EcoStruxure Building Activate

Cybersecurity Hardening Guide

EcoStruxure offers IoT-enabled architecture and platform.

06/2025

DOCA0396EN-00

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

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

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

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

Table of Contents

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

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

A qualified personnel 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.

Cybersecurity Safety Notice

⚠WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.
- Disable unused ports/services and default accounts to help minimize pathways for malicious attackers.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example, least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, or interruption of services.

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

About the Document

Document Scope

This guide provides information on cybersecurity aspects for EcoStruxure™ Flex-Server to help system designers and operators promote a secure operating environment for the product. This guide does not address the more general topic of how to secure your operational technology network, or your company Wi-Fi Ethernet network. For a general introduction to cybersecurity threats and how to address them, refer to How Can I Reduce Vulnerability to Cyber Attacks?

NOTE: In this guide, the term security is used to refer to cybersecurity.

Validity Note

The information in this guide is relevant for EcoStruxure™ Flex-Server.

The characteristics of the products described in this document are intended to match the characteristics that are available on www.se.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.se.com, consider www.se.com to contain the latest 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.

Related Documents

Title of documentation	Reference number
Cybersecurity Best Practices	General Cybersecurity Information, page 7
EcoStruxure™ Building Activate - User Guide	DOCA0343EN-00
How Can I Reduce Vulnerability to Cyber Attacks?	Cybersecurity System Technical Note

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

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.

Introduction to Cybersecurity

EcoStruxure Master Range

EcoStruxure is Schneider Electric's IoT-enabled, plug-and-play, open, interoperable architecture and platform, in Homes, Buildings, Data Centers, Infrastructure and Industries. Innovation at Every Level from Connected Products to Edge Control, and Apps, Analytics and Services.

Introduction

Cybersecurity helps protect your communication network and connected equipment from attacks that could disrupt operations (availability), modify information (integrity), or reveal confidential information (confidentiality). The objective of cybersecurity is to provide increased protection for information and physical assets from theft, corruption, misuse, or accidents, while allowing intended users to access them.

Cybersecurity includes many aspects, such as designing secure systems, restricting access using physical and digital methods, identifying users, and implementing security procedures and best practice policies.

Schneider Electric Guidelines

In addition to the recommendations provided in this guide that are specific to EcoStruxure™ Flex-Server, you should follow the Schneider Electric defense-in-depth approach to cybersecurity. This approach is described in the system technical note How Can I Reduce Vulnerability to Cyber Attacks?

Schneider Electric Cybersecurity Policies and Rules

Schneider Electric uses a Secure Development Lifecycle (SDL) process, a key product development-based framework that helps ensure products follow secure design processes across all lifecycle stages. The Schneider Electric SDL process complies with IEC 62443-4.1.

The SDL process includes the following:

- SDL practices applied to internal development actions, throughout the supply chain.
- Final security review required for project release.
- Security training for personnel involved in the product development.

Device Characteristics

Overview

The EcoStruxure™ Flex-Server has security-enabling features. These features come in a preset state, and you can modify them to meet your installation needs. Qualified personnel must configure and set the EcoStruxure™ Flex-Server because disabling or changing settings affects the overall security robustness of the EcoStruxure™ Flex-Server and your network security.

To set up the EcoStruxure™ Flex-Server features and settings, use this guide along with the EcoStruxure Building Activate - User Guide.

EcoStruxure™ Flex-Server Interfaces

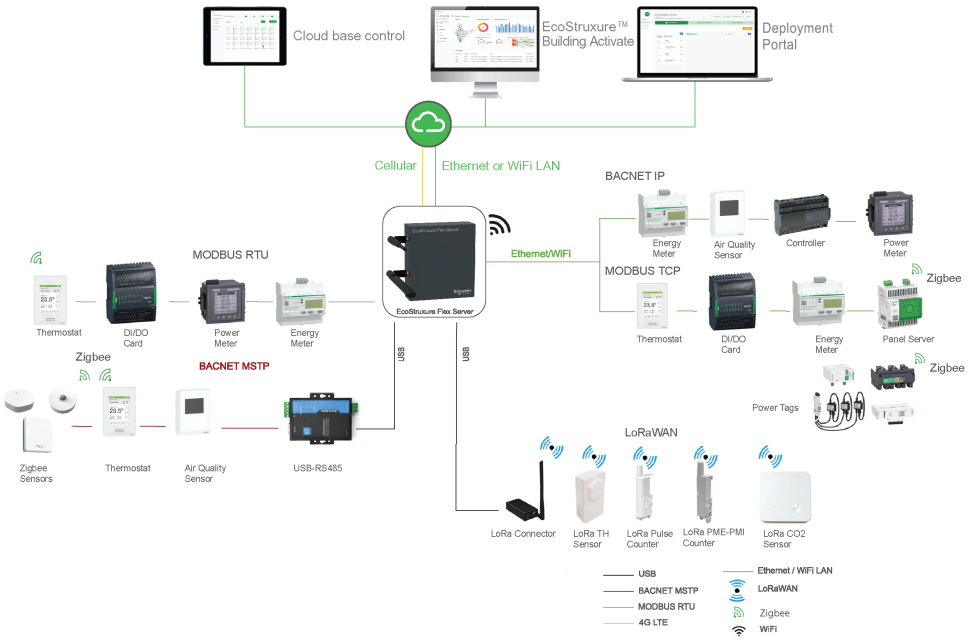
The EcoStruxure™ Flex-Server communicates through the following interface types:

- Wired communication through:
  - One Ethernet port
  - One RS-485 port
  - Two USB Ports
- Radio communication through:
  - Wi-Fi infrastructure
  - LoRaWAN Modem
  - Cellular/LTE Modem

Supported Protocols

The EcoStruxure™ Flex-Server supports the following protocols:

- HTTPS and MQTTS (TLS v1.2)
- CoAP over DTLS
- BACnet MSTP and BACnet IP for communications with other Operational Technology (OT) devices
- SNMP for communications with other Operational Technology (OT) devices
- Modbus TCP and Modbus-RTU for communications with other Operational Technology (OT) devices
- LoRaWAN for wireless communications with IoT devices
- OpenVPN client for remote access (open to Schneider Electric)
- DHCP for network IP addressing
- DNS for network name resolution
- NTP for time synchronization
- WPA2 and WPA for Wi-Fi communication



Security Features

EcoStruxure™ Flex-Server supports the following security features:

- Schneider Electric digitally signs the only firmware that can be installed on the EcoStruxure™ Flex-Server.
- At each boot, the system validates the firmware digital signature before execution, to help ensure that it has not been tampered.
- User passwords are stored as salted and hashed (SHA256) passwords.
- The device has an internal clock and maintains its date and time for a few months without power.

Device Features

Firmware Update

Update your EcoStruxure™ Flex-Server to the latest firmware version to obtain the latest features and keep up-to-date with security patches. Schneider Electric's Public Key Infrastructure (PKI) signs all firmware designed for the EcoStruxure™ Flex-Server to help provide integrity and authenticity of the firmware running on it. For proper PKI operation, synchronize the device date.

Register for Security Notifications on the Schneider Electric Cybersecurity Support Portal for regular security updates. Ensure your device's Date and Time are correctly set.

Date and Time

The EcoStruxure™ Flex-Server contains certificates and digital signatures. To avoid errors, ensure the date and time are synchronized.

TCP Ports

The following TCP ports are used in EcoStruxure™ Flex-Server:

- Outbound:
  - Port 443: HTTPS
  - Port 443: MQTTS
- Inbound (Ethernet/ Wi-Fi):
  - Port 47808: TCP
  - Port 47809: TCP
  - Port 13001: HTTP

Audit Logs

Cloud Apps generates audit logs that record events such as invalid login attempts, device management, configuration changes and firmware updates. These logs do not contain any personal information.

To detect unexpected behavior of EcoStruxure™ Flex-Server (for example, frequent rebooting, incorrect firmware update, changes to network configuration), it is recommended to monitor EcoStruxure™ Flex-Server health streams regularly.

The cloud apps generate internal tickets and assign them to troubleshooting engineers when predefined rules detect anomalies based on these health streams.

NOTE: EcoStruxure™ Flex-Server generate local audit logs that record configuration changes, API calls and firmware update.

Device Disposal

EcoStruxure™ Flex-Server contains confidential information, for example recent data values and logs, Modbus device topology, wireless networks, Wi-Fi passwords, or measured power consumptions.

Completely format the storage before disposing of the EcoStruxure™ Flex-Server . You must have physical access to power cycle theEcoStruxure™ Flex-Server while executing this procedure.

For more information, refer to EcoStruxure Building Activate - User Guide.

Cloud Application Security

Secure Account Management

NOTICE

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Do not sign in the Cloud Portal where humans or cameras may monitor password entry.
- Account managers must only grant access to users (Business users, Partner Administrators, Installers, etc.) authorized to use the Cloud Portal and related applications. If a user chooses to opt out of the system, account managers must disable their inactive accounts.

Failure to follow these instructions can result in equipment damage.

The Admin Dashboard creates new users and assigns appropriate permissions in the system. The service decides each user's level of access to an application across a customer's site(s). This user can then use the password reset portal to verify their credentials and generate a password.

- Whenever creating a new user in the system, ensure that,
  - You verify the user's Email ID and phone number are correct.
  - You set the user's language preference correctly.
  - You select the customer, site, and access carefully to avoid any unwanted access.
  - You give access to individual applications after reviewing the permission groups.
- You cannot create a user in the system if no customer's site is associated with the user.
- Account managers or the program management team at Schneider Electric can create users.
- When signing in for the first time, the user must:
  - Verify the email address and phone number.
  - Set the password.
  - Go through and accept the Privacy Policy to proceed.
- The user must ensure the password they set complies with the password policy displayed on our dashboards alongside the password setting screen. The password policy requires:
  - At least one uppercase (capital) character.
  - At least one lowercase (small) character.
  - At least one number (like 1234).
  - At least one special character (like #?!@$%^&*-).
  - No whitespaces.
  - A minimum length of 8 characters.
  - A maximum length of 15 characters.

We have implemented 2FA across our services, allowing the user to choose email or phone number to verify their credentials at login.

If the user wishes to withdraw from the privacy policy at any point, they can find an option to withdraw in the profile section of the dashboard. However, to access the dashboard again, the user will have to accept the policy at login.

If a user enters an incorrect password or OTP five times consecutively, the system will block access to their account or password reset for 15 minutes.

Network Security

NOTICE

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Install the Ethernet cables inside wall cavities, or in conduit.
- Install the Flex-Server in a way that only authorized people can access the device, for example, in a locked cabinet or secure room, or using a secure wall box.
- When utilizing cellular networks, it is imperative for users to exercise caution regarding data overages, and it is recommended to set up alarms or monitoring systems to mitigate the risk of incurring substantial charges.
- If BACnet is used over Ethernet and Wi-Fi is used for internet, the network priority needs to be adjusted accordingly.

Failure to follow these instructions can result in equipment damage.

EcoStruxure™ Flex-Server has multiple connectivity options to access internet such as cellular, Wi-Fi and Ethernet. It is not designed to withstand direct exposure to the public Internet. It must be installed at least behind Network Address Translation (NAT) or preferably behind multiple firewalls.

EcoStruxure™ Flex-Server has internal firewall rules to prevent incoming traffic over all interfaces namely wwan0 (cellular), *wlan0 (wi-fi) and *eth0 (ethernet).

NOTE: *Two ports are allowed on Wi-Fi and Ethernet for BACnet.

EcoStruxure™ Flex-Server can be connected to internet by either of the following options:

- Cellular: Two SIM cards can be inserted in the EcoStruxure™ Flex-Server.
- Ethernet
- Wi-Fi: It can be connected to the Wi-Fi using Wi-Fi receiver.

The GSM has the highest priority followed by Ethernet and then Wi-Fi. in case connectivity issues are there in GSM and Ethernet is plugged in, then it will automatically switch to Ethernet. In the similar way, it would switch to Wi-Fi (if configured) if Ethernet/GSM is not working.

There are two SIM slots for cellular connectivity. If the internet connection is not working on any one of the SIM cards out of two,EcoStruxure™ Flex-Server switches automatically to the other one after a few minutes. If both the SIM cards are in use, the cellular connectivity toggles between both SIMs on weekly basis.

The Flex-Server requires internet connectivity to access the Cloud therefore it must be installed in a secure location to avoid tampering that can impact the Internet connection. For example, if the Ethernet cable is disconnected, or the LTE antenna is removed, this will cause a loss of internet connectivity.

For more information, consult the following websites:

- Schneider Electric cybersecurity consulting services
- National Institute of Standards and Technology (NIST)
- European Union Agency for Cybersecurity (ENISA)

Radio protocols are vulnerable to physical security breaches. For example, a Denial of Service attack can jam the radio signal with a powerful radio emitter located in the vicinity.

It is therefore recommended to adapt your physical security to the criticality of the information which relies on radio protocols. To this purpose, the wireless networks (Wi-Fi and LoRa) can be permanently disabled in the EcoStruxure™ Flex-Server.

For Wi-Fi network, it is recommended to use WPA2 (Wi-Fi Protected Access version 2) protocol.

Expected Endpoints

Schneider Electric recommends only allowing access to the required domains as per your needs.

The following table lists the domain names and protocols used when the EcoStruxure™ Flex-Server connects to the cloud.

Domain name	Protocol	Description
telemetry.ecostruxure-building-activate.se.app	HTTPS (TCP port 443)	Used for sending IoT Sensor Data streams.
mender.ecostruxure-building-activate.se.app	HTTPS (TCP port 443)	Used to download firmware update.
emqx.ecostruxure-building-activate.se.app	HTTPS (TCP port 443)	Used for communication of Flex-Server with Schneider Electric cloud services such as configuration, data, or alarms.
openvpn.ecostruxure-building-activate.se.app	HTTPS (TCP port 443)	Allows Schneider Electric to remotely access the Flex-Server through VPN.
timesync.ecostruxure-building-activate.se.app	HTTPS (TCP port 443)	Time server allows theFlex-Server clock to remain synchronized.
router.ecostruxure-building-activate.se.app	HTTPS (TCP port 443)	Allows the Flex-Server to download linux updates

Data Security in Motion

Schneider Electric with EcoStruxure cloud applications implements best practices such as:

- All communications to and from EcoStruxure™ Flex-Server with internal Schneider Electric systems or external third-party systems, are encrypted using HTTPS (minimum level required is TLSv1.2).
- Certificate involved in these encrypted sessions are leveraging SHA 256 secure hash algorithm. This applies to communications between EcoStruxure™ Flex-Server application and the servers in 3rd party cloud service provider.

Data Security at Rest

Schneider Electric follows best practices to create secure solutions and to limit the risk of data being compromised in any meaningful manner while protecting the privacy, control, and autonomy of each customer’s data independently from any other.

Deployment Portal

NOTICE
POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY • Do not sign in to the Deployment Portal where humans or cameras might monitor password entry. **Failure to follow these instructions can result in equipment damage.**

The Deployment Portal is used to authenticate users via username and password. It provides the ability to configure internet connectivity, the wireless network and its related devices over various supported protocols.

The Admin Dashboard manages access to the Deployment Portal. Hence, it is critical to ensure that the right set of permissions are granted. The system explicitly gives access to the Deployment Portal to users.

System Defense in Depth

NOTICE

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Install routers, switches, or hubs that may be needed for interconnection of The Flex-Server and Cloud Portal to be accessible by authorized personnel only.
- Ensure that the network only opens the ports required by the system.
- For network segmentation, ensure Flex-Server network design and Cloud API access is planned and implemented according to current guidelines and best practices. The Flex-Server must be isolated from critical systems on the network.
- Ecostruxure Buildings Activate solution is a connected offer with devices installed at a customer site, and a Cloud portal to manage those devices. Various cybersecurity strategies need to be implemented to protect the system, including perimeter hardening, network hardening and more.
- The Flex-Server and sensors support signed and authenticated firmware upgrades. Please ensure that the firmware is regularly updated (via the Cloud portal or Flex-Server) to ensure that the latest security and vulnerability patches are implemented. Only firmware signed by the Schneider Electric public key infrastructure is supported by the system.

Failure to follow these instructions can result in equipment damage.

All system components that may be used to integrate the Flex-Server and/or the Cloud API must be secured.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

DOCA0396EN-00