EcoStruxure Panel Server

User Guide

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

EcoStruxure offers IoT-enabled architecture and platform.

DOCA0172EN-22
10/2026



www.se.com

Legal Information

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

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

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

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

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

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

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

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

Table of Contents

Table of Contents....3
Safety Information....7
About the Document....8
EcoStruxure Panel Server Presentation....12
Introduction....13
EcoStruxure Panel Server System....16
Hardware Description....22
Hardware Connection....30
Device Landing Page....32
EcoStruxure Panel Server Webpages Overview....33
EcoStruxure Power Commission (EPC) Software....34
EcoStruxure Power Commission Web Tool (EPC Web)....36
EcoStruxure Cybersecurity Admin Expert (CAE) Software....37
EcoStruxure System Management (ESM) Software....38
Edge Monitoring and Supervision Software....39
Cloud Applications....40
Technical Characteristics....41
EcoStruxure Panel Server Configuration Functions....46
Date and Time....47
Firmware Update....50
User Management Using Panel Server Webpages....52
User Management Using EcoStruxure Cybersecurity Admin Expert....55
EcoStruxure Panel Server Communication Functions....59
Modbus Gateway Function....60
Examples of Modbus Routing....65
Communication Architectures....71
Network Communication....77
Network Settings....78
DNS....80
RSTP....81
Proxy....84
Device Profile for Web Services (DPWS)....85
Wi-Fi Infrastructure....86
Wi-Fi Access Point....89
TCP/IP Communication....92
Ethernet Communication....93
Modbus TCP/IP Client (Universal and Advanced Models)....98
Modbus TCP/IP Server....100
Modbus-SL Communication (Models with One Modbus-SL Port)....101
Wireless Communication....106
Wi-Fi Communication....107
IEEE 802.15.4 Communication....108
Dynamic Antenna Selection....112
Channel Scan Function....114
Permanent Deactivation of Wireless Networks....116
EcoStruxure Panel Server General Functions....117
Data Sampling....118

Data Publication 122
Publication on Schneider Electric Cloud 123
Publication on SFTP Server 127
Publication on HTTPS Server 130
File Format of Publications 133
Publication of Emails for Alarms (Advanced Model) 135
Publication on SFTP Server and Email Notification for Alarms (Advanced Model) 137
Publication on HTTPS Server and Email Notification for Alarms (Advanced Model) 138
Alarm Management 139
Displaying and Publishing Alarms 140
Alarm File 141
Alarm Description 142
Control Functions and Commands 145
Remote Control and Scheduling From Cloud 146
Sending Commands From Panel Server Webpages 148
Digital Inputs (PAS600L, PAS600LWD, PAS800L) 149
Custom Models for Downstream Modbus Devices (Universal and Advanced Models) 153
Local Energy Server Functions (Advanced Model) 158
Data Logging (Advanced Model) 159
Consumption Overview (Advanced Model) 161
Data Trending (Advanced Model) 163
Exporting Data Locally (Advanced Model) 166
EcoStruxure Panel Server Maintenance Functions 170
Diagnostics 171
Diagnostics Logs 175
Security Logs Using EcoStruxure Cybersecurity Admin Expert 177
Syslog Server Configuration 179
Backup and Restore Panel Server Configuration 180
Cybersecurity Recommendations 183
Recommended Actions for Cybersecurity 184
Security Capabilities 186
Security Recommendations for Commissioning 188
Security Recommendations for Operation 189
Security Recommendations for Decommissioning 190
General Principle to Commission an EcoStruxure Panel Server 191
Overview 192
Commissioning Panel Server with EcoStruxure Power Commission Software 193
First Connection with EcoStruxure Power Commission Software 194
Non-Selective Discovery of Wireless Devices 195
Selective Discovery of Wireless Devices 196
Device Configuration with EcoStruxure Power Commission Software 197
Device Configuration with EcoStruxure Power Commission Mobile App 198

Commissioning Panel Server with Webpages 199
Getting Started with EcoStruxure Panel Server Webpages 200
First Connection to EcoStruxure Panel Server Webpages 201
Using EcoStruxure Panel Server Webpages 203
EcoStruxure Panel Server User Interface Layout 204
EcoStruxure Panel Server Webpage Menus 210
Home Menu (Advanced Model) 211
Notifications Menu (Advanced Model) 212
Monitoring and Control Menu 214
Trending Menu (Advanced Model) 218
Settings Menu 220
Maintenance Menu 223
User Management Menu 226
Commissioning of Modbus Devices 227
Adding Modbus Devices Through Webpages 228
Adding Multi-Meter Devices (MCM) 232
Configuring Modbus Devices Through Webpages 233
Configuring Smart Link Modbus Channels 235
Removing Modbus Devices Through Webpages 237
Commissioning of Wireless Devices Through Webpages 238
Discovery of Wireless Devices Through Webpages 239
Discovery of XB5R Transmitters (ZBRT) 242
Configuring Wireless Devices Through Webpages 244
Configuration of Wireless Energy Devices 246
Configuration of Wireless Indication Auxiliaries 250
Configuration of PowerTag Control Devices Through Webpages 251
Configuration of Ambient Sensors Through Webpages 254
Configuration of Exiway Link Devices 255
Removing Wireless Devices Through Webpages 256
Adding Wireless Devices Connected to a Child Gateway (Universal and Advanced Models) 258
Troubleshooting 260
Appendices 265
Appendix A: Details of Modbus Functions 266
Modbus TCP/IP Functions 267
Modbus-SL Functions 269
Recommendations for Optimizing Networks with Modbus Devices 270
Modbus TCP/IP and Modbus-SL Exception Codes 272
Modbus Registers Tables 274
EcoStruxure Panel Server Modbus Registers 275
Function 43-14: Read Device Identification 276
Function 100-4: Read Non-Adjacent Registers 278
Setting Message Timeout for Modbus Client and Modbus Server 279
Appendix B: Data Availability 281
PowerTag, PowerLogic Tag, and Acti9 Active Data Availability 282
Environmental Sensor Data Availability 286
Appendix C: Wireless Device Network Indicators 287

Appendix D: SFTP and HTTPS Publication File Formats 288
Appendix E: SSH Key Exchange and Cipher 291
Appendix F: Certificate Authorities 293
Appendix G: Retrieve the DHCP IP Address of a PAS400 Panel Server 297
Appendix H: Contextualization Data 299
Glossary 301

Safety Information

Important Information

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



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



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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

Please Note

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

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

About the Document

Document Scope

The aim of this guide is to provide users, installers, and maintenance personnel with the technical information and procedures needed to use and maintain the EcoStruxure™ Panel Server.

Validity Note

This guide applies to the EcoStruxure Panel Server models and firmware versions described in the following table:

Commercial reference	Hardware version		Firmware version
	001.000.000	002.000.000	
PAS400	✓		EcoStruxure Panel Server Entry firmware version 002.008.000 or greater for hardware version 001.000.000
PAS600, PAS600T, PAS600L	✓		EcoStruxure Panel Server Universal firmware version 002.008.000 or greater for hardware version 001.000.000
PAS600, PAS600L		✓	EcoStruxure Panel Server Universal firmware version 002.008.000 or greater for hardware version 002.000.000
PAS600LWD, PAS600PWD		✓	EcoStruxure Panel Server Universal Wired by Design model firmware version 002.008.000 or greater for hardware version 002.000.000
PAS800, PAS800L, PAS800P	✓		EcoStruxure Panel Server Advanced firmware version 002.008.000 or greater for hardware version 001.000.000
		✓	EcoStruxure Panel Server Advanced firmware version 002.008.000 or greater for hardware version 002.000.000

NOTE: The content of this guide also applies to **EcoStruxure Panel Server Wired by Design models PAS600LWD and PAS600PWD**. A Wired by Design model is a Panel Server without the capability to connect to IEEE.802.15.4 wireless devices and without Wi-Fi communication capability. All the information related to the Panel Server presented in this guide applies to Wired by Design models except information about wireless devices and Wi-Fi communication.

Online Information

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.

Product Related Information

⚠WARNING

UNEXPECTED START OF OPERATION

Only allow remote and/or scheduled control of loads for non-critical electrical loads that can safely be left unattended.

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

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.

For more information about cybersecurity related to the EcoStruxure Panel Server, refer to:

- Cybersecurity Recommendations, page 183
- DOCA0211••*EcoStruxure Panel Server - Cybersecurity Guide*, page 10.

Environmental Data

For product compliance and environmental information, refer to the Schneider Electric Environmental Data Program.

Available Languages of the Document

The document is available in these languages:

- English (DOCA0172EN), original language
- French (DOCA0172FR)
- German (DOCA0172DE)
- Italian (DOCA0172IT)
- Portuguese (DOCA0172PT)
- Spanish (DOCA0172ES)

Related Documents

Title of documentation	Reference number
EcoStruxure Panel Server - Catalog	PLSED310196EN
EcoStruxure Panel Server Entry - Instruction Sheet	NNZ76760
EcoStruxure Panel Server Universal - Instruction Sheet	GEX84977
EcoStruxure Panel Server Universal Wired by Design - Instruction Sheet	PKR28607
EcoStruxure Panel Server Advanced - Instruction Sheet	BQT54848
EcoStruxure Panel Server - Wireless Devices / Wi-Fi Antenna - Instruction Sheet	NNZ58425
EcoStruxure Panel Server Entry - Firmware Release Notes	DOCA0249EN DOCA0249DE DOCA0249ES DOCA0249FR DOCA0249IT DOCA0249PT
EcoStruxure Panel Server Universal - Firmware Release Notes	DOCA0178EN DOCA0178DE DOCA0178ES DOCA0178FR DOCA0178IT DOCA0178PT
EcoStruxure Panel Server Advanced - Firmware Release Notes	DOCA0248EN DOCA0248DE DOCA0248ES DOCA0248FR DOCA0248IT DOCA0248PT

Title of documentation	Reference number
EcoStruxure Panel Server - Cybersecurity Guide	DOCA0211EN DOCA0211DE DOCA0211ES DOCA0211FR DOCA0211IT DOCA0211PT
EcoStruxure Panel Server - Modbus File	DOCA0241EN
EcoStruxure Panel Server - Alarm File	DOCA0330EN
EcoStruxure Power Commission Mobile Application - User Guide	DOCA0366EN
EcoStruxure Cybersecurity Admin Expert User Guide	CAE_User_Guide
EcoStruxure Power - Guide for Designing and Implementing a Cyber Secure Digital Power System - Technical Guide	ESXP2TG003EN
Wireless Communication Architectures With EcoStruxure Panel Server - Design Guide	DOCA0289EN

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.

EcoStruxure Panel Server Presentation

What’s in This Part

Introduction 13
EcoStruxure Panel Server System 16
Hardware Description 22
Hardware Connection 30
Device Landing Page 32
EcoStruxure Panel Server Webpages Overview 33
EcoStruxure Power Commission (EPC) Software 34
EcoStruxure Power Commission Web Tool (EPC Web) 36
EcoStruxure Cybersecurity Admin Expert (CAE) Software 37
EcoStruxure System Management (ESM) Software 38
Edge Monitoring and Supervision Software 39
Cloud Applications 40
Technical Characteristics 41

Introduction

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.

Overview

EcoStruxure Panel Server is a high performance gateway which provides, depending on the model:

- easy and fast connection to
  - edge control software such as EcoStruxure Power Monitoring Expert or EcoStruxure Power Operation,
  - Building Management Systems such as EcoStruxure Building Operation,
  - cloud applications such as EcoStruxure Energy Hub (part of EcoStruxure Building Activate), EcoStruxure Resource Advisor, and EcoStruxure Asset Advisor.
- an all-in-one gateway to retrieve data from IEEE 802.15.4 and Modbus devices, and optimize energy and operation management solution.
- ease of operation with user-friendly embedded webpages, and data contextualization for more relevant analytics.
- ease of commissioning:
  - with user-friendly embedded webpages.
  - with EcoStruxure Power Commission software, enabling device plug-and-play and auto-discovery features on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- communication protocols:
  - Ethernet
  - IEEE 802.15.4
  - Wi-Fi
- Wired by Design models with no native wireless chipset, removing the potential threat from unauthorized radio devices

The models of Panel Server are:

- Entry (PAS400)
- Universal (PAS600 series)
- Advanced (PAS800 series)

Convention

EcoStruxure Panel Server is hereafter referred to as Panel Server.

Main Features

Panel Server provides the following main features, depending on the model:

- Gateway functionality Modbus TCP/IP to Modbus Serial Line (Modbus-SL)

- Data concentrator for the following wireless devices: PowerTag Energy and PowerLogic Tag sensors, environmental sensors, Acti9 Active, HeatTag sensors, wireless indication auxiliaries for ComPacT and PowerPacT circuit breakers. For more information, see Supported Devices, page 19.
- Connectivity to FDM128 Ethernet display
- Connectivity to Schneider Electric monitoring software (such as EcoStruxure Power Monitoring Expert (PME), EcoStruxure Power Operation (PO), EcoStruxure Building Operation) or third-party software
- Connectivity to Ethernet or Wi-Fi
- Two Ethernet ports to optionally separate upstream cloud connection from field device network (Universal and Advanced models)
- Supported transfer protocols:
  - Modbus TCP/IP
  - HTTPS (HTTP not supported)
  - SFTP
- Real-time data in easy-to-understand embedded webpages
- 3 years of data logging (Advanced model)
- Dashboard view for reporting (Advanced model)
- Data export with native connection to Schneider Electric cloud services (such as EcoStruxure Energy Hub (part of EcoStruxure Building Activate), EcoStruxure Asset Advisor, and EcoStruxure Resource Advisor)
- Setup through one of the following ways:
  - Embedded webpages
  - EcoStruxure Power Commission software allowing off-line configuration preparation on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.

Feature Availability

The following table presents the availability of the main features on the Panel Server range.

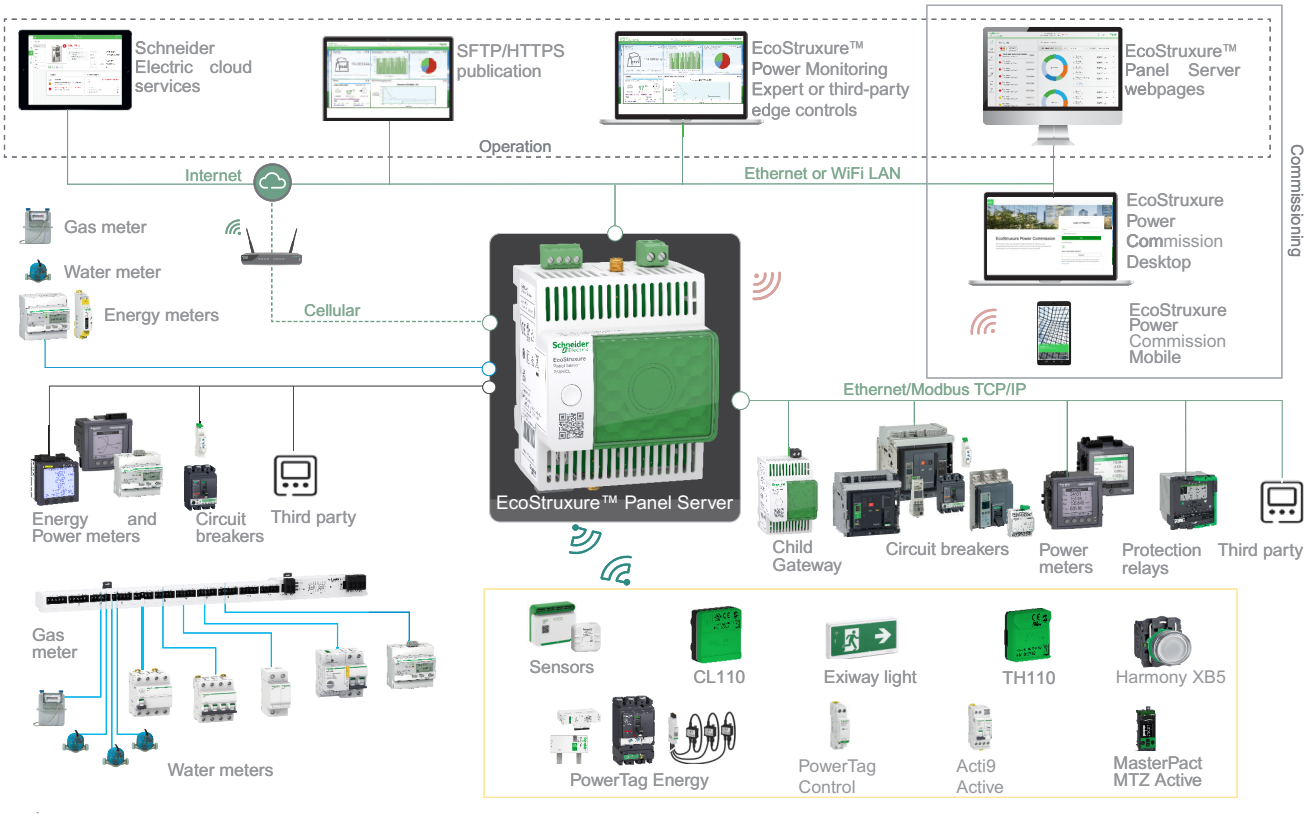
Characteristic		EcoStruxure Panel Server													
		Entry	Universal							Advanced					
		PAS400	PAS600 HW: V1.0	PAS600 HW: V2.0	PAS600T HW: V1.0	PAS600L HW: V1.0	PAS600L HW: V2.0	PAS600LWD HW: V2.0	PAS600PWD HW: V2.0	PAS800 HW: V1.0	PAS800 HW: V2.0	PAS800L HW: V1.0	PAS800L HW: V2.0	PAS800P HW: V1.0	PAS800P HW: V2.0
Power supply	24 Vdc	-	-	-	-	✓	✓	✓	-	-	-	✓	✓	-	-
	110-240 Vac / Vdc	-	-	-	✓	-	-	-	-	-	-	-	-	-	-
	110-277 Vac / Vdc	✓	✓	✓	-	-	-	-	-	✓	✓	-	-	-	-
	Power over Ethernet (PoE)	-	-	-	-	-	-	-	✓	-	-	-	-	✓	✓
10/100BASE-T Ethernet	One RJ45 port	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
	Two RJ45 ports	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Upstream Modbus TCP/IP connectivity		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Upstream Wi-Fi connectivity	2.4 GHz	✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓
	5 GHz	✓	-	✓	-	-	✓	-	-	✓	✓	✓	✓	✓	✓
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		-	-	✓	-	-	✓	-	-	✓	✓	✓	✓	✓	✓
Data sampling		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data logging		-	-	-	-	-	-	-	-	3 years					
Data trending		-	-	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓
Notification of alarms on webpages		-	-	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓
Notification of alarms by email		-	-	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓
Wi-Fi access point		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓
Publication on SFTP or HTTPS server		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Display of active alarms on webpages		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Commissioning tool of Panel Server and connected devices		• EcoStruxure Panel Server webpages • EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.													
Schneider Electric cloud application		• EcoStruxure Energy Hub (part of EcoStruxure Building Activate) • EcoStruxure Asset Advisor • EcoStruxure Resource Advisor													

EcoStruxure Panel Server System

Architecture

From a simple electrical distribution system with one device to large electrical distribution systems, the EcoStruxure Panel Server collects data from any of the supported devices.

The following illustration shows typical architectures of EcoStruxure Panel Server:



Ethernet or Wi-Fi LAN

Modbus-SL communication

ULP system

Digital inputs/outputs

IEEE 802.15.4 wireless communication

Wi-Fi access point

Network Connectivity

EcoStruxure Panel Server network connectivity can be subdivided into two parts:

- Upstream connection to supervision software and cloud applications.
- Downstream connection to local field devices.

Upstream Connection

The upstream network of EcoStruxure Panel Server can be used to connect cloud applications or Modbus TCP/IP monitoring and supervision application.

- Entry model:

  This access is provided either through the Ethernet port on the Panel Server or through the Wi-Fi interface.

- Universal and Advanced models:

  This access is provided through the two Ethernet ports on the EcoStruxure Panel Server or through the Wi-Fi interface, where applicable.

  Depending on the Ethernet port configuration, the data transmission behavior is as follows:

  - In switched mode (default mode), the two Ethernet ports are connected to the internal Ethernet switch of the EcoStruxure Panel Server. Devices connected to either of the Ethernet ports can see each other.
  - In separated mode, Ethernet port **ETH1** is connected to the upstream network while Ethernet port **ETH2** is used to create a downstream Ethernet network separate from the upstream Ethernet network.

  In case of Wi-Fi connection, Wi-Fi is always considered the upstream network and the Ethernet ports are separated from the Wi-Fi network. The upstream (Wi-Fi) network and downstream (Ethernet) network(s) must be different networks using different subnets (see following table. In the table **A**, **B** and **C** represent different networks.):

Connection	Wi-Fi network	ETH1 network	ETH 2 network
Switched mode (Wi-Fi not activated)	–	**A**	**A**
Separated mode (Wi-Fi not activated)	–	**A** (upstream)	**B** (downstream)
Wi-Fi and switched mode	**A** (upstream)	**B** (downstream)	**B** (downstream)
Wi-Fi and separated mode	**A** (upstream)	**B** (downstream)	**C** (downstream)

The Panel Server enables separate IP configuration (**IPv4**, **IPv6**, or **IPv4 & IPv6**) for each interface. Refer to Ethernet Communication, page 93.

Downstream Connection (Entry Model)

Devices in the downstream network can be connected to the Panel Server Entry wireless concentrator through wireless network according to IEEE 802.15.4.

The Panel Server enables separate IP configuration (**IPv4**, **IPv6**, or **IPv4 & IPv6**) for each interface. Refer to Ethernet Communication, page 93.

Downstream Connection (Universal and Advanced Models)

Devices in the downstream network can be connected to Panel Server Universal and Advanced through different means:

- Wireless network according to IEEE 802.15.4 (PAS600, PAS600T, PAS600L, and PAS800 series)
- Modbus-SL
- Modbus TCP/IP (Ethernet and Wi-Fi)
- Panel Server digital inputs (PAS600L, PAS600LWD, PAS800L)

Depending on the configuration of the Panel Server Ethernet ports, data transmission behavior is as follows:

- In switched mode, it is possible to daisy chain several network devices via the Panel Server. The Modbus TCP/IP devices connected to either port of the Panel Server can be directly accessed by monitoring and supervision software running on a device physically connected to either **ETH1** or **ETH2** port.
- In separated mode, the Modbus TCP/IP devices connected via the **ETH2** port to the downstream Ethernet network may be accessed by upstream monitoring and supervision software through **ETH1** port.

The Panel Server enables separate IP configuration (**IPv4**, **IPv6**, or **IPv4 & IPv6**) for each interface. Refer to Ethernet Communication, page 93.

Supported Devices

List of supported devices (depending on Panel Server model):

- Wired devices communicating through Modbus-SL, Modbus TCP/IP, or digital inputs:
  - Circuit breakers and switch-disconnectors
  - Protection relays
  - Power meters
  - Energy meters
  - Pulse meters
  - IO modules
  - Gateways
- Wireless devices:
  - Energy-related devices:
    - PowerTag Energy and PowerLogic Tag power meters
    - Acti9 Active
  - Environmental sensors:
    - PowerLogic TH110/CL110
    - HeatTag sensors
    - Wireless CO_2 sensors
    - Wireless temperature and humidity sensors
    - PowerTag Ambient
    - PowerLogic Thermal Tag TH150/TH200(1) wireless temperature sensors
  - Control devices:
    - PowerTag Control
    - Wireless indication auxiliaries for ComPacT and PowerPacT circuit breakers
  - Circuit breakers: MicroLogic Active AP or EP control unit in MasterPacT MTZ circuit breakers
  - Other wireless devices:
    - PowerLogic PD100
    - Exiway Link emergency lighting devices
    - XB5R transmitters (ZBRT)

The devices supported by the Panel Server are listed in the respective release notes, page 10:

- DOCA0249•• *EcoStruxure Panel Server Entry - Firmware Release Notes*
- DOCA0178•• *EcoStruxure Panel Server Universal - Firmware Release Notes*
- DOCA0248•• *EcoStruxure Panel Server Advanced - Firmware Release Notes*

(1) China-certified devices only.

Panel Server Entry Maximum Configuration

The table shows the maximum number of devices that can be configured in a system with a Panel Server Entry.

Wireless device	Maximum number of concurrent devices
PowerTag Energy sensors	20
PowerLogic Tag energy sensors	20
Acti9 Active devices	20
PowerTag Control devices	10
Wireless indication auxiliaries for ComPacT and PowerPacT circuit breakers	20
MasterPacT MTZ circuit breakers with MicroLogic Active AP or EP control unit	8
Wireless CO_2 sensors	20
Wireless temperature and humidity sensors	20
PowerTag Ambient sensors	20
PowerLogic TH110/CL110 environmental sensors	20
PowerLogic Thermal Tag TH150/TH200 wireless temperature sensors(2)	20
PowerLogic HeatTag sensors	15
PowerLogic PD100 devices	15
Exiway Link devices	20
XB5R transmitters (ZBRT)	20
The recommendation for a mixed configuration of wireless devices is that any combination of wireless devices listed in the rows above should not exceed **20 devices**.	

For more information, contact your local Schneider Electric representative.

Panel Server Universal and Advanced Maximum Configuration

The maximum number of devices that can be configured in a system with a Panel Server Universal or Advanced depends on the type of connected devices:

Device type		Maximum number of concurrent devices
Wireless device (not supported by PAS600LWD and PAS600PWD)	PowerTag Energy sensors	85
	PowerLogic Tag energy sensors	85
	Acti9 Active devices	85
	Wireless indication auxiliaries for ComPacT and PowerPacT circuit breakers	85
	MasterPacT MTZ circuit breakers with MicroLogic Active AP or EP control unit	8
	Wireless CO_2 sensors	100
	Wireless temperature and humidity sensors	100
	PowerTag Ambient sensors	100
	PowerLogic TH110/CL110 environmental sensors	100
	PowerLogic Thermal Tag TH150/TH200 wireless temperature sensors(2)	100
	PowerLogic HeatTag sensors	15
	PowerTag Control devices	10
	PowerLogic PD100 devices	15

(2) China-certified devices only.

Device type		Maximum number of concurrent devices
	Exiway Link devices	20
	XB5R transmitters (ZBRT)	100
	The recommendation for a mixed configuration of wireless devices is as follows: • Any combination of wireless devices listed in the rows above should not exceed **40 devices**. • The total number of PowerTag Control, PowerLogic HeatTag, PowerLogic PD100, MicroLogic Active AP or EP control unit for MasterPacT MTZ, and Exiway Link devices should not exceed **20 devices**.	
Modbus-SL devices	Modbus-SL devices other than I/O devices:	32 **NOTE:** The maximum number depends on the serial line length and the type of device(s).
	I/O devices: • I/O Smart Link device • Acti9 Smartlink Modbus-SL device • SmartLink SIB gateway	• 8 I/O Smart Link or Acti9 Smartlink Modbus-SL devices connected to Panel Server serial line • OR 1 SmartLink SIB + 7 I/O Smart Link or Acti9 Smartlink Modbus-SL devices • OR 8 SmartLink SIB
Modbus TCP/IP devices	Devices physically connected to the Panel Server and virtual devices, that is, IEEE 802.15.4 wireless devices connected to a child Panel Server gateway.	128 **NOTE:** The Panel Server supports 64 simultaneous Modbus TCP/IP client connections (for example, SCADA system).

For more information, contact your local Schneider Electric representative.

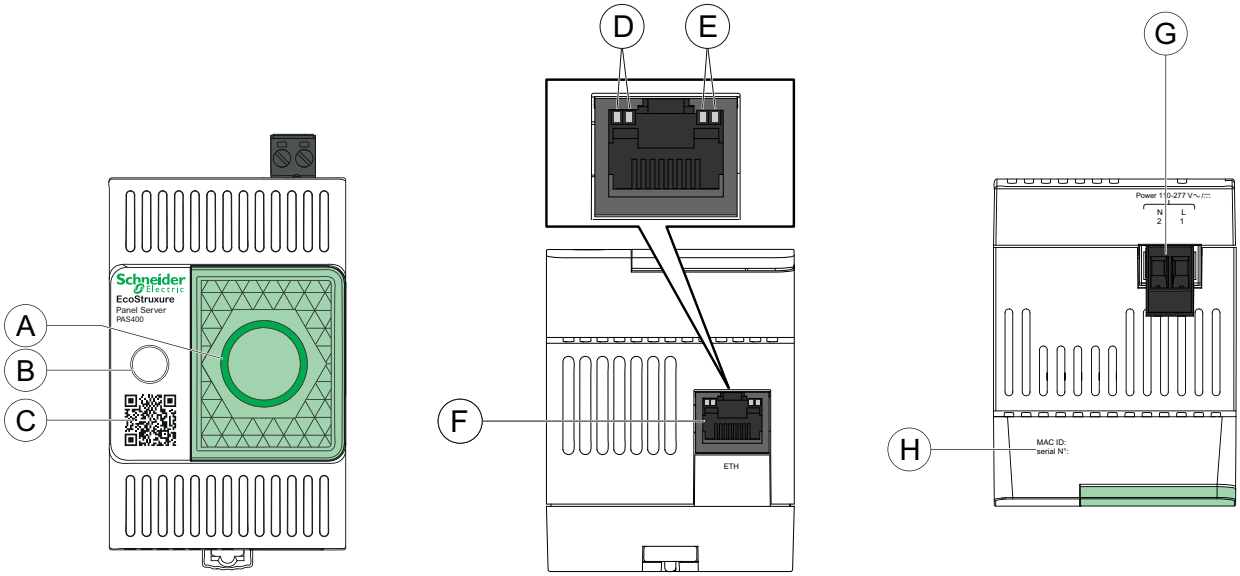
Recommendations for Maximizing Performance (Panel Server Universal and Advanced)

- Do not exceed the maximum number of Modbus-SL devices shown in the table above.
- The suggested maximum of 32 Modbus-SL devices presumes a sampling period of 1 minute or more. Performance may be affected if lower sampling periods are used.
- When the Panel Server is used as a transparent gateway, do not leave the devices connected to the Panel Server after testing or maintenance. Refer to Modbus Transparent Gateway, page 61.
- For architectures including a SCADA system, connect a maximum of 8 Modbus-SL devices.
- For architectures using Power Monitoring Expert, use the PME 2020 Daisy Chain Calculator to calculate the maximum configuration.

Hardware Description

Panel Server Entry

Front face **Bottom** **Top**

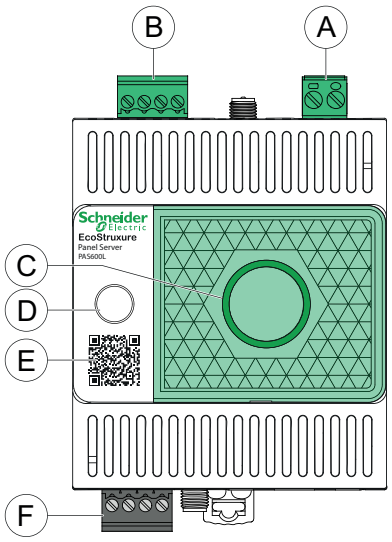


A. Panel Server status LED
B. Multifunction button
C. QR code to product information (including device code, credentials for use in secure claiming of Panel Server from Cloud applications)
D. Ethernet LED 1: Speed
E. Ethernet LED 2: Activity
F. Ethernet communication port
G. Power supply terminal block
H. MAC address and serial number

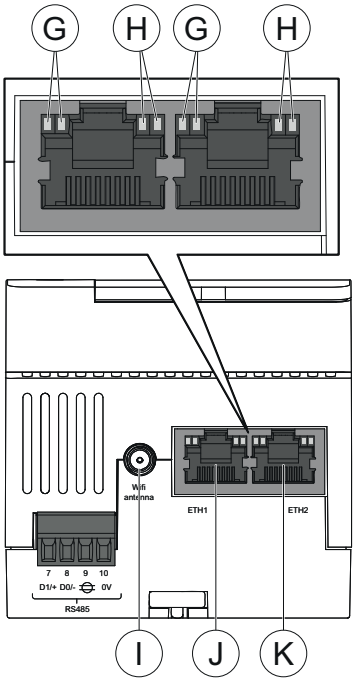
For information about installation of Panel Server Entry, consult the instruction sheet available on the Schneider Electric website: NNZ76760.

Panel Server Universal

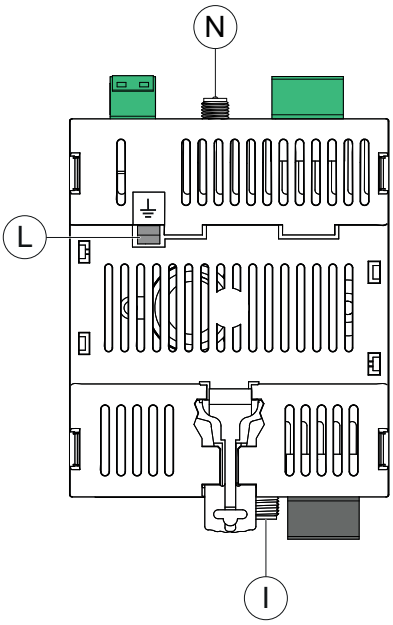
Front face



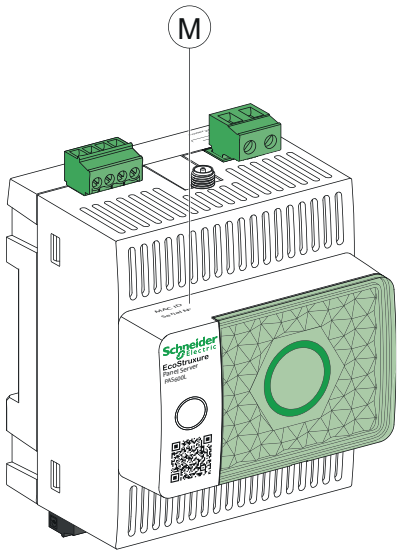
Bottom



Rear



Top

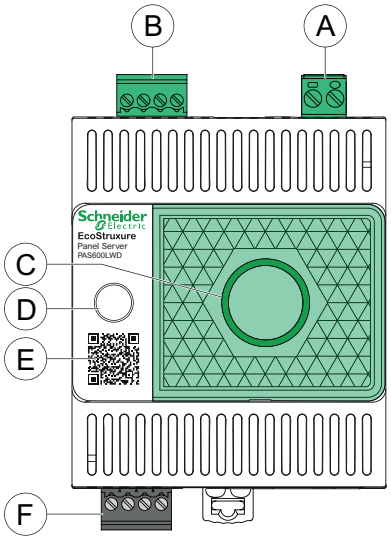


A. Power supply terminal block
B. Digital input terminal block (PAS600L)
C. Panel Server status LED
D. Multifunction button
E. QR code to product information (including device code, credentials for use in secure claiming of Panel Server from Cloud applications)
F. RS485 Modbus communication port
G. Ethernet LED 1: Speed
H. Ethernet LED 2: Activity
I. External Wi-Fi antenna port
J. Ethernet 1 communication port
K. Ethernet 2 communication port
L. Grounding connection
M. MAC address and serial number and hardware version HW: V2.0 (for hardware version 002.000.000 only)
N. External IEEE 802.15.4 antenna port (for HW: V2.0 PAS600, PAS600L only)

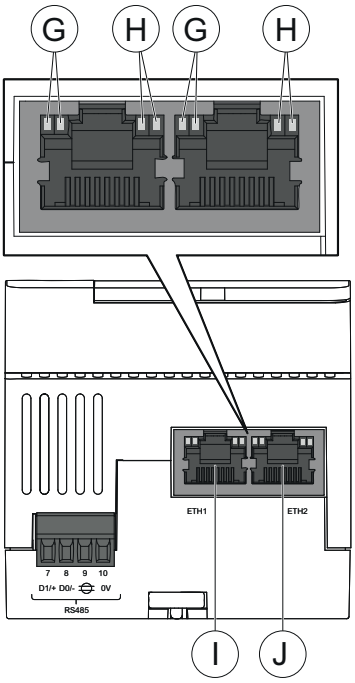
For information about installation of Panel Server Universal, consult the instruction sheet available on the Schneider Electric website: GEX84977

Panel Server Universal Wired by Design

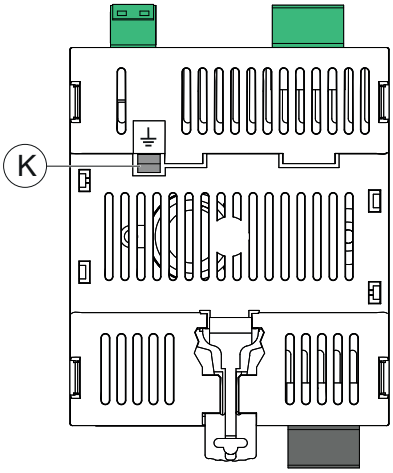
Front face



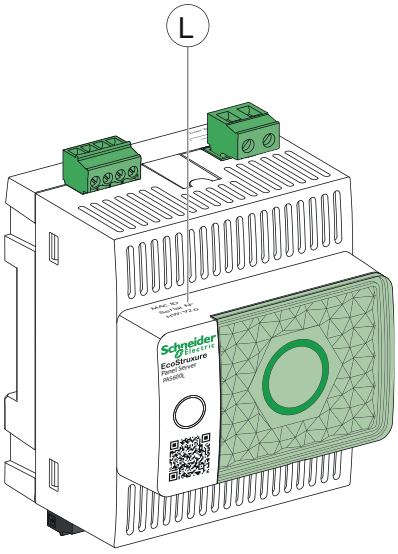
Bottom



Rear



Top

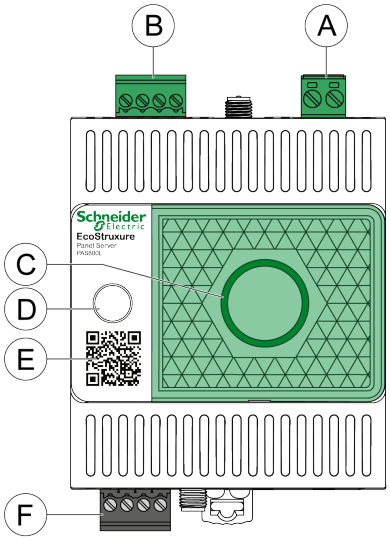


A. Power supply terminal block (PAS600LWD)
B. Digital input terminal block (PAS600LWD)
C. Panel Server status LED
D. Multifunction button
E. QR code to product information (including device code, credentials for use in secure claiming of Panel Server from Cloud applications)
F. RS485 Modbus communication port
G. Ethernet LED 1: Speed
H. Ethernet LED 2: Activity
I. Ethernet 1 communication port
J. Ethernet 2 communication port (PoE port for PAS600PWD)
K. Grounding connection
L. MAC address, serial number, and hardware version HW: V2.0

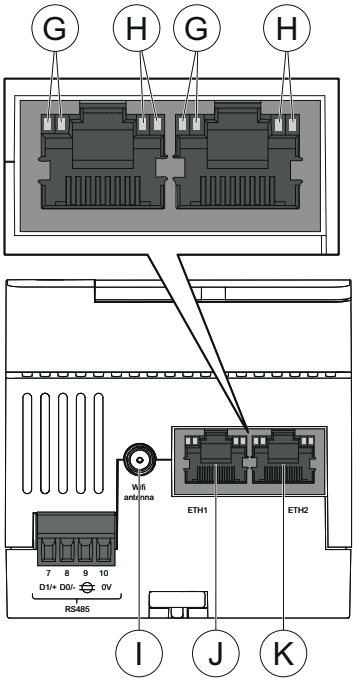
For information about installation of Panel Server Universal Wired by Design, consult the instruction sheet available on the Schneider Electric website: PKR28607.

Panel Server Advanced

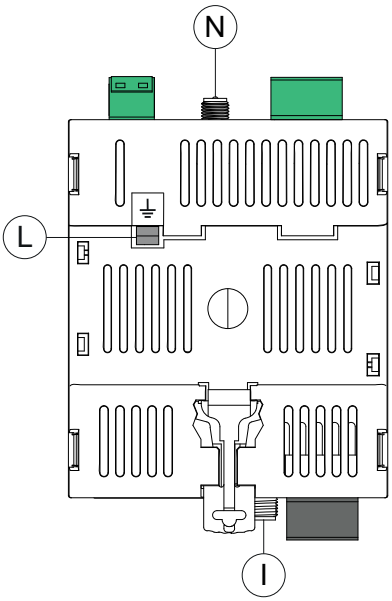
Front face



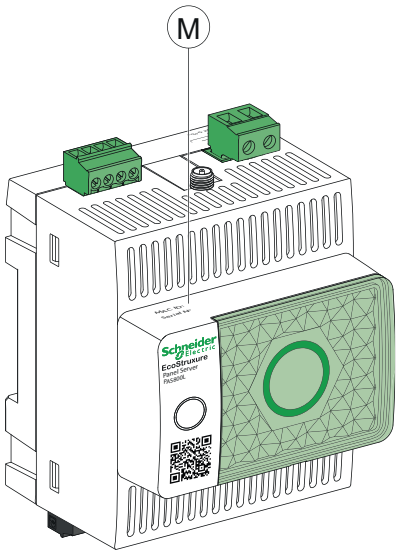
Bottom



Rear



Top



A. Power supply terminal block (PAS800, PAS800L)
B. Digital input terminal block (PAS800L)
C. Panel Server status LED
D. Multifunction button
E. QR code to product information (including device code, credentials for use in secure claiming of Panel Server from Cloud applications)
F. RS485 Modbus communication port
G. Ethernet LED 1: Speed
H. Ethernet LED 2: Activity
I. External Wi-Fi antenna port
J. Ethernet 1 communication port
K. Ethernet 2 communication port (PoE port for PAS800P)
L. Grounding connection
M. MAC address and serial number and hardware version HW: V2.0 (for hardware version 002.000.000 only)
N. External IEEE 802.15.4 antenna port (PAS800, PAS800L)

For information about installation of Panel Server Advanced, consult the instruction sheet available on the Schneider Electric website: BQT54848.

Hardware Version

The Panel Server exists in two hardware versions, depending on the model and the date of manufacture, hardware version 001.000.000 and hardware version 002.000.000.

The following models of EcoStruxure Panel Server are released with hardware version 002.000.000 (HW: V02):

- PAS600PWD Wired by Design model without wireless communication capability
- PAS600LWD Wired by Design model without wireless communication capability

Certain models of Universal and Advanced EcoStruxure Panel Server exist in two hardware versions: 001.000.000 and 002.000.000 (HW: V02). For Advanced EcoStruxure Panel Server, both versions offer the same capabilities and functionality. For PAS600 and PAS600L, hardware version 002.000.000 provides the following functions in addition to those provided by hardware version 001.000.000:

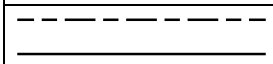
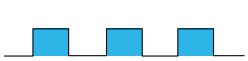
- 5 GHz Wi-Fi connectivity
- External IEEE 802.15.4 antenna port

To identify the hardware version of your Panel Server, check in one of the following ways:

- The information printed on the top of the Panel Server:
  - Hardware version 001.000.000: MAC address and serial number
  - Hardware version 002.000.000: MAC address, serial number, and HW: V2.0
- In the Panel Server webpages at either of the following paths:
  - **Settings > General > Identification > Hardware revision**
  - **Maintenance > Firmware update > Hardware revision**

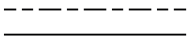
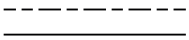
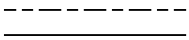
Panel Server Status LED

The LED indicates the operation mode of the Panel Server.

LED indication	Description
	Panel Server switched off.
	Panel Server is powering on. System boots within 2 minutes.
	Panel Server in normal operation.
	Minor malfunction detected. Connect to Panel Server software to diagnose.
	Major malfunction detected. Panel Server must be replaced.
	Wi-Fi access point is available for connection.
	Wi-Fi access point connection is established.

Ethernet Status LEDs

The combination of the two LEDs of one RJ45 port indicates the Ethernet communication status of the Panel Server.

Ethernet LEDs		Description
LED 1: Speed	**LED 2: Activity**	
		No Ethernet communication
		10 Mb Ethernet communication active
		100 Mb Ethernet communication active

Multifunction Button

Use the multifunction button to perform the following functions:

- Initiate connection using the Wi-Fi access point (except Wired by Design models)
- Restart the Panel Server
- Reset the Panel Server to factory settings

Function	Action	LED status	Indicates
Activate Wi-Fi access point	Press the multifunction button for less than 5 s	Blinking blue	The Panel Server Wi-Fi access point is available for connection.
		Steady blue	The Wi-Fi access point connection is established.
		Blinking fast orange	The Wi-Fi access point connection is not authorized.
Restart Panel Server	Press the multifunction button for 5 s to 10 s	Steady orange	The Panel Server is restarting.
		Steady green	The Panel Server is in normal operation after restart.
Reset Panel Server to factory settings, page 190	Press the multifunction button for more than 10 s until the steady orange LED starts blinking fast.	Blinking fast orange	Reset to factory settings is initiated.
	Confirm reset to factory settings by pressing the multifunction button again within 5 seconds.	Blinking fast green	Reset to factory settings is confirmed.
	To cancel reset to factory settings, wait for the LED to change color.	Blinking fast red	Reset to factory settings is cancelled.
	Wait for the Panel Server to restart completely.	Steady orange	The Panel Server is booting
		Steady green	The Panel Server is in normal operation after reset.

QR Code

When the QR code on the front face of a Panel Server is scanned with a smartphone connected to the Internet, the Go2SE landing page is displayed, page 32.

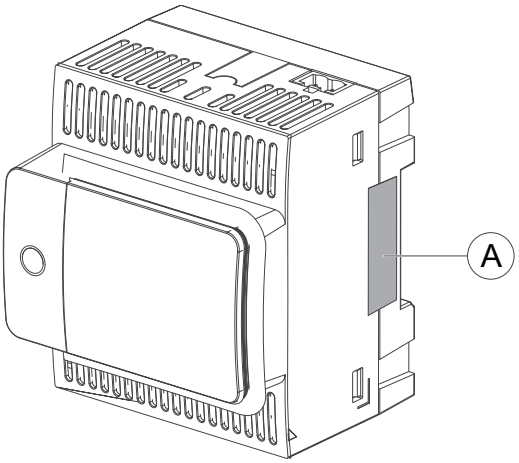
The landing page displays:

- Information about the Panel Server
- A list of menus

Tamper Detection

A tamper-indicating label helps detect unauthorized physical access into the Panel Server. This label is light grey with Schneider Electric written in black.

The following figure illustrates the position of the tamper-indicating label **(A)** affixed on the right-hand side of the Panel Server:



Before installing, operating, servicing, or maintaining the EcoStruxure Panel Server, check the tamper-indicating label integrity.

External Wi-Fi Antenna Port

The optional external wireless devices/Wi-Fi antenna, page 29 can be connected via the Wi-Fi antenna port for:

- Panel Server Universal (except Wired by Design models)
- Panel Server Advanced

Connect the external antenna (reference PASA-ANT1) to the Wi-Fi antenna port at the bottom of the Panel Server and install the antenna on the roof of the switchboard.

For information about configuring the Panel Server after installing the external antenna, refer to Wi-Fi Infrastructure, page 86.

External IEEE 802.15.4 Antenna Port

The optional external wireless devices/Wi-Fi antenna, page 29 can be connected via the IEEE 802.15.4 antenna port for:

- Panel Server Universal hardware version 002.000.000 (except Wired by Design models)
- Panel Server Advanced

Connect the external antenna (reference PASA-ANT1) to the IEEE 802.15.4 antenna port at the top of the Panel Server Universal or Advanced and install the antenna on the roof of the switchboard.

For information about configuring the Panel Server after installing the external antenna, refer to IEEE 802.15.4 Communication, page 108.

Panel Server External Wireless Devices/Wi-Fi Antenna

Use the external wireless devices/Wi-Fi antenna (reference PASA-ANT1) in specific use cases such as when the Panel Server Universal or Advanced is installed in a switchboard with metallic partitions and door, and some wireless devices are located in a different place. The antenna extends the wireless or Wi-Fi network outside the switchboard.

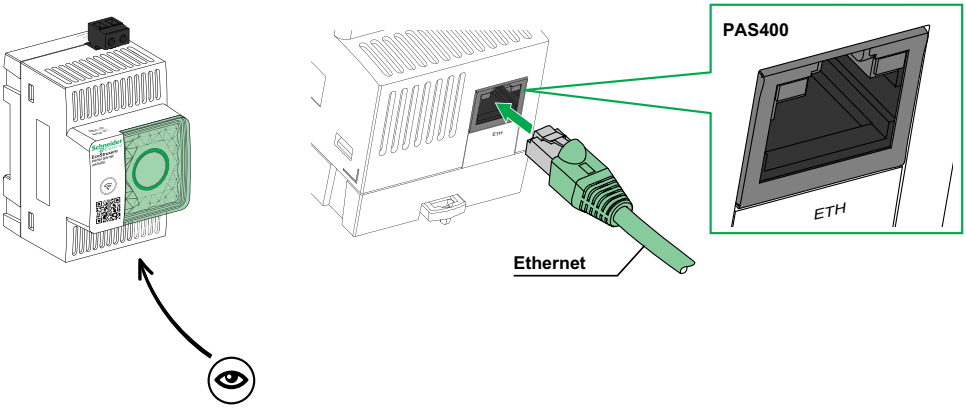
For information about installation of the external antenna, consult the instruction sheet available on the Schneider Electric website: NNZ58425.

For information about wireless communication in the Panel Server system, consult DOCA0289•• *Wireless Communication Architectures With EcoStruxure Panel Server - Design Guide*, page 10.

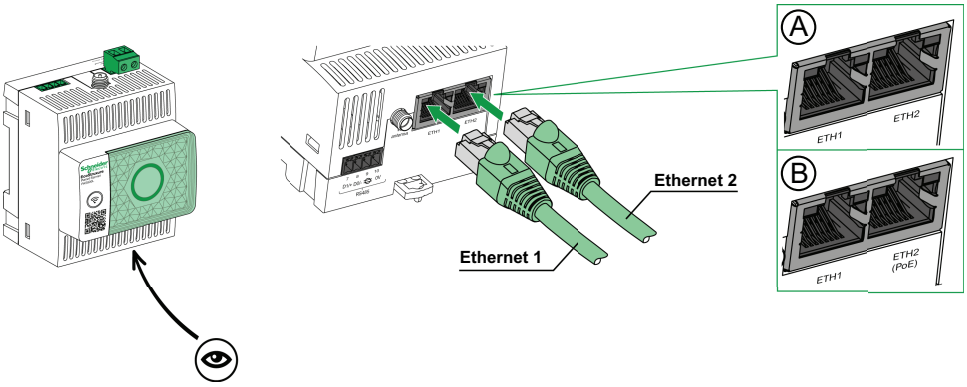
Hardware Connection

Connection to Ethernet

Entry model



Universal, Advanced models

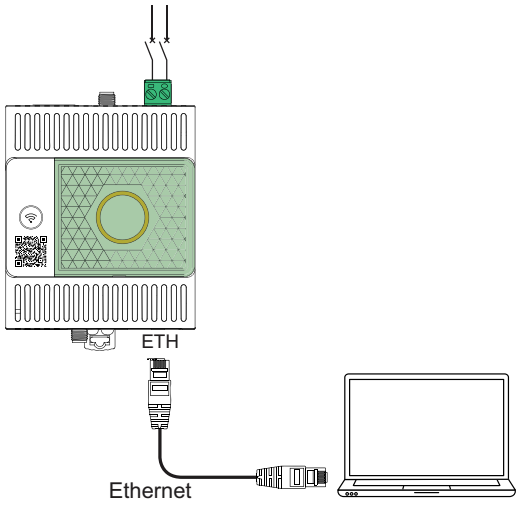


A. Ethernet ports for PAS600, PAS600T, PAS600L, PAS600LWD, PAS800, PAS800L
   - ETH1
   - ETH2

B. Ethernet ports for PAS600PWD, PAS800P
   - ETH1
   - ETH2 (PoE)

   NOTE: PAS600PWD and PAS800P can be powered by Power over Ethernet (PoE) through ETH2 port. For information about connection of these models to an Ethernet switch with Endspan PoE ports or Midspan PoE ports, consult the instruction sheet available on the Schneider Electric website:
   - PKR28607 *EcoStruxure Panel Server Universal Wired by Design - Instruction Sheet* for PAS600PWD
   - BQT54848 *EcoStruxure Panel Server Advanced - Instruction Sheet* for PAS800P

Connection to a PC



Proceed as follows to connect a PC to a Panel Server through Ethernet:

- Entry model: connect an Ethernet cable between the PC and the Ethernet port on Panel Server.
- Universal and Advanced models: connect an Ethernet cable between the PC and one of the Ethernet ports on Panel Server (**ETH1** or **ETH2**).

Device Landing Page

Presentation

When the QR code on the front face of a Panel Server is scanned with a smartphone running a QR code reader and connected to the Internet, a Go2SE link takes you to the device landing page.

Landing Page Description

The landing page is accessible from Android and iOS smartphones. It displays the same list of menus with slight differences in presentation.

The landing page shows:

- Product image
- Links to:
  - Download Product Data Sheet
  - Register Product
- **Overview**
  - Serial number
  - Reference
  - Description
  - Origin
  - Date of Manufacture
  - Device code (code) of the Panel Server (available in models manufactured with serial number 542427••••• or greater).

    NOTE: The device code represents the credentials of the Panel Server. Treat this information as confidential.
- **Resource Center**
  - Access all documents
    - Instruction sheets
    - User guides
    - Brochures
    - Declarations of conformity
  - Environmental data
- **Support**

mySchneider App

Selecting this application gives access to the Schneider Electric customer care mobile application, **mySchneider** app, that can be downloaded on Android and iOS smartphones. For smartphone compatibility, check on your application store. The customer care application offers self-service instructions and easy access to expert support and information.

EcoStruxure Panel Server Webpages Overview

The web server embedded in the EcoStruxure Panel Server provides webpages enabling you to commission electrical products and systems compatible with the EcoStruxure Panel Server in your switchboard.

In addition the webpages provide real-time data and active alarm visualization, and historical analysis from devices (depending on the model), for entry-level energy and operation management.

Electrical product and commissioning capabilities allow you to:

- Discover wireless devices installed in the EcoStruxure Panel Server system (depending on the model).
- Discover Modbus-SL and Modbus TCP/IP devices from EcoStruxure Panel Server (depending on the model).
- Configure I/O devices connected to the EcoStruxure Panel Server through the digital inputs (depending on the model).

Energy and operation monitoring capabilities allow you to:

- Visualize real-time data and events through a supported web browser.
- Monitor and control connected devices.
- Publish data to an SFTP or HTTPS server or to the Schneider Electric cloud.
- Visualize trending on historical data, up to a period of 3 years (Advanced model).
- Export selected logged data to your PC for additional analysis (Advanced model).

For more detailed information about the webpages, refer to Using EcoStruxure Panel Server Webpages, page 203.

EcoStruxure Power Commission (EPC) Software

Overview

NOTICE

SOFTWARE INCOMPATIBILITY

- EcoStruxure Power Commission software and Mobile App do not support Panel Server with firmware versions 002.007.000 and 002.008.000. Use the Panel Server webpages instead for Panel Server firmware update, commissioning and configuration operations.
- For Panel Server with firmware version up to 002.006.001, EcoStruxure Power Commission software and Mobile App can continue to be used for Panel Server firmware update, commissioning and configuration operations.

Failure to follow these instructions can limit the ability to commission and configure the equipment.

EcoStruxure Power Commission is intelligent software that helps you set up, test, and commission the electrical products and systems in your switchboards with efficiency and ease. It also allows you to generate a dedicated QR code for the electrical panel to enable digital collaboration with contractors and facility managers by sharing important documentation.

Key Features

EcoStruxure Power Commission software performs the following actions for the supported devices :

- Easy setup
  - Discover all the smart devices in your electrical switchboard
  - Check firmware compatibility and install upgrades as required
  - View communication architecture and adjust communication settings
  - View the list of devices organized in the switchboard, and configure electrical settings for breakers and meters
- Advanced testing
  - Execute Factory Acceptance Tests (FAT) and reporting:
    - Test MasterPacT MTZ circuit breakers with automatic trip curve tests, zone-selective interlocking tests
    - Test the communication wiring and generate reports
- Fast commissioning
  - Adjust settings without connection to the devices through offline configuration feature
  - Use batch operations features to speed up settings configuration, for several devices at the same time
  - Generate a comprehensive project report that lists your switchboard and related devices, firmware version, and serial numbers, for example.
- Digital collaboration
  - Create a unique QR code for the entire switchboard and then upload all relevant documentation including important CAD drawings, user guides, bill of materials, single-line diagrams, photos and more to Schneider Electric cloud repository.
  - Simplify project handover with the digital logbook functionality, making it faster and easier for the facility manager to access historical information and collaborate with all project partners

For more information, tutorials, and download link, visit the EcoStruxure Power Commission software webpage.

EcoStruxure Power Commission Web Tool (EPC Web)

Overview

The EcoStruxure Power Commission Web tool is intended to help system integrators save time to execute their projects by offering the following actions so that you can cater to different customer requirements in terms of events or measurements of devices to be monitored:

- Giving access to a common single device model library that can be used on any EcoStruxure Panel Server.
- Giving you the ability to manage your own device models by creating, testing, and deploying them.
- Giving access to cloud connected gateways and devices to associate required models.

A custom device model in the EcoStruxure Power Commission Web tool contains the list of measurements, alarms, Modbus frames and events that can be used to monitor Modbus based devices in the field. The user can create, edit, view, and export device model data as per the requirement.

Key Features

The EcoStruxure Power Commission Web tool allows you to perform the following actions:

- Create a model: Create from scratch reusable device models for monitoring Modbus devices using EcoStruxure Panel Server.
- View and Export Models: Select and export device models previously created by you or others so that they can be imported in EcoStruxure Panel Server.

Detailed help and instructions for creating a device model are available in the EcoStruxure Power Commission Web tool at **Help > Documentation**.

For more information, go to EcoStruxure Power Commission Web.

EcoStruxure Cybersecurity Admin Expert (CAE) Software

EcoStruxure Cybersecurity Admin Expert (CAE) is a software-based tool used for security administration including:

- Providing centralized administration of user accounts and roles for devices such as Panel Server gateways.
- Creating a cybersecurity policy.
- Configuring the security of devices.
- Monitoring and auditing security events and logs of the system by using a Syslog server.

CAE software simplifies the management and the maintenance of cybersecurity and improves efficiency of configuration, by incorporating these services in a single tool.

CAE software version 4.3 supports Panel Server gateways with firmware version 002.008.000.

EcoStruxure System Management (ESM) Software

EcoStruxure System Management (ESM) software provides a comprehensive, end-to-end solution for OT asset baseline management, delivering full visibility and control across the entire asset lifecycle, from initial discovery through continuous change tracking. With flexible onboarding capabilities, including IEC 61850, CSV import, manual entry, and automated network scanning, ESM rapidly builds a structured and accurate representation of your infrastructure.

ESM captures automated configuration snapshots and maintains built-in version control to track all changes to firmware, settings, and device configurations over time. Real-time baseline comparison and drift detection enable users to quickly identify deviations, support compliance, and maintain operational consistency.

Designed for real-world OT environments, ESM combines open multi-protocol interoperability with enterprise-grade cybersecurity, enabling seamless integration of diverse devices while maintaining strict control through centralized policies and role-based access.

In addition, ESM continuously collects and contextualizes disturbance records across the fleet. By correlating COMTRADE data with the exact device configuration at the time of each event, it significantly accelerates root cause analysis and enhances overall system reliability.

Starting with ESM version 1.19, Panel Server gateway is supported by ESM.

For more information, visit the EcoStruxure System Management software webpage.

Edge Monitoring and Supervision Software

EcoStruxure Power Monitoring Expert (PME)

EcoStruxure Panel Server allows you to export the panel configuration (list of devices and communication addresses) into PME or EPO by using EcoStruxure Power Commission software, for setup efficiency.

EcoStruxure Power Monitoring Expert is a complete, interoperable, and scalable software package for power management applications. The software collects and organizes data gathered from the electrical network and presents it as meaningful, actionable information through an intuitive Web interface. It allows you to share information with key stakeholders or across your entire operation to influence behavioral changes that can save you money.

EcoStruxure Building Operation (EBO)

EcoStruxure Building Operation is an integrated building management system that delivers the actionable insights needed to better manage and optimize buildings, improve engineering efficiency, and meet cybersecurity needs. EcoStruxure Building Operation is an open building management platform that integrates multiple systems for centralized, real-time control and management across one to many enterprise buildings.

EcoStruxure Power Operation (EPO)

EcoStruxure Power Operation is a SCADA system uniquely designed to help large electrical distribution applications in facilities like data centers, industrials, airports and electro-intensive operations maximize uptime, unite their medium and low voltage networks and integrate mechanical monitoring. With rich data integration from connected devices, EcoStruxure Power Operation unique capabilities provide real-time situational awareness and offer a high-performance, cyber-resilient solution for your specialized power network.

Cloud Applications

EcoStruxure Energy Hub (EEH) (Part of EcoStruxure Building Activate)

Connect your building energy systems and smart devices with EcoStruxure Energy Hub and EcoStruxure Building Activate. Automatically collect, store, visualize, report, and alarm on your data to simplify the energy management of digitalized electrical and energy systems in commercial, industrial and institutional buildings.

As power digitalization continues to transform our electrical distribution infrastructure, today's commercial, industrial and institutional buildings face increasing regulatory requirements and public interest in sustainability and decarbonization. Building owners and operators need to ensure compliance with building codes/standards as well as demonstrate to occupants, future tenants, and investors that their building is up to the sustainability challenge.

- Hit energy targets and comply with standards
- Track and retain energy data for transparency and compliance requirements
- Benchmark buildings' energy performance and identify savings opportunities
- Break down energy use by area, zone, and usage type
- Easily visualize your energy system status and alert maintenance of detected faults
- Diagnose and resolve issues quickly

EcoStruxure Energy Hub is designed to address these challenges with a simple, smart energy application for your building, without a large upfront investment.

EcoStruxure Asset Advisor (EAA)

EcoStruxure Asset Advisor brings a proactive approach to electrical distribution and critical data center assets, combining IoT and cloud-based technologies with Schneider Electric experts and services for business continuity. EcoStruxure Asset Advisor services offer the ability to anticipate and address issues before they become critical incidents, mitigating safety risks, reducing unplanned downtime, operational losses and expensive maintenance interventions.

EcoStruxure Resource Advisor (ERA)

EcoStruxure Resource Advisor helps with aggregating all cross-enterprise, energy and sustainability information in a single, cloud-based platform. EcoStruxure Resource Advisor enables both data analysis and data action. Energy, water, waste, carbon, building metrics, weather, and more can all be integrated into a single platform, which provides the ability to see high-level trends across an enterprise down to granular load profiles of a single building or piece of equipment.

Technical Characteristics

Environmental Characteristics

Characteristic		Value
Conforming to standards		• IEC 61010-1/IEC 61010-2-201 • UL 61010-1/CSA C22.2 no. 61010-1-12 • UL 61010-2-201/CAN/CSA-C22.2 no. 61010-2-201
Certification		• CE • cULus • RCM • UKCA • FCC • IC • EAC • CB • WPC • IMDA
Ambient temperature during storage		-40 °C to +85 °C (-40 °F to +185 °F)
Ambient temperature in operation: < 2,000 m (< 6,500 ft)	Horizontal installation (for indoor use in non-wet locations only)	• Entry model: -25 °C to +60 °C (-13 °F to +140 °F) • Universal, Advanced models: -25 °C to +70 °C (-13 °F to +158 °F)
	Vertical installation (for indoor use in non-wet locations only)	• Entry model: -25 °C to +45 °C (-13 °F to +113 °F) • Universal, Advanced models: -25 °C to +50 °C (-13 °F to +122 °F)
Ambient temperature in operation: 2,000–4,000 m (6,500–13,000 ft)	PAS600L, PAS600LWD, PAS800L	-25 °C to +60 °C (-13 °F to +140 °F)
Ambient temperature in operation: 4,000–5,000 m (13,000–16,400 ft)		-25 °C to +55 °C (-13 °F to +131 °F)
Pollution degree	PAS400, PAS600, PAS600T, PAS600PWD, PAS800, PAS800P	2
	PAS600L, PAS600LWD, PAS800L	3
Altitude	All models	< 2,000 m (< 6,500 ft)
	PAS600L, PAS600LWD, PAS800L	< 5,000 m (< 16,400 ft)
Relative humidity		5–95% relative humidity (without condensation) at 55 °C (131 °F)
Environment		In compliance with the RoHS directive and REACH Regulations
Electromagnetic compatibility		• IEC 61326-1 • IEC 62974-1 • EN 301489-1 • EN 301489-17
Immunity		• IEC 61326-1 • IEC 62974-1 • EN 301489-1 • EN 301489-17
Environment: emissions		• CISPR 11 • EN 55032
Electromagnetic compatibility and Radio spectrum Matters (ERM)		• EN 300328 • EN 301893
Mean time to failure (MTTF)	PAS400	307 years
	PAS600, PAS600T, PAS600L, PAS600LWD, PAS600PWD	208 years
	PAS800, PAS800L, PAS800P	172 years

Communication Characteristics

Characteristic	Value
Communication interface	• 10/100BASE-T Ethernet RJ45 ports: ◦ Entry model: one port ◦ Universal and Advanced models: two ports • RS485 Modbus port • Wi-Fi (excluding WD models), compliant to standard IEEE 802.11 a/b/g/n ◦ Universal models (hardware version 001.000.000): 2.4 GHz ◦ Entry, Universal models (hardware version 002.000.000) and Advanced models: 2.4 GHz, 5 GHz • Wi-Fi access point (excluding WD models), compliant to standard IEEE 802.11 a/b/g/n: all models : 2.4 GHz on channel 11 • IEEE 802.15.4 (all models, excluding WD models) • Ethernet 2 IEEE 802.3af (802.3at Type 1) (PAS600PWD, PAS800P)
Automatic IP configuration	DPWS-ready, DHCP client IPv4, IPv6
IP network	• Modbus TCP/IP connection • HTTPS
Radio frequency ISM band	2.4 GHz to 2.4835 GHz (in accordance with IEEE 802.15.4 standard) (all models, excluding WD models)

Radio Equipment Directive (RED)

From August 2025, EcoStruxure Panel Server products are compliant with the essential requirements of the Radio Equipment Directive (RED), including:

- Article 3.3 (d) Network protection: EN 18031-1:2024
- Article 3.3 (e) Protection of personal data and privacy: EN 18031-2:2024

This compliance applies to products manufactured and sold from August 2025 onwards, and from EcoStruxure Panel Server firmware version 002.002.001.

FCC Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operating in a commercial environment. This equipment generates, uses, and can radiate radiofrequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

NOTE: The country code selection is for non-US model only and is not available to all US models. Per FCC regulation, all Wi-Fi product marketed in the US must be fixed to US operation channels only.

Electrical Characteristics

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
Power supply	110–277 Vac/dc (±10 %)	✓	✓	✓	-	-	-	-	-	✓	✓	-	-	-	-
	24 Vdc (±10 %)	-	-	-	-	✓	✓	✓	-	-	-	✓	✓	-	-
	110–240 Vac/dc (±10 %)	-	-	-	✓	-	-	-	-	-	-	-	-	-	-
	Power over Ethernet (PoE)	-	-	-	-	-	-	-	✓	-	-	-	-	✓	✓
Power consumption (maximum)	3W (10VA for AC input)	-	✓	-	✓	✓	-	-	-	-	-	-	-	-	-
	3.5W (12VA for AC input)	✓	-	✓	-	-	✓	✓	✓	✓	✓	✓	✓	✓	✓
Power input	• Power over Ethernet: Class 0 • Operating Input Range: 37–57 Vdc • Rating: < 3.5 W (72 mA) 48 Vdc typical	-	-	-	-	-	-	-	✓	-	-	-	-	✓	✓
Frequency	50-60 Hz (±5 Hz)	✓	✓	✓	-	-	-	-	-	✓	✓	-	-	-	-
	50-60 Hz (±3 Hz)	-	-	-	✓	-	-	-	-	-	-	-	-	-	-
Overvoltage category		III	III							III					

IEC62974-1 Certification Characteristics

Characteristic	Value
PAS400	Data gateway (in accordance with IEC 62974-1 standard, Class 2, -5° C to +55° C (23 °F to 131 ° F))
PAS600, PAS600T, PAS600L, PAS600LWD, PAS600PWD	Data gateway (in accordance with IEC 62974-1 standard, Class 2, -25° C to +70° C (-13 °F to +158 °F))
PAS800, PAS800L, PAS800P	Energy server (in accordance with IEC 62974-1 standard, Class 2, -25° C to +70° C (-13 °F to +158 °F))

Physical Characteristics

Characteristic		Value
Dimensions (L x H x D)	PAS400	54 x 93 x 70.2 mm (2.12 x 3.66 x 2.76 in)
	PAS600, PAS600T, PAS600L, PAS600LWD, PAS600PWD, PAS800, PAS800L, PAS800P	72 x 93 x 70.2 mm (2.83 x 3.66 x 2.76 in)
Weight	PAS400	163 g (5.7 oz)
	PAS600, PAS600T	201 g (7 oz)
	PAS600L	181 g (6.38 oz)
	PAS600LWD	180 g (6.34 oz)
	PAS600PWD	182 g (6.42 oz)
	PAS800	206 g (7.3 oz)
	PAS800L	186 g (6.6 oz)
	PAS800P	184 g (6.5 oz)
Mounting		DIN rail
Connections		Screw type terminal blocks
Antenna		• External Wi-Fi antenna (option for Universal, excluding WD models, and Advanced models) • External IEEE 802.15.4 antenna (option for Universal models (HW 002.000.000) and Advanced models)
Degree of protection		• Connectors: IP20 • Other faces: IP30 • Front face: IP40

Digital Inputs Characteristics

Characteristic	Value
Number of digital inputs	2
Digital input type	Current sink, compliant with IEC 61131-2, type 1
Rated input voltage	24 V
Input voltage limits	19.2–28.8 Vdc
Input voltage logic	• State 0: 0–5 V • State 1: 15–28 V
Input current	• State 0: 0 mA • State 1: 3–7.5 mA
Isolation	Functional isolation
Maximum cable support	10 m (32.8 ft)

Wi-Fi Antenna Characteristics

Characteristic	Value
Antenna frequency range	Dual band: 2.4 GHz, 5 GHz
Kit composition	Antenna with cable 3 m (9.84 ft)
Input impedance	50 Ω
Connector	RPSMA plug antenna gain 2–3 dBi
Net weight	150 g (5.29 oz)

IEEE 802.15.4 Antenna Characteristics

Characteristic	Value
Antenna frequency range	Dual band: 2.4 GHz, 5 GHz
Kit composition	Antenna with cable 3 m (9.84 ft)
Input impedance	50 Ω
Connector	RPSMA plug antenna gain 2–3 dBi
Net weight	150 g (5.29 oz)

Miscellaneous

The EcoStruxure Panel Server complies with the *DNV rules for classification - Ships, offshore units, high speed and light craft*. The Entry (PAS400), Universal (PAS600) and Advanced (PAS800) models can be installed on all vessels classified by DNV as per the Type Approval Certificate issued by DNV.

EcoStruxure Panel Server Configuration Functions

What’s in This Part

Date and Time 47
Firmware Update 50
User Management Using Panel Server Webpages 52
User Management Using EcoStruxure Cybersecurity Admin Expert 55

Date and Time

Presentation

The date and time function is used to configure date and time either manually or with automatic synchronization. Accurate date and time are required to enable TLS certificate validity checking, as well as to obtain properly time-stamped logs.

Panel Server date and time are used for time stamping events to provide a chronological order.

You can set a local time zone by using the Panel Server webpages. Choose a time zone from the list available. If no local time zone is set, the Panel Server uses UTC for time stamping functions.

The local time zone is used for the following functions:

- For data displayed on:
  - **Monitoring & control**
  - **Home** (Advanced model)
  - **Trending** (Advanced model)
- In emails for alarms (Advanced model)
- For data published to an SFTP or HTTPS server
- For data exported in a local file

UTC is used for the following functions:

- To publish data to cloud applications
- For logging data
- For all functions using a timestamp if local time zone is not set

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

The date and time function is set as follows:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- On the Panel Server webpages, at **Settings > General > Date and time**

General Settings

The following table describes the settings available from the webpages.

Parameter	Description
Synchronization mode	Used to select the date and time configuration mode of the Panel Server: • Select **Schneider Electric Cloud** (default setting) to synchronize the date and time automatically with an NTP server hosted by Schneider Electric cloud services, page 123. • Select **NTP** to synchronize the date and time automatically with an external NTP server. • Select **Manual** to set the date and time manually in the dedicated fields. **NOTE**: Manual date and time settings are available only if the Panel Server is not set up for publication by Schneider Electric cloud services, or for publication by email. See Data Publication, page 122.
Time zone	Used to select your time zone from the list of time zones available (default setting: UTC). A search box opens when you click this field to allow you to search for a key word.
Status	Displayed when **Schneider Electric Cloud** is selected as synchronization mode A message indicates if you are successfully connected to the NTP server.

NTP Settings

The following parameters are displayed only when the parameter of date and time synchronization mode is set to **NTP**.

The following table describes the settings available from the webpages.

Parameter	Description
Status	Displayed when **NTP** is selected as synchronization mode A message indicates if you are successfully connected to the NTP server.
Mode	Used to select the synchronization mode: • Select **Static** to set NTP server address manually. • Select **DHCP** (default setting) to obtain date and time automatically from the NTP server that is specified by a DHCP server. **NOTE:** To use **DHCP** mode, the network settings must be set to **DHCP** (see related topic, page 96).
Polling interval (s)	Allows you to enter the polling interval to set how frequently (in seconds) the Panel Server requests updates from the time server. • 64 • 128 • 256 • 512 • 1024
Primary server address	Used to enter the primary NTP server address when the parameter **NTP settings > Mode** is set to **Static**. **NOTE:** When the parameter **Mode** is set to **DHCP**, the setting is not editable.
Secondary server address	Used to enter the secondary NTP server address when the parameter **NTP settings > Mode** is set to **Static**. **NOTE:** When the parameter **Mode** is set to **DHCP**, the setting is not editable.

Manual Date and Time Settings

- On the Panel Server webpages:

  The manual date and time settings are displayed only when **Synchronization mode** is set to **Manual**.

  The following table describes the settings available from the webpages.

Parameter	Description
Date and Time	Used to set the date and time by using date and time pickers.

- With EcoStruxure Power Commission software:

  Panel Server date and time can be set manually with EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34:

  - By manually setting the date and time in the dedicated fields.
  - By user-initiated synchronization with date and time of the PC running EcoStruxure Power Commission software.

Firmware Update

Presentation

Update the Panel Server to the latest version to:

- Obtain the latest features and fixes
- Keep up to date with security patches
- Allow the Schneider Electric Customer Care Center to remotely access the Panel Server webpages:
  - For firmware versions up to 002.007.000, the Schneider Electric Customer Care Center uses embedded remote access certificates. The certificates for each firmware version are valid up to the dates indicated in the table.

Panel Server firmware version	Remote access certificate validity date
002.008.000	Not applicable
002.007.000	15 June 2027
002.006.001	10 January 2027
002.006.000	10 January 2027

    IMPORTANT: After January 10, 2027, respectively June 15, 2027, the Customer Care Center will no longer be able to establish remote access to a Panel Server running firmware version 002.006.000 or 002.006.001, respectively 002.007.000, due to certificate expiration. To maintain remote access capability, customers must update to the latest firmware version.
  - To enable the Customer Care Center to establish remote access, customers must ensure that the firewall is configured properly. Refer to section *Enabling Schneider Electric Cloud Infrastructure* in DOCA0172•• *EcoStruxure Panel Server - User Guide*, page 10.

Use the Panel Server webpages or EcoStruxure System Management to update your product to the latest available version.

All firmware designed for the Panel Server is signed using the Schneider Electric public key infrastructure (PKI) to provide integrity and authenticity of the firmware running on the Panel Server. Before installation, the Panel Server verifies the digital signature of the firmware.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Checking the Firmware Version

The currently running Panel Server firmware version can be checked:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- On the Panel Server webpages at:
  - **Settings > General**
  - **Maintenance > Firmware Update**

Maintenance > Firmware Update > Last security patch indicates the last installed firmware version which contained a security patch. It is not possible to

downgrade the Panel Server to a previous firmware version if the current firmware version contains a security patch.

Firmware Compatibility

- On the Panel Server webpages at **Maintenance > Firmware Update > Retrieve the appropriate firmware** you can automatically retrieve and download the latest firmware version compatible with the model and hardware version of the connected Panel Server.
- In the **Information** menu of EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34, you can find the device firmware baseline for all communicating devices in the switchboard to check compatibility of firmware versions.

  When selecting the firmware to install, take into consideration the following criteria and select the corresponding firmware:

  - EcoStruxure Panel Server model, Entry, Universal, Universal Wired by Design, or Advanced.
  - The hardware version, 001.000.000 or 002.000.000. To check the hardware version, refer to the specific topic, page 26.

    NOTE: If you try to install a firmware version that is not compatible with your EcoStruxure Panel Server model and hardware, an error message is displayed and the installation is aborted.

Updating the Firmware

IMPORTANT: It is recommended to back up the Panel Server configuration (see detailed topic, page 180), before launching a firmware update.

To update Panel Server firmware, use the Panel Server webpages.

For more information about updating Panel Server firmware, refer to the respective release notes, page 10:

- DOCA0249•• *EcoStruxure Panel Server Entry - Firmware Release Notes*
- DOCA0178•• *EcoStruxure Panel Server Universal - Firmware Release Notes*
- DOCA0248•• *EcoStruxure Panel Server Advanced - Firmware Release Notes*

NOTE: Mass firmware update can be done by using EcoStruxure System Management (ESM), page 38.

User Management Using Panel Server Webpages

Presentation

User account management in systems with a single Panel Server gateway or a limited number of Panel Server gateways, can be performed through the Panel Server webpages. A default security policy is enforced in the Panel Server.

Panel Server supports the following users:

- Administrators with **SECADM** role:
  - Including the default administrator account named **SecurityAdmin**.
  - Can change their password on the Panel Server webpages, subject to the password requirements, page 53.
  - Can create, modify, and delete users with **VIEWER** or **SECADM** role.
  - Can delete any user (with **VIEWER** or **SECADM** role), except the **SecurityAdmin** user.
  - Have administrator rights such as reading and changing the product configuration, adding, configuring, or removing devices, and accessing system logs.
- Users with **VIEWER** role:
  - Can access the Panel Server webpages in read-only mode.
  - Are not authorized to modify Panel Server configuration settings or execute commands on the Panel Server webpages.
  - Can change their password on the Panel Server webpages, subject to the password requirements, page 53.

  NOTE: To help ensure system performance and user experience, it is recommended to limit the number of user accounts to 50.

To help ensure system security, see Recommended Actions for Cybersecurity, page 184.

In case of a large number of Panel Server gateways installed in a system, user management can be performed through the EcoStruxure Cybersecurity Admin Expert (CAE) software. For more information, refer to the specific topic, page 55.

IMPORTANT: When the configuration is deployed from CAE software to the Panel Server gateway(s) connected in the system, all Panel Server-supported parameters managed by CAE software overwrite the corresponding parameters on the Panel Server, including users and passwords.

IMPORTANT: When performing a backup of the Panel Server configuration, user accounts are not saved in the backup file (see detailed topic, page 180).

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

User account management settings are configured on the Panel Server webpages, at **User Management**.

Creating User Account Names

When creating or modifying a user name on the Panel Server webpages, special characters are limited to the following: !"#$%&'()*+-./;<=>?@[\]^_`

Changing the SecurityAdmin Password

The administrator named **SecurityAdmin** (default user account) must enter the default password **AAAAAAAA** in the following cases:

- At first login to Panel Server.
- After a factory reset, page 190.

Then the administrator is required to set a new password by complying with the password requirements, page 53.

Changing the User Account Password

⚠CAUTION

UNAUTHENTICATED, UNAUTHORIZED ACCESS

The users are responsible to change their password frequently.

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

The user account password can be changed as follows:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- On any page of Panel Server webpages.
  1. Click the arrow next to the user account name in the header.
  2. Select **Change password** from the drop-down list.
  3. Enter the old password.
  4. Enter the new password.
  5. Confirm the new password.
  6. Click **Apply**.

Password Requirements

The EcoStruxure Panel Server enforces a default password policy which applies to all users, regardless of their role.

The user account password must conform to the following rules:

- Between 8 and 50 characters
- Must contain at least three of the following types of character:
  - Uppercase letters (A-Z)
  - Lowercase letters (a-z)
  - Digits (0-9)
  - Special characters among !"#$%&'()*+,-./:;<=>?@[\]^_`

Password Lockout

After 5 invalid login attempts to the EcoStruxure Panel Server within a three-minute period, the user account is locked out.

NOTE: The counter of login attempts is reset every 3 minutes.

When the user account is locked, the user must wait 10 minutes before being able to log in again.

NOTE: User account lock state remains in case of reboot, including reboot after power loss.

User Management Using EcoStruxure Cybersecurity Admin Expert

Presentation

EcoStruxure Cybersecurity Admin Expert (CAE) is an optional software-based tool which can be used for security configuration of systems with Panel Server gateways. For detailed information, see the CAE user guide (EcoStruxure Cybersecurity Admin Expert User Guide, page 10).

CAE software provides enhanced centralized user management capabilities through security policy and user account management, compared to the Panel Server webpages (see related topic, page 52).

IMPORTANT: When the configuration is deployed from CAE software to the Panel Server gateway(s) connected in the system, all Panel Server-supported parameters managed by CAE software overwrite the corresponding parameters on the Panel Server, including users and passwords.

CAE software supports the following users:

- Security administrators with **SECADM** role with the following rights in CAE software:
  - Define the Panel Server security policy.
  - Can create, modify, and delete users with **VIEWER** role or **SECADM** role, but at least one user with the **SECADM** role must remain.
  - Can deploy security configuration to multiple Panel Server gateways.
- Users with **VIEWER** role with the following rights once the configuration has been deployed from CAE software to the Panel Server:
  - Can access the Panel Server webpages in read-only mode.
  - Are not authorized to modify Panel Server configuration settings or execute commands on the Panel Server webpages.
  - Can change their password on the Panel Server webpages.

    IMPORTANT: Password changes made locally on the Panel Server webpages are not synchronized with CAE software.

NOTE: To help ensure consistent security management, it is recommended to configure security settings only in CAE software. Avoid modifying security settings through the Panel Server webpages, as the same parameters can be configured in both interfaces: settings and user accounts will be overwritten if a new configuration is deployed from CAE software.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

The Panel Server security parameters can be set in CAE software.

CAE-configurable Parameters

The table shows the CAE-configurable parameters supported by Panel Server and the corresponding parameters available in the Panel Server.

IMPORTANT: Once the CAE configuration is deployed to the Panel Server, the corresponding Panel Server settings are overwritten with the CAE-configured values, including the user accounts.

Parameter		Settings in CAE software	Local Panel Server settings
Security policy	Password complexity	• **None** (default setting) • **IEEEStd1686** • **NERC** • **Custom** (not supported by Panel Server; when deployed, the Panel Server default security policy IEEEStd1686 will apply.)	**IEEEStd1686**. Setting not editable.
	Minimum inactivity period (user session timeout)	Setting editable (default setting: 15 minutes).	60 minutes. Setting not editable.
	Allow user account locking	Enabled (default setting) or disabled.	Enabled. Setting not editable.
	Maximum login attempts	Setting editable (default setting: 5 attempts).	5 attempts. Setting not editable.
	Password attempts timer	Setting editable (default setting: 3 minutes).	3 minutes. Setting not editable.
	User account locking duration	Setting editable (default setting: 240 seconds).	600 seconds. Setting not editable.
User accounts		Editable fields: • User first name and last name (not used in Panel Server) • Login user name and password • Role(s) (**SECADM** or **VIEWER**)	Editable fields: • Login user name and password • Role(s) (**SECADM** or **VIEWER**) Default account: **SecurityAdmin** with **SECADM** role
Syslog configuration	Security Logs	• BDEW • E3 • NERC_CIP • IEEE1668 • IEC62351 • CS_PH1 • CS_PH2	–
	Server address	Editable field.	–
	Server port	Editable field.	–
	Transport type	• **TCP** (Transmission Control Protocol) (default setting) • **UDP** (User Datagram Protocol) (not supported by Panel Server; when deployed, security logs will not be forwarded to the Syslog server.)	–
	Enable security	Enabled or disabled.	–

Managing a Project in CAE Software

CAE software allows you to create and manage projects that centralize and store security policy, user accounts, security log settings, and the list of managed Panel Server gateways. For detailed information about *Projects management*, see the CAE user guide (EcoStruxure Cybersecurity Admin Expert User Guide, page 10).

Follow this procedure to manage a CAE project with a Panel Server gateway:

1. Connect to CAE software with sufficient privileges.
2. Create a project in CAE software.
3. Configure the security policy of user accounts at **SECURITY SETTINGS > User Accounts** and **Login Parameters**.
4. Configure the user accounts at **USER ACCOUNTS**.
5. Configure the security logs (Syslog configuration), if required (see related topic, page 179).

6. Save the project.

Security Policy

In CAE software, users with **SECADM** role can configure the Panel Server security policy at **SECURITY SETTINGS > User Accounts**.

NOTE: From a cybersecurity perspective, CAE software also enables the configuration of security logs, page 179.

Password Parameters Settings

Parameter	Description
Password complexity	Defines the rules that the passwords must satisfy in order to be accepted by the Panel Server: • **None** (default setting) • **IEEEStd1686** • **NERC** **IMPORTANT: Custom** is not supported by Panel Server. If **Custom** is configured in CAE software, it will not be deployed to the Panel Server and the Panel Server default security policy will apply.

Login Parameters Settings

Parameter	Description
Minimum inactivity period (min)	Defines the session timeout after which the user session in the Panel Server webpages is terminated (default setting: 15 minutes). The user must re-enter their password to extend the session.
Allow user account locking	Used to enable/disable user account locking (enabled by default).
Maximum Login attempts	Defines the maximum number of failed login attempts allowed, before the account is locked (default setting: 5). Must be greater than or equal to **2**. **IMPORTANT:** If this instruction is not followed, the configuration cannot be deployed from CAE software to Panel Server. The Panel Server must then be reset to factory settings.
Password attempts timer (min)	Time after which the login attempt counter resets (default setting: 3 minutes). Is available only if **Allow user account locking** is enabled.
User account locking duration (s)	Defines how long the account remains locked (default setting: 240 seconds). Is available only if **Allow user account locking** is enabled.

Managing User Accounts

In CAE software, user accounts are configured at **USER ACCOUNTS**.

IMPORTANT: To enable users to log in to the Panel Server webpages, user names created in CAE software or directly on the Panel Server must comply with the following rules:

- 4 to 16 characters
- Contain only alphanumeric characters (A-Z, a-z, and 0-9) and the following special characters: !"#$%&'()*+-./;<=>?@[\]^_`
- Not contain any spaces
- Be unique

The password of the CAE administrator may be different to the password used to access the Panel Server webpages. Therefore, once the security configuration has been deployed from CAE software to the Panel Server, the Panel Server security administrator must enter the password configured in CAE software.

Deploying Security Configuration

NOTE: It is recommended to perform a backup of the Panel Server configuration before deploying the security configuration from CAE software. For information about the backup file contents, see Backup and Restore Panel Server Configuration, page 180.

The pre-requisites for deploying the configuration include the following actions:

- Connect to CAE software with sufficient privileges.
- Create a project, that will contain the security configuration to be deployed to Panel Server. See related topic, page 56.
- Configure the Syslog server, if required, at **SECURITY SETTINGS > Logs and Monitoring > SYSLOG Parameters**. See related topic, page 179.
- Upload the Syslog server certificate in CAE software, if required for your configuration. See EcoStruxure Cybersecurity Admin Expert User Guide, page 10.
- Enable DPWS at **SECURITY SETTINGS**. It is required for discovery of the Panel Server gateways in the system.
- Discover each Panel Server at **MANAGEMENT OF SYSTEM**.

Follow this procedure to deploy the configuration from CAE software to one or several Panel Server gateways:

1. Connect to CAE software with sufficient privileges.
2. Open the project previously created.
3. At **MANAGEMENT OF SYSTEM**, trust the Panel Server by right-clicking and selecting **Trust Selected Devices**.
4. Send the CAE signing certificate to the Panel Server certificate store.
5. Send the security configuration to the Panel Server.

Result:

- In the Panel Server webpages, the date of the last configuration deployed from CAE software is displayed at **User management > CAE configuration**.
- When the configuration is deployed from CAE software to the Panel Server gateway(s) connected in the system, all Panel Server-supported parameters managed by CAE software overwrite the corresponding parameters on the Panel Server, including users and passwords. Refer to the list of parameters, page 55.

EcoStruxure Panel Server Communication Functions

What’s in This Part

Modbus Gateway Function 60
Examples of Modbus Routing 65
Communication Architectures 71
Network Communication 77
TCP/IP Communication 92
Modbus-SL Communication (Models with One Modbus-SL Port) 101
Wireless Communication 106

Modbus Gateway Function

Presentation

The Panel Server implements a Modbus gateway function. It can serve requests received from the Modbus TCP/IP clients connected upstream so that each client can access data simultaneously from downstream devices, connected through:

- IEEE 802.15.4 wireless network (depending on the model)
- or Modbus-SL wired network (Universal and Advanced models)

The maximum number of downstream Modbus TCP/IP devices connected to one Panel Server is 128 and includes devices physically connected to the Panel Server and any type of device connected to a child gateway. For more information, see *Maximum Configuration*, page 20.

The Modbus protocol exchanges information using a request-reply mechanism between a client (formerly *master*) and a server (formerly *slave*). The client-server principle is a model for a communication protocol in which one device (the client) controls one or more other devices (the servers). Modbus client ID was formerly known as *Master* and Modbus server ID was formerly known as *Slave*.

Availability

This function is available on Panel Server Universal and Advanced.

Modbus Gateway Functioning

The Panel Server implements its own Modbus registers that are available at unit ID 255, to provide its own identification information. The register table of the Panel Server is described in DOCA0241EN *EcoStruxure Panel Server - Modbus File*.

By default, out-of-the-box, the Modbus gateway uses the unit ID in the Modbus TCP/IP request as unit ID / Server ID of the physical Modbus-SL device.

For Modbus TCP/IP devices, when carrying out commissioning, a virtual server ID is added to a Modbus TCP/IP device to allow access in case of separate topology or to enable the Modbus TCP proxy feature.

The Panel Server implements a set of virtual Modbus register tables per discovered IEEE 802.15.4 wireless device. Each time a new wireless device is discovered by the Panel Server, the device is automatically assigned a virtual Modbus server ID. The first discovered wireless device is assigned virtual server ID 100. Each subsequent wireless device takes the next virtual ID, which gets automatically incremented by one each time a new device is discovered. For detailed information about the registers of supported wireless devices, refer to DOCA0241EN *EcoStruxure Panel Server - Modbus File*.

To avoid conflicts between the server IDs of the physical Modbus-SL devices and the virtual server IDs of the wireless devices, it is possible to update the virtual server ID through one of the following:

- EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- The Panel Server webpages (select **Settings > Wireless devices** then choose one connected device and change value in **Modbus virtual > Virtual server ID**).

  NOTE: The Modbus gateway function should not be confused with a network gateway or a router. The Panel Server does no routing and no forwarding at the network (IP) layer.

Modbus Transparent Gateway

The Panel Server can also act as a transparent Modbus-SL to Modbus TCP/IP gateway. It converts Modbus TCP/IP client requests received on unit ID X to Modbus-SL or Modbus TCP/IP requests sent on server ID X. Responses obtained from the downstream devices are then forwarded upstream to the Modbus TCP/IP client.

When used as a transparent gateway, the client (for example, SCADA) is connected via a Modbus TCP/IP connection. Any Modbus-SL settings for that connection are not taken into account, except the message timeout setting, page 279. The following table lists the function codes that are passed on by the Panel Server acting as a transparent gateway:

Function code type	Function code	Description
Modbus function codes	01	Read coils
	02	Read discrete inputs
	03	Read holding registers
	04	Read input registers
	05	Write single coil
	06	Write single register
	07	Read exception status
	15	Write multiple coils
	16	Read multiple registers
	17	Report server ID
	22	Mask write register
	23	Write and read registers
Extended function codes	08	Diagnostics
	11	Get com event counter
	12	Get com event log
	20	Read file record
	21	Write file record
	24	Read FIFO queue
	43	Read device identification
	100	Scattered read

When using the Panel Server as a transparent gateway, you can discover downstream devices for test purposes (for example, checking connected status). After checking the connection, remove the downstream devices from the list of connected devices in the Panel Server webpages to maintain optimal communication between upstream edge systems and downstream devices.

Definitions of Modbus Unit ID / Server ID and Virtual Server ID

To enable an external Modbus TCP/IP client to access a device connected to the Panel Server, each device must have a unique ID named *virtual server ID*.

The *virtual server ID* is automatically assigned:

- when a wireless device is connected to the Panel Server.
- whenever a Modbus device is created and associated to a device Unit ID / Server ID.

The *unit ID / server ID* is either:

- the configured unit ID of any device connected to the RS485 serial port,
- the configured unit ID of a connected Modbus TCP/IP device, or
- the unit ID used by a Modbus TCP/IP gateway that connects a device to an Ethernet network.

The Panel Server uses the following rules to assign the *virtual server ID* when a downstream device is discovered or added:

- For Modbus-SL devices, if the physical server ID / unit ID (also known as the Modbus address) is not already used as a virtual server ID by another device, it will be assigned as the virtual server ID. If not, then, the first available virtual server ID in the range 1–254 will be assigned starting from virtual server ID 1.
- For wireless devices, the first available virtual server ID in the range 1–254 will be given starting from virtual server ID 100.
- For Modbus TCP/IP devices, the first available virtual server ID in the range 1–254 will be given starting from virtual server ID 200.

  IMPORTANT: It is recommended to set the Modbus physical address of Modbus-SL devices in the range 1–99.

Following this recommendation, in most configurations with less than 100 Modbus-SL devices, less than 100 wireless devices, and less than 48 Modbus TCP/IP devices, the virtual server ID will automatically be given as follows:

- Modbus-SL devices will have their physical server ID assigned as virtual server ID in the range 1–99.
- Virtual server ID of wireless devices will be in the range 100–199.
- Virtual server ID of Modbus TCP/IP devices will be in the range 200–254.

The virtual server ID can be changed using EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34, or on the Panel Server webpages (see **Modbus Discovery** settings, page 104). The virtual server ID must be unique.

EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34, and the Panel Server webpages provide the following information for each device (see addition of Modbus devices, page 228):

- Virtual server ID
- Connection:
  - Unit ID / server ID for Modbus-SL devices
  - IP address for remote devices and unit ID / server ID for Modbus TCP/IP devices
  - RFID for wireless devices
- Device type as defined in the device settings

For information about how to manage virtual server ID conflict, see Example of Modbus Server ID Conflict and Resolution, page 63.

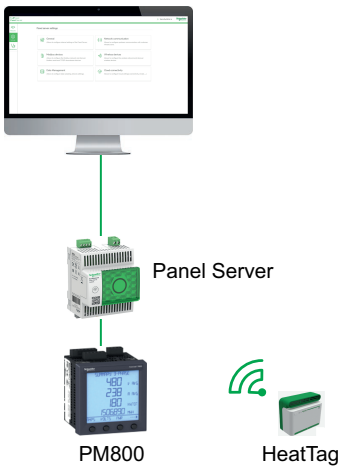
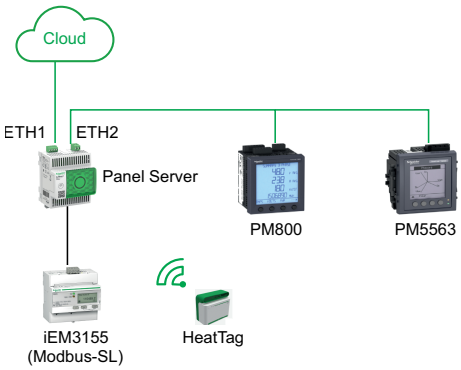
For examples of how to use virtual server ID to access data in downstream devices according to the communication architecture, refer to Examples of Modbus Routing, page 65.

Modbus TCP/IP Service Activation

To help reinforce security of data access and avoid malicious access to device data from an upstream connection, Modbus TCP/IP server can be enabled/disabled per interface (ETH1 port/ETH2 port/Wi-Fi, depending on the model and the mode configuration) on the Panel Server webpages at **Settings > Network communication > Services > Communication services activation**, page 221.

Do not disable Modbus service on port ETH1, ETH2, or Wi-Fi if the interface is used to connect EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34, or a monitoring software such as SCADA.

Examples of typical cases of architectures for which Modbus TCP/IP service is disabled for the upstream connection:

Architecture	Modbus TCP/IP service configuration
Panel Server connected to Panel Server webpages, Modbus devices and wireless devices 	To allow access only to the upstream application (such as a web browser), it is recommended to disable Modbus service on Ethernet ports and Wi-Fi. This avoids malicious access to the downstream devices.
Panel Server connected to the cloud and in the separated mode to Modbus and wireless devices 	When the Ethernet network is configured in the separated mode, it is recommended to: • Disable Modbus service on Panel Server ETH1 port to avoid malicious access to data of the downstream devices. • Enable Modbus service on Panel Server ETH2 port to allow data acquisition from the downstream devices only if you need to connect a Modbus TCP/IP client on ETH2 through EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.

Modbus Server ID Conflict and Resolution

With the above discovery and addition mechanism, the Panel Server will always assign an available and unique virtual server to every device.

However, it is possible to assign the same virtual server ID to two devices when carrying out commissioning.

To resolve this situation, update the virtual server ID in one of the two devices to an available server ID.

Example of Modbus Server ID Conflict and Resolution

In the following example, Panel Server is used as a gateway with the following devices installed in the switchboard:

- One PM3250 Power Meter communicating through Modbus-SL, and configured with server ID 100
- One PowerTag Energy

Consider the following sequence that will generate a conflict and see how to resolve it:

1. Connect the PM3250 Power Meter configured with server ID 100 to the RS485 Modbus communication port on Panel Server.
2. Power up the Panel Server.
3. From the monitoring tool connected upstream, you can access the Modbus registers of PM3250 by sending Modbus TCP/IP requests to unit ID 100 of the Panel Server Modbus server.
4. From EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34, discover the Panel Server and access the Panel Server homepage without performing a Modbus-SL device discovery. From the wireless device discovery card, launch a wireless device discovery for the first time. The PowerTag Energy sensor is then discovered and added to Panel Server.

   Result: The PowerTag Energy sensor is automatically assigned a virtual server ID equal to 100. Because it is the same ID as for PM3250, there is a conflict.
5. If you send Modbus TCP/IP requests to unit ID 100 of the Panel Server Modbus server:
   - The virtual registers of the PowerTag Energy will be available.
   - You will no longer be able to send requests to the PM3250 Power Meter.
   - The PM3250 Power Meter is now masked by the virtual device.
6. To resolve this situation, you need to update the virtual server ID to any value you choose, except 100. This can be performed from the wireless device configuration by using EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.

Modbus TCP/IP Proxy

The Panel Server can act as a Modbus TCP proxy for a Modbus TCP/IP device connected to the Panel Server. This function can be used to connect several devices simultaneously to a TCP/IP device offering a single TCP/IP connection.

With this function, the upstream communication system establishes as many TCP/IP connections as required by the Panel Server. This is done by using the virtual server ID of the Modbus TCP/IP device managed by the Panel Server. The Panel Server establishes a single connection to the downstream Modbus TCP/IP device.

For more information about Modbus routing and assignment of virtual Modbus server IDs, see Examples of Modbus Routing, page 65.

Examples of Modbus Routing

Presentation

This topic presents examples to illustrate how an upstream SCADA using Modbus TCP/IP accesses the devices connected to a Panel Server depending on the communication architecture using the Modbus virtual server ID. For detailed information about *Modbus unit ID / server ID* and *virtual server ID*, see definitions, page 62.

NOTE: Modbus routing should not be confused with network routing at the network (IP) layer.

Recommendations for Virtual Server ID Mapping

To help ensure consistency of device data being communicated to upstream system, follow these rules for virtual server ID mapping:

- 1–99 for Modbus-SL devices (Universal and Advanced models)
- 100–199 for wireless devices
- 200–254 for Modbus TCP/IP devices (Universal and Advanced models)

Example of Modbus TCP/IP Requests for Wireless Devices

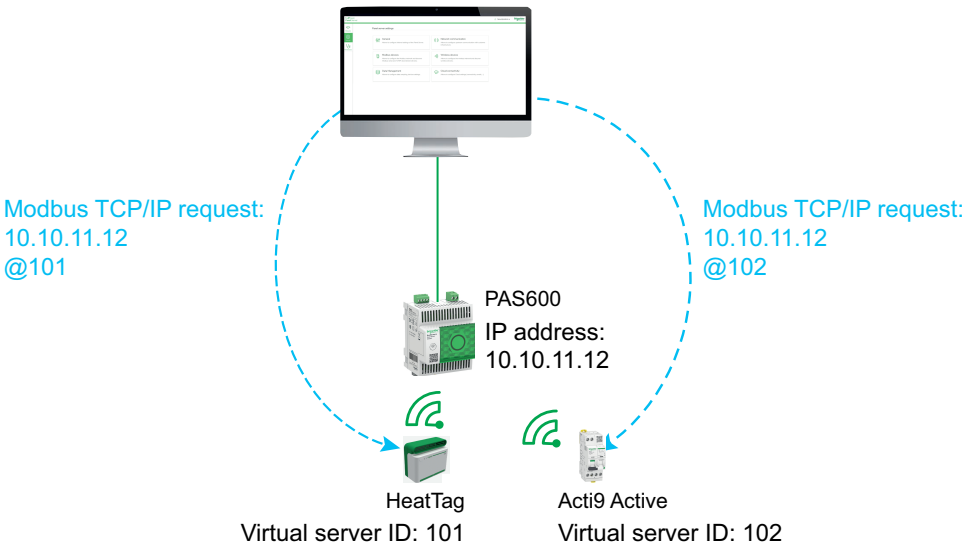
This example presents the Modbus TCP/IP requests for wireless devices. The example applies to all models of Panel Server except Wired by Design models.

Panel Server with IP address `10.10.11.12` is connected to:

- a HeatTag configured with virtual server ID `101`, and
- an Acti9 Active configured with virtual server ID `102`.

To collect and gather data from the wireless devices, the monitoring system will issue the following Modbus TCP/IP requests:

- `10.10.11.12`, address `101` for HeatTag
- `10.10.11.12`, address `102` for Acti9 Active



Example of Modbus TCP/IP Requests for Modbus-SL Devices

This example applies to Universal and Advanced models.

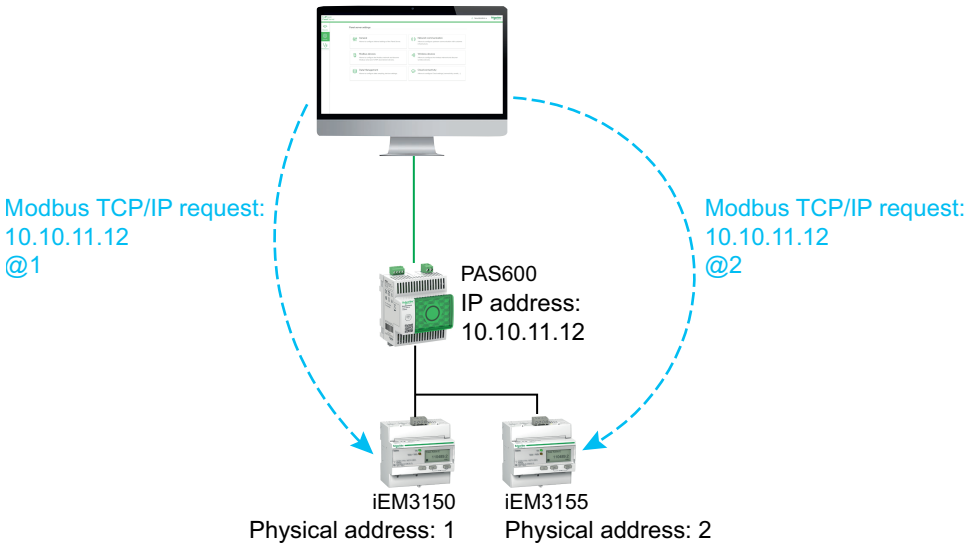
This example presents the Modbus TCP/IP requests for Modbus-SL devices when the serial physical address is used as virtual server ID.

Panel Server with IP address `10.10.11.12` is connected to:

- an iEM3150 energy meter with physical address `1`, and
- an iEM3155 energy meter with physical address `2`.

To collect and gather data from the Modbus RS485 devices, the monitoring system will issue the following Modbus TCP/IP requests:

- `10.10.11.12`, address `1` for iEM3150
- `10.10.11.12`, address `2` for iEM3155



Example of Modbus TCP/IP Requests for Modbus-SL Devices With Virtual Server ID Different from the Physical Address

This example applies to Universal and Advanced models.

A virtual server ID which is different from the physical address can be used in the following cases:

- The physical address is already used as a virtual server ID for a different device (either a wireless, Modbus-SL, or Modbus TCP/IP device).
- This use case helps to apply a dedicated communication address plan for easier and consistent integration in the upstream system.

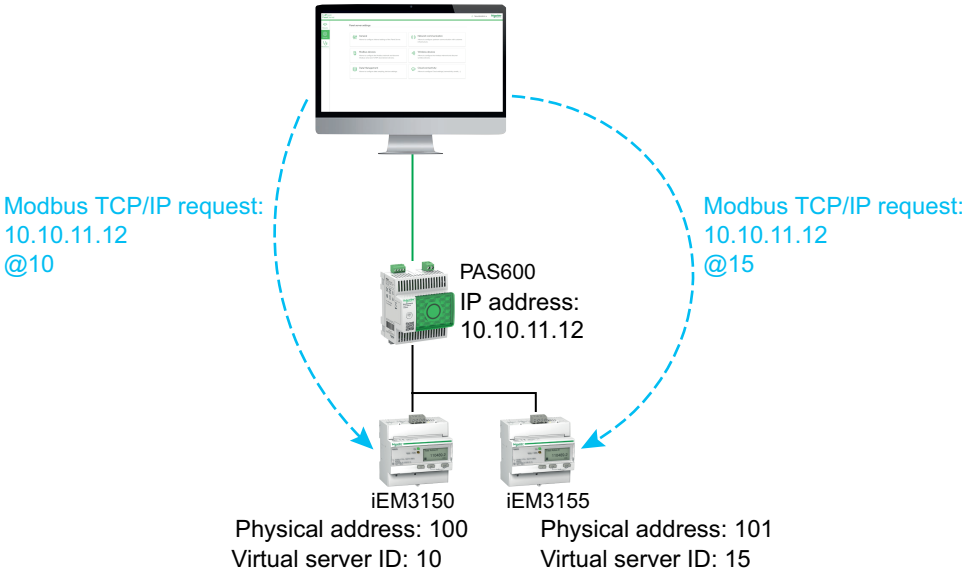
This example presents the Modbus TCP/IP requests when the virtual server ID of Modbus-SL devices is different from the serial physical address.

Panel Server with IP address `10.10.11.12` and virtual server ID `15` is connected to:

- an iEM3150 energy meter with physical address `100` and virtual server ID `10`, and
- an iEM3155 energy meter with physical address `101` and virtual server ID `15`.

To collect and gather data from the Modbus devices, the monitoring system will issue the following Modbus TCP/IP requests:

- `10.10.11.12`, address `10` for iEM3150
- `10.10.11.12`, address `15` for iEM3155



Example of Modbus TCP/IP Requests for Devices in Separate Topology

This example applies to Universal and Advanced models.

This example presents the Modbus TCP/IP requests for devices in a separate topology.

Panel Server with

- IP address on ETH1 port: `10.10.10.10`
- IP address on ETH2 port: `192.168.10.1`

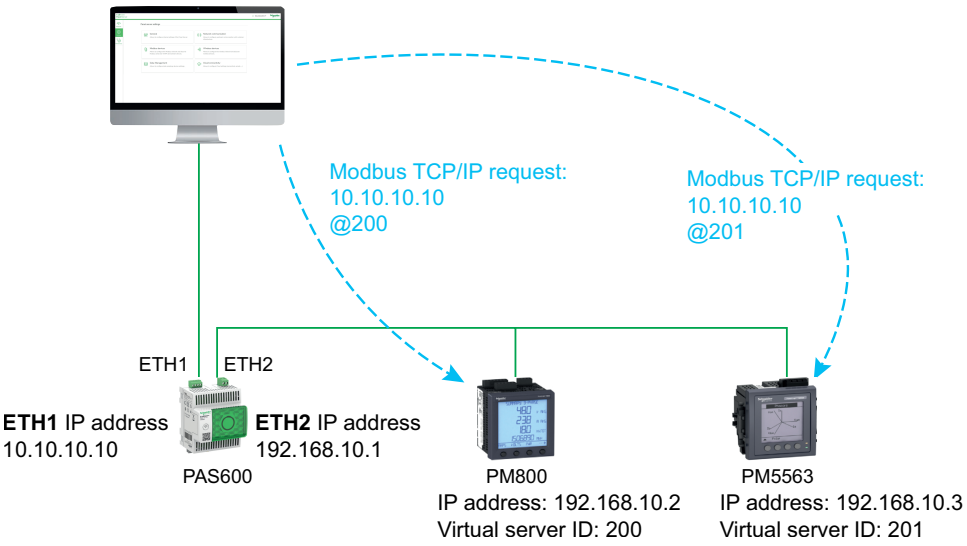
is connected to:

- a PM800 power meter with IP address `192.168.10.2` and virtual server ID `200`, and
- a PM5563 power meter with IP address `192.168.10.3` and virtual server ID `201`

To collect and gather data from the Ethernet devices, the monitoring system will issue the following Modbus TCP/IP requests:

- `10.10.10.10`, address `200` for PM800
- `10.10.10.10`, address `201` for PM5563

Modbus service is to be enabled on ETH1.



Example of Modbus TCP/IP Requests for Devices in Switched Topology

This example applies to Universal and Advanced models.

This solution offers multiple Modbus TCP client connections. If a device supports only one Modbus TCP/IP client, the Panel Server acts as a Modbus TCP/IP proxy and can support several upstream connections.

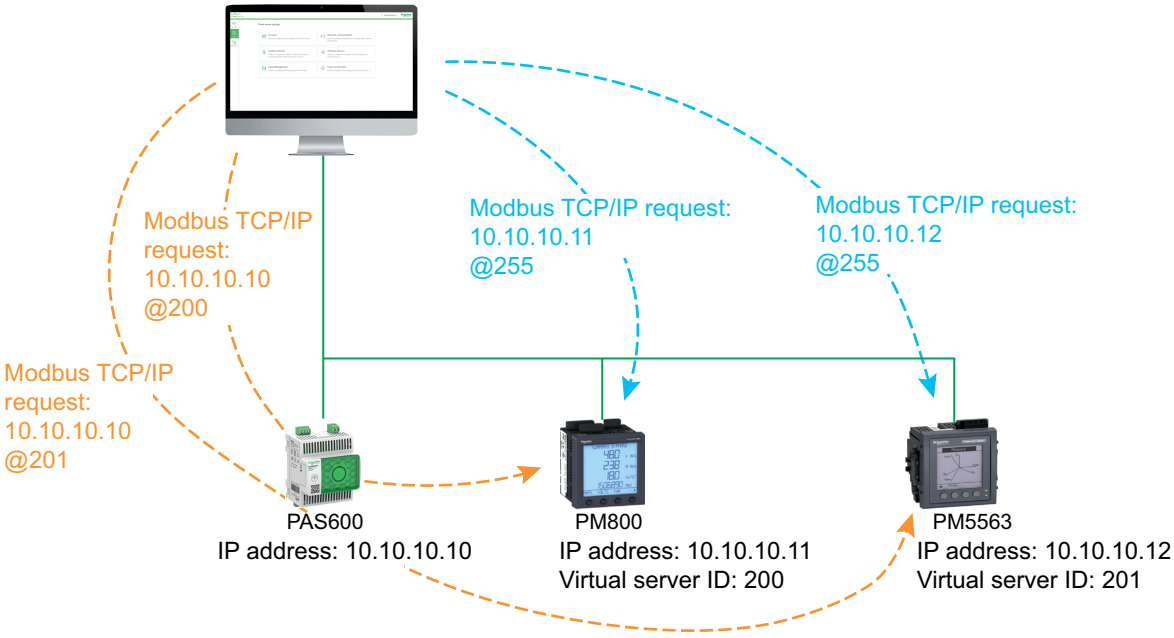
This example presents the Modbus TCP requests for devices in a switched topology.

Panel Server with IP address `10.10.10.10` is connected to:

- a PM800 power meter with IP address `10.10.10.11` and virtual server ID `200`, and
- a PM5563 power meter with IP address `10.10.10.12` and virtual server ID `201`.

To collect and gather data from the Ethernet devices, the monitoring system will issue the following Modbus TCP/IP requests in one of the following ways:

- Requests are issued directly to the downstream device:
  - `10.10.10.11`, address `255` for PM800
  - `10.10.10.12`, address `255` for PM5563
- or requests are issued through the Panel Server and the Modbus device discovery uses the virtual server ID:
  - `10.10.10.10`, address `200` for PM800
  - `10.10.10.10`, address `201` for PM5563



Example of Modbus TCP/IP Requests for Modbus-SL Devices under a Child Panel Server in Separate Topology

This example applies to Universal and Advanced models.

This example presents the Modbus TCP/IP requests for Modbus-SL devices when they are connected to a child/downstream Panel Server in a separate topology: the child/downstream Panel Server (PAS#2) is connected to one Ethernet port on the parent/upstream Panel Server (PAS#1).

For information on how to discover Modbus-SL devices connected to a child/downstream Panel Server by using Panel Server webpages, see detailed topic, page 230.

PAS#1 with

- IP address on ETH1 port: `10.10.10.10`
- IP address on ETH2 port: `192.168.10.10`

is connected to child PAS#2 with IP address `192.168.10.11` and connected to:

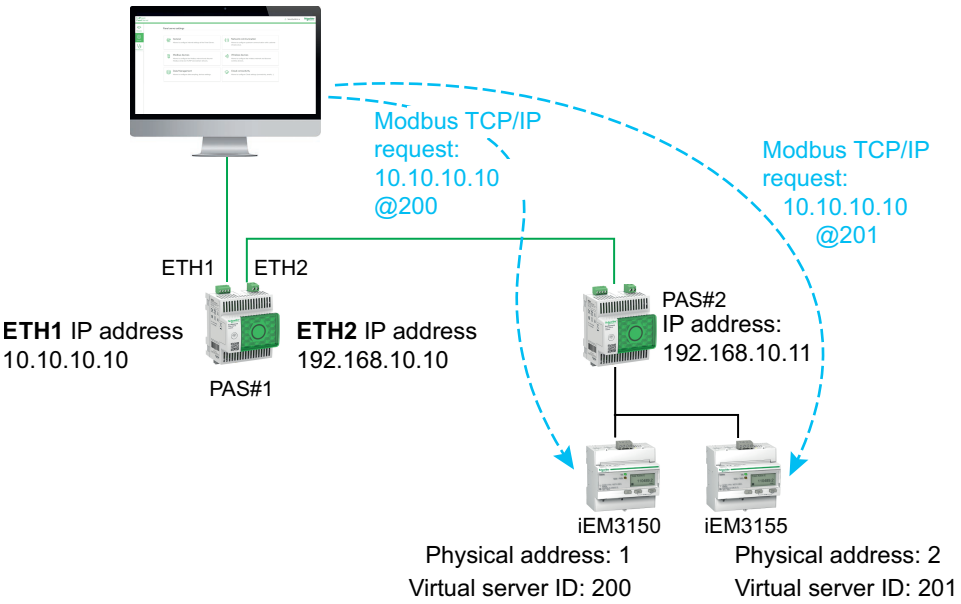
- an iEM3150 energy meter with physical address `1`, and
- an iEM3155 energy meter with physical address `2`.

To access the Modbus-SL devices under the child/downstream Panel Server (PAS#2) from the monitoring system, first the Modbus-SL devices must be manually added to the parent/upstream Panel Server (PAS#1) with the Panel Server webpages:

- Manual addition of iEM3150 to PAS#1 is done by using `192.168.10.11`, address `1`, assigned to virtual server ID `200`.
- Manual addition of iEM3155 to PAS#1 is done by using `192.168.10.11`, address `2`, assigned to virtual server ID `201`.

Then to collect and gather data from the Modbus devices, the monitoring system will issue the following Modbus TCP/IP requests:

- `10.10.10.10`, address `200` for iEM3150
- `10.10.10.10`, address `201` for iEM3155



Communication Architectures

Overview

Panel Server Universal and Advanced feature two Ethernet ports and Wi-Fi connection. The Panel Server Entry features one Ethernet port and Wi-Fi connection.

This topic presents several typical architectures that can be built with a Panel Server Entry, Universal or Advanced to highlight the use cases they serve.

For the network configuration settings, refer to Network Communication, page 77.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

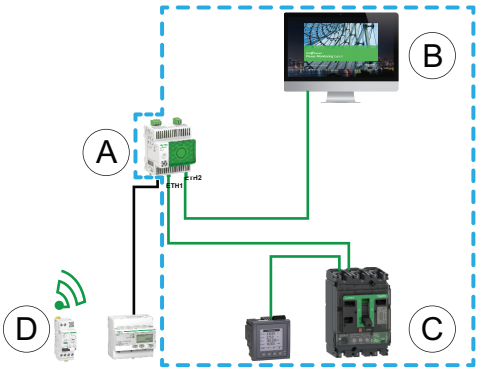
Switched Ethernet Network

When the Panel Server is configured in switched Ethernet mode, either ETH1 or ETH2 can be used for cloud connectivity and/or downstream device aggregation (single IP interface). Downstream devices connected to the same subnet as the Panel Server are reachable.

The following diagram illustrates a daisy-chain architecture with Ethernet port configuration in switched mode. Both Ethernet ports are connected together using the Panel Server internal Ethernet switch.

This architecture enables devices located upstream or downstream from the Panel Server to communicate together as part of the same network.

Switched Mode Configuration is available only for Universal and Advanced Models.



A. Panel Server
B. Edge monitoring and supervision software such as EcoStruxure Power Monitoring Expert or EcoStruxure Power Operation or EcoStruxure cloud services such as EcoStruxure Asset Advisor and EcoStruxure Resource Advisor
C. Wired devices
D. Wireless devices

IP communication area where **ETH1** and **ETH2** ports belong to the same IP network.

For more information about setting up upstream and downstream networks, refer to Network Connectivity, page 16.

To set up this architecture:

- Configure Ethernet network in the switched mode.
- Enable Modbus service on Panel Server Ethernet ports.

Separated Ethernet Network

This architecture is recommended for network security:

- This architecture keeps the Ethernet network segregated.
- No IP packet is forwarded between Panel Server ports ETH1 and ETH2.
- Modbus server can be enabled on Panel Server port ETH1 or ETH2.

The Panel Server supports direct connection to a PC on either of the Ethernet ports (ETH1 and ETH2). When connected, it is possible to ping and/or access the Panel Server webpages from a PC. Note that SSH connection is not supported.

When the Panel Server is configured in separated Ethernet mode, ETH1 is used as the upstream interface (default route passes through ETH1). ETH2 port is used for downstream device aggregation and only devices connected to the same subnet are reachable.

The Panel Server enables separate IP configuration (**IPv4**, **IPv6**, or **IPv4 & IPv6**) for each interface. Refer to Ethernet Communication, page 93.

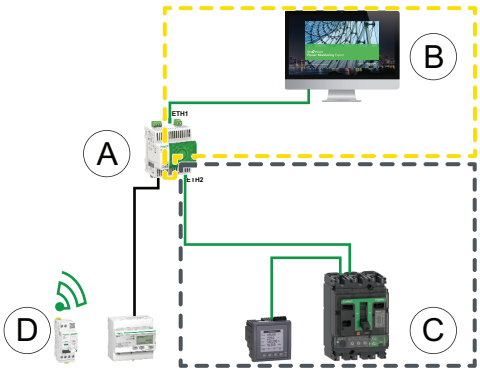
The following diagram illustrates an architecture with Ethernet port configuration in separated mode:

- In the case of cloud connection, this architecture allows you to avoid malicious access to the downstream devices (including Modbus TCP/IP devices connected on ETH2). Cloud connection is done through ETH1 port. Modbus TCP/IP server is disabled on ETH1 port.

  Modbus TCP/IP server on ETH2 port can also be disabled.
- In the case of edge software, this architecture allows you to separate electrical distribution devices from the IT network (LAN) and also allows you to have a single IP address to access the electrical distribution devices. Modbus TCP/IP client is enabled on ETH1 port to allow the edge software to access data within devices connected to ETH2 port.

  Modbus TCP/IP server on ETH2 port can be disabled.

Separated mode configuration is available only for Universal and Advanced Models.



A. Panel Server
B. Edge monitoring and supervision software such as EcoStruxure Power Monitoring Expert or EcoStruxure Power Operation or EcoStruxure cloud services such as EcoStruxure Asset Advisor and EcoStruxure Resource Advisor
C. Wired devices
D. Wireless devices

IP communication area accessible from **ETH1** port

IP communication area accessible from **ETH2** port

To set up this architecture:

- Configure Ethernet network in the separated mode.

- Disable Modbus service on ETH1 port if you want to block upstream software using Modbus TCP/IP to access Panel Server and downstream devices.

In this case, an edge software connected upstream will not have access to the Panel Server and the devices connected.

The Panel Server supports polling of serial devices connected downstream from two isolated Ethernet networks.

For more information about setting up upstream and downstream networks, refer to Network Connectivity, page 16.

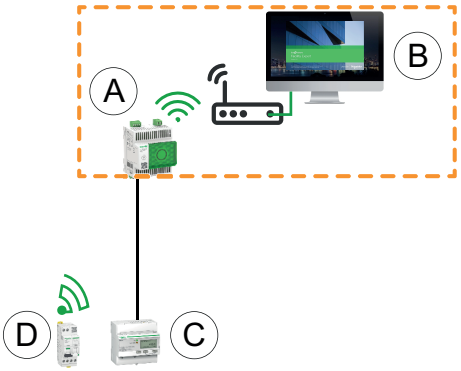
To set up this architecture:

- Configure Ethernet network in the separated mode.
- Enable Modbus service on ETH1 and ETH2 ports to allow upstream software using Modbus TCP/IP to access the Panel Server and downstream devices.

Wi-Fi Network

The following diagram illustrates an architecture with Wi-Fi only.

This architecture allows you to leverage Wi-Fi infrastructure network to avoid wiring a solid Ethernet cable. Depending on the upstream application (for example, SCADA or cloud), Modbus service on Wi-Fi interface can be disabled to avoid malicious access to downstream Modbus and wireless devices.



A. Panel Server
B. Edge monitoring and supervision software such as EcoStruxure Power Monitoring Expert or EcoStruxure Power Operation or EcoStruxure cloud services such as EcoStruxure Asset Advisor and EcoStruxure Resource Advisor
C. Wired devices
D. Wireless devices

IP communication area accessible from Wi-Fi interface

For more information about setting up upstream and downstream networks, refer to Network Connectivity, page 16.

To set up this architecture:

- Enable Wi-Fi.
- Disable Modbus service on Wi-Fi interface if you want to block upstream software using Modbus TCP/IP to access Panel Server and downstream devices.

Network with Wi-Fi and Switched Ethernet Network

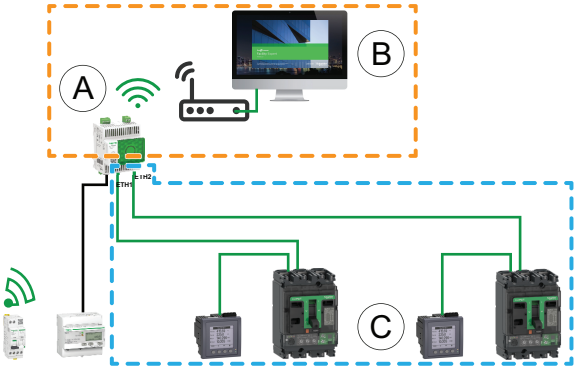
The following diagram illustrates an architecture with Wi-Fi upstream and Ethernet port configuration in switched mode downstream. There is one downstream Ethernet network. The Wi-Fi and Ethernet networks managed by the Panel Server are separated.

This architecture allows you to leverage Wi-Fi infrastructure network to avoid wiring a solid Ethernet cable. Depending on the upstream application (SCADA, cloud, or web browser), Modbus service can be disabled to avoid malicious access to Modbus and wireless devices.

If the upstream system is an edge control software using Modbus TCP/IP service, then Modbus service needs to be enabled on Wi-Fi. Modbus service can be disabled on ports ETH1 and ETH2.

If the upstream system is a web browser accessing the Panel Server webpages or a cloud application, then Modbus service can be disabled on Wi-Fi and on ports ETH1 and ETH2.

Switched mode configuration is available only for Universal and Advanced models.



A. Panel Server

B. Edge monitoring and supervision software (for example, EcoStruxure Power Monitoring Expert or EcoStruxure Power Operation) or EcoStruxure cloud services (for example, EcoStruxure Asset Advisor and EcoStruxure Resource Advisor)

C. Devices

IP communication area accessible from Wi-Fi interface

IP communication area accessible from ports **ETH1** and **ETH2**

For more information about setting up upstream and downstream networks, refer to Network Connectivity, page 16.

To set up this architecture:

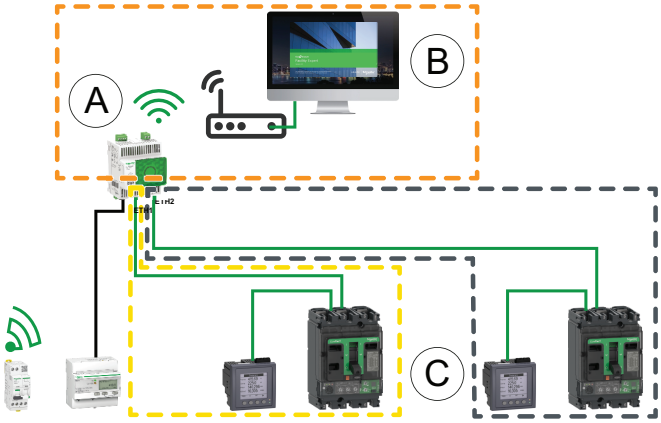
- Enable Wi-Fi network and configure settings, page 107.
- Configure Ethernet network in the switched mode, page 93.
- Use different IP addresses for the Wi-Fi network and the Ethernet network, to help ensure communication between the networks.
- Disable Modbus service on Wi-Fi interface if you want to block Wi-Fi access to Panel Server and downstream devices.

Network with Wi-Fi and Separated Ethernet Network

The following diagram illustrates an architecture with Wi-Fi upstream and Ethernet port configuration in separated mode downstream. There are two downstream Ethernet networks. The Wi-Fi and Ethernet networks managed by the Panel Server are always separated.

This architecture allows you to leverage Wi-Fi infrastructure network to avoid wiring a solid Ethernet cable. Depending on the upstream application (SCADA, cloud, or web browser), Modbus service can be disabled on a per interface basis (ETH1/ETH2/Wi-Fi) for optimized security.

Separated mode configuration is available only for Universal and Advanced models.



A. Panel Server

B. Edge monitoring and supervision software (for example, EcoStruxure Power Monitoring Expert or EcoStruxure Power Operation) or EcoStruxure cloud services (for example EcoStruxure Asset Advisor and EcoStruxure Resource Advisor)

C. Devices

IP communication area accessible from Wi-Fi interface

IP communication area accessible from **ETH1** port

IP communication area accessible from **ETH2** port

For more information about setting up upstream and downstream networks, refer to Network Connectivity, page 16.

To set up this architecture:

- Enable Wi-Fi network and configure settings, page 107.
- Configure Ethernet network in the separated mode, page 93.
- Use different IP addresses for the Wi-Fi network and the Ethernet network, to help ensure communication between the networks.
- Disable Modbus service on the one or several interfaces where Modbus TCP/IP server is not used if you want to help prevent malicious access to the Modbus devices through these interfaces.

  NOTE: This architecture is technically feasible but complex to set up, therefore the architecture with Wi-Fi and switched ETH1/ETH2 ports should be preferred.

Network Communication

What’s in This Chapter

Network Settings....78
DNS....80
RSTP....81
Proxy....84
Device Profile for Web Services (DPWS)....85
Wi-Fi Infrastructure....86
Wi-Fi Access Point....89

Network Settings

Overview

Panel Server features wired and wireless communication and enables network communication. The Panel Server offers the following connection interfaces:

- Ethernet:
  - One port on Entry model
  - Two ports on Universal and Advanced models
- Wi-Fi (except Wired by Design models)

Panel Server offers the capability to activate or deactivate IPv4 and IPv6 communication separately on each interface communication.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

The network configuration is set as follows:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- On the Panel Server webpages, at **Settings > Network communication**.

Select the appropriate network configuration for your system. Enter the parameters for each connection interface displayed.

For detailed information about network configuration option and settings, see:

- Single Ethernet Port Configuration (Entry Model), page 94
- Ethernet Switched Mode Configuration (Universal and Advanced Models), page 94
- Ethernet Separated Mode Configuration (Universal and Advanced Models), page 95
- Wi-Fi, page 107
- Modbus TCP/IP Client (Universal and Advanced Models), page 98
- Modbus TCP/IP Server, page 100

Network Configuration Settings

Network configuration settings are available on a single webpage under **Network > Network configuration**. It helps improve network management and reduce the risk of configuration errors by configuring the network topology (Ethernet mode and Wi-Fi infrastructure).

Depending on the selected network topology, the corresponding configuration parameters are displayed on the webpage allowing detailed configuration. Note that DNS settings are always displayed (for details, page 80).

The following table describes the settings available from the webpages.

Parameter	Description
Rapid Spanning Tree Protocol (RSTP)	Indicates whether the RSTP protocol is enabled or disabled (for details, page 81).
Ethernet mode	Used to select the Ethernet configuration mode (for details, page 93): • Select **Separated** to define two different IP addresses: one for each Panel Server Ethernet port. The separated mode enables to segregate downstream Modbus TCP/IP devices connected to ETH2 port, from upstream communication systems connected to ETH1 port. • Select **Switched** (default setting) to define one single unique IP address applied to both Ethernet ports ETH1 and ETH2.
ETH1 Ethernet port	Indicates whether an Ethernet cable is connected to the Panel Server ETH1 port (for details, page 93): • **Active** indicates that an Ethernet cable is connected to the port. • **Inactive** indicates that no Ethernet cable is connected.
ETH2 Ethernet port (Universal and Advanced models)	Indicates whether an Ethernet cable is connected to the Panel Server ETH2 port (for details, page 93): • **Active** indicates that an Ethernet cable is connected to the port. • **Inactive** indicates that no Ethernet cable is connected.
Wi-Fi Infrastructure activation	Used to enable/disable an existing Wi-Fi infrastructure (disabled by default) (for details, page 86). The infrastructure settings are displayed and editable when **Wi-Fi Infrastructure activation** is enabled, including configuring communication by disabling/enabling IPv4 and IPv6. **NOTE:** Activating the Wi-Fi infrastructure and the Wi-Fi access point at the same time may result in some instability on the Wi-Fi network.
Antenna (Universal and Advanced models)	When Wi-Fi is enabled, used to select the type of IEEE 802.15.4 antenna used in the architecture (for details, page 86): • **Internal** (Panel Server internal antenna) (default setting) • **External** (Panel Server external antenna (reference PASA-ANT1) for Panel Server Universal hardware version 002.000.000 and Advanced models.
DNS Settings	Used to configure the DNS server (for details, page 80).

DNS

Presentation

TCP/IP communication is used to perform commissioning, data collection and data publishing, and connection to supervision software.

TCP/IP communication general principles, such as DNS and proxy settings, apply to Ethernet and Wi-Fi.

Domain Name System (DNS) is the naming system for PCs and devices connected to a local area network (LAN) or the Internet.

The following features require DNS service:

- Cloud connection.
- HTTP/HTTPS proxy if a domain name is used.
- SFTP if a domain name is used.
- NTP if a domain name is used.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

The DNS is set as follows:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- On the Panel Server webpages, at **Settings > Network communication > Network > DNS Settings**

DNS Settings

The following table describes the settings available from the webpages.

Parameter	Description
Mode	Used to select the DNS server configuration mode: • Select **Static** to set manually the primary and secondary server addresses. • Select **DHCP** (default setting) to obtain the DNS server configuration automatically from the DHCP server.
Primary DNS IP	Used to enter manually the IPv4 or IPv6 address of the primary DNS server when the parameter DNS configuration mode is set to **Static**.
Secondary DNS IP	Used to enter manually the IPv4 or IPv6 address of the secondary DNS server when the parameter DNS configuration mode is set to **Static**.

RSTP

Presentation

RSTP (Rapid Spanning Tree Protocol) allows IT specialists to re-establish communication paths through Ethernet after a detected interruption.

NOTICE
HAZARD OF INCORRECT CONFIGURATION • Do not enable RSTP if you do not have the necessary skills to configure the network. • Ensure that the network supports RSTP and is correctly configured before enabling RSTP. **Failure to follow these instructions can result in the interruption of normal operation.**

Availability

This function is available on Panel Server Universal and Advanced.

Setting the Parameters

The RSTP function is available when the Ethernet ports are set to **Switched** mode, page 93.

NOTE: When RSTP is enabled, it is not possible to change the Ethernet ports to **Separated** mode.

The RSTP function is set on the Panel Server webpages at **Settings > Network communication > RSTP**. Enable RSTP to display all settings.

NOTE: The default parameters proposed in the Panel Server webpages differ from RSTP standards in order to optimize network stability.

General Settings

Parameter	Description
Ethernet mode	Displays the mode selected in Ethernet settings. RSTP is only available to enable if the Ethernet ports are set to **Switched** mode.
Rapid Spanning Tree Protocol (RSTP) activation	Click the toggle switch to enable RSTP.

Bridge Settings

Parameter	Description	Setting
Bridge priority	Used to enter the bridge priority.	Setting range: 12288–61440 (in multiples of 4096) Default setting: 32768
Bridge hello time (s)	Used to enter the bridge hello time in seconds.	Setting range: 1–2 s Default setting: 2 s
Bridge max age time (s)	Used to enter the bridge maximum age time in seconds.	Setting range: 6–40 s Default setting: 40 s **NOTE:** Follow this rule when setting the Bridge max age time: 2 x (Bridge hello time + 1 s) ≤ Bridge max age time ≤ 2 x (Bridge forward delay - 1 s)
Transmit hold count (messages)	Used to enter the number of messages in the transmit hold count.	Setting range: 1–10 messages Default setting: 6 messages
Bridge forward delay (s)	Used to enter the bridge forward delay time in seconds.	Setting range: 4–30 s Default setting: 21 s

Ethernet Port Settings

Port	Parameter	Setting
ETH1 port settings	**Port priority**	Setting range: 0–240 (in steps of 16) Default setting: 128
	Port cost	Setting range: 0–200,000,000 Default setting: 0. The port cost is calculated based on the ETH port link speed. The calculated value is available in the auto-diagnostic log file, page 171.
ETH2 port settings	**Port priority**	Setting range: 0–240 (in steps of 16) Default setting: 128
	Port cost	Setting range: 0–200,000,000 Default setting: 0. The port cost is calculated based on the ETH port link speed. The calculated value is available in the auto-diagnostic log file, page 171.

RSTP Diagnostics

The following diagnostic data is available by exporting diagnostic logs, page 175.

- Bridge diagnostics:
  - Total topology changes
- Port diagnostics (available for each port):
  - Received RST (BPDUs) : total number of RSTP BPDUs received by Port 1 since the RSTP feature was activated
  - Transmitted RST (BPDUs) : total number of RSTP BPDUs transmitted by Port 1 since the RSTP feature was activated
  - Received TCN (BPDUs) : total number of topology change BPDUs received by Port 1 since the RSTP feature is activated
  - Transmitted TCN (BPDUs) : total number of topology change BPDUs transmitted by Port 1 since the RSTP feature is activated

Proxy

Presentation

It is necessary to configure proxy settings in the Panel Server when both the following conditions are met:

- if you use the remote access or cloud connection, and
- if your network administrator has implemented a proxy on your local network.

The proxy address and port number are provided by your network administrator.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

Proxy is set on the Panel Server webpages, at **Settings > Network communication > Proxy**.

Proxy Activation Settings

Parameter	Description
HTTP proxy	Used to enable/disable the HTTP proxy (disabled by default).
HTTPS proxy	Used to enable/disable the HTTPS proxy (disabled by default).

HTTP and HTTPS Proxy Settings

The following parameters are displayed only when the parameter **HTTP proxy** or **HTTPS proxy** is enabled.

Parameter	Description
Address	Used to enter the IP address or domain name of the HTTP or HTTPS proxy server. **IMPORTANT**: Do not type prefix **http://** or **https://**.
Port	Used to enter the HTTP or HTTPS port.
Authentication	Used to enable/disable if proxy authentication is required (disabled by default).
Non-proxy hosts	Used to enter the exceptions of hosts in a non-proxy host list.

Device Profile for Web Services (DPWS)

Presentation

The EcoStruxure Panel Server supports Devices Profile for Web Services (DPWS) protocol for IP network discovery. When DPWS is enabled on Panel Server gateways, they can be discovered from a PC.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

NOTE: DPWS is not supported when the Wi-Fi access point is enabled on Panel Server Universal and Advanced. DPWS with Wi-Fi access point is supported on Panel Server Entry.

Setting the Parameters

The IP network services are set on the EcoStruxure Panel Server webpages, at **Settings > Network communication > DPWS**.

DPWS can be enabled or disabled.

DPWS Settings

Parameter	Description
DPWS Activation	Used to enable/disable the DPWS service (enabled by default).
Silent mode	Used to enable/disable the silent mode (disabled by default). In silent mode, DPWS only answers requests.
Discovery type	Used to set the IP discovery type: • **IPv4** • **IPv4 & IPv6** (default setting) • **IPv6**
TCP listening port	Used to enter manually the port number. Default setting: **5357** (setting range: 1024–65535).

Wi-Fi Infrastructure

Presentation

The Panel Server supports the following protocols on Wi-Fi infrastructure:

- HTTPS to provide access to the Panel Server embedded webpages
- Modbus TCP/IP
- Devices Profile for Web Services (DPWS) protocol for IP network discovery

If the Panel Server Universal or Advanced is installed in a metallic enclosure, a Wi-Fi external antenna (reference PASA-ANT1) can be installed to extend the Wi-Fi network outside the metallic enclosure. The settings of output power for the external antenna are predefined and not editable. For information about installation of the external antenna, consult the instruction sheet available on the Schneider Electric website: NNZ58425.

If the Panel Server Entry is installed in a metallic enclosure, use the Ethernet port connection instead of Wi-Fi to avoid interruptions in communication.

Availability

This function is available on Panel Server Entry, Universal (except Wired by Design models), and Advanced.

Setting the Parameters

Wi-Fi infrastructure is configured on the EcoStruxure Panel Server webpages. Proceed as follows:

1. Access the Panel Server webpages (see detailed topic, page 201).
2. Enable the **Wi-Fi Infrastructure activation** toggle switch under **Network configuration** on the webpage **Settings > Network communication > Network**.

   NOTE: Wi-Fi activation is enabled automatically when the **Wi-Fi Infrastructure activation** toggle switch is turned on.

Network Configuration Settings

⚠WARNING

UNINTENDED EQUIPMENT OPERATION OR ALTERED FEATURE OF PROTECTIVE DEVICES

Do not set Wi-Fi **Antenna** parameter to **External** if the external Wi-Fi antenna is not connected to the Panel Server Universal or Advanced gateway.

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

For details on the network topology and **Network configuration** settings, see the related topic, page 79.

Infrastructure Settings

The following parameters are displayed only when the parameter **Wi-Fi Infrastructure activation** is enabled.

Parameter	Description
Connection status	Shows the Panel Server connection status to Wi-Fi network: • **Connected** • **Not Connected** **NOTE:** If the Wi-Fi network is temporarily out of service, the Panel Server connects to the Wi-Fi network again within three minutes after network recovery.
SSID	Used to select the Wi-Fi network name by typing it in the field or displayed when double-clicked in **Network list**. **IMPORTANT:** It is recommended to use WPA2 (Wi-Fi Protected Access version 2) (or WPA3 if available) for wireless network security. **NOTE:** Temporal Key Integrity Protocol (TKIP) is not supported.
Authentication key	Used to enter the authentication key for Wi-Fi network.
Network list	Used to select a Wi-Fi network. The SSID field is automatically filled with the corresponding data by double-clicking the network name. For each network name in the list, the following information is displayed: • A Wi-Fi strength indicator icon • A lock icon if a password is required to connect to the network

Wi-Fi Infrastructure IP Settings

The following parameters are displayed only when the parameter **Wi-Fi Infrastructure activation** is enabled.

Parameter	Description
Interface status	Shows the status of the Wi-Fi interface.
MAC address	Shows the Media Access Control (MAC) address. Setting not editable.
IP mode	Used to disable or enable IPv4 or IPv6 communication: • **IPv4** • **IPv4 & IPv6** (default setting) • **IPv6**

To help improve security, IPv4 can be disabled for upstream and downstream communication. When **IP mode** is set to **IPv6**, IPv6 is enabled and IPv4 is automatically disabled, that is, IPv4 downstream devices are disconnected and upstream communication over IPv4 is no longer permitted.

IPv6 Settings

The following parameters are displayed only when **IP mode** is set to **IPv6** or **IPv4 & IPv6**.

NOTE: When **IP mode** is set to **IPv6**, IPv6 is enabled and IPv4 is automatically disabled, that is, upstream communication over IPv4 is no longer permitted.

Parameter	Description
IPv6 local link address	Displays the auto-generated link-local IPv6 address.
IPv6 assignment mode	Used to select the IPv6 assignment mode: • Select **Auto** (default setting) to obtain IPv6 parameters automatically (DHCP or SLAAC). • Select **Static** to enter the IPv6 address manually.
IPv6 address	Used to enter the static IP address of the Panel Server when the parameter **IPv6 assignment mode** is set to **Static**. You can enter a unique local address, or a global address. Displays the IP address automatically obtained when **IPv6 assignment mode** is set to **Auto**.
IPv6 prefix length	Enter the IPv6 address prefix length as an integer between 1 and 128 when the parameter **IPv6 assignment mode** is set to **Static**. Displays the IPv6 address prefix length as an integer between 1 and 128 when the parameter **IPv6 assignment mode** is set to **Auto**.
IPv6 gateway address	Used to enter manually the gateway (router) IP address when the parameter **IPv6 assignment mode** is set to **Static**. Displays the IPv6 gateway address automatically obtained when **IPv6 assignment mode** is set to **Auto**.

IPv4 Settings

The following parameters are displayed only when **IP mode** is set to **IPv4** or **IPv4 & IPv6**.

Parameter	Description
IPv4 assignment mode	Used to select the IPv4 assignment mode: • Select **DHCP** (default setting) to obtain IPv4 parameters automatically. • Select **Static** to enter the IPv4 address manually.
IPv4 address	Used to enter the static IP address of the Panel Server when the parameter **IPv4 assignment mode** is set to **Static**. Displays the IP address automatically obtained when **IPv4 assignment mode** is set to **DHCP**.
IPv4 netmask	Used to enter the netmask address of your network when the parameter **IPv4 assignment mode** is set to **Static**. Displays the IPv4 netmask automatically obtained when **IPv4 assignment mode** is set to **DHCP**. **NOTE:** When Wi-Fi is activated, the Wi-Fi configuration takes precedence over the Ethernet IP configuration. **IMPORTANT:** Use a different netmask for Wi-Fi from the netmask used for Ethernet to avoid connectivity issues on the Panel Server.
IPv4 gateway address	Used to enter manually the gateway (router) IP address when the parameter **IPv4 assignment mode** is set to **Static**.

Wi-Fi Access Point

Presentation

The Wi-Fi access point allows you to use the Panel Server as a router (access point) to commission connected devices. Direct access to devices is not available.

Pressing the multifunction button on the front face of the Panel Server, page 27:

- Enables Wi-Fi.
- Enables the Wi-Fi access point for a period of 5 minutes.

The LED on the front face of the Panel Server blinks blue. If no device connection is established in the 5-minute period, the access point deactivates and the LED reverts to its previous state.

If the LED does not blink blue when the button is pressed, check that Wi-Fi and the Wi-Fi access point are enabled in the webpages.

When the device using the Wi-Fi access point is disconnected, it can take up to 5 minutes for the Panel Server to detect that there is no longer a device connected and to revert to a blue blinking LED. The LED stops blinking after 5 minutes with no device connection.

Availability

This function is available on Panel Server Entry, Universal (except Wired by Design models), and Advanced.

Setting the Parameters

The Wi-Fi access point feature is enabled or disabled on the webpage **Settings > Network communication > Wi-Fi Access point**.

NOTE: Activating both Wi-Fi infrastructure and the Wi-Fi access point may result in some instability on the Wi-Fi network of Panel Server Entry.

Wi-Fi Access Point Settings

Parameter		Description
Enable Wi-Fi access point feature		Click the toggle switch to enable or disable the capability to connect to the access point (enabled by default).
Panel Server Identification	**Device code**	Panel Server credentials used as password for first connection to Wi-Fi access point. **NOTE:** Change the password to help protect the physical security of the device.
Change SSID/ password	**SSID**	Displays the default name for the Wi-Fi access point network. The default name is composed of the product code and serial number of the Panel Server, for example: PAS600L_123456789012. This information is also available by scanning the QR code on the front face of the Panel Server. Use this field to change the name of the Wi-Fi access point network. **NOTE:** If you change the network name (SSID), it is no longer possible to use the information obtained by scanning the QR code on the device to connect to the Wi-Fi access point. You need to use the new network name.

Parameter		Description
	New password	Use this field to change the password to improve the security of your device. **NOTE:** If you change the password, it is no longer possible to use the device code to connect to the Wi-Fi access point. You need to use the new password or reset Panel Server to factory settings, page 190 to restore the device code as default password.
	Confirm password	Use this field to retype the new password to confirm.

Wi-Fi Access Point Connection Pre-requisites

The pre-requisites for connecting to the Wi-Fi access point are as follows:

- Wi-Fi access point feature is enabled on the Panel Server (enabled by default).
- The following information relating to the Panel Server you want to connect to:
  - Product code
  - Serial number
  - Device code

    NOTE: The device code represents the credentials of the Panel Server. Treat this information as confidential.

  This information can be obtained by using a smartphone to scan the QR code on the front face of the Panel Server.

  NOTE: Device code is integrated in the QR code of Panel Server manufactured with serial number 542427•••••• or greater. See hardware description, page 22 to locate the serial number on each Panel Server type.

  The device code is also available in the Panel Server webpages at **Settings > Network communication > Wi-Fi Access point**.

Connecting to the Wi-Fi Access Point from a PC

1. Press the multifunction button on the front face of the Panel Server for less than 5 seconds. The LED on the front face starts blinking blue to indicate that the Wi-Fi access point on the Panel Server is available for pairing.
2. In the list of networks on your PC, locate the Panel Server network name (composed of the product code and serial number you noted earlier, for example: PAS600L_123456789012).

   NOTE: If the network name and/or password have been changed from the default values, you need to find the new name and enter the new password. If you lose or forget the password, you can set a new password in the Panel Server webpages, accessed through an Ethernet connection.
3. Select the network and enter the password (default password: device code). The LED on the front of the Panel Server is on steady blue to indicate that the connection is established.
4. To open the webpages of the Panel Server, on your PC, open the settings of the Panel Server wi-fi access point network you selected. In the list of properties, copy the IPv4 address.
5. In your browser, type *https://* and then paste the IPv4 address, **replacing the last digit by 1**, for example, if the IPv4 address is *nnn.NNN.mmm.2*, type *https://nnn.NNN.mmm.**1***.

   Result: The Panel Server webpages open.
6. Log in using your user account.

   NOTE: For a first connection to the Panel Server:

   a. Log in using the default user account name **SecurityAdmin**.

   b. Enter the default password **AAAAAAAA**. A window opens requiring you to set a new password.

   c. Set a password, following the requirements (see Password Requirements, page 53).

TCP/IP Communication

What's in This Chapter

Ethernet Communication 93
Modbus TCP/IP Client (Universal and Advanced Models) 98
Modbus TCP/IP Server 100

Ethernet Communication

Presentation

The Panel Server uses dual-stack IPv4/IPv6 to manage Ethernet communication and to allow network hosts to communicate with Panel Server.

The Panel Server enables separate IP configuration for each interface.

IP mode	Description
IPv4	Only IPv4 communication is enabled.
IPv4 and IPv6	IPv4 and IPv6 communication are enabled.
IPv6	Only IPv6 communication is enabled; IPv4 communication is completely disabled.

IMPORTANT: When IPv6 is selected for downstream communication, Panel Server cannot communicate with existing or newly discovered Modbus TCP/IP devices.

IMPORTANT: When IPv6 is selected for upstream communication, Panel Server cannot publish data to the Schneider Electric cloud, and remote access from Customer Care Center is also not possible.

The Panel Server supports the following protocols on Ethernet:

- **Modbus TCP/IP:** Modbus TCP/IP is a protocol which provides client/server communication between devices over an Ethernet connection. Modbus TCP/IP is used to exchange data through the TCP port that has been configured (port 502 by default).
- **Hypertext Transfer Protocol Secure (HTTPS):** HTTPS is 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. HTTPS enables encrypted communication and helps to secure connection between a remote user and the Panel Server.
- **Devices Profile for Web Services (DPWS)**: DPWS is a minimal set of implementation constraints that helps to enable secure web service messaging, discovery, description, and events on resource-constrained devices.
- **Secure File Transfer Protocol (SFTP) Client:** SFTP is a variant of the standard file transfer protocol (FTP) that uses secure shell encryption to provide a high level of security for file transfer.
- **Rapid Spanning Tree Protocol (RSTP):** RSTP is an advanced version of spanning tree protocol (STP), a link layer protocol executed within bridges or switches (Panel Server Universal and Advanced).

The number of Ethernet ports depends on the model:

- The Entry model has one Ethernet port.

- The Universal and Advanced models have two Ethernet ports. The Ethernet ports can be configured in one of the following modes:
  - Switched mode:
    - Both Ethernet ports belong to the same network.
    - An Ethernet switch function is enabled.
    - RSTP can be configured and activated.
  - Separated mode:
    - Both Ethernet ports are connected to separate local area networks (LAN).
    - Ports are isolated one from another, that is, neither router nor forwarding packets are enabled from TCP/IP standpoint.
    - Modbus routing can be enabled from port ETH1 to the devices discovered over ETH2 by enabling Modbus TCP/IP server service on ETH1.
    - Modbus routing can be enabled from port ETH2 to the devices discovered over ETH1 by enabling Modbus TCP/IP server service on ETH2.

    Modbus TCP/IP server service can be enabled or disabled in the Panel Server webpages at **Settings > Network communication > Services**.

Availability

The Ethernet communication function is available on Panel Server Entry, Universal, and Advanced.

Single Ethernet Port Configuration (Entry Model)

The Panel Server Entry has only one Ethernet port. For the settings, refer to Setting the Parameters, page 95.

Switched Mode Configuration (Universal and Advanced Models)

In switched mode, both Ethernet ports (ETH1, ETH2) share the same settings. The Panel Server has one single unique IP address applied to both Ethernet ports. Devices connected to either Ethernet port belong to the same Ethernet network.

Using two ports simplifies wiring, for example:

- One port can be connected to a switch in the local network.
- One port can be used to connect a PC for configuration operations or to connect a data collection device locally with an Ethernet port.
- Multiple Ethernet devices relying on the embedded hardware switch inside the Panel Server can be daisy-chained. Daisy-chaining allows devices located on either side of the Panel Server to communicate with each other as part of the same network.

  NOTE: Ring topology is supported if RSTP is activated, page 81.

For more information and a diagram illustrating this architecture, refer to Switched Ethernet Network, page 72. For the settings, refer to Setting the Parameters, page 95.

Separated Mode Configuration (Universal and Advanced Models)

In separated mode, one IP network is assigned to each Panel Server Ethernet port and each IP network assigns an IP address to the Panel Server. The separated mode is used to segregate downstream Modbus TCP/IP devices connected to **ETH2** port from upstream communication systems connected to **ETH1** port. There are neither router nor forwarding packets at the network level. Only Modbus routing can be enabled.

The two Ethernet ports have different settings and function independently.

- **ETH1** port is used for data publishing (to a cloud application or a SCADA system).
  Modbus service can be disabled if the upstream system is a cloud application or a web browser to access the Panel Server webpages. Modbus service needs to be enabled if the upstream system is a SCADA or a Building Management System using Modbus TCP/IP communication.
- **ETH2** port can be used for one of the following purposes:
  - Data collection from downstream Modbus TCP/IP devices for publication on ETH1.
  - Management by a SCADA system connected to ETH2 port and different from the SCADA system connected to ETH1.

  Modbus service needs to be enabled on ETH1 in case of connection to a SCADA system. It is recommended to disable it in case of connection to a cloud application.

For more information and a diagram illustrating this architecture, refer to Separated Ethernet Network, page 73. For the settings, refer to Setting the Parameters, page 95.

Setting the Parameters

NOTICE
IMPAIRED NETWORK PERFORMANCE Only qualified personnel should modify the Ethernet settings. Perform such modifications only after you have read about and understood the Ethernet settings. **Failure to follow these instructions can result in loss of network connectivity**

The Ethernet communication function is set as follows:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- On the Panel Server webpages, at **Settings > Network communication > Network**

Depending on the configuration (Ethernet switched mode, Ethernet separated mode, or Wi-Fi infrastructure), the Modbus service can be activated individually at **Settings > Network communication > Services**.

Network Configuration Settings

For details on the network topology and **Network configuration** settings, see the related topic, page 79.

Ethernet Settings

IP configuration settings are available as follows:

- For Entry model: **ETH1 port settings**
- For Universal and Advanced models:
  - In the case of separated mode: **ETH1 port settings** and **ETH2 port settings**. The settings in the table below are duplicated for ETH2 port settings.
  - In the case of switched mode: **Ethernet Settings**

Parameter	Description
Interface status	Displays **Up** or **Down**: • **Up**: The interface is enabled and ready to send and receive data. • **Down**: The interface is disabled and not ready to send and receive data.
MAC address	Displays the Media Access Control (MAC) address, a unique identifier for each Panel Server port. The MAC address is marked on the Panel Server front face.
IP mode	Used to disable or enable IPv4 or IPv6 communication: • **IPv4** • **IPv4 & IPv6** (default setting) • **IPv6**

To help improve security, IPv4 can be disabled for upstream and downstream communication. When **IP mode** is set to **IPv6**, IPv6 is enabled and IPv4 is automatically disabled, that is, IPV4 downstream devices are disconnected and upstream communication over IPv4 is no longer permitted.

IPv4 Settings

The following parameters are displayed only when **IP mode** is set to **IPv4**, or **IPv4 & IPv6** is enabled.

Parameter	Description
IPv4 assignment mode	Used to select the IPv4 assignment mode: • Select **DHCP** (default setting) to obtain IPv4 parameters automatically. • Select **Static** to enter the IPv4 address manually.
IPv4 address	Used to enter the static IP address of the Panel Server when the parameter **IPv4 assignment mode** is set to **Static**. Displays the IP address automatically obtained when **IPv4 assignment mode** is set to **DHCP**.
IPv4 netmask	Used to enter the Ethernet IP netmask address of your network when the parameter **IPv4 assignment mode** is set to **Static**. Displays the IPv4 netmask automatically obtained when **IPv4 assignment mode** is set to **DHCP**.
IPv4 gateway address	The parameter is displayed only for **ETH1 port settings** and **Switched port settings** when Wi-Fi activation is disabled (see Wi-Fi Infrastructure, page 86). Used to enter manually the gateway (router) IP address when the parameter **IPv4 assignment mode** is set to **Static**. Displays the gateway address automatically when **IPv4 assignment mode** is set to **DHCP**.

IPv6 Settings

The following parameters are displayed only when **IP mode** is set to **IPv6**, or **IPv4 & IPv6** is enabled.

NOTE: When **IP mode** is set to **IPv6**, IPv6 is enabled and IPv4 is automatically disabled, that is, IPV4 downstream devices are disconnected and upstream communication over IPv4 is no longer permitted.

Parameter	Description
IPv6 link-local address	Displays the auto-generated link-local IPv6 address.
IPv6 assignment mode	Used to select the IPv6 assignment mode: • Select **Auto** (default setting) to obtain IPv6 parameters automatically (DHCP or SLAAC). • Select **Static** to enter the IPv6 address manually.
IPv6 address	Used to enter the static IP address of the Panel Server when the parameter **IPv6 assignment mode** is set to **Static**. You can enter a unique local address, or a global address. Displays the IP address automatically obtained when **IPv6 assignment mode** is set to **Auto**.
IPv6 prefix length	Used to enter the IPv6 address prefix length as an integer between 1 and 128 when the parameter **IPv6 assignment mode** is set to **Static**. Displays the IPv6 address prefix length as an integer between 1 and 128 when the parameter **IPv6 assignment mode** is set to **Auto**.
IPv6 gateway address	The parameter is displayed only for **ETH1 port settings** and **Switched port settings** when Wi-Fi activation is disabled (see Wi-Fi Infrastructure, page 86). Used to enter manually the gateway (router) IP address when the parameter **IPv6 assignment mode** is set to **Static**. Displays the IPv6 gateway address automatically obtained when **IPv6 assignment mode** is set to **Auto**.

NOTE: When **IPv6 assignment mode** is set to **Auto**, the parameters initially display **No data** at **IPv6 address** and **IPv6 gateway**, and **0** at **IPv6 prefix length**.
When the IPv6 address is generated, **IPv6 gateway** displays a gateway address if one is provided by the upstream gateway (usually a router). If no gateway address is provided by the upstream gateway, **No data** remains displayed at **IPv6 gateway**.

Modbus TCP/IP Client (Universal and Advanced Models)

Presentation

The Panel Server acts as both a Modbus TCP/IP gateway and a Modbus device by using the internal Modbus TCP server.

To correctly configure your Modbus TCP/IP client to access data from Panel Server and from devices under Panel Server, see Modbus Gateway Function, page 60.

The Panel Server acts as a Modbus gateway for wired or wireless Ethernet communications from an upstream PC to Ethernet devices and field devices on the downstream network. By using a local monitoring software you can access information from devices for data collection and other functions.

The Panel Server manages Modbus communication on all interfaces including Wi-Fi.

For more information, see Modbus TCP/IP functions, page 267 and Modbus TCP/IP exception codes, page 272 in appendix.

Availability

This function is available on Panel Server Universal and Advanced.

Setting the Parameters

NOTICE

IMPAIRED NETWORK PERFORMANCE

Only qualified personnel should modify the Modbus TCP/IP settings. Perform such modifications only after you have read about and understood the Modbus TCP/IP settings.

Failure to follow these instructions can result in loss of network connectivity.

Modbus TCP/IP client function is set as follows:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- On the Panel Server webpages, at **Settings > Modbus devices > Network configuration > Modbus TCP/IP client**.

For information about the Modbus registers, see the guide of each Modbus-SL device and DOCA0241EN *EcoStruxure Panel Server - Modbus File* for wireless devices.

Modbus TCP/IP Client Settings

The following table describes the settings available from the webpages.

Parameter	Description
Connection timeout (ms)	Used to set the time the Panel Server waits for a remote Modbus TCP/IP device to establish the connection with the Panel Server. Values from 100 to 10000 ms in a list (default setting: 2000 ms)
Message timeout (ms)	Used to set the time the Panel Server waits for a remote Modbus TCP/IP device to respond and send a message following a Modbus TCP/IP request initiated by the Panel Server. Values from 1000 to 20000 ms with step 1000 (default setting: 3000 ms)

For recommendations and more information about setting the message timeout parameter, refer to Setting Message Timeout for Modbus Client and Server, page 279.

Modbus Device Addition Settings

The following table describes the **Modbus TCP/IP** settings available from the webpages.

Parameter	Description
Discovery	Used to enter the selective list of IP address, port and Unit ID of devices to be discovered. Click **Start** to launch discovery. Displays **Discovery status**.
Discovered devices table	Displays information about each device discovered in the Modbus TCP/IP network: • Picture • Name • IP address • Port • Unit ID • Virtual server ID
Manual addition	Used to manually add Modbus TCP/IP devices: • Enter the following information: ◦ IP address ◦ Port ◦ Unit ID • Select the device type in the **Device** drop-down list. • Click **Add**.

NOTE: Modbus devices are listed under **MODBUS TCP/IP** section in the device list.

Modbus TCP/IP Server

Presentation

Devices connected downstream from the Panel Server can be accessed from an upstream edge system through Modbus TCP/IP.

Availability

This function is available on Panel Server Universal and Advanced.

Setting the Parameters

Modbus TCP/IP server function is set as follows:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- On the Panel Server webpages, at **Settings > Modbus devices > Network configuration > Modbus TCP server**.

Modbus TCP Server Settings

The following table describes the settings available from the webpages.

Parameter	Description
Message timeout (ms)	In Modbus network configuration, you can set the message timeout period for the Modbus TCP server. The setting is used to set the time-to-live of a Modbus request in the Panel Server. Any messages older than this setting will be dropped without sending any response back to upstream SCADA. Enter a value from 1000 to 320000 ms with step 100 (default setting: 6000 ms). The value that you set for the Modbus TCP server must meet both the following conditions: • Be equal to the message timeout that is defined on the upstream Modbus client (SCADA or another Panel Server). • Be higher than the timeout defined in the Panel Server Modbus client setting (Modbus TCP/IP and Modbus-SL). For recommendations and more information about setting the parameter, refer to Setting Message Timeout for Modbus Client and Server, page 279.

Modbus-SL Communication (Models with One Modbus-SL Port)

Presentation

Panel Server Universal and Advanced with one Modbus Serial Line port are Modbus-SL clients and they can be connected to any Modbus-SL server devices. The Panel Server acts as a Modbus gateway and then allows any upstream software such as EcoStruxure Power Monitoring Expert and EcoStruxure Power Operation using Modbus TCP/IP communication to access the Modbus-SL devices.

The Panel Server is also able to collect data from the Modbus-SL devices for publishing to a cloud application or for historization by the energy server in a Panel Server Advanced.

Modbus-SL server devices are connected downstream to the Panel Server.

For more information, see Modbus-SL functions, page 269 and Modbus-SL exceptions codes, page 272 in appendix.

The Panel Server Modbus serial port can be configured in reverse mode (see Modbus-SL Reverse Mode, page 104).

Availability

This function is available on Panel Server Universal and Advanced.

Setting the Parameters

NOTICE
IMPAIRED NETWORK PERFORMANCE Only qualified personnel should modify the Modbus-SL settings. Perform such modifications only after you have read about and understood the Modbus-SL settings. **Failure to follow these instructions can result in loss of network connectivity.**

The Modbus-SL communication function is set as follows:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- On the Panel Server webpages, at **Settings > Modbus devices > Network configuration**.

For information about the Modbus registers, see the guide of each Modbus-SL device and DOCA0241EN *EcoStruxure Panel Server - Modbus File* for wireless devices.

Modbus Serial Mode Settings

The following table describes the settings available from the webpages.

Parameter	Description
Modbus mode	Used to select the configuration of Modbus-SL mode: • **Client** (default setting) • **Server**

Modbus Serial Client Configuration Settings

The following parameters are displayed only when the parameter of Modbus-SL mode is set to **Client**.

The following table describes the settings available from the webpages.

Parameter	Description
Activation	Used to enable/disable the Modbus-SL feature (enabled by default).
Transmission mode	**RTU**. Setting not editable.
Baud rate (Bd)	Used to set the transmission rate: • 1200 • 2400 • 4800 • 9600 • 19200 (default setting) • 38400 • 57600 • 115200
Parity	Used to define the parity bit of the transmitted bytes: • **Odd** • **None** • **Even** (default setting)
Number of bits	8 bits. Setting not editable.
Number of stop bits	Used to define the number of stop bits transmitted: 1 or 2 (default setting: 1)
Silent interval (ms)	Used to define the silent time after the end of a Modbus-SL packet communication. Values from 0 to 10 ms with step 1 (default setting: 5 ms)
Frame delay (ms)	Used to define the minimum silent time between the end of a received response and the beginning of a new request on the serial line. Values from 0 to 100 ms with step 10 (default setting: 50 ms) **NOTE:** The frame delay value needs to be aligned with the end device frame delay. For example, if end device frame delay equals 50 ms, then set 50 ms on Panel Server). Data loss may occur if these values are not aligned.
Timeout (ms)	Used to define the timeout value after which a loss of communication is declared by the Panel Server. Values from 100 to 20000 ms with step 1 (default setting: 3000 ms)
Line termination resistor	Used to connect/disconnect the RS485 termination resistor embedded in the Panel Server to help prevent reflection (default setting: **Connect**).
Line polarisation resistor	Used to prevent invalid data bits by forcing the transmission line into a known state. Setting polarization to **Connect** (default setting) enables the forcing of the transmission line into a known state.

Modbus Serial Server Configuration Settings

The following parameters are displayed only when the parameter of Modbus-SL mode is set to **Server**.

The following table describes the settings available from the webpages.

Parameter	Description
Transmission mode	**RTU**. Setting not editable
Baud rate (Bd)	Used to set the transmission rate: • 1200 • 2400 • 4800 • 9600 • 19200 (default setting) • 38400 • 57600 • 115200
Parity	Used to define the parity bit of the transmitted bytes: • **Odd** • **None** • **Even** (default setting)
Number of bits	8 bits. Setting not editable.
Number of stop bits	Used to define the number of stop bits transmitted: 1 or 2 (default setting: 1).
Silent interval (ms)	Used to define the silent time after the end of a Modbus-SL packet communication. Values from 0 to 10 ms with step 1 (default setting: 5 ms)
Frame delay (ms)	Used to define the minimum silent time between the end of a received response and the beginning of a new request on the serial line. Values from 0 to 100 ms with step 10 (default setting: 50 ms) **NOTE:** The Frame delay value needs to be aligned with the end device frame delay. For example, if end device frame delay equals 50 ms, then set 50 ms on Panel Server). Data loss may occur if these values are not aligned.
Line termination resistor	Used to connect/disconnect the RS485 termination resistor embedded in the Panel Server to help prevent reflection (default setting: **Connect**)
Line polarisation resistor	Used to enable/disable forcing the transmission line into a known state to help prevent invalid data bits (enabled by default). The transmission line into the RS485 port enters an indeterminate state when it is not being transmitted to. This indeterminate state causes the receivers to receive invalid data bits from the noise picked up on the cable.
Message timeout (ms)	In Modbus network configuration, you can set the message timeout period for the Modbus-SL server. The setting is used to set the time-to-live of a Modbus request in the Panel Server. Any messages older than this setting will be dropped. Values from 1000 to 320000 ms with step 100 (default setting: 6000 ms) The value that you set for the Modbus-SL server must meet both the following conditions: • Be equal to the message timeout that is defined on the upstream Modbus client (SCADA or another Panel Server). • Be higher than the timeout defined in the Panel Server Modbus client setting (Modbus TCP/IP and Modbus-SL).

Modbus Device Addition Settings

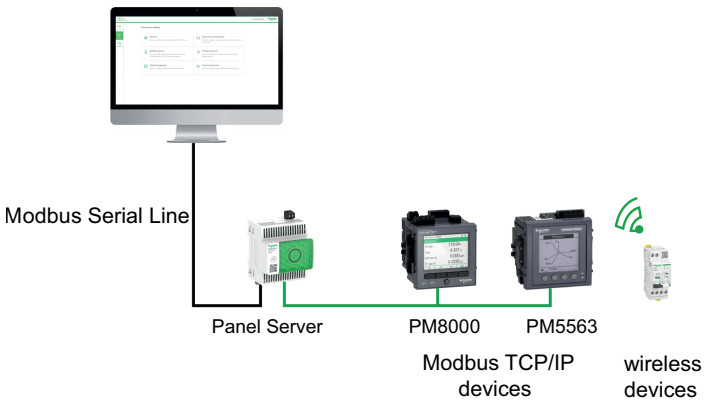
The following table describes the **Modbus serial** settings available from the webpages.

Parameter	Description
Discovery	**Selective list**: Used to enter the selective list of Modbus addresses (1–254) for which the devices must be discovered. If no selective list is entered, the range 1-10 is used for discovery. Click **Start** to launch discovery. Displays **Discovery status**, status of the device discovery on the Modbus network: • **Idle**: device discovery is inactive. • **InProgress**: device discovery is in progress. • **Done**: device discovery is completed.
Discovered devices table	Displays information about each device discovered in the Modbus-SL network: • Picture • Name • Modbus Serial Line: **1** • Physical server ID • Virtual server ID
Manual addition	Used to manually add Modbus-SL devices: • Enter the physical server ID. A virtual server ID is assigned as part of the process. • Select the device type in the **Device** drop-down list. • Click **Add**.

NOTE: Modbus devices are listed under **MODBUS SERIAL LINE 1** section in the device list.

Modbus-SL Reverse Mode

Panel Server Modbus serial port can be configured in reverse mode. The Modbus-SL reverse mode allows any Modbus client (for example, SCADA) connected to the RS485 port, to access data from Modbus TCP/IP devices connected to ETH1 and/or ETH2 Ethernet port, and from any associated wireless devices by means of the virtual Modbus ID of the wireless device, as shown on this diagram:



Modbus Serial Line network

Ethernet network

The Modbus-SL reverse mode is set and monitored on the Panel Server webpages at **Settings > Modbus devices**. In **Modbus configuration** change the **Modbus mode** from **Client** to **Server**.

I/O Smart Link Modbus Settings

If you configure or change the Modbus settings of an I/O Smart Link device by using EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34, or through Smartlink SIB webpages, and then connect to Panel Server webpages, you must update the I/O Smart Link Modbus settings in the Panel Server webpage to synchronize the configuration.

It takes approximately one minute to get the I/O Smart Link Modbus configuration refreshed on the Panel Server webpages. You can navigate through the other Panel Server webpages during the synchronization.

You cannot launch the synchronization of two I/O Smart Link devices at the same time.

When you have launched a synchronization, you cannot cancel the process.

Wireless Communication

What’s in This Chapter

Wi-Fi Communication 107
IEEE 802.15.4 Communication 108
Dynamic Antenna Selection 112
Channel Scan Function 114
Permanent Deactivation of Wireless Networks 116

Wi-Fi Communication

Presentation

The EcoStruxure Panel Server supports the following Wi-Fi functions:

- Wi-Fi infrastructure, that is, the Panel Server can connect to a Wi-Fi router (access point). For more information, refer to Wi-Fi Infrastructure, page 86.
- Wi-Fi access point, that is, Panel Server can serve as a Wi-Fi router (access point) to which you can connect a smartphone or a PC. For more information, refer to Wi-Fi Access Point, page 89.

Availability

This function is available on Panel Server Entry, Universal (except Wired by Design models), and Advanced.

Setting the Parameters

Wi-Fi activation can be enabled and disabled on the Panel Server webpages (disabled by default). Proceed as follows:

1. Access the Panel Server webpages (see detailed topic, page 201).
2. To enable or disable the Wi-Fi function on the webpage:
   - For Wi-Fi infrastructure: Click the toggle switch **Wi-Fi Infrastructure activation** on webpage **Settings > Network communication > Network > Network configuration**.

     NOTE: Wi-Fi activation is enabled automatically when the **Wi-Fi Infrastructure activation** toggle switch is turned on.
   - For Wi-Fi access point: Click the toggle switch **Enable Wi-Fi access point feature** on webpage **Settings > Network communication > Wi-Fi Access point**.

     NOTE: Wi-Fi activation is enabled automatically when the multifunction button on the front face of the Panel Server is pressed during commissioning of the Panel Server through EcoStruxure Energy Hub Essential (part of EcoStruxure Building Activate). For more information, refer to Wi-Fi Access Point Connection Pre-requisites, page 90.

IEEE 802.15.4 Communication

Presentation

In an EcoStruxure system where IEEE 802.15.4 wireless devices are connected to a Panel Server, these wireless devices are required to withstand EMC levels as per IEEE 802.15.4 standard for proper device performance. For details about supported Schneider Electric IEEE 802.15.4 wireless devices, refer to the relevant Panel Server firmware release notes, page 10:

- DOCA0249•• *EcoStruxure Panel Server Entry - Firmware Release Notes*
- DOCA0178•• *EcoStruxure Panel Server Universal - Firmware Release Notes*
- DOCA0248•• *EcoStruxure Panel Server Advanced - Firmware Release Notes*

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

Use IEEE 802.15.4 communication only with ComPacT, PowerPacT, MasterPacT MTZ, and other qualified devices.

Failure to follow these instructions will result in death or serious injury.

IEEE 802.15.4 wireless communication devices provide a compact and high-density metering solution with numerous and accurate data for building systems. These wireless devices can send temperature, humidity, energy, power, current, voltage, and power factor to the Panel Server.

Wireless devices are connected downstream to the Panel Server.

All wireless devices are connected on the same channel. If you change the channel, the wireless devices scan other nearby channels until they reestablish communication with the Panel Server. The scan function can be disabled on compatible devices if required. Refer to Managing the Channel Scan, page 114.

The maximum number of wireless devices that can be connected to one Panel Server is detailed in the related topic, page 20.

The Panel Server Universal (hardware version 002.000.000) and Panel Server Advanced can be connected to an external IEEE 802.15.4 antenna to extend the wireless network.

Availability

This function is available on Panel Server Entry, Universal (except Wired by Design models), and Advanced.

Setting the Parameters

IEEE 802.15.4 communication function is set as follows:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
- On the Panel Server webpages, at **Settings > Wireless devices > Network configuration**

Configuration Settings

⚠WARNING

UNINTENDED EQUIPMENT OPERATION OR ALTERED FEATURE OF PROTECTIVE DEVICES

When installing a Panel Server in a metallic enclosure, and connecting it to an external IEEE 802.15.4 antenna, do not install this antenna within the enclosure.

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

Correct operation of protective devices installed in a metallic enclosure can be altered by a high level of IEEE 802.15.4 network radio frequency transmission power.

The following table describes the settings available from the webpages.

Parameter	Settings	Description
Wireless network settings	**Wireless activation**	Used to enable/disable wireless emission of the Panel Server (disabled by default).
	Channel mode	Used to specify how the IEEE 802.15.4 channel is selected: • When you select **Auto** (default setting), the most appropriate channel is automatically selected by the Panel Server. • When you select **Manual**, configure the wireless parameters: 1. Enter the required channel (value between 11 and 26) 2. Save your settings by clicking the icon at bottom right of the screen and selecting **Save**. **NOTE:** When ZBRT devices are connected to the Panel Server, decommission and remove the ZBRT devices, page 257 before changing the channel mode or channel number, and add them again after the change.
	Channel	Enter the channel number.
	Antenna selection	Used to select the type of IEEE 802.15.4 antenna used in the architecture: • **Internal** (Panel Server internal antenna) (default setting) • **External** (Panel Server external antenna, Panel Server Universal hardware version 002.000.000 and Advanced model option) • **Both** (internal and external antennas are used with Panel Server Universal hardware version 002.000.000 and Advanced.)
	Output power	Output power level cannot be changed when the internal antenna or both antennas (internal and external) are used. **Output power** can be set only when an external IEEE 802.15.4 antenna is connected to a Panel Server Advanced: • If **Antenna selection** is set to **Internal** or **Both**, the internal antenna is used and **Low level** is displayed (setting not editable). • If **Antenna selection** is set to **External**, set the output power to **Low level** or **High level** depending on your network. **NOTE:** When a Panel Server connected to an external IEEE 802.15.4 antenna is installed in a metallic enclosure, check that the antenna is not installed within the enclosure.
Dynamic antenna selection (Available when **Internal** is selected in **Antenna selection**.)	**Dynamic antenna selection**	An advanced feature to be used with caution. Disabled by default. Refer to Manage dynamic antenna selection, page 112. Used to enable the Panel Server to switch between internal antennas, based an analysis of the signal quality. The following fields are displayed when **Dynamic antenna selection** is enabled.
	Automatic analysis	Enabled by default. Used to enable automatic launch of analysis when the Panel Server detects a communication loss with a TH110 or CL110 sensor.
	Launch analysis/Stop analysis	Used to start an analysis or stop an analysis that is in progress.

Parameter	Settings	Description
		NOTE: Check that TH110 and CL110 sensors are powered on before launching an analysis.
	Analysis status	Indicates the status of the analysis: • **In progress** • **Successful** • **Canceled**
	Analysis result	Indicates which antenna is selected after the analysis is done: • **AntennaA** • **AntennaB** • **Antenna switching mode**
Wireless communication For more information about setting the communication period, refer to Setting the Communication Period for Device Family, page 110.	**Communication period for ambient sensors (s)**	Used to set the communication period for the ambient sensor family. Select a value between 60 and 600 seconds from the list. Default setting: 120 seconds **NOTE:** The ambient sensor family includes any type of environmental sensor, for example, HeatTag, TH110, CL110.
	Communication period for control devices (s)	Used to set the communication period for the control device family. Select a value between 5 and 120 seconds from the list. Default setting: 60 seconds
	Communication period for energy related devices (s)	Used to set the communication period for the energy related device family. Select a value between 5 and 120 seconds from the list. Default setting: 15 seconds
	Network occupancy	Indicates the network occupancy as a percentage.
Wireless device management	**Remove all devices**	Used to remove all wireless devices connected to the Panel Server.
Manage scan function	**Scan activation**	Used to enable or disable scan function of wireless devices (enabled by default). Refer to Managing the Channel Scan Function, page 114. • **Status on wireless device**: indicates the result of the change to the scan function. • **Retry**: button used to try to enable or disable the function again after an unsuccessful attempt, with status displayed as **Not applied on all devices**.

Setting the Communication Period for Device Family

The communication period defines the frequency (in seconds) at which each wireless device sends data to the Panel Server. This is only applicable to real-time data and not to alarms that are immediately notified in case of event.

Set the communication period for all discovered devices that support this feature, and for each family of devices.

Any change to the communication period takes time to be applied on devices, as it is not applied until the next communication with the device.

NOTE: If the communication period is reduced, it can potentially impact the stability of the wireless network, and indicator of radio quality may be degraded. Use the network occupancy information to help you understand the impact of the changes. As standard, the Panel Server has a defined default value for each family of wireless devices.

The communication period can be changed as follows, if needed:

1. Select the required communication period from the **Communication Period** list.

2. Save your settings by clicking the icon at bottom right of the screen and selecting **Save**. The communication period updates in the webpages. A command to change the communication period is sent to each connected device. For each device the change is applied at its next communication with the Panel Server.

   NOTE: On the settings page for each individual device to which the change is relevant, the change may take up to three times the original communication period to be updated. During this time you may observe one of the three following results in the **Communication period (s)** field:

   - The communication period is updated to the new setting. The Panel Server communicated with the device.
   - A spinner icon with the text **Updating device** is displayed. The Panel Server is in communication with the device.
   - The communication period is not updated to the new setting. The Panel Server has not yet communicated with the device.

3. **Update successful** is displayed once the wireless communication setting is updated.

Settings of Wireless Devices Discovery

The following table describes the settings available in the Panel Server webpages.

Parameter	Settings	Description
Discovery	**Discovery method**	**Automatic** (enabled by default): Used to discover any available devices. **Selective**: Used to discover a selective list of wireless devices to be connected to the Panel Server. Click **Upload file** to import a prepared selective list in CSV format. **Protect Plus** (enabled by default): Enable this function for a selective discovery process with heightened security for 16-character RF-ID devices, using the install code Click **Start** to launch the discovery. For more information, refer to Discovery of Wireless Devices Through Webpages, page 239
Discovery result	**Discovery status**	Indicates the status of the device discovery on the wireless network: • **Idle**: device discovery is inactive. • **InProgress**: device discovery is in progress. • **Done**: device discovery is performed.
	Discovery	Table displaying the discovered wireless devices with device picture, name, and RF-ID.
	Rejected discovery	Table displaying the wireless devices for which the discovery was not successful. A **Status** column indicates the cause of the rejected discovery.

Dynamic Antenna Selection

Presentation

NOTICE

REDUCED DATA ACQUISITION

Only enable dynamic antenna selection if your configuration contains TH110 and/or CL110 ambient sensors and you observe fading issues. All connected devices are impacted by the choice of internal antenna.

Failure to follow these instructions can result in reduction is data acquisition from connected devices.

Dynamic antenna selection is an advanced function intended for use with specific configurations containing TH110 and CL110 ambient sensors, where fading issues are observed. It is only available when **Internal** is selected in **Antenna selection**. The function should be used with caution. You should understand the consequences of the action before selecting it.

The dynamic antenna function analyses the signal quality of the available internal antennas to select the antenna that provides the best signal. The analysis takes **n** seconds to complete, where
n = 10 x ambient sensor communication period (seconds). When the default communication period is set (120 seconds), the analysis takes approximately 20 minutes.

During the analysis, the Panel Server switches between the available internal antennas (antenna A and antenna B), spending an equal time on each, to assess the quality of the signal. Data acquisition is impacted during the analysis if some devices do not have good signal on one or other antenna. Based on the result of the analysis, the Panel Server chooses the antenna with the best signal quality. If neither antenna is fully satisfactory, **Antenna switching mode** is automatically activated. The system switches between antennas after every **n** seconds, where **n** = 2 x ambient sensor communication period (seconds). In this way, the switching period remains below the communication loss trigger.

Devices may have better signal quality on one or other of the antennas. Switching between antennas allows the Panel Server to maintain communication with all devices, but the frequency of the communication is reduced.

The function also offers the possibility of activating automatic analyses. When activated, the Panel Server launches an automatic analysis when it detects a communication loss with a device.

You can launch an analysis when you want by clicking **Launch analysis**.

Availability

This function is available on Panel Server Entry, Universal (except Wired by Design models), and Advanced.

Setting the Parameters

Dynamic antenna selection is configured on the Panel Server webpages, at **Settings > Wireless devices > Network configuration**

Procedure to Enable Dynamic Antenna Selection

Follow this procedure to enable dynamic antenna selection:

1. In **Wireless network settings**, enable **Wireless activation**.
2. Click the button to enable **Dynamic antenna selection**.
3. If not required, click the button to deactivate **Automatic analysis** (enabled by default).
4. Save your settings. After saving the settings the **Launch analysis** button is active.

   NOTE: If Automatic analysis is enabled, you can launch an immediate analysis, or you can wait for the analysis to be launched automatically. Automatic analysis is launched when the Panel Server detects a communication loss with a device.
5. Click **Launch analysis**.
6. Check the **Analysis status**:
   - **Successful**: the analysis is complete and the result is displayed below and executed.
   - **In progress**
   - **Canceled**: the analysis can be canceled if one of the following actions is initiated during an analysis:
     - Adding or removing a device
     - Changing the channel configuration
     - Changing the ambient sensor communication period
     - Clicking on **Stop analysis**
7. When the analysis is successful, check the analysis result:
   - **AntennaA**
   - **AntennaB**
   - **Antenna switching mode**

Channel Scan Function

Presentation

Connected IEEE 802.15.4 wireless devices scan other channels to reestablish communication with the Panel Server in the event that communication is lost. If the channel setting for wireless devices is changed manually on the Panel Server webpages, wireless devices scan nearby channels until communication is established. This function can be disabled on compatible devices to help reduce disturbance on other IEEE 802.15.4 wireless devices.

Disabling the scan function is an advanced feature and should be used with caution. You should understand the consequences of the action before disabling it.

Availability

This function is available on Panel Server Entry, Universal (except Wired by Design models), and Advanced.

Setting the Parameters

Dynamic antenna selection is configured on the Panel Server webpages, at **Settings > Wireless devices > Network configuration**.

Managing the Channel Scan Function

To disable the function on the webpages at **Manage scan function**, click the **Scan activation** toggle switch. The switch is green when the function is enabled (default configuration) and white when disabled.

> **NOTE:** If not all wireless devices are in connected state, a popup message indicates that the changes have not been saved and provides the following guidance: **It is not recommended to deactivate the scan function without first saving changes to the wireless network settings. Check all the wireless devices are using the current channel prior to deactivating the scan function.** Connect all wireless devices and try again.

When the function is disabled:

- Connected devices do not scan to find a new channel if communication is lost with the Panel Server. They continue to communicate on the current channel at every communication period.
- It is not possible to modify the channel configuration settings on the webpages. You must reactivate the scan function in order to make modifications to the settings.

Status on wireless device can be one of the following:

- **In progress**
- **Applied on all devices**

  > **NOTE:** Devices not compatible with disabling of scan function continue to scan.

- **Not applied on all devices**

  NOTE: If the change is not applied on all devices, check that the firmware version of your devices is compatible with the function. Otherwise click **Retry** to check that the issue was not a temporary one.

Devices Supporting Disabling of Channel Scan

The following table indicates devices which support disabling of the scan function. The list is not exhaustive.

Device family	Device	Minimum firmware version
Power meter	PowerTag Rope compliant with IEC and UL standards	001.003.002
	PowerTag F160	001.003.002
	PowerTag Energy	004.002.000
Ambient sensors	PowerLogic TH110 wireless thermal sensor	001.000.003
	PowerLogic CL110 wireless environmental sensor	002.001.003
	Wireless CO2 sensor SED-CO2–G-5045	001.001.004
	Wireless temperature and humidity sensor SED-TRH-G-5045	001.001.004

Permanent Deactivation of Wireless Networks

Presentation

Panel Server models PAS600LWD and PAS600PWD natively have no IEEE 802.15.4 or Wi-Fi wireless network capability.

IEEE 802.15.4 and Wi-Fi wireless networks can be permanently and concurrently disabled in other Panel Server Universal models and in Advanced models. **Once the wireless networks are disabled via this command, it is permanent and cannot be undone.** Neither a factory reset, nor a backup restore can activate the radio capabilities again. If an IEEE 802.15.4 or Wi-Fi network is required, the Panel Server must be replaced by a new one.

The permanent deactivation of the wireless networks is not saved in the backup file of Panel Server configuration (see detailed topic, page 180).

Availability

This function is available on Panel Server Universal (except WD models, which have no wireless capability) and Panel Server Advanced.

Setting the Parameters

Permanent deactivation of wireless networks is set on the EcoStruxure Panel Server webpages, at **Settings > Security > Network Management > Wireless networks disable**.

Deactivating Wireless Networks Permanently

NOTICE

PERMANENT LOSS OF COMMUNICATION WITH WIRELESS DEVICES

Permanent deactivation of wireless networks permanently disables communication with wireless devices. Only follow this procedure if you are sure you do not want to communicate with wireless devices in the future.

Failure to follow these instructions can result in unintentional loss of communication.

To permanently and concurrently disable the IEEE 802.15.4 and Wi-Fi wireless networks in the Panel Server, proceed as follows:

1. In the **Network Management** webpage, click **Disable all wireless networks**.
2. Read the pop-up message carefully before confirming or cancelling the deactivation in the window that appears.

   Result: After confirming deactivation, the Panel Server automatically reboots. After rebooting, **both types of wireless network are permanently deactivated** in the Panel Server and indicated as such on the webpages. The deactivation is irreversible.

EcoStruxure Panel Server General Functions

What’s in This Part

Data Sampling 118
Data Publication 122
Alarm Management 139
Control Functions and Commands 145
Custom Models for Downstream Modbus Devices (Universal and Advanced Models) 153
Local Energy Server Functions (Advanced Model) 158

Data Sampling

Presentation

The data sampling function on Panel Server samples data from connected devices at a defined frequency for a defined set of measurements. The frequency and measurements depend on the configuration of the function, set either by a connected cloud application or manually in the Panel Server webpages.

The Panel Server provides the ability to use a default sampling configuration, including a predefined set of measurements and associated sampling frequency depending on the connected devices.

Once data sampling is activated, it is possible at any time to permanently delete the sampled data for a specific measurement of a given device.

For Panel Server Entry and Universal, the sampled data is pushed to a buffer before being published. The buffer stores data for up to two weeks and publishes to the cloud application, SFTP or HTTPS server when data publication is activated or when the connection is restored after an interruption.

> **NOTE:** Data stored in the buffer are used only for data publication and cannot be accessed by users through the webpages.

For Panel Server Advanced, the data is logged in the Panel Server, page 159 to support the local energy server functions (see detailed topic, page 158).

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

Access data sampling settings on the EcoStruxure Panel Server webpages, at **Settings > Data Management > Data sampling**.

Before activating data sampling: Enable the default sampling configuration by switching on the **Use default sampling configuration** toggle button, or manually configure sampling by setting the sampling frequency and measurements individually, page 119.

Data Sampling Configuration from Cloud Application

When a connection to a cloud application is enabled, data sampling is automatically activated and configured by the cloud system. The settings are not editable (read only) with Panel Server webpages.

Data measured on the connected devices is sampled and published to the cloud application.

Default Data Sampling Configuration

The default sampling configuration for each device includes the most commonly used data for its device type.

Manual Data Sampling Configuration

Manual data sampling allows you to configure the measurements to be sampled for each device in the system:

- Modbus devices
- Wireless devices
- Input/output devices

After the commissioning of all the devices connected to the Panel Server, the choice of measurements and sampling period can be set individually for each device in the **Settings > Data Management** webpage:

1. In the device list, select the means to group the devices by clicking the list icon:
   - Usage (default)
   - Zone
2. For each device, click the device name.
3. Click **Data**.
4. Select or deselect sampling for every measurement with the **Data sampling** checkbox.
5. Select the sampling period for the measurement. Refer to Changing the Data Sampling Frequency, page 120, if relevant.
6. Click **Save** to apply changes.

   IMPORTANT: Applying the changes may take up to a few minutes, during which pages and functions are not accessible until the pop-up message disappears.

NOTE: If applicable, a message describing the oversampling error along with the oversampled measurements is displayed.

Calculation of Valid Configurations for Data Measurements

Consider how much data is being sampled across the devices when defining the sampling parameters for the system. To maintain system performance, it is recommended to follow these performance criteria:

- A maximum of 5,000 simultaneous individual data points from different devices whatever the type (wireless, Modbus-SL, or Modbus TCP/IP, input/output devices)
- A maximum of 500 samples per minute
- A maximum of 500 individual alarms for monitoring and sending email notifications (with a maximum of 300 of those from Modbus-SL devices)

  NOTE: Any remote configuration that tries to enable more than these limits is rejected.

The following table shows examples of data sampling configurations and indicates if they are valid or not:

Number of devices (A)	Number of measure-ments (B)	Sampling period (min) (C)	Total number of simultane-ous data points (A x B)	Samples per minute (A x B) / C	Number of alarms	Valid configuration
30	30	15	900	60	**550**	No - number of alarms > 500
30	170	15	**5,100**	340	90	No - total number of simultaneous data points > 5,000
30	30	1	900	**900**	90	No - samples per minute > 500
30	30	15	900	60	90	Yes: - total number of simultaneous data points < 5,000 - samples per minute < 500 - number of alarms < 500

The following data sampling information is displayed at **Settings > Data Management > Data sampling information** to provide assistance with sampling calculation:

- Data maintenance status
- Number of sampled measurements
- Maximum number of allowed sampled measurements
- Number of samples per hour
- Maximum number of allowed samples per hour

Changing the Data Sampling Frequency

For Panel Server Advanced, when the sampling period (frequency) is changed locally or by a remote configuration, historical logged data points are retained and migrated to comply with the new sampling period, with the following results:

- Reducing the frequency (for example, changing the period from 5 minutes to 10 minutes): The data points relevant to the reduced frequency are retained. Intermediate data points are deleted.

  NOTICE

  HAZARD OF LOSS OF DATA

  Reducing the sampling frequency results in the permanent loss of intermediate historized data points.

  Perform a data log export before reducing the frequency to avoid losing data.

  Failure to follow these instructions can result in loss of data

  For more information about exporting data, refer to Exporting Data Locally, page 166.
- Increasing the frequency (for example, changing the period from 10 minutes to 5 minutes): Data points for which no historical data exists are extrapolated (duplicated) from existing historical data (data points on either side), which may create non-linear trends where linear trends are expected. These data points are indicated as **Approximate value** in the **Trending** webpage graphs and charts.

Data Sampling Activation and Flushing

The following table describes the settings for **Data Sampling**.

Parameter	Description
Sampling activation	Used to activate/deactivate data sampling by the Panel Server. • Click button **Activate sampling** to activate the function. • Click button **Deactivate sampling** to deactivate the function.
Use default sampling configuration	Used to set automatically the sampling frequency and select measurements depending on the device model (enabled by default). If it is disabled before discovering or adding devices, you have to manually set sampling for each device. Refer to Manual Data Sampling Configuration, page 119.
Flush data	Used to delete all sampled data. To delete data: 1. Deactivate sampling. 2. Click button **Flush data**. 3. Confirm the data flush request by clicking **Confirm** in the popup message. **NOTE:** During the operation, which may take up to a few minutes, the following pages and functions are not accessible due to data maintenance operation: • Home page dashboard • Trending - device and aggregated data views • Custom models - custom model updates • CSV export • Backup and restore • Data sampling • Measurement sampling

Delete Sampled Data for Specific Measurement

To delete sampled data for a specific measurement of a single device, proceed as follows in the **Settings > Data Management** webpage:

1. In **Device list**, select the device.
2. In the table, navigate to the data measurement you want to delete.
3. Click the corresponding bin icon on the right.
4. Confirm the data flush request by clicking **Confirm** in the popup message.

   Result: All the sampled data of this measurement for this device are flushed permanently and cannot be retrieved.

Data Publication

What's in This Chapter

Publication on Schneider Electric Cloud 123
Publication on SFTP Server 127
Publication on HTTPS Server 130
File Format of Publications 133
Publication of Emails for Alarms (Advanced Model) 135
Publication on SFTP Server and Email Notification for Alarms (Advanced Model) 137
Publication on HTTPS Server and Email Notification for Alarms (Advanced Model) 138

Presentation

Data publication allows you to publish sampled data from connected devices (Modbus, wireless or input/output) using one of the following methods:

- **Schneider Cloud services**
- **SFTP**
- **HTTPS**

With Panel Server Advanced, you can also activate email notifications on active alarms.

NOTE: When **Schneider Cloud services** is activated, data publication on SFTP or HTTPS servers are no longer available.

Set up data sampling, page 118 before activating data publication. Data sampled before activation of data publication is also published, with the following limits:

- Panel Server Entry and Universal: up to two weeks of sampled data
- Panel Server Advanced: up to three months of sampled data. Previously logged data is retained, up to a maximum of 788,400,000 data points, which is equivalent to approximately three years of data, based on 500 data points sampled per minute across all connected devices.

Publication Methods

You can select the method and activate data publication from Panel Server on the EcoStruxure Panel Server webpages, at **Settings > Data publication > Publication method**:

- Select **Schneider Cloud services** to send the sampled data to the Schneider Electric cloud. See detailed topic, page 123.
- Select **SFTP** to send the sampled data to an SFTP server. See detailed topic, page 127.
- Select **HTTPS** to send the sampled data to an HTTPS server. See detailed topic, page 130.
- Select **Email service for alarms** to send email notifications on active alarms (Panel Server Advanced). See detailed topic, page 135.
- Select **SFTP & Email for alarms** to activate SFTP publication or to combine both services (Panel Server Advanced). See detailed topic, page 137.
- Select **HTTPS & Email for alarms** to activate HTTPS publication or to combine both services (Panel Server Advanced). See detailed topic, page 138.

Publication on Schneider Electric Cloud

Presentation

The publication to cloud function allows you to send sampled data and alarm information from connected devices to Schneider Electric cloud services such as EcoStruxure Energy Hub (part of EcoStruxure Building Activate), EcoStruxure Asset Advisor, and EcoStruxure Resource Advisor.

The data is published as a .json file. For more information, refer to File Format of JSON Publication, page 134.

When **Schneider Cloud services** is activated, data publication on SFTP or HTTPS servers is no longer available.

> **NOTE:** Schneider Electric cloud services and service of publication of emails for alarms, page 135 are mutually exclusive, that is, both features cannot be enabled concurrently.

For details about alarms available on each device, refer to spreadsheet DOCA0330EN *EcoStruxure Panel Server - Alarm File* or refer to the user guide of the selected device.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

The publishing function is set on the EcoStruxure Panel Server webpages, at **Settings > Data Publication > Publication method > Schneider Cloud services**.

To publish data in the cloud, the Panel Server network settings must allow access to the internet (cloud). For example, DNS must be configured and a proxy setting may be needed. The firewall on your network may also need to be open to allow access to the Schneider Electric servers via port 443.

Enabling Schneider Electric Cloud Infrastructure

To enable Panel Server to access services of Schneider Electric cloud infrastructure, the access to the following URLs and ports must be authorized in LAN protection configuration:

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. **NOTE:** It is required with Panel Server with firmware version up to 002.007.000.
vpn0.prod.struxurewarecloud.com	HTTPS (TCP port 443)	Allows Schneider Electric Customer Care Center to remotely access the Panel Server webpages through VPN. **NOTE:** It is required with Panel Server with firmware version greater than or equal to 002.008.000.
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.

Cloud Connection Settings

The following table describes the settings.

Parameter	Description
Schneider Cloud service applications management	Button **Connect**/**Disconnect** to connect and disconnect the Panel Server from the Schneider Electric cloud.
Connection status	Shows the Panel Server connection status to the cloud: • **Not connected** **NOTE:** If the Panel Server does not succeed in connecting to the cloud, check that communication settings are correctly set (for example, proxy required but not defined) and that the date and time synchronization mode is set to **Cloud** (see Troubleshooting, page 262). • **Connection in progress** • **Connected** The service status icon in the header is updated accordingly. For details, refer to Service Status List (Detail), page 205.
Connection diagnostics	When **Connection status** displays **Connected**, shows diagnostic of connection to the cloud: • **Device activated** indicates that the Panel Server is connected to the cloud services. • **Device not registered** indicates that the Panel Server is not recognized by the cloud services. • **Network unreachable** indicates that the Panel Server is not able to reach the Schneider Electric cloud platform. Check your network configuration. Refer to Troubleshooting, page 261. • **Bad credentials** indicates that the security certificates used to connect to the Schneider Electric cloud platform could not be validated. Check that date and time synchronization mode has been set as **Cloud** on the Panel Server webpages or EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.
Panel Server Identification	Displays the following information: • **Serial number**: unique identifier of the device • **Device code**: Panel Server credentials, used for secure claiming of device in EcoStruxure Energy Hub (part of EcoStruxure Building Activate) You can copy and paste this information to identify your device in other applications. **NOTE:** The device code represents the credentials of the Panel Server. Treat this information as confidential.
Topology and publication period	**Publish topology** button used to send the list of the devices connected to the Panel Server to the cloud, as well as information such as device name and label entered at commissioning, available measurements, and usage or other contextualization information. **NOTE:** Topology does not contain personal data. Schneider Electric does not scan, nor use, nor sell this data. This data is for the sole usage of the customer. Displays the following information: • **Last remote configuration status**: indicates if the last remote configuration was successful • **Last successful remote configuration date** The **Publication period** is displayed. It is set by the cloud service and not editable.
Remote control	**Enable remote control**: click the toggle switch to enable this function. For more information, refer to Remote Control and Scheduling From Cloud, page 146. **Schedule(s) from Cloud under execution**: Displays **Yes** or **No**

Connecting to the Schneider Electric Cloud

To publish data and alarms on the Panel Server to Schneider Electric cloud:

1. In the **Publication** webpage, select **Publication method > Schneider cloud services** and click **Connect**.
   The **Cloud service** status icon in the webpage header is blue.
2. Wait until **Connection status** indicates **Connected**.
3. Click **Publish topology** to send information about the Panel Server and connected devices to the cloud.

   IMPORTANT: Every time you change the configuration of Panel Server or the connected devices, check with the cloud application whether the topology needs to be republished.

   Result: The cloud service sends back a remote configuration to the Panel Server. The remote configuration imposes the selection of measurements and alarms, and the sampling and publisher configuration. The settings are not editable (read only) with Panel Server webpages.

   NOTE: During application of the remote configuration, the data migration process may be triggered if the data measurement frequency is modified. As a result, a progress bar may be displayed several times, corresponding to different sections of the configuration. This is normal behavior.
4. Check the **Cloud service** icon in the webpage header, page 205:
   - Green: valid remote configuration
   - Red: invalid remote configuration

   NOTE: If a remote configuration of the Panel Server from cloud services attempts to enable more than 5,000 measurements, or 500 samples per minute or 500 alarms (with a maximum of 300 from Modbus SL devices), the configuration is rejected.

   IMPORTANT: The first publication to the cloud happens as follows:
   - Panel Server Universal and Entry: 1 hour after the remote configuration is applied successfully on the Panel Server
   - Panel Server Advanced models: 10 minutes after the remote configuration is applied successfully on the Panel Server

   The **Cloud service** icon changes from blue to green when the remote configuration is successfully applied, and a first publication cycle is successful.

Disconnecting from Cloud Services

To temporarily disconnect Panel Server from Schneider Electric cloud:

1. Click **Disconnect**.
2. Wait until **Connection status** indicates **Not connected**.
   Result: The service status icon in the header will become blue after disconnection from the cloud.

Publication on SFTP Server

Presentation

Panel Server provides a connection to an SFTP server.

When data sampling and publication to SFTP are activated, the sampled data of devices is published to the SFTP server in json or csv files. A maximum of two weeks of data (Entry or Universal) or three months of data (Advanced) is published to the SFTP server. If data sampling was activated before this period, older data is not published.

Alarms are managed as follows when SFTP publication is active:

- Alarms can be monitored and displayed in Panel Server webpages.
- Alarms are not published in the CSV or JSON files.
- Alarms can be enabled for email notification.

When SFTP publication is active, data publication on cloud services or HTTPS is not available.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

Publishing function is set on the Panel Server webpages:

- For Panel Server Entry and Universal at **Settings > Data Publication > Publication method > SFTP**
- For Panel Server Advanced at **Settings > Data Publication > Publication method > SFTP & Email for alarms**

Fill in the **Connection information** and **Publication settings** described in the following tables.

SFTP Publication Settings

The following table describes the settings.

Parameter	Settings	Description
Connection information	**Server**	The host name of the SFTP server can be defined as the IP address value or as, for example, `mysftpserver.mydomain.com`.
	Port	Used to define the SFTP server TCP port. It is usually set to 22.
	Path	Used to enter the path to use on the SFTP server for data publishing. For example, if `/home/user/` is the default directory for the SFTP server, then the path configured with `/mySFTPPath` will publish on `/home/user/mySFTPPath`.
	User ID	Used to enter the SFTP user account name for the user account on the target SFTP server.
	Authentication method	Used to select the authentication method to use when connecting to the SFTP server: • **By password** • **By key**

Parameter	Settings	Description
	Password	Used to type the password for SFTP server access.
	Import key file	Button used to upload to Panel Server a file containing the encrypted password to use to connect to the SFTP server. Displayed when authentication method is by key.
	Test connection	Button used to test connection to the SFTP server.
Publication settings	**Publication format**	Used to select the exported file format: • **JSON** (for details, page 134) • **CSV** (for details, page 133)
	Publication period	Used to select the publication frequency to the SFTP server (default setting: 10 min). **NOTE:** The publication period is calculated from the end of one publication to the start of the next. The time needed for a publication varies depending on the quantity of data to be analyzed and published.
	Include previously historized data toggle switch	• For Panel Server Entry or Universal: used to include all data for the past two weeks, or from the beginning of data sampling if less than two weeks. • For Panel Server Advanced: used to include all data for the past three months, or from the beginning of data sampling if less than three months.
	Start	Button used to launch data publication to the SFTP server. Refer to Date and Content of the First Data Publication, page 128.

Date and Content of First Data Publication

The date and time of the first publication depends on the publication period set, as indicated in the following table.

Publication period	First publication date and time and start of data collection
Weekly	00:00 on first Thursday following publication launch
Daily	00:00 following publication launch
12h	00:00 following publication launch
4h	At the next full hour (for example, launch publication at 10:47, publication starts at 11:00)
3h	At the next full hour (for example, launch publication at 10:47, publication starts at 11:00)
2h	At the next full hour (for example, launch publication at 10:47, publication starts at 11:00)
1h	At the next full hour (for example, launch publication at 10:47, publication starts at 11:00)
10 min	At the next interval of 10 minutes (for example, 10:10, 10:20, 10:30 etc)

When the **Include previously historized data** toggle switch is green, the first publication will contain:

- For Entry or Universal: all data for the past two weeks, or from the beginning of data sampling if less than two weeks.
- For Advanced: all data for the past three months, or from the beginning of data sampling if less than three months.

Connecting to SFTP Server

To connect the Panel Server to an SFTP server:

1. On the SFTP server, configure a connection for the publication of data from the Panel Server.
2. In the Panel Server webpage **Settings > Network communication > Proxy**, click **HTTP proxy** or **HTTPS proxy** and enter the required information, page 84.
3. In the **Settings > Data publication** webpage, select the **Publication method** as follows:
   - For Panel Server Entry and Universal select **SFTP**
   - For Panel Server Advanced select **SFTP & Email for alarms**

   By default, SFTP data publications (CSV or JSON file format) are stored at the top of the hierarchical file tree of the SFTP server. If you customize the file path for the data storage, make sure that the path is created and validated on the SFTP server. For more information, refer to the user guide of your SFTP server.
4. To connect to the SFTP server, enter the user ID and password or user ID and SSH key in PEM (Privacy Enhanced Mail) format in the **Connection information** section. Save your settings by clicking the icon at bottom right of the screen and selecting **Save**. The **SFTP** status icon in the webpage header is blue.
5. Click **Test connection**. The list of SSH key exchanges and ciphers supported by the Panel Server is available in Appendix E, page 291.

   When using SSH key authentication, the key must be provided in PEM format (default setting when relying on OpenSSH version less than 7.8).

   NOTE: If it is the first time the Panel Server connects to this SFTP server, a message appears and requests that you confirm the authenticity of the SFTP server.
6. Once the test is performed, the Panel Server webpage displays information:
   - In case of success, a file has been successfully uploaded on the SFTP server.
   - In case of dysfunction, check the SFTP server parameters, user credentials, and write access privileges on the SFTP server.
7. To publish data, set **Publication settings** and click **Start**.

   Result: The **SFTP** status icon in the header turns green and the sampled data of devices, related to the selected sampling period, is published to SFTP, in CSV file format, page 133 or JSON format, page 134.
8. If you update the SFTP server, the SFTP server fingerprint changes. In this case, click **Test connection** to allow you to connect to the SFTP server again.

   NOTE: The **SFTP** service is displayed in the **Service status** drop-down list in the webpage header. The status is indicated by the icon color. For details, refer to Service Status List (Detail), page 205.

Disconnecting from Publishing Services

To disconnect Panel Server from the SFTP server, click **Stop**. The **SFTP** status icon in the header turns blue.

Disconnecting from the service allows you to connect to another publishing service.

Publication on HTTPS Server

Presentation

EcoStruxure Panel Server provides a secure connection to an HTTPS server with a certificate authority.

When data sampling and publication to HTTPS are activated, the sampled data of devices is published to the HTTPS server in json or csv files. A maximum of two weeks of data (Entry or Universal) or three months of data (Advanced) is published to the HTTPS server. If data sampling was activated before this period, older data is not published.

When HTTPS publication is active, data publication on cloud services or SFTP is not available.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

Publishing function is set on the Panel Server webpages:

- For Panel Server Entry and Universal at **Settings > Data Publication > Publication method > HTTPS**
- For Panel Server Advanced at **Settings > Data Publication > Publication method > HTTPS & Email for alarms**

Fill in the **Connection information** and **Publication settings** described in the following tables.

HTTPS Publication Settings

The following table describes the settings.

Parameter	Settings	Description
Connection information	**Server**	The host name of the HTTPS server can be defined as the IP address value or as, for example, `myHTTPSserver.mydomain.com`.
	Port	Used to define the HTTPS server TCP port.
	Path	Used to enter the path to use on the HTTPS server for data publishing. For example, if `/home/user/` is the default directory for the HTTPS server, then the path configured with `/myHTTPSPath` will publish on `/home/user/myHTTPSPath`.
	Field name	Used to specify the value of the name parameter part of the form-data section included in the file that is being published. By default the filed name is *datafile1*. The field name is necessary to communicate with the HTTPS server.
	Authentication method	Radio button used to enable ID authentication. Setting not editable.
	Username	Used to enter the HTTPS user account name for the user account on the target HTTPS server.
	Password	Used to type the password for HTTPS server access.

Parameter	Settings	Description
	Test connection	Button used to test the connection to the HTTPS server.
Publication settings	**Publication format**	Used to select the exported file format: • **JSON** (for details, page 134) • **CSV** (for details, page 133)
	Publication period	Used to select the publication frequency to the HTTPS server (default setting: 10 min). **NOTE:** The publication period is calculated from the end of one publication to the start of the next. The time needed for a publication varies depending on the quantity of data to be analyzed and published.
	Include previously historized data toggle switch	• For Panel Server Entry or Universal: used to include all data for the past two weeks, or from the beginning of data sampling if less than two weeks. • For Panel Server Advanced: used to include all data for the past three months, or from the beginning of data sampling if less than three months.
	Start	Button used to launch data publication to the HTTPS server. Refer to Date and Content of the First Data Publication, page 131.

Date and Content of the First Data Publication (Panel Server Advanced)

The date and time of the first publication depends on the publication period set, as indicated in the following table.

Publication period	First publication date and time and start of data collection
Weekly	00:00 on first Thursday following publication launch
Daily	00:00 following publication launch
12h	00:00 following publication launch
4h	At the next full hour (for example, launch publication at 10:47, publication starts at 11:00)
3h	At the next full hour (for example, launch publication at 10:47, publication starts at 11:00)
2h	At the next full hour (for example, launch publication at 10:47, publication starts at 11:00)
1h	At the next full hour (for example, launch publication at 10:47, publication starts at 11:00)
10 min	At the next interval of 10 minutes (for example, 10:10, 10:20, 10:30 etc)

When the **Include previously historized data** toggle switch is green, the first publication will contain:

- For Entry or Universal: all data for the past two weeks, or from the beginning of data sampling if less than two weeks.
- For Advanced: all data for the past three months, or from the beginning of data sampling if less than three months.

Connecting to HTTPS Server

To connect the Panel Server to an HTTPS server:

1. On the HTTPS server, configure a connection for the publication of data from the Panel Server.
2. In **Settings > Network communication > Proxy** , click **HTTPS proxy** and enter the required information, page 84.
3. In the **Settings > Data publication** webpage, select the **Publication method** as follows:
   - For Panel Server Entry and Universal select **HTTPS**
   - For Panel Server Advanced select **HTTPS & Email for alarms**

   By default, HTTPS data publications (CSV or JSON file format) are stored at the top of the hierarchical file tree of the HTTPS server. If you customize the file path for the data storage, make sure that the path is created and validated on the HTTPS server. For more information, refer to the user guide of your HTTPS server.

   NOTE: The **HTTPS** status icon in the webpage header is blue.
4. Before connecting to the HTTPS server, fill in the information in the **Connection information** section. Save your settings by clicking the icon at bottom right of the screen and selecting **Save**.
5. Click **Test connection**.

   NOTE: If it is the first time the Panel Server connects to this HTTPS server, a message appears and requests that you confirm the authenticity of the HTTPS server. Check that your HTTPS server certificate is issued by one of the trusted certificate authorities (Appendix F, page 293). Your IT department should be able to provide this information. If the server certificate does not comply, do not publish over HTTPS.
6. Once the test is performed, the Panel Server webpage displays information:
   - In case of success, a file has been successfully uploaded on the HTTPS server.
   - In case of dysfunction, check the HTTPS server parameters, user credentials, and write access privileges on the HTTPS server.
7. To publish data, set **Publication settings** and click **Start**.

   Result: The **HTTPS** status icon in the webpage header turns green. The sampled data of devices, related to the selected sampling period, is published to HTTPS, in the CSV file format, page 133 or JSON format, page 134. A maximum of two weeks of data (Entry or Universal) or three months of data (Advanced) is published to the HTTPS server. If data sampling was activated before this period, older data is not published.
   The **HTTPS** status icon in the webpage header turns red if the publication .is inoperative.
8. If you update the HTTPS server, the HTTPS server fingerprint changes. In this case, click **Test connection** to allow you to connect to the HTTPS server again.

   NOTE: The HTTPS service is displayed in the **Service status** drop-down list in the webpage header. The status is indicated by the icon color. For details, refer to Service Status List (Detail), page 205.

Disconnecting from Publishing Services

To disconnect Panel Server from the HTTPS server, click **Stop**. The **HTTPS** status icon in the header turns blue.

Disconnecting from the service allows you to connect to another publishing service.

File Format of Publications

Presentation

The file format of published files depends on the choice of publication method:

- Schneider Electric cloud services: json file format
- SFTP and HTTPS: select json or csv file format on Panel Server webpages

File Format of CSV Publication

One .csv file contains:

- Data relating to a single downstream device
- All measurements configured with the same sampling period for that device
- Data from a maximum of 24 hours of sampling

The name of the CSV files that are exported follows the naming convention *ReducedID_DeviceName_DateTime_IndexNumber.csv* where:

- *ReducedID* is the internal identifier of the device, which ensures that files produced are unique for devices that would share the same name (for example, *10_mb*, *21_zd*).
- *DeviceName* is the name given to the downstream device.
- *DateTime* is the time stamp corresponding to when the file was published, expressed down to the millisecond in the format YYYYMMDDhhmmssSSS.
- *IndexNumber* in the format _<nn> indicates the number of the file in the total number of files for a single publication (same ID, same device name and same timestamp). If there are 20 files in the publication, they are numbered _1 to _20.
- Only the following characters are allowed in the .csv file name : UTF-8 and basic ASCII (32 to 7F, excluding \ / : * ? " < > |). Any non-supported characters will be replaced by **~**.

Example: Considering the following file name:
11_mb_F160 3P 3P+N_202412161020_19.csv where:

- *ReducedID* is **11_mb**.
- *DeviceName* is **F160 3P 3P+N**, name of the device.

  NOTE: This name is the default value (product model) if the user has not updated it.
- *DateTime* is **202412161020**, which means that the file was published on December 16, 2024 at 10:20.
- *Index number* is _19, which means that the file is the 19th file in the publication.

The .csv file content only supports UTF-8 standard character encoding for device name, event name, measurement name, and file name.

Quotation marks in all data fields of the .csv file help ensure compatibility with special characters.

For details and examples of the .csv file, see *Appendix D SFTP and HTTPS Publication File Formats*, page 288.

File Format of JSON Publication

One .json file contains measurements of multiple downstream devices configured with the same sampling period.

Each file contains the data from 24 hours of sampling, up to a limit of 256 KB of data.

The name of the JSON file that is exported follows the naming convention *DateTime_IndexNumber.json* where:

- *DateTime* is the time stamp corresponding to when the file was published, expressed down to the millisecond in the format YYYYMMDDhhmmssSSS.
- *IndexNumber* in the format _<nn> indicates the number of the file in the total number of files for a single publication (same ID, same device name and same timestamp). If there are 20 files in the publication, they are numbered _1 to _20.

For an example of a .json file, see *Appendix D SFTP and HTTPS Publication File Formats*, page 288.

Publication of Emails for Alarms (Advanced Model)

Presentation

The Panel Server Advanced allows you to trigger an email notification when an alarm becomes active.

To execute the email service tasks, the Panel Server Advanced must be connected to the Internet through an Internet service provider or a firewall with or without proxy management. The email service is provided through the Schneider Electric cloud infrastructure to provide a high quality of service.

To perform email notification, proceed as follows:

1. Activate the email service, page 135.

   NOTE: Service of publication of emails for alarms and Schneider Electric cloud services, page 123 are mutually exclusive, that is, both features cannot be enabled concurrently.
2. Create the list of recipients, page 135.
3. Select the alarms that trigger an email notification when activated, page 140.
4. Send email notification, page 136.

If the Panel Server Advanced does not succeed in connecting to the cloud services, see Troubleshooting, page 262.

Availability

This function is available on Panel Server Advanced.

Setting the Parameters

Publishing function is set on the EcoStruxure Panel Server webpages, at **Settings > Data publication > Publication method > Email service for alarms**.

Activating the Email Service

To activate the email notification service, click the **Activate** button.

Result: Connection status turns to **Connection in progress** and the **Email service** status icon in the webpage header is blue.

NOTE: Email service is displayed in the **Service status** drop-down list in the webpage header. The status is indicated by the icon color. For details, refer to Service Status List (Detail), page 205.

Creating Recipients

When email notification service is activated, you can complete the list of recipients with a maximum of 10 different recipients. In **Email recipients**, enter the email address for each recipient and click the **Save** button. The list can be edited or deleted.

An email address must be less than 128 characters.

To test the function, you can send an email to one selected recipient.

Recommendations for Email Addresses

NOTICE
POTENTIAL COMPROMISE OF PERSONAL DATA Do not enter personal email addresses in the list of recipients. **Failure to follow these instructions can result in privacy-related issues.**

Schneider Electric recommends that you use professional or generic email addresses to send alarms to avoid any privacy-related issue.

The email addresses are sent to the Schneider Electric cloud when an alarm occurs and only kept for the lifetime of the transaction. Email addresses are ephemeral data from the cloud point of view. The Panel Server keeps the email addresses locally and transmits them each time an alarm occurs.

Schneider Electric does not keep or use the email addresses for any other purpose than sending alarms and events.

Testing Emails

When the email notification service is activated, one or several recipients have been created in the recipient list, and one recipient have been selected from the list, then click the **Send test email** button.

Result: The **Email service** status icon in the webpage header turns green and an email notification is sent to each recipient in the list for all selected alarms.

Sending Email Notification

When email notification service is activated, all alarms that have been enabled trigger a notification to the recipients defined in the list. You cannot select the emails to be sent to some of the recipients.

The address from the Internet service provider has the format `noreply@xxx.mail.ecostruxure.se.com`. Email messages are only in English whatever the language selected for the Panel Server webpages or EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.

> **NOTE:** A variable period of time can occur between an event occurring and the email being received, depending on different factors, including domain name and network quality.

Publication on SFTP Server and Email Notification for Alarms (Advanced Model)

Presentation

This service combines the publication to SFTP server and email notification for alarms.

For more information on each individual service, see the detailed topic:

- Publication on SFTP Server, page 127
- Publication of Emails for Alarms, page 135

Availability

This function is available on Panel Server Advanced.

Setting the Parameters

Publishing function is set on the EcoStruxure Panel Server webpages, at **Settings > Data publication > Publication method > SFTP & Email for alarms**.

Publication on HTTPS Server and Email Notification for Alarms (Advanced Model)

Presentation

This service combines publication to HTTPS server and email notification for alarms.

For more information on each individual service, see the detailed topic:

- Publication on HTTPS server, page 130
- Publication of Emails for Alarms, page 135

Alarm Management

What's in This Chapter

Displaying and Publishing Alarms..... 140
Alarm File..... 141
Alarm Description..... 142

⚠WARNING

INCOMPATIBLE OR INOPERABLE EQUIPMENT

Do not rely solely on alarms for the maintenance of your equipment.

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

Displaying and Publishing Alarms

Consulting Active Alarms

This function is available on Panel Server Entry, Universal, and Advanced.

Active alarms issued by connected devices are displayed on the Panel Server webpages at **Monitoring and Control**, on the **Data** page of each device. An active alarm disappears when conditions of the alarm are no longer met.

Alarms are defined by severity:

- High severity
- Medium severity
- Low severity

For information about identifying alarm severity, refer to Alarm Icons, page 209.

Publishing Alarms

Active alarms can be published by the following methods, depending on the data publication method selected, page 122:

- Schneider Electric cloud (all models): when the Panel Server is connected to the Schneider Electric cloud, alarms are published to the cloud application. The selection of alarms is managed at the cloud level, and is available for display only at **Settings > Data management > Alarms**.
- By email (Advanced model): when the **Email service for alarms** is activated, page 135, email notifications for selected alarms, page 140 are sent to the recipient list.
- On the Panel Server webpages at **Notifications** (Advanced model): appearance and disappearance of selected alarms are displayed on the **Notifications** webpage, page 212.

Selecting Alarms for Notification and Publication by Email (Advanced Model)

For each device connected to the Panel Server Advanced, you can select or deselect the notification and publication by email of alarms issued in the case of electrical events or communication loss. By default, publication of each alarm is deselected.

A maximum of 500 alarms can be selected concurrently. Of the 500 selected alarms, a maximum of 300 can be from Modbus-SL devices.

Alarms to be published in the **Notifications** page and by email when they become active can be selected individually for each device as follows.

1. Click the device name on the Panel Server webpages, at **Settings > Data management**.
2. Click **Alarms**. The alarms are displayed in a table with a column indicating the severity. Click the double arrow icon at the top of the column to sort the alarms by severity.
3. Select/deselect an alarm for publication with the **Alarm publication** checkbox.

   NOTE: Selecting or deselecting alarms in **Settings > Data management** has no impact on the alarm bits in Modbus register.

Alarm File

The alarms available on the Panel Server webpages depend on the device type. For details about alarms available on each device, refer to spreadsheet DOCA0330EN *EcoStruxure Panel Server - Alarm File* or refer to the user guide of the selected device.

IMPORTANT:

- Concerning IO module generic function, alarm activation is enabled when the input status is 1.
- When Acti9 iATL24, OFSD or iACT24 auxiliaries are connected under an I/O Smart Link device and commissioned in the Panel Server, if the cable is disconnected from the I/O Smart Link device, a **Circuit breaker opened alarm** is triggered into the Panel Server instead of the **Communication loss alarm**.

Alarm Description

The following alarms are described in detail:

- ERMS, page 142
- Communication loss, page 142
- Voltage loss, page 142
- Overcurrent at voltage loss, page 142
- 80% of nominal current, page 143
- 50% of nominal current, page 143
- 45% of nominal current, page 143
- Zero current, page 143
- Undervoltage (80%), page 144
- Overvoltage (120%), page 144

ERMS Alarm

For MasterPacT NT/NW circuit breakers, the ERMS (Energy Reduction Maintenance Setting) feature is limited. ERMS alarm is compatible from Panel Server only when ERMS application is configured on IO module 1. When the application switch of IO module 1 is set to position 3, you may receive a notification of ERMS activation due to electrical noise on the IO module. It does not necessarily indicate that the ERMS mode is activated. Schneider Electric recommends always confirming by checking the present alarm status from the Panel Server webpages and ERMS status indicator on the MasterPacT NT/NW circuit breaker. For more information, refer to NHA67346 *Energy Reduction Maintenance Setting (ERMS) System Installation and User Guide*.

Communication Loss

This alarm indicates that the gateway has lost the communication with a device.

The communication loss happens if the gateway has not received packets for a period of time equal to 9 times the communication period of the device.

The alarm automatically disappears as soon as the wireless device is connected to the RF network.

Voltage Loss

This alarm indicates that the circuit on which a wireless device is installed is no longer under voltage. The cause of the voltage loss can be a manual opening of the circuit, a mains power outage, or a circuit breaker tripping. The wireless device sends the voltage loss alarm to the gateway as soon as it happens, and before being fully de-energized, meaning that the alarm response-time does not depend on the wireless communication period. The alarm will automatically disappear as soon as the wireless device is powered again.

Overcurrent at Voltage Loss

This alarm indicates that an overcurrent occurred during the time of voltage loss. This alarm occurs only if the option is activated. The alarm is managed only if the nominal current or the breaker rating (Ir) of the associated protection device has been set.

NOTE: The RMS value of the current during the voltage loss is available in the Modbus table. For more details, refer to DOCA0241EN *EcoStruxure Panel Server - Modbus File* . These measurements help to diagnose the root cause of the overcurrent.

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

Make sure that the cause of the overcurrent is identified and is fixed before closing the circuit.

Failure to follow these instructions will result in death or serious injury.

80% of Nominal Current

This alarm indicates that the load current exceeded 80% of the nominal current or exceeded 80% of the associated circuit breaker rating (Ir). On polyphase circuits, the alarm triggers if the current of one of the phases meets the above conditions. The gateway manages the alarms based on the values of the currents sent by the wireless device. The response time of the alarm depends on the communication period set into the Panel Server wireless network (default = 5 seconds). The alarm automatically disappears when the load current remains below the threshold value for 15 minutes.

NOTE: Hysteresis of 10% is applied on the threshold value.

50% of Nominal Current

This alarm indicates that the load current exceeded 50% of the nominal current or exceeded 50% of the associated circuit breaker rating (Ir). On polyphase circuits, the alarm triggers if the current of one of the phases meets the above conditions. The gateway manages the alarms based on the values of the currents sent by the wireless device. The response time of the alarm depends on the communication period set into the Panel Server wireless network (default = 5 seconds). The alarm automatically disappears when the load current remains below the threshold value for 15 minutes.

NOTE: Hysteresis of 10% is applied on the threshold value.

45% of Nominal Current

This alarm indicates that the load current exceeded 45% of the nominal current or exceeded 45% of the associated circuit breaker rating (Ir). On polyphase circuits, the alarm triggers if the current of one of the phases meets the above conditions. The gateway manages the alarms based on the values of the currents sent by the wireless device. The response time of the alarm depends on the communication period set into the Panel Server wireless network (default = 5 seconds). The alarm automatically disappears when the load current remains below the threshold value for 15 minutes.

NOTE: Hysteresis of 10% is applied on the threshold value.

Zero Current

This alarm indicates that the load current value is 0 A. On polyphase circuits, the alarm happens if the current of one of the phases meets the above condition. The gateway manages the alarms based on the values of the currents sent by the wireless device. The response time of the alarm depends on the communication period set into the PowerTag system wireless network (default = 5 seconds). Zero

current alarm allows the monitoring of full time running loads. The alarm automatically disappears when the load current is greater than 0 A on all phases.

Undervoltage (80%)

This alarms triggers when a phase-to-neutral voltage or a phase-to-phase voltage falls below the threshold of 80% of the nominal value. The alarm automatically disappears when the voltage remains greater than 88% of the nominal value (a hysteresis of 10% is applied).

Overvoltage (120%)

This alarms triggers when a phase-to-neutral voltage or a phase-to-phase voltage exceeds the threshold of 120% of the nominal value. The alarm automatically disappears when the voltage remains lower than 108% of the nominal value (a hysteresis of 10% is applied).

Control Functions and Commands

What's in This Chapter

Remote Control and Scheduling From Cloud..... 146
Sending Commands From Panel Server Webpages 148
Digital Inputs (PAS600L, PAS600LWD, PAS800L) 149

Remote Control and Scheduling From Cloud

Presentation

⚠WARNING

UNEXPECTED START OF OPERATION

Only allow remote and/or scheduled control of loads for non-critical electrical loads that can safely be left unattended.

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

Remote control allows you to manage non-critical electrical loads remotely or send commands when the EcoStruxure Panel Server is connected to the Schneider Electric cloud service.

The function is supported for the following devices:

- PowerTag C IO devices
- Exiway Link devices

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

The output remote control function is enabled and disabled in the EcoStruxure Panel Server webpages, at **Settings > Data Publication**.

1. Connect to the Schneider Electric cloud, page 126.
2. In **Publication method**, select **Schneider cloud services**.
3. In **Remote control**, click the toggle switch to enable and schedule remote control of outputs.
4. Save the settings.
5. Read the safety message popup and click **Confirm** or **Cancel**.

   Result: Cloud service status icon in the header turns blue.
6. Remote control and scheduling are available when **Schedule(s) from Cloud under execution** displays **Yes**.

Remote Control Orders to PowerTag C IO Devices

The function allows you to:

- Remotely execute control orders on a device connected via a PowerTag C IO device configured as contactor with feedback loop mode or impulse relay mode, by using the a Schneider Electric cloud application. For more information, refer to *Configuration of PowerTag Control Devices Through Webpages*, page 251.

- Send a control schedule when the EcoStruxure Panel Server is connected to the Schneider Electric cloud service. The schedule allows the Panel Server to remotely execute scheduled control orders, even if the connection to the cloud is interrupted.

  When a schedule is received and running, the following information is displayed on the webpages :

  - In the page header, **Control scheduling** is displayed to the right of **Cloud service**
  - At **Settings > Data publication > Remote control**, the toggle switch is green.
- Send real-time status updates of the monitored device to the Schneider Electric cloud.

Sending Commands to Exiway Link Devices

You can send the following commands to Exiway Link devices from the Schneider Electric cloud:

- Locate a device
- Disable/Enable periodic test
- Start functional test
- Switch on/switch off light
- Synchronize Exiway Link devices

Sending Commands From Panel Server Webpages

Presentation

You can send commands from EcoStruxure Panel Server webpages.

Output Control Commands to Smart Link Devices

⚠WARNING

UNEXPECTED START OF OPERATION

Only send output control commands for non-critical electrical loads that can safely be left unattended.

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

Output control commands to I/O Smart Link devices and Acti9 Smartlink Modbus-SL devices can be sent from Panel Server webpages (in data widgets at **Monitoring & Control > Input/Output**). Open and close commands are used to control non-critical electrical loads.

Individual Commands

Individual commands are executed on one device only. To do this, select a device from the device tree on the relevant webpage, indicated in the list below.

The following functions are available:

- Locate a wireless device (at **Settings > Wireless devices**).

  When the **Locate** button is clicked, the wireless device blinks for 30 seconds. Exiway Link devices blink for five minutes.
- Reset all energies per device (in data widgets at **Monitoring & Control > Wireless devices**).
- Reset peak demand per device (in data widgets at **Monitoring & Control > Wireless devices**).
- Send Exiway Link order (in data widgets at **Monitoring & Control > Wireless devices**).
  - Disable/Enable periodic test.
  - Start functional test.

Global Commands

Global commands are executed on a device family. The command is applied to all the connected devices in the family.

To execute global commands, navigate to **Monitoring & Control > Device view > Global commands**.

The function allows you to:

- Reset all peak power demands. See Monitoring and Control Menu, page 214.
- Launch synchronized tests for all Exiway Light devices. See Monitoring and Control Menu, page 214.

Digital Inputs (PAS600L, PAS600LWD, PAS800L)

Presentation

The two embedded digital inputs on Panel Server Universal PAS600L, PAS600LWD, and Advanced PAS800L are used to monitor the state of an external contact or as a pulse counter.

When configured as a pulse counter, the falling edge of the pulse is counted. Modbus registers are refreshed every 60 seconds.

Availability

This function is available on Panel Server Universal PAS600L, PAS600LWD, and Advanced PAS800L.

Digital Input Types

There are two types of digital input:

- Standard digital inputs, used to record the state of a normally open or normally closed external contact.
- Pulse digital inputs, used to count pulses delivered by a WAGES (Water, Air, Gas, Electricity, Steam) metering device compliant with standard IEC 62052-11 (minimum pulse width of 30 ms). Pulse digital inputs support up to 16 pulses/second, as per the requirements of the standard.

Each digital input can be individually configured as either standard or pulse.

Pulse Digital Input Parameters

The pulse weight and pulse unit of each pulse input can be configured using EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34, or Panel Server webpages. A pulse counter is activated when the corresponding digital input is configured as a pulse input.

The pulse weight must be calculated according to the characteristics of the pulses delivered by the meter, and the meter element unit. For the Panel Server, the pulse weight is the pulse value expressed in the meter element unit. The following table shows some examples:

Examples:

WAGES pulse value	Meter element unit	Pulse value in meter element unit	Pulse weight in webpages
125 liters	m^3	1 pulse = 0.125 m^3	0.125
1 liter	m^3	1 pulse = 0.001 m^3	0.001
10 Wh	Wh	1 pulse = 10 Wh	10
1 kWh	Wh	1 pulse = 1000 Wh	1000

Setting the Parameters

The digital inputs are set as follows:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34
- On the Panel Server webpages, at **Settings > Embedded Input Management**

Digital Input Settings

The following table describes the settings of the digital inputs:

- **Embedded input 1 (DI01)**
- **Embedded input 2 (DI02)**

Parameter	Description
Connected device	Used to select the type of each digital input (**Embedded input 1 (DI01)**/**Embedded input 2 (DI02)**): • **Not Connected** • **Pulse counter** • **Standard I/O**

Standard Input Settings

The following table describes the settings of **Embedded input 1 (DI01)** or **Embedded input 2 (DI02)** when the digital input is set to **Standard I/O**:

Type of parameter	Parameter	Description
Identification	**Name**	Enter the input name.
	Label	Enter the input label.
Configuration	**Type**	Displays the type of connected device. Setting not editable.
Status settings	**I/O Contextualization**	Select the contextualization from the list.
	Status name	If you select Custom as contextualization option, then enter the custom name for the device.
	Meaning of input = 0	Displays a value depending on the I/O contextualization selected. Enter your custom values if you select **Custom** as contextualization option.
	Meaning of input = 1	Displays a value depending on the I/O contextualization selected. Enter your custom values if you select **Custom** as contextualization option.
Contextualization data	**Commodity**	Select the commodity type in the list, as contextualization data.
	Usage	Select the usage in the list, as contextualization data.
	Zone	Select the zone in the list, as contextualization data. Click the Settings icon to: • Create a new zone • Modify a zone name • Delete a zone For more information about creating, modifying and deleting zones, refer to Zone Management, page 300.

Pulse Counter Settings

The following table describes the settings of **Embedded input 1 (DI01)** or **Embedded input 2 (DI02)** when the digital input is set to **Pulse counter**:

Type of parameter	Parameter	Description
Identification	**Name**	Enter the input name of the device.
	Label	Enter the input label as per the name plate in the network.
Configuration	**Type**	Displays the type of digital input. Setting not editable.
Pulse settings	**Meter element**	Select either a pre-defined meter element or **Custom** in the list. **NOTE:** If a meter element is selected, the meter unit, flow element, and flow unit are displayed.
	Meter element name	Enter the name of the custom meter element. **NOTE:** Displayed when **Custom** is selected.
	Meter element unit	Displays the consumption unit of the meter element. **NOTE:** Editable when **Custom** is selected.
	Flow element	Displays the name of the flow the meter element is intended for. **NOTE:** Editable when **Custom** is selected.
	Flow unit	Displays the unit of the meter element flow. **NOTE:** Editable when **Custom** is selected. Flow results for a custom element is calculated as flow per hour.
	Pulse weight	Enter the pulse weight (pulse value expressed in meter element unit). **NOTE:** Depending on the language of your browser, to add a decimal value, for example 1.125, you may need to copy and paste the value into the field.
	Preset meter value	Allows you to set a value for consumption prior to starting metering through the current Panel Server, for example, when the metering device is replaced.
Contextualization data	**Commodity**	Select the commodity type in the list, as contextualization data.
	Usage	Select the usage in the list, as contextualization data.
	Zone	Select the zone in the list, as contextualization data. Click the Settings icon to: • Create a new zone • Modify a zone name • Delete a zone For more information about creating, modifying and deleting zones, refer to Zone Management, page 300.

Consumption and Flow Calculation for Pulse Counter

When a digital input is configured as a pulse counter, the following information is available through Modbus registers and is displayed in the **Monitoring & Control** webpage:

- Consumption: total consumption since monitoring began
- Flow: instantaneous value calculated between the last two pulses

The data is calculated and stored in Modbus registers every 60 seconds.

NOTE: The Panel Server counts the pulse on the falling edge.

Consumption is calculated as (number of pulses x pulse weight) + preset meter consumption value (if any).

Example with pulse weight = 0.125: (20 pulses x 0.125 m^3) + 0 = 2.5 m^3.

Flow is calculated as the consumption between the last two pulses/ time between last two pulses (t) in seconds. As the consumption between the last two pulses is always equal to the pulse weight, this can be simplified as Pulse weight/ t.

Example: with pulse weight = 0.125 and one pulse every 3 minutes 0.125/180 = 0.00069 m^3/s.

The average power data (or average flow) between two pulses is reset to 0 after a duration d = (3 x t), where t is the time in seconds between the last two pulses received. If (3 x t) is less than 5 seconds, the duration d is five seconds.

Meter values are saved each time the value changes. Cumulative pulse count values are stored to memory after each change. The meter parameter setting dates are saved instantly to memory.

Custom Models for Downstream Modbus Devices (Universal and Advanced Models)

Presentation

NOTICE

BACKWARD COMPATIBILITY WITH EXISTING CUSTOM MODELS AFTER FIRMWARE UPDATE

After updating the Panel Server firmware, if devices associated with a custom model display erroneous data, or cannot be imported, update the custom model using EcoStruxure Power Commission Web portal tool and import it again into the Panel Server. Perform a **Switch versions and update** action for the custom model.

Failure to follow these instructions can result in erroneous data.

The Panel Server supports the use of custom models for downstream Modbus devices. A custom model can be created to manage a Modbus device that is not natively managed by the Panel Server built-in models or when a different model than the built-in one is desired.

Custom models are only dedicated to support EcoStruxure Asset Advisor EcoStruxure Resource Advisor, and EcoStruxure Energy Hub (part of EcoStruxure Building Activate) applications and Panel Server Advanced energy server functions. On other applications, custom models can be used, but only allow the visualization of device data on the monitoring screen.

Custom models are created or modified in the EcoStruxure Power Commission Web portal tool (EPC Web). The EPC Web tool contains context help to guide you.

New and modified custom models are imported in the Panel Server by using the Panel Server webpages. For more information about discovering Modbus devices automatically or manually, see Addition and Removal of Modbus Devices, page 228.

Availability

This function is available on Panel Server Universal and Advanced.

Setting the Parameters

Custom models are available on the Panel Server webpages at **Settings > Modbus devices > Custom models**.

Creating a Custom Model

Create the custom model by using the EcoStruxure Power Commission Web portal tool (EPC Web).

The custom model contains the list of measurements and alarms supported by the Modbus device connected to the Panel Server.

Custom device models can be used to add wireless devices through a parent/child architecture, page 258.

The custom device model must contain the following content. It cannot be imported into the Panel Server webpages if it does not follow these rules:

- modelingInformation
- productIdentification
- measure
- modbusMapping
- modbusDataModel

Custom models can include alarms, event names, conditions, values and severity.

Custom models can include the Modbus discovery rules, which allows the Panel Server to use custom models in addition to built-in models to discover Modbus devices. For more information about the rules, refer to the EPC Web tool.

The custom units in the custom device model must comply with the following syntax rules:

- Maximum number of characters: 16
- Use only characters from the following table.

Characters	Description
Alphanumeric characters	All upper case letters from A to Z All lower case letters form a to z All numbers from 0 to 9
/	forward slash
*	star (multiply)
-	minus
+	plus
%	percent
(	left parenthesis
)	right parenthesis
.	point
Ω	omega (ohm)
µ	mu (micro)
‘space’	the space character
°	degrees, for example °C
superscript characters	All numbers from 0 to 9 Plus and minus characters

Export the custom model to a zip file.

Importing a Custom Device Model

To import a custom device model previously created in EPC Web tool and exported in a zip file, follow this procedure:

1. From the Panel Server webpages, navigate to **Settings > Modbus devices > Custom models**.
2. Click **Import**. You can import:
   - A new custom model. This is a custom model which is not currently imported to the Panel Server and is compatible with the firmware version of Panel Server. Refer to the compatibility table, page 155.
   - A modified custom model. This is a modification of a custom model which is already imported and used by connected Modbus devices.

     NOTE: A modified version of a custom model with deprecated format is not supported for import to the Panel Server.

3. Select a custom device model stored locally in a zip file.

   The zip file can contain both new and modified custom models. Panel Server can host a maximum of two different versions with the same custom model name. Only one version (current version) is used by Modbus devices. The other version is stored as an available version in the **Custom models table**.

   NOTE: An error message is displayed if the custom model does not comply with the syntax rules (see Creating a Custom Model, page 153).

When the custom model is successfully imported, it is listed in the custom models table. A maximum of 50 custom models can be imported to the Panel Server.

A new custom model is automatically instantiated so that new Modbus devices can be added using that custom model. It is displayed as the current version in the custom models table.

For modified custom models, the new version is available for use in the custom models table. It is not automatically instantiated. Select **Switch versions and update devices** to apply the new version to selected Modbus devices.

NOTE: It is recommended to perform a backup of the Panel Server configuration before switching versions.

Custom Model Compatibility

The following table indicates compatibility between custom models in the EPC Web tool and firmware versions of Panel Server.

Date of creation of custom model	**EPC Web tool version**	**Panel Server firmware version**			
		002.000.000	**002.001.000**	**002.002.000** **002.003.000**	**002.004.000** **or greater**
October 2025 or later	2.6 or greater	–	–	–	✓
March 2025 - September 2025	2.5	✓	–	✓	■
January 2025 - February 2025	2.4	✓	–	✓	■
September 2024 - December 2025	2.3	✓	✓	✓	■
August 2024 or earlier	2.2	✓	✓	✓	■

✓ Compatible

– Not compatible

■ Not compatible for import to Panel Server. Current and available versions seen in custom model table in Panel Server webpages continue to be supported by Panel Server.

Custom Models Table

The custom models table displays the following information and allows you to perform version updates, and delete custom models:

Column	Description
Model name	Name of imported custom model.
Current version	Current version of the custom model, used by associated Modbus devices. A maximum of 50 custom models can be imported. **NOTE:** An icon (!) indicates if the current version of the custom model has deprecated format. The custom model is still supported.
Includes discovery rules	**True**/**False** Indicates if the current version of the custom device model contains Modbus discovery rules. If **True** is displayed, the current version of the model can be selected by the Panel Server to automatically discover Modbus devices.
Model modification date	Indicates the last date that the current custom model was modified.
Available version	An alternative version of the custom model available to be applied on associated Modbus devices. **NOTE:** An icon (!) indicates if the available version of the custom model has deprecated format.
Associated devices	The number of Modbus devices associated with the current version of the custom model. This number is updated when new Modbus devices are discovered manually or automatically.
⋮ (Contextual menu)	Click this icon to open a contextual menu. The items displayed depend on the device: • **Switch versions and update devices**: Click to switch the current version to the available version. Switching the model to a more recent version automatically updates all associated devices with the new features of the updated version, for example, new measurements. **NOTE:** For availability of **Switch versions and update devices**, refer to the following table. **NOTE:** After updating to a new version, the original version appears in the **Available version** column and can be reinstated to the associated devices by switching the versions again. • **Remove unused version(s)**: Click to delete the available version (if any), and the current version if no devices are associated with the model (0 in **Associated devices** column).

Switching between versions in Panel Server webpages depends on the format of the current and available versions, as indicated in the following table:

Current version	Available version	Can be switched?
Deprecated format	Deprecated format	Yes
Deprecated format	Updated format	Yes
Updated format	Deprecated format	No
Updated format	Updated format	Yes

Supported Functions

Modbus functions are described in the appendix:

- Modbus TCP/IP functions, page 267
- Modbus-SL functions, page 269

Checking Association between Custom Device Model and Modbus Device

To check which custom device model (if any) is associated with your device, navigate to **Settings > Modbus devices** and select your device in the list. In the **Custom device model information** section, the following information is displayed:

- **Custom device model name**
- **Custom device model version**

Local Energy Server Functions (Advanced Model)

What's in This Chapter

Data Logging (Advanced Model) 159
Consumption Overview (Advanced Model) 161
Data Trending (Advanced Model) 163
Exporting Data Locally (Advanced Model) 166

Data Logging (Advanced Model)

Presentation

When data sampling is activated, the Panel Server Advanced historizes (or logs) the sampled data.

Data is logged in the logging memory. The memory stores approximately three years of data of a system (calculated based on a maximum of 500 data points sampled per minute) or 788,400,000 measurement data points. For more detail about quantities of logged data, see Calculating Time Period of Historized Data, page 160.

When the logging memory is full, new data points overwrite the oldest data points stored.

Availability

This function is available on Panel Server Advanced.

In addition to published data, the historized data is available on the Panel Server webpages at **Home** and at **Data Trending**.

Setting the Parameters

To enable data logging, activate data sampling on the Panel Server webpages, at **Settings > Data Management > Data sampling**.

Data Logging Configuration

Configure data logging in the same way as for data sampling, page 118.

Consider the maximum number of data points that can be stored and the recommended sampling limits, page 119 when configuring data logging.

Logging too many data samples per period may affect your Advanced model performance, including degraded web page response, missed logging periods, and less responsive Panel Server operation.

> **NOTE:** Historical data is maintained if the settings of a measurement are modified. Refer to Changing the Data Sampling Frequency, page 120.

Data Logging Configuration from Cloud Application

When a Panel Server Advanced is connected to a cloud application, the data that is sampled and published is logged in the Panel Server Advanced in addition to being published to the cloud application.

> **NOTE:** The Panel Server Advanced publishes the last three months of sampled data when publication is activated.

The logged data can be seen in the **Trending** screens. The sampling and publishing configuration is directly received from the cloud application and cannot be set with the Panel Server commissioning webpages. The logging memory of the Panel Server Advanced serves as a buffer if the cloud connection is lost. The data is published when the cloud connection is restored.

Calculating Time Period of Historized Data

The logging memory stores up to 788,400,000 data points. The equivalent period of time depends on the number of connected devices and the sampling period of each device. Use the following formula to calculate the period of time over which your Panel Server stores data.

Calculate the number of sampled data points per minute for your Panel Server:

(Number of devices x Number of measurements) / Sampling period = Number of sampled data points per minute (Ndp/m)

Divide the total number of data points that can be stored by the number of sampled data points for your device and then divide by the number of minutes in a year (525,950):

788,400,000 / Ndp/m / 525,950 = number of years of data logging held in logging memory

The following table shows some examples:

Number of devices	Number of measure-ments	Total number of sampled data points	Sampling period (min)	Samples per minute	Calculation	Logging memory in years
30	30	900	15	60	788,400,000/60/525,950	24.9
10	200	2,000	10	200	788,400,000/200/525,950	7.5
30	160	4,800	10	480	788,400,000/480/525,950	3.1

Consumption Overview (Advanced Model)

Presentation

The Panel Server Advanced **Home** menu allows you to see an analytical overview of energy consumption. For more information, see Home menu, page 211.

Availability

This function is available on Panel Server Advanced.

Setting the Parameters

The Home menu is available on the EcoStruxure Panel Server webpages, at **Home**.

Consumption Settings

The following table describes the settings.

Parameter	Description
Commodity	Used to select the commodity type (**Electricity** (default setting), **Gas**, **Fuel Oil**, **Air**, **Steam**, **Water**)
Period	Used to select the period duration (**One day**, **One week**, **4 weeks**, **Custom**).
From	Used to select the start date for each period: 1. Select the current period (**Period 1**) start date. 2. Select the previous period (**Period 2**) start date. **NOTE:** The default start date for pre-defined periods depends on the period selected: • One day: Period 1: D-1; Period 2: D-2 • One week: Period 1: D-7; Period 2: D-14 • 4 weeks: Period 1: D-4 weeks; Period 2: D-8 weeks For the **Custom** period, the end date of the second period is set automatically to ensure that the two periods are of the same length. **NOTE:** The default period is one day and the start date is yesterday (D-1).
To	Used to select the period end date.

Pie-Chart Display

The top consumers are displayed in the form of a pie-chart:

- **By usage (Period 1 compared to period 2)**
- **By zone (Period 1 compared to period 2)**

The pie-chart shows the distribution of the top five consumers over the first period, from devices where usage or zone has been defined. A sixth group shows all other consumers.

Different data are displayed on the Home page:

- A table to the right of each pie-chart shows:
  - The consumers by color
  - The percentage of the total consumption that each consumer represents
  - The consumption for each consumer
  - An indication of the increase or decrease in the second period, compared to the first, as a percentage
  - An arrow icon indicating if the trend of the change is increasing or decreasing. If there is no change, no icon is displayed.
- In the centre of the pie-chart **By usage (Period 1 compared to period 2)**, the following information is displayed:
  - Line 1: **Main supply** with:
    - Main incomer total over period 1
    - A percentage indicating the overall change in period 2 compared to period 1
    - An arrow icon indicating the trend. If there is no change, no icon is displayed.
  - Line 2: **Loads** with:
    - Total consumption over period 1
    - A percentage indicating the overall change in period 2 compared to period 1
    - An arrow icon indicating the trend. If there is no change, no icon is displayed.
  - Line 3: **kWh not assigned** indicates the difference between the main incomer total (see **Main supply**) and total consumption (**Loads**), if any. It is recommended to install and configure a meter to monitor each load, and assign the **Main/Incomer** usage to at least one meter so that this line is not displayed, meaning that **Main supply** and **Loads** display the same total.
    Thus, no information is displayed if **Main supply** and **Loads** display the same total.
- In the centre of the pie-chart **By zone (Period 1 compared to period 2)**, the following information is displayed:
  - 1 Line with:
    - Total consumption over period 1
    - A percentage indicating the overall change in period 2 compared to period 1
    - An arrow icon indicating the trend. If there is no change, no icon is displayed.

Icons are listed in Trending Icons (**Home** Page), page 208.

Data Trending (Advanced Model)

Presentation

The Panel Server Advanced allows you to display trending graphs based on the logged historical data over a selected time period.

The trending of the logged data on a Panel Server Advanced requires that the measurements to be viewed have been selected for logging, and that data sampling is activated. For more information, see Data Sampling, page 118.

You can trace trends of historical data over a single period of time or, using the compare mode, you can compare the same data from two different periods of the same duration (for example, comparing data from the week starting July 10th 2022 to the week starting July 17th 2022).

> **NOTE:** The energy values shown in the trending graphs and exported from the **Trending** page differ from the raw data values exported in the local export CSV file, page 166.

You can view the data in the following ways:

- Device view: view trending graphs for a selected device
- Aggregated view by usage
- Aggregated view by zone

For more information about the **Trending** page and how to view data, refer to Trending Menu, page 218.

For more information about usages and zones, refer to Appendix H: Contextualization Data, page 299.

Availability

This function is available on Panel Server Advanced webpages, at **Trending**.

Aggregation Principle

The trending figures in **Aggregated view by usage** and **Aggregated view by zone** are the result of an aggregation algorithm used to calculate the consumption of energy.

For electricity, the aggregation algorithm calculates consumption of active energy in Wh. For other commodities the algorithm calculates consumption by volume in cubic meters (m^3).

> **NOTE:** In order to aggregate the consumed energy of the loads, all usages are considered in the aggregated view by usage except:
>
> - Main/Incomer
> - Sub/Head of group
> - Total
>
> Any device configured with one of these usages is not displayed in aggregated views or in the **Home** page. You can filter by Main/Incomer in **Aggregated view by usage** to display the relevant data. Refer to Trending Menu, page 218

Data Trending Device View Settings

The following table describes the settings.

Parameter	Description
	Used to select the means to group devices in the list: • Usage (default) • Zone
Devices	Used to select one or several devices.
Data	Used to select the data to be used for the graph. The types of data available in the list depend on the devices selected.
Compare mode	• Disable to display the graph over a single period. • Enable to get compared data over two periods of the same duration.
Period	When the parameter **Compare mode** is enabled, used to select the period duration: • **One day** • **One week** • **4 weeks** • **Custom**
From	When the parameter **Compare mode** is disabled, used to select the period start date and time. **NOTE:** The default period is one day, the start date is yesterday (D-1), and the start time is 12.00 AM. When the parameter **Compare mode** is enabled, used to select the start date and time for each period: 1. Select the current period (**Period 1**) start date and time. 2. Select the previous period (**Period 2**) start date. The time is automatically set at the same time as Period 1. **NOTE:** The default start date depends on the period selected: • One day: Period 1: D-1; Period 2: D-2 • One week: Period 1: D-7; Period 2: D-14 • 4 weeks: Period 1: D-4 weeks; Period 2: D-8 weeks • Custom: Period 1: D-1; Period 2: D-2
To	Used to select the period end date and time. **NOTE:** The default end date is today (D). When the parameter **Compare mode** is enabled, the end date is defined automatically according to the selected start date and period for fixed time periods (day, week, 4 weeks). For the **Custom** period, select the end date of the first period. The end date and time of the second period are set automatically to ensure that the two periods are of the same length.
Interval	Used to select the interval of integrated data displayed in bar charts: by hour (**H**), day (**D**), or **Month**. **NOTE:** Interval is only displayed when the type of data selected is integrated data (displayed with a bar chart icon in the list).
Clear filters	Used to erase any selection of devices, data or periods of time previously selected.

Data Trending Aggregated View Settings

The following table describes the settings.

Parameter	Description
Filter by zone/Filter by usage	Used to select the following filters: • Zones to display (when in **Aggregated view by usage**) • Usages to display (when in **Aggregated view by zone**
Commodity	Used to select a commodity from a drop-down list of values.

Parameter	Description
Usage (**Aggregated view by usage**)	Used to select usages: • **Specific usages** ◦ **All usages** ◦ **Main/Incomer usage** ◦ **Main usages** (displays five main usages, and other usages grouped together, based on consumption) • **Individual usages** (one or several) **NOTE:** For the calculation of main usages: • With compare mode disabled, usages are calculated over the period selected (period 1). • With compare mode enabled, usages are calculated over the sum of periods 1 and 2.
Zone (**Aggregated view by zone**)	Used to select zones: • **Specific zones** ◦ **All zones** ◦ **Main zones** (displays five main zones, and other zones grouped together, based on consumption) • **Individual zones** (one or several)
Compare mode	• Disable to display the graph over a single period. • Enable to get compared data over two periods of the same duration.
Period	When the parameter **Compare mode** is enabled, used to select the period duration: • **One day** • **One week** • **4 weeks** • **Custom**
From	When the parameter **Compare mode** is disabled, used to select the period start date and time. **NOTE:** The default period is one day and the start date is yesterday (D-1). When the parameter **Compare mode** is enabled, used to select the start date and time for each period: 1. Select the current period (Period 1) start date and time. 2. Select the previous period (Period 2) start date. The time is automatically set at the same time as Period 1. **NOTE:** The default start date depends on the period selected: • One day: Period 1: D-1; Period 2: D-2 • One week: Period 1: D-7; Period 2: D-14 • 4 weeks: Period 1: D-4 weeks; Period 2: D-8 weeks • Custom: Period 1: D-1; Period 2: D-2
To	Used to select the period end date and time. **NOTE:** The default end date is today (D). For the **Custom** period, select the end date and time of the first period. The end date and time of the second period are set automatically to ensure that the two periods are of the same length.
Interval	Used to select the interval of data displayed in bar charts: by hour (**H**), day (**D**), or **Month**.
Clear filters	Used to erase any selection of devices, data or periods of time previously selected.
Export	Used to export the data from the current display to a csv file. For more information, refer to Trending Data Export, page 218

Exporting Data Locally (Advanced Model)

Presentation

The Panel Server Advanced can export data measured on the connected devices and logged through data sampling, page 118. Data can be exported to your PC in a .csv file.

To export data logged on a Panel Server Advanced:

1. Configure data to be sampled (see Selecting Measurements to Log, page 119).
2. Activate sampling.

   NOTE: To enable exporting of logged data to a CSV file after backup restore on the same Panel Server Advanced (see detailed topic, page 180), you must first reset the Panel Server to factory settings (see procedure, page 190).

Availability

This function is available on Panel Server Advanced.

Setting the Parameters

Local export of data is set on the Panel Server webpages, at **Settings > Data Management > Local export**.

Local Export Settings

The following table describes the settings.

Parameter	Description
From	Used to select the start date of the period.
To	Used to select the end date of the period.
Device	Used to select one or more devices from which to export sample data: • One device in the list • Several devices in the list • **All devices**

Exporting Data

To export data that has been sampled by the Panel Server Advanced, click **Export data**. Data is exported into a CSV file on your PC. Data can be exported for a period of time by selecting the start-date and the end-date of the required period of time.

> **NOTE:** The export file contains all data points sampled during the period requested for the export, including for measurements which are no longer sampled or for devices which are no longer connected.

Up to 6.5 million data points can be exported to a single file; larger sets of data must be exported to several files. An error is generated if you attempt to export more than 6.5 million data points. Take note of the over configuration factor included in the error to assist your selection of a valid shorter export period. For example, if you attempt to export 20 days of data, but receive an error that you are 1.0 times over the limit, you would reduce the duration of each export period to less than 10 days.

You can calculate the size of your export file by calculating for each device, the number of samples, and then adding the samples of all devices together. For example, if you have three currents for one device configured for data logging at a 1 minute sampling rate, the total number of samples is 1,581,120. The following table illustrates the calculation.

Measurement	Sampling period (minute)	Start date	End date	Elapsed time (minute)	Number of samples
Current A	1	July 28, 2024	July 29, 2025	527,040	527,040
Current B	1	July 28, 2024	July 29, 2025	527,040	527,040
Current C	1	July 28, 2024	July 29, 2025	527,040	527,040

File Format of CSV Export Saved on a PC

Data is logged in a .csv file. The date is appended in the format yyyymmdd to the file name *data-export_*. For example, data exported on June 8, 2022 are in the file named *data-export_20220608.csv*.

Data time stamps in the CSV file are in the format YYYY-MM-DDTHH:MM:SS±FF:ff. The time shown is that of the time zone set in the webpages and indicates the offset of this time zone from UTC in hours and minutes (±FF:ff), in accordance with ISO 8601.

The following table provides the details of each row of the .csv file, with sample data. Data for each device is displayed per column.

Row	Data in .csv file	Description	Example of data in comma-separated values (CSV) format
1	Element ID	Element ID for each of the columns	*modbus:2_mb_PkWD, modbus:1_mb_PFTtl*
2	*Device Name*	Customer specified device name for each of the columns	*myPM5560, myPM8000*
3	*Device Type*	Device type defined by the Panel Server for each of the columns	*PM5560, PM8000*
4	*Measurement Name*	Data name for each of the columns	*Total Demand Max Active Power, Total Rms Power Factor*
5	*Measurement Unit*	Unit of the data for each of the columns	*Wh*
6 and more	*YYYY-MM-DDTHH:MM:SS ±FF:ff*	Column 1: Timestamp of logged data, recorded with date (YYYY-MM-DD) and time (HH:MM:SS). The time shown is that of the time zone set in the webpages and indicates the offset of this time zone from UTC in hours and minutes (±FF:ff), in accordance with ISO 8601. Columns 2 and more: Data values for each device	*2024-08-27T08:25:00+01:00* In this example, the time is 08:25 in the local time zone, with an offset of +1 hour from UTC, so UTC is 07:25.

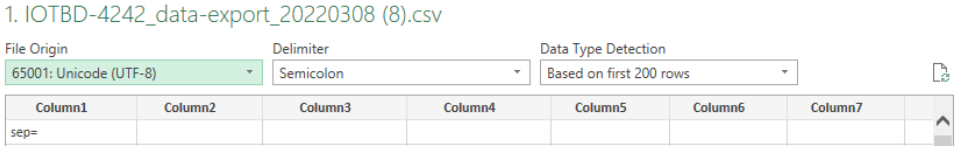
Reading the CSV File

To read the .csv file, you need to import data into Microsoft Excel and use the correct data encoding.

By default, Excel uses Western European character encoding, as shown below:



However, the Panel Server Advanced exports data using UTF-8 character encoding. Therefore, to get all characters to display correctly, such as °C, you need to select UTF-8 as **File Origin** as shown below:

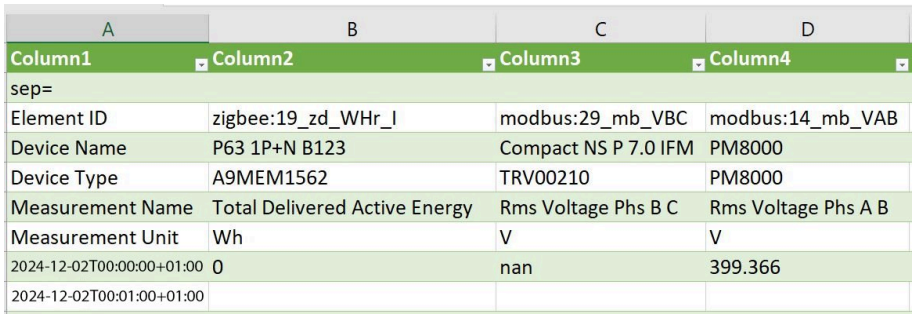


To select UTF-8 encoding in the exported .csv file, proceed as follows:

1. Open Microsoft Excel and select **Data** then, in **Get & Transform Data**, select **From Text/CSV**.
2. Select the .csv file exported from the Panel Server Advanced and click **Import**.
3. In the window that opens, select these parameters:
   - **65001: Unicode (UTF-8)** in **File Origin**.
   - **Based on entire dataset** in **Data Type Detection**.

4. Click **Load**.

   Result: The Panel Server Advanced data logging file displays in Excel with UTF-8 character encoding, as shown in the following illustration:



A	B	C	D
Column1	Column2	Column3	Column4
sep=			
Element ID	zigbee:19_zd_WHr_I	modbus:29_mb_VBC	modbus:14_mb_VAB
Device Name	P63 1P+N B123	Compact NS P 7.0 IFM	PM8000
Device Type	A9MEM1562	TRV00210	PM8000
Measurement Name	Total Delivered Active Energy	Rms Voltage Phs B C	Rms Voltage Phs A B
Measurement Unit	Wh	V	V
2024-12-02T00:00:00+01:00	0	nan	399.366
2024-12-02T00:01:00+01:00			

To ensure that the separators are correctly configured to avoid data reading issues, proceed as follows:

1. In Excel, select **File > Options > Advanced**
2. Uncheck **Use system separators**.
3. In **Decimal separator**, check that , (comma) is entered.
4. Click **OK**.
5. Reload the .csv file, if necessary.

EcoStruxure Panel Server Maintenance Functions

What’s in This Part

Diagnostics 171
Diagnostics Logs 175
Security Logs Using EcoStruxure Cybersecurity Admin Expert 177
Syslog Server Configuration 179
Backup and Restore Panel Server Configuration 180

Diagnostics

Presentation

Diagnostics data provides statistical data about the Panel Server and connected devices. The events are gathered by type of application: cloud connection, Modbus Serial network, and wireless network.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

Diagnostics are set on the Panel Server webpages:

- At **Maintenance > System monitoring > Health state**, system diagnostics, page 174
- At **Maintenance > Devices communication**, device diagnostics:
  - Panel Server, page 171
  - Modbus devices, page 172
  - Wireless devices, page 172
  - Embedded input devices, page 173

EcoStruxure Panel Server Diagnostics

Parameter	Description
Ethernet information	**Ethernet information switched port** • ETH1 link status • ETH1 Duplex transmission speed information • ETH1 Duplex transmission information • ETH2 link status • ETH2 Duplex transmission speed information • ETH2 Duplex transmission information • Received frames • Transmitted frames • Received errors • Transmitted errors • Transmitted collisions
Modbus serial client counter information	Displays diagnostics counters for Modbus-SL protocol: • Received messages • Transmitted messages • Messages timeout • Protocol errors • Received exceptions • Cyclic Redundancy Check (CRC) errors **Reset counters** button allows you to reset the counters to zero.
Modbus TCP/IP server connection information	Displays connection information for Modbus TCP/IP protocol: • Number of active connections

Parameter	Description
	• Maximum number of connections allowed • Maximum number of simultaneous connections occurred • Failed connection counter **Reset counters** button allows you to reset the counter to zero.
Modbus TCP server counter information	Displays message counters for Modbus TCP/IP protocol: • Received messages • Transmitted messages • Protocol errors **Reset counters** button allows you to reset the counters to zero.
Wireless (802.15.4) identification(3)	Displays identification of IEEE 802.15.4 wireless network: • RF-ID • Personal Area Network (PAN) identifier • Extended PAN identifier • Network address
Wireless (802.15.4) network status(3)	Displays status of the IEEE 802.15.4 wireless network • Network status

Modbus Devices Diagnostics

Parameter	Description
Modbus information	Displays identification and diagnostics counters for Modbus devices: • Server identifier historical data (1–254)(4) • Received messages • Transmitted messages • Protocol errors counter • Message timeout counter • Received exceptions counter • Connection timeout counter • Detail of received exceptions **Reset device counters** button allows you to reset the device counters to zero.

The table of channels displays information about Input 1 and Input 2 devices, where relevant.

Wireless Devices Diagnostics

Parameter	Description
Modbus identification(4)	Displays Modbus identification: • Virtual server identifier (1–254)
Wireless network indicator(4) For more information, see Appendix C, page 287.	Displays connection information of the wireless devices:

(3) Depending on the model
(4) Depending on device.

Parameter	Description
	• **Signal quality level** ◦ Weak ◦ Fair ◦ Good ◦ Excellent For information about how the signal quality level is calculated, see Appendix C, page 287. • **Device indicator** ◦ Device received signal strength indicator (RSSI)(5) ◦ Device link quality indicator (LQI)(5) ◦ Device packet error rate (PER)(5) • **Panel Server indicator** ◦ Device received signal strength indicator (RSSI) ◦ Device link quality indicator (LQI) ◦ Device packet error rate (PER)(6) • **Link indicator** ◦ Device received signal strength indicator (RSSI) ◦ Device link quality indicator (LQI) ◦ Device packet error rate (PER)(6)
Status	**Power source** Displays power source of the wireless devices.
	Power source backup(5) Displays backup power source of the wireless devices, where relevant.
Inputs/output(5)	Displays the following information: • Name • Label • Status Input

Embedded Input Device Diagnostics (PAS600L, PAS600LWD and PAS800L Models)

Parameter	Description
Embedded input	For digital input configured as **Pulse counter**, displays **Raw counter value**.
	For digital input configured as **Standard input**, displays **Status**.

(5) Depending on device.
(6) For ZBRT devices, the PER value is not available and 0% is displayed.

System Monitoring Diagnostics

Parameter	Description
Health state	**Uptime** indicates how long the Panel Server has been running for.
	Health state indicates the Panel Server state: • **Nominal** • **Degraded**: If the **Health state** is indicated as **Degraded**, a table indicates the possible causes of the degradation, refer to table below.
Global performance	Displays Panel Server performances: • **CPU usage** (in %) • **Memory usage** (in %)

The following table shows examples of possible causes of health state degradation:

Topic	Level	Date
Lost communication with Modbus serial device(s)	Indicates the level of severity of the cause.	Indicates the date and time the degraded state occurred.
Lost communication with Modbus TCP/IP device(s)		
Lost communication with wireless device(s)		

Diagnostics Logs

Presentation

The Panel Server can log data for diagnostics. You can change log level and export diagnostics logs locally to your PC.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

Logs are set on the Panel Server webpages, at **Maintenance > Logs > Local Log**.

Exporting All Logs

In **Collecting all logs** click **Export all logs** to export a .zip file containing all logs to the Downloads folder of your PC. The file includes the following logs:

- Audit logs
- Autodiagnostic logs
- db JSON files
- System logs

NOTE: The *diagnostic_topology.txt file* contains a list of devices connected to the Panel Server, and the corresponding internal name for each device used in the .json file.

The *diagnostic_modbus.txt* file contains the Modbus application autodiagnostic report per device.

Log Configuration Settings

The log files are mainly used by Schneider Electric Customer Care Center for technical support to facilitate diagnosis in the event of an unexpected behavior.

To display the application name of the log level selected, click **Show application log levels table**.

The events of the log are grouped in four levels:

Log level	Description
Debug	Fine-grained informational events that are most useful to debug an application.
Info	Informational messages that highlight the progress of the application at coarse-grained level.
Warning	Medium severity event that still allows the application to run.
Error	High severity event that designates potential harmful situations.

Changing Log Level

If you are requested to do so by the Schneider Electric Customer Care Center, you can change the level of a log as follows:

1. Select a log level in **Global log level**.
2. Click **Show application log levels table**.
3. In the table that displays, change the log level of one or several logs.
4. Click the **Save** button to apply changes.

Downloading Logs

To download logs, proceed as follows:

1. Select a log level in **Global log level**.

   IMPORTANT: If you export **Debug** logs, it can result in slowdown of the Panel Server performance. It is recommended that you export **Debug** logs for a limited, temporary period during troubleshooting and then apply **Info** as default setting for each application.
2. Click **Export partial logs**.
3. Wait until the .zip file is downloaded on your PC.
4. Unzip the .zip file to access the detailed logs.

Security Logs Using EcoStruxure Cybersecurity Admin Expert

Presentation

Security logs enable the detection and investigation of security incidents. Syslog feature can be configured in EcoStruxure Cybersecurity Admin Expert (CAE) software to forward the security logs to a centralized Syslog server.

When Syslog parameters are configured in CAE software, Syslog is automatically enabled on the Panel Server. For detailed information about configuration in CAE software, see the related topic Syslog Server Configuration, page 179.

Security logs can be used to track events such as:

- Successful and failed login attempts
- User account creation and deletion
- Password changes
- Security configuration changes
- Firmware update events
- Backup and restore events

NOTE: When not using CAE software to configure Panel Server security, security logs are available in local logs by using the Panel Server webpages, at **Maintenance > Logs > Local Log**. Refer to Exporting all logs, page 175.

NOTE: It is recommended to perform a backup of the Panel Server configuration before deploying the security configuration from CAE software. For information about the backup file contents, see Backup and Restore Panel Server Configuration, page 180.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

Syslog parameters are displayed as read-only on the Panel Server webpages, at **Maintenance > Logs > Centralized Log**.

Syslog Server Configuration

If Syslog is not configured in CAE software, then only **Syslog activation > Inactive** is displayed on the webpage.

The following parameters are displayed only when Syslog parameters are configured in CAE software and deployed to the Panel Server.

Parameter	Description
Syslog activation	Shows the status of the Syslog service: **Active** **NOTE:** The **Syslog** service is displayed in the **Service status** drop-down list in the Panel Server webpage header. The status is indicated by the icon color. For details, refer to Service Status List (Detail), page 205.
Syslog server connection status	Shows the status of the Syslog server: • **Connected** • **Disconnected**
Syslog IP address	Syslog server IP address (in IPv4 format).
Syslog port	Syslog server port.
Transport protocol	**TCP** (Transmission Control Protocol).
Secured connection	• **True**: Syslog will be encrypted by using a certificate. • **False**: Syslog will be unencrypted.

Service Status Icon

Once the Syslog configuration has been deployed to the Panel Server, **Syslog** is displayed in the **Service status** drop-down list in the Panel Server webpage header. The Syslog status is indicated by the icon color:

- The icon is green when the Syslog service is operational.
- The icon is red when communication with the Syslog server is disrupted.

For details, refer to Service Status List (Detail), page 205.

Syslog Server Configuration

Presentation

EcoStruxure Cybersecurity Admin Expert (CAE) is an optional software-based tool which can be used for security configuration of systems with Panel Server gateways. For detailed information, see the CAE user guide (EcoStruxure Cybersecurity Admin Expert User Guide, page 10).

When managing a project in CAE software (see related topic, page 56), you can configure Panel Server security logs to be forwarded to a Syslog server. Then deploy the CAE security configuration to the Panel Server gateway (see related topic, page 58).

> **IMPORTANT:** When the configuration is deployed from CAE software to the Panel Server gateway(s) connected in the system, all Panel Server-supported parameters managed by CAE software overwrite the corresponding parameters on the Panel Server, including users and passwords. For detailed information about the CAE-configurable parameters supported by Panel Server, refer to the list of parameters, page 55.

For information about the read-only Syslog parameters available on the Panel Server webpages, see Security Logs, page 177.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

The Syslog server can be set in CAE software.

Syslog Server Configuration

The following table describes the settings available in CAE software at **SECURITY SETTINGS > Logs and Monitoring > SYSLOG Parameters**.

Parameter	Description
Server address	The Syslog server IP address; only IPv4 format supported for Panel Server. (Empty by default)
Server port	The Syslog server IP port.
Transport type	**TCP** (Transmission Control Protocol). **IMPORTANT: UDP** (User Datagram Protocol) transport type is not supported by Panel Server. If UDP is configured in CAE software, security logs will not be forwarded to the Syslog server.
Enable security	If enabled, a CAE certificate must be uploaded to use the secure Syslog.

Managing Security Certificates

To manage security certificates, follow the procedure outlined in the CAE user guide (EcoStruxure Cybersecurity Admin Expert User Guide, page 10).

Backup and Restore Panel Server Configuration

Presentation

At any moment after commissioning, or before updating the firmware, the configuration of a Panel Server can be saved into a file and used to restore the configuration in a Panel Server of the same model and hardware version, or the same Panel Server. It is strongly recommended to perform this backup before any firmware update.

Note that the backup and restore function enables you to restore a Panel Server configuration only. There is no backup or restoration of sampled data.

IMPORTANT: When the configuration is restored in the same Panel Server, existing logged data are not flushed.

Schneider Electric recommends that you encrypt the backup file with a password to help secure sensitive information. Safeguard the backup file in a protected location to prevent unauthorized access.

NOTICE

UNAUTHORIZED DATA ACCESS

- Secure access to the backup file by setting up a password.
- Do not communicate a backup file to unauthorized persons.

Failure to follow these instructions can result in equipment damage.

IMPORTANT: The backup file password is stored irreversibly. If you do not remember the password, the configuration backed up in the file becomes unusable.

Data related to commissioning is stored in the backup file, for example:

- Commissioning data
  - System settings including date and time, networks (Ethernet, Wi-Fi), DPWS, Modbus-SL, Proxy, and Schneider Electric cloud platform activation status
  - IEEE 802.15.4 network settings and status
  - End-device settings and contextualization, including Modbus-SL, Modbus TCP/IP, IEEE 802.15.4, and inputs/outputs
  - Data sampling settings and contextualization
  - Events and alarms settings including notification configuration per alarm.
- Custom models

The backup file only contains data that allows you to restore an installation back to a previous state, that is, the state it was in when generating the backup file. Therefore, it does not include data unrelated to commissioning, for example:

- User accounts (created using CAE software, page 52 or the Panel Server webpages, page 55)
- Permanent deactivation of wireless networks, page 116
- Setting of Remote control and scheduling from cloud function, page 146
- Logs including diagnostics counters, page 171 and diagnostics logs, page 175
- Alarms, page 140
- Sampled data, page 118
- Firmware revision of the Panel Server
- SFTP server password and SFTP server key fingerprint. These settings need to be entered again after a restore operation.

Availability

This function is available on Panel Server Entry, Universal, and Advanced.

Setting the Parameters

Backup restore is set as follows:

- With EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34
- On the EcoStruxure Panel Server webpages, at **Maintenance > Backup & restore**

Panel Server Configuration Backup Settings

The following table describes the settings available from the webpages.

Parameter	Description
Backup	Used to save the Panel Server configuration.
Backup settings	Used to name the backup file in **Label** parameter (optional) and help secure backup data by encrypting the backup file with a password. You are requested to enter a password by complying with the password requirements, page 53, and to confirm the same password. Otherwise select the checkbox next to the security warning confirmation message displayed at the bottom of the dialog box, and acknowledge that you do not set a password for backup file which means that no password will be required when restoring the backup configuration file. **IMPORTANT:** The file password is stored irreversibly. If you do not remember the password, the configuration backed up in the file becomes unusable.

Panel Server Configuration Restore Settings

The following table describes the setting where it is available.

Parameter	Description
Restore	Used to restore configuration from a backup file. Check that the Panel Server receiving the backup meets the following conditions: • Is the same model or the same Panel Server. • Has a hardware version equal to or greater than the hardware version of the Panel Server used to create the backup file. To check the hardware version, refer to the specific topic, page 26. • Has a firmware revision equal to or greater than the firmware revision of the Panel Server used to create the backup file. To check the firmware version, refer to the specific section, page 50. **IMPORTANT:** A backup file from a different Panel Server can be restored only once and on only one Panel Server. When the configuration is restored in the Panel Server, an error message may be displayed. The message indicates that the number of Modbus devices on the current Panel Server differs from the number of Modbus devices on the previous Panel Server when configuration was backed up. **IMPORTANT:** When the configuration is restored: • Remote control and scheduling from cloud are deactivated by default. • All control schedules are deleted. **IMPORTANT:** When the configuration is restored in the same Panel Server, existing logged data are not flushed.

Restoring Configuration With Wireless Networks Permanently Disabled

The permanent deactivation of the wireless networks is not saved in the Panel Server backup file.

Setting this feature depends on the type of restored Panel Server:

If...	Then...
Data is restored in a new Panel Server	The wireless networks are enabled by default. If permanent deactivation is required as in the backed-up Panel Server, follow the procedure, page 116.
Data is restored in the same Panel Server	Wireless networks remain deactivated.

Cybersecurity Recommendations

What’s in This Part

Recommended Actions for Cybersecurity 184
Security Capabilities 186
Security Recommendations for Commissioning 188
Security Recommendations for Operation 189
Security Recommendations for Decommissioning 190

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 general cybersecurity information, page 9.	Use available resources to increase your cybersecurity knowledge and awareness.
	Review the system defense-in-depth assumptions. Refer to the Panel Server Cybersecurity Guide, page 10.	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, page 186.	Understand how the device security features can be used in a protected environment.
	Review the security risks and compensation controls, page 187.	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. Refer to *Physical Security of the Device* in the Panel Server Cybersecurity Guide, page 10.	Tamper-evident label prevents modification of the device before installation.
	Follow the installation guidelines. Refer to *Physical Security of the Device* in the Panel Server Cybersecurity Guide, page 10.	Help reduce unauthorized physical access.
	Use EcoStruxure Cybersecurity Admin Expert (CAE) software to configure centralized security policy and user accounts, page 55.	Enables centralized security management of system by configuring the following: • Security policy: ◦ Password strength ◦ User session timeout ◦ User account lockout ◦ Maximum number of login attempts ◦ Password attempts timer ◦ User account locking duration • User accounts: ◦ Unique user name ◦ Strong password ◦ Role with least-privileges required
	Change the **SecurityAdmin** default password at first login to the Panel Server webpages (mandatory), page 52.	Help reduce the risk of unauthorized access to configuration functions. Default account settings are often the source of unauthorized access by malicious users.
	Create a separate account for each user (with a unique user name and password per role) and do not use shared accounts.	Help ensure user accountability, traceability of actions through individual identification, and reduces the risk of unauthorized access through shared credentials.
	Assign the least-privileges required among the available	Help reduce the risk of unauthorized access to configuration functions and operational information.

Life cycle stage	Recommended action	Defense-in-depth role
	roles (**VIEWER** or **SECADM**) to each user.	
	Create user accounts only when necessary.	Help reduce your attack surface and risk of unauthorized access.
	Recommend each user to change their user account password at first login.	Create a password following the password requirements. Default account settings and weak passwords are often the source of unauthorized access by malicious users.
	Use EcoStruxure Cybersecurity Admin Expert (CAE) software to configure Syslog parameters for a centralized Syslog server, page 179.	Help strengthen security monitoring and auditing through centralized collection of security logs on a centralized Syslog server.
	Change the Wi-Fi access point password, page 89 at first activation.	Create strong password. Default account settings are common targets for malicious users.
	Disable unused protocols and ports. Refer to *Disable Unused Features* in the Panel Server Cybersecurity Guide, page 10.	Disable unnecessary and unused communication protocols and ports, for example, Wi-Fi, Wi-Fi access point, IEEE.802.15.4.
Operate	Review user accounts on a regular basis and delete accounts no longer required.	Help reduce your attack surface and risk of unauthorized access.
	Encrypt backup configuration files. Refer to *Backup Function* in the Panel Server Cybersecurity Guide, page 10.	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. Refer to *Cloud Application Security* in the Panel Server Cybersecurity Guide, page 10.	Limit access to known and required domains, according to your needs.
	Report a cybersecurity incident or vulnerability, page 9.	Report suspicious activity, a cybersecurity incident, or a vulnerability to Schneider Electric Cybersecurity Support Portal web page.
Maintain	Maintain firmware up to date, page 50.	Update to the latest firmware version to benefit from the latest security patches.
	Monitor the audit logs for unexpected behaviors. Refer to topics about Diagnostics Logs, page 175, or Security Logs when Syslog parameters are configured in CAE software, page 177.	Locally in the Panel Server webpages or on the centralized Syslog server, 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. Refer to *Physical Security of the Device* in the Panel Server Cybersecurity Guide, page 10.	Tamper-evident label prevents modification of the device.
	Check the connected devices for the presence of unknown devices. Refer to *Connected Devices* in the Panel Server Cybersecurity Guide, page 10.	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, page 190.	Help prevent the potential disclosure of data.

Security Capabilities

General Cybersecurity Recommendations

⚠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.

For detailed information about cybersecurity for the EcoStruxure Panel Server, see DOCA0211•• *EcoStruxure Panel Server - Cybersecurity Guide*, page 10.

For more information about cybersecurity, refer to General Cybersecurity Information, page 9.

Security Features

Security features have been built into the EcoStruxure Panel Server to help the device to operate correctly and behave according to its intended purpose.

The key features are:

- Authentication when accessing the product resources from EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34, or from the webpages
- Secure communications between the EcoStruxure Panel Server and its associated wireless devices (supporting confidentiality and integrity)
- Configurable security services and settings
- Firmware update mechanism

The Wired by Design EcoStruxure Panel Server models (PAS600LWD and PAS600PWD) are offered with no native wireless chipset. This removes the potential threat from unauthorized radio devices.

These features provide security capabilities which help to protect the product from potential security threat, that could disrupt the product operation (availability), modify information (integrity) or disclose confidential information (confidentiality).

The security capabilities features are intended to mitigate the inherent threats which are linked to the use of the EcoStruxure Panel Server in an Operational Technology environment.

However, the effectiveness of these capabilities depends on the adoption and application of the following recommendations:

- Recommendations provided in this chapter to cover the commissioning, operation, maintenance, and decommissioning of the EcoStruxure Panel Server
- Recommended Cybersecurity Best Practices

Potential Risks and Compensation Controls

Area	Issue	Risk	Compensating controls
Unsecure protocols	Modbus and some IT protocols (NTP, DHCP, DNS, and DPWS) are unsecure. The device does not have the capability to transmit data encrypted using these protocols.	If a malicious user gained access to your network, they could intercept communications.	If transmitting data over an internal network, physically or logically segment the network. If transmitting data over an external network, encrypt protocol transmissions over all external connections using a VPN (Virtual Private Network) or a similar solution. For communication with Modbus devices limit access to Modbus TCP/IP devices on you network by deactivating Modbus communication per Panel Server interface (ETH1/ETH2/Wi-Fi) on the Panel Server webpages.
Wireless radio communication	During the discovery window, unauthorized radio devices may try to join the network.	If a rogue device gained access to your network, they could eavesdrop on the communication of your wireless network, create an integrity data breach (for example, by sending fake data), or create a Denial of Service (DoS).	Reduce commissioning window to limit exposure. For 16-character RF-ID devices, use the install code when discovering the wireless device. Once the discovery is performed, consult the list of discovered devices in the EcoStruxure Panel Server configuration and make sure that the list of devices contains no unexpected or rogue devices.

Security Recommendations for Commissioning

Configuration of Security Services

Most EcoStruxure Panel Server services are disabled by default to reduce the attack surface and exposure to a minimum. Consequently, it is recommended to only enable the services that are strictly required for the EcoStruxure Panel Server operation.

Secure Communications with Wireless Devices

The control of wireless communications between the EcoStruxure Panel Server and wireless devices is enforced through a pairing mechanism. Only wireless devices that have been paired with the EcoStruxure Panel Server can join its wireless network.

In addition, the wireless communications are secured by cryptographic mechanisms supporting the integrity and confidentiality of data exchanged through the wireless network.

For 16-character RF-ID devices, it is recommended to use the install code when discovering the device to help optimize security.

Once the discovery is performed, it is recommended to periodically verify the list of discovered devices configured in the EcoStruxure Panel Server to make sure that the list of devices contains no unexpected or malicious devices. Reinforce access to device data by disabling Modbus TCP/IP service, page 63.

Security Recommendations for Operation

Maintain the Firmware Up-to-date

Security updates and patches are published on a regular basis. Register to the Security Notifications service to be informed about security updates.

Manage User Accounts

The organization or people operating or maintaining the Panel Server gateway may change over time. It is recommended to verify the list of user accounts periodically to make sure that all the configured user accounts represent the valid product users and administrators. Keeping the user accounts up-to-date helps to ensure that user accounts are set up with correct roles, and unused accounts are removed.

Recommendations for Security Logs

The security log feature of the Panel Server gateway enables the generation of security related events such as successful or failed login attempts, user configuration, object access, and firmware updates. These events are recorded in security logs which provide information that can be used to monitor activities carried out on the system. The security team can use this information to detect and respond in the event of a security compromise.

The security team can retrieve the generated security logs by configuring the Syslog parameters in the CAE software. In this case, the generated security logs will be automatically sent to the configured Syslog server.

To help ensure that security logs are downloaded on a regular basis, use one of the following:

- The automatic log export feature via Syslog service by using CAE software.
- The manual log export from the Panel Server webpages.

Secure Communication with Wireless Devices

It is recommended to periodically verify the list of discovered devices configured in the EcoStruxure Panel Server to make sure that the list of devices are up-to-date and the list contains no unexpected or malicious devices.

Security Recommendations for Decommissioning

Decommissioning

The Panel Server is configured with sensitive and confidential information, such as user account identifiers, IP addresses, Wi-Fi passwords, and cryptographic keys.

When disposing of the Panel Server, it is required to reset it to factory settings to make sure that no sensitive or confidential information can be disclosed or reused.

Resetting to Factory Settings

When following the procedure below, all data (including logs and keys) that have been stored are erased.

NOTICE
HAZARD OF IP ADDRESS CONFLICT Disconnect the EcoStruxure Panel Server from any Ethernet networks before resetting the IP settings to factory values. **Failure to follow these instructions can result in impaired communications.**

To reset the Panel Server completely, follow this procedure to set all configuration settings to factory values:

1. Remove all wireless devices from the Panel Server.
2. Power up the Panel Server while pressing the multifunction button for more than 10 seconds.
   Result: The status LED turns steady orange then blinks fast orange when the reset to factory setting is initiated.
3. Release the button once the status LED starts to blink fast orange.
4. Confirm or cancel reset to factory settings:
   - To confirm reset to factory settings:
     Press the button again within 5 seconds.
     Result: The status LED blinks fast green indicating that reset to factory setting is confirmed.
   - To cancel reset to factory settings:
     Wait until the status LED blinks fast red.
5. Wait for the Panel Server to restart completely:
   a. The status LED turns steady orange while the Panel Server is booting.
   b. The status LED turns steady green when the Panel Server is in normal operation.

General Principle to Commission an EcoStruxure Panel Server

What’s in This Part

Overview 192
Commissioning Panel Server with EcoStruxure Power Commission Software 193
Commissioning Panel Server with Webpages 199

Overview

The commissioning of an Panel Server can be performed using one of the following tools:

- EcoStruxure Power Commission software, page 193. See *EcoStruxure Power Commission Online Help*.

  Use the software for a system-focused, global approach to configure the Panel Server gateways with firmware version up to 002.006.001, and all the devices in the switchboard. In addition, the software advanced features allow you to:

  - prepare a project off-line.
  - save a project (system configuration).
  - create a new project from an existing one.
  - generate a report with data collected during configuration testing and to retrieve the settings updated through the Panel Server webpages.
  - to export a project to a supervision software (for example, EcoStruxure Power Monitoring Expert).
- Panel Server webpages, page 200.

  Use the webpages for a device-focused approach to

  - add or remove Modbus and/or wireless devices
  - configure or modify settings of connected devices
  - set up data contextualization of connected devices
  - set up data sampling and data publishing
  - export data to files
- EcoStruxure Power Commission Mobile app in conjunction with EcoStruxure Energy Hub (part of EcoStruxure Building Activate).

  Use the app for a device-focused commissioning of a limited selection of settings through a Wi-Fi connection, on Panel Server gateways with firmware version up to 002.006.001. For more information, refer to the detailed topic, page 198.

During commissioning of the Panel Server through an Ethernet connection, update the firmware of the Panel Server, page 50.

Pre-requisites to Commissioning

To commission the Panel Server with firmware version up to 002.006.001 with EcoStruxure Power Commission software, or Panel Server gateways with Panel Server webpages, use one of the following connection methods:

- Connect the Panel Server to Ethernet (see Connection to a PC, page 31).
- Connect a PC to the Panel Server through the Wi-Fi access point (see Connecting to the Wi-Fi Access Point from a PC, page 91).

To commission the Panel Server with firmware version up to 002.006.001 with EcoStruxure Power Commission Mobile app, connect to the Panel Server Wi-Fi access point.

Commissioning Panel Server with EcoStruxure Power Commission Software

What's in This Chapter

First Connection with EcoStruxure Power Commission Software 194
Non-Selective Discovery of Wireless Devices 195
Selective Discovery of Wireless Devices 196
Device Configuration with EcoStruxure Power Commission Software 197
Device Configuration with EcoStruxure Power Commission Mobile App 198

NOTICE

SOFTWARE INCOMPATIBILITY

- EcoStruxure Power Commission software and Mobile App do not support Panel Server with firmware versions 002.007.000 and 002.008.000. Use the Panel Server webpages instead for Panel Server firmware update, commissioning and configuration operations.
- For Panel Server with firmware version up to 002.006.001, EcoStruxure Power Commission software and Mobile App can continue to be used for Panel Server firmware update, commissioning and configuration operations.

Failure to follow these instructions can limit the ability to commission and configure the equipment.

First Connection with EcoStruxure Power Commission Software

Presentation

EcoStruxure Power Commission software supports self-discovery of EcoStruxure Panel Server with firmware version up to 002.006.001 and connected devices.

Connection Procedure

Follow these steps to connect to the EcoStruxure Panel Server through EcoStruxure Power Commission

1. Disconnect the PC from the local area network (LAN) and switch off Wi-Fi, if any.
2. Connect an Ethernet cable from the PC to the Panel Server (see Connection to Ethernet, page 30).
3. Open the EcoStruxure Power Commission application on your PC.
4. Click the EcoStruxure Panel Server panel to launch self-discovery of the EcoStruxure Panel Server.
5. Identify your EcoStruxure Panel Server by selecting the correct MAC address (see the MAC address on the top of your EcoStruxure Panel Server).
6. Click **Next** to open the device page.
7. Click **Add device**.
8. When the EcoStruxure Panel Server displays with the device characteristics, click the green **Connect** button.

   During the connection, a firmware update is proposed. Follow the on-screen instructions to update the firmware. Click the cross at the top right of the window to come back to the device page.
9. When the connection is complete, start the commissioning of the EcoStruxure Panel Server.

If the self-discovery does not find the Panel Server, refer to Troubleshooting, page 260.

Non-Selective Discovery of Wireless Devices

Presentation

It is possible to achieve a non-selective discovery of wireless devices by using EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.

All wireless devices in the network and available for discovery are discovered by the EcoStruxure Panel Server. The feature enables you to discover a large number of wireless devices at the same time.

The Protect Plus function is not available when discovering and commissioning devices through EcoStruxure Power Commission software. For more information about the heightened security that the Protect Plus function offers during discovery, refer to Discovery of Wireless Devices Through Webpages, page 239.

Commissioning Procedure

To commission a Panel Server gateway with firmware version up to 002.006.001 by using EcoStruxure Power Commission software, proceed as follows:

1. Check that the wireless devices that are to be part of the EcoStruxure Panel Server project are powered on.
2. Connect the EcoStruxure Panel Server to the PC (see Ethernet connection, page 30).
3. Launch EcoStruxure Power Commission software.
4. In the EcoStruxure Panel Server home page, click the **CONNECT TO DEVICE** button.

   Result: When the EcoStruxure Panel Server is connected, the connection parameters (IP and EcoStruxure Panel Server address) display.
5. To add wireless devices, click the **Add Wireless Devices** card.
6. To automatically find all the wireless devices available within the range of the EcoStruxure Panel Server, click the **Automatic discovery** card. Wait until the wireless devices are discovered and displayed in the list of devices.

   NOTE: When the IEEE 802.15.4 network is established for the first time, the operation takes an extra 21 seconds while communication is enabled and automatic channel selection is performed (see settings, page 109).
7. Locate a device in a switchboard by clicking the associated icon.

   Result: The **Locate Device** dialog box is displayed and the associated wireless device in the switchboard continuously blinks green.
8. Click **STOP BLINK** to stop blinking of the device once it is identified.
9. Click **CONFIRM** to proceed.
10. Configure the specific parameters for each wireless device.
11. Download EcoStruxure Panel Server discovered devices and associated parameters to EcoStruxure Panel Server by clicking the **WRITE TO PROJECT** button.
12. Confirm to proceed.

    Result: Message **Write to project successful** is displayed when finished.
13. In **COMMUNICATION VIEW**, click the EcoStruxure Panel Server in the communication diagram.
14. Save EcoStruxure Panel Server settings in the project by clicking the **APPLY TO SERVER** button.

    Result: Message **Write to project successful** is displayed when finished.

Selective Discovery of Wireless Devices

Presentation

It is possible to achieve a selective discovery by using EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, see related topic, page 34.

To discover the wireless devices with EcoStruxure Panel Server, define and upload a selective list to EcoStruxure Power Commission software. The Panel Server will discover only the wireless devices belonging to the list.

Device Configuration with EcoStruxure Power Commission Software

NOTICE

SOFTWARE INCOMPATIBILITY

- EcoStruxure Power Commission software and Mobile App do not support Panel Server with firmware versions 002.007.000 and 002.008.000. Use the Panel Server webpages instead for Panel Server firmware update, commissioning and configuration operations.
- For Panel Server with firmware version up to 002.006.001, EcoStruxure Power Commission software and Mobile App can continue to be used for Panel Server firmware update, commissioning and configuration operations.

Failure to follow these instructions can limit the ability to commission and configure the equipment.

It is possible to configure a wireless device or a Modbus-SL device by using EcoStruxure Power Commission software. For more information, see *EcoStruxure Power Commission Online Help*.

Device Configuration with EcoStruxure Power Commission Mobile App

NOTICE

SOFTWARE INCOMPATIBILITY

- EcoStruxure Power Commission software and Mobile App do not support Panel Server with firmware versions 002.007.000 and 002.008.000. Use the Panel Server webpages instead for Panel Server firmware update, commissioning and configuration operations.
- For Panel Server with firmware version up to 002.006.001, EcoStruxure Power Commission software and Mobile App can continue to be used for Panel Server firmware update, commissioning and configuration operations.

Failure to follow these instructions can limit the ability to commission and configure the equipment.

It is possible to configure a wireless device by using EcoStruxure Power Commission Mobile app, in conjunction with EcoStruxure Energy Hub (part of EcoStruxure Building Activate), connected via the Wi-Fi access point. For more information, follow the on-screen instructions in the app.

The following configuration settings are available:

- General
- Network communication
- Wireless devices
- Data publication

For more information about EcoStruxure Power Commission Mobile app, refer to DOCA0366EN *EcoStruxure Power Commission Mobile Application - User Guide*, page 10.

Commissioning Panel Server with Webpages

What’s in This Chapter

Getting Started with EcoStruxure Panel Server Webpages 200
First Connection to EcoStruxure Panel Server Webpages 201

Getting Started with EcoStruxure Panel Server Webpages

Follow these stages to set up the Panel Server device through the webpages:

1. Connect the Panel Server. Refer to First Connection to Panel Server Webpages, page 201.
2. Set the date and time for the Panel Server at **Settings > General**. Refer to Date and Time, page 47.
3. Configure the network settings, page 71.
4. Add Modbus devices, page 228 and/or discover wireless devices, page 238.
5. Configure the connected devices:
   - Modbus devices: at **Settings > Modbus Devices**. Refer also to Custom Models, page 153.
   - Wireless devices: at **Settings > Wireless Devices**. Refer also to sections on configuring wireless devices in Commissioning of Wireless Devices Through Webpages, page 238.
   - Configure embedded digital inputs, page 149, if relevant.
   - Set up data sampling, page 118.
   - Set up data publishing and/or cloud services, page 122.

First Connection to EcoStruxure Panel Server Webpages

Overview

EcoStruxure Panel Server manages webpages to configure settings or monitor wireless devices (depending on the model), wired devices (through Modbus-SL or Modbus TCP/IP), and local digital inputs with the Panel Server Universal PAS600L, PAS600LWD, and Advanced PAS800L.

Recommended Web Browsers

The Panel Server webpages are accessible from a PC with Windows operating system.

To access the Panel Server webpages, the latest version of web browser Google Chrome or a Chromium-based browser is highly recommended. Other browsers may experience limitations.

Security Certificate

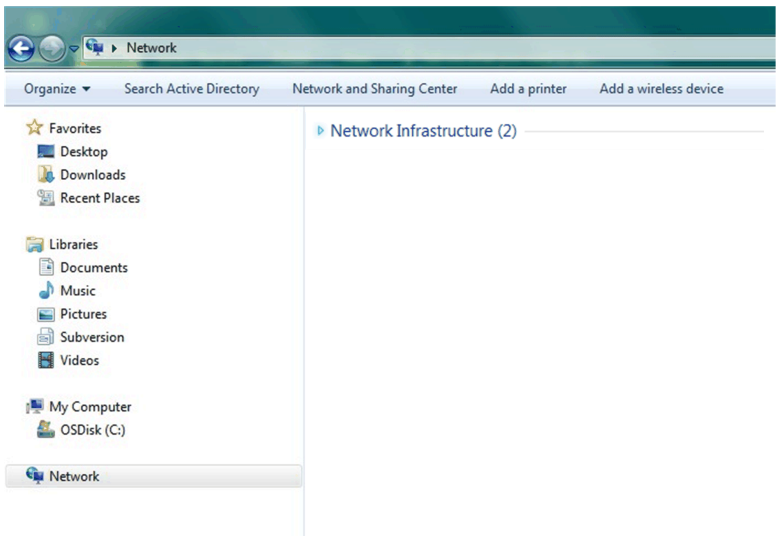
The Panel Server has a self-signed security certificate. A security message appears on the web browser when connecting to the Panel Server. Before accepting and continuing, check that communication with the Panel Server has been established either by directly connecting your PC to the Panel Server or making sure that your network is free of any rogue devices.

Connecting to a Panel Server on a PC Through Ethernet

The Panel Server supports Device Profile for Web Service (DPWS) that allows self-discovery of the Panel Server.

To discover the Panel Server through your PC for the first time, proceed as follows:

1. Disconnect the PC from the local area network (LAN) and switch off Wi-Fi, if any.
2. Connect an Ethernet cable from the PC to the Panel Server (see Connection to Ethernet, page 30).
3. On the PC, launch the File Explorer (Windows file manager application) and click **Network**.



4. Wait until the EcoStruxure Panel Server icon displays in the list of devices in the network. It may take up to 2 minutes after the Panel Server is powered on.

   Result: The EcoStruxure Panel Server icon that displays under **Network** is as follows:

5. Double-click the Panel Server icon.

   Result: The Panel Server webpages open.

6. If the Panel Server is not displayed under **Network**:
   a. Perform the following checks:
      - Check that your firewall allows the necessary access to discover your Panel Server. For more details about allowing access, refer to the Cloud Application Security section in DOCA0211•• *EcoStruxure Panel Server - Cybersecurity Guide*, page 10.
      - Check that the Panel Server and the PC are connected to the same sub-network.
      - If the Panel Server uses a static IP, check that the PC uses a static IP in the same network (same Subnet mask).
      - If the Panel Server IPV4 is in DHCP mode (default setting), set DHCP mode on your PC:
        - Access the Windows control panel of your PC.
        - Click **Network and Sharing Center**.
        - Click **Change adapter settings**.
        - Right-click the **Local Area Connection** icon then click **Properties**.
        - Select **Internet Protocol Version 4 (TCP/IPv4)** from the list and click **Properties**.
        - Select **Obtain an IP address automatically** and click **OK**.

   b. Go to step 1 and do the procedure again.
   c. If the Panel Server is still not displayed under **Network**, see Troubleshooting, page 260.
7. Log in using the default user account name SecurityAdmin.
8. Enter the default password **AAAAAAAA**. A window opens requiring you to set a new password.
9. Set a password, following the requirements (see Password Requirements, page 53).
10. Check the Panel Server firmware version:
    a. From the Panel Server webpages, select **Maintenance > Firmware update > Firmware update** and take note of the firmware version.
    b. Compare the firmware version with the one available in your Schneider Electric country website.
    c. Update the Panel Server firmware if it is not in the latest version (see details to update firmware, page 51).

Connecting to a Panel Server on a PC Through Wi-Fi Access Point

Follow the procedure outlined in Wi-Fi Access Point, page 89.

Using EcoStruxure Panel Server Webpages

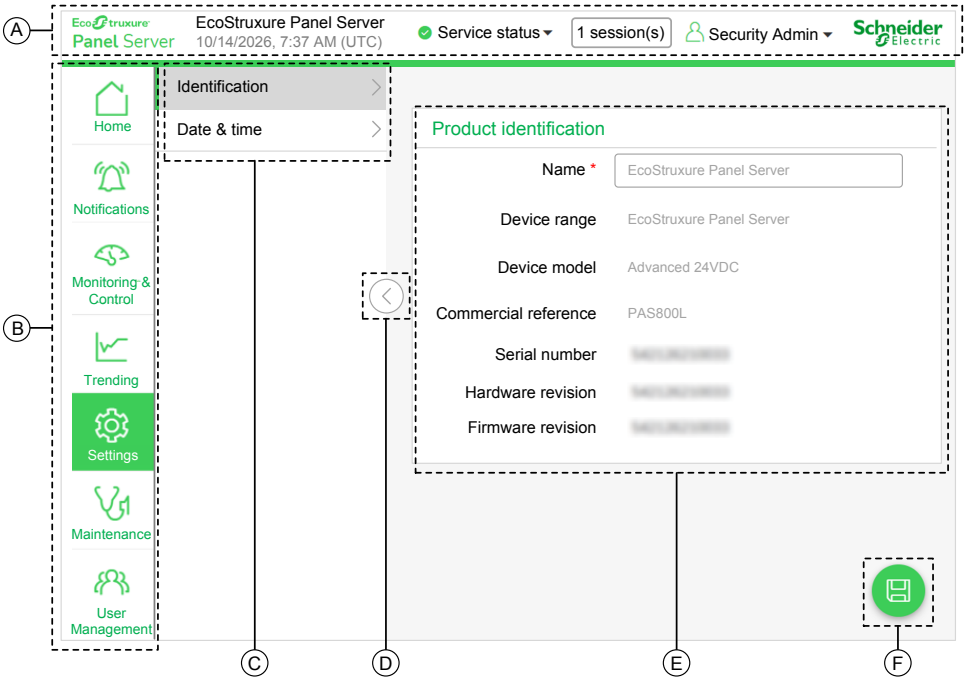
What’s in This Part

EcoStruxure Panel Server User Interface Layout 204
EcoStruxure Panel Server Webpage Menus 210
Commissioning of Modbus Devices 227
Commissioning of Wireless Devices Through Webpages 238

EcoStruxure Panel Server User Interface Layout

Overview

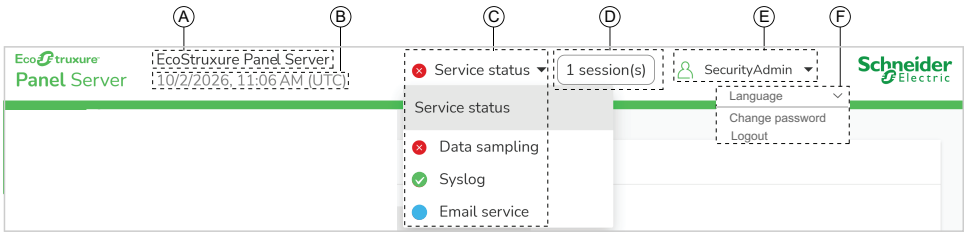
The illustration shows the Panel Server user interface layout.



A. Header
B. Main menus (The main menus displayed depend on the model. The image illustrates a Panel Server Advanced model.)
C. Sub menus
D. Icon to collapse or expand left pane
E. Display zone
F. Icon for contextual menu

Header

The header displays the following information at the top of every page.



A. Panel Server name
B. Date, time and time zone selected
C. Service status drop-down list
D. Number of active sessions in the Panel Server webpages
E. User account name
F. User account settings drop-down list (**Language**, **Change password**, **Logout**)

The data maintenance icon is displayed to the left of the Service status list when data maintenance operation is in progress. The icon will disappear when the data maintenance operation is completed.

Header part		**Description**
A	Panel Server name	The name entered at **Settings > General > Identification**
B	Date, time and selected time zone	Date in format MM/DD/YYYY Time in 12 hour format (AM or PM) correct for the selected time zone (shown in brackets). The time zone is set at **Settings > General > Date and time**
C	**Service status** drop-down list	An icon displays the general status of services: • If all services are OK, the icon is green. • If at least one of the services in the list displays blue or red status, the icon displays as blue or red. • If one service displays blue status, and another red status, the icon displays red status. Clicking the service name takes you to the settings page for that service. Refer to Service Status List, page 205 for more detail of the list.
D	Number of active sessions	Number of users logged in to the Panel Server webpages.
E	User account name	Any user account name to log in the webpages.
F	User account settings drop-down list	• **Language**: The webpage language is English (US) by default. Other languages are available in the list. • **Change password**: Click to change the user password (see password requirements, page 53). • **Logout**: Click to log out from the Panel Server session. It is recommended that you log out from the Panel Server when it is not in use. You are logged out automatically after 60 minutes.

Service Status List (Detail)

Services in the list are displayed depending on the Panel Server model:

- SFTP
- HTTPS
- Data sampling

- Cloud service
- Syslog
- Control scheduling
- Email service (Advanced model)

The following table shows the status of each service.

Icon	Service status
	Service activated and operative
	For **Cloud service**: Initial configuration of Panel Server is complete, but cloud services are not operational until all required actions are completed: 1. Connect to the cloud. 2. Publish the topology from Panel Server. 3. Associate the Panel Server on the cloud application side. 4. Send remote configuration from the cloud application.
	For **SFTP** or **HTTPS**: SFTP or HTTPS data publication is partially configured but the user needs to perform these actions: 1. Test the connection by clicking the **Test connection** button. 2. Launch data publication to the SFTP or HTTPS server publication by clicking the **Start** button.
	For **Email service**: Service is activated but the user needs to perform these actions: 1. Add an email address in the **Recipient list** field. 2. Select this recipient and send a test email by clicking the **Send test email** button.
	Service activated but inoperative as in the case of communication issues with the corresponding service server (cloud, HTTPS, SFTP, email, or Syslog).
	For **Cloud service**: The remote configuration sent by the cloud application is invalid and is rejected by the Panel Server. An error is logged in the auto-diagnostic log file to assist with troubleshooting, page 171. Data publication does not start. If data publication is in progress, it stops. Feedback is sent to the cloud application that sent the remote configuration.

Main Menus

The main menus are:

- **Home** (Advanced model), page 211
- **Notifications** (Advanced model), page 212
- **Monitoring and Control**, page 214
- **Trending** (Advanced model), page 218
- **Settings**, page 220
- **Maintenance**, page 223
- **User Management**, page 226

Cards and Sub-menus

Cards display sub-levels for the following main menus:

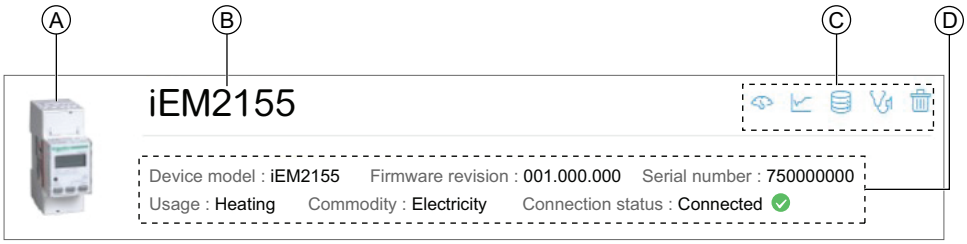
- **Settings**
- **Maintenance**

Sub-menus display the levels available under the selected card or main menu.

Display Area

The display area shows the cards or the selected sub-menu in detail with all related fields. Fields with a red star icon should be filled in to help ensure the proper behavior of the gateway and devices.

Device Page



A. Device image (depending on the device)
B. Device name
C. Icons with links to other pages related to the device
   - Link to the **Monitoring & control** page of the device.
   - Link to the **Trending** page of the device.
   - Link to the **Settings** page of the device.
   - Link to the **Data management** page of the device.
   - Link to the **Maintenance** page of the device.
   - Delete a device. Confirm the removal in the pop-up message.
D. Device information, including (depending on the device and settings)
   - Device model
   - Firmware revision
   - Serial number
   - RF-ID (wireless devices)
   - Usage
   - Commodity
   - Zone
   - Connection status (with icon)

Contextual Menu

The context-specific function icons displayed depend on the selected menu.

Icon	Action	
	Open the contextual menu.	
		In **Settings** pages, save the setting changes and apply them on the Panel Server. Can be used to update a consistent set of parameters through multiple webpages. • If a mandatory field is left blank, the field is highlighted in red. • If inappropriate characters are entered in a field, the field is highlighted in red.

Icon	Action	
		In **Settings** pages, save the setting changes without applying the configuration on the Panel Server.
		Contextual icon: • In **Settings** pages, cancel the setting changes to return to the last saved settings. • In **Network communication** pages, restore settings of the network communication configuration. Used to reapply the full list of settings previously saved.
	Close the contextual menu.	

Monitoring and Control Icons

Icon	Description
	The device is connected.
	The device is not connected.
	The device connection status is out-of-date or invalid.
	Data measurement value is out-of-date or invalid.

Trending Icons (Home Page)

The trending icons are displayed on the Home page depending on consumption trends.

Icon	Description
	The consumption of the commodity (for example, electricity) or a selected usage (for example, lighting) is increasing.
	The consumption of the commodity (for example, electricity) or a selected usage (for example, lighting) is decreasing.
	No icon is displayed if the consumption rate is not changing.
	In pie-chart **By usage (Period 1 compared to period 2)**, indicates a difference between the total consumption of main incomer and total loads.

Custom Model Icons

Icon	Description
	Custom model version has deprecated format.
	No icon is displayed if the custom model version has the latest format.

Alarm Severity Icons

The severity of an alarm is indicated by an icon in the following webpages:

- **Notifications** (Advanced model)
- **Monitoring & Control > Active alarms**

NOTE: Disappearance of alarms is only displayed in Notifications

Icon	Description
	High-severity alarm appearance.
	High-severity alarm disappearance.
	Medium-severity alarm appearance.
	Medium-severity alarm disappearance.
	Low-severity alarm appearance.
	Low-severity alarm disappearance.

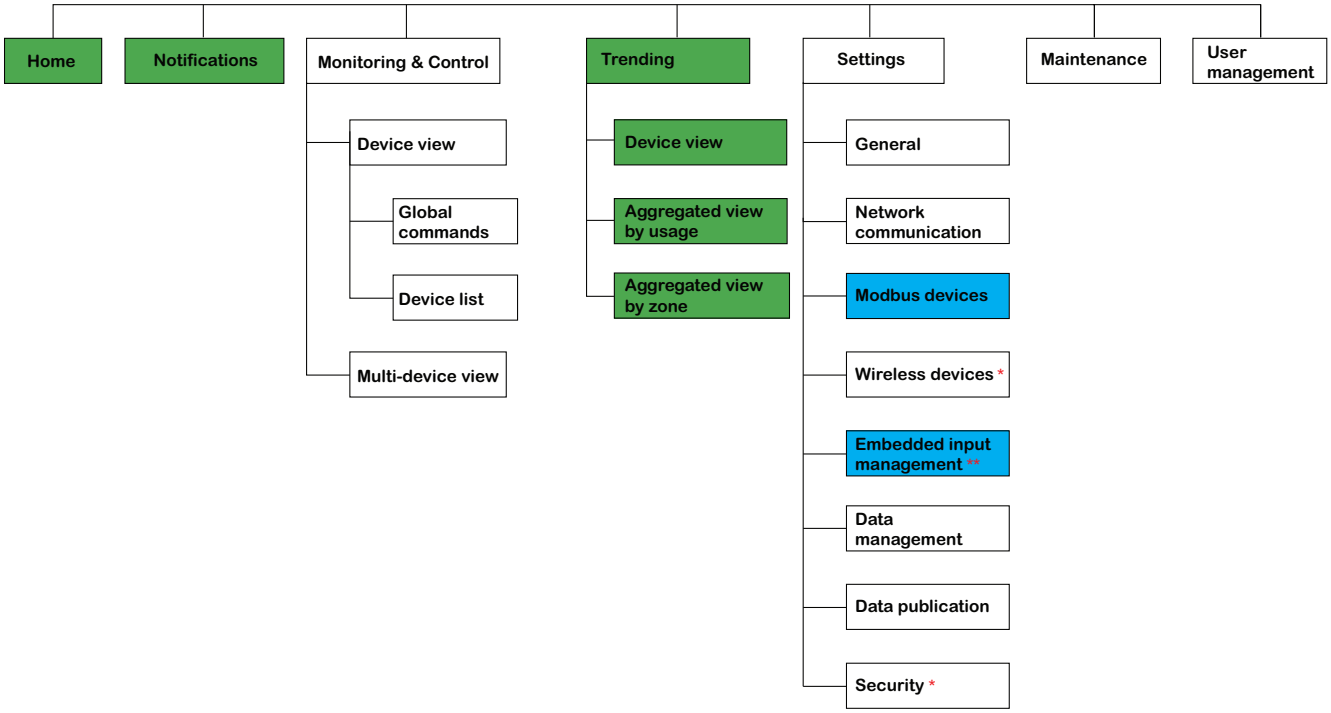
EcoStruxure Panel Server Webpage Menus

What's in This Chapter

Home Menu (Advanced Model) 211
Notifications Menu (Advanced Model) 212
Monitoring and Control Menu 214
Trending Menu (Advanced Model) 218
Settings Menu 220
Maintenance Menu 223
User Management Menu 226

Overview

The following diagram gives an overview of the structure of webpages.



* Not available on Wired by Design models.

** Available on PAS600L, PAS600LWD, PAS800L models.

Available on all models.

Available on Advanced models.

Available on Universal and Advanced models.

Home Menu (Advanced Model)

The webpage for the **Home** menu displays the consumption of energy of the system managed by the Panel Server.

By default, the consumption of electricity is displayed for a period of one day (yesterday, day before yesterday) in two pie-charts. Other commodities and periods can be selected. Consumption charts are organized:

- By usage
- By zone

In each case, the top five consumers are displayed, arranged from highest to lowest consumption. Other consumers of the selected commodity are displayed as a sixth category, labelled **Miscellaneous other usages** or **Miscellaneous other zones**, depending on the chart. Main consumers are calculated based on consumption over Period 1.

A pie-chart shows the distribution of the top five consumers, with all other consumers grouped into a sixth category. The webpage displays for each consumer:

- The consumption of period 1
- The change in consumption over period 1, compared to period 2 (as a percentage)
- The trend: increasing, decreasing (indicated by an arrow icon),or flat (no icon)

You can click on the name of a consumer in the legend to the right of the chart to get detailed information about that consumer.

In the **Home** page you can select a different commodity (for example, gas) and a different period (one day, one week, or 4 weeks). For more information about settings, see Consumption Overview, page 161.

When you are logged into the Panel Server webpages, the **Home** page automatically displays if historized data is available.

For more information about trending data, click the  **Trending** icon:

- In **By Usage** to go to **Trending > Aggregated view by usage**
- In **By Zone** to go to **Trending > Aggregated view by zone**

Notifications Menu (Advanced Model)

Overview

The Panel Server Advanced allows you to display a list of alarm notifications issued by connected downstream devices.

The notification list is for display only.

By default, the list displays alarm notifications issued in the 30 days prior to the current date. You can select other time periods or customize the time period.

You can sort the information by clicking the arrow icons at the top of each column. By default the alarm notifications are displayed in chronological order, with the most recent at the top of the table.

The list of notifications displays the following information for each alarm:

- Date of alarm
- Severity icon
- Name of device which triggered the alarm. Click the name to open the monitoring page of the device, with details of the alarm.
- Alarm name
- Status of alarm

Display Settings

The time period of alarms notifications to display can be selected from a list of options:

- Last 24 hrs
- Last 7 days (default setting)
- Last 30 days
- Last 90 days
- Custom (select the start and end dates of the period required)

You can filter notifications on the following fields:

- Severity
- Device name
- Alarm name
- Status

Alarm Icons

Icon	Description
	High-severity alarm. Appearance.
	High-severity alarm. Disappearance.
	Medium-severity alarm. Appearance.
	Medium-severity alarm. Disappearance.

Icon	Description
	Low-severity alarm. Appearance.
	Low-severity alarm. Disappearance.

Monitoring and Control Menu

Overview

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

Do not rely only on the measurements or equipment status provided on the Panel Server webpages before working on or inside the equipment.

Failure to follow these instructions will result in death or serious injury.

The webpage for the **Monitoring and Control** menu displays devices installed in the system and associated with the Panel Server.

Two views are available:

- **Device view** displays:
  - **Global commands**. The function allows you to:
    - Reset all peak power demands.
    - Synchronize tests on Exiway Light devices, page 255.
  - **Device list** displays associated devices in a list on the left pane (tree view). The list can be displayed sorted by usage or by zone. Select the means to group the devices in the list by clicking the list icon  . The device tree view can be collapsed. Monitoring and control data for the selected device is displayed in widgets on the main screen, with one widget for each data type.
- **Multi-device view** displays data from selected devices and up to two data types, as a table.

The data is refreshed automatically every 15 seconds in both views.

Device View

Click on a device name to see information specific to that device:

- Header: Information about the device:
  - Device model
  - Device firmware version
  - Device serial number
  - Contextual data (if assigned):
    - Commodity
    - Usage
    - Zone
  - Device connection status
  - RF-ID of the device (wireless devices)
- **Data** tab: Real-time data of the device, displayed as widgets, with one widget for each data type relevant to the device.

  The data is displayed as a graph or data values, depending on the data type.

  Active alarms are displayed when the following conditions are met:
  - the alarm is active when you access the webpages,
  - the alarm is not acknowledged.

  Control operations are displayed in the relevant widget as buttons which can be clicked to launch the operation.

- **Advanced data** tab, page 215

The following individual commands can be sent from the **Device view**, depending on the device:

- Reset all energies
- Reset active power delivered - received peak demands
- Breaker status position indicator status (Open/Closed)
- Standard output disconnected off status (Off/Disconnected)

Icons at the top right of the page give you direct access to the following pages for that device:

- Access to the device maintenance page by clicking the Maintenance icon .
- Access to the device settings page by clicking the Settings icon .
- Access to the data management page by clicking the Database icon .
- Access to the trending data by clicking the Trending icon .

Multi-Device View

Select up to five devices and two data types from the drop down menus and click away from the list to display the results in a table. Select the means to group the devices in the list by clicking the list icon . The list is sorted in alphabetical order by **Usage** or by **Zone**.

The table displays:

- A column with data and measurement names
- A column for each selected device
- A data block for **Overview** and each data type selected. The **Overview** block displays:
  - **Label**
  - **Device family**
  - **Commodity**
  - **Usage**
  - **Zone**

The following blocks display the data types selected. Empty cells indicate that no data is available for that device and data type.

Advanced Data

In the **Monitoring and Control** menu in **Device view**, the **Advanced data** tab of the selected device shows the exhaustive list of real-time data related to this device. The data is refreshed every 15 seconds.

The following table presents data available per measurement family. The availability of measurements depends on the type of connected device.

Data type	Data on Panel Server webpage
Active power	Active power total
	Active power A
	Active power B
	Active power C
	Power factor total
Apparent power	Apparent power total
	Apparent power A
	Apparent power B
	Apparent power C
Circuit breaker	Breaker position
	Trip indicator (SD position)
	Trip cnt (Close to SD position) non resettable
	Trip Electrical fault cnt (Close > SDE) non resettable
Current	Current
	Current A
	Current B
	Current C
	Current N
	Current ground
Current THD	THD fund current A
	THD fund current B
	THD fund current C
	THD fund current N
Embedded inputs	Status input 1
	Status input 2
	Consumption
	Flow
	Status output
Energy	Active energy delivered
	Active energy received
	Reactive energy delivered
	Reactive energy received
	Apparent energy
	Apparent energy delivered
Environment	Temperature
	Relative humidity
	CO_2 concentration
	Air quality
	Temperature phase A
	Temperature phase B
	Temperature phase C
	Temperature neutral
Health state	Battery voltage
	Internal temperature
	RSSI link
	LQI link
	PER link

Data type	Data on Panel Server webpage
Harmonic current	Load harmonics current A
	Output harmonics current A
	Load harmonics current B
	Output harmonics current B
	Load harmonics current C
	Output harmonics current C
	Output harmonics neutral current
IGBT temperature	Temperature board in device
	Temperature IGBT A
	Temperature IGBT B
	Temperature IGBT C
Insulation	Insulation ground
	Earth coupling capacity
Motor	Trip indicator
	Motor running
	Motor operating mode
	Pole state
	Contactor state
	Speed setpoint
	Motor speed
	Direction of motor rotation
Reactive power	Reactive power total
	Reactive power A
	Reactive power B
	Reactive power C
Unbalance	Current unbalance A
	Current unbalance B
	Current unbalance C
	Current unbalance N
	Voltage unbalance A-B
	Voltage unbalance B-C
	Voltage unbalance C-A
	Voltage unbalance A-N
	Voltage unbalance B-N
	Voltage unbalance C-N
Voltage	Voltage L-L
	Voltage A-B
	Voltage B-C
	Voltage C-A
	Voltage L-N
	Voltage A-N
	Voltage B-N
	Voltage C-N
Winding temperature	Temperature transformer winding A
	Temperature transformer winding B
	Temperature transformer winding C

Trending Menu (Advanced Model)

Overview

The **Trending** menu allows you to display selected data types for selected devices over a selected time period to see trends in integrated data such as energy consumption, or in continuous data such as power or temperature.

You can display data in the following ways:

- Over one period of time, selected from a list or customized
- Compared between two similar periods of time

When integrated data, such as energy, is selected in the **Trending** page, you can view the accumulated value per hour, day, or month. The accumulated values are calculated by subtracting the value at the beginning of the subsequent interval from the value at the beginning of the current time interval.

For example, if you are visualizing active energy per hour in the **Trending** page, and the active energy at 01:00 is 200 Wh and at 02:00 is 300 Wh, then the accumulated data displayed for active energy at 01:00 is 100 Wh. If one of the two data points required in the calculation is missing, then the accumulated data cannot be calculated and is not displayed.

You can view data trends in the following ways:

- **Device view** provides a device centric view. It displays data from a selection of devices for a specified period of time and compares data within an equivalent period of time. A drop-down menu allows you to group the devices in the list by usage or by zone.
- The following aggregated views provide a data centric view:
  - **Aggregated view by usage** (can be filtered by zone)
  - **Aggregated view by zone** (can be filtered by usage)

  They display aggregated data of energy consumption based on a commodity and/or usage or zone, without reference to specific devices.

The type of trending graph displayed depends on the type of data selected. There are two types of graph:

- Bar chart: used to display integrated data (for example, active energy, reactive energy) or aggregated data
- Line graph: used to display continuous data (for example, temperature, active power)

The type of graph is indicated by an icon next to each type of data in the **Data** drop down menu. The types of data available in the list depend on the device selected.

A legend below the graph indicates device and data type per curve. A tooltip pops up when hovering the cursor over the graphs, indicating date, time, device name, value and unit for each data plot. For an optimized user experience, a maximum of 16 curves should be displayed on a line graph.

NOTE: Extrapolated data points are included in the graph or chart with a legend indicating **Approximate value**. For more information about extrapolated data points see Changing the Data Sampling Frequency, page 120.

You can export the data trends. See Trending Data Export, page 219.

For information about trending settings, see Data Trending, page 163.

Displaying Trends

To customize data displayed in **Device view**:

1. Select the means to group the devices in the list by clicking the list icon  :
   - **Usage** (default)
   - **Zone**
2. Select the device(s) you want to view from the drop-down **Devices** list.
3. Select the data you want to view. Only two different types of data can be displayed together.
4. Activate compare mode by clicking the toggle switch if you want to compare periods.
5. Select the period of time you want to display.

For more information about settings, refer to Data Trending Device View Settings, page 163.

To customize data displayed in **Aggregated views**:

1. Select the commodity you want to view. Only one commodity can be selected.
2. Select the usage(s) or zone(s) you want to view.
3. If required, filter the usage by zone, or filter the zone by usage.
4. Activate compare mode by clicking the toggle switch if you want to compare periods.
5. Select the period of time you want to display.

For more information about settings, refer to Data Trending Aggregated View Settings, page 164.

Trending Data Export

The selected data can be exported as a csv file by clicking **Export** at the top right of the webpage. The csv export contains a file for the selected view (**Device view** or **Aggregated view**), in the language displayed on the screen. The format of the csv file enables you to visualize rapidly the data in a graph.

NOTE: Data export is not available in **Compare mode**.

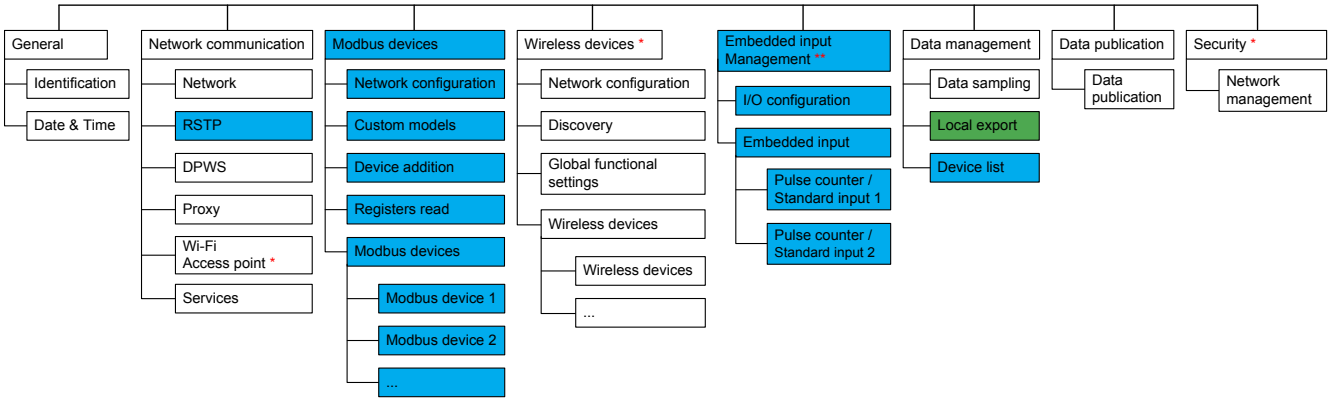
The name of the CSV file that is exported follows the naming convention: *PASType_PASSerialNumber_DataExportType_Date-Time* where:

- *PASType* is the Panel Server model
- *PASSerialNumber* is the serial number of the Panel Server
- *DataExportType* indicates:
  - *device_data_export* for data exported from the **Device view**
  - *usages_data_export* for data exported from the **Aggregated view**
- *Date-Time* in the format YYYYMMDD-hhmm

Example: **PAS800L_542126210003_device_data_export_20250115-1002.csv** indicates data exported at 10:02 on 15th January 2025 from the **Device view** page of PAS800L Panel Server with serial number 542126210003

Settings Menu

Settings Menu Structure



* Not available on Wired by Design models.

** Available on PAS600L, PAS600LWD, PAS800L models.

Available on all models.

Available on Universal and Advanced models.

Available on Advanced models.

For more information, refer to **Settings** menu, page 221.

Settings Menu Description

NOTICE

IMPAIRED NETWORK PERFORMANCE

Only qualified personnel should modify the Ethernet and/or Modbus-SL settings. Perform such modifications only after you have read about and understood the Ethernet and/or Modbus-SL settings.

Failure to follow these instruction can result in loss of network connectivity

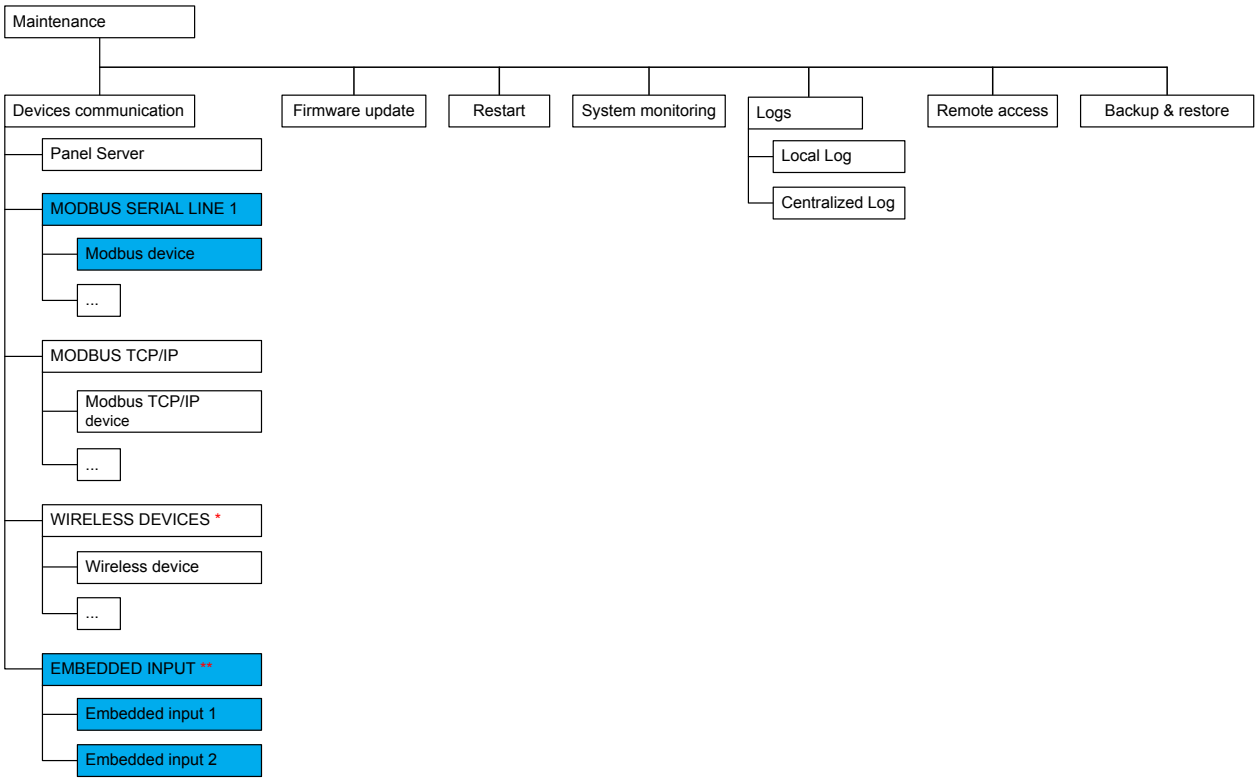
The webpage for the **Settings** menu displays the cards and sub-menus for configuration and communication settings. The cards and sub-menus on the webpages depend on the Panel Server model.

Card	Sub-menu		Description
General	**Identification**		Information about the Panel Server identification: • Device name • Device range • Device model • Commercial reference • Serial number • Hardware revision • Firmware revision
	Date & Time, page 47		Used to set the date and time manually or via NTP (Network Time Protocol).
Network communication	**Network**	**Network configuration**, page 79	Allows you to configure your network topology: • **Ethernet mode** • **Wi-Fi Infrastructure activation** • **Antenna**
		Infrastructure Settings, page 86	Allows you to configure the Wi-Fi settings and configure communication by disabling/enabling IPv4 and IPv6.
		Ethernet Settings, page 93	Allows you to configure the selected Panel Server Ethernet mode and configure communication by disabling/enabling IPv4 and IPv6.
		DNS Settings, page 80	Allows you to configure the DNS server.
	RSTP, page 81		Allows IT specialists to configure RSTP protocol.
	DPWS, page 85		Allows you to configure the IP network discovery.
	Proxy, page 84		Allows you to configure the Internet proxy settings.
	Wi-Fi Access point, page 89		Allows you to configure the Wi-Fi access point settings.
	Services, page 98		**Communication services activation**: Allows you to enable or disable the following services per interface: Modbus TCP/IP: • in switched mode • on ETH1 port in separated mode • on ETH2 port in separated mode • on Wi-Fi

Card	Sub-menu	Description
Modbus devices	**Modbus configuration**, page 101	Allows you to define the Modbus-SL and Modbus TCP/IP network.
	Custom models, page 153	Allows you to upload Modbus-SL and Modbus TCP/IP devices that are not natively managed by the Panel Server built-in models. Displays a link to access EPC Web tool directly to create custom device models.
	Device addition, page 228	Allows you to discover the Modbus-SL and Modbus TCP/IP devices by using a selective list.
	Registers read, page 231	Allows you to troubleshoot the addition of Modbus devices.
	Modbus devices organized as follows: • **MODBUS SERIAL LINE 1** • **MODBUS TCP/IP**	Detailed information about each device discovered in the Modbus network. Information (for example, device identification, custom model name and version, electrical characteristics) and contextualization data (entered by the user) depend on the device type.
Wireless devices, page 108	**Network configuration**	Allows you to define the IEEE 802.15.4 network when activated.
	Discovery	Allows you to discover the wireless devices in the IEEE 802.15.4 network by using a selective list or non-selective discovery.
	Global functional settings	Allows you to: • Set retention time: the time the status of a XB5R transmitter (ZBRT1) is retained (in ms) • Set the power demand calculation time interval (in minutes), page 248 • Set the address of the **Synthesis table** (**247** by default) which shows a consolidated view of information from all the wireless devices at once. For detailed information about the Modbus synthesis table, refer to DOCA0241EN *EcoStruxure Panel Server - Modbus File*.
	Wireless devices	Allows you to send a **Locate** command to make the wireless device blink for 30 seconds (5 minutes for Exiway Link devices). Provides detailed information about each wireless device in the IEEE 802.15.4 network. Information (for example, device identification, device RF-ID, electrical characteristics, Modbus virtual server ID) and contextualization data (entered by the user) depend on the device type.
Embedded Input Management	**I/O configuration**, page 149	Allows you to configure the Panel Server digital inputs.
	Embedded input	Allows you to configure inputs/outputs of I/O devices associated with Panel Server.
Data Management	**Data sampling**, page 118	Allows you to: • activate/deactivate the default sampling configuration, • activate/deactivate data sampling of the connected devices, • flush all the data measurements, • view data sampling information.
	Local export, page 166	Allows you to export sampled data for one, multiple, or all the devices to a local .csv file. (Available in Advanced model only.)
	Device tree view	Detailed information about sampling for each device connected to the Panel Server. Devices are sorted by usage or zone. Select the means to group the devices in the list by clicking the list icon  . Measurements and alarms depend on the device type.
Data Publication, page 122	**Data Publication**	Allows you to set the means used to publish data and to enable the email of alarms service.
Security	**Network management**, page 116	Allows you to configure the security feature to permanently disable the wireless networks.

Maintenance Menu

Maintenance Menu Structure



* Not available on Wired by Design models.

Available on all models.

Available on Universal and Advanced models.

For more information, refer to **Maintenance** menu, page 224.

Maintenance Menu Description

The webpage for the **Maintenance** menu displays the cards and sub-menus for maintenance and diagnostic functions, based on diagnostic counters.

Card	Sub-menu	Description
Devices communication, page 171	Click the Panel Server icon to get communication data. This data can help with troubleshooting Panel Server communication.	Allows you to check the communication status of the Panel Server with downstream devices (Modbus-SL and wireless devices). Allows you to reset all Modbus network counters. For details, refer to Panel Server Diagnostics, page 171.
	Modbus devices organized as follows: • **MODBUS SERIAL LINE 1** • **MODBUS TCP/IP**	Displays information about and status of the selected device. Allows you to reset individual Modbus device counters. Allows you to remove a previously added or associated downstream device.
	Wireless devices	
	Embedded Input (PAS600L, PAS600LWD, PAS800L)	Displays information about and status of the embedded inputs.
Firmware update, page 50	–	Allows you to: • Click **Learn more** to access information about Panel Server models and documentation. • Read the current firmware version and hardware revision of the Panel Server • Retrieve the correct firmware for your device. • Perform a local firmware update of the Panel Server. For more information, refer to the firmware updates available for each model and the respective release notes, page 10: • DOCA0249•• *EcoStruxure Panel Server Entry - Firmware Release Notes* • DOCA0178•• *EcoStruxure Panel Server Universal - Firmware Release Notes* • DOCA0248•• *EcoStruxure Panel Server Advanced - Firmware Release Notes*
Restart	–	Allows you to restart the Panel Server. **NOTE:** The Panel Server webpages are disconnected and cannot be accessed while the Panel Server is rebooting.
System monitoring, page 174	–	Displays Panel Server health status indicators and global performance.
Logs	**Local Log**, page 175	Allows you to: • Change the log level (if requested to do so by Customer Care Centre) and download the partial logs in a .zip file. • Collect all logs and export a detailed report of the Panel Server configuration and a status report per internal application in a .zip file.
	Centralized Log, page 177	Displays Syslog configuration set in CAE software. For details, see Syslog Server Configuration, page 179. When Syslog parameters are configured in CAE software, Syslog is automatically enabled on the Panel Server and the security logs generated by the Panel Server are forwarded to the Syslog server.

Card	Sub-menu	Description
Remote access	**Anytime remote access**	The section allows you to authorize a remote connection with the Schneider Electric Customer Care Center through the Schneider Electric cloud. The Customer Care Center is able to connect remotely to the Panel Server without any action from the user's side and as long as the Cloud service is connected. Each session lasts for a maximum of three hours. • Enable the toggle switch to proceed. The following Schneider Electric cloud connection settings are displayed (for details, page 125): • **Schneider cloud connection status** • **Connection diagnostics** For information about the cloud infrastructure, see Schneider Electric cloud services, page 123.
Backup & restore, page 180	–	Allows you to save the Panel Server current configuration and restore it.

User Management Menu

User Account Management

A Panel Server administrator with **SECADM** role (default user account **SecurityAdmin**) can create, modify, and delete any user account with **SECADM** or **VIEWER** role. The **SecurityAdmin** user cannot be deleted.

IMPORTANT: User accounts can be managed in EcoStruxure Cybersecurity Admin Expert (CAE) software. See related topic, page 55. When the configuration is deployed from CAE software to the Panel Server gateway(s) connected in the system, all Panel Server-supported parameters managed by CAE software overwrite the corresponding parameters on the Panel Server, including users and passwords.

Creating a User Account

1. Navigate to **User Management > Add User**.
2. In the **Add new user** popup, enter a user name and a password which complies with the password requirements, page 53.

   NOTE:

   - The user name must comply with the following rules:
     - 4 to 16 characters
     - Contain only alphanumeric characters (A-Z, a-z, and 0-9) and the following special characters: !"#$%&'()*+-./;<=>?@[\]^_`
     - Not contain any spaces
     - Be unique
   - The user name cannot be changed after it is saved.
   - The user name is case-insensitive. For example, JSmith, jsmith, or JSMITH are considered the same user name. As a result, duplicate user names cannot be created. If a duplicate user name is entered, an error message is displayed.
   - The user names **SecurityAdmin** and **supportuser** are reserved. Creating a user with this user name displays an error message.

   Result: The new user is displayed in the user table.

Changing a User Password

1. Open the **User Management** menu.
2. Click the pencil icon next to the account name.
3. Enter and confirm the new password (complying with the password requirements, page 53).
4. Click **Edit User** to save the new password.

Removing a User Account

1. Open the **User Management** menu.
2. Click the bin icon next to the account name to delete.
3. Confirm deletion.

   NOTE: At least one user with the **SECADM** role is required.

Commissioning of Modbus Devices

What’s in This Chapter

Adding Modbus Devices Through Webpages 228
Adding Multi-Meter Devices (MCM) 232
Configuring Modbus Devices Through Webpages 233
Configuring Smart Link Modbus Channels 235
Removing Modbus Devices Through Webpages 237

Adding Modbus Devices Through Webpages

Presentation

Modbus TCP/IP and Modbus-SL devices can be added to or removed from the EcoStruxure Panel Server system through the Panel Server webpages.

Discovery of Modbus TCP/IP Devices With a Selective List

In the **Settings > Modbus devices > Device addition > Modbus TCP/IP** webpage, in the **Discovery > Selective list** section, create a list of devices to be discovered by entering the IPv4 address for each device. The default port is `502` (see Ethernet Communication, page 93) and the default unit ID is `255` (see Modbus Gateway Function, page 60).

NOTE: Discovery of Modbus TCP/IP devices using an IPv6 address is not supported.

During device discovery the Panel Server uses, in priority order:

- A custom device model, if applicable (the most recently modified custom device model if more than one apply)
- A built-in model

NOTE: Delete the device and manually discover it using a specific custom model if the choice of custom model used is not appropriate.

Result: The **Discovery result** table shows the following information for each device discovered on the Modbus TCP/IP network:

- Picture (built-in device models)
- Name
- IP address
- Port
- Unit ID
- Virtual server ID

The device is displayed in the **Modbus devices** section.

Manual Addition of Modbus TCP/IP Devices

In the **Settings > Modbus devices > Device addition** webpage, in the **Modbus TCP/IP > Manual addition** section, enter the following information for each device:

- **IP address**
- **Port**
- **Unit ID**
- **Device**

  NOTE: Manual addition of Modbus TCP/IP devices using an IPv6 address is not supported.

Result: Once the device is discovered, it is displayed in the **Modbus devices** section.

To manually add a Modbus TCP/IP device applying a custom device model from the drop-down list, select **Settings > Modbus devices > Device addition > Modbus TCP/IP > Manual addition** then:

- Type the values for
  - **IP address**
  - **Port**
  - **Unit ID**
- Select the device model name in **Device**.

Discovery of Modbus-SL Devices With a Selective List

In the **Settings > Modbus devices > Device addition > Modbus serial** webpage, in the **Discovery > Selective list** section, enter the list of Modbus addresses (1–254) for which the devices must be discovered.

NOTE: If no addresses are entered, discovery is done for addresses 1 to 10.

During device discovery the Panel Server uses, in priority order:

- A custom device model, if applicable (the most recently modified custom device model if more than one apply)
- A built-in model

  NOTE: Delete the device and manually discover it using a specific custom model if the choice of custom model used is not appropriate.

Result: The table shows the following information for each device discovered on the Modbus-SL network:

- Picture
- Name
- Modbus Serial Line
- Physical server ID
- Virtual Server ID

The device is displayed in the **Modbus devices** section.

Manual Addition of Modbus-SL Devices

In the **Settings > Modbus devices > Device addition > Modbus serial > Manual addition > Server ID** webpage, enter the physical server ID of the device to be added and select the device type.

Result: Once the device is added, it is displayed in the **Modbus devices** section.

To manually add a Modbus Serial device applying a custom device model from the drop-down list, select **Settings > Modbus devices > Device addition > Modbus serial > Manual addition** then:

- Type the value for **Physical server ID**.
- Select the custom device model name in **Device**.

Addition of Modbus-SL Devices Connected to a Child Panel Server Gateway

To add Modbus-SL devices connected to a child/downstream Panel Server (see example, page 70), navigate to **Settings > Modbus devices > Device addition > Modbus TCP/IP > Manual addition > IP address**.

Enter:

- The IP address of the child/downstream Panel Server
- The virtual server ID of the Modbus device in **Unit ID**
- The Modbus device type

Result: Once the device is discovered, it is displayed in the **Modbus devices** section.

Modbus Registers Read

To troubleshoot the addition of Modbus devices, navigate to the webpage **Settings > Modbus devices > Registers read > Modbus registers read**. Fill in the Modbus device identification parameters described in the following table and click the **Read registers** button.

NOTE: When a device discovery is in progress, you cannot use the Modbus register reading function.

Result: A table is displayed containing the list of register numbers and the register content in the selected format.

NOTE: When the Panel Server is configured in Reverse gateway mode, the reading register function is supported for Modbus TCP/IP devices only.

Parameter	Availability by device		Description
Device Type	Modbus Serial	Modbus TCP/IP	Select from the list either Modbus Serial or Modbus TCP/IP. Other parameters displayed depend on the device type selected.
Device ID	✓	-	Enter the virtual device ID you want to read registers from. Value range 1–254.
IP address	-	✓	Enter the address of the TCP network.
Port	-	✓	Enter the port of the device.
Unit ID	-	✓	Enter the ID of the device. Value range 1–255.
Function code	✓	✓	Select from the list the Modbus function to use to read the registers of the identified device: • **FC01 Read coils status** • **FC02 Read inputs status** • **FC03 Read holding registers** • **FC04 Read input registers**
Starting register/coil	✓	✓	Enter the number of the first register or coil to be read. For function codes FC01 and FC02, use the following calculation to specify the bit number: (Register number - 1) * 16 + (bit offset+1) where offset is the bit order (from 0 to 15).
Number of registers/coils	✓	✓	Enter the total number of consecutive registers or coils to be read.
Format	✓	✓	For function codes FC03 and FC04, select from the list the format to display the results: • Hexadecimal (default format) • Binary • Signed integer 16 • Unsigned integer 16 The result of function codes FC01 and FC02 is 1 when true and 0 when false.

Adding Multi-Meter Devices (MCM)

Presentation

A multi-component meter (MCM) is composed of a head unit and multiple circuits.

Modbus serial devices associated with multiple meters can be added or removed from the Panel Server through the webpages. The meters must share the same physical server ID or Unit ID. They must be added using custom models, with one custom model for the head unit and one custom model for each associated meter. For example, the Rayleigh multi-circuit meter can be configured as:

- Either 2 three-phase circuits, using 2 dedicated custom models
- Or 6 single-phase circuits, using 6 dedicated custom models

The 2 or 6 circuits (meters) are added manually to the Panel Server as Modbus devices.

Manual Addition of Multi-Meter Devices (MCM)

Follow this procedure to add a device associated with multiple meters.

1. Create a custom model for the head unit and one custom model for each meter associated with the multi-meter device using EPC Web tool, page 153. Import the custom models into Panel Server.
2. At **Settings > Modbus devices > Device addition**, add the head unit and associated meters one by one, using either Modbus serial manual addition or Modbus TCP/IP manual addition, as appropriate for your device..
3. Enter the same physical server ID for Modbus serial devices or the same IP address, port and Unit ID for Modbus TCP/IP devices.
4. For the head unit and each meter, select the appropriate custom model from the drop-down device list. The custom model must be different for each meter.

Once discovered, the devices are displayed in the **Modbus devices** section.

Configuring Modbus Devices Through Webpages

Presentation

You can configure the parameters of connected devices and save your settings using the Panel Server webpages.

Procedure to Configure Modbus Devices

To configure Modbus devices with Panel Server webpages, proceed as follows:

1. Navigate to **Settings > Modbus devices** to view the list of the discovered Modbus devices.

   Result: The list of devices is displayed (with **Connected** written in green under the device name).

2. Select the required device to modify its configuration.

   Result: The parameters of the device are displayed.

3. Enter the data in the fields, referring to the following tables for more information about the parameters.
4. Save your settings by clicking the icon at the bottom right of your screen and selecting **Save**.

Parameter Tables

The following tables list the parameters for the configuration of Modbus devices.

NOTE: For the configuration of Smart Link devices, refer to *Configuring Smart Link Modbus Channels*, page 235.

Identification

Parameter name	Description
Name	Enter the name of the Modbus device.
Label (optional)	Enter the label of the Modbus device.
Device range	For display only
Commercial reference	For display only
Hardware revision	For display only
Device family	For display only

Modbus TCP/IP Information: only displayed for Modbus TCP/IP devices

Parameter name	Description
IP address	IP address of the discovered device
Port	Displays the port used for manual or automatic addition of the device. (Port 502 by default.)
Unit ID	Displays the unit ID used for manual or automatic addition of the device. **NOTE:** Unit ID is generally 255 (or sometimes 1 depending on the physical device).

Modbus Serial Information: only displayed for Modbus SL devices

Parameter name	Description
Physical server ID	IP address detected by the Panel Server on the Modbus serial network. Do not change this value unless you change the Modbus address on your device.
Modbus Serial Line	**1**. Setting not editable.

Modbus virtual

Parameter name	Description
Virtual server ID	Enter the ID of the Modbus virtual server.

Contextualization data

Parameter name	Description
Commodity (optional)	Select the commodity required from the list to indicate the main purpose of the device.
Usage (optional)	Select the usage required from the list to indicate the precise function of the device, for example, the type of lighting to be monitored: Lighting (Exterior and Park) or Lighting (Interior).
Zone (optional)	Select the zone in the list, as contextualization data. Click the Settings icon to: • Create a new zone • Modify a zone name • Delete a zone For more information about creating, modifying and deleting zones, refer to Zone Management, page 300.

Configuring Smart Link Modbus Channels

Presentation

For Smart Link devices configured in the Panel Server webpages, you can configure each of the available channels at **Settings > Modbus Devices > Configuring channel settings**. The following information is displayed:

Parameter name	Description
Data status	Indicates the status of the data.
Last synchronization status	Indicates if the last synchronization was successful.
Refresh the configuration	Click on this button to refresh the configuration.
Table indicating channel configuration	Columns in the table display the following information for each channel: • **Channel** number • **Input 1 name** • **Input 2 name** • **Output name**

Procedure to Configure Channels

Follow this procedure to configure channels:

1. Click on the pencil icon to open the configuration for a channel.

   Result: Editable fields open below the channels table.
2. Select the **I/O Type** from the following list:
   - **Not connected**
   - **Wired device**
   - **Pulse counter**
   - **Standard I/O**

   The settings shown below are for configuration of a **Wired device**. The settings for **Pulse counter** and **Standard I/O** are the same as those for the Panel Server digital inputs, which are described in the specific topic, page 149.
3. Select the **Device Type** for **Input 1**.

   NOTE: If you select **OF24** as the **Device Type**, you need to enter data for **Input 2** in addition.
4. Enter the data for **Input 1** in the fields, referring to the following table for more information about the parameters.

Parameter Tables

Input 1

Parameter	Description
Name	Enter the input name of the device.
Label	Enter the input label.
Commodity	Select the commodity type in the list, as contextualization data.
Usage	Select the usage in the list, as contextualization data.

Input 1 (Continued)

Parameter	Description
Zone	Select the zone in the list, as contextualization data. Click the Settings icon to: • Create a new zone • Modify a zone name • Delete a zone For more information about creating, modifying and deleting zones, refer to Zone Management, page 300.
I/O Contextualization with I/O type **Standard I/O**	Select the contextualization data in the list. **NOTE:** Refer to the following table for interpretation of **Meaning of input = 0** and **Meaning of input = 1** for certain signal elements.

For inputs configured as **Standard I/O**, the following **I/O Contextualization** selections, display a result for **Meaning of input = 0** and **Meaning of input = 1** that should be interpreted as shown in the table below. For other **I/O Contextualization** selections, the result displayed requires no interpretation.

Contextualization (Signal element)	Displayed		Interpretation	
	Meaning of input = 0	**Meaning of input = 1**	**Meaning of input = 0**	**Meaning of input = 1**
Trip indicator status (SD)	On	Off	In fault	No fault
Electrical trip indicator status (SDE)	On	Off	In fault	No fault
Earth leakage fault	On	Off	In fault	No fault
Ground fault	On	Off	In fault	No fault
Forced freewheel stop	Off	On	Inactive	Active
Battery status	OK	Error	OK	In fault
Advanced protection	In fault	No fault	In fault	OK
Motor preheating	Off	On	Off	Preheat
UPS status	OK	Error	OK	In fault
UPS running mode	Supplying	Standby	Supplying	By pass
Under temperature	NotUnderTemperature	UnderTemperature	Inactive	Active
Over temperature	NotOverTemperature	OverTemperature	Inactive	Active
Equipment status	Stopped	Running	Stop	Start
Tariff status (1–5)	Off	On	Inactive	Active

Removing Modbus Devices Through Webpages

Presentation

It is possible to remove Modbus devices from the Panel Server system. This allows you to discover the device from another Panel Server, for example.

Removal Procedure

Follow this procedure to remove Modbus devices from the system:

1. Navigate to **Settings > Modbus devices > Modbus devices** to view the list of connected devices.
2. Select the device to be removed from the system.
3. Click the bin icon on the top right side of the webpage.
4. Confirm removal process.

   Result: Once the Modbus device is successfully disconnected from the Panel Server, it is no longer visible in the list of Modbus devices.

Commissioning of Wireless Devices Through Webpages

What's in This Chapter

Discovery of Wireless Devices Through Webpages 239
Discovery of XB5R Transmitters (ZBRT) 242
Configuring Wireless Devices Through Webpages 244
Configuration of Wireless Energy Devices 246
Configuration of Wireless Indication Auxiliaries 250
Configuration of PowerTag Control Devices Through Webpages 251
Configuration of Ambient Sensors Through Webpages 254
Configuration of Exiway Link Devices 255
Removing Wireless Devices Through Webpages 256
Adding Wireless Devices Connected to a Child Gateway (Universal and Advanced Models) 258

Discovery of Wireless Devices Through Webpages

Presentation

Wireless devices installed in the Panel Server system can be discovered through the EcoStruxure Panel Server webpages by using one of the methods described: Automatic or Selective.

- **Automatic** (default): discovers wireless devices in the Panel Server system
- **Selective**: discovers only the wireless devices belonging to a selective list. You can enter the list manually in the webpages or you can upload a prepared file containing the list.

The **Protect Plus** function allows you to launch a discovery with heightened security by using the 36-character install code of 16-character RF-ID devices. The following device families have a 16-character RF-ID:

- PowerTag Control
- PowerLogic HeatTag
- PowerLogic PD100
- MasterPacT MTZ with MicroLogic Active AP or EP control unit
- Exiway Link

With **Protect Plus** selected (selected by default), automatic discovery is available for 8-character RF-ID devices, for example, PowerTag Energy. To discover 16-character RF-ID devices, use a selective list which includes the 36-character install code of the devices.

With **Protect Plus** deselected, all devices can be discovered without benefiting from the heightened security level.

Automatic Discovery of Wireless Devices Through Webpages

The following table indicates automatic discovery availability depending on **Protect Plus** setting:

Device type	Example	Discovery available	
		Protect Plus selected	Protect Plus deselected
8-character RF-ID	PowerTag Energy	Yes	Yes
16-character RF-ID	PowerLogic HeatTag	No	Yes

NOTE: For automatic discovery of XB5R transmitters (ZBRT), follow the specific procedure, page 242.

To perform an automatic discovery of wireless devices through webpages, proceed as follows:

1. Log in to the Panel Server webpages (see how to access the webpages, page 201).
2. Navigate to **Settings > Wireless devices > Discovery > Discovery method** and click **Automatic**.

3. Click **Start** to scan the environment and discover available wireless devices.

   Result: Devices appear in the list of discovered wireless devices and in the device tree view as they are discovered.

   In certain cases, devices may not be fully discovered by the Panel Server. In the **Rejected Discovery** table, a column labelled **Status** gives the cause of the rejected discovery.

   For devices indicating **Install code not provided**, use a selective list to enter the missing information and launch a selective discovery.

   NOTE: A popup message indicates if the network occupancy is high or saturated and suggests solutions. If action is required, navigate to **Settings > Wireless devices > Network configuration > Wireless communication**.

4. If required, you can select the wireless device in the device tree view and click **Locate** to find the device in the panel.

   Result: The status LED of the selected device blinks fast green in the panel.

5. If one of the located wireless devices is not part of your system, click **Delete** to reject the device.
6. Configure the wireless devices.

Selective Discovery of Wireless Devices Through Webpages

Selective discovery uses the RF-ID of a wireless device to perform a discovery.

The following table indicates selective discovery availability depending on **Protect Plus** setting:

Device type	Example	Discovery available	
		Protect Plus selected	Protect Plus deselected
8-character RF-ID	PowerTag Energy	Yes	Yes
16-character RF-ID	PowerLogic HeatTag	With install code*	Yes
* Recommended to benefit from heightened security during installation			

To perform selective discovery of wireless devices through webpages, proceed as follows:

1. Log in to the Panel Server webpages (see how to access the webpages, page 201).
2. Navigate to **Settings > Wireless devices > Discovery > Discovery method** and click **Selective**.

   All and only the wireless devices in the selective list can be discovered by the Panel Server. The Panel Server uses the RF-ID of each device to discover it.

3. Upload a prepared list file, page 241 by clicking **Upload file**, or fill in the table that opens with the following information for each device in the selective list:
   - RF-ID
   - Virtual server ID in the range 1 to 254 (optional). If the ID is not specified, the Panel Server assigns the first available value.
   - Install code (with **Protect Plus** enabled) for applicable devices

   IMPORTANT: Uploading a prepared selective list erases any data that has been added manually to the selective list in the webpages.

4. Click **Start** to scan the environment and discover the wireless devices in the list.

   Result: Devices appear in the list of discovered wireless devices and in the device tree view as they are discovered.

   In certain cases, devices may not be fully discovered by the Panel Server. In the **Rejected Discovery** table, a column labelled **Status** gives the cause of the rejected discovery. Check the cause and correct the issue before relaunching the selective discovery.

   If the device is not discovered and does not appear in the **Rejected Discovery** table, refer to Troubleshooting webpages, page 261.

   NOTE: A popup message indicates if the network occupancy is high or saturated and suggests solutions. To check the network occupancy, navigate to **Settings > Wireless devices > Network configuration > Wireless communication**.

Virtual Server ID

A virtual ID address is applied during the discovery process with the Panel Server. The first virtual server ID is allocated to the first discovered device and incremented by one for each device discovered. By default, virtual server IDs allocated to wireless devices start from 100.

When using the selective discovery process, the virtual server IDs can be defined in the selective list. If they are not defined in the list, virtual server IDs are allocated in order of discovery, as above.

The virtual server ID assigned to the wireless devices can be changed after the discovery process is done.

Defining the List of Selected Devices

The selective list is a csv file that lists the selected wireless devices to be uploaded on the Panel Server webpages. Each row in the csv file contains the data for one device in the following format, separated by semi-colons:

- RF-ID with 0x prefix (mandatory)
- Virtual server ID (optional)
- Install code with 0x prefix (for use with **Protect Plus**)

Example of csv file:

```
1  0xFFA018F4FFA018F4;100;0x12345678912345678912345678912345678
2  0x5C0272FFFE1E561C;;0x98765432198765432198765432198765432
3  0x086BD7FFFED29F1D;104;0x987654320987654321987654320987654321
4  0x8FFED123;103;
```

Finding the Device RF-ID and Install Code

To obtain the RF-ID and install code of a device, scan the QR code of the device. Follow the link to the Go2SE landing page of the device to find the relevant information:

zb = RF-ID (8 or 16 characters)

ic = install code made up of 36 characters (available depending on the device)

Discovery of XB5R Transmitters (ZBRT)

Presentation

XB5R transmitters for wireless and batteryless ZBRT pushbutton devices can be discovered in the Panel Server.

Discovery Procedure

1. Launch the Panel Server webpage in the web browser.
2. Log in to the webpages (see how to access the webpages, page 201).
3. Navigate to **Settings > Wireless devices > Discovery** and click **Automatic**.
4. Check that the ZBRZ1 commissioning module is not connected to any ZBRT pushbutton device.
5. Click **Start**.
6. Connect the ZBRZ1 commissioning module to each ZBRT pushbutton device in turn. For more information, consult the *ZBRZ1 Instruction sheet* NNZ21729.
7. Maintain the connection for a few seconds. The ZBRT device is paired when the accessory is connected, and appears in the discovery result table.
8. Once discovery is completed you can view the list of the discovered wireless devices in webpage **Settings > Wireless devices > Wireless devices**.
9. Configure the wireless devices.

   NOTE: The Modbus virtual ID assigned to the wireless devices can be changed after the discovery process is done.

Configuration Procedure

To configure ZBRT devices with Panel Server webpages, proceed as follows:

1. Navigate to **Settings > Wireless Devices** to view the list of the discovered wireless devices.

   Result: The list of discovered devices is displayed (with **Connected** written in green under the device name).
2. Select the required device to modify its configuration.

   Result: The parameters of the device are displayed.
3. Enter the data in the fields, referring to the following tables for more information about the parameters.
4. Save your settings by clicking the icon at the bottom right of your screen and selecting **Save**.

Parameter Tables

Identification

Parameter name	Description
Name	Enter the name of the wireless device.
Label (optional)	Enter the label of the wireless device.
Device range	For display only
Commercial reference	For display only

Identification (Continued)

Parameter name	Description
Hardware revision	For display only
Device family	For display only

Modbus virtual

Parameter name	Description
Virtual server ID	Enter the ID of the Modbus virtual server.

Contextualization data

Parameter name	Description
Commodity (optional)	Select the commodity required from the list to indicate the main purpose of the device.
Usage (optional)	Select the usage required from the list to indicate the precise function of the device.
Zone (optional)	Select the zone in the list, as contextualization data. Click the Settings icon to: • Create a new zone • Modify a zone name • Delete a zone For more information about creating, modifying and deleting zones, refer to Zone Management, page 300.

Setting the Retention Time for ZBRT1 Pushbutton Devices

The retention time is the length of time the ZBRT1 pushbutton status remains ON after being pressed.

Set the button status retention time of the ZBRT1 pushbutton device between 100 and 1000 ms (default value 500 ms) at **Settings > Wireless devices > Global functional settings**. Select a value from the list.

Removal Procedure

Follow the removal procedure for ZBRT devices, described in Removing Wireless Devices Through Webpages, page 257.

Configuring Wireless Devices Through Webpages

Presentation

Wireless devices can be configured through Panel Server webpages. The procedure is similar for most wireless devices, with families of devices having specific parameters, depending on the device. The procedure and parameters common to all wireless devices is described in this topic. For the following device families, click the link to see parameters and other information specific to that family:

- Wireless energy devices, page 246, for example, PowerTag Energy devices
- Wireless indication auxiliaries, page 250
- PowerTag Control devices, page 251
- Ambient sensors, page 254
- Exiway Link devices, page 255

Configuration Procedure

To configure wireless devices with Panel Server webpages, proceed as follows:

1. Navigate to **Settings > Wireless Devices** to view the list of the discovered wireless devices.

   Result: The list of discovered devices is displayed (with **Connected** written in green under the device name).
2. Select the required device to modify its configuration.

   Result: The parameters of the device are displayed.
3. Enter the data in the fields, referring to the following tables and specific tables for the device family for more information about the parameters.
4. Save your settings by clicking the icon at the bottom right of your screen and selecting **Save**.

   NOTE: When saving the settings, a message may be displayed indicating either that 90% of wireless bandwidth capacity is reached or that the Panel Server is over configured. Follow the recommendation in the message to increase the communication period of a particular device or to reduce the number of wireless devices.

The following tables list the parameters common to the configuration of all wireless devices.

Parameter Tables

Identification

Parameter name	Description
Name	Enter the name of the wireless device.
Label (optional)	Enter the label of the wireless device .
Device range	For display only
Commercial reference	For display only
Hardware revision	For display only
Device family	For display only

Modbus virtual

Parameter name	Description
Virtual server ID	Enter the ID of the Modbus virtual server.

Contextualization data

Parameter name	Description
Commodity (optional)	Select the commodity required from the list to indicate the main purpose of the device.
Usage (optional)	Select the usage required from the list to indicate the precise function of the device, for example, the type of lighting to be monitored: Lighting (Exterior and Park) or Lighting (Interior).
Zone (optional)	Select the zone in the list, as contextualization data. Click the Settings icon to: • Create a new zone • Modify a zone name • Delete a zone For more information about creating, modifying and deleting zones, refer to Zone Management, page 300.

Configuration of Wireless Energy Devices

Presentation

Wireless energy devices can be configured through Panel Server webpages.

Configuration Procedure

To configure wireless energy devices follow the procedure in Configuring Wireless Devices Through Webpages, page 244.

The following tables list the parameters for the configuration of wireless energy devices.

The fields displayed depend on the type of device.

Parameter Tables

Identification

Refer to Configuring Wireless Devices Through Webpages, page 244.

Electrical characteristics

Parameter name	Description
Phase sequence	Select from the list to define the phase sequence of the meter depending on the way the physical panel is wired and according to the phase indication printed on the product, for example ACB.
External neutral voltage sensor	Select the availability from the list: • **Available** • **Not available** **NOTE: Available** for display only, depending on the power meter.
Mounting position	Select the mounting position from the list: • **Top/Line**: The PowerTag Energy device is mounted on the top of the device. • **Bottom/Load**: The PowerTag Energy device is mounted at the bottom of the device.
Current flow	Select the **Current flow** to define the convention for the energy device to count energies. See the section Current Flow, page 247 for more information about filling this parameter.
Power factor sign convention	Select the power factor sign convention form the list. The setting has an influence on the convention used to sign the power factor. • IEC • IEEE For more information, see the section Power Factor Sign Convention, page 248.

Communication Settings

Parameter name	Description
Communication period (s)	When available for the selected wireless device, you can set the communication period at a value different from the value set at family devices level, page 110. Select a value of between 2 and 120 seconds from the list (default setting 5 seconds). **NOTE:** It is possible to set 2 seconds as the communication period of a device which belongs to the Energy-related wireless devices family, like Acti9 Active, Acti9 PowerTag, Acti9 Vigi, PowerLogic Tag (PLT). **NOTE:** Use a maximum setting of 90 seconds if power demand calculation is required.

Modbus virtual

Refer to Configuring Wireless Devices Through Webpages, page 245.

Associated circuit breaker

Parameter name		Description
Circuit breaker characteristics	**Circuit breaker label** (optional)	Enter the label of the associated circuit breaker.
	Rated current (A)	Enter the value for the rated current in Amps of the associated circuit breaker or the protective device rating. It cannot be higher than Imax of the device.
	Rated Voltage (V) (optional)	Enter the value of the rated voltage for the associated circuit breaker. • LN rated voltage for 3P4W installation. • LL rated voltage for 3P3W installation.

Contextualization data

Refer to Configuring Wireless Devices Through Webpages, page 245.

Protection

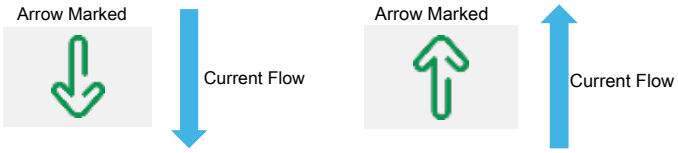
Parameter name	Description
Protection curve	For display only
Earth leakage pre-alarm threshold	Select the threshold for the earth-leakage pre-alarm.
Over voltage pre-alarm threshold	Select the threshold for the over voltage pre-alarm.
Overcurrent pre-alarm threshold	Select the threshold for the overcurrent pre-alarm.

Current Flow

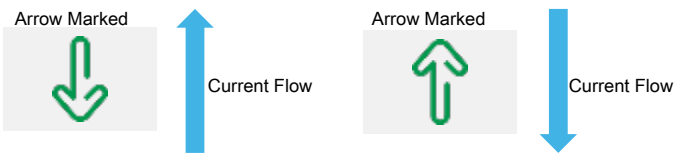
For PowerTag Energy devices F160 and Rope, selecting the current flow defines the convention for the PowerTag Energy device to count energies.

The current flow can be **Direct** or **Reverse**:

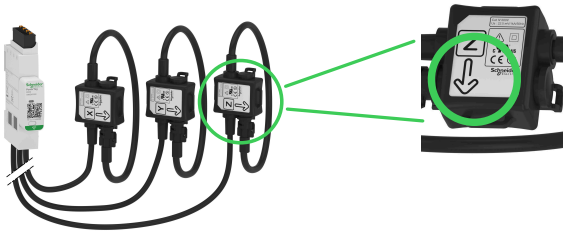
- **Direct**: If the arrow marked on the PowerTag Energy device is in the same direction as the current flow.



- **Reverse**: If the arrow marked on the PowerTag Energy device is in the opposite direction to the current flow.



The following figures show the location of the arrow marked on the PowerTag Energy F160 and Rope:

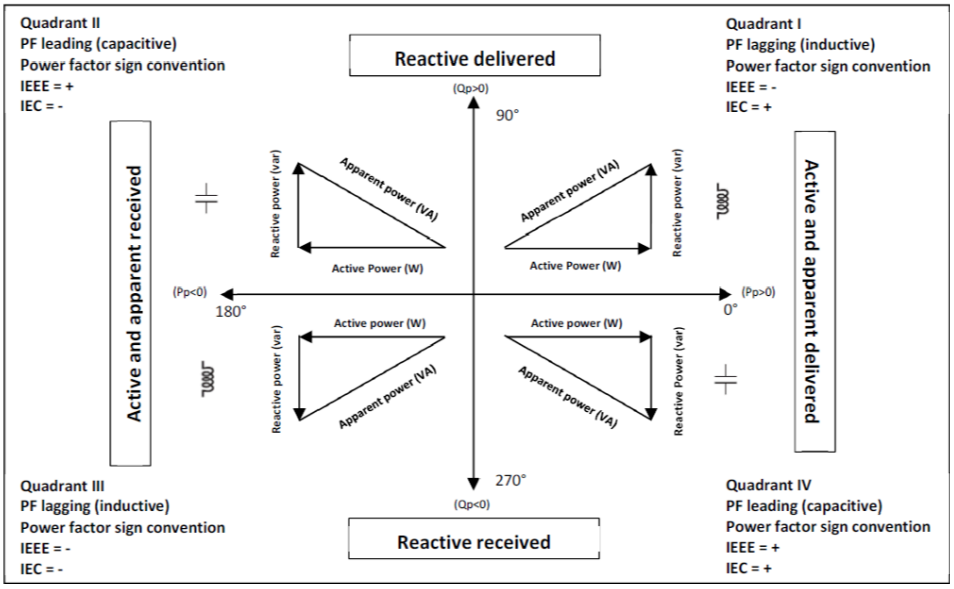
PowerTag Energy F160	PowerTag Rope
	

Power Factor Sign Convention

The power factor sign convention setting can be one of the following:

- IEC: In this setting,
  - when active power is negative, the power factor sign is **–**.
  - when active power is positive, the power factor sign is **+**.
- IEEE: In this setting,
  - when the load is capacitive, the power factor sign is +.
  - when the load is inductive, the power factor sign is –.

The following diagram summarizes the power factor sign convention:



Power Demand Calculation Time Interval

The Panel Server calculates the following values:

- Active power demand over the specified time interval
- Peak active power demand value during the specified interval

Set the demand calculation time interval between 1 and 60 minutes at **Settings > Wireless devices > Global functional settings**. A pop-up message is displayed if you try to set an invalid value.

NOTE: Power demand calculation is not compatible with devices using a communication period longer than 90 seconds.

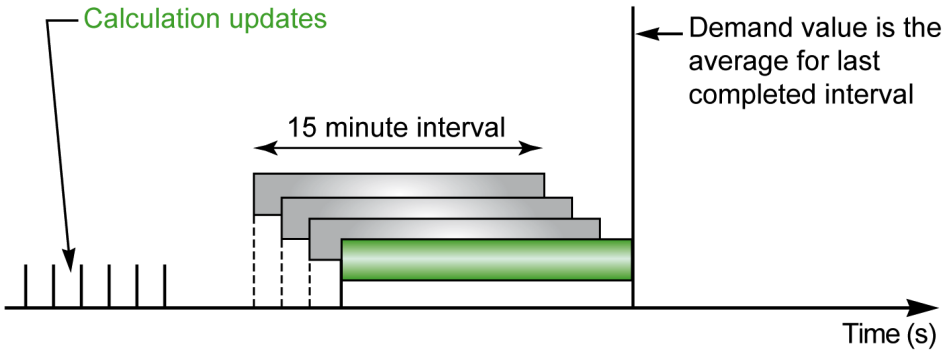
You can reset the peak power demand value to 0 for:

- All PowerTag devices connected to the Panel Server, including PowerTag Rope on the Panel Server webpages at **Settings > Wireless devices > Global functional settings**
- Individual devices at **Monitoring & Control**, by clicking on the device name to open the device page and scrolling to **Active power demand**.

The Panel Server stores the date and time of:

- Each new maximum (peak) value of active power demand since the last reset
- Reset of peak active power demand

The power demand value is calculated using arithmetical integration of power RMS values over a period of time, divided by the length of the period. The result is equivalent to the energy accumulated during the period of time divided by the length of the period. The power demand is calculated according to the sliding block method.



At the end of the power demand calculation interval and then every one tenth of the interval, for example, for an interval of 15 minutes, every 1 minute 30 seconds:

- The demand value over the interval is calculated and updated.
- Calculation of a new demand value is initialized on a new interval:
  - By eliminating the contribution of the first tenth of the previous interval
  - By adding the contribution of the latest tenth

Configuration of Wireless Indication Auxiliaries

Presentation

Wireless indication auxiliaries can be configured through Panel Server webpages.

Configuration Procedure

To configure wireless indication auxiliaries, follow the procedure in Configuring Wireless Devices Through Webpages, page 244.

The following tables list the parameters for the configuration of wireless indication auxiliaries.

Parameter Tables

Identification

Refer to Configuring Wireless Devices Through Webpages, page 244.

Communication Settings

Parameter name	Description
Communication period	8 hours (for display only)

Modbus virtual

Refer to Configuring Wireless Devices Through Webpages, page 245.

Auxiliary position

Parameter name	Description
Auxiliary position	Select the position from the list.

Contextualization data

Refer to Configuring Wireless Devices Through Webpages, page 245.

Configuration of PowerTag Control Devices Through Webpages

Presentation

PowerTag Control devices can be configured through Panel Server webpages.

Configuration Procedure

To configure PowerTag Control devices follow the procedure in Configuring Wireless Devices Through Webpages, page 244.

Parameter Tables

Identification

Refer to Configuring Wireless Devices Through Webpages, page 244.

Communication Settings

Parameter name	Description
Communication period (s)	When available for the selected wireless device, you can set the communication period at a value different from the value set at family devices level, page 110. Select a value of between 5 and 120 seconds from the list.

Modbus virtual

Refer to Configuring Wireless Devices Through Webpages, page 245.

Input/Output Settings

Parameter name	Description
Local Control	Toggles local control on or off. **IMPORTANT:** When **Local Control** is disabled, no manual control is possible on the device.
Configuration Type	Select from the list: • **Contactor without feedback loop**: Configure parameters for Output and Input separately • **Contactor with feedback loop** • **Impulse relay** The parameters displayed depend on the selection of configuration type. See details in the following tables.

Parameters for Contactor without feedback loop

Parameter name		Description
Output	**I/O Type**	Select from the list: • **Standard I/O** • **Not connected**
	Name	Enter the name of the wireless device.
	Label	Enter the label of the wireless device (optional).
	I/O Contextualization	Select an option from the list.
	Status name	If you select **Custom** as contextualization option, then enter the custom name for the device.

Parameters for Contactor without feedback loop (Continued)

Parameter name		Description
	Meaning of output = 0	Displayed values depend on selection of **I/O Contextualization**. Enter your custom values if you select **Custom** as contextualization option. **NOTE:** Clicking the double arrow icon on the right allows you to swap the meanings of outputs 0 and 1.
	Meaning of output = 1	Displayed values depend on selection of **I/O Contextualization**. Enter your custom values if you select **Custom** as contextualization option. **NOTE:** Clicking the double arrow icon on the right allows you to swap the meanings of outputs 0 and 1.
	Commodity	Select the commodity to be monitored from the list.
	Usage	Select the usage to be monitored from the list.
	Zone	Select the zone in the list, as contextualization data. Click the Settings icon to: • Create a new zone • Modify a zone name • Delete a zone For more information about creating, modifying and deleting zones, refer to Zone Management, page 300.
Input	**I/O Type**	Select from the list: • **Standard I/O** • **Not connected**
	Name	Enter the name of the wireless device.
	Label	Enter the label of the wireless device (optional).
	I/O Contextualization	Select an option from the list.
	Meaning of output = 0	**Engaged** (for display only). **NOTE:** Clicking the double arrow icon on the right allows you to swap the meanings of outputs 0 and 1.
	Meaning of output = 1	**Released** (for display only). **NOTE:** Clicking the double arrow icon on the right allows you to swap the meanings of outputs 0 and 1.
	Commodity	Select the commodity to be monitored from the list.
	Usage	Select the usage to be monitored from the list.
	Zone	Select the zone in the list, as contextualization data. Click the Settings icon to: • Create a new zone • Modify a zone name • Delete a zone For more information about creating, modifying and deleting zones, refer to Zone Management, page 300.

Parameters for Contactor with feedback loop and for Impulse Relay

Parameter name		Description
I/O Type		Select from the list: • **Standard I/O** • **Not connected** **NOTE:** No parameters are displayed if **Not connected** is selected.
Output/Input Feedback Loop	**Name**	Enter the name of the wireless device.
	Label	Enter the label of the wireless device (optional).
	Commodity	Select the commodity to be monitored from the list.
	Usage	Select the usage to be monitored from the list.
	Zone	Select the zone in the list, as contextualization data. Click the Settings icon to: • Create a new zone • Modify a zone name • Delete a zone For more information about creating, modifying and deleting zones, refer to Zone Management, page 300.
	I/O Contextualization	Select an option from the list.
	Status name	If you select **Custom** as contextualization option, then enter the custom name for the device.
	Meaning of output = 0	Displayed values depend on selection of **I/O Contextualization**. Enter your custom values if you select **Custom** as contextualization option. **NOTE:** Clicking the double arrow icon on the right allows you to swap the meanings of outputs 0 and 1.
	Meaning of output = 1	Displayed values depend on selection of **I/O Contextualization**. Enter your custom values if you select **Custom** as contextualization option. **NOTE:** Clicking the double arrow icon on the right allows you to swap the meanings of outputs 0 and 1.

Configuration of Ambient Sensors Through Webpages

Presentation

Ambient sensors can be configured through Panel Server webpages.

For a complete list of supported ambient sensors, refer to the respective release notes, page 10:

- DOCA0249•• *EcoStruxure Panel Server Entry - Firmware Release Notes*
- DOCA0178•• *EcoStruxure Panel Server Universal - Firmware Release Notes*
- DOCA0248•• *EcoStruxure Panel Server Advanced - Firmware Release Notes*

Configuration Procedure

To configure ambient sensors, follow the procedure in Configuring Wireless Devices Through Webpages, page 244.

Depending on the sensor, if necessary, during the configuration procedure, identify the specific sensor in its location by clicking **Start** in **Locate**. The sensor LED blinks for 30 seconds. This enables you to select the required sensor to modify its configuration.

Parameter Tables

Identification

Refer to Configuring Wireless Devices Through Webpages, page 244.

Communication Settings

Parameter name	Description
Communication period (s)	When available for the selected wireless device, you can set the communication period at a value different from the value set at device family level, page 110. Select a value of between 60 and 600 seconds from the list. The change is applied at the next communication with the device.

Modbus virtual

Refer to Configuring Wireless Devices Through Webpages, page 245.

Contextualization data

Refer to Configuring Wireless Devices Through Webpages, page 245.

Configuration of Exiway Link Devices

Presentation

Exiway Link devices are wireless emergency lighting devices.

Configuration Procedure

To configure Exiway Link devices follow the procedure in Configuring Wireless Devices Through Webpages, page 244:

Parameter Tables

Identification

Refer to Configuring Wireless Devices Through Webpages, page 244.

Modbus virtual

Refer to Configuring Wireless Devices Through Webpages, page 245.

Contextualization data

Refer to Configuring Wireless Devices Through Webpages, page 245.

Removing Exiway Link Devices

NOTICE

HAZARD OF INCORRECT REMOVAL OF DEVICES ON A SHARED NETWORK

- Before removing an Exiway Link device, check if other devices on the same network may be impacted.
- Remove devices in the correct order if they are part of a mesh architecture.

Failure to follow these instructions may result in incorrect functioning of devices.

Exiway Link devices can be part of a mesh network. Removing one device on this network can have an impact on other devices. If you need to remove all devices, ensure that you remove them in the correct order.

Removing Wireless Devices Through Webpages

Presentation

To remove one or several wireless devices through EcoStruxure Panel Server webpages, follow the procedures in the subsequent sections, as applicable:

- Remove all connected wireless devices
- Remove one connected wireless device
- Forcing removal of one or several unconnected wireless devices

Some wireless devices have a local method to remove the devices. Refer to the instruction sheet of the specific device. For example, for wireless indication auxiliaries for ComPacT NSX and ComPacT NSXm circuit breakers, consult the instruction sheet available on the Schneider Electric website: NNZ8882801.

Procedure to Remove All Wireless Devices

1. Navigate to **Settings > Wireless devices > Network Configuration** to view the list of discovered wireless devices.
2. In the **Wireless device management** section, click the **Remove all devices** button.

   Result: A message displays to confirm the removal of the wireless devices from the configuration.

   NOTE: If your list of discovered wireless devices contains Exiway Link devices, a popup message is displayed to indicate that the removal of all devices may not function correctly. See Removing Exiway Link Devices for more information, page 255.

   NOTE: For removal of ZBRT devices, see Procedure to Remove a ZBRT Pushbutton Device, page 257.
3. Click **Yes** to initiate the removal process for all devices in the Panel Server system.
4. A progress bar shows the progress of the request execution. Wait until the progress bar is completed, indicating that all wireless devices should have received removal order. The process duration depends on the device. It may take up to 10 minutes.

   Result: Once a wireless device is successfully removed, it is no longer visible in the list of discovered wireless devices.

Procedure to Remove One Wireless Device

1. Navigate to **Settings > Wireless devices** to view the list of discovered wireless devices.
2. Select the device to be removed from the configuration.
3. Click the bin icon on the right side of the webpage.

   NOTE: If the selected device is an Exiway Link device, a popup message is displayed to indicate that the removal of this device may impact other devices on the same network. See Removing Exiway Link Devices for more information, page 255.

   NOTE: For removal of ZBRT devices, see Procedure to Remove a ZBRT Pushbutton Device, page 257.
4. Click **Yes** to initiate the removal process.
5. Wait until removal is completed. The process duration depends on the devices. It may take up to 10 minutes.

   Result: Once the wireless device is successfully removed, it is no longer visible in the list of discovered wireless devices.

Procedure to Remove an XB5R Transmitter (ZBRT)

1. In the webpages, navigate to **Settings > Wireless devices** to view the list of discovered wireless devices.
2. Connect the ZBRZ1 commissioning module to the ZBRT pushbutton.
3. Immediately press the ZBRT pushbutton six times to decommission the device.
4. Wait 30 seconds.

   If the device in still on the discovered wireless devices list, continue with this procedure.
5. Select the ZBRT pushbutton device to be removed from the configuration.
6. Click the bin icon on the right side of the webpage.
7. Click **Yes** to initiate the removal process.

   Result: The status of the device is shown as **Removing**.
8. Click the **Force remove** button

   NOTE: After performing a **Remove all devices**, the status of all connected ZBRT devices is shown as **Removing**. Perform a **Force remove** for each device individually.

Procedure to Force Removal of Wireless Devices

It is possible that the removal process of one or several devices is unsuccessful when a device is not powered or is out of order. If a device has not been removed 10 minutes after the removal process began, the status is shown as **Removing** in red in the list of discovered devices. You can force removal of a device from the Panel Server system.

To force device removal, from **Settings > Wireless devices**, select the device and click the **Force remove** button.

Result: Once the wireless device is successfully removed from the Panel Server configuration, it will not be visible in the list of discovered devices .

If you want to discover the forced removed device with a new Panel Server, reset and power off this device.

Adding Wireless Devices Connected to a Child Gateway (Universal and Advanced Models)

Presentation

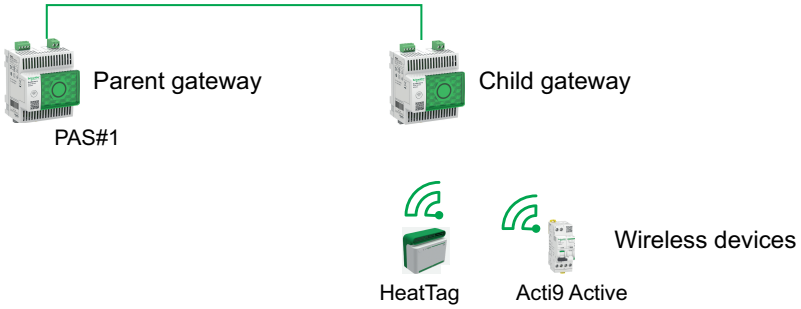
With Panel Server Universal and Advanced, you can display and publish data from wireless devices connected to a child gateway. In addition, the Panel Server Advanced can log the data, display them in the trending screens and export them in a csv file.

A wireless child gateway is a gateway that is connected downstream to one Panel Server via Modbus TCP. It incorporates wireless data aggregation tables to be enable direct and autonomous response to Modbus requests. In this family of products, only Smartlink SIB, PowerTag Link, and Panel Server are supported. Other gateways, such as EGX100, EGX300, and Link150, operate as transparent gateways which transfer Modbus requests and responses to and from end devices. They have no data aggregation table to handle Modbus requests, and are therefore not impacted by the limitations introduced by such tables.

The child gateway can be one of the following:

- Panel Server
- PowerTag Link
- Smartlink SIB

The following diagram shows a typical architecture of wireless devices connected to a child/downstream Panel Server in a separate topology. The child/downstream gateway is connected to one Ethernet port of the parent/upstream Panel Server (PAS#1).



NOTE: Panel Server Universal and Advanced allow you to display data from wireless devices connected to a child gateway. The parent Panel Server gateway monitors the Modbus TCP/IP communication status of the child gateway and its downstream wireless devices, and reports an alarm when the child gateway disconnects.

Availability

This function is available on Panel Server Universal and Advanced.

Procedure to Add the Wireless Devices to the Child Gateway and to the Parent Gateway

1. Connect to the child gateway using EcoStruxure Power Commission desktop or Panel Server webpages
2. Discover all the wireless devices in the child gateway.

   NOTE: Parameter settings entered in the child gateway are not transferred to the parent gateway.
3. Connect to the parent gateway using the Panel Server webpages.

4. Each wireless device is added to the parent gateway using the Modbus/TCP manual addition procedure by accessing the **Settings > Modbus devices > Device addition > Modbus TCP/IP > Manual addition** webpage and entering the following information for each wireless device:
   - IP address: enter the IP address of the child gateway.

     NOTE: When using a Panel Server Entry (PAS400) as child gateway, it is recommended to use a static IP address to simplify the commissioning procedure (refer to Ethernet Communication, page 93). If the Panel Server Entry is connected in DHCP mode, follow the procedure in Appendix G, page 297 to retrieve the IP address.
   - Port: usually port 502
   - Unit ID: enter the virtual server ID assigned by the child gateway to the wireless device
   - Device: select the device type in the drop-down selection list
5. Repeat step 4 for each wireless device.

Troubleshooting

Troubleshooting the EcoStruxure Panel Server

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. See NFPA 70E, CSA Z462, NOM 029-STPS or local equivalent.
- This equipment must only be installed and serviced by qualified electrical personnel.
- Turn off all power supplying this equipment before working on or inside equipment.
- Always use a properly rated voltage sensing device to confirm power is off.
- Re-install all devices, doors, and covers before turning on power to this equipment.
- Do not exceed the device ratings for maximum limits.

Failure to follow these instructions will result in death or serious injury.

Problem	Diagnostics	Action
The Panel Server is not found by EcoStruxure Power Commission software during self-discovery.	The Panel Server firmware version is greater than or equal to 002.007.000.	None. Self-discovery by using EcoStruxure Power Commission software is not supported on Panel Server gateways with firmware version greater than or equal to 002.007.000.
The Panel Server with firmware version up to 002.006.001 is not found by EcoStruxure Power Commission software during self-discovery. On first connection to the Panel Server from a PC, the Panel Server is not displayed under **Network**.	MAC address (printed on the Panel Server front face) not recognized. You need to convert the hexadecimal value of the MAC address to a decimal value to get the Panel Server IP address.	Follow the procedure to convert the hexadecimal value of the MAC address to the decimal value to get the IP address, page 263.
The status LED is not lit.	Source power not applied or not stable.	Apply power or check power source.
The status LED goes off on a PoE (Power over Ethernet) Panel Server configured in switch mode.	Both Ethernet ports are connected, with ETH2 connected to a power supply. The Ethernet port was closed by the router to avoid an IP loop.	Perform one of the following actions: • Configure the Ethernet ports in separated mode to continue using both ETH1 and ETH2 ports. • Use ETH2 port only, connected to the power supply, to continue using switched mode. Correct the configuration of the Panel Server and apply power.
Panel Server status LED blinking orange	Panel Server in degraded health state.	See the Panel Server Diagnostics webpages, page 171. In particular, you can look at the Panel Server health state, which gives information about which internal component caused the Panel Server to start blinking orange. For example: • If Modbus is identified, then a Modbus-SL device may have been powered off or removed from EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, but EcoStruxure Power Commission software did not remove the device as seen from the gateway. • If IEEE 802.15.4 is identified, then a device may be powered off and stopped communicating for a few cycles. • If a local device is identified, then there may be an IPv4 address conflict.
Panel Server status LED steady red	Major malfunction.	Call your local Schneider Electric service representative for assistance.

Troubleshooting Webpages and Wireless Communication

Problem	Diagnostics	Action
Unable to log into webpages due to lost or forgotten password.	Password lost	Reset the Panel Server to factory settings, page 190.
Unable to browse the Panel Server webpages.	Incorrect network configuration	Verify that all IP parameters are correct.
		Verify that Panel Server receives requests (ping Panel Server in the DOS prompt. Type **ping** and Panel Server IP address. For example, ping `169.254.0.10`).
		Verify that all connection settings in your browser Internet options are correct.
The Panel Server has lost communication with wireless devices.	Pollution on the radio frequency channel	Change the radio frequency channel that communicates between wireless devices and Panel Server in EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001, or Panel Server webpages.
A wireless device is not discovered by the Panel Server.	Panel Server does not recognize this type of wireless devices.	Verify that the device is in the list of supported devices. See the respective release notes, page 10: • DOCA0249•• *EcoStruxure Panel Server Entry - Firmware Release Notes* • DOCA0178•• *EcoStruxure Panel Server Universal - Firmware Release Notes* • DOCA0248•• *EcoStruxure Panel Server Advanced - Firmware Release Notes*
A 16-character RF-ID wireless device does not appear in either discovery table or rejected discovery table after a selective discovery.	The RF-ID and the install code do not match.	Check and correct the RF-ID and install code in the prepared selective list, or re-enter the details in the selective discovery list and relaunch the selective discovery.
Status of wireless devices (for example, PowerLogic TH110) does not update in Panel Server webpages or EcoStruxure Power Commission software(7).	The wireless device is powered off or has stopped communicating with the Panel Server (for example, if the wireless device has been moved out of range) and has status **Not connected**in red in the webpages.	• Verify that the device is powered on. • Verify that the wireless device is not installed out of range of the Panel Server.
Status of wireless device is displayed in orange, either **Not connected** or **Connected**, or with an orange icon .	The device is discovered and the status of the connection is unknown.	Wait for the status to change to **Connected** (green) or **Not connected** (red).
Alarms are not displayed in the **Monitoring & Control** page of the Panel Server webpages.	The device may be associated with a custom model.	1. Select the device in **Settings > Modbus devices** and check information at **Custom model device information**. If a custom model is indicated, proceed to step 2. 2. In the webpage **Settings > Data management**, select the device and enable the alarms to be displayed in the Alarm widget.

(7) Starting with Panel Server firmware version 002.007.000, firmware update, commissioning, and configuration of Panel Server gateways by using EcoStruxure Power Commission software or Mobile app are no longer supported. For more information, see related topic, page 34.

Problem	Diagnostics	Action
The Panel Server cannot reach the Schneider Electric cloud. **Network unreachable** is displayed in **Connection diagnostics**.	Incorrect network or communication configuration.	Verify that the network and communication settings are correctly set (for example, proxy or DNS is required but not defined).
		Verify that the firewall allows network access and connection from the Panel Server, in particular ports and protocols are enabled and correctly configured.
		Check that time is set to **Schneider Electric cloud** on the Panel Server webpage (see **Date & Time**, page 47).
The Panel Server is not recognized by the Schneider Electric cloud services.	–	Check that port 443 has been opened to cloud services (see parameters for cloud connection and services, page 123). If a reset to factory settings was performed on the Panel Server, contact your Schneider Electric Customer Care Center to have the Panel Server re-associated to Schneider Electric cloud services.

Troubleshooting Modbus Devices

Use diagnostic information and counters available in Panel Server and SCADA client. For details on diagnostic information available through the webpages, refer to Panel Server Diagnostics, page 171.

Problem	Diagnostics	Action
A Modbus device is not discovered by the Panel Server.	Incorrect device configuration settings.	• Verify that the device is in the list of supported devices. If not, create a custom model, page 153. • Verify that the device settings are set according to the Panel Server (see Serial Configuration Settings, page 102).
A Modbus device does not communicate with the Panel Server.	The same server ID is set to two Modbus devices in the network.	Verify that a server ID is not used twice in the Modbus network. See the detailed topic, page 60 to correct conflicts by using EcoStruxure Power Commission software on Panel Server gateways with firmware version up to 002.006.001.
Intermittent communication	Loose wiring, electromagnetic interference (EMI), or power issues.	Inspect connectors and/or stabilize power supply.
Connection refused (TCP)	Port 502 is blocked, or the device is busy.	Check firewall and/or ensure device is listening on port 502.
Data missing or not correctly published in webpages, SFTP server, HTTPS server, or Cloud, for device imported with custom device model.	Custom device model is not in updated format. Enumerated values do not match measurement in custom device model.	Correct (if necessary) the custom device model in EPC Web tool and import it into Panel Server webpages again.

Troubleshooting Connected Devices Using Panel Server Autodiagnostics Logs

For diagnostic information relating to connected devices, download Panel Server **Autodiagnostics** by performing an **Export all logs**, page 175. Refer to *diagnostic_modbus.txt* for the following diagnostic information:

- Modbus device information and diagnostics for specific Modbus TCP/IP and Modbus serial devices
- Downstream Modbus serial communication diagnostics for Panel Server serial port diagnostics
- Downstream Modbus TCP communication diagnostics: Global diagnostics for Modbus TCP devices aggregated by Panel Server

- Upstream Modbus TCP communication diagnostics: Diagnostics for Modbus TCP server side connection with SCADA
- Upstream Modbus Serial communication diagnostics: Diagnostics for Modbus serial server side connection with SCADA for reverse gateway mode

Problem	Diagnostics	Action
CRC (cyclic redundancy check) error (RTU)	Electrical noise, incorrect baud rate, or unsuitable cable.	Use shielded twisted-pair cable, verify baud rate, and/or check grounding.
Timeout / No response	The device is offline, has the wrong server ID, or a low timeout setting.	Check device status, confirm server ID, and/or increase timeout.
Panel Server autodiagnostic log indicates *Timeout between upstream reception and downstream availability total* High transmit (Tx) count, or low receive (Rx) count	Serial line bandwidth is saturated.	• Increase SCADA timeout and Panel Server Modbus TCP server **Message timeout (ms)** in **Settings > Modbus devices > Network configuration**. • Delete disconnected devices and/or stop sampling on disconnected devices. • Reduce sampling frequency or group registers more efficiently. • Increase baud rate if the environment allows. • Split the network between multiple serial ports or gateways. • Distribute sampling requests over time to avoid bursts of traffic.
Illegal function (Modbus exception code 01)	Function code not supported by server.	Check device manual for supported functions.
Illegal data address (Modbus exception code 02)	Register is out of range.	Verify register map and correct the address.
Target device failed to respond (Modbus exception code 0B)	Server not responding through gateway.	Check server status and serial wiring, or increase timeout.

Procedure to Convert MAC Address to IP Address

The following procedure describes how to convert the last two elements of the hexadecimal value of the MAC address to their equivalent decimal values to get the last two elements of the Panel Server IPv4 address. The IP address last two elements are represented in the procedure by `X` and `Y`. The first two elements of the default IPv4 address are `169.254`.

1. Convert the last elements of the MAC address to the correct decimal value, depending on the Panel Server Ethernet mode and MAC address:

   - **For Panel Server MAC address starting with `54-21-44` or lower**

If...	Then...	Example with MAC address `00-00-54-01-70-92`
The Panel Server is in Ethernet switched mode (default setting).	`X` is equal to the last but one element of the MAC address converted into decimal value. `Y` is equal to the last element of the Panel Server MAC address converted into decimal value + `1`.	Hexadecimal `70` converted to decimal is `112` Hexadecimal `92` converted to decimal is `146` `X` = `112` `Y` = `146` + `1` = `147` Therefore IPV4 address is `169.254.112.147`
The Panel Server is in Ethernet separated mode and the PC is connected to Panel Server ETH1 port.		
The Panel Server is in Ethernet separated mode and the PC is connected to Panel Server ETH2 port.	`X` is equal to the last but one element of the MAC address converted into decimal value. `Y` is equal to the last element of the Panel Server MAC address converted into decimal value + `2`.	Hexadecimal `70` converted to decimal is `112` Hexadecimal `92` converted to decimal is `146` `X` = `112` `Y` = `146` + `2` = `148` Therefore IPV4 address is `169.254.112.148`

   - **For Panel Server MAC address starting with `54-21-45` or higher**

If...	Then...	Example with MAC address `00-00-54-E9-D0-10`
The Panel Server is in Ethernet switch mode (default setting).	`X` is equal to the last but one element of the MAC address converted into decimal value. `Y` is equal to the last digits of the Panel Server MAC address converted into decimal value.	Hexadecimal `D0` converted to decimal is `208` Hexadecimal `10` converted to decimal is `16` Therefore IPV4 address is `169.254.208.16`
The Panel Server is in Ethernet separated mode and the PC is connected to Panel Server ETH1 port.		
The Panel Server is in Ethernet separated mode and the PC is connected to Panel Server ETH2 port.	`X` is equal to the last but one element of the MAC address converted into decimal value. `Y` is equal to the last digits of the Panel Server MAC address converted into decimal value + `1`.	Hexadecimal `D0` converted to decimal is `208` Hexadecimal `10` converted to decimal is `16` `Y` = `16` + `1` = `17` Therefore IPV4 address is `169.254.208.17`

2. Launch one of the recommended web browsers on your PC.
3. In the address field, type the IPv4 address starting with `https://` and using the format `https://169.254.X.Y` (where `X` and `Y` are the elements found by following the conversion procedure described). Press **Enter** to access the login page.

   IMPORTANT: Start the IPv4 address with `https://`

NOTE: If you do not remember the IP configuration of your gateway or in case of duplicate IP detection, follow the procedure above to connect to the Panel Server webpages to recover or update the network configuration.

Appendices

What’s in This Part

Appendix A: Details of Modbus Functions 266
Appendix B: Data Availability 281
Appendix C: Wireless Device Network Indicators 287
Appendix D: SFTP and HTTPS Publication File Formats 288
Appendix E: SSH Key Exchange and Cipher 291
Appendix F: Certificate Authorities 293
Appendix G: Retrieve the DHCP IP Address of a PAS400 Panel Server 297
Appendix H: Contextualization Data 299

Appendix A: Details of Modbus Functions

What's in This Chapter

Modbus TCP/IP Functions 267
Modbus-SL Functions 269
Recommendations for Optimizing Networks with Modbus Devices 270
Modbus TCP/IP and Modbus-SL Exception Codes 272
Modbus Registers Tables 274
EcoStruxure Panel Server Modbus Registers 275
Function 43-14: Read Device Identification 276
Function 100-4: Read Non-Adjacent Registers 278
Setting Message Timeout for Modbus Client and Modbus Server 279

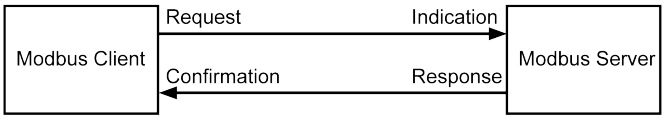
Modbus TCP/IP Functions

General Description

The Modbus messaging service provides a client/server communication between devices connected to an Ethernet TCP/IP network.

The client/server model is based on four types of messages:

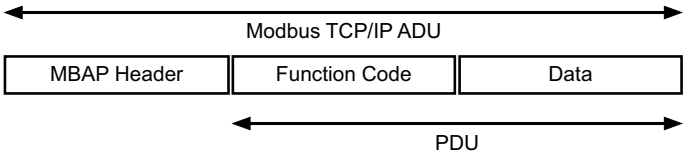
- Modbus Request, the message sent on the network by the client to initiate a transaction.
- Modbus Indication, the request message received on the server side.
- Modbus Response, the response message sent by the server.
- Modbus Confirmation, the response message received on the client side.



The Modbus messaging services (client/server model) are used for real time information exchange between:

- Two device applications.
- Device application and other device.
- HMI/SCADA applications and devices.
- A PC and a device program providing on line services.

A dedicated header is used on TCP/IP to identify the Modbus Application Data Unit. It is called the MBAP header (Modbus Application Protocol header).



The MBAP header contains the following fields:

Fields	Length	Description	Client	Server
Transaction Identifier	2 bytes	Identification of a Modbus Request/Response transaction	Initialized by the client	Recopied by the server from the received request
Protocol Identifier	2 bytes	0 = Modbus protocol	Initialized by the client	Recopied by the server from the received request
Length	2 bytes	Number of following bytes	Initialized by the client (Request)	Initialized by the server (Response)
Unit Identifier	1 byte	Identification of a remote server connected to a serial line or on other buses	Initialized by the client	Recopied by the server from the received request

Table of Modbus Functions

The following table describes in detail the functions supported by the Panel Server to read from or write data on Modbus TCP/IP devices.

Function code	Function name
03	Read n words
06	Write 1 word
16	Write n words

Function code	Function name
43-14	Read device identification (refer to Function 43-14: Read Device Identification, page 276)
100-4	Read n non-adjacent words where n ≤ 100 (refer to Function 100-4: Read Non-Adjacent Registers, page 278)

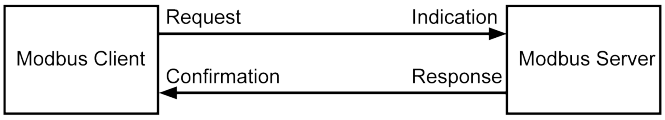
Modbus-SL Functions

General Description

The Modbus messaging service provides a client/server communication between devices connected to a Modbus Serial Line (Modbus-SL) network.

The client/server model is based on four types of messages:

- Modbus Request, the message sent on the network by the client to initiate a transaction.
- Modbus Indication, the request message received on the server side.
- Modbus Response, the response message sent by the server.
- Modbus Confirmation, the response message received on the client side.



The Modbus messaging services (client/server model) are used for real time information exchange between:

- Two device applications.
- Device application and other device.
- HMI/SCADA applications and devices.
- A PC and a device program providing on line services.

On Serial Line, the Modbus Application Data Unit (ADU) encapsulates the Protocol Data Unit (PDU) adding the server address and a Cyclic Redundancy Check (CRC). A dedicated header is used on TCP/IP to identify the Modbus Application Data Unit. It is called the MBAP header (Modbus Application Protocol header).

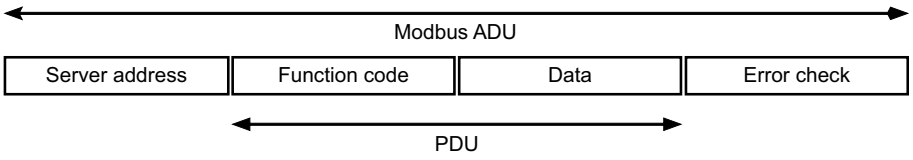


Table of Modbus Functions

The following table describes in detail the functions supported by the Panel Server to read from or write data on Modbus-SL devices.

Function code	Function name
03	Read n words
04	Read input register
06	Write 1 word
16	Write n words
43-14	Read device identification (refer to Function 43-14: Read Device Identification, page 276)
100-4	Read n non-adjacent words where n ≤ 100 (refer to Function 100-4: Read Non-Adjacent Registers, page 278)

IMPORTANT: Function codes 1 and 2 are not supported.

Recommendations for Optimizing Networks with Modbus Devices

General Recommendations

Optimize the Panel Server configuration:

- Set appropriate timeouts for the following:
  - Modbus serial client timeout, page 102: increase the response timeout to accommodate slower devices
  - Message timeouts for Modbus client and Modbus server, page 279
- Set an appropriate Modbus serial client frame delay (default setting 50 ms)to prevent communication errors on the serial bus. Refer to Modbus Serial Client Configuration Settings, page 102.
- When used as a transparent gateway, do not add the devices in the Panel Server.
- In a parent-child architecture, avoid discovering the devices in the child Panel Server. Discover the devices at parent level.

Optimize the configuration of connected devices:

- Disable unused features to reduce processing time.
- Use the **Registers read** function, page 231 available in Panel Server webpages to check connectivity and register response from the connected device.

Monitor performance and diagnostics:

- Monitor error rates. Check for CRC (cyclic redundancy check) errors and timeouts, which can indicate wiring or configuration issues. CRC error information is available as follows:
  - For the Panel Server: available on the webpages. Refer to Panel Server Diagnostics, page 171.
  - For devices: through **Autodiagnostics** logs. Refer to Exporting all logs, page 175
- Use diagnostic tools, for example protocol analyzers or dedicated software like ModScan or Modbus Poll.

Test and tune the system:

- Start with conservative sampling frequencies. Gradually reduce them while monitoring for the following:
  - CRC errors
  - Messages timeout
  - Missed responses in SCADA
- Adjust sampling frequencies based on actual device response times and network conditions.

Modbus Serial Line Recommendations

Follow best practices for network design:

- Minimize the number of devices per serial network to avoid overloading the bus. Try to stay below 32 devices per RS485 segment.
- Use repeaters or bridges for long distances or for high numbers of devices.
- Terminate the bus correctly. Use 120 ohm resistors at both ends of RS485 lines.
- Use shielded twisted-pair cables to reduce noise and interference. If available, connect shield and 0 Volt.

Understand the impact of baud rate. Baud rate determines how fast data is transmitted over the network:

- Higher baud rates (for example, 115200 bps) allow faster sampling but are more susceptible to noise.
- Lower baud rates (for example, 9600 bps) are more stable over long distances but reduce throughput.

Match the baud rate to the network conditions:

- Use higher baud rates (for example, 38400–115200) in electrically clean environments with short cable runs.
- Use lower baud rates (for example, 9600–19200) in noisy environments or long-distance setups.

Optimize the connected device configuration:

- Set unique server IDs for each connected device to avoid conflicts.
- Use consistent baud rates and parity settings across all devices connected on the same segment.

Optimize data sampling strategy:

- Read/write multiple contiguous registers in one request to reduce traffic.
- Adjust sampling periods to avoid sampling too frequently. Aim for a balance between responsiveness and bandwidth.
- Consider all devices in the serial network. The presence of a device with a slower response can impact the overall performance of the network.
- Consider using multiple gateways if you have high numbers of serial devices or high volume data.
- Avoid overloading the serial line with too many requests.

Modbus TCP/IP Recommendations

Manage Modbus TCP clients as follows:

- Limit the number of simultaneous upstream Modbus TCP clients to avoid overloading the Panel Server, page 20.
- Use persistent TCP connections instead of frequent connect/disconnect cycles.
- When establishing multiple simultaneous TCP client connections to the Panel Server, configure higher response timeouts on the client side. This helps ensure reliable communication and prevents premature disconnections or timeouts due to increased load during concurrent connections.

Troubleshooting

Refer to Troubleshooting Modbus Devices, page 262.

Modbus TCP/IP and Modbus-SL Exception Codes

Exception Responses

Exception responses issued by the client or a server can be the result of data processing errors. One of the following events can occur after a request from the client:

- If the server receives the request from the client without a communication error and manages the request correctly, it sends back a normal response.
- If the server does not receive the request from the client due to a communication error, it does not send back a response. The client program ends by applying a time delay condition to the request.
- If the server receives the request from the client but detects a communication error, it does not send back a response. The client program ends by applying a time delay condition to the request.
- If the server receives the request from the client without a communication error but cannot perform it (for example, the request consists of reading a register that does not exist), the server sends back an exception response to inform the client of the nature of the error.

Exception Frame

The server sends an exception frame to the client to indicate an exception response. An exception response consists of four fields:

Field	Definition	Size
1	Server number	1 byte
2	Exception function code	1 byte
3	Exception code	n bytes
4	Check	2 bytes

Managing Modbus Exceptions

The exception response frame consists of two fields that distinguish it from a normal response frame:

- The exception function code is the same as the original request function code plus 128 (0x80).
- The exception code depends on the communication error detected by the server.

The following table describes the exception codes managed by the EcoStruxure Panel Server:

Exception Code	Name	Description
01	Illegal function	The function code received in the request is not a permitted action for the server. It is possible that the server is in an unsuitable state to process a specific request.
02	Illegal data address	The data address received by the server is not a permitted address for the server.
03	Illegal data value	The value of the request data field is not a permitted value for the server.
04	Server device failure	The server is unable to perform a required action due to an unrecoverable error.
06	Server device busy	The server is busy processing another command. The client should send the request when the server is free.

NOTE: For more information, a detailed description of the Modbus protocol is available on www.modbus.org.

Access to Variables

A Modbus variable can have the following attributes:

- Read-only
- Read/write
- Write-only

NOTE: An attempt to write to a read-only variable generates an exception response.

Modbus Registers Tables

Presentation

The Modbus registers of EcoStruxure Panel Server and the Modbus registers of the supported wireless devices connected to it provide measurement and monitoring information.

The Panel Server provides a consolidated table (**Synthesis table**) of information from all connected wireless devices at once. The content of the table is built dynamically; a maximum of 100 wireless devices are listed in the table organized by virtual server ID.

The address of the synthesis table (**247** by default) can be configured at **Settings > Wireless devices > Global functional settings** (for details, page 221).

For detailed information about these Modbus registers, refer to DOCA0241EN *EcoStruxure Panel Server - Modbus File*.

Table of Modbus Functions

The following table describes the functions supported by the Panel Server to read and/or write data on the Modbus registers of wireless devices.

Function code	Function name
03	Read n words
16	Write n words
100-4	Read n non-adjacent words where n ≤ 100 (refer to Function 100-4: Read Non-Adjacent Registers, page 278)

EcoStruxure Panel Server Modbus Registers

The Panel Server implements its own Modbus registers which start at address 255.

For a full list of available data, refer to DOCA0241EN *EcoStruxure Panel Server - Modbus File*.

The available data includes the following settings:

- **Modbus TCP/IP server settings:**
  - Modbus ID of Panel Server
  - Message timeout: (Modbus TCP/IP server)
- **Modbus TCP/IP client settings:**
  - Timeout of Modbus TCP/IP client
  - Message timeout of Modbus TCP/IP client request
- **Modbus SL settings for downstream communication:**
  - Modbus parity
  - Modbus baud rate
  - Number of stop bits
  - Silent interval after Modbus SL packet end
  - Delay between Modbus SL packets
  - Connect/Disconnect the RS485 termination resistor
  - Transmission line state
- **Modbus SL client settings**
  - Message timeout of Modbus SL request

Function 43-14: Read Device Identification

Structure of Modbus Read Device Identification Messages

The ID consists of ASCII characters called objects.

Request for basic information:

Definition	Number of Bytes	Value
Server number	1 byte	0xFF
Function code	1 byte	0x2B
Sub-function code	1 byte	0x0E
Product ID	1 byte	0x01
Object identifier	1 byte	0x00

Response with basic information:

Definition		Number of Bytes	Value
Server number		1 byte	0xFF
Function code		1 byte	0x2B
Sub-function code		1 byte	0x0E
Product ID		1 byte	0x01
Conformity level		1 byte	0x01
Reserved		1 byte	0x00
Reserved		1 byte	0x00
Number of objects		1 byte	0x03
Object 0: manufacturer name	Object number	1 byte	0x00
	Object length	1 byte	0x12
	Object content	18	Schneider Electric
Object 1: product code	Object number	1 byte	0x01
	Object length	1 byte	0x20 (maximum)
	Object content	0x20 (maximum)	EcoStruxure Panel Server product code
Object 2: firmware version	Object number	1 byte	0x02
	Object length	1 byte	0x0B
	Object content	11 bytes	XXX.YYY.ZZZ

Request for complete information:

Definition	Number of Bytes	Value
Server number	1 byte	0xFF
Function code	1 byte	0x2B
Sub-function code	1 byte	0x0E
Product ID	1 byte	0x02
Object identifier	1 byte	0x00

Response with complete information:

NOTE: This table describes how to read the ID of an EcoStruxure Panel Server.

Definition		**Number of Bytes**	**Value**
Server number		1 byte	0xFF
Function code		1 byte	0x2B
Sub-function code		1 byte	0x0E
Product ID		1 byte	0x02
Conformity level		1 byte	0x02
Reserved		1 byte	0x00
Reserved		1 byte	0x00
Number of objects		1 byte	0x05
Object 0: manufacturer name	Object number	1 byte	0x00
	Object length	1 byte	0x12
	Object content	0x12	Schneider Electric
Object 1: product code	Object number	1 byte	0x01
	Object length	1 byte	0x20 (maximum)
	Object content	0x20 (maximum)	EcoStruxure Panel Server product code
Object 2: firmware version	Object number	1 byte	0x02
	Object length	1 byte	0x0B
	Object content	0x0B	XXX.YYY.ZZZ
Object 3: vendor URL	Object number	1 byte	0x03
	Object length	1 byte	0x20 (maximum)
	Object content	0x20 (maximum)	Vendor URL
Object 4: product range	Object number	1 byte	0x04
	Object length	1 byte	0x20 (maximum)
	Object content	0x20 (maximum)	EcoStruxure Panel Server product range
Object 5: product model	Object number	1 byte	0x05
	Object length	1 byte	0x20 (maximum)
	Object content	0x20 (maximum)	EcoStruxure Panel Server product model
Object 6: user application name	Object number	1 byte	0x06
	Object length	1 byte	0x20 (maximum)
	Object content	0x20 (maximum)	EcoStruxure Panel Server user application name

Function 100-4: Read Non-Adjacent Registers

Structure of Modbus Read n Non-Adjacent Registers Messages Where n ≤ 100

The example below is the case of reading of 2 non-adjacent registers.

Request

Definition	Number of Bytes	Value
Modbus server number	1 byte	0x2F
Function code	1 byte	0x64
Length of data in bytes	1 byte	0x06
Sub-function code	1 byte	0x04
Transmission number(1)	1 byte	0xXX
Address of the first word to be read (MSB)	1 byte	0x00
Address of the first word to be read (LSB)	1 byte	0x65
Address of the second word to be read (MSB)	1 byte	0x00
Address of the second word to be read (LSB)	1 byte	0x67
(1) The client gives the transmission number in the request.		

NOTE: The table above describes how to read addresses 101 = 0x65 and 103 = 0x67 of a Modbus server. The Modbus server number is 47 = 0x2F.

Response

Definition	Number of Bytes	Value
Modbus server number	1 byte	0x2F
Function code	1 byte	0x64
Length of data in bytes	1 byte	0x06
Sub-function code	1 byte	0x04
Transmission number(1)	1 byte	0xXX
First word read (MSB)	1 byte	0x12
First word read (LSB)	1 byte	0x0A
Second word read (MSB)	1 byte	0x74
Second word read (LSB)	1 byte	0x0C
(1) The server sends back the same number in the response.		

NOTE: The table above describes how to read addresses 101 = 0x65 and 103 = 0x67 of a Modbus server. The Modbus server number is 47 = 0x2F.

Setting Message Timeout for Modbus Client and Modbus Server

The message timeout that you set depends on the response time of the devices within your configuration. The information given here helps you to decide how to set the message timeout.

The message timeout defines the time-to-live of a Modbus request in the Panel Server. Any messages older than this setting are dropped.

The message timeout for the Modbus TCP server is called **Upstream timeout**, set in ms (see Modbus TCP/IP Server Settings, page 100).

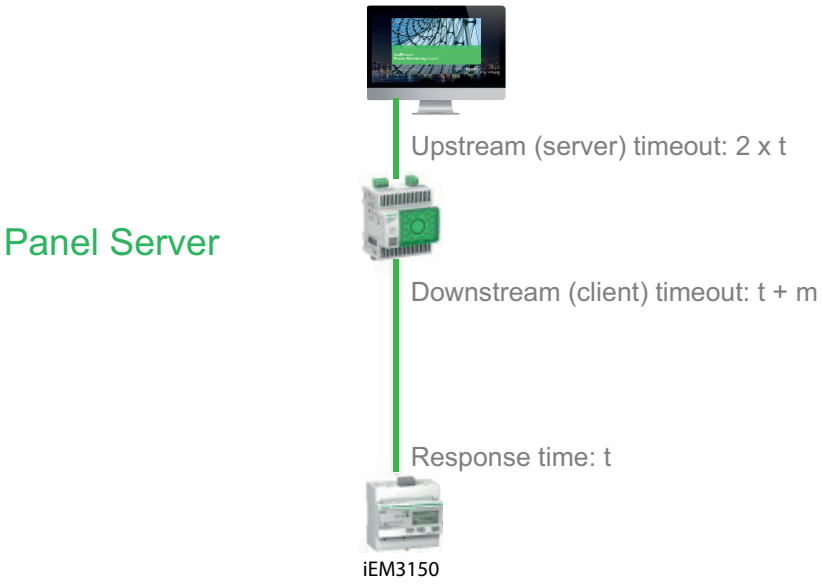
The message timeout for the Modbus client is called **Downstream timeout**, set in s (see Modbus TCP/IP Client Settings, page 99).

The following diagram illustrates a simple architecture between a Panel Server and connected devices (represented by a single device here). The response time (t) of the connected devices should be taken into consideration when calculating the message timeout of the Panel Server.

Set the Modbus client timeout (downstream timeout) as the response time (t) of the connected device plus an additional time as a margin (m).

Set the Modbus server timeout (upstream timeout) as the response time (t) of the connected device multiplied by 2.

Message timeout for Panel Server architecture



t: response time of device

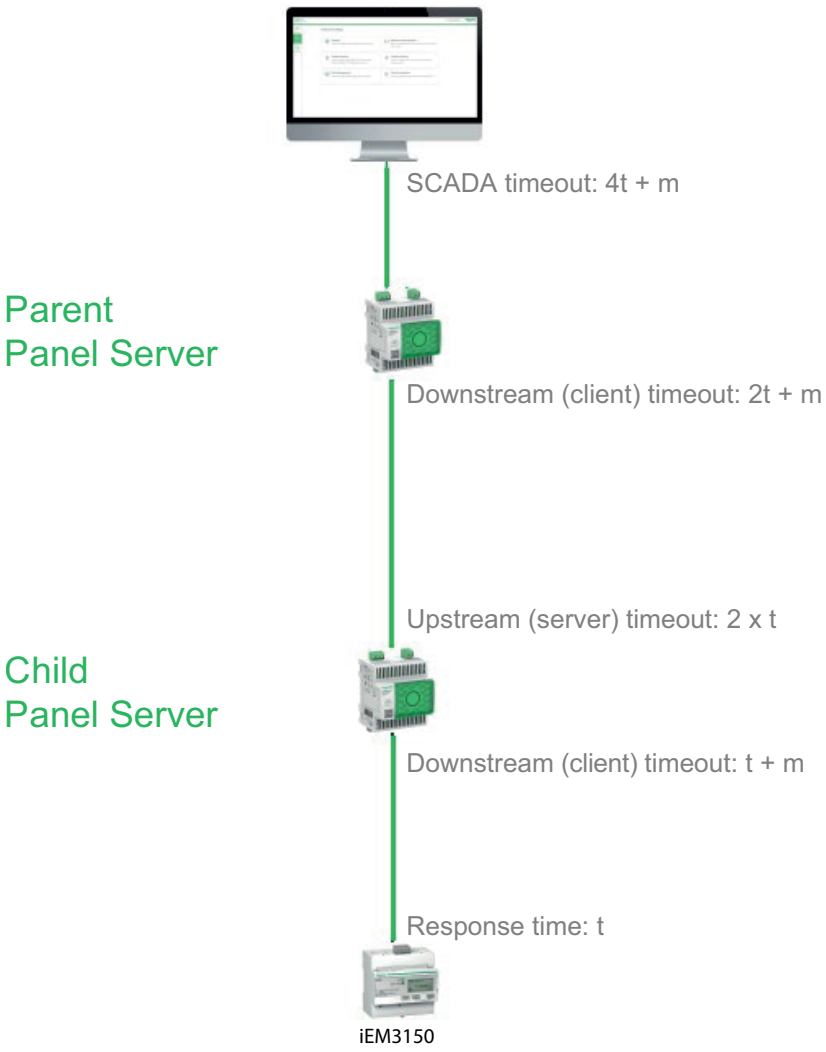
m: margin to add

For a parent child configuration with two Panel Server devices, for the child Panel Server use the recommendation above.

For the parent Panel Server, set timeouts as follows:

- Downstream timeout: child Panel Server upstream timeout plus an additional time as a margin (m)
- Upstream timeout: response time (t) of the child Panel Server connected device multiplied by 4
- SCADA timeout: response time (t) of the child Panel Server connected device multiplied by 4 plus an additional time as a margin (m)

Message timeout for parent/child Panel Server architecture



t: response time of device

m: margin to add

Appendix B: Data Availability

What's in This Chapter

PowerTag, PowerLogic Tag, and Acti9 Active Data Availability 282
Environmental Sensor Data Availability 286

PowerTag, PowerLogic Tag, and Acti9 Active Data Availability

Presentation

The data transmitted by the PowerTag Energy and PowerLogic Tag and Acti9 Active devices to the EcoStruxure Panel Server depends on the type of device. The following tables indicate which data is available in the EcoStruxure Panel Server according to each type of device.

Device Commercial References

The device commercial references used for each type of sensors are:

- A1: A9MEM1520, A9MEM1521, A9MEM1522, A9MEM1541, A9MEM1542, PLTQO●, PLTE60●
- A2: A9MEM1540, A9MEM1543
- P1: A9MEM1561, A9MEM1562, A9MEM1563, A9MEM1571, A9MEM1572
- F1: A9MEM1560, A9MEM1570
- F2: A9MEM1573, A9MEM1575
- F3: A9MEM1564, A9MEM1574
- FL: A9MEM1580
- M0: LV434020
- M1: LV434021
- M2: LV434022
- M3: LV434023
- R1: A9MEM1590, A9MEM1591, A9MEM1592, A9MEM1593, PLTR●
- C: Acti9 Active iC40/iC60 (A9TAA●●●●, A9TAB●●●●, A9TDEC●●●, A9TDFC●●●, A9TDFD●●●, A9TPDD●●●, A9TPED●●●, A9TYAE●●●, A9TYBE●●●)

Power

Data	PowerTag M63, PowerLogic Tag QO, PowerLogic Tag E-Frame		PowerTag P63	PowerTag F63			Power-Tag F160	Power-Tag M250		Power-Tag M630		PowerTag Rope, PowerLogic Tag Rope	Acti9 Active
	A1	A2	P1	F1	F2	F3	FL	M0	M1	M2	M3	R1	C
Total active power	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Per phase active power	✓	NA (8)	✓	✓	NA (8)	✓	✓(9)	✓(9)	✓	✓(9)	✓	✓(9)	✓
Total reactive power	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Per phase reactive power	–	–	–	–	–	–	✓(9)	–	–	–	–	✓(9)	–
Total apparent power	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

(8) Not applicable because there is no neutral voltage on the PowerTag Energy sensors.
(9) The values are significant only if the neutral voltage picking is connected.

Data	PowerTag M63, PowerLogic Tag QO, PowerLogic Tag E-Frame		PowerTag P63	PowerTag F63			Power-Tag F160	Power-Tag M250		Power-Tag M630		PowerTag Rope, PowerLogic Tag Rope	Acti9 Active
	A1	A2	P1	F1	F2	F3	FL	M0	M1	M2	M3	R1	C
Per phase apparent power	–	–	–	–	–	–	✓(10)	–	–	–	–	✓(10)	–
Total factor power	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Per phase factor power	–	–	–	–	–	–	✓(10)	–	–	–	–	✓(10)	–
Active power demand	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Active power peak demand (Resettable, page 248)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Energy

Data	PowerTag M63, PowerLogic Tag QO, PowerLogic Tag E-Frame		PowerTag P63	PowerTag F63			Power-Tag F160	Power-Tag M250		Power-Tag M630		PowerTag Rope, PowerLogic Tag Rope	Acti9 Active
	A1	A2	P1	F1	F2	F3	FL	M0	M1	M2	M-3	R1	C
Total resettable active energy delivered	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Total non resettable active energy delivered	✓	✓	✓	✓	✓	✓	✓(10)	✓	✓	✓	✓	✓(10)	✓(10)
Per phase resettable active energy delivered	–	–	–	–	–	–	✓(10)	–	–	–	–	✓(10)	✓(10)
Per phase non resettable active energy delivered	–	–	–	–	–	–	✓(10)	–	–	–	–	✓(10)	✓(10)
Total resettable active energy received	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Total non resettable active energy received	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Per phase resettable active energy received	–	–	–	–	–	–	✓(10)	–	–	–	–	✓(10)	✓(10)
Per phase non resettable active energy received	–	–	–	–	–	–	✓(10)	–	–	–	–	✓(10)	✓(10)

(10) The values are significant only if the neutral voltage picking is connected.

Data	PowerTag M63, PowerLogic Tag QO, PowerLogic Tag E-Frame		PowerTag P63	PowerTag F63			Power-Tag F160	Power-Tag M250		Power-Tag M630		PowerTag Rope, PowerLogic Tag Rope	Acti9 Active
	A1	A2	P1	F1	F2	F3	FL	M0	M1	M2	M-3	R1	C
Total resettable active energy delivered and received	✓	✓	✓	✓	✓	✓	NA(11)	NA(11)	NA(11)	NA(11)	NA(11)	NA(11)	NA(11)
Total non resettable active energy delivered and received	✓	✓	✓	✓	✓	✓	NA(11)	NA(11)	NA(11)	NA(11)	NA(11)	NA(11)	NA(11)
Per phase resettable active energy delivered and received	–	–	–	–	–	–	NA(11)	–	–	–	–	NA(11)	NA(11)
Per phase non resettable active energy delivered and received	–	–	–	–	–	–	NA(11)	✓(12)	✓	✓(12)	✓	NA(11)	NA(11)
Total resettable reactive energy delivered	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Total non resettable reactive energy delivered	–	–	–	–	–	–	✓(12)	–	–	–	–	✓(12)	✓(12)
Per phase resettable reactive energy delivered	–	–	–	–	–	–	✓(12)	–	–	–	–	✓(12)	✓(12)
Per phase non resettable reactive energy delivered	–	–	–	–	–	–	✓	–	–	–	–	✓	✓
Total resettable reactive energy received	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Total non resettable reactive energy received	–	–	–	–	–	–	✓	–	–	–	–	✓	✓
Per phase resettable reactive energy received	–	–	–	–	–	–	✓(12)	–	–	–	–	✓(12)	✓(12)
Per phase non resettable reactive energy received	–	–	–	–	–	–	✓(12)	–	–	–	–	✓(12)	✓(12)

(11) Not applicable because energy is individually cumulated in received and delivered counters.
(12) The values are significant only if the neutral voltage picking is connected.

Data	PowerTag M63, PowerLogic Tag QO, PowerLogic Tag E-Frame		PowerTag P63	PowerTag F63			Power-Tag F160	Power-Tag M250		Power-Tag M630		PowerTag Rope, PowerLogic Tag Rope	Acti9 Active
	A1	A2	P1	F1	F2	F3	FL	M0	M1	M2	M-3	R1	C
Total resettable apparent energy delivered and received	–	–	–	–	–	–	✓	–	–	–	–	✓	✓
Total non resettable apparent energy delivered and received	–	–	–	–	–	–	✓	–	–	–	–	✓	✓
Per phase resettable apparent energy delivered and received	–	–	–	–	–	–	✓(13)	–	–	–	–	✓(13)	✓(13)
Per phase non resettable apparent energy delivered and received	–	–	–	–	–	–	✓(13)	–	–	–	–	✓(13)	✓(13)

Other Measurements

Data	PowerTag M63, Power-Logic Tag QO, Power-Logic Tag E-Frame		PowerTag P63	PowerTag F63			PowerTag F160	Power-Tag M250		Power-Tag M630		PowerTag Rope, PowerLogic Tag Rope	Acti9 Active
	A1	A2	P1	F1	F2	F-3	FL	M0	M1	M2	M3	R1	C
Phase current (measured)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Neutral current (calculated)	–	–	–	–	–	–	✓	–	–	–	–	✓	
Phase-to-phase voltage	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Phase-to-neutral voltage	✓	NA(14)	✓	✓	NA(14)	✓	✓(13)	✓(13)	✓	✓(13)	✓	✓	✓(13)
Frequency	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	
Quadrant	1	1	1	1	1	1	4	4	4	4	4	4	
Internal temperature	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Load operating time counter	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

(13) The values are significant only if the neutral voltage picking is connected.
(14) Not applicable because there is no neutral voltage on the PowerTag Energy sensors

Environmental Sensor Data Availability

Presentation

The data transmitted by the environmental sensors to the Panel Server depends on the type of environmental sensor. The table indicates examples of data available in the Panel Server according to the type of environmental sensors.

Device Commercial References

The device commercial references used for each type of environmental sensor are:

- CL110 (Contact your Schneider Electric representative for information about commercial references.)
- TH110 (Contact your Schneider Electric representative for information about commercial references.)
- TH150S(15), TH150M(15)
- TH200M(15)
- TRH (SED-TRH-G-5045)
- TRHC02 (SED-CO2-G-5045)

For a full list of supported commercial references, refer to the following documents, page 10

- DOCA0241EN *EcoStruxure Panel Server - Modbus File*
- DOCA0249•• *EcoStruxure Panel Server Entry - Firmware Release Notes*
- DOCA0178•• *EcoStruxure Panel Server Universal - Firmware Release Notes*
- DOCA0248•• *EcoStruxure Panel Server Advanced - Firmware Release Notes*

Other Measurements

Data	CL110	TH110	TRH	TRHC02
Temperature	✓	✓	✓	✓
Temperature phase A	–	–	–	–
Temperature phase B	–	–	–	–
Temperature phase C	–	–	–	–
Temperature neutral	–	–	–	–
Relative humidity	✓	–	✓	✓
CO_2 concentration	–	–	–	✓
Internal temperature	–	✓	–	–
Battery voltage	✓	–	✓	✓
RSSI link	✓	✓	✓	✓

For a full list of measurements transmitted by environmental sensors, refer to DOCA0241EN *EcoStruxure Panel Server - Modbus File*.

(15) China-certified devices only.

Appendix C: Wireless Device Network Indicators

Network Indicators

The following table describes the network indicators of wireless devices.

Information type	Description
RSSI (received signal strength indicator)	Displays the power level of the wireless signal: • 0 to -75 dBm indicates a good power level. • -75 to -85 dBm indicates an average power level. • ≤ -85 dBm indicates a poor power level with risk of outage.
LQI (link quality indicator)	Displays the measurement of the strength and/or the quality of the received frames.
PER (packet error rate)	Displays the ratio of the number of packets which do not reach a destination over the total expected number of packets. It is expressed as a percentage. The calculation of the PER (packet error rate) indicator depends on the type of indicator: • Device indicator: provided by the device. • Panel Server indicator: calculated over a sliding window equal to 20 x publication period, and refreshed every 30 seconds. • Link indicator: displays the higher of the two previous indicators.

Signal Quality Level

- **PER Link indicator**:
  The PER link indicator is based on the PER of the Panel Server and the PER of the device as explained in the following table:

		PER of the device		
		PER < 20% or no device PER	**20% ≤ PER < 30%**	**30% ≤ PER**
PER of Panel Server	**PER < 10%**	Low	Medium	High
	10% ≤ PER < 15%	Medium	Medium	High
	15% ≤ PER	High	High	High

- **Signal quality level**:
  The signal quality level is based on the PER link indicator and RSSI as explained in the following table:

		RSSI		
		RSSI > -75 dBm	**-85 dBm < RSSI ≤ -75 dBm**	**RSSI ≤ -85 dBm**
PER link indicator	**Low**	Excellent	Excellent	Good
	Medium	Good	Good	Fair
	High	Fair	Weak	Weak

Appendix D: SFTP and HTTPS Publication File Formats

CSV Publication

The following table provides the details of each row of the .csv file, with sample data:

Row	Data in .csv file	Description
1	"Gateway Name","Gateway SN","Gateway IP Address","Gateway MAC Address","Device Name","Device Local ID","Device Type ID","Device Type Name","Logging Interval","Historical Intervals"	This row contains the column headings for the information provided in row 2: • Gateway Name: name given to Panel Server during commissioning • Gateway SN: serial number of Panel Server • Gateway IP: IP address of Panel Server • Gateway MAC Address: MAC address of Panel Server • Device Name: name given to the device during commissioning • Device Local ID: reference of the logged device, unique across Panel Server • Device Type ID: device model • Device Type Name: device model • Logging Interval: sampling period expressed in minutes • Historical Intervals: total number of rows of logged data in this file
2	"Device TypeEcoStruxure Panel Server","542206310926","10.195.253.81","00:00:54:E5:8A:36","F160 3P 3P+N","modbus:1_mb_81","F160 3P 3P+N","F160 3P 3P+N","5","7"	This row contains information about the Panel Server that produced the file, and the downstream device from which the measurements were sampled.
3	–	–
4	" "," "," ","Topic ID1","Topic ID2"	This row contains the column headings for the topic IDs. A topic ID is a reference to the quantity being logged. The name given to a quantity may differ between devices and languages. Topic IDs are used to identify the quantity regardless of the device or language. Topic IDs are unique across the Panel Server. **NOTE:** The first 3 commas are used for layout purposes in a spreadsheet application.
5	" "," ","","modbus:1_mb_VAB","modbus:1_mb_VAN"	This row contains the topic IDs of the measurements logged.
6	–	–
7	"Error","UTC Offset (minutes)","Local Time Stamp","RmsVoltagePhsAB (V)","RmsVoltagePhsAN (V)"	This row contains the column headings for the data logged in rows 8 and more: • Error: 0 for success, 19 when at least one measurement was invalid or not available for sampling (NaN). • UTC Offset (minutes): offset of local timestamp from UTC timezone. • Local Time Stamp: date and time of the samples From the fourth item onward, each measure is described by its name and unit (if known).
8 and more	"0","0","2022-11-04 08:10:00","127.80000305","235.3999939" "0","0","2022-11-04 08:15:00","128.1000061","235.69999695" "0","0","2022-11-04 08:20:00","127.69999695","234.8999939"	These rows contain the logged data.

JSON Publication

The following table provides an explanation of the .json file content, with example content taken from the example file to illustrate.

Data in json file	Description	Example
valueItemId	Device name and measurement/ event. The device name used in the .json file is an internal name. To get the correspondence between this name and the device name listed in the Panel Server, follow the procedure to export all logs, page 175. The *diagnostic_topology.txt* file in the exported logs lists device names and internal names.	**Io_block:7_iod_827_DO1** denotes IO device number 7, and the record of the actions on Digital Input 1
timestamp	Time reference of beginning of sampling period	**2023-03-28T08:13:00Z**
v	Measurement/event	**Open**
t	Time offset in ms to add to time reference	120000 ms = 120 s = 2 min so sample taken at 08.13 + 2 min = 08.15
s	Invalid measurement	**false**

The following lines provide an example of a .json file with data consisting of a list of two time series with a collection of several records:


```
{
 "$schema": "ESX/EDM/Protocol/Specific/CloudMessaging/DeviceToCloud/Data/CewsMessage",
 "message": {
  "remoteId": "urn:dev:cer:a66e3ea13bbe1b67aa46b4a5c1552f162b467cb4",
  "contentType": "data",
  "cewsVersion": "3.0.0",
  "timestamp": "2023-03-28T08:22:13.342Z",
  "content": {
   "data": {
    "timeseries": [
     {
      "valueItemId": "io_block:7_iod_827_DO1",
      "timestamp": "2023-03-28T08:13:00Z",
      "records": [
       {
        "v": "Open",
        "t": 120000
       },
       {
        "v": "Open",
        "t": 180000
       },
       {
        "v": "Open",
        "t": 240000
       },
       {
        "v": "Open",
        "t": 300000
       },
       {
        "v": "Open",
        "t": 360000
       },
       {
        "v": "Open",
        "t": 420000
       },
       {
        "v": "Open",
        "t": 480000
       }
      ]
     },
     {
      "valueItemId": "io_block:10_iod_827_DO1",
      "timestamp": "2023-03-28T08:13:00Z",
      "records": [
       {
        "v": "Disengaged",
        "t": 120000
       },
 {
        "v": "Disengaged",
        "t": 180000
       },
       {
        "v": "Disengaged",
        "t": 240000
       },
       {
        "v": "Disengaged",
        "t": 300000
       },
       {
        "v": "Disengaged",
        "t": 360000
       },
       {
        "v": "Disengaged",
        "t": 420000
       },
       {
        "v": "Disengaged",
        "t": 480000
       }
      ]
     }
    ]
   }
  }
 }
}
```

Appendix E: SSH Key Exchange and Cipher

The following table lists the HTTPS cybersecurity elements supported by the Panel Server firmware versions greater than or equal to 002.008.000.

Element type: HTTPS	Element	Panel Server firmware versions greater than or equal to 002.008.000
Cipher	aes128-gcm-sha256	✓
	aes128-sha	✓
	aes128-sha256	✓
	aes256-gcm-sha384	✓
	aes256-sha	✓
	aes256-sha256	✓
	dhe-rsa-aes128-gcm-sha256	✓
	dhe-rsa-aes128-sha	✓
	dhe-rsa-aes128-sha256	✓
	dhe-rsa-aes256-gcm-sha384	✓
	dhe-rsa-aes256-sha	✓
	dhe-rsa-aes256-sha256	✓
	ecdhe-ecdsa-aes128-gcm-sha256	✓
	ecdhe-ecdsa-aes128-sha	✓
	ecdhe-ecdsa-aes128-sha256	✓
	ecdhe-ecdsa-aes256-gcm-sha384	✓
	ecdhe-ecdsa-aes256-sha	✓
	ecdhe-ecdsa-aes256-sha384	✓
	ecdhe-rsa-aes128-gcm-sha256	✓
	ecdhe-rsa-aes128-sha	✓
	ecdhe-rsa-aes128-sha256	✓
	ecdhe-rsa-aes256-gcm-sha384	✓
	ecdhe-rsa-aes256-sha	✓
	ecdhe-rsa-aes256-sha384	✓
	tls_aes_128_gcm_sha256	✓
	tls_aes_256_gcm_sha384	✓

The following table lists the cybersecurity elements supported by the Panel Server across firmware versions.

Element type	Element	Panel Server firmware version		
		002.008.000 or greater	002.004.000 to 002.007.000	002.003.000 or lower
		SFTP element	HTTPS/SFTP element	HTTPS/SFTP element
Key exchange	curve25519-sha256	✓	✓	
	mlkem768x25519-sha256		✓	
	diffie-hellman-group1-sha1	✓		✓
	diffie-hellman-group14-sha1	✓		✓
	diffie-hellman-group14-sha256	✓	✓	
	diffie-hellman-group16-sha512	✓	✓	
	diffie-hellman-group18-sha512	✓	✓	
	diffie-hellman-group-exchange-sha1	✓		✓
	diffie-hellman-group-exchange-sha256	✓	✓	✓
	ecdh-sha2-nistp256	✓	✓	✓

Element type	Element	Panel Server firmware version		
		002.008.000 or greater	002.004.000 to 002.007.000	002.003.000 or lower
		SFTP element	HTTPS/SFTP element	HTTPS/SFTP element
	ecdh-sha2-nistp384	✓	✓	✓
	ecdh-sha2-nistp521	✓	✓	✓
	ext-info-c	✓		
	kex-strict-c-v00	✓		
Cipher	3des-cbc	✓		✓
	aes128-cbc	✓		✓
	aes128-ctr	✓	✓	✓
	aes128-gcm	✓	✓	
	aes192-cbc	✓		✓
	aes192-ctr	✓	✓	✓
	aes256-cbc	✓		✓
	aes256-ctr	✓	✓	✓
	aes256-gcm	✓	✓	
	blowfish-cbc	✓		✓
	cast128-cbc	✓		
	chacha20-poly1305	✓		
	rijndael-cbc	✓		
MAC	hmac-md5	✓		✓
	hmac-md5-96	✓		✓
	hmac-ripemd160	✓		
	hmac-sha1	✓	✓	✓
	hmac-sha1-96	✓		✓
	hmac-sha1-etm	✓	✓	
	hmac-sha2-256		✓	
	hmac-sha2-256-etm		✓	
	hmac-sha2-512		✓	
	hmac-sha2-512-etm		✓	
Host Key	ecdsa-sha2-nistp256	✓	✓	✓
	ecdsa-sha2-nistp256-cert-v01	✓	✓	
	ecdsa-sha2-nistp384	✓	✓	✓
	ecdsa-sha2-nistp384-cert-v01	✓	✓	
	ecdsa-sha2-nistp521	✓	✓	✓
	ecdsa-sha2-nistp521-cert-v01	✓	✓	
	rsa-sha2-256		✓	
	rsa-sha2-256-cert-v01	✓	✓	
	rsa-sha2-512		✓	
	rsa-sha2-512-cert-v01	✓	✓	
	ssh-dss			✓
	ssh-ed25519	✓	✓	
	ssh-ed25519-cert-v01	✓	✓	
	ssh-rsa	✓		✓
	ssh-rsa-cert-v01	✓		✓

Appendix F: Certificate Authorities

- actalisauthenticationrootca
- addtrustclass1ca
- addtrustexternalca
- addtrustqualifiedca
- affirmtrustcommercialca
- affirmtrustnetworkingca
- affirmtrustpremiumca
- affirmtrustpremiumeccca
- amazonrootca1
- amazonrootca2
- amazonrootca3
- amazonrootca4
- baltimorecybertrustca
- buypassclass2ca
- buypassclass3ca
- camerfirmachambersca
- camerfirmachamberscommerceca
- camerfirmachambersignca
- cert_10_geotrust_universal_ca_210
- cert_102_cfca_ev_root102
- cert_103_oiste_wisekey_global_root_gb_ca103
- cert_104_szafir_root_ca2104
- cert_105_certum_trusted_network_ca_2105
- cert_106_hellenic_academic_and_research_institutions_rootca_2015106
- cert_107_hellenic_academic_and_research_institutions_ecc_rootca_2015107
- cert_109_ac_raiz_fnmt_rcm109
- cert_115_tubitak_kamu_sm_ssl_kok_sertifikasi___surum_1115
- cert_116_gdca_trustauth_r5_root116
- cert_117_trustcor_rootcert_ca_1117
- cert_118_trustcor_rootcert_ca_2118
- cert_119_trustcor_eca_1119
- cert_120_ssl_com_root_certification_authority_rsa120
- cert_121_ssl_com_root_certification_authority_ecc121
- cert_122_ssl_com_ev_root_certification_authority_rsa_r2122
- cert_123_ssl_com_ev_root_certification_authority_ecc123
- cert_125_oiste_wisekey_global_root_gc_ca125
- cert_126_gts_root_r1126
- cert_127_gts_root_r2127
- cert_128_gts_root_r3128
- cert_129_gts_root_r4129
- cert_130_uca_global_g2_root130
- cert_131_uca_extended_validation_root131
- cert_132_certigna_root_ca132
- cert_133_emsign_root_ca___g1133

- cert_134_emsign_ecc_root_ca___g3134
- cert_135_emsign_root_ca___c1135
- cert_136_emsign_ecc_root_ca___c3136
- cert_137_hongkong_post_root_ca_3137
- cert_20_taiwan_grca20 cert_31_secure_global_ca31
- cert_32_comodo_certification_authority32
- cert_33_network_solutions_certificate_authority33
- cert_35_oiste_wisekey_global_root_ga_ca35
- cert_36_certigna36 cert_37_cybertrust_global_root37
- cert_39_certsign_root_ca39
- cert_46_netlock_arany__class_gold__f_tan_s_tv_ny46
- cert_48_hongkong_post_root_ca_148
- cert_49_securesign_rootca1149
- cert_50_microsec_e_szigno_root_ca_200950
- cert_52_autoridad_de_certificacion_firmaprofesional_cif_a6263406852
- cert_53_izenpe_com53 cert_64_twca_root_certification_authority64
- cert_66_ec_acc66 cert_67_hellenic_academic_and_research_institutions_rootca_201167
- cert_69_trustis_fps_root_ca69
- cert_73_ee_certification_centre_root_ca73
- cert_76_ca_disig_root_r276
- cert_77_accvraiz177
- cert_78_twca_global_root_ca78
- cert_80_e_tugra_certification_authority80
- cert_82_atos_trustedroot_201182
- cert_96_staat_der_nederlanden_root_ca___g396
- cert_97_staat_der_nederlanden_ev_root_ca97
- certumca
- certumtrustednetworkca
- chunghwaepkirootca
- comodoaaaca
- comodoeccca
- comodorsaca
- digicertassuredidg2
- digicertassuredidg3
- digicertassuredidrootca
- digicertglobalrootca
- digicertglobalrootg2
- digicertglobalrootg3
- digicerthighassuranceevrootca
- digicerttrustedrootg4
- dtrustclass3ca2
- dtrustclass3ca2ev
- entrust2048ca
- entrustevca
- entrustrootcaec1
- entrustrootcag2

- geotrustglobalca
- geotrustprimaryca
- geotrustprimarycag2
- geotrustprimarycag3
- geotrustuniversalca
- globalsignca
- globalsigneccrootcar4
- globalsigneccrootcar5
- globalsignr2ca
- globalsignr3ca
- globalsignrootcar6
- godaddyclass2ca
- godaddyrootg2ca
- identrustcommercial
- identrustdstx3
- identrustpublicca
- keynectisrootca
- letsencryptisrgx1
- luxtrustglobalroot2ca
- luxtrustglobalrootca
- quovadisrootca
- quovadisrootca1g3
- quovadisrootca2
- quovadisrootca2g3
- quovadisrootca3
- quovadisrootca3g3
- secomscrootca1
- secomscrootca2
- securetrustca
- soneraclass2ca
- starfieldclass2ca
- starfieldrootg2ca
- starfieldservicesrootg2ca
- swisssigngoldg2ca
- swisssignplatinumg2ca
- swisssignsilverg2ca
- teliasonerarootcav1
- thawtepremiumserverca
- thawteprimaryrootca
- thawteprimaryrootcag2
- thawteprimaryrootcag3
- ttelesecglobalrootclass2ca
- ttelesecglobalrootclass3ca
- usertrusteccca
- usertrustrsaca
- verisignclass2g2ca
- verisignclass3ca

- verisignclass3g2ca
- verisignclass3g3ca
- verisignclass3g4ca
- verisignclass3g5ca
- verisigntsaca
- verisignuniversalrootca
- xrampglobalca

Appendix G: Retrieve the DHCP IP Address of a PAS400 Panel Server

Follow this procedure to retrieve the DHCP IP address for a Panel Server Entry connected to the network in DHCP mode:

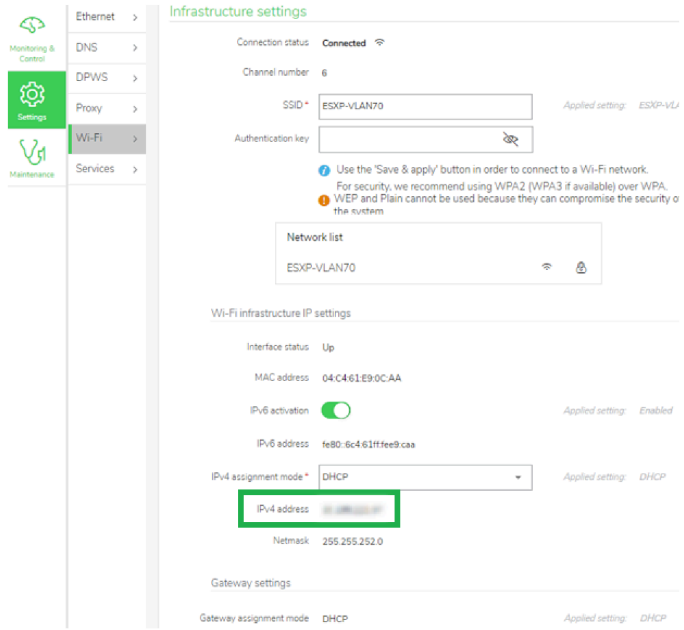
1. On your smartphone, activate the Wi-Fi access point function.
2. Disconnect the Panel Server Entry from the customer network and connect it to your PC with an RJ45 cable.
3. Discover the Panel Server Entry using your Windows file explorer.
4. Wait until the EcoStruxure Panel Server icon displays in the list of devices in the network. It may take up to 2 minutes after the Panel Server is powered on.

   Result: The EcoStruxure Panel Server icon that displays under **Network** is as follows:

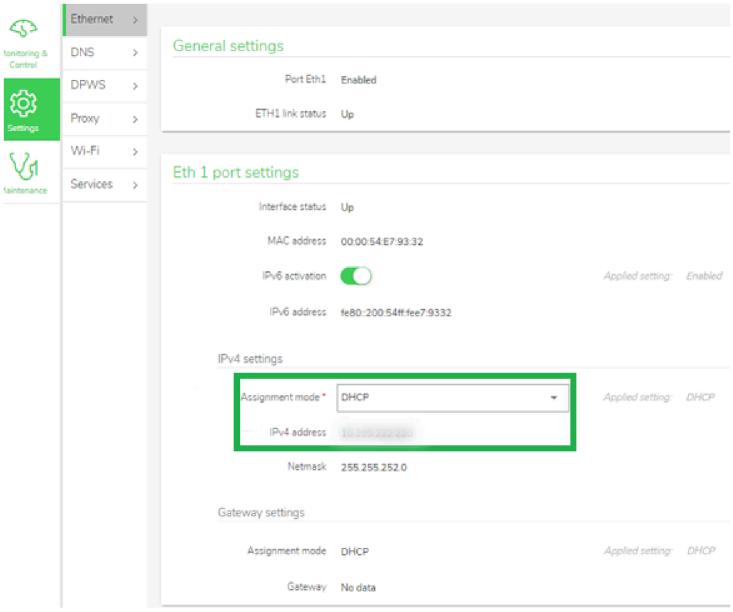
5. Double-click the EcoStruxure Panel Server icon.

   Result: The Panel Server webpages open.
6. On the Panel Server webpages at **Settings > Network configuration**, activate Wi-Fi.
7. Connect the Panel Server to the Wi-Fi network of your smartphone
8. On the webpages at **Settings > Network configuration > Wi-Fi > Infrastructure settings** make a note of the IPv4 address to use later.



9. Disconnect the Panel Server from your PC and connect it to the customer network with the RJ45 cable.
10. Connect your PC to the Wi-Fi network of your smartphone.
11. From your PC, connect to the Panel Server webpages by opening a Web browser page and entering the Wi-Fi IP address noted earlier.

12. At **Settings > Network configuration > Ethernet > Eth 1 port settings**, retrieve the DHCP IP address, as indicated in the following screenshot:



13. Return to Panel Server webpages at **Settings > Network configuration** to deactivate the Wi-Fi.
14. Disconnect your PC from your smartphone Wi-Fi network and switch off the Wi-Fi access point on your smartphone.

Appendix H: Contextualization Data

Presentation

Contextualization data is assigned to devices during commissioning. It provides information about the context and use of the devices within the Panel Server system. The following types of contextualization data can be assigned:

- Commodity
- Usage
- Zone

Commodity List

The following list indicates the commodities available to be assigned to devices and to use for filtering data on the Panel Server webpages:

- Air
- Electricity
- Environment
- Fuel Oil
- Gas
- Other
- Steam
- Water

Usage List

The following list indicates the usages available to be assigned to devices and to use for filtering data on the Panel Server webpages:

- Air conditioning
- Compressed air
- Computer
- Cooking
- Cooling
- Domestic hot water
- Electrical vehicle charging station
- Elevator
- Emergency lighting
- Food refrigeration
- Genset
- Heating
- Heating & Air conditioning
- Hot sanitary water
- HVAC
- IT
- Lighting
- Lighting (Exterior and Park)

- Lighting (Interior)
- Loads associated with renewable power source
- Machine
- Main/Incomer
- Mixed usages
- Office equipment
- Other
- Plug loads
- Process
- Refrigeration
- Renewable power source
- Sockets
- Special loads
- Sub/Head of group
- Total
- Transportation system
- Vapor
- Ventilation
- Water
- Water pump system

Zone Management

You can create up to 50 zones and assign devices to each zone to enable you to view data associated with a specific zone in your system more easily.

> **NOTE:** Zone data is not published to Cloud or to SFTP or HTTPS servers. Zone data is not exported in a local csv export or through the **Trending** webpage (Advanced model)

From the device page in **Settings**, click the zone settings icon next to **Zone** in **Contextualization data**. The zone setting table opens. The table displays the list of all created zones and the number of devices associated with each zone.

Zones are displayed in alphabetical order by default. You can display them in reverse alphabetical order by clicking the arrow in the **Zone name** header. You can also display them in order of number of associated devices by clicking the arrow in the **Associated devices** header.

From the table you can perform the following actions:

- **Create a new zone**: enter the name of the new zone in the empty cell at the bottom of the table. A zone name can be up to 50 characters in length and can contain letters, numbers, spaces and/or special characters. A message pops up to inform you if the zone name already exists. Click on the ✓ to add the new zone to the table.
- **Modify a zone name**: click the edit icon ( ). Enter the new name and click ✓. The name is automatically updated for all associated devices.
- **Delete a zone**: click the bin icon ( ). A popup message requires you to confirm that you wish to delete the zone. Devices previously assigned to this zone are no longer associated with a zone.

Glossary

A

Aggregated data:

Integrated data which is collected and combined from devices associated with selected usages or zones to present a summary or overview of consumption. It is applicable in the **Home** and **Trending** menus.

C

Continuous data:

A measurement, for example Active power A, Apparent power C, Temperature. Data is displayed in a line graph.

Custom model:

A device model created by the user, which defines the list of measurements and alarms supported by the Modbus device connected to the Panel Server. The custom model can be for a device for which no built-in model exists, or for a device where a built-in model exists but only a limited list of measurements and alarms are required by the user. The custom model is created using the EPC Web tool.

D

Data publication:

Sampled data exported to a dedicated server in a defined format with a defined frequency, depending on the publication method selected.

Data sampling:

Function that allows you to log and historize the measurements in the Panel Server or in the Schneider Cloud. The Panel Server webpages allow you to select a subset of measurements and to configure the sampling period.

Device code:

Panel Server unique identifier and the credentials used in the following cases:

- Secure claiming of the Panel Server from a cloud application.
- As a password for first connection to Wi-Fi access point of the Panel Server.

The Panel Server device code should be treated as confidential information.

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.

E

EcoStruxure Power Commission Web (EPC Web):

An online tool for creating, testing and deploying custom device models for use with EcoStruxure Panel Server.

EcoStruxure Power Commission:

An all-in-one software tool used to configure, test, and provide reporting for smart devices in customer electrical equipment.

H

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 16-character RF-ID wireless device, which enables you to launch a discovery of the device with heightened security from the Panel Server. Find the install code of my device.

Integrated data:

A measurement calculated over a period of time, for example, reactive energy received, measured in kWh. Data is displayed as a bar chart.

L

LQI: Link quality indicator

M

Modbus TCP/IP:

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

P

PER: Packet error rate

R

RF-ID:

An IEEE 802.15.4 address assigned to each wireless device. It is the unique identifier of the device and is used during discovery of the device by the Panel Server. Find the RF-ID of my device.

RSSI: Received signal strength indicator

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.

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.

Schneider Electric
1884 Boulevard de la Défense
92000 Nanterre
France

www.se.com

© 2026 – Schneider Electric. All rights reserved.

DOCA0172EN-22