EcoStruxure Panel Server

Cybersecurity Guide

Wireless Concentrator and Modbus Gateway, Datalogger and Energy Server

EcoStruxure offers IoT-enabled architecture and platform.

DOCA0211EN-07
02/2023

www.se.com

Legal Information

Table of Contents

Safety Information

Important Information

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

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

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

Please Note

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

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

Cybersecurity Safety Notice

⚠WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Disable unused ports/services 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 Book

Document Scope

This guide provides information on cybersecurity aspects for EcoStruxure™ Panel 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 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 Panel Server.

Convention

EcoStruxure Panel Server is hereafter referred to as Panel Server.

Online Information

The information contained in this guide is likely to be updated at any time. Schneider Electric strongly recommends that you have the most recent and up-to-date version available on www.se.com/ww/en/download.

The technical characteristics of the devices described in this guide also appear online. To access the information online, go to the Schneider Electric home page at www.se.com.

Related Documents

Title of documentation	Reference number
EcoStruxure Panel Server - User Guide	DOCA0172EN
How Can I Reduce Vulnerability to Cyber Attacks?	Cybersecurity System Technical Note
EcoStruxure Power - Guide for Designing and Implementing a Cyber Secure Digital Power System - Technical Guide	ESXP2TG003EN

You can download these technical publications and other technical information from our website at www.se.com/ww/en/download.

An 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 is intended to help protect your communication network and all equipment connected to it from attacks that could disrupt operations (availability), modify information (integrity), or give away confidential information (confidentiality). The objective of cybersecurity is to provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users. There are many aspects to cybersecurity including designing secure systems, restricting access using physical and digital methods, identifying users, as well as implementing security procedures and best practice policies.

Schneider Electric Guidelines

In addition to the recommendations provided in this guide that are specific to Panel 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?*.

In addition, you will find many useful resources and up-to-date information on the Cybersecurity Support Portal on the Schneider Electric global website, page 19.

Schneider Electric Cybersecurity Policies and Rules

Schneider Electric use 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 Panel Server is equipped with security-enabling features. These features come in a preset state and can be modified to meet your installation needs. The Panel Server must only be configured and set by qualified personnel because disabling or changing settings affect the overall security robustness of the Panel Server and your network security.

Use this guide in conjunction with DOCA0172EN *EcoStruxure Panel Server - User Guide* for detailed configuration of functions and settings of Panel Server.

EcoStruxure Panel Server Interfaces

The EcoStruxure Panel Server communicates through the following interface types:

- Wired through:
  - Two Ethernet ports
  - One Modbus-SL port
- Radio through:
  - IEEE 802.15.4 (not active by default)
  - Wi-Fi infrastructure

Supported Protocols

The EcoStruxure Panel Server supports the following protocols:

- HTTPS (TLS v1.2) for configuration through configuration tools and embedded webpages
- VPN client for remote access (open to Schneider Electric Customer Care Center)
- Modbus TCP and Modbus-SL for communications with other Operational Technology (OT) devices
- DHCP for network IP addressing
- DNS for network name resolution
- NTP for time synchronization
- DPWS for network discovery
- IEEE 802.15.4 for wireless communication using radio frequency communication ISM band 2.4 GHz
- WPA2 and WPA for Wi-Fi communication
- SFTP for publication of CSV files to an SFTP server

Security Features

The EcoStruxure Panel Server supports the following security features:

- Only firmware digitally signed by Schneider Electric can be installed on the Panel Server.
- At each boot, the firmware digital signature is validated before execution, to help ensure that it has not been tampered with.
- User passwords are stored as salted and hashed (SHA256) passwords.
- You can erase all information from the Panel Server using the Restart button.

- The device has an internal clock and remembers its date and time for a few months without power.
- Panel Server authenticity key is stored in a highly secure Common Criteria CC EAL6+ chip.

Device Features

Firmware Update

Update the EcoStruxure Panel Server to the latest firmware version to obtain the latest features and keep up-to-date with security patches. All firmware designed for the EcoStruxure Panel Server is signed using the Schneider Electric Public Key Infrastructure (PKI) to help to provide integrity and authenticity of the firmware running on the EcoStruxure Panel Server. For proper PKI operation, keep the device date synchronized (see Date and Time, page 11).

To be informed about security updates, register with the Security Notifications on Schneider Electric Cybersecurity Support Portal.

Date and Time

Certificates and digital signatures are present in the EcoStruxure Panel Server. To avoid errors, it is important to keep the date and time synchronized. For more information about date and time, see DOCA0172EN *EcoStruxure Panel Server - User Guide*.

Disable Unused Features

The EcoStruxure Panel Server allows you to deactivate unused ports/services to help minimize pathways for malicious attackers.

It is recommended to disable:

- Wi-Fi (not active by default). Wi-Fi can be permanently deactivated.
- IEEE 802.15.4 (not active by default). IEEE 802.15.4 can be permanently deactivated.
- Modbus gateway (active by default). Can be deactivated on each interface (Ethernet 1, Ethernet 2, and/or Wi-Fi) in the Panel Server webpages.
- DPWS discovery protocol over IP v4/6 (active by default)

For more information about disabling EcoStruxure Panel Server unused features, see DOCA0172EN *EcoStruxure Panel Server - User Guide*.

TCP Ports

The following TCP ports are used in the EcoStruxure Panel Server:

- Port 443: HTTPS
- Port 502: Modbus
- Port 5357: DPWS (can be changed)

NOTE: Panel Server does not embed any kind of SSH server.

Audit Logs

The EcoStruxure Panel Server generates audit logs that record events such as invalid login attempts and firmware update.

The logs do not contain any personal information.

To detect unexpected behaviors (for example, frequent rebooting, incorrect firmware update, or invalid login attempts), it is recommended to monitor audit logs regularly. For more information about diagnostics logs, see DOCA0172EN *EcoStruxure Panel Server - User Guide*.

Device Disposal

The EcoStruxure Panel Server contains confidential information configured during commissioning, recent data values and logs. For example, this information can include Modbus device topology, wireless networks, Wi-Fi passwords, or measured power consumptions.

It is required to perform a factory reset before disposing of the EcoStruxure Panel Server. You must have physical access to power cycle the EcoStruxure Panel Server while executing this procedure. See how to reset EcoStruxure Panel Server to factory settings in DOCA0172EN *EcoStruxure Panel Server - User Guide*.

Network Security

Introduction

The EcoStruxure Panel Server 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. 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)

Network Segmentation

The EcoStruxure Panel Server is a gateway. It creates a bridge between different networks. Network segmentation helps ensure cyber defense. To enhance network segmentation, the Panel Server features two Ethernet ports. They can be leveraged in separate mode to have one port dedicated to Information Technology (IT) and one port dedicated to Operational Technology (OT). Network segmentation allows you to keep OT and IT networks segmented, as network packets are not forwarded from one side to the other.

It is recommended to configure the network in separate mode (for more information about network settings, see DOCA0172EN *EcoStruxure Panel Server - User Guide*).

This allows you to connect the Panel Server to :

- Downstream OT devices via Modbus TCP on one Ethernet port.
- Upstream IT PC with SCADA and commissioning software applications on the other Ethernet port.

HTTPS and Modbus are available on Panel Server Ethernet interfaces (ETH1, ETH2) and Wi-Fi.

The following table presents the default setting for each interface:

Interface		**Modbus**
Ethernet in switched topology		Activated
Ethernet in separated topology	ETH1 port	Activated
	ETH2 port	Deactivated
Wi-Fi		Deactivated

It is recommended to disable the Modbus service on networks where it is not used. For more information about service activation, see DOCA0172EN *EcoStruxure Panel Server - User Guide*.

Product Web Server Certificate

To support HTTP secure communications, the EcoStruxure Panel Server is equipped with an X.509v3 certificate by default. This certificate helps ensure the integrity and confidentiality to set up HTTPS communication.

Web browsers only recognize certificates for public web sites. Since the Panel Server is installed in a Local Area Network (LAN), web browsers cannot distinguish one Panel Server from another one. Therefore, a security message appears on the web browser when connecting to the Panel Server.

A direct wired connection helps secure the communication path with the Panel Server. For more information about first access to EcoStruxure Panel Server

webpages through PC, see DOCA0172EN *EcoStruxure Panel Server - User Guide*.

SFTP Server Key Fingerprint

If you publish your data to a SFTP server, make sure that the key fingerprint, displayed when configuring the server address, matches your server SFTP key.

In case you renew the SFTP key on your server, the Panel Server will not be able to send the files anymore, as the connection will not be authenticated. You must re-configure the publication for the Panel Server to record the new SFTP key fingerprint.

Wireless Network

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 IEEE 802.15.4) can be permanently disabled in the Panel Server. If you are confident that you will never need wireless networks (Wi-Fi and IEEE 802.15.4), and only in this case, you can permanently disable them. For more information about permanent and concurrent deactivation of the wireless networks, see DOCA0172EN *EcoStruxure Panel Server - User Guide*.

It is recommended to perform the commissioning of IEEE 802.15.4 wireless devices in a place secure from rogue radio transmitters, such as an administrator room.

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

NOTE: Temporal Key Integrity Protocol (TKIP) is not supported.

Connected Devices

It is recommended to regularly check the list of devices connected to the IEEE 802.15.4 network of the Panel Server. In the case of an unknown connected device, locate it and remove it. You can also rebuild the network and reconnect only identified devices.

Cloud Application Security

Data Security in Motion

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

- All communications to and from EcoStruxure Panel Server with internal Schneider Electric systems or external third-party systems, are encrypted using HTTPS (minimum level required is TLS 1.2).
- Certificate involved in these encrypted sessions are leveraging SHA 256 secure hash algorithm. This applies to communications between Panel Server application and the servers in Microsoft Azure cloud platforms.

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.

All system to system credentials and tokens are stored and encrypted in Microsoft Azure cloud platforms.

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 Panel Server connects to the cloud.

Domain name	Protocol	Description
cbBootStrap.gl.StruXureWareCloud.com	HTTPS (TCP port 443)	Used at first connection of Panel Server to the cloud (or after a factory reset) to authenticate and register the Panel Server.
cnm-ih-na.azure-devices.net	HTTPS (TCP port 443)	Used for communication of Panel Server with Schneider Electric cloud services such as configuration, data, or alarms.
time.gl.StruXureWareCloud.com	NTP (UDP 123)	Allows the Panel Server clock to remain synchronized.
etp.gl.StruXureWareCloud.com	HTTPS (TCP port 443)	Used to download firmware update.
RemoteShell.rsp.Schneider-Electric.com	HTTPS (TCP port 443)	Allows Schneider Electric Customer Care Center to remotely access the Panel Server webpages.
https://cnmdapiappstna.blob.core.windows.net/	HTTPS (TCP port 443)	Allows the Panel Server to upload logs and diagnostics files upon request from Schneider Electric Customer Care Center.
https://cnmiothubappstna.blob.core.windows.net/file-upload	HTTPS (TCP port 443)	Allows the Panel Server to upload large topology (>250 kB) to the Schneider Electric cloud services.

NOTE: Domain names are not case-sensitive.

Physical Security of the Device

Tamper-Indicating Label

The EcoStruxure Panel Server has a tamper-indicating label which helps protect the device physical security. It must be clean and show no sign of tampering (for example, rips, tears, or scratches). Schneider Electric advises against using a device that has visibly been tampered with.

Installation

To help protect the device physical security, the following installation is advised:

- Install the EcoStruxure Panel Server in a cabinet that is secured in a manner appropriate to the risk level of your installation (for example, a cabinet with padlock or a key).
- If the EcoStruxure Panel Server is mounted in a switchboard, install the switchboard in a secured room (for example, with locked door or camera).

Security Recommendations for Maintenance

Maintenance Operations

Over the lifetime of the EcoStruxure Panel Server, it is recommended to regularly do the following operations:

- Check physical security of the EcoStruxure Panel Server (see tamper-indicating label, page 16).
- Make sure that you have the latest firmware update. You should have registered to receive security notifications, page 11.
- Check the connected devices, page 14 for the presence of unknown devices.
- Check the audit logs, page 11 for unexpected behaviors such as invalid login attempts or frequent rebooting.
- Check the date and time, page 11 to avoid drifting away from the current date.

Security Functionality Verification

To comply with IEC 62443 certification, the following tests allows you to verify the intended operation of security functions through the EcoStruxure Panel Server webpages.

Web Authentication

1. Try to log in to the EcoStruxure Panel Server webpages with no password or enter a wrong password.

   Result: The EcoStruxure Panel Server does not give you access to the webpages.
2. Repeat this action 9 more times.

   Result: The EcoStruxure Panel Server locks for 10 minutes.
3. Try again 5 times.

   Result: The EcoStruxure Panel Server locks for 60 minutes.

Web Authorization

1. Log in to the EcoStruxure Panel Server webpages.
2. Bookmark a webpage (for example, **Settings**)
3. Open a private navigation window in your browser and open the previously bookmarked webpage.

   Result: You cannot access the webpage, however you are redirected in the login page.

Audit

1. After some or all the preceding tests, access the Logs webpage.
2. Download the log files.
3. Check that the failing attempts are present in the logs.

Firmware Update

1. Go to the **Firmware Update** webpage.
2. Upload a random file (for example, an image or a text document).

   Result: The EcoStruxure Panel Server reports a wrong signature.
3. Access the audit logs.
4. Check that the failed firmware update is present in the logs.

Disabling Services

1. To access the menu to disable services, select **Settings > Network Communication > DPWS**.
2. Connect a PC with Windows operating system to the same local network.
3. Click Network from the File Explorer.

   Result: The EcoStruxure Panel Server is not discovered, therefore, does not appear in the list of devices in the network.

Schneider Electric Cybersecurity Support Portal

Overview

The Schneider Electric cybersecurity support portal outlines the Schneider Electric vulnerability management policy.

The aim of the Schneider Electric vulnerability management policy is to address vulnerabilities in cybersecurity affecting Schneider Electric products and systems, in order to protect installed solutions, customers, and the environment.

Schneider Electric works collaboratively with researchers, Cyber Emergency Response Teams (CERTs), and asset owners to ensure that accurate information is provided in a timely fashion to adequately protect their installations.

Schneider Electric's Corporate Product CERT (CPCERT) is responsible for managing and issuing alerts on vulnerabilities and mitigations affecting products and solutions.

The CPCERT coordinates communications between relevant CERTs, independent researchers, product managers, and all affected customers.

Information Available on the Schneider Electric Cybersecurity Support Portal

The support portal provides the following:

- Information about cybersecurity vulnerabilities of products.
- Information about cybersecurity incidents.
- An interface that enables users to declare cybersecurity incidents or vulnerabilities.

Vulnerability Reporting and Management

Cybersecurity incidents and potential vulnerabilities can be reported via the Schneider Electric website: Report a Vulnerability.

Glossary

D

DPWS - Devices Profile for Web Services:

Minimal set of implementation constraints that helps to enable secure web service messaging, discovery, description, and events on resource-constrained devices.

H

HTTP - Hypertext Transfer Protocol:

A network protocol that handles delivery of files and data on the World Wide Web.

HTTPS - Hypertext Transfer Protocol Secure:

A variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit through a Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocol connection.

I

IP - Internet protocol:

IP addresses are used to identify devices connected to the company intranet or to the Internet.

IT - Information technology:

Refers to the company information systems and information network as opposed to its OT (operational technology) network.

L

LAN - Local area network:

Refers to the company intranet, or IT network.

M

Modbus TCP/IP:

A protocol, which provides client/server communication between devices and TCP/IP that provides communications over an Ethernet connection.

O

OT - Operational technology:

Refers to the hardware and software systems the company uses to directly monitor and control the production processes and equipment, also called the industrial control (IC) network. OT is often used to refer to the company operational network as opposed to its IT network.

P

PKI - Public key infrastructure:

Defines a set of services used to generate and authenticate digital signatures. A public key infrastructure is designed to guarantee confidentiality, integrity, and authenticity of information.

S

SCADA - Supervisory control and data acquisition:

Refers to systems designed to get real-time data on production processes and equipment for monitoring and controlling them remotely.

Security policy:

A system security policy is the security settings that are applied throughout the entire secured system. A security policy generally refers to the use of standards. It is used to define any security-related configuration shared between all devices.

SFTP - Secure File Transfer Protocol:

A secure version of File Transfer Protocol which facilitates data access and data transfer over a Secure Shell (SSH) data stream.

T

TCP/IP - Transmission control protocol/Internet protocol:

Refers to the suite of protocols used for communications over the Internet.

V

VPN - Virtual private network:

A VPN is used to establish a secured / private "tunnel" between an authenticated external access point and the trusted enterprise network.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

DOCA0211EN-07