EcoStruxure Panel Server

Cybersecurity Guide

Wireless Devices Concentrator and Modbus Gateway, Datalogger, and Energy Server

EcoStruxure offers IoT-enabled architecture and platform.

DOCA0211EN-14
01/2026

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 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.

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.

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 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

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 General Cybersecurity Information, page 6.

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 with firmware version 002.005.000 or greater.

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.

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

⚠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.

Available Languages of the Document

The document is available in these languages:

- English (DOCA0211EN) original language
- French (DOCA0211FR)
- German (DOCA0211DE)
- Italian (DOCA0211IT)
- Portuguese (DOCA0211PT)
- Spanish (DOCA0211ES)

Related Documents

Title of documentation	Reference number
EcoStruxure Panel Server - User Guide	DOCA0172EN DOCA0172DE DOCA0172ES DOCA0172FR DOCA0172IT DOCA0172PT
Cybersecurity Best Practices	7EN52-0390
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/.

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.

Trademarks

QR Code is a registered trademark of DENSO WAVE INCORPORATED in Japan and other countries.

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 and the general cybersecurity information, page 6.

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 DOCA0172•• *EcoStruxure Panel Server - User Guide*, page 7 for detailed configuration of functions and settings of Panel Server.

EcoStruxure Panel Server Interfaces

The following table summarizes the communication architectures available with Panel Server by model:

Characteristic		EcoStruxure Panel Server													
		Entry	Universal							Advanced					
		PAS400	PAS600 HW: V1.0	PAS600 HW: V2.0	PAS600T HW: V1.0	PAS600L HW: V1.0	PAS600L HW: V2.0	PAS600LWD HW: V2.0	PAS600PWD HW: V2.0	PAS800 HW: V1.0	PAS800 HW: V2.0	PAS800L HW: V1.0	PAS800L HW: V2.0	PAS800P HW: V1.0	PAS800P HW: V2.0
10/100BASE-T Ethernet	One RJ45 port	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
	Two RJ45 ports	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Upstream Modbus TCP/IP connectivity		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Upstream Wi-Fi connectivity		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓
Downstream Modbus TCP/IP connectivity		-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Downstream IEEE 802.15.4 connectivity		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓
Downstream Modbus-SL connectivity		-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Two digital inputs (for WAGES (Water, Air, Gas, Electricity, Steam))		-	-	-	-	✓	✓	✓	-	-	-	✓	✓	-	-
Wi-Fi external antenna		-	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓
IEEE 802.15.4 external antenna		-	-	✓	-	-	✓	-	-	✓	✓	✓	✓	✓	✓
Wi-Fi access point		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓
Notification of alarms by email		-	-	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓
Publication on SFTP or HTTPS server		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Convention

EcoStruxure Panel Server is hereafter referred to as Panel Server.

Supported Protocols

The EcoStruxure Panel Server supports the following protocols:

- DHCP for network IP addressing
- DNS for network name resolution
- DPWS for network discovery
- HTTPS (TLS v1.2) for configuration through configuration tools and embedded webpages
- IEEE 802.15.4 for wireless communication using radio frequency communication ISM band 2.4 GHz (not available for Wired by Design models)
- Modbus TCP and Modbus-SL for communications with other Operational Technology (OT) devices
- NTP for time synchronization
- RSTP to allow robust Ethernet ring topologies for critical applications
- SFTP for publication of CSV files to an SFTP server
- VPN client for remote access (open to Schneider Electric Customer Care Center)
- WPA2 and WPA for Wi-Fi communication (not available for Wired by Design models)

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.

Recommended Actions for Cybersecurity

Your device is designed to be used in a protected environment that uses a defense-in-depth strategy.

To help secure your device, you must take specific actions at every stage of the project life-cycle.

> **NOTE:** list of recommended actions below is not a complete list of possible cybersecurity measures. It is meant to be a starting point to improve the security of your device in a protected environment. Consult with cybersecurity experts to plan, configure, operate, maintain, and decommission your device based on your needs.

The following table lists the recommended actions for you to take to help secure your device in a protected environment, organized by life-cycle stage:

Life cycle stage	Recommended action	Defense-in-depth role
Plan	Review cybersecurity awareness, page 6.	Use available resources to increase your cybersecurity knowledge and awareness.
	Review the system defense-in-depth assumptions. Follow the recommendations in this guide.	Understand the security measures expected to be provided by the external environment in which the device is to be used. These include, but are not limited to: • Site and device location security • Network security
	Review the device security features. Refer to *Security Capabilities* in DOCA0172•• Panel Server User Guide, page 7.	Understand how the device security features can be used in a protected environment.
	Review the security risks and compensation controls. Refer to *Security Capabilities* in DOCA0172•• Panel Server User Guide, page 7.	Understand known security risks and the compensation controls to help minimize the risks.
Install and configure	Check the state of the anti-tamper label before installation of the device, page 20.	Tamper-evident label prevents modification of the device before installation.
	Follow the installation guidelines, page 20.	Help reduce unauthorized physical access.
	Change the default password at first login. Refer to *User Management* in DOCA0172•• Panel Server User Guide, page 7.	Help reduce unauthorized access. Default account settings are often the source of unauthorized access by malicious users.
	Change the Panel Server user password and Wi-Fi access point password. Refer to *User Management* and *Wi-Fi Access Point* in DOCA0172•• Panel Server User Guide, page 7.	Create strong passwords following the guidelines. Default account settings and weak passwords are often the source of unauthorized access by malicious users.
	Disable unused protocols and ports, page 14.	Disable unnecessary and unused communication protocols and ports, for example, Wi-Fi, Wi-Fi access point, IEEE.802.15.4.
Operate	Encrypt backup configuration files, page 20.	Use strong passwords to encrypt configuration backup files. Unprotected files and weak passwords can be the source of unauthorized access by malicious users
	Manage access to domains, page 19.	Limit access to known and required domains, according to your needs.
	Report a cybersecurity incident or vulnerability, page 6.	Report suspicious activity, a cybersecurity incident, or a vulnerability to Schneider Electric Cybersecurity Support Portal web page.
Maintain	Maintain firmware up to date. Refer to *Firmware Update* in DOCA0172•• Panel Server User Guide, page 7.	Update to the latest firmware version to benefit from the latest security patches.
	Monitor the audit log for unexpected behaviors. Refer to *Diagnostics Logs* in DOCA0172•• Panel Server User Guide, page 7.	Monitor the audit logs for unexpected activity and to help identify the cause of cybersecurity breaches that could lead to a cybersecurity incident.
	Check the state of the anti-tamper label regularly, page 20.	Tamper-evident label prevents modification of the device.

Life cycle stage	Recommended action	Defense-in-depth role
	Check the connected devices for the presence of unknown devices, page 18.	Locate and remove unknown devices to help protect the system against cybersecurity breaches.
	Keep your network security up to date.	Helps reduce your attack surface, decreasing the likelihood of a vulnerability.
	Perform security audits	Help verify the security status of your system.
Decommission	Reset the device to factory settings. Refer to *Security Recommendations for Decommissioning* in DOCA0172•• Panel Server User Guide, page 7.	Help prevent the potential disclosure of data.

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 14).

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

Date and Time

It is important to keep the date and time synchronized for the following purposes:

- To avoid errors in certificates and digital signatures in the EcoStruxure Panel Server
- To provide an accurate timestamp in audit logs to assist forensic security

For more information about date and time, see DOCA0172•• *EcoStruxure Panel Server - User Guide*, page 7.

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 activation and Wi-Fi infrastructure. Wi-Fi can be permanently deactivated, if required.
- Wi-Fi access point (enabled by default). When the access point is disabled, pressing the button on the front face of the Panel Server does not trigger the access point activation. Deactivating Wi-Fi activation also disables the Wi-Fi access point and interrupts any active connection.
- IEEE 802.15.4 (not active by default). IEEE 802.15.4 can be permanently deactivated.
- Modbus gateway services (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)
- RSTP Rapid Spanning Tree Protocol (not active by default)

NOTE: Wi-Fi and IEEE 802.15.4 are natively unavailable on Wired by Design (WD) models, which have no wireless chipset.

For more information about disabling EcoStruxure Panel Server unused features, see DOCA0172•• *EcoStruxure Panel Server - User Guide*, page 7.

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 DOCA0172•• *EcoStruxure Panel Server - User Guide*, page 7.

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 DOCA0172•• *EcoStruxure Panel Server - User Guide*, page 7.

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, Panel Server Universal and Advanced feature 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 DOCA0172•• *EcoStruxure Panel Server - User Guide*, page 7).

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 infrastructure		Deactivated
Wi-Fi access point		Not available

It is recommended to disable the Modbus service on networks where it is not used. For more information about service activation, see DOCA0172•• *EcoStruxure Panel Server - User Guide*, page 7.

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 DOCA0172•• *EcoStruxure Panel Server - User Guide*, page 7.

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.

If 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 DOCA0172•• *EcoStruxure Panel Server - User Guide*, page 7.

NOTE: Wired by Design (WD) models of Panel Server allow you to comply with no-wireless policies as they contain no wireless chipset.

It is recommended to:

- Use the install code to discover wireless devices. For more information, see DOCA0172•• *EcoStruxure Panel Server - User Guide*, page 7
- 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.

Remote Access (VPN)

The Panel Server provides a remote access feature that allows the Schneider Electric Customer Care Center (CCC) to connect to the Panel Server webpages.

Access is not enabled by default and requires the firewall to enable the connection. For more information, refer to Expected Endpoints, page 19.

The remote access feature relies on a layer 3 VPN that, by design, does not provide access to the network, but only to the Panel Server. In addition, only HTTPS is authorized to be tunneled via this VPN.

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.
etp.prod.StruXureWareCloud.com	HTTPS (TCP port 443)	Used to download firmware update.
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.
RemoteShell.rsp.Schneider-Electric.com	HTTPS (TCP port 443)	Allows Schneider Electric Customer Care Center to remotely access the Panel Server webpages through VPN.
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.
cnmiothubappstna.Blob.Core.Windows.net/file-upload	HTTPS (TCP port 443)	Allows the Panel Server to upload a topology to the Schneider Electric cloud services.
time.gl.StruXureWareCloud.com	NTP (UDP port 123)	NTP server allows the Panel Server clock to remain synchronized.

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).

  NOTE: The protection of the physical security of the device includes the protection of the QR code. The QR code gives access to the device code of the Panel Server, which should be considered as a credential for the device. It is used:

  - In the secure claiming of the device for cloud applications
  - As the password for connecting to the Wi-Fi access point

Password Management

To help protect the device from malicious attack, change the Panel Server user password and Wi-Fi access point password by using the Panel Server webpages.

The user password and SupportUser password must conform to the following rules:

- Between 8 and 50 characters
- Must contain at least three of the following types of character:
  - Uppercase
  - Lowercase
  - Digits
  - Special characters (limited to space character and !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~)

The Wi-Fi access point password must conform to the following rules:

- Between 8 and 32 characters
- Must contain at least one of each of the following types of character:
  - Uppercase
  - Lowercase
  - Digits
- Can contain special characters (limited to space character and !"#$%&'()*+,-./:;<=>?@[]^_`{|}~)

Backup Function

When downloading a backup file, encrypt the file with a strong password, composed of:

- Between 6 and 32 characters
- At least one of each of the following types of character:
    - Uppercase
    - Lowercase
- Special characters (limited to space character and !"#$%&'()*+,-./:;<=>?@[] ^_`{|}~)

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 20).
- Make sure that you have the latest firmware update. You should have registered to receive security notifications, page 14.
- Check the connected devices, page 18 for the presence of unknown devices.
- Check the audit logs, page 15 for unexpected behaviors such as invalid login attempts or frequent rebooting.
- Check the date and time, page 14 to avoid drifting away from the current date.
- Make sure that all unnecessary services and features are disabled, page 14.

Security Functionality Verification

The following tests allow 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.

Disabling Wireless Services

To access the menus to temporarily disable wireless services:

- For Wi-Fi, navigate to **Settings > Network Communication > Wi-Fi**, click the **Wi-Fi activation** slider, and save your changes.

  Result: In your Wi-Fi access point management interface, there is no EcoStruxure Panel Server connected.
- For IEEE 802.15.4, navigate to **Settings > Wireless devices > Network configuration**, click the **Wireless activation** slider, and save your changes.

  Result: All wireless devices listed at **Settings > Wireless devices > Wireless devices** will indicate a **Not connected** state after a certain time, depending on the wireless device (see your device documentation for more details).

Glossary

D

DHCP - Dynamic Host Configuration Protocol:

A network management protocol used on Internet Protocol networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.

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

IEEE 802.15.4:

Standard defined by the IEEE and used by the EcoStruxure Panel Server to communicate with wireless devices.

Install code:

A unique 36-character code associated with a Modbus device which enables you to launch a discovery of the device with heightened security from the Panel Server.

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.

N

NTP - Network Time Protocol:

A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

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.

R

RSTP - Rapid Spanning Tree Protocol:

A network protocol that promotes high availability and loop-free topology within Ethernet networks.

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.

SDL - Secure Development Lifecycle:

A product development framework that helps ensure products follow secure design processes across all lifecycle stages.

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

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.