# EcoStruxure™ Control Engineering

## Administration and Hardening Guide

**Original instructions**

**EIO0000004982.02**
**06/2026**

www.se.com

# Legal Information

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

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

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

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

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

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

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

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

# Table of Contents


Table of Contents ..... 3
Safety Information ..... 5
About the Document ..... 6
Introduction ..... 13
- Overview ..... 13
- Working With This User Guide ..... 13
- Network Architecture ..... 14
- Components of the Dedicated Server Version ..... 15
- Potential Risks and Threats to Mitigate ..... 16

Installation ..... 18
- Preparation ..... 18
- Delivery and Verification ..... 18
- Requirements ..... 19

Hardening ..... 20
- User Access Levels ..... 20
- Built-In Hardening Features ..... 20
- Hardening Measures to be Taken ..... 21
- Physical Security of the Infrastructure ..... 22

Operation ..... 23
- User Accounts ..... 23
- Management of Personal Data ..... 23
- Backups ..... 23
- Update ..... 24
- Schneider Electric Security Notifications ..... 24

Decommissioning ..... 25
- Deleting an Account ..... 25
- Erasing the Dedicated Server Version From the Infrastructure ..... 26

VM / On-Premise Servers ..... 27
- IT Interface ..... 27
- Server Administration ..... 29
- Network and Security ..... 30
- Users and Admins ..... 32

# 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 Document

## Document Scope

The present user guide describes cybersecurity aspects for the dedicated server version of the EcoStruxure Control Engineering software applications.

The information provided in the present hardening guide supplements the user guides of the EcoStruxure Control Engineering software applications.

For more information on Cybersecurity at Schneider Electric refer to https://www.se.com/ww/en/about-us/cybersecurity-data-protection/.

**⚠WARNING**

**UNINTENDED EQUIPMENT OPERATION, LOSS OF CONTROL, LOSS OF DATA**

You, and anyone owning, designing, operating and/or maintaining equipment using EcoStruxure Control Engineering, must read, understand, and follow the instructions outlined in the present document.

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

## Validity Note

This document has been updated for the release of EcoStruxure Control Engineering V26.0.

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.

# Product Related Information

The security of an IT infrastructure depends on the entirety of its components, their interconnections and a great array of additional factors. Only you, the owner, operator or user, can be aware of all factors that impact your specific IT infrastructure.

**⚠WARNING**

**INSUFFICIENT AND/OR INEFFECTIVE CYBERSECURITY**

- Perform a cybersecurity risk assessment as per ISO 27001 and/or as per Cybersecurity Framework of the National Institute of Standards and Technology (NIST) and/or other equivalent or required assessment in view of your use of EcoStruxure Control Engineering.
- Verify that all IT security requirements relating to your specific IT infrastructure are properly considered in your usage of EcoStruxure Control Engineering.
- Do not assume the information provided in the present user guide to be exhaustive with regard to your specific IT infrastructure and your specific cybersecurity requirements and obligations.

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

Machines, controllers, and related equipment are usually integrated into networks. Unauthorized persons and malware may gain access to the machine as well as to other devices on the network/fieldbus of the machine and connected networks because of insufficiently secure access to software and networks.

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 MACHINE OPERATION**

- Evaluate whether your application environments 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, such as an Intrusion Prevention System or Intrusion Detection System.
- Monitor activities within your systems.
- Prevent subject devices from direct access or direct link by unauthorized parties or unauthenticated actions.
- Install certificates that are issued by publicly known Trusted Certificate Authorities.
- Keep your systems up-to-date and rely only on legitimate sources.
- 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.

For reasons of Internet security, for those devices that have a native Ethernet connection, TCP/IP forwarding is disabled by default. Therefore, you must manually enable TCP/IP forwarding. However, doing so may expose your network to possible cyberattacks if you do not take additional measures to protect your enterprise. In addition, you may be subject to laws and regulations concerning cybersecurity.

## ⚠WARNING

**UNAUTHENTICATED ACCESS AND SUBSEQUENT NETWORK INTRUSION**

- Observe and respect any and all pertinent national, regional and local cybersecurity and/or personal data laws and regulations when enabling TCP/IP forwarding on an industrial network.
- 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.

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

Consult the Schneider Electric Cybersecurity Best Practices for additional information.

# General Cybersecurity Information

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

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

Schneider Electric provides additional information and assistance:

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

# Product Related Cybersecurity Information

Machines, controllers, and related equipment are usually integrated into networks. Unauthorized persons and malware may gain access to the machine as well as to other devices on the network/fieldbus of the machine and connected networks because of insufficiently secure access to software and networks.

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 MACHINE OPERATION**

- Evaluate whether your application environments 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, such as an Intrusion Prevention System or Intrusion Detection System.
- Monitor activities within your systems.
- Prevent subject devices from direct access or direct link by unauthorized parties or unauthenticated actions.
- Install certificates that are issued by publicly known Trusted Certificate Authorities.
- Keep your systems up-to-date and rely only on legitimate sources.
- 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.

For reasons of Internet security, for those devices that have a native Ethernet connection, TCP/IP forwarding is disabled by default. Therefore, you must manually enable TCP/IP forwarding. However, doing so may expose your network to possible cyberattacks if you do not take additional measures to protect your enterprise. In addition, you may be subject to laws and regulations concerning cybersecurity.

## ⚠WARNING

**UNAUTHENTICATED ACCESS AND SUBSEQUENT NETWORK INTRUSION**

- Observe and respect any and all pertinent national, regional and local cybersecurity and/or personal data laws and regulations when enabling TCP/IP forwarding on an industrial network.
- 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.

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

Consult the Schneider Electric Cybersecurity Best Practices for additional information.

# Related Documents

| Title of documentation | Reference number |
|---|---|
| EcoStruxure Control Engineering - Documentation - User Guide | EIO0000004426 (eng) |
| EcoStruxure Control Engineering - Converter - User Guide | EIO0000004425 (eng) |
| EcoStruxure Control Engineering - Verification - User Guide | EIO0000004424 (eng) |
| EcoStruxure Control Engineering - Tester - User Guide | EIO0000005747 (eng) |
| Cybersecurity Best Practices | CS-Best-Practices-2019-340 |

# Information on Non-Inclusive or Insensitive Terminology

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

# Terminology Derived from Standards

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

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

Among others, these standards include:

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

In addition, terms used in the 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.

# Introduction

## Overview

EcoStruxure Control Engineering is a suite of software applications that support developers of logic controller applications, engineers, system integrators and other industrial stakeholders in developing and maintaining logic controller code.

EcoStruxure Control Engineering is available in two versions:

- The EcoStruxure Control Engineering cloud version is a Software as a Service (SaaS) solution accessible at https://ecostruxure-control-engineering.se.app/. The cloud version is managed by Schneider Electric and provides compliance with pertinent cybersecurity standards.

  Available EcoStruxure Control Engineering software applications:

  - EcoStruxure Control Engineering - Documentation
  - EcoStruxure Control Engineering - Converter
  - EcoStruxure Control Engineering - Tester
  - EcoStruxure Control Engineering - Verification
- The dedicated server version is installed and operated on a local server in the infrastructure of the user.

  Available EcoStruxure Control Engineering software applications:

  - EcoStruxure Control Engineering - Documentation
  - EcoStruxure Control Engineering - Converter
  - EcoStruxure Control Engineering - Tester
  - EcoStruxure Control Engineering - Verification

The information provided in the present user guide relates to the dedicated server version.

## Working With This User Guide

The present user guide focuses on security aspects related to the installation, setup, operation and decommissioning of the dedicated server version of EcoStruxure Control Engineering.

It describes best practices for each phase of the lifecycle of the dedicated server version.

The typical phases are:

1. Installation/general setup
2. Hardening (initial setup of the appropriate security measures as determined by, among other things, the requirements of your organization)
3. Operation by the authorized users
4. Decommissioning (uninstalling and removing of the software components)

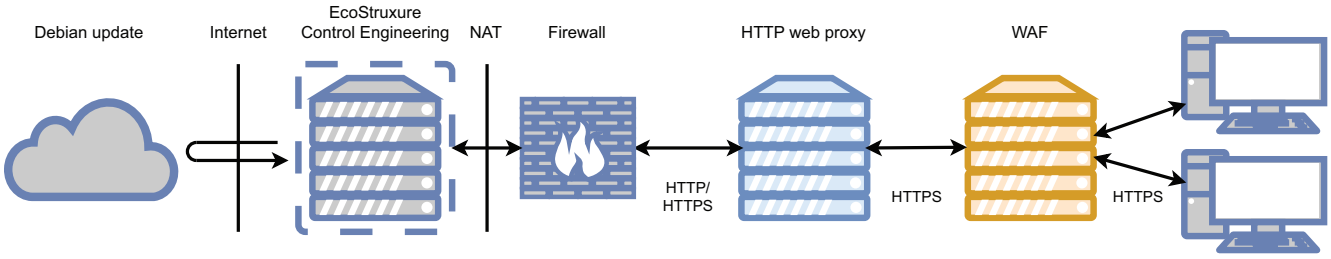
# Network Architecture

To integrate the dedicated server version in your network architecture, depending on your risks assessment and security policy, use additional network security components such as:

- Network Address Translation (NAT)-based network, isolated from the corporate network
- Firewall in front of the Virtual Machine
- Proxy server
- Web Application Firewall (WAF) in front of the other network components
- Virtual Machine with the ability to connect to and download content from the Debian security updates server
- Syslog Server

Use a self-hosted network architecture instead of a cloud-based setup.

Overview of the network architecture:



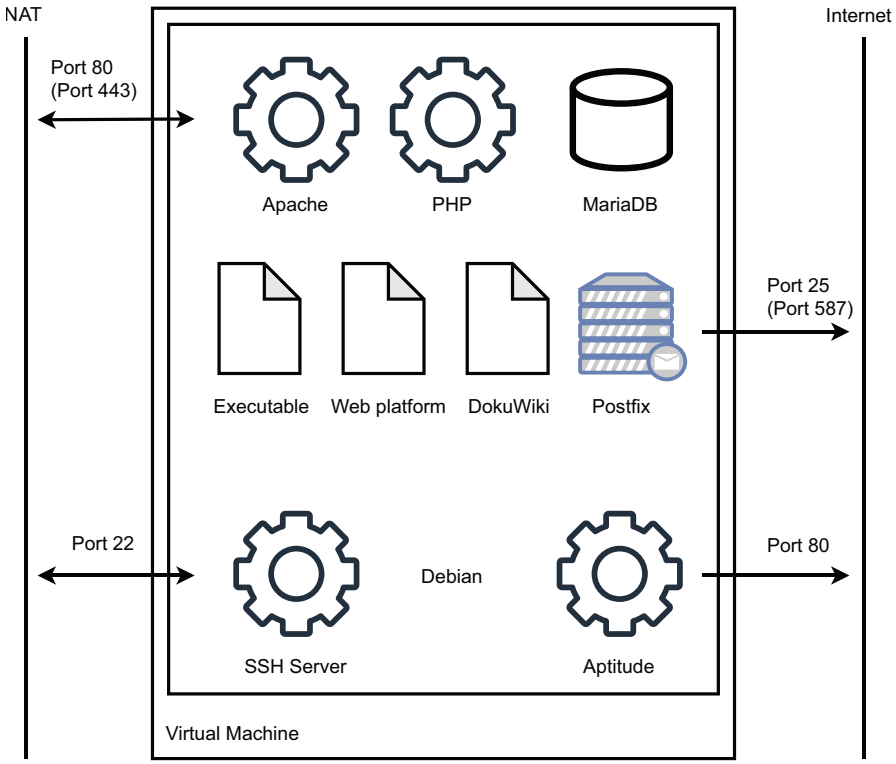

The present document provides details on setting up and operating this network architecture.

# Components of the Dedicated Server Version

The dedicated server version includes the following components:

| Component name | Description | Firewall rules |
|---|---|---|
| Debian | Operating system | - |
| Apache 2 | Web server | Open port 80.<br>Open port 443, if required |
| Postfix | SMTP mail relay, use is optional | - |
| SSH | SSH administration access<br>Disabled by default. To enable SSH, refer to **SSH Access**, page 30. | Open port 22 if required by Schneider Electric service representative |
| MariaDB | Database server | - |
| Texlive | PDF file generation | - |
| PHP | HTML generation | - |
| CakePHP | HTML framework | - |
| DokuWiki | Wiki engine | - |
| Subversion | Versioning system | - |
| EcoStruxure Control Engineering | EcoStruxure Control Engineering software applications, backend and frontend | - |
| Aptitude | Debian packet manager | Outgoing connections to Debian updates repository |

Graphical overview:




For further details contact your Schneider Electric service representative.

# Potential Risks and Threats to Mitigate

The following table helps you identify potential risks and threats related to the setup and use of your EcoStruxure Control Engineering software applications and provides good practices that can help mitigate these risks.

**NOTE:** The potential risks and mitigation measures described here are not exhaustive. Take all required measures to identify additional risks and vulnerabilities that may apply to your infrastructure.

| Category | Potential risk | Potential mitigation |
|---|---|---|
| Data theft or loss | Sensitive data are at risk of loss, leading to financial losses, reputational damage, legal issues and other detrimental consequences. | Network traffic monitoring, appropriate user account configuration, appropriate measures to verify the integrity of the software, appropriate Virtual Machine software, appropriate third-party protection<br>**NOTE:** In the present user guide, the generic term "Virtual Machine software" is used to refer to the software that executes the Virtual Machine. |
| Malware infections | Infection of the environment with malware, leading to a compromised or weakened component in the IT infrastructure | Network traffic monitoring, appropriate Virtual Machine software, appropriate third- party protection |
| Unauthorized access | Unauthorized users may gain access to the software, leading to data disclosure, corporate spying, installation of malware or other exploits, reputational damage, legal issues and other detrimental consequences | Network traffic monitoring, appropriate user accounts configuration, appropriate Virtual Machine software, appropriate third-party protection |
| Downtime and productivity loss | Unrecoverable conditions during which the software applications are not able to operate, leading to reduced productivity, financial losses, and other detrimental consequences | Appropriate backup and recovery policy, appropriate Virtual Machine software, appropriate third-party protection |
| Compliance violations | Any kind of non-compliance with regulatory requirements, leading to legal issues, financial losses, and other detrimental consequences | Appropriate user data management, corporate guidelines, appropriate third- party protection |

The following table links some of the potential risks and threats from the preceding table to individual software and hardware components:

| Potential risk | Impacted component | Cause | Potential mitigation |
|---|---|---|---|
| Unauthorized access | Administrative interfaces of Virtual Machine | Misconfigured firewall or web proxy, or vulnerability | Restrict access to the URLs **/server** and **/apis**, as described in Hardening Measures to be Taken, page 21. |
| | Firewall | Misconfigured user access management or vulnerability | Set up appropriate access management measures. |
| | HTTP web proxy | Misconfigured user access management or vulnerability | Set up appropriate access management measures. |
| | WAF | Misconfigured user access management or vulnerability | Set up appropriate access management measures. |
| Server not accessible | Hosting system for the Virtual Machine | Misconfigured virtual machine software<br>Hosting system unavailable | Ensure appropriate component configuration.<br>Implement redundancy. |
| | Virtual Machine | Virtual Machine shutdown<br>Misconfigured firewall, web proxy and/or WAF<br>Hosting system inoperative | Ensure appropriate configuration of third-party components, see also Hardening Measures to be Taken, page 21.<br>Implement redundancy. |
| | Firewall | Misconfiguration<br>Component inoperative | Ensure appropriate component configuration.<br>Implement redundancy. |
| | HTTP web proxy | Misconfiguration<br>Component inoperative | Ensure appropriate component configuration.<br>Implement redundancy. |

| Potential risk | Impacted component | Cause | Potential mitigation |
|---|---|---|---|
| | WAF | Misconfiguration<br><br>Component inoperative | Ensure appropriate component configuration.<br><br>Implement redundancy. |
| | Administrative interface of SSH | VM shutdown<br><br>Misconfigured firewall, web proxy and/or WAF<br><br>Hosting system inoperative | Ensure appropriate configuration of third-party components, see also Hardening Measures to be Taken, page 21. |
| Data loss | Virtual Machine | Virtual machine unavailable<br><br>Hardware inoperative | Implement appropriate backup policy, see Backups, page 23.<br><br>Implement redundancy. |
| Malware infection | Virtual Machine | Malware uploaded by a malicious user | Perform live scans of the network traffic as described in Hardening Measures to be Taken, page 21. |
| | WAF | Inability to scan malware in transit | Select a technology that can scan malware in transit, enable the functionality and verify correct operation on a regular basis. |
| | Administrative interface of SSH | Malware uploaded to the operating system by malicious user | Ensure appropriate firewall and NAT network settings as described in Hardening Measures to be Taken, page 21. |
| Data theft | Virtual Machine | Incorrect DHCP configuration<br><br>Impersonation of the Virtual Machine by a third-party component | Use static IP addressing.<br><br>Ensure appropriate configuration of third-party components, see also Hardening Measures to be Taken, page 21. |
| | Web proxy | Incorrect DHCP configuration<br><br>Man-In-The-Middle attack | Use static IP addressing.<br><br>Set up an HTTPS connection between the web proxy and other architecture components as described in Hardening Measures to be Taken, page 21. |
| | WAF | Improper DHCP configuration<br><br>Man-In-The-Middle attack | Use static IP addressing.<br><br>Set up an HTTPS connection between the web proxy and other architecture components as described in Hardening Measures to be Taken, page 21. |
| | Administrative interface of SSH | Improper DHCP configuration<br><br>Man-In-The-Middle attack | Use static IP addressing<br><br>Validate the SSH server signing certificate before connecting. |

# Installation

## Preparation

The EcoStruxure Control Engineering dedicated server version can be ordered from your Schneider Electric sales representative. During the preparation process, you may be contacted by Schneider Electric to gather information on the system configuration you require.

The Schneider Electric representative may request the following information:

- Environment on which the dedicated server will be hosted and executed
  - Type of network adapter connection to the dedicated server (for example, NAT or bridge)
- Type of connections for using the dedicated server
  - Other systems between the end user and the dedicated server, such as a proxy server and/or a WAF
  - Required HTTPS protocol setup (for example, corporate SSL certificate)
- Number of expected users of the dedicated server to help identify the amount of resources that need to be allocated to the Virtual Machine
- Single point of contact for delivery

## Delivery and Verification

The dedicated server version is delivered as an online shared folder by Schneider Electric. You will receive an e-mail containing the link to download:

- The Virtual Machine
- The integrity verification checksum of the Virtual Machine
- The hardening guide (the present guide)

The recipient of the e-mail is identified by the Schneider Electric service representative during the preparation of the dedicated server version. The delivery e-mail will only be sent from one of the following valid Schneider Electric e-mail addresses:

- *@se.com*
- *@non.se.com*
- *@verified.se.com*

Then, download the Virtual Machine export file and verify its integrity before installing or using it to ensure that the Virtual Machine originates from a Schneider Electric source and that it has not been altered between the time of preparation by Schneider Electric and your download.

To do so, ensure that the integrity verification checksum you have received in the delivery e-mail is the same as the checksum of the downloaded file. On **Microsoft Windows**, use the following command to compute the checksum of the downloaded file:

```
Get-FileHash <Path to the OVA file> -Algorithm SHA256
| Format-List
```

For **Linux-based operating systems**, use the following command to compute the checksum of the downloaded file:

```
sha256sum <Path to the OVA file>
```

The result on **Microsoft Windows** is, for example:

```
PS C:\Users\SE> Get-FileHash C:\Users\SE\Downloads\vm.ova -Algorithm SHA256
| Format-List

Algorithm : SHA256
Hash      : E370488754F2090E0FBD79D941BF24A83892B89BB5E252B2B2006E5E7D16230A
Path      : C:\Users\SE\Downloads\vm.ova
```

The result on a **Linux-based operating system** is, for example:

```
[SE@localhost ~]$ sha256sum /home/SE/Download/vm.ova

8ebfa12bf5f7cf3362d19177c6ee071a309b1efd8675208c6d05eebcdfa73557  /home/SE/
Download/vm.ova
```

Compare the result of the command (hash value displayed by Microsoft Windows or line displayed by Linux-based operating system) to the integrity verification checksum contained in the delivery e-mail. If the checksums are not identical, re-download the file and repeat the checksum comparison. If the condition persists, contact your Schneider Electric service representative.

# Requirements

After you have verified the correctness of the delivery, you can integrate it into your infrastructure.

Requirements for virtualization:

| Requirement | Description |
|---|---|
| Virtual Machine software examples (1) | VMware Workstation, Oracle VirtualBox<br><br>The Virtual Machine software must support OVA file version 1.0. |
| Network configuration | NAT, with the host OS ports 80 (HTTP) and/or 443 (HTTPS) redirected to the Virtual Machine ports 80.<br><br>Bridge if the Virtual Machine uses external services such as email server. |
| Disk space requirement | 200 GB minimum |
| RAM requirement | 8 GB minimum (up to four concurrent, intensive processes) |
| CPU requirement | 3 GHz, 1 core per logged-in user, 2 cores minimum |
| (1) Requires secure Virtual Machine software (also known as "virtualization hypervisor"). Secure Virtual Machine software includes features such as secure boot, encryption, and access control. You can also implement authenticated access to the Virtual Machine software and/or piece of software that may host or execute it. | |

For further details on requirements contact your Schneider Electric service representative.

# Hardening

## User Access Levels

Three user access levels are available:

| | Standard user | IT | General administrator |
|---|---|---|---|
| Description | This role is automatically assigned to any user who registers to EcoStruxure Control Engineering. | This role is applicable for your IT engineers. | This role is applicable for Schneider Electric service representative. |
| Task | Use the EcoStruxure Control Engineering software application. | Configure the EcoStruxure Control Engineering software application.<br><br>Set up and maintain the network components. | Administrate the EcoStruxure Control Engineering Virtual Machine. |
| Roles and access rights with regard to the network components: | | | |
| Virtual Machine | Use | Configure | Administrate |
| Firewall | Use | Administrate | Use |
| Web Proxy | Use | Administrate | Use |
| WAF | Use | Administrate | Use |
| Access points to Virtual Machine: | | | |
| Access point to Virtual Machine | http://<host>/ (if applicable)<br><br>https://<host>/ (if applicable) | http://<host>/server (if applicable)<br><br>https://<host>/server (if applicable) | Internal tool |

**NOTE:** The term "host" refers to the IP address or host name used to access the web interface.

## Built-In Hardening Features

The dedicated server version is hardened using several software features:

- Sessions are automatically terminated when the users are not active for a certain period of time
- User sessions are monitored and concurrent sessions of the same user can be closed remotely
- Input and output are filtered
- Access to user accounts is protected by restrictive rules for password definition
- User access levels to resources are enforced with an Access Control List (ACL) strategy
- Default settings are restrictive by default
- No third-party components such as Content Delivery Network (CDN)

# Hardening Measures to be Taken

The dedicated server version is not designed for direct exposure to public Internet or direct access, even in an internal, secured network. Install it in a properly secured environment behind a proxy server, a firewall or multiple firewalls, and, if appropriate, a WAF. Take all necessary measures to secure the access to the dedicated server version.

Measures to be taken:

- Ensure, with a specific configuration in the Virtual Machine hypervisor or using Network Segregation technics for the physical servers, that the proxy server is the only server able to contact the dedicated server version to help prevent external access to the dedicated server.
- Establish an HTTPS entry point at each component to secure the communication.
- Use a static IP address for each component, even if a DHCP server is used.
- Restrict access to inappropriate ports using a firewall and, when running the dedicated server using a NAT network driver, at the virtual network level. For example, if SSH is not used, close port 22.
- Restrict access to specific file types, for example third-party intellectual property.
- Create access logs to conduct a post-mortem analysis of any critical event.
- Monitor the infrastructure network for specific network events and/or conditions (for example, a large amount of data being transferred from the dedicated server may reveal an ongoing data extraction process).

To help protect the administration interface of the server version against unauthorized access, restrict access (based on password authentication, for example) by means of a proxy configuration to the **/server** endpoint. Monitor access to this endpoint and require users to authenticate because this endpoint is designed to configure the dedicated server.

If you do not need to use the integrated API, restrict access to the endpoint **/apis**. Monitor access to this endpoint.

Install the dedicated server version behind an HTTP proxy server. An HTTP proxy server allows you to customize access and security logs and to create an HTTPS to HTTP proxy.

Place the dedicated server version behind a WAF in the case of exposed servers. A WAF (Web Application Firewall) is an intermediary server that collects the queries sent from a client, subjects the queries to security analyses and then forwards the analyzed queries to another server which answers the queries.

Such a type of firewall helps to improve the security of the dedicated server. The additional security level provided by a WAF depends on its capabilities. Use a WAF designed to protect against or to help diagnose, at a minimum, the Open Worldwide Application Security Project (OWASP) TOP 10 vulnerabilities. At the date of publication of the present user guide, the OWASP TOP 10 vulnerabilities are:

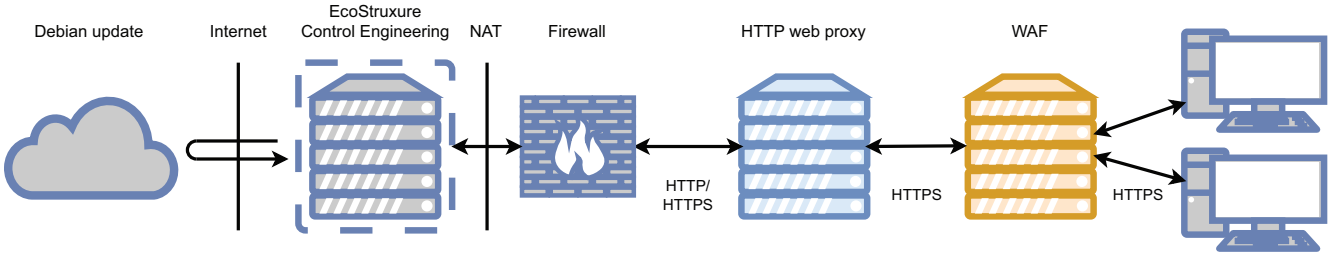
- Broken access control
- Cryptographic failures
- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated components
- Identification and authentication failures
- Software and data integrity failures
- Security logging and monitoring failures
- Server-side request forgery

**NOTE:** Implement measures to ensure that your organization keeps track of and assesses new threats and vulnerabilities, and adopt and/or complement your security measures accordingly.

Security features that the WAF should include are behavioral analytics to help detect unauthorized actions, and anti-virus detection software that helps to prevent malware injection into the infrastructure.

Establish a standard firewall that is relevant for your security strategy. Restricting access to ports 80 and 443 (if HTTPS is enabled) using a firewall is a practice that can help prevent misconfiguration resulting from inadequately defined security settings.

The following illustration shows a typical setup:




# Physical Security of the Infrastructure

Take all measures as defined by your risk assessment and security policies to secure the physical infrastructure.

For example, install the physical infrastructure (including the servers and related equipment required to run the system) in a room that is secured in an appropriate manner (such as locked doors, locked equipment, surveillance cameras, restricted physical access with per-user or per-role based authorization using keycards, biometric authorization, or other access control authorization).

# Operation

## User Accounts

Create one account for each physical user to monitor compliance with terms of service. Verify that the user accounts comply with the password or authentication policy of EcoStruxure Control Engineering.

A single user account can be used to authenticate multiple simultaneous sessions. A notification is sent to the web browsers of currently authenticated sessions of an individual user account whenever an additional session is started with that user account. This notification allows you to close other sessions with your user account in the case of, for example, suspected impersonation. Do not ignore such notifications.

## Management of Personal Data

The dedicated server version includes content that may lead to data disclosure if not used properly.

Data misuse can include:

- Sharing of results, comments, intellectual property and personal information (identity and e-mail address) for the purpose of team collaboration on a project.
- Listing of personal information on specific users (identity and e-mail address) when a contract model is used (paid once for several users during a specified time) for the purpose of team collaboration.

The following measures can help to protect personal information of users from disclosure:

- Create a privacy policy outlining the objectives of collecting such information and the extent to which it is used and shared, and have the users accept this privacy policy.
- Only use corporate data such as corporate e-mail addresses to register users for the dedicated server version.
- Limit the amount of information saved by the dedicated server version to the necessary minimum.
- Avoid traceable personal information by using, for example, initials instead of full names or anonymized e-mail addresses
- Verify compliance with all regulatory requirements concerning data protection and privacy such as, but not limited to, the General Data Protection Regulation (GDPR) in Europe or the Personal Information Protection Law (PIPL) in China.

## Backups

Perform backups as defined by your risk assessment, security policies, and other process definitions of your organization.

A robust backup policy helps to reduce the potential of downtimes and loss of data (for example, caused by malware, data corruption, inoperable hardware). Perform regular backups of the Virtual Machine. The frequency of backups depends on, among other things, the acceptable risk level with regard to loss of data as defined by your organization. For example, if it is acceptable to lose up to two days of data in the case of an unrecoverable condition, perform backups of the Virtual Machine at a minimum frequency of two days.

In your backup policy, also consider all other factors affecting a backup, such as, but not limited to, the backup technology, the number of backups to be kept, the time required to perform a backup, the integrity of the backup, and the storage of the backup media. Verify that backups can be restored as intended. Perform regular tests of the backup and restore process.

# Update

If updates of the EcoStruxure Control Engineering application software are available, Schneider Electric provides an update patch that you must install.

Procedure:

| Step | Action |
|---|---|
| 1 | Access the administration interface at **/server**.<br>**NOTE:** Depending on the security measures in place in your organization, you may need to log in to access the page. |
| 2 | Select **Apply a server update package**. |
| 3 | Upload the update package either by selecting **Select Files...** or by using drag & drop. The upload progress is displayed during the upload process. |
| 4 | Select **Update** to complete the update. |

An update patch only updates the EcoStruxure Control Engineering application software.

The Virtual Machine is delivered with a pre-installed operating system and a pre-installed software stack (HTTP server, database server, etc.), see Components of the Dedicated Server Version, page 15. This software stack is managed by Schneider Electric and configured in such a way that it can receive and automatically set up the security updates distributed by the operating system vendor.

The Virtual Machines require access to http://security.debian.org/, to obtain such updates.

The security updates are verified and performed daily, if necessary. Allow the dedicated server version to download security updates on a daily basis. The updates help to ensure that core operating system components have the latest available level of security provided by the operating system vendor.

For further details refer to https://www.debian.org/security/.

# Schneider Electric Security Notifications

Subscribe to the Schneider Electric security notifications at https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp. The security notifications support you in tracking and mitigating vulnerabilities.

Verify that your subscription to the Schneider Electric security notifications is valid and effective on an ongoing basis.

# Decommissioning

# Deleting an Account

## Creating a Backup

Before decommissioning a user account, create a backup of the information that was created with the download function of the EcoStruxure Control Engineering software applications. The download function is not available with the free trial license.

Procedure for a backup:

| Step | Action |
|---|---|
| 1 | Identify the content of the program(s) to be downloaded. |
| 2 | Navigate to the dashboard of the program(s) using the **PROJECTS** menu.<br>Select the project in which the program is located.<br>Select the program(s). |
| 3 | Display the tab **Admin** and select **Repository**.<br>**Result**: The list of the files contained in the program repository is displayed. |
| 4 | Select **Download repository (ZIP)**.<br>**Result**: The content of the repository is downloaded by the web browser as a ZIP file. |
| 5 | Repeat the steps for each project and program you want to download. |

## Deleting an Account

You can request your account to be deleted in your personal profile. Account deletion requires two-factor authentication.

A deleted account cannot be restored, therefore create a record before deleting an account.

**NOTE:** This process is only available if an e-mail server is properly setup.

Procedure for requesting account deletion and deleting an account:

| Step | Action |
|---|---|
| 1 | Click your user name displayed in the top right part of each page and select **My Account** from the menu.<br>**Result**: The user profile page is displayed. |
| 2 | Display the **Privacy** tab. |
| 3 | Scroll down to and select **Click here to start the user account deletion process**.<br>Confirm that you want to continue the user account deletion process.<br>**Result**: An e-mail is sent to you. |
| 4 | Click the link in the e-mail you have received<br>**Result**: The dedicated server version opens. |
| 5 | Confirm that you want to continue the user account deletion process.<br>**Result**: The user is redirected to the login page. The user account is deleted. |

Identifying information is removed from the user account after this process; the personal information of the user is no longer available on the server.

# Erasing the Dedicated Server Version From the Infrastructure

The procedure for decommissioning the dedicated server depends on, among other things, the decommissioning procedures set up by your organization. Adapt these procedures to the EcoStruxure Control Engineering installation in your organization.

Typical steps include:

- Identify the usage level and business implication of decommissioning the dedicated server.
- Notify the users in compliance with the process definitions effective in your organization.
- Create a backup, page 25 of the data identified as important and verify that the backup works as intended.
- Disconnect the dedicated server from the network to make it unavailable to users.
- Delete the image of the dedicated server and the instances from the infrastructure.
- Erase the data such as usage logs (HTTP server access logs, operations), intellectual property (logic controller code), results of your work with EcoStruxure Control Engineering software applications, on the hard disk of the physical server in such a way that no data can be restored.

Erasing the dedicated server version from the hard disk can be performed by, for example, hard disk formatting with random bits/pattern rewriting before using the hard disk for other purposes.

Backup media may be a source of unintended data leaks if they are not handled properly.

# VM / On-Premise Servers

# IT Interface

## Authentication

The login page allows authorized persons only to access management functions. As long as an administrator is not logged in, it is not possible to access the other pages of the interface.

The credentials used to connect to the administration interface are distinct from those used on the web version. If the web platform credentials are compromised, access to the administration interface is not affected.

Monitor access to administration pages using the appropriate systems, depending on your IT installation.

**NOTE:** The admin account created and supplied by default is unique for each server. However, for enhanced confidentiality and security, you must create a new admin account and delete the default account.

## Dashboard

The dashboard provides an overview of the system environment components, enabling system management by providing data and alerts on critical issues:

- **Statistics widgets:** Displaying factual data about the VM. They allow to view essential information and provide direct links to the pages dealing with this data.
- **Notifications area:** This area highlights important information on potential issues, such as security concerns, hard drive space, or activity logs.

## Menu Bar

The menu bar on the left allows to move between the different sections of the interface. There are also 3 possible actions accessible at any time from this bar:

- The reboot of the VM
- The shutdown of the VM
- The disconnection of the admin interface

For more details about reboot and shutdown see **Reboot**/ **Shutdown** Operations Buttons, page 28.

## Email Server Configuration

This page is used to configure an email server so that the web platform can use email as a means of communication. Once configured, the platform can send emails to notify that analyses have been completed, or to inform of suspicious activities detected on the account.

**NOTE:** Configuring a mailbox also allows to set a new password, if needed.

# Reboot/ Shutdown Operations Buttons

The dashboard features two buttons for stopping and restarting the VM:

- **Reboot button:** When the reboot is initiated, all running tasks are stopped. The restart is then performed. Throughout the process, a progress bar is displayed to keep the user informed on the progress. At the end of the restart, the user is redirected to the dashboard page.
- **Shutdown button:** When shutdown is initiated, all running tasks are also stopped. The shutdown is then performed. Once the web browser can no longer contact the VM, a message is displayed to inform the user that the VM has been stopped.

# Server Administration

## Apply Update

This page allows you to send files supplied by Schneider Electric to update specific internal components of the VM. The intended recipients of these updates are the VM administrators responsible for the management and maintenance of the system.

These updates can have several different objectives:

- Upgrade of the web platform: This refers to the enhancement or update of the interface and features.
- Update of the binaries (backend): This concerns the executable files and programs that operate in the background to run the system.
- Apply security patches to help strengthen system security against vulnerabilities.
- Install patches that fix bugs or improve performance.
- Implement mitigations to help reduce the risk of security issues.

**NOTE:** The VM operating system can automatically update itself when connected to Internet. It is possible to check if the VM is able to update itself by consulting the Network and Security, page 30.

## Component Version Switching

The version selection page in the VM offers flexibility and enables management of different versions of platform components. When several versions of the web platform, backend, integrated wiki and integrated downloadable files are available. Here is why and how it works:

- **Downgrade version:** If a new version of the backend is deployed but does not meet your needs or expectations, you can revert to a previous version that did.
- **Manage versions:** This enables different versions to be tested without affecting the stability of the production environment. You can compare the performance and functionalities of different versions.

To use these features, use the **Available Versions** header to display all the versions available for each component (web platform, backend, integrated wiki, downloadable files). You can then select here the version that you want to use.

**NOTE:** If the feature is not available, the component has only one version. Therefore, it is not possible to choose another version for this component.

## Running Jobs Management

This page displays all tasks currently running and allows you to stop them. This includes tasks such as Verification, Documentation and Conversion.

Administrators can choose to stop a task in progress. When a task is stopped in this way, it is considered to have failed by the web platform.

If the task uses a single-use license, this license is regenerated, meaning it can be reused for another task.

Stopping the task is recorded in the program history, keeping track of the actions performed.

# Network and Security

## Network Diagnostic

This page lists all the servers that the VM uses or communicates with. This includes both internal and external servers. For each server, the page indicates whether communications are valid or not, helping to identify potential network problems. This feature is intended to diagnose problems, but it does not replace the expertise of an IT administrator.

**NOTE:** This page also allows to check if the automatic updates are enabled.

## Mail Server

This page allows you to configure an e-mail server for user notifications and user account management.

## Secure Connection

On the **Secure Connection** page, it is possible to switch between the three connection protocols at any time:

- **HTTP (Hypertext Transfer Protocol):** This is the standard protocol for data transmission on the Web. However, it is considered insecure, as the data exchanged is not encrypted.
- **HTTPS (HTTP Secure):** HTTP with a self-signed certificate of HTTP, using encryption to help protect exchanged data. However, because the certificate is not issued by a trusted authority, users cannot verify the server's identity. As a result, the connection may still be vulnerable to impersonation or interception.
- **HTTPS with a personalized certificate:** This is the most secure option. A personalized certificate is signed by a recognized certification authority. The website identity is authentic and communications are both encrypted and authenticated.

## Platform Timeouts

This page permits to configure customized expiration times. The platform supports two types of expiration times:

- **Inactivity timeout:** The timer disconnects you after a certain period of time if you have not performed any operations on the web platform. This feature is designed to help protect your sessions by automatically disconnecting you in the event of prolonged inactivity. You can modify the default inactivity time-out.
- **Session timeout:** The timer disconnects you after a certain period of time, whether you have been active or not. This forces the system to regenerate sessions, reducing the risks associated with compromised or leaked sessions.

## SSH Access

This page allows you to enable or disable an SSH access to the operating system. By default, the SSH access is disabled. If you enable the SSH access, it is automatically disabled on server reboot.
On the **SSH Access** page, you can monitor users connected with SSH, if any.

# Syslog Server Configuration

You can configure your VM to forward system logs to an external Syslog server. This is useful for centralized log management, monitoring, and auditing.

Communications with the external Syslog server can be in plaintext, encrypted, or encrypted and verified.

| Step | Action |
|---|---|
| 1 | Click on Syslog Server. |
| 2 | Choose your Syslog communication type.<br>Enter Syslog Server Details:<br>• Server Address: Enter the IP address of your Syslog server.<br>• Port (optional): Specify the port number if different from 514.<br>• Protocol: Choose the protocol used by your Syslog server:<br>◦ UDP<br>◦ TCP<br>◦ UDP / TCP<br>For **Encrypted Communications, server authenticated**, provide a Syslog Certificate authority file.<br>For **Encrypted Communications, server and client authenticated**, provide a Syslog Certificate authority file and a Signed Client Syslog Certificate file. |
| 3 | Click **Apply Configuration** to enable the log forwarding option to start sending logs to the specified server.<br>**NOTE:** You can disable log forwarding at any time. Click **Disable The Syslog Server** to toggle off the configuration. |
| 4 | Use the **Generate A Dummy Log** feature to verify that your Syslog server is receiving logs correctly. |

# View Administration Logs

This page permits to read and download the logs of the administrator website. The logs contain a detailed list of operations carried out by administrators (connection/disconnection, change of protocol, account updates, creation of admins, and so on).

**NOTE:** Administrators cannot delete or update these logs. For integrity and traceability reasons.

# Users and Admins

## Administrative Accounts Management

This page allows administrators to add and remove other administrators. When an administrator is added, it is necessary to define a password as it is not possible to do it afterwards.

## Standard Users Accounts Management

This page permits to manage users registered. Here are the main features it offers to administrators:

- **Enable/Disable users:**
  - Activate: Enables users to access EcoStruxure Control Engineering.
  - Disable: Prevents users from accessing EcoStruxure Control Engineering in the case of a departure or temporary suspension of a user.
- **List licenses associated with user accounts:**
  Administrators can see all the licenses associated with each user account. They cannot assign licenses to other users, but users themselves can transfer licenses if they are eligible.
- **Reset user account passwords:**
  Administrators can reset user passwords. This feature is useful when no email server has been configured.

  **NOTE:** If you configured an email server, users can also reset their password autonomously.

## Notification Configuration

This page allows you to configure two types of notifications that are displayed only on the login screen.

- **Privacy notification:**
  - This notification is displayed in addition to the standard privacy policy of the platform.
  - It helps to meet certain requirements of the GDPR (General Data Protection Regulation), for example by providing additional information on how user data is processed.
- **Generic notification:**
  - This notification is not contextualized and is displayed in a single pop-up window. It can be configured or altered according to each situation.
  - It can be used to inform users of an upcoming maintenance operation, for example, alerting them before the operation is due to take place, without disrupting their user experience.

Schneider Electric
1884 Boulevard de la Défense
92000 Nanterre
France

www.se.com

© 2026 Schneider Electric. All rights reserved.

EIO0000004982.02