✓
✓ 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 sections 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 instance modification	–	–	–	–	–	–	–	–	✓
DFB instance minor attributes modification	–	✓	–	✓	–	✓	–	✓	✓
Safety DFB instance 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 the configuration	–	–	–	–	–	–	–	✓	✓
Modify the safety configuration	–	–	–	–	–	–	–	–	✓
I/O 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 I/O configuration	–	–	–	–	–	–	–	✓	✓
Modify the safety I/O configuration	–	–	–	–	–	–	–	–	✓
Adjust the I/O	–	✓	–	✓	–	✓	–	✓	✓
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									

Cyber Security

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 PLC.
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						

Index