
Chapter 4

Global project management

Subject of this Chapter

This chapter introduces the various tools used for project management: security and user access rights management, project creation, project backup, transfer of the project to the PLC, management of the user memory, etc.

What Is in This Chapter?

This chapter contains the following sections:

Section	Topic	Page
4.1	Access security management	64
4.2	Project management	86

Section 4.1

Access security management

Subject of this Section

This section introduces the tools used to manage security for a project.

What Is in This Section?

This section contains the following topics:

Topic	Page
Control Expert access security management	65
Security editor	68
User Information	69
User Functions	71
User Profiles	74
Policies	78
Recovery procedure with an error	80
Access rights	81

Control Expert access security management

At a Glance

A security configuration tool lets you limit and control access to the software different functionalities.

NOTE: Protected access to the 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.

Super User (Supervisor)

The super user is the only person with rights to manage access security for the software. The super user defines the list including the names of users who can access the software and their access rights.

During installation of the software on the drop, only the super user can access the security configuration without any limitation of rights (without a password).

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

The super user has the following rights:

- 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

Software users are defined in the list of users by the super user, if Control Expert access security is active. 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.

A user has the following rights:

- access the rights defined by his user 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 to 16 characters), an optional comment (maximum of 256 characters) and a list of access rights. Control Expert provides 5 preconfigured user profiles that cannot be modified. To complete this list, the super user can create all the personalized profiles that he requires.

Preconfigured User Profiles

Control Expert provides the following 5 user profiles:

Profile	Description
ReadOnly	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	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.).
Adjust	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 , ...).
Debug	The user has the same rights as with an Adjust profile, with the added possibility of using the debugging tools.
Program	The user has the same rights as with a Debug profile, with the added possibility of modifying the program.
Disabled	User cannot access the project.

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
ReadOnly	SystemObserver
Operate	SystemOperator
Adjust	MaintenanceEngineer
Debug	SystemOperator
Program	PlanningEngineer
Supervisor	Administrator
New user profile (<i>see page 75</i>)	Any right level among the 5 predefined roles. The DTM role needs to be chosen in accordance with the user access rights selected.

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.

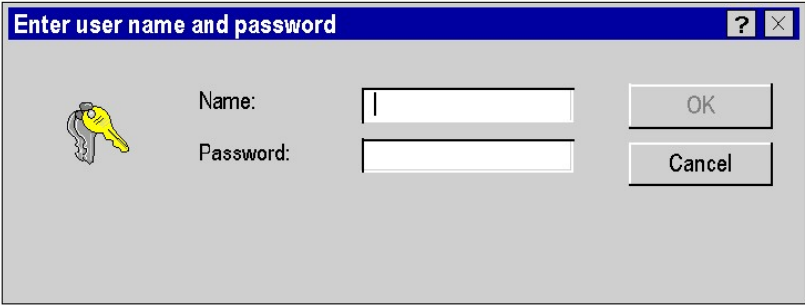
Security editor

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 → Schneider Electric → EcoStruxureControlExpert → Security Editor. The following dialog appears: 
2	Enter your name and password.
3	Confirm with OK.
4	If you are a user (see page 65), you can access the User information screen (see page 69) which allows you to consult your user profile or to modify your password.
5	If you are the Super User (Supervisor) (see page 65) the Security Editor (see page 69) will launch enabling administration of Control Expert 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**:

The screenshot shows the 'Security Editor' window with the 'User Information' tab selected. The window has a title bar with a close button. Below the title bar is a tabbed interface with four tabs: 'User Information' (active), 'Users', 'Profiles', and 'Policies'. The 'User Information' tab contains the following elements:

- A 'Name:' label followed by the text 'supervisor'.
- A 'Password' section with a title bar. Inside, there are two text input fields: 'New password:' and 'Confirm the new password:'. Below these fields is a note: 'Password can contain from 2 to 16 characters with spaces or be left blank.' and an 'Apply' button.
- A 'Profile(s)' section with a title bar. Inside, there is a 'Product:' label followed by a dropdown menu showing 'Control Expert'. Below this is a 'Profile:' label and a 'View profile' button.
- At the bottom of the window are three buttons: 'OK', 'Cancel', and 'Help'.

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).
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: In our case, Control Expert.
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

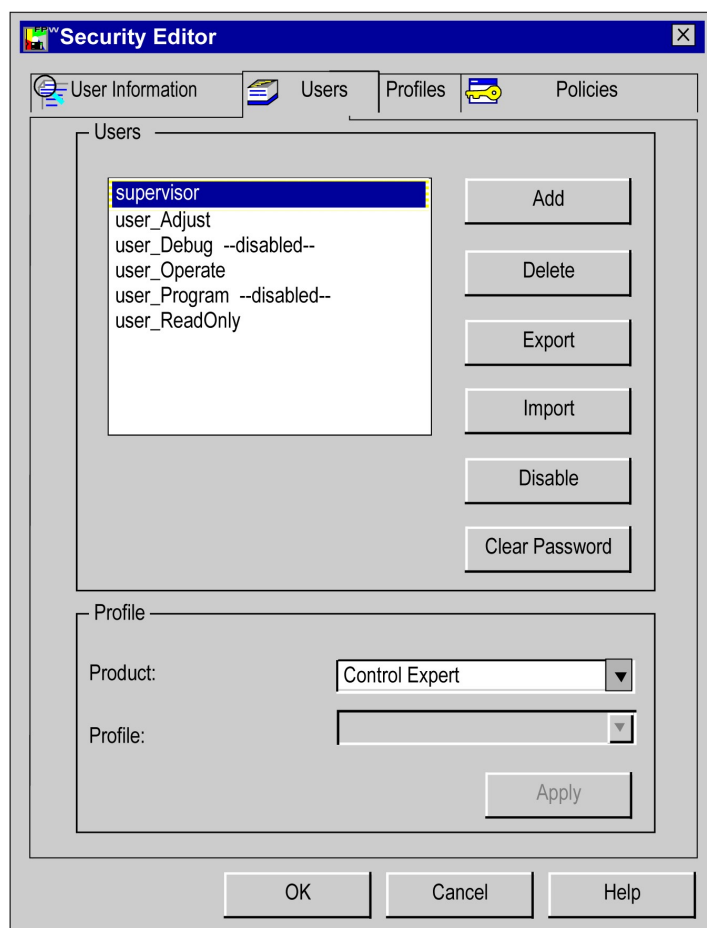
Only the Super User ([see page 65](#)) can access this tab. It enables the execution of the following functions:

- 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.

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

Users tab

The User tab looks like this. It contains the two areas User and Profile:



Description of the parameters

Users field

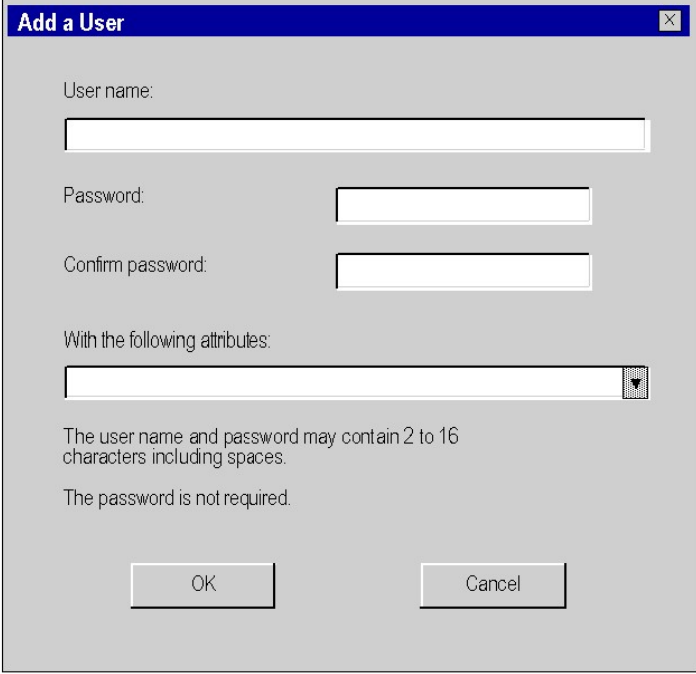
Parameter	Description
Users	List of users with access to Control Expert. The name of the super user is Supervisor. The Preconfigured User (<i>see page 66</i>) field is also available for selection: ● user_Adjust, ● user_Debug, ● user_Operate, ● user_Program, ● user_ReadOnly.
Add	Command used to add a new user to the list.
Delete	Command used to delete the selected user(s) from the list.
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 during login. 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 grayed out and -disabled- is displayed in the profile. If a disabled user attempts to start Control Expert, 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.
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 dialog window titled "Add a User" contains the following fields and controls:

- User name:** A text input field.
- Password:** A text input field.
- Confirm password:** A text input field.
- With the following attributes:** A dropdown menu.
- Help text:**
 - "The user name and password may contain 2 to 16 characters including spaces."
 - "The password is not required."
- Buttons:** "OK" and "Cancel".

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).
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

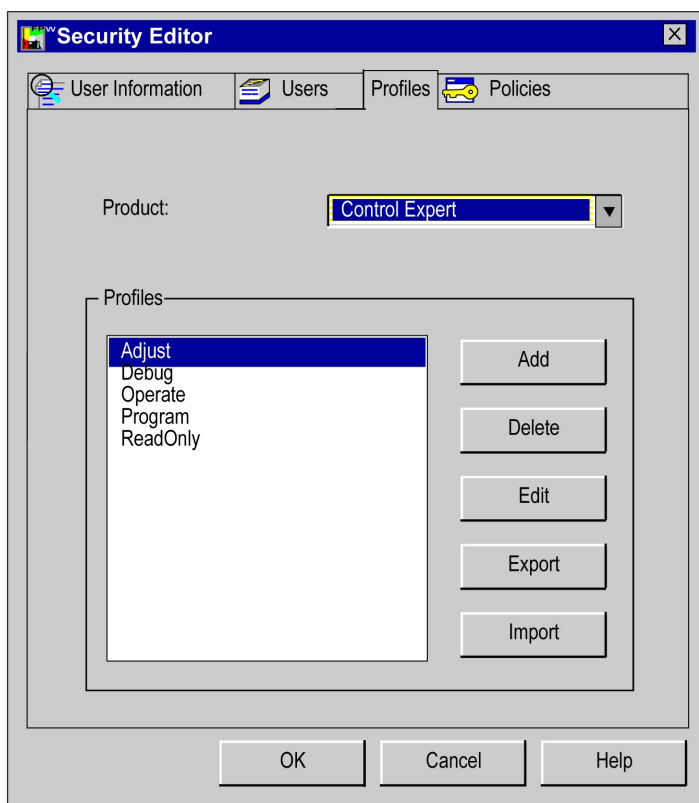
At a Glance

Only the Super User (*see page 65*) 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:



Description of the parameters

Product area:

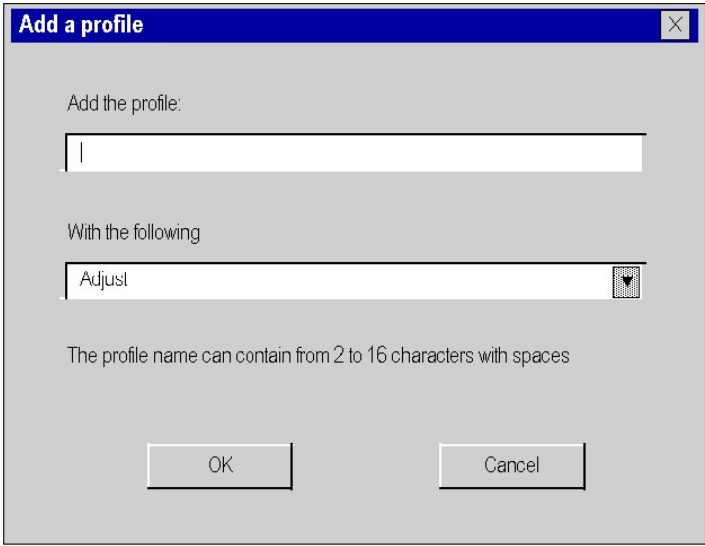
Parameter	Description
Product	Used to specify the product whose user profile you would like to access.

Profiles area:

Parameter	Description
Profiles	When the product chosen is Control Expert, list of user profiles associated with Control Expert.
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. Preconfigured user profiles cannot be deleted from the list.
Edit	Command used to modify access rights associated with the selected user profile.
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

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

OK Cancel

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:

Edit profile

Tool:

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:

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.
Access rights list	This list displays the access rights associated with the selected user profile. ● Access right: List of access rights associated with the user profile. ● DTM access rights: 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. 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

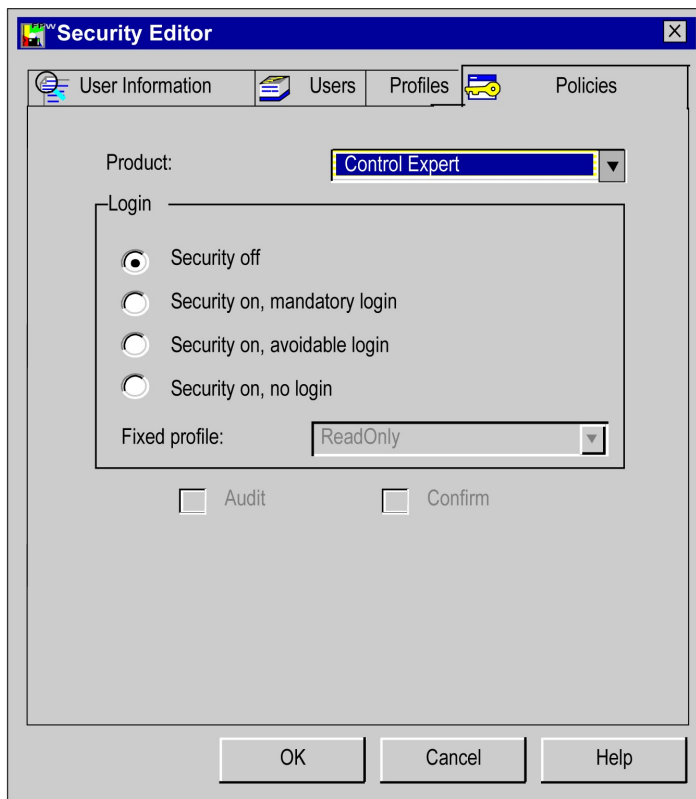
At a Glance

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 **Check** option.
- Enable/disable the **Confirm** option.

Policies

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



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. In our case, Control Expert.
Login	Used to define Control Expert access rules: ● Security off: Security is disabled. You have direct access to Control Expert. This is the default setting. ● Security on, mandatory login: Security is enabled. To access Control Expert, it is mandatory that you enter your name and password, which will determine your profile. ● Security on, avoidable login: Security is enabled. To access Control Expert, enter your name and password. In this case, you will have your user profile. You can also access Control Expert 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 Control Expert. The profile then is the default profile. When the security is disabled, the Audit and Confirm options will also be disabled.
Specified 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 checkbox is enabled, a log file will be created to store Control Expert user events. The log file is located at Start → Settings → Control Panel → 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 74). 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 Control Expert products.

Recovery procedure with an error

At a Glance

The security editor is used to control access to Control Expert. 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 editor, 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 with the default profile,
- Access is configured with **mandatory login (Security On, Password Required)**: in this case, the unknown user cannot access Control Expert.

If the database of the security editor is damaged or it was deleted, access to Control Expert 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.

Access rights

At a Glance

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

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).
Update init values with current values	You can copy the current values to update the initial values.
Transfer project from PLC	You can transfer the executable program from the PLC to the terminal.
Transfer data init values from PLC	You can transfer the initial values from the PLC.

Access right	Description
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.
Transfer data values from file to PLC	You can transfer data from the PLC to a file.
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.
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.
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).
Task cycle time modification	You can modify cycle time for cyclical 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.

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.
Delete libraries or families	You can delete libraries or families of user functions.
Put an object into library	You can insert an object in a library.
Delete an object from library	You can delete an object from a library.
Get an object from a library	You can import an object from a 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 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 program sections	You can modify the executable code for a section.
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.
Variable main attributes modifications	You can modify a variable's name, type, and address.
Variable minor attributes modifications	You can modify the comment and the initial value for a 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.
DFB type structure modification	You can modify the structure of a DFB type.
DFB type sections modification	You can modify the code section of a 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.
DFB instance minor attributes modification	You can modify the comment and the initial value for a 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.
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.
Adjust the I/O	You can adjust 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.