



Process Expert

Security Deployment Guide

Original instructions

EIO0000004234.04
05/2023

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 SE and its subsidiaries referred to in this document are the property of Schneider Electric SE 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.

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.

As part of a group of responsible, inclusive companies, we are updating our communications that contain non-inclusive terminology. Until we complete this process, however, our content may still contain standardized industry terms that may be deemed inappropriate by our customers.

© 2023 – Schneider Electric. All rights reserved.

Table of Contents

Safety Information.....	4
About the Book.....	5
Security Capabilities of the Software	9
Software Defense-in-Depth	9
Securing the Environment	10
Hardening the Computer	10
Secure Software Operation	13
Secure Software Operation Guidelines.....	13
Resources	17
Account Management	18
Account Management Guidelines	18
Removing the Software.....	20
Software Removal Guidelines.....	20
Index	22

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.

About the Book

Document Scope

This document describes the Defense-in-Depth capabilities of EcoStruxure Process Expert and contains guidelines to help you use it securely from installation to removal.

It also describes the Defense-in-Depth measures that are necessary in the environment in which the software is used.

Validity Note

This document has been updated for the release of EcoStruxure Process Expert 2023.

The characteristics that are described in the present document, as well as those described in the documents included in the Related Documents section below, can be found online. To access the information online, go to the Schneider Electric home page www.se.com/ww/en/download/.

The characteristics that are described in the present document should be the same as those characteristics that appear online. In line with our policy of constant improvement, we may revise content over time to improve clarity and accuracy. If you see a difference between the document and online information, use the online information as your reference.

Related Documents

Title of documentation	Reference number
EcoStruxure™ Process Expert, Installation and Configuration Guide	EIO0000001255 (ENG)
EcoStruxure™ Process Expert, User Guide	EIO0000001114 (ENG)
EcoStruxure™ Process Expert, Control Participant Services, User Guide	EIO0000001524 (ENG)
EcoStruxure™ Process Expert, Supervision Participant Services, User Guide	EIO0000001525 (ENG)
EcoStruxure™ Process Expert, Runtime Navigation Services, User Guide	EIO0000001574 (ENG)
EcoStruxure™ Process Expert, Global Templates, Reference Manual	EIO0000001986 (ENG)
EcoStruxure™ Process Expert, Controlling Application Execution on Computers, Cybersecurity Application Note	EIO0000004778 (ENG)
EcoStruxure™ Control Expert, Security Editor, Operation Guide	EIO0000004105 (ENG) EIO0000004106 (FRE) EIO0000004107 (GER) EIO0000004108 (ITA) EIO0000004109 (SPA) EIO0000004110 (CHS)
<i>Modicon Controllers Platform, Cyber Security, Reference Manual</i>	EIO0000001999 (ENG)
<i>Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment, User Guide</i>	EIO0000004242 (ENG)

mySchneider Support Portal

Visit <https://www.se.com/myschneider> for support, software updates, and latest information on EcoStruxure Process Expert.

Trademarks

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

InterSystems Caché is a registered trademark of InterSystems Corporation.

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.

NOTE: Schneider Electric adheres to industry best practices in the development and implementation of control systems. This includes a "Defense-in-Depth" approach to secure an Industrial Control System. This approach places the controllers behind one or more firewalls to restrict access to authorized personnel and protocols only.

⚠ WARNING

UNAUTHENTICATED ACCESS AND SUBSEQUENT UNAUTHORIZED OPERATION

- Evaluate whether your environment or your processes are connected to your critical infrastructure and, if so, take appropriate steps in terms of prevention, based on Defense-in-Depth, before connecting the automation system to any network.
- Limit the number of devices connected to a network to the minimum necessary.
- Isolate your industrial network from other networks inside your company.
- Protect any network against unintended access by using firewalls, VPN, or other, proven security measures.
- Monitor activities within your systems.
- Prevent subject devices from direct access or direct link by unauthorized parties or unauthenticated actions.
- Prepare a recovery plan including backup of your system and process information.

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

For more information on organizational measures and rules covering access to infrastructures, refer to ISO/IEC 27000 series, *Common Criteria for Information Technology Security Evaluation*, ISO/IEC 15408, IEC 62351, ISA/IEC 62443, *NIST Cybersecurity Framework*, *Information Security Forum - Standard of Good Practice for Information Security* and refer to *Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment*.

⚠ 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 that are given in this manual 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.

Terminology Derived from Standards

The technical terms, terminology, symbols and the corresponding descriptions in this manual, 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 13849-1:2015	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 62061:2015	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 61784-3:2016	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 present document 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.

Security Capabilities of the Software

Software Defense-in-Depth

Overview

Here is an overview of the software Defense-in-Depth, for details about the security capabilities of the software, refer to the EcoStruxure Process Expert help for additional information.

Refer also to *Modicon Controllers Platform, Cyber Security, Reference Manual* in the help of the Control Participant (see *EcoStruxure Process Expert, User Guide*).

User Authentication and Protection Against Unauthorized Access

The system server uses the access configuration that is performed by the system administrator in Security Editor to allow authorized users to log into EcoStruxure Process Expert. Usernames and passwords must be entered in the log-in window (see *EcoStruxure Process Expert, User Guide*) of at least one software component per computer.

Successful and unsuccessful attempts to log into an EcoStruxure Process Expert component are shown as follows:

- System server: Information is shown in the system server console (see *EcoStruxure Process Expert, Installation and Configuration Guide*) whether the system server is running or not.
- Engineering and operation clients: Information is shown in the notification panel (see *EcoStruxure Process Expert, User Guide*) of all open engineering clients that are connected to the same system server.

Once a user is authenticated, the system server identifies their rights based on the associated profiles (see *EcoStruxure Process Expert, Installation and Configuration Guide*) and grants access to the corresponding software components or functionality.

Client/Server Communication Authentication and Integrity

The software implements a public key infrastructure (PKI) based on the X.509 standard. It uses a Schneider Electric self-signed certification authority (CA) to create root and entity certificates to help secure client/server communication in the EcoStruxure Process Expert infrastructure.

For configuration details, refer to the topic describing how to secure client/server communication (see *EcoStruxure Process Expert, Installation and Configuration Guide*).

Securing the Environment

Hardening the Computer

Overview

The computers located in the control room are exposed to attacks. Those running EcoStruxure Process Expert, AVEVA Plant SCADA, OPC Factory Server, or OPC UA Server Expert need to be hardened.

For more detailed information, refer to the System Technical Note *How can I... Reduce Vulnerability to Cyber Attacks*.

Hardening Engineering Workstations

Customers may choose from various commercial computer systems for their engineering workstation needs. Key hardening techniques include:

- Strong password management.
- User account management.
- Methods of least privilege applied to applications and user accounts.
- Removal or disabling unneeded services.
- Removing remote management privileges, if not necessary.
- Systematic patch management.

Using Antivirus Software

Use an antivirus software on each computer of the EcoStruxure Process Expert infrastructure and keep it up-to-date.

Configure it so that file scanning is not performed while EcoStruxure Process Expert is in use.

Disabling Unused Network Interface Cards

Verify that network interface cards that are not required by the application are disabled. For example, if your system has two cards and the application uses only one, verify that the other network card is disabled.

Refer to the help of the operating systems for instructions on how to proceed.

Configuring the Local Area Connection

Various Windows network settings provide enhanced security aligned with the Defense-in-Depth approach.

To access these settings in Windows 10 systems, from the Start button, click **Settings > Network & Internet**.

The following are examples of configuration changes that you can make on your system by using **Change Adapter Options**:

- Disable all IPv6 stacks on their respective network cards.
- Clear all **Local Area Connection Properties** items except for **QoS Packet Scheduler** and **Internet Protocol Version 4 (TCP/IPv4)**.
- In the **WINS** tab of **Advanced TCP/IP Settings** of **Internet Protocol Version 4 (TCP/IPv4)**, clear the **Enable LMHOSTS** and **Disable NetBIOS over TCP/IP** check boxes.
- Enable **File and Print Sharing for Microsoft Network**.

Defense-in-Depth also includes the following:

- Define only static IPv4 addresses, subnet masks, and gateways.
- Do not use DHCP or DNS in the control room.

Disabling the Remote Desktop Protocol

The Defense-in-Depth approach includes disabling Remote Desktop Protocol (RDP) unless your application requires the RDP. The following steps describe how to disable the protocol:

Step	Action
1	In Windows 10, enter <code>Remote desktop settings</code> in the search field of the taskbar.
2	In the Remote Desktop settings screen, disable remote desktop.

Updating Security Policies

Ensure that the security policies on the computers in your system are up-to-date.

Contact your system administrator or refer to the `gpupdate` command in the Microsoft help.

Disabling LANMAN and NTLM

Disable the Microsoft LAN Manager protocol (LANMAN or LM) and its successor NT LAN Manager (NTLM) to help minimize vulnerabilities.

The following steps describe how to disable LM and NTLM in a Windows 10 system.

Step	Action
1	In the search field of the taskbar, enter <code>secpol.msc</code> to open the Local Security Policy window.
2	Open Security Settings > Local Policies > Security Options .
3	Select Send NTLMv2 response only. Refuse LM & NTLM in the Network Security: LAN Manager authentication level field.
4	Select the Network Security: Do not store LAN Manager hash value on next password change check box.
5	In a command prompt, enter <code>gpupdate</code> to apply the security policy change.

Applying Operating System Updates

Before deployment, update the computer operating systems by using the **Windows Update** tool. To access this tool in Windows 10, from the Start menu, click **Settings > Update & Security**.

The supported operating systems and versions are indicated in the topic describing system requirements (see *EcoStruxure Process Expert, Installation and Configuration Guide*).

NOTE: Ensure to test the compatibility of these updates in a test environment before installing them in a production environment.

Secure Software Operation

Secure Software Operation Guidelines

Installing the Software

Install EcoStruxure Process Expert at the default location, that is to say, *<default system drive>\Program Files\Schneider Electric\EcoStruxure\Process Expert*.

Opening the System Server Console and Starting Clients

To help improve security:

- Log in by using a user with a strong password.
- Start clients by double-clicking the desktop shortcuts or clicking entries in the Microsoft Windows Start menu.

Do not start the software by using the **Run as administrator** command on system server or client desktop shortcuts and Microsoft Windows Start menu entries.

Passwords

Use strong passwords and change them regularly.

The table describes the various passwords that you need to manage when using the software.

Password-protected object	Description	Action
Control Participant project files (.stu) of Control projects and that encapsulate Control logic in Control facet templates.	<ul style="list-style-type: none"> In the projects, application, and topology domains, the System Access Password is used as application password for Control Participant project files (.stu) and file encryption is enabled. In the Global Templates domain, the Control Constituent Password is used as application password for Control Participant project files (.stu) that encapsulate Control logic in Control facet templates and file encryption is enabled. 	<p>Enable password protection for systems and Control facet templates either way:</p> <ul style="list-style-type: none"> For both at the same time by enabling the Control application and facet template password protection setting (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>) in the System Server Configuration Wizard. <p>This also makes the use of the Controller and Simulator passwords mandatory.</p> <ul style="list-style-type: none"> Individually, by enabling the following: <ul style="list-style-type: none"> For systems: The System Access Password property (see <i>EcoStruxure Process Expert, User Guide</i>) of each system. For Control facet templates: Control constituent application password protection setting (see <i>EcoStruxure Process Expert, User Guide</i>) of the Global Templates library.
The <i>simulatorprofile.sta</i> Control project that is loaded in the controller simulator (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>) when you start it.	<p>Helps secure the Ethernet port that is used by the controller simulator on the local computer.</p> <p>Can also be used to restrict deployment and execution operations performed on the Control project that is deployed to the controller simulator by using the engineering client and operations performed by using the operation client when using Runtime Navigation Services (RTNS).</p> <p>The default password is documented in the Installation and Configuration Guide.</p>	<p>You can perform either action:</p> <ul style="list-style-type: none"> Change the default password of the simulatorprofile.sta project. Have your own password-protected Control project loaded when the controller simulator starts. <p>NOTE: If the Windows session is not the one that was used to install the software, the simulator needs to be configured manually (see <i>EcoStruxure Process Expert, User Guide</i>) to load a password-protected Control project at startup.</p>
Control project that is deployed in the controller.	<p>Restricts deployment and execution operations performed on the Control project by using the engineering client.</p> <p>Also restricts operations performed by using the operation client when using Runtime Navigation Services (RTNS).</p>	Set the Controller password after configuring the controller.
Safety-related program and configuration of M580 safety controllers.	The safety-related password restricts access to the safety-related program and configuration offline and to the maintenance mode online.	Leave the safety-related password (see <i>EcoStruxure Process Expert, User Guide</i>) property of the M580 safety controller enabled and set a password after creating the safety controller entity.
Default user (see <i>EcoStruxure Process Expert, Supervision Participant Services, User Guide</i>) and role when you create a Supervision project.	Used for access control management in the Supervision Participant.	Set a password and modify the role of the user according to your particular application.

Password-protected object	Description	Action
Users that are associated to a Process Expert profile in Security Editor.	Only users that exist in the security database that is managed by Security Editor or on an LDAP server can log into the software.	<ul style="list-style-type: none"> Create users with a password (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>) rather than using existing users for a new software installation. Enable only active users. Immediately change the default password of existing users that have been migrated to Security Editor from EcoStruxure Process Expert 2021 or earlier. Keep the appropriate security level when using the local authentication mode in Security Editor.
The <i>SecurityAdmin</i> user of Security Editor.	After installing EcoStruxure Process Expert, the <i>SecurityAdmin</i> user is the only one that can log into Security Editor and configure Role-Based Access Control (RBAC).	Immediately change the password of the <i>SecurityAdmin</i> user (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>).

Folder Sharing

Using the software requires sharing folders so that the software can copy files to or read files from these folders.

This is the case, for example, for the folder to which Supervision projects are deployed and that are located on the network.

When sharing a folder apply the following practices:

- Restrict access to the folder by giving permissions only to users who need to access this folder.
- Disable sharing after the data transfer is complete.

Locking Sessions

When the computer that runs an EcoStruxure Process Expert component is left unattended, lock the component (see *EcoStruxure Process Expert, User Guide*) and the Windows session to help protect against unwanted access to the software and its files.

Software Updates

Install the Schneider Electric Software Update (SESU) tool and enable update notifications to stay informed of the latest software updates for installed Schneider Electric products.

The option to install the tool can be selected during software installation or thereafter by using the installer of the tool, which is located in the SESU folder in the root of the software installation package.

If the computer is not connected to the Internet, visit the mySchneider support portal regularly from another computer, which is connected to the Internet.

Log Files and Data Backup Files

Back up installation log files (see *EcoStruxure Process Expert, Installation and Configuration Guide*) and activity log files (see *EcoStruxure Process Expert, User Guide*) on a regular basis and store them securely.

Back up the database (see *EcoStruxure Process Expert, Installation and Configuration Guide*) and systems (see *EcoStruxure Process Expert, User Guide*) on a regular basis and store them securely.

Exporting Data in CSV Format

The software lets you export data of the following objects in comma-separated value (.csv) format:

- Application objects (see *EcoStruxure Process Expert, User Guide*)
- I/O devices of the topology (see *EcoStruxure Process Expert, User Guide*)

If a free-form text parameter of an exported object (such as **Description** of a folder or instance of the application) contains a formula (string starting with the equal sign (=)), the formula can be executed when the export file is opened by using Microsoft Excel or a similar type of application.

Before opening a file exported in .csv format, perform the appropriate and complete verification of the properties of exported objects by using the **Application Explorer** to ensure that they do not contain malicious code, which could lead to formula injection.

WARNING

UNINTENDED EQUIPMENT OPERATION

Thoroughly examine an exported, .csv formatted file for any and all objects and ensure that the use of Microsoft Excel symbols do not allow the importation of unintended consequences, such as malicious code.

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

Importing Data in the Software

The software lets you import the following editable files containing data of systems. These files may have been previously exported from the software or may be user-created:

- Application export files (.csv and .xml) (see *EcoStruxure Process Expert, User Guide*)
- Topological I/O device export files (.csv) (see *EcoStruxure Process Expert, User Guide*)
- Hardware mapping export files (.csv) (see *EcoStruxure Process Expert, User Guide*)

Before importing such files in the same or a different EcoStruxure Process Expert infrastructure, perform the appropriate and complete verification of these files to ensure that they have not been tampered with and are free from malicious code.

WARNING

UNINTENDED EQUIPMENT OPERATION

Thoroughly examine an exported, .csv formatted file for any and all objects and ensure that the use of Microsoft Excel symbols do not allow the importation of unintended consequences, such as malicious code.

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

Resources

Cybersecurity Support Portal

Register to the support portal to stay informed about cybersecurity vulnerabilities and security notifications for Schneider Electric solutions.

Visit <https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

Reporting Vulnerabilities

The Cybersecurity Support Portal lets you report vulnerabilities that are not addressed yet.

Account Management

Account Management Guidelines

Overview

The actions that users are allowed to perform depend on the profiles that are assigned to them.

By default, for a new software installation, no users associated to a Process Expert profile exist. In case of a software upgrade, existing users are disabled.

For a description of profiles, refer to the topic describing role-based access control (see *EcoStruxure Process Expert, Installation and Configuration Guide*).

Actions Based on User Accounts and Profiles

Action	Required account type, profile, and scope of actions
Installation	<p>A user with administrator privileges on the local computer can install the software.</p> <p>During installation, the following can be configured:</p> <ul style="list-style-type: none"> • Installation paths, page 13. • The station role. • Simulator Ethernet port (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>).
Engineering	<p>A user, page 13 associated to one or more Process Expert profiles (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>) and authenticated either locally or centralized can log into (see <i>EcoStruxure Process Expert, User Guide</i>) the corresponding EcoStruxure Process Expert components that are installed on the computer and use them (for example, the system server or the engineering client depending on the station role).</p> <p>The user who is allowed to use a component can also lock (see <i>EcoStruxure Process Expert, User Guide</i>) and configure it.</p>
Configuration	<p>After installation, a user associated to a Process Expert profile with system server rights can configure it as follows once they are logged into the server:</p> <ul style="list-style-type: none"> • Access to the parameters of the System Server Configuration Wizard. • Creation of root CA certificates and installation of security certificates on the local computer (requires elevated privileges). • Installation of security certificates for communication with the syslog server. • Access to advanced parameters. <p>The engineering and operation clients can be configured as follows by a user who is allowed to log into the computer:</p> <ul style="list-style-type: none"> • Engineering client: <ul style="list-style-type: none"> ◦ Access to the parameters of the Engineering Client Configuration Wizard. ◦ Installation of security certificates on the local computer (requires elevated privileges). • Operation client: <ul style="list-style-type: none"> ◦ Access to the parameters of the Operation Client Configuration Wizard. ◦ Installation of security certificates on the local computer (requires elevated privileges). <p>After installation, the <i>SecurityAdmin</i> user can configure role-based access control for EcoStruxure Process Expert by using Security Editor.</p>

Action	Required account type, profile, and scope of actions
Maintenance	<p>A user who can log into the computer as administrator can update the software.</p> <p>A user who can log into the computer can perform the following actions:</p> <ul style="list-style-type: none"> Repair the software. Add and remove EcoStruxure Process Expert components proposed by the installer. <p>Log files created by the software can be viewed, edited, and deleted by the following users:</p> <ul style="list-style-type: none"> Installation log files (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>): A user who is allowed to log into the computer. Activity log files (see <i>EcoStruxure Process Expert, User Guide</i>): A user who is logged into the computer. <p>To back up, restore, and purge data, users require the following rights:</p> <ul style="list-style-type: none"> Database backups (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>): Users associated to a profile allowing them to use the system server. System (see <i>EcoStruxure Process Expert, User Guide</i>) and controller data backups (see <i>EcoStruxure Process Expert, User Guide</i>): Users associated to a profile allowing them to use the engineering client (ESX PE Engineer). Purging templates (see <i>EcoStruxure Process Expert, User Guide</i>): Users associated to a profile allowing them to use the Global Templates Explorer of the engineering client (ESX PE Template Designer). Users and their profiles (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>): Only the <i>SecurityAdmin</i> user can back up and restore this Security Editor data.
Removal	A user who can log into the computer can remove the software (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>).

Default Supervision Project User

When you create a Supervision project, the software creates the *viewonly* user (see *EcoStruxure Process Expert, Supervision Participant Services, User Guide*) with *EsxViewer* role to allow for access control management in the Supervision Participant.

Removing the Software

Software Removal Guidelines

Overview

Detailed software removal procedures are provided in the topic describing how to remove the software (see *EcoStruxure Process Expert, Installation and Configuration Guide*). They need to be applied on each computer of an EcoStruxure Process Expert architecture.

The data that remains on the computer after the software is removed is described here.

Removal Methods

You can remove the software from the computer by using either of the following methods. In each case, some data remains on the computer, which needs to be removed manually, if necessary.

Method	Description
Double-clicking <i>setup.exe</i> in the installation package and selecting the Remove option.	Removes the software from the local computer with the option to remove also the following components: <ul style="list-style-type: none"> Security certificates Associated and third-party components
In the Microsoft Windows Control Panel , clicking Uninstall or change a program > EcoStruxure Process Expert > Change and selecting the Remove option.	
In the Microsoft Windows Control Panel , clicking Uninstall or change a program > EcoStruxure Process Expert > Uninstall and selecting the Remove option.	Removes only the software from the local computer.

Data to Be Removed Manually

The following table indicates which data remains on the computer when you remove the software.

Data	Description and location
Database	Data of systems and their content as well as global templates that are accessed by the system server. Refer to the topic describing default destination folders (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>) for the location of the <i>Db</i> folder, which contains the database that was used last.
Associated and third-party components	Software managing the InterSystems Caché database. Refer to the topic describing installed software components (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>). In addition, the <i>InterSystems</i> folder at the path <i>C:\Program Files</i> as well as third-party configuration files remain on the computer on which the system server is installed. Also, some components installed by AVEVA Plant SCADA and EcoStruxure Control Expert may not be removed. Verify their presence by using the Microsoft Windows Control Panel .
Schneider Electric licensing software	License Manager and Floating License Manager. Refer to the topic describing installed software components (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>) and the Licensing Guide (see <i>EcoStruxure Process Expert, Licensing Guide</i>) for details.

Data	Description and location
Deployed files	<p>Supervision project files that have been deployed to shared folders on station nodes.</p> <p>These are the station nodes that are mapped to Supervision executables in the service mapping (see <i>EcoStruxure Process Expert, User Guide</i>).</p>
Exported and generated files	The various user-created files, such as topology, application, project, hardware mapping, and template export files as well as system engineering documentation remain at the location where they have been created.
Log files	Installation log files (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>).
Database, system, and data backup files	The various user-created backup files, such as database, system, and Security Editor backup files remain at the location where they were created.
Software help files	<p>HTML help files of templates of a previous software version or user-created HTML help files.</p> <p>Refer to the topic describing how to use the help (see <i>EcoStruxure Process Expert, User Guide</i>).</p>
Security certificates	<p>EcoStruxure Process Expert root CA and entity certificates that are installed on the local computer.</p> <p>Refer to the topic describing certificate properties (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>) for the name and location.</p>
Control project file	<p>Default password-protected Control project file (.sta) that can be loaded when the controller simulator starts.</p> <p>Refer to the topic describing the installation of the controller simulator (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>).</p>
User groups	<p>Groups created by the software (versions 2021 and earlier) on the local computer when local authentication is selected.</p> <p>Refer to the topic describing role based access control (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>) for details.</p>
Firewall entries	<p>Entries that are created by the software during installation for Schneider Electric and third-party components.</p> <p>Refer to the topic describing firewall exceptions (see <i>EcoStruxure Process Expert, Installation and Configuration Guide</i>) for details.</p>
Folder sharing configurations	The configuration of shared folders is not modified when you remove the software.
Other data	<p>Data in the <software name> folder (for example, Process Expert), which is located at the path %localappdata%\Schneider Electric.</p> <p>If you had upgraded a version of the software that was using a virtual machine (VM) for Participants (for example, EcoStruxure Process Expert 2020 R2 or earlier), the Vm folder may be present at the path C:\Users\<Username>\AppData\Local\Schneider Electric\<upgraded version>.</p>

Index

A

account management	
account management guidelines	18
antivirus software	
using antivirus software	10

C

computers	
hardening computers	10
cybersecurity	
default supervision project user	19
Defense-in-Depth	9
LANMAN / NTLM	11
local area connections	11
network interface card settings	10
remote desktop	11
resources	17
software operation guidelines	13

D

Defense-in-Depth	
security capabilities of the software	9

H

hardening	
hardening computers	10

L

LAN	
cybersecurity guidelines	11
LANMAN / NTLM	
cybersecurity guidelines	11

N

network interface cards	
cybersecurity guidelines	10

O

operation	
software operation guidelines	13

R

remote desktop	
cybersecurity	11
removing	
removing the software	20
reporting	
reporting vulnerabilities	17

S

support	
Cybersecurity Support Portal	17

U

uninstalling	
removing the software	20
user accounts	
account management guidelines	18

V

vulnerabilities	
reporting vulnerabilities	17

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time,
please ask for confirmation of the information given in this publication.

© 2023 Schneider Electric. All rights reserved.

EIO0000004234.04