EcoStruxure™

Process Expert

Security Deployment Guide

EIO0000004234.03
02/2022

www.se.com

Schneider Electric™

Legal Information

Table of Contents

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 expected from the environment in which the software is used.

Validity Note

This document is valid for EcoStruxure Process Expert 2021 or later. It supersedes any previous version.

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)

You can download these technical publications at https://www.se.com/myschneider, *Document Downloads* section.

Registration required.

mySchneider Support Portal

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

Registration required.

Product Related Information

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.

Security Capabilities of the Software

Software Defense in Depth

Overview

This guide does not describe in detail the security capabilities of the software. Refer to the EcoStruxure Process Expert help for additional information on how to use them.

Refer also to the *Modicon Controllers Platform Cyber Security* 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 password of the Windows® local or Active Directory® accounts to validate that users are who they claim to be. 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. That is, the system server or a client.

Successful and unsuccessful attempts to log in to a 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 the roles (see EcoStruxure™ Process Expert, Installation and Configuration Guide) that the user has been assigned and grants them access to the corresponding software components or functionality thereof.

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 highly 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.
- 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 that Schneider Electric recommends.

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 recommendations by Schneider Electric also include 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 strategy recommended by Schneider Electric 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 `Remote desktop settings` 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

The Microsoft LAN Manager protocol (LANMAN or LM) and its successor NT LAN Manager (NTLM) have vulnerabilities that make their use in control applications inadvisable.

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 `secpol.msc` 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 Manger 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 `gpupdate` to commit the security policy change.

Applying Operating System Updates

Before deployment, update all 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: Schneider Electric recommends that you 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

During installation, you can change the location where the software will be installed (see EcoStruxure™ Process Expert, Installation and Configuration Guide).

Schneider Electric recommends installing EcoStruxure Process Expert at the default location, that is <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 standard Windows user account to use the software.
- 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	Recommended action
Control Participant project files (.stu) of Control projects and that encapsulate Control logic in Control facet templates.	• 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.	Enable password protection for systems and Control facet templates either way: • For both at the same time by enabling the **Control application and facet template password protection** setting (see EcoStruxure™ Process Expert, Installation and Configuration Guide) in the **System Server Configuration Wizard**. This also makes the use of the **Controller** and **Simulator** passwords mandatory. • Individually, by enabling the following: ◦ For systems: The **System Access Password** property (see EcoStruxure™ Process Expert, User Guide) of each system. ◦ For Control facet templates: **Control constituent application password protection** setting (see EcoStruxure™ Process Expert, User Guide) of the Global Templates library.
The simulatorprofile.sta Control project that is loaded in the controller simulator (see EcoStruxure™ Process Expert, Installation and Configuration Guide) when you start it.	Helps secure the Ethernet port that is used by the controller simulator on the local computer. 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). The default password is documented in the Installation and Configuration Guide.	You can perform either action: • Change the default password of the simulatorprofile.sta project. • Have your own password-protected Control project loaded when the controller simulator starts. **NOTE:** If the current Windows® session is not the one that was used to install the software, the simulator needs to be configured manually (see EcoStruxure™ Process Expert, User Guide) to load a password-protected Control project at startup.
Control project that is deployed in the controller.	Restricts deployment and execution operations performed on the Control project by using the engineering client. Also restricts operations performed by using the operation client when using Runtime Navigation Services (RTNS).	Set the **Controller** password after configuring the controller.
Safety program and safety configuration of M580 safety controllers.	The safety password restricts access to the safety program and configuration offline and to the maintenance mode online.	Leave the safety password (see EcoStruxure™ Process Expert, User Guide) property of the M580 safety controller enabled and set a password after creating the safety controller entity.
Default user (see EcoStruxure™ Process Expert, Supervision Participant Services, User Guide) and role when you create a Supervision project.	Used for access control management in the Supervision Participant.	Change the password and modify the role of the user according to your particular application.
The maintenance mode of the system server console.	Restricts access to advanced functionalities and settings (see EcoStruxure™ Process Expert, Installation and Configuration Guide) of the system server. The default password is documented in the Installation and Configuration Guide.	The password cannot be changed. **NOTE:** To access the system server console, a user must belong to the group (see EcoStruxure™ Process Expert, Installation and Configuration Guide) allowing them to use the system server.

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 secure practices:

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

Locking Sessions

When the computer that runs a 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.

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 =) either because it has been entered by using the **Application Explorer** or added through an import operation, 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, it is your duty to 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.

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, it is your duty to perform the appropriate and complete verification of these files to ensure that they have not been tampered with and are free from malicious code.

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 type of account they have and their group membership.

By default, users are not members of any group for EcoStruxure Process Expert.

For a description of predefined RBAC roles and the corresponding groups, refer to the topic describing role-based access control (see EcoStruxure™ Process Expert, Installation and Configuration Guide).

Actions Based on User Accounts and Group Membership

Action	Required account type, group membership, and scope of actions
Installation	Any user with administrator privileges on the local computer can install the software. During installation, the following can be configured: • Installation paths, page 11. • Selection of station role. • Simulator Ethernet port configuration (see EcoStruxure™ Process Expert, Installation and Configuration Guide). • Local or domain RBAC authentication selection (see EcoStruxure™ Process Expert, Installation and Configuration Guide) when installing the system server.
Operation	Any user, page 11 who belongs to one or more predefined groups (see EcoStruxure™ Process Expert, Installation and Configuration Guide), either on the local computer or on the domain controller can log in (see EcoStruxure™ Process Expert, User Guide) to 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). The user who is allowed to use a component can also lock (see EcoStruxure™ Process Expert, User Guide) and configure it.
Configuration	After installation, any user who belongs to the group that allows them to use the system server can configure it as follows once they log in to the server: • 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. The engineering and operation clients can be configured as follows by any user who is allowed to log in to the computer: • Engineering client: ◦ Access to the parameters of the **Engineering Client Configuration Wizard**. ◦ Installation of security certificates on the local computer (requires elevated privileges). • Operation client: ◦ Access to the parameters of the **Operation Client Configuration Wizard**. ◦ Installation of security certificates on the local computer (requires elevated privileges).

Action	Required account type, group membership, and scope of actions
Maintenance	Any user who can log in to the computer as administrator can update the software. Any user who can log in to the computer can perform the following actions: • Repair the software. • Add and remove EcoStruxure Process Expert components proposed by the installer. • Modify the RBAC authentication domain (system server computer only). To configure and modify RBAC, the following rights are required: • Domain authentication: Network administrator. Can create and delete groups on the domain controller and add/remove users. • Local authentication: Computer administrator. Can only add/remove users to/from groups created locally by the software and can delete groups. Log files created by the software can be viewed, edited, and deleted by the following users: • Installation log files (see EcoStruxure™ Process Expert, Installation and Configuration Guide): Any user who is allowed to log in to the computer. • Activity log files (see EcoStruxure™ Process Expert, User Guide): User who is logged in to the computer. To back up, restore, and purge data, users require the following rights: • Database backups (see EcoStruxure™ Process Expert, Installation and Configuration Guide): Users who belong to the group allowing them to use the system server. • System (see EcoStruxure™ Process Expert, User Guide) and controller data backups (see EcoStruxure™ Process Expert, User Guide): Users who belong to the group allowing them to use the engineering client (Engineer role). • Purging templates (see EcoStruxure™ Process Expert, User Guide): Users who belong to the group allowing them to use the engineering client (Template Designer role)
Removal	Any user who can log in to the computer can remove the software (see EcoStruxure™ Process Expert, Installation and Configuration Guide).

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 *Esx Viewer* 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 has been 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.

Method	Description
Double-clicking setup.exe 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: • 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 EcoStruxure™ Process Expert, Installation and Configuration Guide) for the location of the Db folder, which contains the database that was used last.
Associated and third-party components	Software managing the Cache database. Refer to the topic describing installed software components (see EcoStruxure™ Process Expert, Installation and Configuration Guide). In addition, the InterSystems folder at the path C:\Program Files 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 EcoStruxure™ Process Expert, Installation and Configuration Guide) and the Licensing Guide (see EcoStruxure™ Process Expert, Licensing Guide) for details.
Deployed files	Supervision project files that have been deployed to shared folders on station nodes.

Data	Description and location
	These are the station nodes that are mapped to Supervision executables in the service mapping (see EcoStruxure™ Process Expert, User Guide).
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 when you remove the software.
Log files	Installation log files (see EcoStruxure™ Process Expert, Installation and Configuration Guide).
Database, system, and data backup files	The various user-created back-up files, such as database and system backup files remain at the location where they have been created when you remove the software.
Software help files	HTML help files of templates of a previous software version or user-created HTML help files. Refer to the topic describing how to use the help (see EcoStruxure™ Process Expert, User Guide).
Security certificates	EcoStruxure Process Expert root CA and entity certificates that are installed on the local computer. Refer to the topic describing certificate properties (see EcoStruxure™ Process Expert, Installation and Configuration Guide) for the name and location.
Control project file	Default password-protected Control project file (.sta) that can be loaded when the controller simulator starts. Refer to the topic describing the installation of the controller simulator (see EcoStruxure™ Process Expert, Installation and Configuration Guide).
User groups	Groups created by the software on the local computer when local authentication is selected. Refer to the topic describing role based access control (see EcoStruxure™ Process Expert, Installation and Configuration Guide) for details.
Firewall entries	Entries that are created by the software during installation for Schneider Electric and third-party components. Refer to the topic describing firewall exceptions (see EcoStruxure™ Process Expert, Installation and Configuration Guide) for details.
Folder sharing configurations	The configuration of shared folders is not modified when you remove the software.
Other data	Data in the <software name> folder (for example, Process Expert), which is located at the path %localappdata%\Schneider Electric.
	If you had upgraded a version of the software that was still using a 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>.

Index

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.

EIO0000004234.03