EcoStruxure™ Control Engineering

Hardening Guide

Original instructions

EIO0000004982.00
06/2023

www.se.com

Legal Information

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

This guide and its content are protected under applicable copyright laws and furnished for informational use only. No part of this guide 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 guide or its content, except for a non-exclusive and personal license to consult it on an "as is" basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change 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 material or consequences arising out of or resulting from the use of the information contained herein.

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.

Table of Contents

Safety Information 5
About the Book 6
Introduction 10
- Overview 10
- Working With This User Guide 10
- Network Architecture 11
- Components of the Dedicated Server Version 12
- Potential Risks and Threats to Mitigate 13

Installation 15
- Preparation 15
- Delivery and Verification 15
- Requirements 16

Hardening 17
- User Access Levels 17
- Built-In Hardening Features 17
- Hardening Measures to be Taken 18
- Physical Security of the Infrastructure 19

Operation 20
- User Accounts 20
- Management of Personal Data 20
- Backups 20
- Update 21
- Schneider Electric Security Notifications 21

Decommissioning 22
- Deleting an Account 22
- Erasing the Dedicated Server Version From the Infrastructure 23

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

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 V23.1.

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™ Control Engineering - Hardening Guide (this user guide)	EIO0000004982 (eng)
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 - Monitoring - User Guide	EIO0000004427 (eng)
Cybersecurity Best Practices	CS-Best-Practices-2019-340

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 environment or your machines 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.

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.

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.

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, maintaining and monitoring 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 - 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 - Verification
  - EcoStruxure Control Engineering - Monitoring

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)

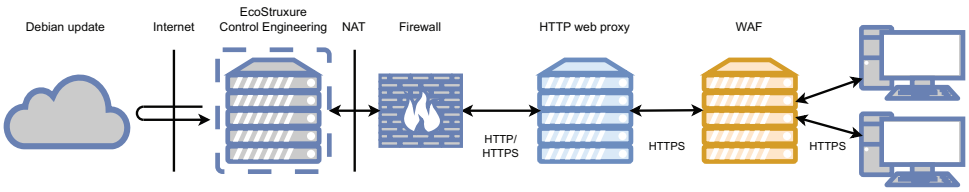
Network Architecture

The dedicated server version must be integrated into your network architecture with the following components:

- 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

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. Contact your Schneider Electric representative if you want to use a different network architecture.

The following components are not included in the dedicated server version. You must select, set up, operate and monitor these components as defined by your risk assessment and security policies:

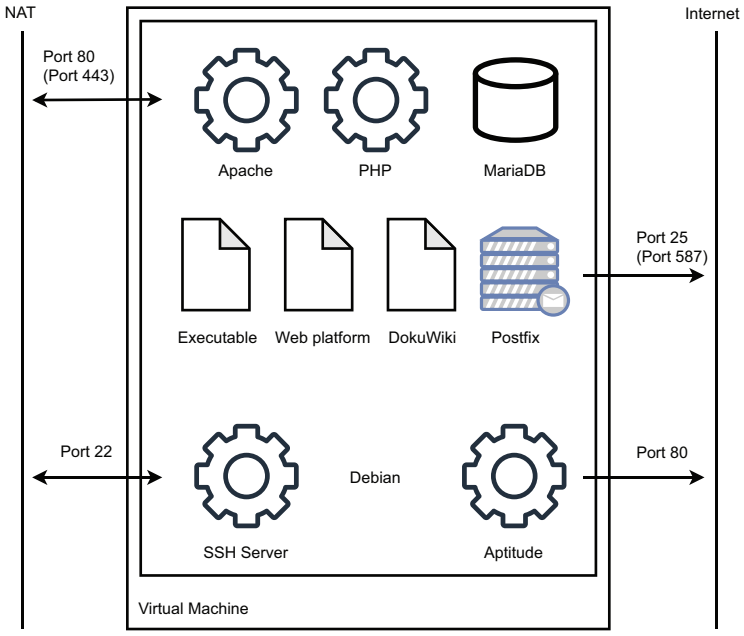
- Firewall in front of the Virtual Machine
- Proxy server
- WAF in front of the other network components

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. Open port 443, if required
Postfix	SMTP mail relay, use is optional	-
SSH	SSH administration access	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 **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 18.
	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 Hosting system unavailable	Ensure appropriate component configuration. Implement redundancy.
	Virtual Machine	Virtual Machine shutdown Misconfigured firewall, web proxy and/or WAF Hosting system inoperative	Ensure appropriate configuration of third-party components, see also Hardening Measures to be Taken, page 18. Implement redundancy.
	Firewall	Misconfiguration Component inoperative	Ensure appropriate component configuration. Implement redundancy.
	HTTP web proxy	Misconfiguration Component inoperative	Ensure appropriate component configuration. Implement redundancy.

Potential risk	Impacted component	Cause	Potential mitigation
	WAF	Misconfiguration Component inoperative	Ensure appropriate component configuration. Implement redundancy.
	Administrative interface of SSH	VM shutdown Misconfigured firewall, web proxy and/or WAF Hosting system inoperative	Ensure appropriate configuration of third-party components, see also Hardening Measures to be Taken, page 18.
Data loss	Virtual Machine	Virtual machine unavailable Hardware inoperative	Implement appropriate backup policy, see Backups, page 20. 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 18.
	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 18.
Data theft	Virtual Machine	Incorrect DHCP configuration Impersonation of the Virtual Machine by a third-party component	Use static IP addressing. Ensure appropriate configuration of third-party components, see also Hardening Measures to be Taken, page 18.
	Web proxy	Incorrect DHCP configuration Man-In-The-Middle attack	Use static IP addressing. Set up an HTTPS connection between the web proxy and other architecture components as described in Hardening Measures to be Taken, page 18.
	WAF	Improper DHCP configuration Man-In-The-Middle attack	Use static IP addressing. Set up an HTTPS connection between the web proxy and other architecture components as described in Hardening Measures to be Taken, page 18.
	Administrative interface of SSH	Improper DHCP configuration Man-In-The-Middle attack	Use static IP addressing 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 file and 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 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 (HTTP) and/or 443 (HTTPS). Bridge if the Virtual Machine uses external services such as a mail 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. 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) https://<host>/ (if applicable)	http://<host>/server (if applicable) 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:

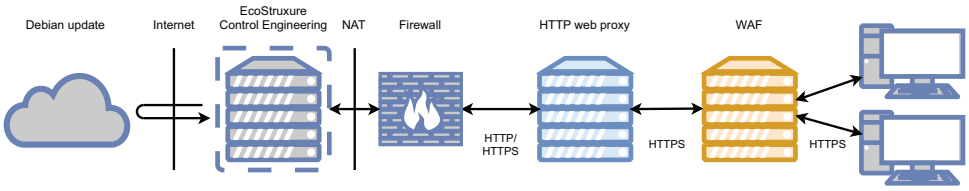
- Broken access control
- Cryptographic failures
- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated components
- Identification and authentication failures
- Software and data integrity failures
- Security logging and monitoring failures
- Server-side request forgery

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**. **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 12. 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 the following address on the Internet to obtain such updates:

- http://security.debian.org/

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. Select the project in which the program is located. Select the program(s).
3	Display the tab **Admin** and select **Repository**. **Result**: The list of the files contained in the program repository is displayed.
4	Select **Download repository (ZIP)**. **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. **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**. Confirm that you want to continue the user account deletion process. **Result**: An e-mail is sent to you.
4	Click the link in the e-mail you have received **Result**: The dedicated server version opens.
5	Confirm that you want to continue the user account deletion process. **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 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 on the hard disk of the physical server in such a way that no data can be restored.

Erase the data on the hard disk of the physical server in such a way that no data can be restored because the Virtual Machine may still contain 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, etc. 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.

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.

EIO0000004982.00