



EcoStruxure Panel Server

User Guide

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

EcoStruxure offers IoT-enabled architecture and platform.

DOCA0172EN-13
05/2024



Legal Information

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

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

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

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

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

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

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

Table of Contents

Safety Information.....	7
About the Book.....	10
EcoStruxure Panel Server Presentation	13
Introduction	14
EcoStruxure Panel Server System	17
Hardware Description	22
Hardware Connection	29
Go2SE Landing Page	31
EcoStruxure Power Commission (EPC) Software.....	34
Edge Monitoring and Supervision Software	35
Cloud Applications.....	36
Technical Characteristics	38
Schneider Electric Green Premium™ Ecolabel	42
EcoStruxure Panel Server Communication Functions.....	45
Communication Architectures.....	46
Network Settings	51
TCP/IP Communication.....	52
Ethernet Communication	53
Wi-Fi Communication.....	57
Permanent Deactivation of Wireless Networks	60
DNS.....	61
Proxy	62
IP Network Services (DPWS).....	63
Modbus TCP/IP Client (Universal and Advanced Models)	64
Modbus TCP/IP Server.....	66
IEEE 802.15.4 Communication.....	67
Modbus-SL Communication	70
EcoStruxure Panel Server General Functions	75
Modbus Gateway Function.....	76
Examples of Modbus Routing	80
Data Publication	87
Publication on Schneider Electric Cloud.....	88
Publication on SFTP Server.....	91
Publication on HTTPS Server	94
Publication of Emails for Alarms (Advanced Model)	97
Publication on SFTP Server and Email Notification for Alarms (Advanced Model).....	99
Publication on HTTPS Server and Email Notification for Alarms (Advanced Model).....	100
Output and Scheduled Control from Cloud.....	101
Date and Time.....	102
Data Sampling.....	104
Data Logging (Advanced Model).....	107
Home (Advanced Model).....	109
Data Trending (Advanced Model).....	110
Exporting Data Locally (Advanced Model)	113

Custom Models for Downstream Modbus Devices (Universal and Advanced Models).....	116
Alarms	119
Notifications (Advanced Model)	124
Firmware Update.....	126
User Management.....	127
Digital Inputs (PAS600L, PAS600LWD, PAS800L).....	128
Diagnostics	131
Diagnostics Logs	134
Backup and Restore Panel Server Configuration.....	136
Cybersecurity Recommendations	138
Security Capabilities	139
Security Recommendations for Commissioning	141
Security Recommendations for Operation	142
Security Recommendations for Decommissioning.....	143
General Principle to Commission an EcoStruxure Panel Server	144
Getting Started with EcoStruxure Power Commission Software	145
First Connection with EcoStruxure Power Commission Software.....	146
Non-Selective Pairing of Wireless Devices	147
Selective Pairing of Wireless Devices.....	148
Device Configuration with EcoStruxure Power Commission Software	149
Getting Started with EcoStruxure Panel Server Webpages	150
First Connection to EcoStruxure Panel Server Webpages.....	151
Using EcoStruxure Panel Server Webpages.....	154
EcoStruxure Panel Server User Interface Layout	155
EcoStruxure Panel Server Webpage Menus	159
Addition and Removal of Modbus Devices	170
Pairing/Unpairing of Wireless Devices Through Webpages.....	174
Selective Pairing of Wireless Devices Through Webpages	175
Controlled Pairing of Wireless Devices (PowerTag Energy, HeatTag) Through Webpages	176
Configuration of Wireless Energy Devices Through Webpages	177
Configuration of PowerTag Control Devices Through Webpages.....	182
Configuration of Ambient Sensors Through Webpages	185
Unpairing Wireless Devices Through Webpages	187
Adding Wireless Devices Paired Under a Child Gateway (Universal and Advanced Models).....	189
Troubleshooting	191
Appendices	194
Appendix A: Details of Modbus Functions.....	195
Modbus TCP/IP Functions	196
Modbus-SL Functions	198
Modbus TCP/IP and Modbus-SL Exception Codes	199
Modbus Registers Tables	201
Function 43-14: Read Device Identification	202

Function 100-4: Read Non-Adjacent Registers 204

Setting Message Timeout for Modbus Client and Modbus
Server 205

Appendix B: Data Availability 207

PowerTag, PowerLogic Tag, and Acti9 Active Data Availability 208

Environmental Sensor Data Availability 213

Appendix C: Wireless Device Network Indicators 214

Appendix D: SFTP and HTTPS Publication File Formats 215

Appendix E: SSH Key Exchange and Cipher 218

Appendix F: Certificate Authorities 219

Appendix G: Retrieve the DHCP IP Address of a PAS400 Panel
Server 223

Glossary 225

Safety Information

Important Information

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



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



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

DANGER

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

WARNING

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

CAUTION

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

NOTICE

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

Please Note

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

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

Cybersecurity Safety Notice

⚠ WARNING
POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY
<ul style="list-style-type: none">• 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.

Remote Control

⚠ 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.

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.

About the Book

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	Firmware version
PAS400	EcoStruxure Panel Server Entry firmware version 001.010.000 or greater for hardware version 001.000.000
PAS600, PAS600T, PAS600L	EcoStruxure Panel Server Universal firmware version 001.010.000 or greater for hardware version 001.000.000
PAS600LWD, PAS600PWD	EcoStruxure Panel Server Universal Wired by Design model firmware version 001.010.000 or greater for hardware version 002.000.000
PAS800, PAS800L, PAS800P	EcoStruxure Panel Server Advanced firmware version 001.010.000 or greater for hardware version 001.000.000

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.

Convention

EcoStruxure Panel Server is hereafter referred to as Panel Server.

Online Information

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

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

Related Documents

Title of documentation	Reference number
<i>EcoStruxure Panel Server - Catalog</i>	PLSED310196EN
<i>EcoStruxure Panel Server Entry - Instruction Sheet</i>	NNZ76760

Title of documentation	Reference number
<i>EcoStruxure Panel Server Universal - Instruction Sheet for PAS600, PAS600L and PAS600T</i>	GDE74119
<i>EcoStruxure Panel Server Universal Wired by Design - Instruction Sheet for PAS600LWD and PAS600PWD hardware version 002.000.000</i>	PKR28607
<i>EcoStruxure Panel Server Advanced - Instruction Sheet for PAS800, PAS800L and PAS800P</i>	JYT24469
<i>EcoStruxure Panel Server - Wireless Devices / Wi-Fi Antenna - Instruction Sheet</i>	NNZ58425
<i>EcoStruxure Panel Server Entry - Firmware Release Notes</i>	DOCA0249EN DOCA0249DE DOCA0249ES DOCA0249FR DOCA0249IT DOCA0249PT
<i>EcoStruxure Panel Server Universal - Firmware Release Notes</i>	DOCA0178EN DOCA0178DE DOCA0178ES DOCA0178FR DOCA0178IT DOCA0178PT
<i>EcoStruxure Panel Server Advanced - Firmware Release Notes</i>	DOCA0248EN DOCA0248DE DOCA0248ES DOCA0248FR DOCA0248IT DOCA0248PT
<i>EcoStruxure Panel Server - Cybersecurity Guide</i>	DOCA0211EN DOCA0211DE DOCA0211ES DOCA0211FR DOCA0211IT DOCA0211PT
<i>EcoStruxure Panel Server - Modbus File</i>	DOCA0241EN
<i>EcoStruxure Panel Server - Alarm File</i>	DOCA0330EN
<i>How Can I Reduce Vulnerability to Cyber Attacks?</i>	Cybersecurity System Technical Note
<i>EcoStruxure Power - Guide for Designing and Implementing a Cyber Secure Digital Power System - Technical Guide</i>	ESXP2TG003EN
<i>Wireless Communication Architectures With EcoStruxure Panel Server - Design Guide</i>	DOCA0289EN DOCA0289DE DOCA0289ES DOCA0289FR DOCA0289IT DOCA0289PT

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.....	14
EcoStruxure Panel Server System.....	17
Hardware Description	22
Hardware Connection	29
Go2SE Landing Page	31
EcoStruxure Power Commission (EPC) Software	34
Edge Monitoring and Supervision Software	35
Cloud Applications	36
Technical Characteristics	38
Schneider Electric Green Premium™ Ecolabel	42

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, EcoStruxure Facility Expert, 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 commissioning with EcoStruxure Power Commission software, enabling device plug-and-play and auto-discovery features.
- ease of operation with user-friendly embedded webpages, and data contextualization for more relevant analytics.
- 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)

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 18.
- 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), and 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, EcoStruxure Facility Expert, EcoStruxure Asset Advisor, and EcoStruxure Resource Advisor)
- Setup through EcoStruxure Power Commission software allowing off-line configuration preparation, and embedded webpages

Feature Availability

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

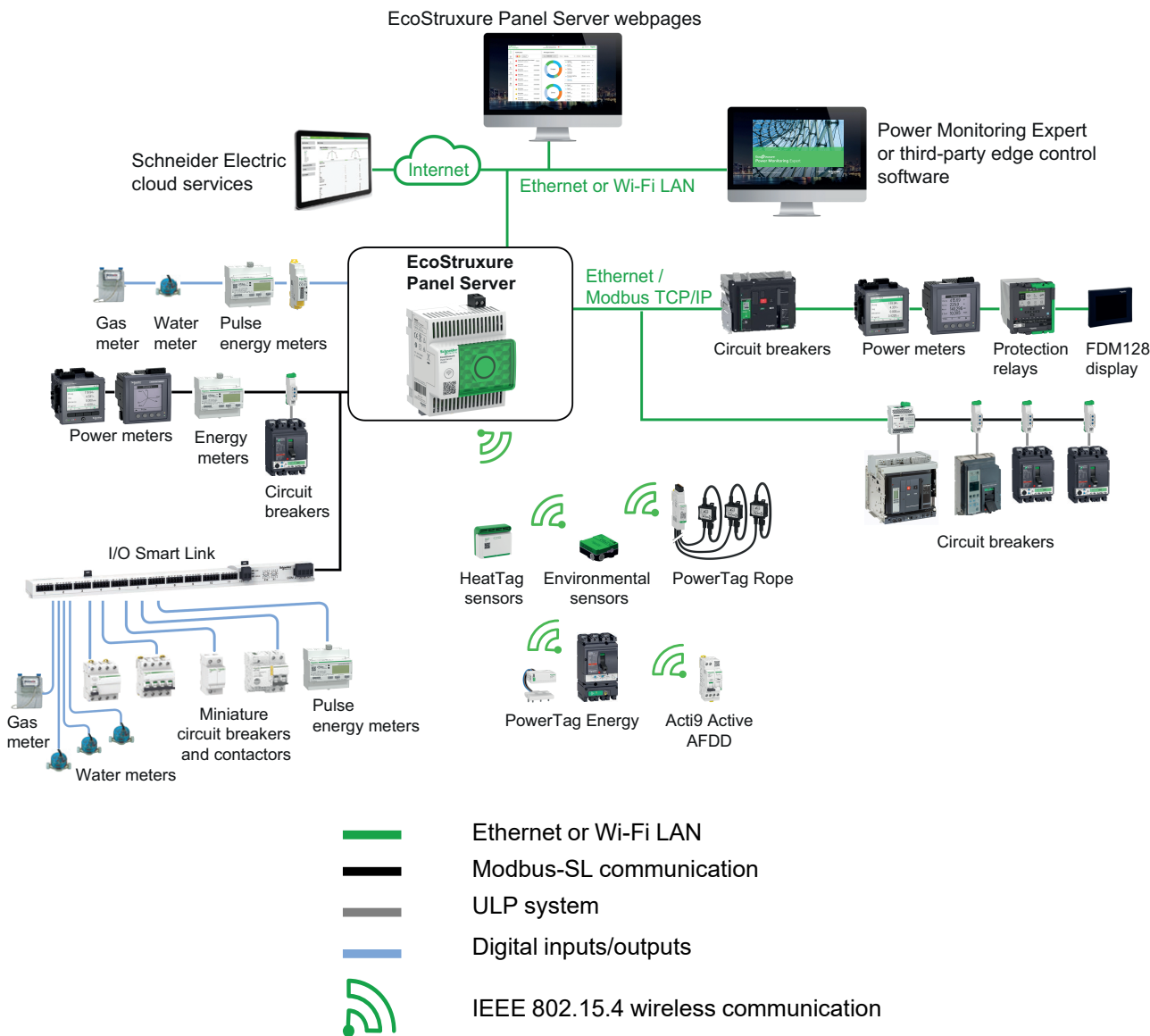
Main Features		EcoStruxure Panel Server								
		Entry	Universal					Advanced		
		PAS400	PAS600	PAS600T	PAS600L	PAS600LWD	PAS600PWD	PAS800	PAS800L	PAS800P
Power supply	24 Vdc	-	-	-	✓	✓	-	-	✓	-
	110-240 Vac / Vdc	-	-	✓	-	-	-	-	-	-
	110-277 Vac / Vdc	✓	✓	-	-	-	-	✓	-	-
	Power over Ethernet (PoE)	-	-	-	-	-	✓	-	-	✓
10/100BASE-T Ethernet	One RJ45 port	✓	-	-	-	-	-	-	-	-
	Two RJ45 ports	-	✓	✓	✓	✓	✓	✓	✓	✓
Upstream Modbus TCP/IP connectivity		✓	✓	✓	✓	✓	✓	✓	✓	✓
Upstream Wi-Fi connectivity		✓	✓	✓	✓	-	-	✓	✓	✓
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		-	-	-	-	-	-	✓	✓	✓
Commissioning tool of Panel Server and connected devices		<ul style="list-style-type: none"> EcoStruxure Power Commission software EcoStruxure Panel Server webpages 								
Schneider Electric cloud application		<ul style="list-style-type: none"> EcoStruxure Energy Hub EcoStruxure Facility Expert 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:



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.

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.

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.

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 sensors
 - Acti9 Active
 - Environmental sensors:
 - Easergy TH110/CL110
 - HeatTag sensors
 - Wireless CO₂ sensors
 - Wireless temperature and humidity sensors
 - PowerTag Ambient
 - PowerTag A
 - Control devices:
 - PowerTag Control
 - Wireless indication auxiliaries for ComPacT and PowerPacT circuit breakers
 - Other wireless devices: PowerLogic PD100

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*

Maximum Configuration

The maximum number of devices that can be configured in a system with a Panel Server depends on the model.

Panel Server Entry

Wireless device	Maximum concurrent number of devices
PowerTag Energy sensors	20
PowerLogic Tag energy sensors	20
Acti9 Active devices	20
PowerTag Control devices	20
Wireless indication auxiliaries for ComPacT and PowerPacT circuit breakers	20
Wireless CO ₂ sensors	20
Wireless temperature and humidity sensors	20
PowerTag A devices	20
PowerTag Ambient sensors	20
Easergy TH110/CL110 environmental sensors	20
PowerLogic HeatTag sensors	15
PowerLogic PD100 devices	15
Constraints within a mixed configuration: Any combination of wireless devices listed in the rows above must not exceed 20 devices .	

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 concurrent number of 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
	Wireless CO ₂ sensors	100
	Wireless temperature and humidity sensors	100
	PowerTag A devices	100
	PowerTag Ambient sensors	100
	Easergy TH110/CL110 environmental sensors	100
	PowerLogic HeatTag sensors	15
	PowerTag Control devices	10
	PowerLogic PD100 devices	15
	Constraints within a mixed configuration of wireless devices: <ul style="list-style-type: none"> Any combination of wireless devices listed in the rows above must not exceed 40 devices. The total number of PowerTag Control, PowerLogic HeatTag, and PowerLogic PD100 should not exceed 20 devices. 	
Modbus-SL devices	without repeater	32
	with repeater	128

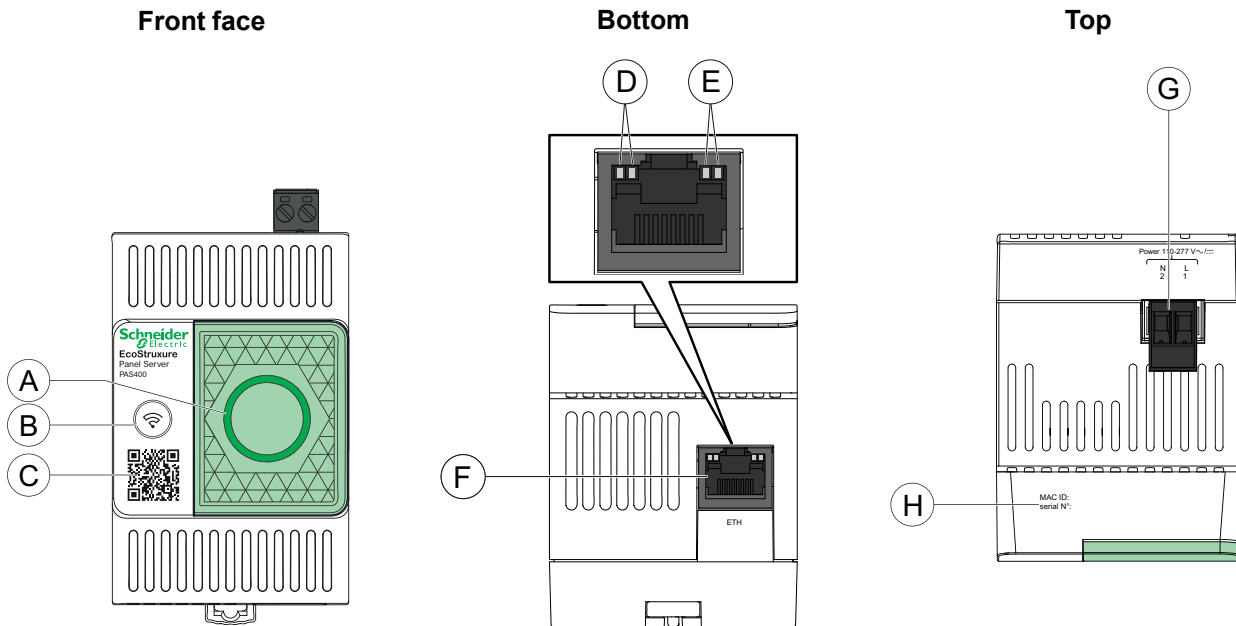
NOTE: The maximum number depends on the serial line length and the type of device(s)

Device type		Maximum concurrent number of devices
	I/O devices: <ul style="list-style-type: none"> • I/O Smart Link device • Acti9 Smartlink Modbus-SL device • SmartLink SIB gateway 	<ul style="list-style-type: none"> • 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.

Hardware Description

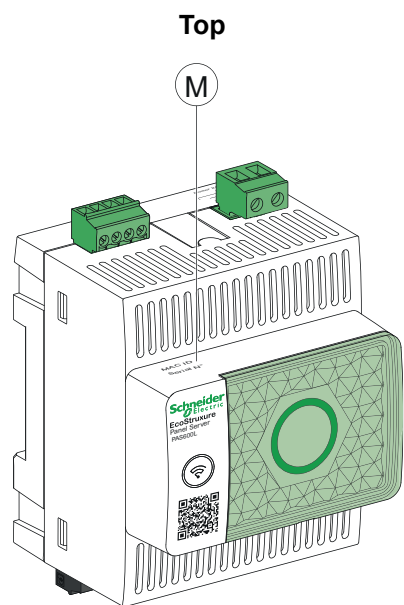
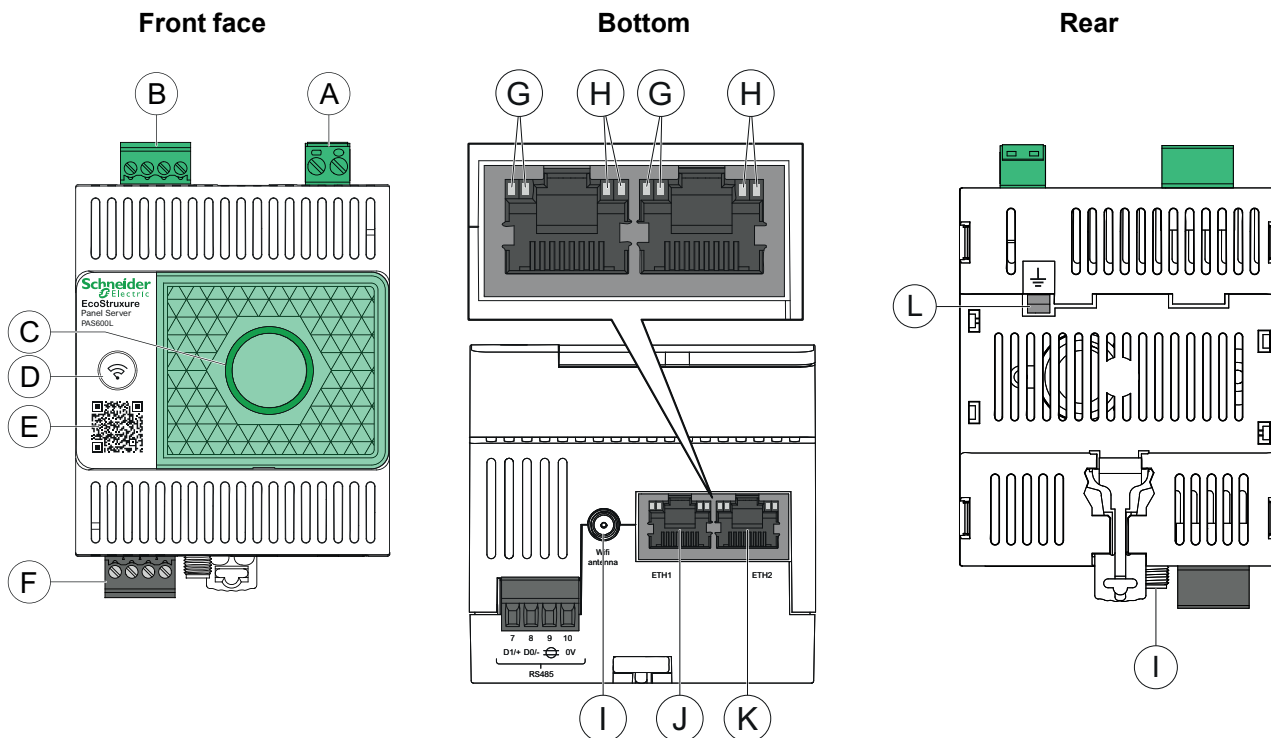
Panel Server Entry



- A. Panel Server status LED
- B. Restart button
- C. QR code to product information (including device code 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.

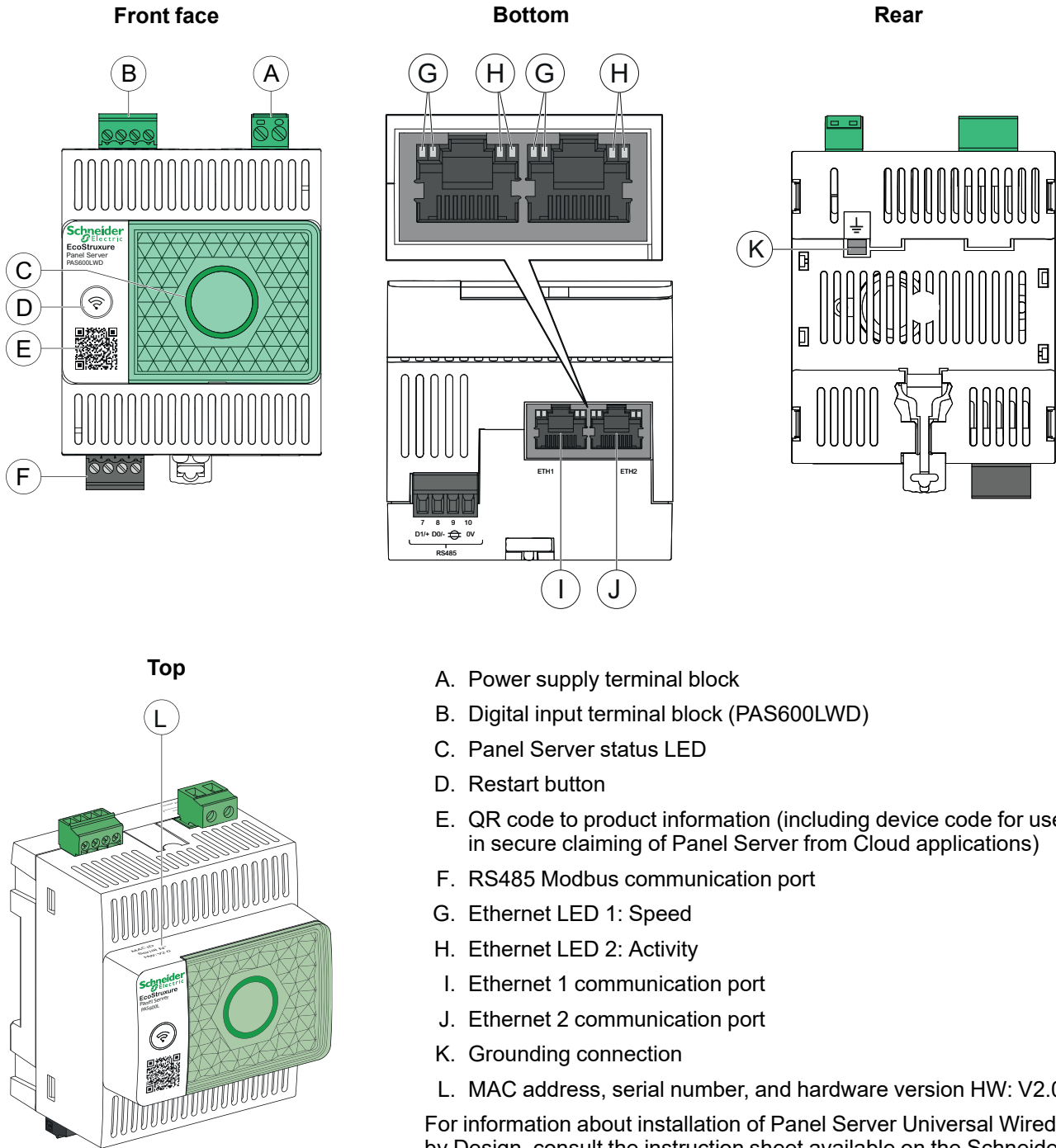
Panel Server Universal



- A. Power supply terminal block
- B. Digital input terminal block (PAS600L)
- C. Panel Server status LED
- D. Restart button
- E. QR code to product information (including device code 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

For information about installation of Panel Server Universal, consult the relevant instruction sheet available on the Schneider Electric website: GDE74119

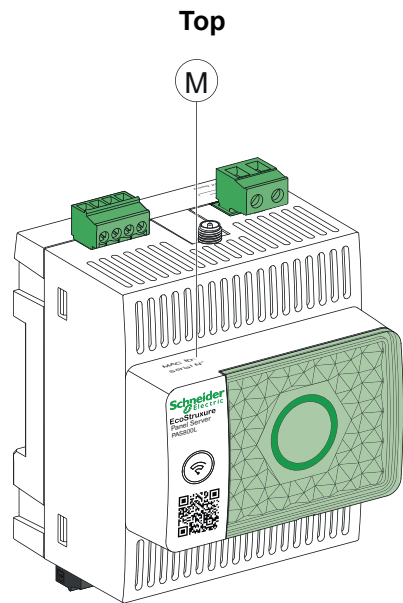
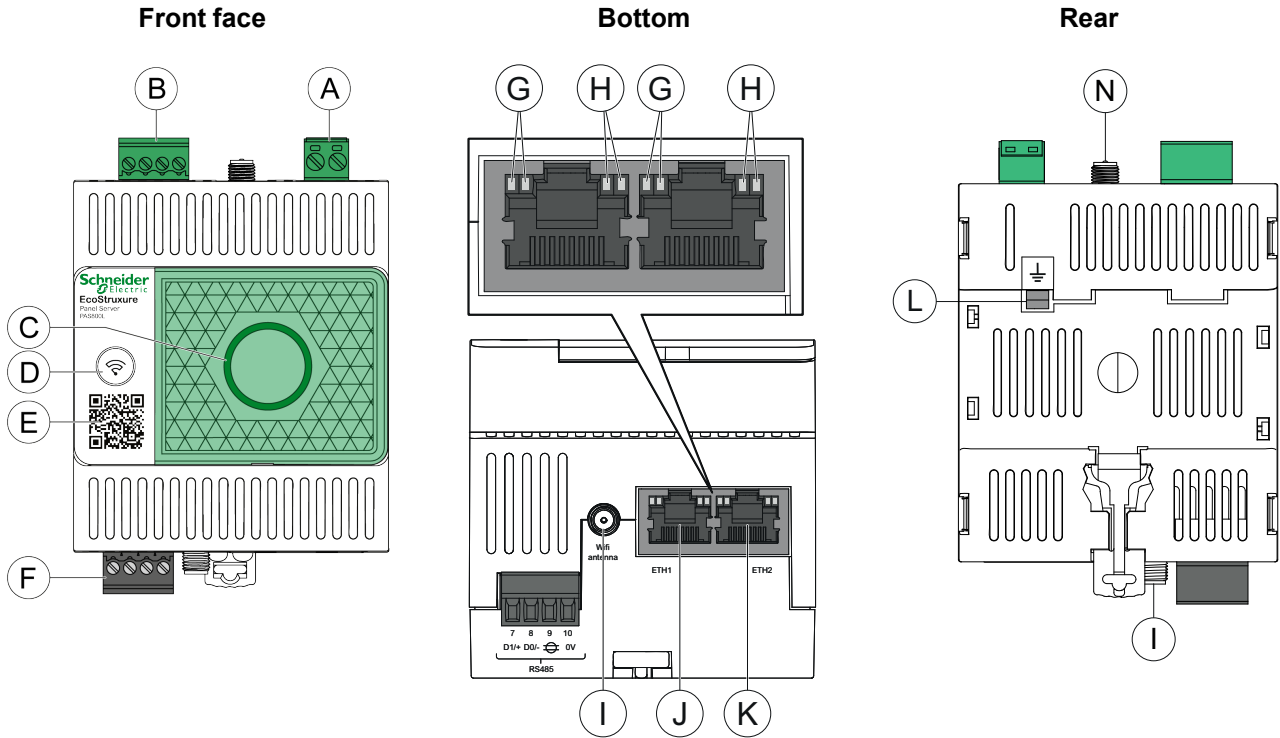
Panel Server Universal Wired by Design



- A. Power supply terminal block
- B. Digital input terminal block (PAS600LWD)
- C. Panel Server status LED
- D. Restart button
- E. QR code to product information (including device code 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
- 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



- A. Power supply terminal block (PAS800, PAS800L)
- B. Digital input terminal block (PAS800L)
- C. Panel Server status LED
- D. Restart button
- E. QR code to product information (including device code 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
- N. External IEEE 802.15.4 antenna port (PAS800, PAS800L)

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

For information about installation of Panel Server Advanced, consult the instruction sheet available on the Schneider Electric website: JYT24469.

Hardware Version

The new models of Panel Server, PAS600LWD and PAS600PWD are released with hardware version 002.000.000.

To identify your hardware version, 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.

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

Restart Button

To restart the Panel Server:

1. Press and hold the button for more than 10 seconds then release it.

Result: The status LED turns steady orange.

2. Wait for the Panel Server to restart completely:
 - a. The status LED remains steady orange while the Panel Server is rebooting.
 - b. The status LED turns steady green when the Panel Server is in normal operation.

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 31.

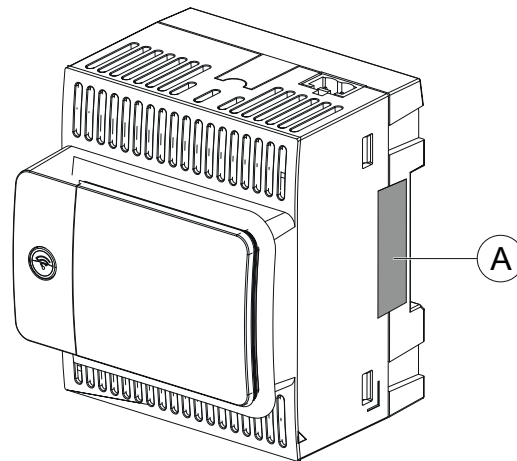
The landing page displays:

- 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 (Optional)

The external Wi-Fi antenna is an option for

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

Use the external Wi-Fi antenna in specific use cases such as when the Panel Server is installed in a switchboard with metallic partitions and door. The antenna improves the quality of radio frequency signal.

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

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

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

External IEEE 802.15.4 Antenna (Optional)

The external IEEE 802.15.4 antenna is an option for Panel Server Advanced.

Use the external IEEE 802.15.4 antenna in specific use cases such as when the Panel Server 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 network outside the switchboard.

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

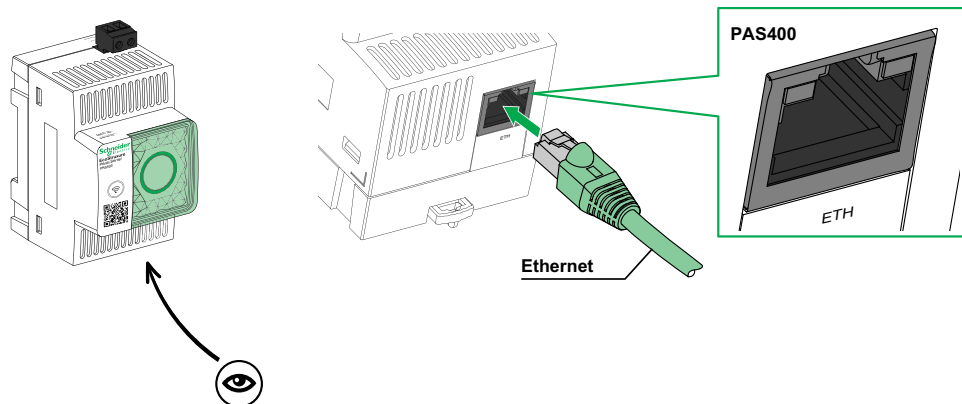
For information about installation of the external antenna, consult the instruction sheet available on the Schneider Electric website: NNZ58425.

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

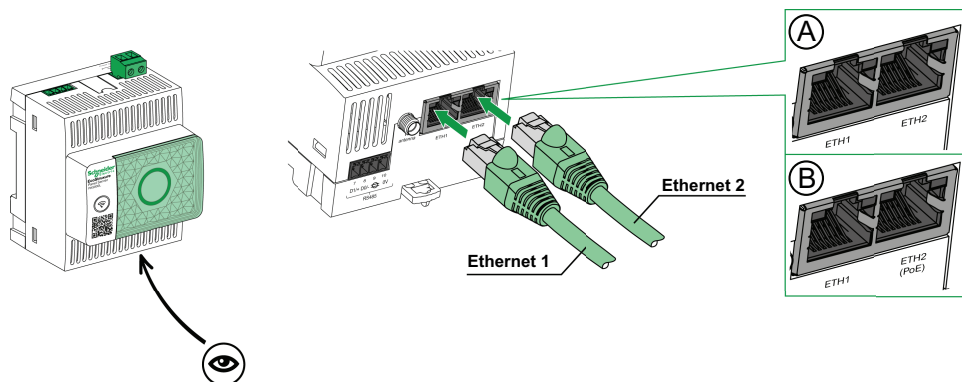
Hardware Connection

Connection to Ethernet

Entry model



Universal, Advanced models



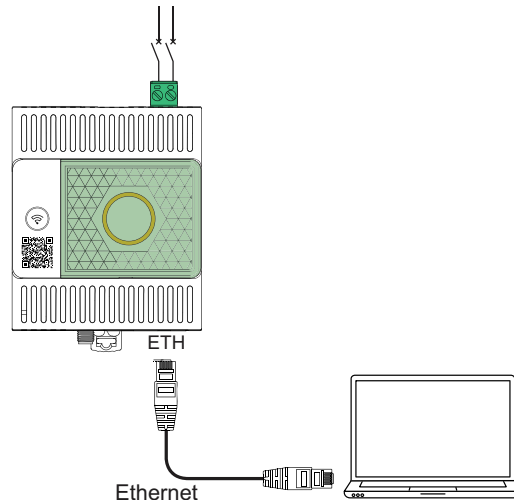
A. Ethernet ports for PAS600, PAS600T, PAS600L, PAS600LWD, PAS800, PAS800L

B. Ethernet ports for PAS600PWD, PAS800P

NOTE: PAS600PWD and PAS800P can be powered by Power over Ethernet (PoE). 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*
- JYT24469 *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**).

Go2SE 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, the Go2SE landing page is displayed.

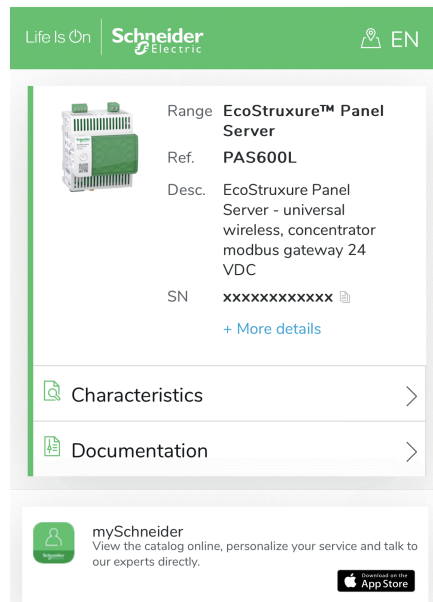
Landing Page Description

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 range
- Product reference
- Product description
- Product serial number
- Landing page menus:
 - Characteristics
 - Documentation
- Downloadable applications

The following example shows the landing page displayed on an Android smartphone:



Characteristics

Selecting this menu gives access to a product datasheet with detailed information about your Panel Server.

Documentation

Selecting this menu gives access to technical publications associated with Panel Server

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 alarm views, and historical analysis from devices (depending on the model), for entry-level energy and operation management.

Electrical product and commissioning capabilities allow you to:

- Define and pair wireless devices installed in the EcoStruxure Panel Server system (depending on the model)
- Define and discover Modbus TCP/IP devices from EcoStruxure Panel Server (depending on the model)

Energy and operation management capabilities allow you to:

- View real-time data and events locally or remotely through a supported web browser.
- View trending on historical data, up to a period of 3 years (Advanced model).
- Select the device data you want to log, and set logging intervals (Advanced model).
- Export selected logged data to your PC or an SFTP server for additional analysis (Advanced model).
- Provide data and improve system security through password protection and controlled access to individual webpages.

For more detailed information about the webpages, refer to [Using EcoStruxure Panel Server Webpages](#), page 154.

EcoStruxure Power Commission (EPC) Software

Overview

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 and initiating maintenance plans through the digital logbook functionality in EcoStruxure Facility Expert.

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.
 - Initiate preventive maintenance plans and export data to the digital logbook feature in EcoStruxure Facility Expert, app and cloud-based software for facility and building management.
 - 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](#).

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)

Connect your building energy systems and smart devices with EcoStruxure Energy Hub. 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 Facility Expert (EFE)

EcoStruxure Facility Expert is a cloud-based software application from Schneider Electric to improve energy efficiency, and manage assets and maintenance.

EcoStruxure Facility Expert is used for small and medium buildings in industry, retail, public, and healthcare markets.

EcoStruxure Facility Expert allows you to outsource energy management and maintenance, reducing your energy costs and increasing operating efficiency in buildings.

EcoStruxure Facility Expert provides the following features:

- Support for data acquisition hardware: meters, gateways, and sensors.
- Cloud platform for data displays.
- Consulting services from Schneider Electric expert teams.
- A network of local partners to implement solutions.

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		<ul style="list-style-type: none"> 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		<ul style="list-style-type: none"> 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: < 2000 m (< 6500 ft)	Horizontal installation (for indoor use in non-wet locations only)	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 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: 2000–4000 m (6500–13000 ft)	PAS600L, PAS600LWD, PAS800L	-25 °C to +60 °C (-13 °F to +140 °F)
Pollution degree	PAS400, PAS600, PAS600T, PAS600PWD, PAS800, PAS800P	2
	PAS600L, PAS600LWD, PAS800L	3
Altitude	All models	< 2000 m (< 6500 ft)
	PAS600L, PAS600LWD, PAS800L	< 4000 m (< 13000 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		<ul style="list-style-type: none"> IEC 61326-1 IEC 62974-1 EN 301489-1 EN 301489-17
Immunity		<ul style="list-style-type: none"> IEC 61326-1 IEC 62974-1 EN 301489-1 EN 301489-17
Environment: emissions		<ul style="list-style-type: none"> CISPR 11 EN 55032
Electromagnetic compatibility and Radio spectrum Matters (ERM)		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> • 10/100BASE-T Ethernet RJ45 ports: <ul style="list-style-type: none"> ◦ Entry model: one port ◦ Universal and Advanced models: two ports • RS485 Modbus port • Wi-Fi compliant to standard IEEE 802.11 a/b/g/n <ul style="list-style-type: none"> ◦ Entry, Universal, and Advanced models: 2.4 GHz, 5 GHz • 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	<ul style="list-style-type: none"> • 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)

Electrical Characteristics

Characteristic		EcoStruxure Panel Server								
		Entry	Universal					Advanced		
		PAS400	PAS600	PAS600T	PAS600L	PAS600LWD	PAS600PWD	PAS800	PAS800L	PAS800P
Power supply	110–277 Vac/dc (±10 %)	✓	✓	-	-	-	-	✓	-	-
	24 Vdc (±10 %)	-	-	-	✓	✓	-	-	✓	-
	110–240 Vac/dc (±10 %)	-	-	✓	-	-	-	-	-	-
	Power over Ethernet (PoE)	-	-	-	-	-	✓	-	-	✓
Power consumption	3W (10VA) (maximum)	-	✓	✓	-	-	-	-	-	-
	3W (maximum)	-	-	-	✓	-	-	-	-	-
	3.5W (12VA) (maximum)	✓	-	-	-	-	-	✓	-	-
	3.5W (maximum)	-	-	-	-	✓	✓	-	✓	✓
Power input	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> External Wi-Fi antenna (option for Advanced models) External IEEE 802.15.4 antenna (option for Universal, excluding WD models, and Advanced models) 	
Degree of protection	<ul style="list-style-type: none"> Connectors: IP20 Other faces: IP30 Front face nose: 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	<ul style="list-style-type: none"> State 0: 0–5 V State 1: 15–28 V
Input current	<ul style="list-style-type: none"> 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.

Schneider Electric Green Premium™ Ecolabel

Description

Green Premium is a label that allows you to develop and promote an environmental policy while preserving your business efficiency. This ecolabel is compliant with up-to-date environmental regulations.



Accessing Green Premium

Green Premium data on labeled products can be accessed online through any of the following ways:

- By navigating to the Green Premium page on the Schneider Electric website.
- By navigating to the product page on the mySchneider application on your smartphone

NOTE: To download and install the mySchneider app, scan the QR code on the front face of any Schneider Electric product and click the mySchneider link to go to your app store.


Checking Products Through the Schneider Electric Website

To check the environmental criteria of a product using a PC or smartphone, follow these steps:

Step	Action
1	On the Green Premium page, select Sustainability > For customers > Green Premium products .
2	Click Check your product and access environmental data .
3	On the page Check a product , manually enter the commercial reference or product range of the product to search for. NOTE: You can also select the Search a list of part numbers tab to send a file with a list of commercial references of products to search for.
4	To search for several products simultaneously, click Add product and then fill in the fields.
5	Click Check product(s) to generate a report of the environmental criteria available for the products with the entered commercial references.
6	A window named Green Premium Declaration appears. Click on I accept to access the product information.
7	The Check a product page is displayed with the list of documents for the selected products for each type of environmental data. Each document can be downloaded to your PC.

Checking Products Through the mySchneider App

To check the environmental criteria of a product using mySchneider app on your smartphone, follow these steps:

Step	Action
1	Open the mySchneider app.
2	In the search field at the top of the Product Catalog page: <ul style="list-style-type: none"> • Enter the commercial reference of the product to search for • or press the QR code icon in the search box  and scan the QR code on the front face of the product to search for.
3	When the page of the commercial reference searched for opens, scroll down and select Green Premium .
4	The Green Premium documents attached to the product are listed on the Green Premium page. Select the required document to refer or download it.

Environmental Criteria

The Green Premium ecolabel provides documentation on the following criteria about the environmental impact of the products:

- RoHS: Restriction of Hazardous Substances (RoHS) directive
 - For European Union
 - For China
- REACH: European Union Registration, Evaluation, Authorization, and Restriction of Chemicals regulation.
- Product Environmental Profile (PEP)
- End of Life Instructions (EoLI).

RoHS

Schneider Electric products are subject to RoHS requirements at a worldwide level, even for the many products that are not required to comply with the terms of the regulation. Compliance certificates are available for products that fulfill:

- The RoHS criteria defined by the European Union.
- The RoHS criteria defined by China.

REACH

Schneider Electric applies the strict REACH regulation on its products at a worldwide level, and discloses extensive information concerning the presence of Substances of Very High Concern (SVHC) in all of these products.

Product Environmental Profile (PEP)

Schneider Electric publishes complete set of environmental data, including carbon footprint and energy consumption data for each of the life cycle phases on all of its products, in compliance with the ISO 14025 PEP ecopassport program. Product environmental profile is especially useful for monitoring, controlling, saving energy, and/or reducing carbon emissions.

End of Life Instructions (EoLI)

The end of life instructions are in compliance with the Waste Electrical and Electronic Equipment (WEEE) directive and provide:

- Recyclability rates for Schneider Electric products.
- Guidance to mitigate personnel hazards during the dismantling of products and before recycling operations.
- Part identification for recycling or for selective treatment, to mitigate environmental hazards/incompatibility with standard recycling processes.

EcoStruxure Panel Server Communication Functions

What's in This Part

Communication Architectures.....46
Network Settings.....51
TCP/IP Communication52
IEEE 802.15.4 Communication.....67
Modbus-SL Communication.....70

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.

Availability

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

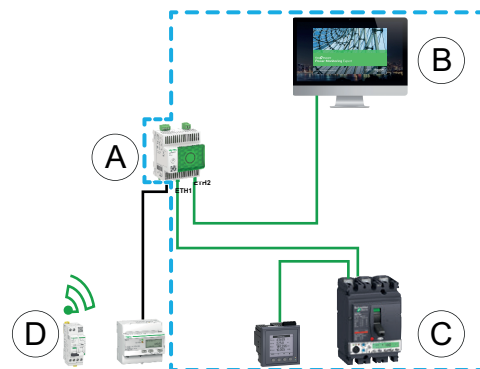
Switched Ethernet Network

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.

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.

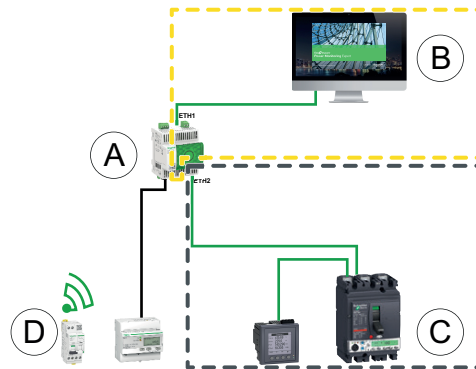
The Panel Server supports direct connection to a PC on either of the Ethernet ports (ETH1 and ETH2). When connected, it is possible to ping and/or access the Panel Server webpages from a PC. Note that SSH connection is not supported.

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 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.

Separated Ethernet network with two Ethernet ports enabled upstream

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

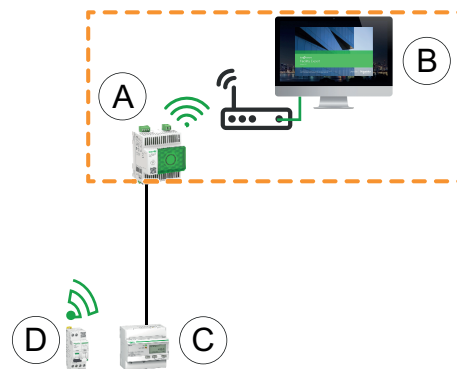
To set up this architecture:

- 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

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.

This set up is possible through the Panel Server webpages, not EcoStruxure Power Commission software.

Network with Wi-Fi and Switched Ethernet Network

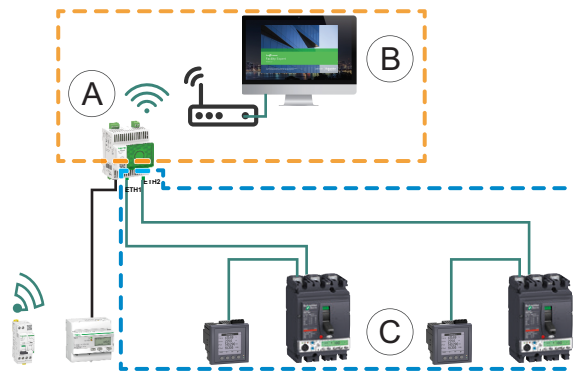
The following diagram illustrates an architecture with Wi-Fi upstream and Ethernet port configuration in switched mode downstream. There is one downstream Ethernet network. The Wi-Fi and Ethernet networks managed by the Panel Server are separated.

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**

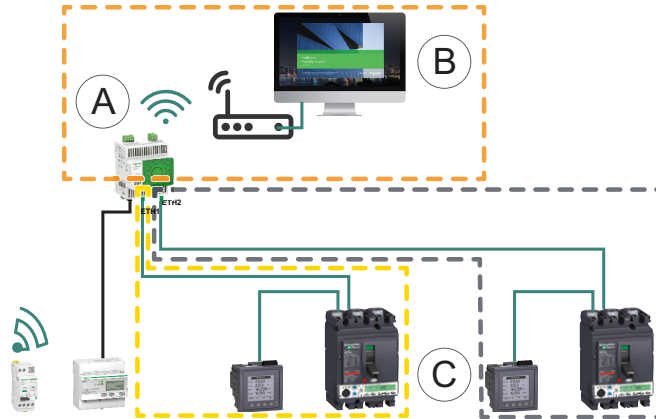
To set up this architecture:

- Enable Wi-Fi.
- Configure Ethernet network in the switched mode.
- 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.




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

To set up this architecture:

- Enable Wi-Fi.
- Configure Ethernet network in the separated mode.
- 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 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 (depending on the model)

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 the Panel Server webpages, at **Settings > Network communication**.

Select the appropriate network configuration for your system. If necessary, enter the parameters for each connection interface displayed.

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

- Switched Mode Configuration (Universal and Advanced models), page 53
- separated Mode Configuration (Universal and Advanced models), page 54
- Wi-Fi, page 57
- Modbus TCP/IP Client (Universal and Advanced models), page 64
- Modbus TCP/IP Server, page 76

TCP/IP Communication

What's in This Chapter

Ethernet Communication	53
Wi-Fi Communication	57
Permanent Deactivation of Wireless Networks.....	60
DNS	61
Proxy.....	62
IP Network Services (DPWS)	63
Modbus TCP/IP Client (Universal and Advanced Models).....	64
Modbus TCP/IP Server.....	66

Ethernet Communication

Presentation

The Panel Server supports the following applicative 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.
- **Secure File Transfer Protocol (SFTP) Client:** A variant of the standard file transfer protocol (FTP) that uses secure shell encryption to provide a high level of security for file transfer.

The Entry model has one Ethernet port.

The Universal and Advanced models have two Ethernet ports. The Ethernet ports can be configured in two modes:

- Switched mode:
 - Both Ethernet ports belong to the same network.
 - An Ethernet switch function is enabled.
- 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 ETH2 by enabling Modbus service on ETH1.
 - Modbus routing can be enabled from port ETH2 to ETH1 by enabling Modbus service on ETH2.

Availability

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

Switched Mode Configuration (Universal and Advanced Models)

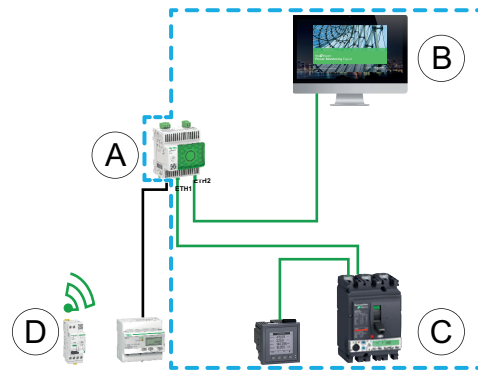
In switched mode, both Ethernet ports (ETH1, ETH2) share the same settings. The Panel Server has one single unique IP address applied to both Ethernet ports. Devices connected to either Ethernet port belong to the same Ethernet network.

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 not supported.

The following diagram illustrates a daisy-chain architecture with Ethernet port configuration in switched mode. Both Ethernet ports are connected to each other using the Panel Server internal Ethernet switch. This enables devices located upstream or downstream from the Panel Server to communicate with each other as part of the same network.



- 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 Resource Advisor)
- C. Wired devices
- D. Wireless devices

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

Separated Mode Configuration (Universal and Advanced Models)

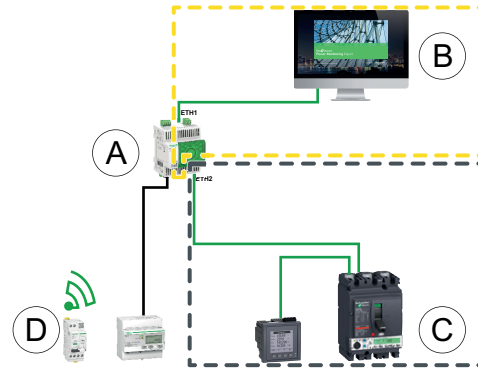
In separated mode, one IP network is assigned to each Panel Server Ethernet port and each IP network assigns an IP address to the Panel Server. The separated mode is used to segregate downstream Modbus TCP/IP devices connected to **ETH2** port from upstream communication systems connected to **ETH1** 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 is the port used for data publishing to a cloud application or a SCADA system. This port can be configured in DHCP client or static IPv4 address. 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 is the port used for data collection to connect downstream Modbus TCP/IP devices for either data collection to a cloud application connected to ETH1 or management by a SCADA system connected to ETH1. This port can be configured in DHCP client or static IPv4 address. 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.

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



- A. Panel Server
- B. Edge monitoring and supervision software like EcoStruxure Power Monitoring Expert or EcoStruxure Power Operation or EcoStruxure cloud services like 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

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 equipment damage.

The Ethernet communication function is set as follows:

- With EcoStruxure Power Commission software
- On the Panel Server webpages, at **Settings > Network communication > Ethernet**

Ethernet Settings (Universal and Advanced Models)

The following table describes the settings and where they are available.

Parameter	Description	EPC software	Webpages
Ethernet port configuration	Used to select the Ethernet configuration mode: <ul style="list-style-type: none"> • Select Separated to define 2 different IP addresses: one for each Panel Server Ethernet port. The separated mode is configured 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. 	✓	✓

IP Configuration 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**
 - In the case of switched mode: **Switched port settings**

Parameter	Description	EPC software	Webpages
Interface status	<ul style="list-style-type: none"> • Active indicates that an Ethernet cable is connected to Panel Server Ethernet port. • Inactive indicates that no Ethernet cable is connected. <p>NOTE: Setting not editable.</p>	✓	✓
MAC address	<p>The Media Access Control (MAC) address is a unique identifier for each Panel Server port.</p> <p>The MAC address is marked on the Panel Server front face nose.</p> <p>NOTE: Setting not editable.</p>	✓	✓
IPv6 activation	Used to enable/disable the IPv6 configuration (enabled by default).	–	✓
IPv6 address	Shows the IPv6 address. Setting not editable. NOTE: Displayed when the parameter IPv6 Activation is enabled.	✓	✓
Assignment mode	Used to select the IPv4 assignment mode: <ul style="list-style-type: none"> • Select DHCP client (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 Configuration mode is set to Static IPv4 address .	✓	✓
Netmask	Used to enter the Ethernet IP netmask address of your network when the parameter IPv4 Configuration mode is set to Static IPv4 address .	✓	✓

Gateway Settings

The following table describes the settings and where they are available.

Parameter	Description	EPC software	Webpages
Assignment mode	<p>The gateway configuration is the same as the IPv4 Configuration mode settings, page 56 and not editable:</p> <ul style="list-style-type: none"> • DHCP (default setting) • Static <p>NOTE: The gateway embeds a DHCP client that receives the IP configuration from the DHCP server.</p>	✓	✓
Gateway	Used to enter manually the gateway (router) IP address when the parameter Gateway settings > Assignment mode is set to Static .	✓	✓

Wi-Fi Communication

Presentation

The EcoStruxure Panel Server supports Wi-Fi infrastructure, that is, the Panel Server can connect to a Wi-Fi router (access point).

By default, Wi-Fi is not active in the Panel Server.

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

- 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.

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 is set on the EcoStruxure Panel Server webpages. Proceed as follows:

1. Access the Panel Server webpages (see detailed topic, page 151).
2. Activate and configure connection to Wi-Fi on the webpage **Settings > Network communication > Wi-Fi**.

General 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.

Parameter	Description
Wi-Fi activation	Used to activate/deactivate Wi-Fi (deactivated by default).
Infrastructure activation	Used to activate the capability to connect to an existing infrastructure (deactivated by default).
Antenna (Universal and Advanced models)	When Wi-Fi is enabled, used to set the type of antenna used: <ul style="list-style-type: none"> • Internal (default setting) • External

Infrastructure Settings

The following parameters are displayed only when the parameter **Infrastructure Activation** is enabled.

Parameter	Description
Connection status	Shows the Panel Server connection status to Wi-Fi network: <ul style="list-style-type: none"> • 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 wireless 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: <ul style="list-style-type: none"> • 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 **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.
IPv6 activation	Used to enable/disable the IPv6 configuration (enabled by default).
IPv6 address	Shows the IPv6 address. Setting not editable. NOTE: Displayed when the parameter IPv6 activation is enabled.
IPv4 Configuration mode	Used to select the IPv4 configuration mode: <ul style="list-style-type: none"> • 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 Configuration mode is set to Static IPv4 address .
Netmask	Used to enter the netmask address of your network when the parameter IPv4 Configuration mode is set to Static IPv4 address . 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.

Gateway Settings

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

Parameter	Description
Gateway assignment mode	The gateway configuration is the same as the IPv4 configuration mode settings, page 58 and not editable: <ul style="list-style-type: none">• DHCP• Static NOTE: The gateway embeds a DHCP client that receives the IP configuration from the DHCP server.
Gateway IPv4 address	Used to enter manually the gateway (router) IP address when the parameter Gateway settings > Assignment mode is set to Static .

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 136).

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.

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 the Panel Server webpages, at **Settings > Network communication > DNS**

DNS Settings

The following table describes the settings and where they are available.

Parameter	Description	EPC software	Webpages
DNS assignment mode	Used to select the DNS server configuration mode: <ul style="list-style-type: none"> • 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 server	Used to enter manually the IPv4 address of the primary DNS server when the parameter DNS configuration mode is set to Static .	✓	✓
Secondary DNS server	Used to enter manually the IPv4 address of the secondary DNS server when the parameter DNS configuration mode is set to Static .	✓	✓

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.

IP Network Services (DPWS)

Presentation

The EcoStruxure Panel Server supports Devices Profile for Web Services (DPWS) protocol for IP network discovery.

Availability

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

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: <ul style="list-style-type: none">• IPv4• IPv6• IPv4 & IPv6 (default setting)
TCP listening port	Used to enter manually the port number (default setting: 5357).

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 76.

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 196 and *Modbus TCP/IP exception codes*, page 199 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 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 and where they are available.

Parameter	Description	EPC software	Webpages
Connection timeout (s)	Used to set the length of time the Panel Server will wait for a remote Modbus TCP/IP device to establish the connection with the Panel Server. Values from 0.1 to 10 seconds (default setting: 2 seconds)	✓	✓
Message timeout (s)	Used to set the length of time the Panel Server will wait 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 1 to 20 seconds (default setting: 3 seconds)	–	✓

For recommendations and more information about setting the message timeout parameter, refer to [Setting Message Timeout for Modbus Client and Server](#), page 205.

Modbus TCP/IP Server

Presentation

Modbus TCP/IP devices connected downstream from the Panel Server can be accessed from an upstream SCADA system.

Availability

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

Setting the Parameters

Modbus TCP/IP server function is set as follows:

- With EcoStruxure Power Commission software
- On the Panel Server webpages, at **Settings > Modbus devices > Network configuration > Modbus TCP server**.

Modbus TCP Server Settings

The following table describes the settings and where they are available.

Parameter	Description	EPC software	Webpages
Message timeout (ms)	<p>In Modbus network configuration, you can set the message timeout period for the Modbus TCP server.</p> <p>Setting used to set the time-to-live of a Modbus request in the Panel Server. Any messages older than this setting will be dropped.</p> <p>Values from 1,000 to 320,000 ms (default setting: 6,000 ms)</p> <p>The value that you set for the Modbus TCP server must meet both following conditions:</p> <ul style="list-style-type: none"> • 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). <p>For recommendations and more information about setting the parameter, refer to Setting Message Timeout for Modbus Client and Server, page 205.</p>	–	✓

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.

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 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 the Panel Server webpages, at **Settings > Wireless devices**

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 and where they are available.

Parameter	Settings	Description	EPC software	Webpages
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: <ul style="list-style-type: none"> 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: <ol style="list-style-type: none"> Select the required channel from the channel list. Click: <ul style="list-style-type: none"> Apply Changes to save the settings. Cancel Changes to revert the settings, as applicable. 	✓	✓
	Channel	Enter the channel number.	✓	✓
	Antenna selection	Used to select the type of IEEE 802.15.4 antenna used in the architecture: <ul style="list-style-type: none"> Internal (Panel Server internal antenna) External (Panel Server external antenna, Advanced model option) Both (internal and external antennas are used with Panel Server 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: <ul style="list-style-type: none"> If Antenna selection is set to Internal or Both, the internal antenna is used therefore level is low (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	✓	✓

Parameter	Settings	Description	EPC software	Webpages
		antenna is not installed within the enclosure.		
Wireless communication	Communication period	<p>It defines the length of time (in seconds) each wireless device (sensor, control, energy related) 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.</p> <p>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. As standard, the Panel Server has a defined default value for each family of wireless devices.</p> <p>The communication period can be adapted as follows, if needed:</p> <ol style="list-style-type: none"> 1. Select the required communication period from the Communication Period list. 2. Apply the selected values. 3. Click: <ul style="list-style-type: none"> • Apply Changes to save the settings. • Cancel Changes to revert the settings, as applicable. 	✓	✓
Wireless device management	Remove all devices	Used to remove all wireless devices connected to the Panel Server.	✓	✓

Settings of Wireless Devices Discovery

The following table describes the settings and where they are available.

Parameter	Settings	Description	EPC software	Webpages
Wireless discovery	Selective list	Used to discover a selective list of wireless devices to be connected to the Panel Server.	✓	✓
	Discovery status	<p>Indicates the status of the device discovery on the wireless network:</p> <ul style="list-style-type: none"> • Idle: device discovery is inactive. • InProgress: device discovery is in progress • Done: device discovery is performed. 	–	✓
Discovered devices	Remove all devices	Identification of the discovered wireless devices with device type, name, and model.	✓	✓

Modbus-SL Communication

Presentation

Panel Server Universal and Advanced 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 198](#) and [Modbus-SL exceptions codes, page 199](#) in appendix.

The Panel Server Modbus serial port can be configured in reverse mode (see [Modbus-SL Reverse Mode, page 73](#)).

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 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 and where they are available.

Parameter	Description	EPC software	Webpages
Modbus mode	Used to select the configuration of Modbus-SL mode: <ul style="list-style-type: none"> • 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 and where they are available.

Parameter	Description	EPC software	Webpages
Activation	Used to enable/disable the Modbus-SL feature (enabled by default).	–	✓
Baud rate (bits per sec)	Used to set the transmission rate: <ul style="list-style-type: none"> • 1200 • 2400 • 4800 • 9600 • 19200 (default setting) • 38400 • 57600 • 115200 	✓	✓
Parity	Used to define the parity bit of the transmitted bytes: <ul style="list-style-type: none"> • 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 (default setting: 5 ms)	–	✓
Frames 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 (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 320,000 ms (default setting: 3,000 ms)	✓	✓
Termination resistor	Used to connect/disconnect the RS485 termination resistor embedded in the Panel Server to help prevent reflection. (Connect by default)	✓	✓
Line polarization 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 and where they are available.

Parameter	Description	EPC software	Webpages
Baud rate (bits per sec)	Used to set the transmission rate: <ul style="list-style-type: none"> • 1200 • 2400 • 4800 • 9600 • 19200 (default setting) • 38400 • 57600 • 115200 	✓	✓
Parity	Used to define the parity bit of the transmitted bytes: <ul style="list-style-type: none"> • 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 (default setting: 5 ms)	–	✓
Frames 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 (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.	–	✓
Termination resistor	Used to connect/disconnect the RS485 termination resistor embedded in the Panel Server to help prevent reflection. (Connect by default)	✓	✓
Serial line polarization	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. Setting 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 320 000 ms (default setting: 6000 ms) The value that you set for the Modbus-SL server must meet both following conditions: <ul style="list-style-type: none"> • 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). 	✓	✓

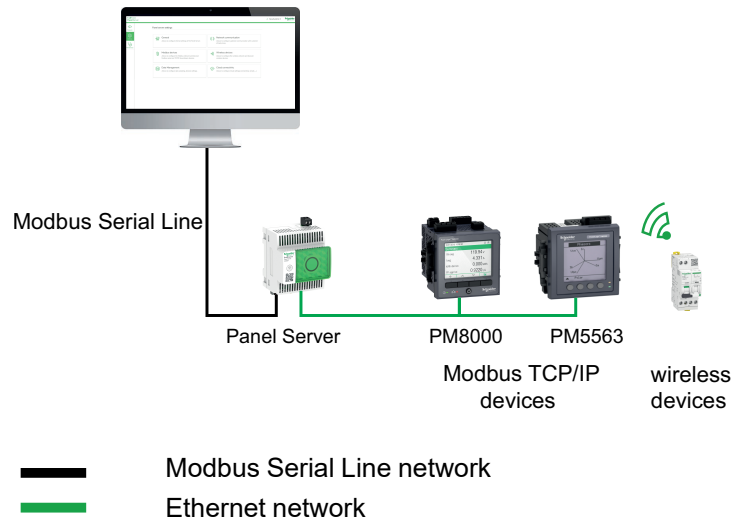
Modbus Discovery Settings

The following table describes the settings and where they are available.

Parameter	Description	EPC software	Webpages
Modbus serial discovery	Used to enter the list of Modbus addresses (1–254) for which the devices must be discovered.	✓ ¹	✓ ²
Discovered devices table	Displays information about each device discovered in the Modbus-SL network: <ul style="list-style-type: none"> • Picture • Device name • Server ID 	✓	✓
Manual addition	Used to manually enter Modbus-SL devices: <ul style="list-style-type: none"> • Enter the physical server ID / Unit ID. A virtual server ID is assigned as part of the process. • Select the device type in the drop-down list. 	–	✓ ³

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:



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

1. When commissioning wireless devices with EcoStruxure Power Commission software, it is recommended to discover the Modbus devices connected to the EcoStruxure Panel Server by using a selective list of addresses.
2. If no addresses are entered, discovery is done for addresses 1 to 10.
3. For detailed information, see addition of Modbus devices, page 170.

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 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 synchronize two I/O Smart Link devices at the same time.

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

NOTE: When commissioning an I/O Smart Link device in the Panel Server webpages at **Settings > Modbus devices**, and configuring the inputs of the channels, for the following I/O contextualization selections, the result displayed for **Meaning of input = 0** and **Meaning of input = 1** should be interpreted as shown in the table below:

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
Motor start	Off	On	Off	Start
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

I/O Smart Link Output Control

▲ 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.

Output control orders can be sent through Panel Server webpages. This feature is used to control non-critical electrical loads.

EcoStruxure Panel Server General Functions

What's in This Part

Modbus Gateway Function.....	76
Examples of Modbus Routing.....	80
Data Publication.....	87
Output and Scheduled Control from Cloud.....	101
Date and Time.....	102
Data Sampling.....	104
Data Logging (Advanced Model).....	107
Home (Advanced Model).....	109
Data Trending (Advanced Model).....	110
Exporting Data Locally (Advanced Model).....	113
Custom Models for Downstream Modbus Devices (Universal and Advanced Models).....	116
Alarms.....	119
Notifications (Advanced Model).....	124
Firmware Update.....	126
User Management.....	127
Digital Inputs (PAS600L, PAS600LWD, PAS800L).....	128
Diagnostics.....	131
Diagnostics Logs.....	134
Backup and Restore Panel Server Configuration.....	136

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 Modbus TCP/IP devices connected to one Panel Server is 128 and includes devices physically connected to the Panel Server and any type of devices 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 Entry, Universal, and Advanced.

Modbus Gateway Function

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*.

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

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 paired IEEE 802.15.4 wireless device. Each time a new wireless device is paired to the Panel Server, the device is automatically assigned a virtual Modbus server ID. The first paired 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 paired. 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 EcoStruxure Power Commission software or 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.

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 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 or on the Panel Server webpages (see **Modbus Discovery** settings, page 73). The virtual server ID must be unique.

EcoStruxure Power Commission software and the Panel Server webpages provide the following information for each device (see addition of Modbus devices, page 170):

- 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 78.

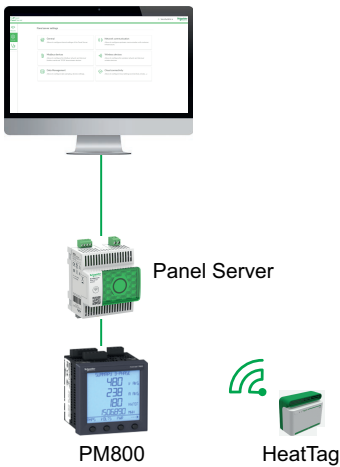
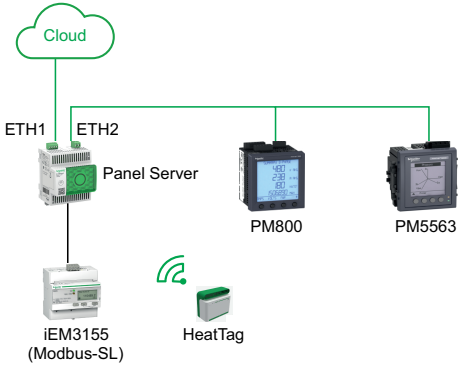
For examples how to use virtual server ID to access data in downstream devices according to the communication architecture, see Examples of Modbus Routing, page 80.

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/ETH2 (not on Entry model)/Wi-Fi) on the Panel Server webpages at **Settings > Network communication > Services > Service activation**.

Do not disable Modbus service on port ETH1, ETH2, or Wi-Fi if the interface is used to connect EcoStruxure Power Commission software 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
<p>Panel Server connected to Panel Server webpages and Modbus and wireless devices</p> 	<p>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.</p>
<p>Panel Server connected to the cloud and in the separated mode to Modbus and wireless devices</p> 	<p>When the Ethernet network is configured in the separated mode, it is recommended to:</p> <ul style="list-style-type: none"> • 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.

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, 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 paired 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.

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 80.

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 77.

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

Availability

This function is available on Panel Server Entry, Universal, and Advanced. The function is available depending on the model.

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

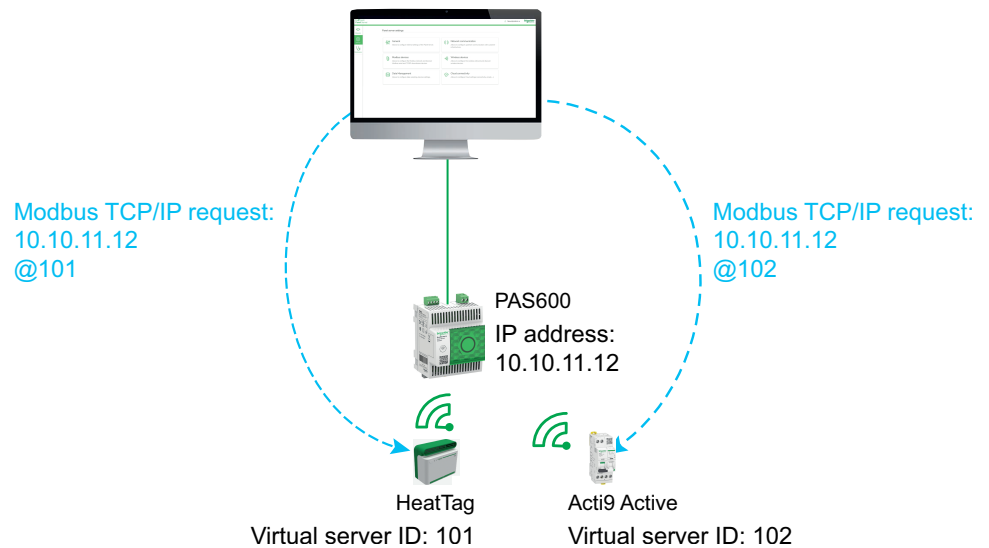
This example presents the Modbus TCP/IP requests for wireless devices.

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.

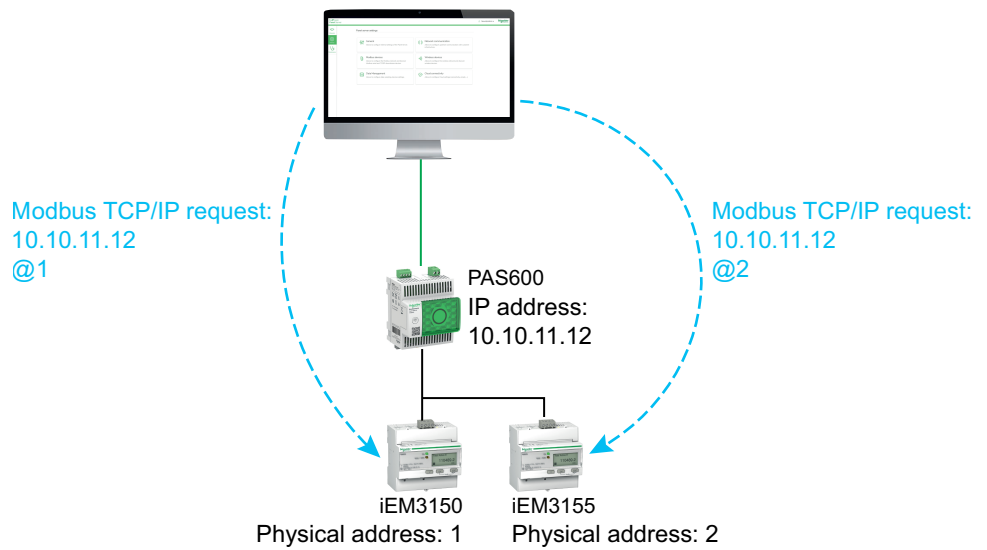
This example presents the Modbus TCP/IP requests for Modbus-SL devices when the serial physical address is used as virtual server ID.

Panel Server with IP address 10.10.11.12 is connected to:

- an iEM3150 with physical address 1, and
- an iEM3155 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.

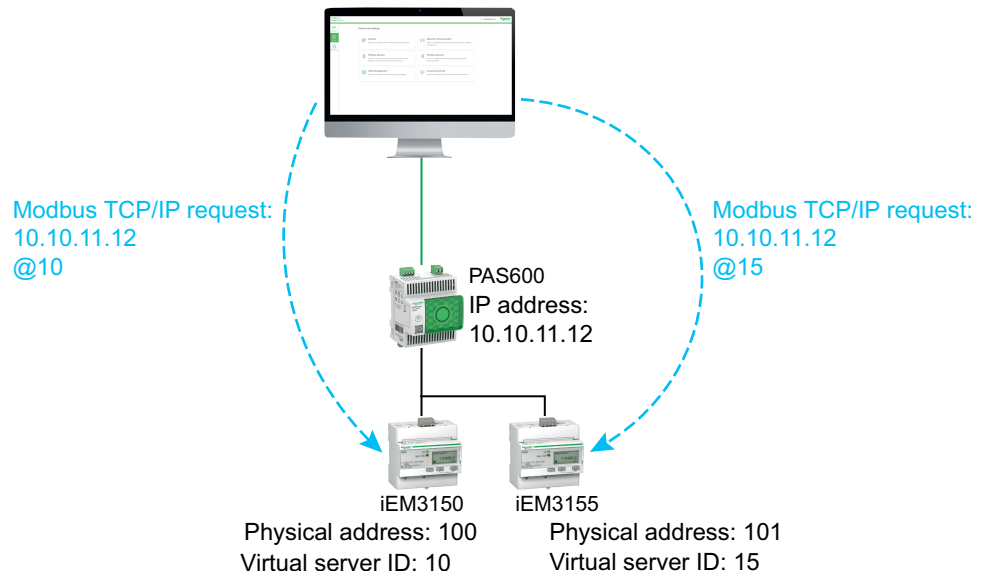
This example presents the Modbus TCP/IP requests when the virtual server ID of Modbus-SL devices is different from the serial physical address.

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

- an iEM3150 with physical address 100 and virtual server ID 10, and
- an iEM3155 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

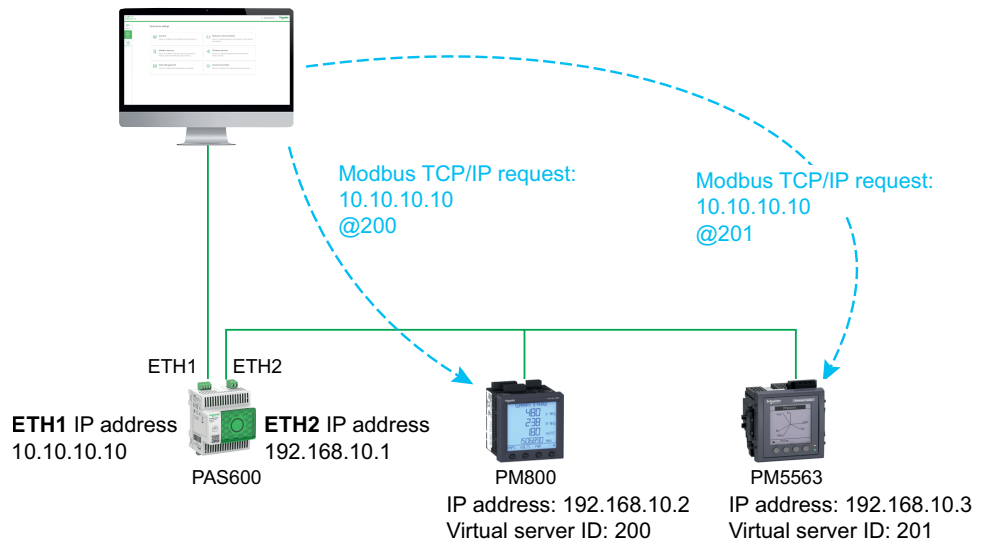
is connected to:

- a PM800 with IP address 192.168.10.2 and virtual server ID 200, and
- a PM5563 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.

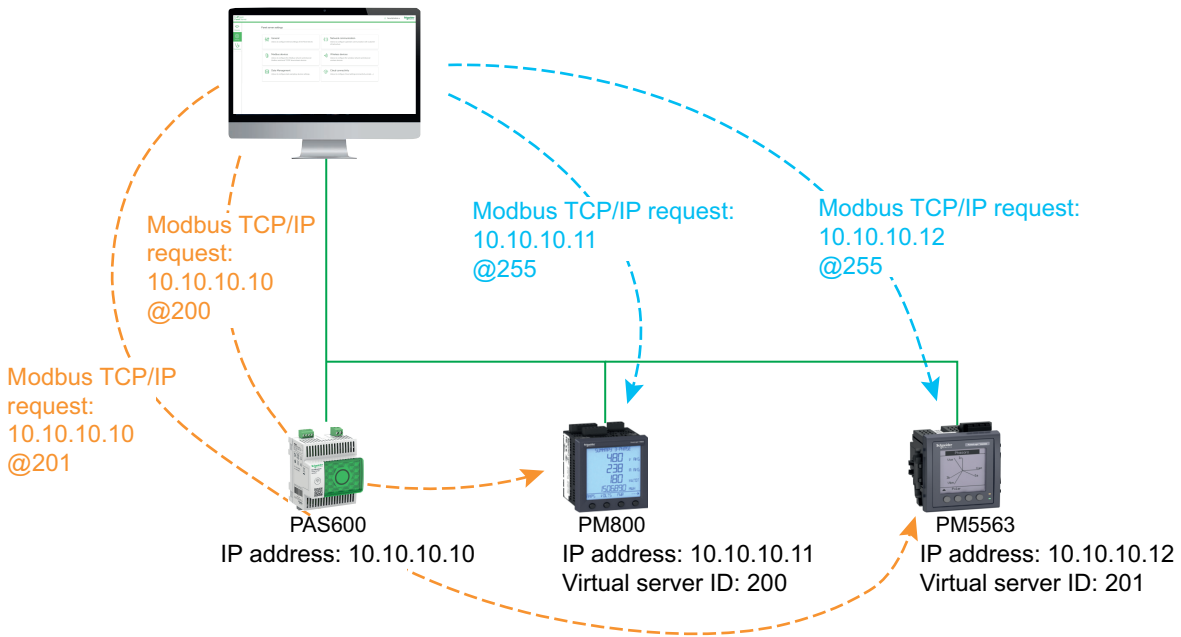
This example presents the Modbus TCP requests for devices in a switched topology.

Panel Server with IP address 10.10.10.10 is connected to:

- a PM800 with IP address 10.10.10.11 and virtual server ID 200, and
- a PM5563 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 171.

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:

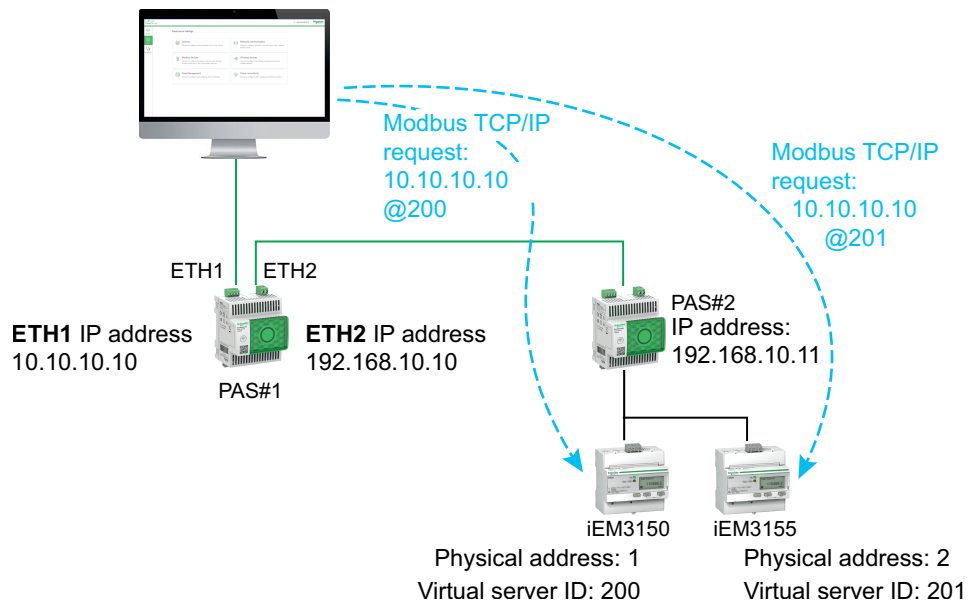
- an iEM3150 with physical address 1, and
- an iEM3155 with physical address 2.

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



Data Publication

What's in This Chapter

Publication on Schneider Electric Cloud	88
Publication on SFTP Server	91
Publication on HTTPS Server.....	94
Publication of Emails for Alarms (Advanced Model).....	97
Publication on SFTP Server and Email Notification for Alarms (Advanced Model).....	99
Publication on HTTPS Server and Email Notification for Alarms (Advanced Model).....	100

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.

Set up [data sampling](#), [page 104](#) 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 one month of sampled data
- Panel Server Advanced: up to three months of sampled data. All previously logged data is retained, up to a maximum of three years of data.

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** (default value) to send the sampled data to the Schneider Electric cloud. See [detailed topic](#), [page 88](#).
- Select **SFTP** to send the sampled data to an SFTP server. See [detailed topic](#), [page 91](#).
- Select **HTTPS** to send the sampled data to an HTTPS server. See [detailed topic](#), [page 94](#).
- Select **Email service for alarms** to send email notifications on active alarms (Panel Server Advanced). See [detailed topic](#), [page 97](#).
- Select **SFTP & Email for alarms** to activate SFTP publication or to combine both services (Panel Server Advanced). See [detailed topic](#), [page 99](#).
- Select **HTTPS & Email for alarms** to activate HTTPS publication or to combine both services (Panel Server Advanced). See [detailed topic](#), [page 100](#).

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, EcoStruxure Facility Expert, EcoStruxure Asset Advisor, and EcoStruxure Resource Advisor.

NOTE: Schneider Electric cloud services and service of publication of emails for alarms, page 97 are mutually exclusive, that is, both features cannot be enabled concurrently.

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 100 alarms, the configuration is rejected.

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.
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 large topology (>250 kB) 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
Cloud applications management	Buttons used to connect to and disconnect from the cloud: <ul style="list-style-type: none"> • Button Connect to connect the Panel Server to the Schneider Electric cloud. • Button Disconnect to disconnect from the Schneider Electric cloud.
Connection status	Shows the Panel Server connection status to the cloud: <ul style="list-style-type: none"> • 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 193). • Connection in progress • Connected
Connection diagnostics	Shows diagnostic of connection to the cloud: <ul style="list-style-type: none"> • 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 192. • 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.
Panel Server Identification	Displays the following information: <ul style="list-style-type: none"> • Serial number: unique identifier of the device • Device code: used for secure claiming of device in EcoStruxure Energy Hub <p>You can copy and paste this information to identify your device in other applications.</p>
Outputs remote control	Enable outputs remote control: click the slider to enable this function. For more information, refer to Output and Scheduled Control from Cloud, page 101.
Topology	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: <ul style="list-style-type: none"> • Last remote configuration status: indicates if the last remote configuration was successful • Last successful remote configuration date
Publication period	The publication period is set by the cloud service and not editable.

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 > Cloud** and click **Connect**.

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, you must publish the topology again.

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, 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 155:
 - Green: valid remote configuration
 - Orange: invalid remote configuration

Disconnecting from Cloud Services

To temporarily disconnect Panel Server from Schneider Electric cloud:

1. Click **Disconnect**.
2. Wait until **Connection Status** indicates **Not connected**.

Publication on SFTP Server

Presentation

Panel Server provides connection to an SFTP server.

If SFTP publication is active:

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

When SFTP function is active, the data publication on cloud 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, at **Settings > Publication > Publication method > SFTP**.

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, <code>mysftpserver.mydomain.com</code> .
	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 <code>/home/user/</code> is the default directory for the SFTP server, then the path configured with <code>/mySFTPPath</code> will publish on <code>/home/user/mySFTPPath</code> .
	User ID	Used to type the username for SFTP server access.
	Authentication method	Connection to the SFTP server is done with either user name and password or user name and SSH key in PEM (Privacy Enhanced Mail) format.
	Password	Used to type the password for SFTP server access.
	Test connection	Button used to test connection to the SFTP server.
Publication settings	Publication format	Used to select the exported file format: <ul style="list-style-type: none"> • JSON (for details, page 93) • CSV (for details, page 92)
	Publication period	Used to select the publication frequency to the SFTP server (default setting: 1h).
	Start	Button used to activate data publication to the SFTP server.

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 **Settings > Network communication > Proxy**, click **SFTP proxy** and enter the required information, page 62.
3. In the **Settings > Data publication** webpage, select **SFTP** as **Publication method**.

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 name and password or user name 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**.
5. Click **Test connection**. The list of SSH key exchanges and ciphers supported by the Panel Server is available in Appendix E, page 218.

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 sampled data of devices, related to the selected sampling period, is published to SFTP, in the CSV file format, page 92 or JSON format, page 93. A maximum of one month 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.

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.

Disconnecting from Publishing Services

To disconnect Panel Server from the SFTP server, click **Stop**.

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

File Format of CSV Publication

One .csv file is produced per downstream device and includes measurements configured with the same sampling period.

The name of the CSV files that are exported follows the naming convention *ReducedID_DeviceName_DateTime.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*.
- 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_20221104084830994.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 **20221104084830994**, which means that the file was published on November 4, 2022 at 8:48:30.994.

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 Publication File Formats*, page 215.

File Format of JSON Publication

One .json file is produced, which includes measurements of multiple downstream devices configured with the same sampling period.

The name of the JSON file that is exported follows the naming convention *DateTime.json* where *DateTime* is the time stamp corresponding to when the file was published, expressed down to the millisecond in the format *YYYYMMDDhhmmssSSS*.

For an example of a .json file, see *Appendix D SFTP Publication File Formats*, page 215.

Publication on HTTPS Server

Presentation

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

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

Availability

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

Setting the Parameters

Publishing function is set on the EcoStruxure Panel Server webpages, at **Settings > Data Publication > Publication method > HTTPS**.

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, <code>myHTTPSServer.mydomain.com</code> .
	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 <code>/home/user/</code> is the default directory for the HTTPS server, then the path configured with <code>/myHTTPSPath</code> will publish on <code>/home/user/myHTTPSPath</code> .
	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 field name is <code>datafile1</code> . The field name is necessary to communicate with the HTTPS server.
	Connection method	Radio button used to enable ID authentication.
	Username	Used to type the user name for HTTPS server access.
	Password	Used to type the password for HTTPS server access.
	Test connection	Button used to test the connection to the HTTPS server.
Publication settings	Publication format	Used to select the exported file format: <ul style="list-style-type: none"> • JSON (for details, page 96) • CSV (for details, page 95)
	Publication period	Used to select the publication frequency to the HTTPS server (default setting: 1h).
	Start	Button used to activate data publication to the HTTPS server.

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 62.
3. In the **Settings > Data publication** webpage, select **HTTPS** as **Publication method**.

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.

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 219). 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 sampled data of devices, related to the selected sampling period, is published to HTTPS, in the **CSV file format**, page 95 or **JSON format**, page 96. A maximum of one month 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.

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.

Disconnecting from Publishing Services

To disconnect Panel Server from the HTTPS server, click **Stop**.

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

File Format of CSV Publication

One .csv file is produced per downstream device and includes measurements configured with the same sampling period.

The name of the CSV files that are exported follows the naming convention *ReducedID_DeviceName_DateTime.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.
- *Date Time* is the time stamp corresponding to when the file was published, expressed down to the millisecond in the format *YYYYMMDDhhmmssSSS*.
- 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_20221104084830994.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.

- *Date Time* is **20221104084830994**, which means that the file was published on November 4, 2022 at 8:48:30.994.

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 215.

File Format of JSON Publication

One .json file is produced, which includes measurements of multiple downstream devices configured with the same sampling period.

The name of the JSON file that is exported follows the naming convention *DateTime.json* where *Date Time* is the time stamp corresponding to when the file was published, expressed down to the millisecond in the format *YYYYMMDDhhmmssSSS*.

For an example of a .json file, see *Appendix D SFTP and HTTPS Publication File Formats*, page 215.

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 97.

NOTE: Service of publication of emails for alarms and Schneider Electric cloud services, page 88 are mutually exclusive, that is, both features cannot be enabled concurrently.

2. Create the list of recipients, page 97.
3. Select the alarms that trigger an email notification when activated, page 119.
4. Send email notification, page 98.

If the Panel Server Advanced does not succeed in connecting to the cloud services, see Troubleshooting, page 193.

Availability

This function is available on Panel Server Advanced.

Setting the Parameters

Publishing function is set on the EcoStruxure Panel Server webpages, at **Settings > 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 from **Not connected** to **Connected**.

When email notification is activated, alarms are displayed in the webpages.

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 name and 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

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.

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.

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 91
- Publication of Emails for Alarms, page 97

Availability

This function is available on Panel Server Advanced.

Setting the Parameters

Publishing function is set on the EcoStruxure Panel Server webpages, at **Settings > 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 94](#)
- [Publication of Emails for Alarms, page 97](#)

Output and Scheduled Control 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.

Output remote control allows you to manage non-critical electrical loads remotely when the EcoStruxure Panel Server is connected to the Schneider Electric cloud service.

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. See *Configuration of PowerTag Control Devices Through Webpages*, page 182 for more information about configuring contactor with feedback loop mode and impulse relay mode.
- 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 > Outputs remote control**, the slider is green.
- Send real-time status updates of the monitored device to the Schneider Electric cloud.

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. In **Publication method**, select **Schneider cloud services**.
2. In **Output remote control**, click the slider to enable remote control of outputs.
3. Save the settings.
4. Read the safety message popup and click **Confirm** or **Cancel**.

NOTE: The output remote control function is supported for PowerTag C IO devices only.

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.

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 the Panel Server webpages, at **Settings > General > Date and time**

General Settings

The following table describes the settings and where they are available.

Parameter	Description	EPC software	Webpages
Synchronization mode	<p>Used to select the date and time configuration mode of the Panel Server:</p> <ul style="list-style-type: none"> • Select Manual to set the date and time manually in the dedicated fields. <p>NOTE: Manual setting is available only if the Panel Server is not set up for publication by Schneider Electric cloud services, or for publication by email. See <i>Data Publication</i>, page 87.</p> <ul style="list-style-type: none"> • Select NTP to synchronize the date and time automatically with an external NTP server. • Select Cloud (default setting) to synchronize the date and time automatically with an NTP server hosted by Schneider Electric cloud services, page 88. 	✓	✓

NTP Server 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 and where they are available.

Parameter	Description	EPC software	Webpages
Mode	Used to select the synchronization mode: <ul style="list-style-type: none"> 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. <p>NOTE: To use DHCP mode, the network settings must be set to DHCP (see related topic, page 56).</p>	✓	✓
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. <ul style="list-style-type: none"> 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 .	✓	✓
Secondary server address	Used to enter the secondary NTP server address when the parameter NTP settings > Mode is set to Static .	✓	✓

Setting Date and Time Manually

Panel Server date and time can be set manually:

- With EcoStruxure Power Commission software
 - 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.
- On the Panel Server webpages, at **Settings > General > Date & Time > General settings > Synchro mode > Manual**
 - By user-initiated synchronization with date and time of the PC.

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

Parameter	Description	EPC software	Webpages
Date & Time	Used to set the date by using a date picker. Set time in UTC +00:00.	✓	✓

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.

Availability

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

Setting the Parameters

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

NOTE: In the case of manual configuration, set the sampling frequency and measurements individually, page 104 before activating data sampling.

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.

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

For Panel Server Advanced, the data is logged in the Panel Server, page 107.

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. For each device, click the device name.
2. Click **Data**.
3. Select or deselect sampling for every measurement with the **Sampling** checkbox.

4. Select the sampling period for the measurement. Refer to [Changing the Data Sampling Frequency](#), page 105, if relevant.
5. Click **Save** to apply changes.

IMPORTANT: Applying the changes may take up to a few minutes. during which the following pages and functions are not accessible:

- Home page dashboard (Advanced)
- Trending - device and aggregated data views (Advanced)
- Custom models - custom model updates
- CSV export
- Backup and restore
- Data sampling
- Measurement sampling

NOTE: The default sampling configuration for every device comprises of the most commonly used data for each device type.

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 100 individual alarms for monitoring and sending email notifications

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	Number of measurements	Sampling period (min)	Total number of sampled data points	Samples per minute	Number of alarms	Valid configuration
30	30	15	900	60	90	Yes - < 5,000 simultaneous measurements, < 500 samples per minute and < 100 alarms
30	30	15	900	60	150	No - number of alarms > 100
30	170	15	5,100	340	90	No - total number of simultaneous measurements > 5,000
30	30	1	900	900	90	No - samples per minute > 500

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
<p>HAZARD OF LOSS OF DATA</p> <p>Reducing the sampling frequency results in the permanent loss of intermediate historized data points.</p> <p>Perform a data log export before reducing the frequency to avoid losing data.</p> <p>Failure to follow these instructions can result in equipment damage.</p>

For more information about exporting data, refer to [Exporting Data Locally](#), page 113.

- Increasing the frequency (for example, changing the period from 10 minutes to 5 minutes): Data points for which no historical data exists are duplicated from existing historical data (data points on either side), which may create non-linear trends where linear trends are expected.

Data Sampling Activation and Reset

The following table describes the settings.

Parameter	Description
Activation mode	Used to activate/deactivate data sampling by the Panel Server. <ul style="list-style-type: none"> • Click button Activate sampling to activate the function. • Click button Deactivate sampling to deactivate the function.
Flush data	Used to delete all sampling data. To delete data: <ol style="list-style-type: none"> 1. Deactivate data. 2. Click button Flush data. <p>NOTE: During the operation, which may take up to a few minutes, the following pages and functions are not accessible:</p> <ul style="list-style-type: none"> • Home page dashboard • Trending - device and aggregated data views • Custom models - custom model updates • CSV export • Backup and restore • Data sampling • Measurement sampling 3. Confirm the data flush request by clicking Confirm in the popup message

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 108.

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 104.

Consider the maximum number of data points that can be stored and the recommended sampling limits, page 105 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 105.

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):

$788,400,000 / \text{Ndp/m} / 525,950 = \text{number of years of data logging held in logging memory}$

The following table shows some examples:

Number of devices	Number of measurements	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	$788,400,000/60/525,950$	3.1

Home (Advanced Model)

Presentation

The Panel Server Advanced Home menu allows you to see an analytical view of energy consumption.

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).
From	Used to select the start date for each period: <ol style="list-style-type: none"> Select the current period (Period 1) start date. Select the previous period (Period 2) start date. <p>NOTE: The default start date depends on the period selected:</p> <ul style="list-style-type: none"> 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 <p>NOTE: The default period is one day and the start date is yesterday (D-1).</p>
To	Used to select the period end date.

By Usage Display

A pie-chart shows the distribution of the top five consumers from devices where usage has been defined.

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 data sampling is activated. For more information, see [Data Sampling](#), page 104.

You can view data trends in two 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.
- **Aggregated view** provides a data centric view. It displays aggregated data of energy consumption based on a commodity and/or usage, without reference to specific devices.

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 differ from the raw data values in the [CSV file exported to your PC](#), page 113.

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, energy, reactive energy) or aggregated data
- Line graph: used to display continuous data (for example, temperature, apparent energy)

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.

NOTE: A maximum of 16 curves can be displayed on a line graph.

Availability

This function is available on Panel Server Advanced webpages, at **Trending**.

Aggregation Principle

The trending figures in **Aggregated view** are the result of an aggregation algorithm used to calculate the consumption of energy. Only Active energy is calculated.

In order to aggregate the consumed energy of the loads, all usages are considered in the aggregation except:

- Main/Incomer
- Sub/Head of group
- Total

Any device configured with one of these usages is not displayed in **Aggregated view** or in the **Home** page.

Data Trending Device View Settings

To customize data displayed in **Device view**:

1. Select the device(s) you want to view.
2. Select the data you want to view. Only two different types of data can be displayed together.
3. Activate compare mode by clicking the slider icon if you want to compare periods.
4. Select the period of time you want to display.

The following table describes the settings.

Parameter	Description
Devices	Used to select one or several devices.
Data	Used to select the data to be used for the graph. For different types of data with continuous measurements (for example, voltage and current).
Compare mode	<ul style="list-style-type: none"> • Disable to get the graph on a single period. • Enable to get comparing data from two periods of same duration.
Period	When the parameter Compare mode is enabled, used to select the period duration (One day, One week, 4 weeks).
From	<p>When the parameter Compare mode is disabled, used to select the period start date.</p> <p>NOTE: The default period is one day and the start date is yesterday (D-1).</p> <p>When the parameter Compare mode is enabled, used to select the start date for each period:</p> <ol style="list-style-type: none"> 1. Select the current period (Period 1) start date. 2. Select the previous period (Period 2) start date. <p>NOTE: The default start date depends on the period selected:</p> <ul style="list-style-type: none"> • 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
To	<p>When the parameter Compare mode is disabled, used to select the period end date.</p> <p>NOTE: The default end date is today (D).</p> <p>NOTE: When the parameter Compare mode is enabled, the end date is defined automatically according to the selected start date and period.</p>
Interval	<p>When the parameter Compare mode is disabled, used to select the interval of data displayed by hour (H), day (D), or Month.</p> <p>NOTE: Week is only applicable for integrated data, for example, to display Energy consumption over a period of month displayed as energy consumed by day.</p>
Clear filters	Used to erase any selection of devices, data or periods of time previously selected.

Data Trending Aggregated View Settings

To customize data displayed in **Aggregated view**:

1. Select the commodity you want to view. Only one commodity can be selected.
2. Select the usage(s) you want to view.
3. Activate compare mode by clicking the slider icon if you want to compare periods.

NOTE: When compare mode is activated, a maximum of 16 usages can be displayed.

4. Select the period of time you want to display.

The following table describes the settings.

Parameter	Description
Commodity	Used to select one or several commodities from a drop-down list of values.
Usage	Used to select one or several or all usages.
Compare mode	<ul style="list-style-type: none"> • Disable to get the graph on a single period. • Enable to get comparing data from two periods of same duration.
Period	When the parameter Compare mode is enabled, used to select the period duration (One day, One week, 4 weeks).
From	<p>When the parameter Compare mode is disabled, used to select the period start date.</p> <p>NOTE: The default period is one day and the start date is yesterday (D-1).</p> <p>When the parameter Compare mode is enabled, used to select the start date for each period:.</p> <ol style="list-style-type: none"> 1. Select the current period (Period 1) start date. 2. Select the previous period (Period 2) start date. <p>NOTE: The default start date depends on the period selected:</p> <ul style="list-style-type: none"> • 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
To	<p>When the parameter Compare mode is disabled, used to select the period end date.</p> <p>NOTE: The default end date is today (D).</p> <p>NOTE: When the parameter Compare mode is enabled, the end date is defined automatically according to the selected start date and period.</p>
Interval	<p>When the parameter Compare mode is disabled, used to select the interval of data displayed by hour (H), day (D), or Month.</p> <p>NOTE: Week is only applicable for integrated data, for example, to display Energy consumption over a period of month displayed as energy consumed by day.</p>
Clear filters	Used to erase any selection of devices, data or periods of time previously selected.

Exporting Data Locally (Advanced Model)

Presentation

The Panel Server Advanced can export data measured on the connected devices and logged through data sampling, page 104. 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 105).
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 136), you must first reset the Panel Server to factory settings (see [procedure](#), page 143).

When the Panel Server is connected to Schneider Electric cloud services, data logged on Panel Server is controlled by the cloud configuration. When a new cloud configuration is received by the Panel Server, data previously logged in the Panel Server is lost.

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 selection	Used to select one of the following from which to export sample data: <ul style="list-style-type: none"> • One device • All devices <p>NOTE: To export data from several devices, consider performing multiple single device exports to improve readability. Select one device and click Export data to generate the .csv file for the selected device. Repeat for each device.</p>

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 2022	July, 29 2023	527,040	527,040
Current B	1	July, 28 2022	July, 29 2023	527,040	527,040
Current C	1	July, 28 2022	July, 29 2023	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 `DD/MM/YYYY HH:MM UTC` (Coordinated Universal Time).

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	<code>modbus:2_mb_PkWD, modbus:1_mb_PFTtI</code>
2	<i>Device Name</i>	Customer specified device name for each of the columns	<code>myPM5560, myPM8000</code>
3	<i>Device Type</i>	Device type defined by the Panel Server for each of the columns	<code>PM5560, PM8000</code>
4	<i>Measurement Name</i>	Data name for each of the columns	<code>Total Demand Max Active Power, Total Rms Power Factor</code>
5	<i>Measurement Unit</i>	Unit of the data for each of the columns	<code>W</code>
6 and more	<i>DD/MM/YYYY HH:MM</i>	Logged data	<code>02/10/2022 20:20, 8880.13, -1</code>

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:

1. IOTBD-4242_data-export_20220308 (8).csv

File Origin	Delimiter	Data Type Detection
1252: Western European (Windows)	Semicolon	Based on first 200 rows

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:

1. IOTBD-4242_data-export_20220308 (8).csv

File Origin	Delimiter	Data Type Detection
65001: Unicode (UTF-8)	Semicolon	Based on first 200 rows

Column1	Column2	Column3	Column4	Column5	Column6	Column7
sep=						

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
2022/06/08 00:00:00	0	nan	399.366
2022/06/08 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.

Custom Models for Downstream Modbus Devices (Universal and Advanced Models)

Presentation

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 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.

New and modified custom models are imported in the Panel Server by using the Panel Server webpages. To connect a new Modbus device or to automatically discover Modbus devices, see [Addition and Removal of Modbus Devices](#), page 170.

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.

The custom model contains measurements and alarms.

The custom device model must contain the following facets:

- modelingInformation
- productIdentification
- measure
- modbusMapping
- modbusDataModel

The custom model cannot be imported into the Panel Server webpages if it does not follow these rules.

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 from 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 and exported in a zip file, from the Panel Server webpages, select **Settings > Modbus Devices > Custom models**, and follow this procedure:

1. Click **Import**. You can import:
 - A new custom model. This is a custom model which is not currently imported to the Panel Server.
 - A modified custom model. This is a modification of a custom model which is already imported and used by connected Modbus devices.
2. Select a custom device model stored locally in a zip file.

The zip file can contain both new and modified custom models. You can have a maximum of two different versions with the same custom model name. Only one version is used by Modbus devices.

NOTE: An error message is displayed if the custom model does not comply with the syntax rules (see [Creating a Custom Model, page 116](#)).


When the custom model is successfully imported, it is listed in the custom models table.

A new custom model is automatically instantiated so that new Modbus devices can be added using that custom model.

For modified custom models, the new version is available for use in the custom models table. It is not automatically instantiated. Perform an update to apply the new version to selected Modbus devices. See the following table for more information.

Custom Models Table

The custom models table displays the following information and allows you to perform version updates, and delete and export custom models:

Column	Description
Model name	Name of imported custom model.
Model version	Current version of the custom model, used by associated Modbus devices.
Available version	An alternative version of the custom model available to be applied on associated Modbus devices.
Associated devices	The number of Modbus devices associated with the custom model. This number is updated when new Modbus devices are discovered manually or automatically.
 Contextual menu	<p>Click this icon to open a contextual menu. The items displayed depend on the device:</p> <ul style="list-style-type: none"> Update model: Click to update the model to the available version. <p>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 clicking the Update icon again.</p> Export model: Click to export a custom model to a zip file. Remove model: Click to delete a previously imported device.

Supported Functions

Modbus functions are described in the appendix:

- Modbus TCP/IP functions, page 196
- Modbus-SL functions, page 198

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**

Alarms

What's in This Chapter

Communication Loss	121
Voltage Loss	122
Overcurrent at Voltage Loss	122
80% of Nominal Current.....	123
50% of Nominal Current.....	123
45% of Nominal Current.....	123
Zero Current	123
Undervoltage (80%)	123
Overvoltage (120%)	123

▲ WARNING

EQUIPMENT INCOMPATIBILITY 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 Alarms (All Models)

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.

NOTE: For devices associated with custom device models, active alarms are not displayed by default and alarms need to be selected manually, page 120. Check if your device is associated with a custom device model, page 118.

Alarms are defined by severity:

- High severity
- Medium severity
- Low severity

For information about identifying alarm severity, refer to **Alarm Icons**, page 158.

Publishing Alarms

Active alarms can be published by the following methods, depending on the data publication method selected, page 87:

- 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 97, email notifications for selected alarms, page 120 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 124

Selecting Alarms for Publication (Advanced Model)

For each device connected to the Panel Server Advanced, you can enable and/or disable the publication of alarms issued in the case of electrical events or communication loss. By default, publication of alarms is disabled.

A maximum of 100 alarms can be enabled concurrently.

Alarms to be published when they become active can be enabled individually for each device as follows.

1. Click the device name on the Panel Server webpages, at **Settings > Data management**.
2. Click **Alarms**.
3. Enable/disable an alarm with the **Enable alarm** checkbox.

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

Alarms

The complete list of alarms is as follows:

Alarm severity	Alarm description
High-severity alarms	Capacitor abnormal cosphi alarm
	Capacitor broken step alarm
	Capacitor hunting alarm
	Capacitor low current alarm
	Capacitor max cycles and count step alarm
	Capacitor over current alarm
	Capacitor overload alarm
	Capacitor over temperature alarm
	Capacitor step power loss alarm
	Capacitor too high THDV alarm
	Capacitor voltage tolerance alarm
	Maximum operating time alarm
	Circuit breaker fault trip alarm
	Circuit breaker opened alarm
	Circuit breaker trip alarm
	Current transformer supervision alarm
	Device replacement alarm
	Voltage loss alarm
	Fan error alarm
	Ground-fault alarm
	HeatTag alarm
	Falling edge on input alarm
	Rising edge on input alarm
	Instantaneous overcurrent trip alarm
	Integrated instantaneous overcurrent trip alarm
	Internal cause trip alarm
	Long-time protection trip alarm
	Overcurrent when voltage loss alarm
	Overvoltage alarm
	Overvoltage trip alarm

Alarm severity	Alarm description
	Parallel arc fault detection protection trip alarm
	Serial arc fault detection protection trip alarm
	SF6 alarm
	Short-time protection trip alarm
	Tripping chain malfunctioning trip alarm
	Internal trip unit malfunctioning alarm
	Undervoltage alarm
	Voltage transformer supervision alarm
	Zero current alarm
Medium-severity alarms	Battery low alarm
	ERMS alarm
	Trip test not performed alarm
Low-severity alarms	Battery alarm
	Earth-leakage pre-alarm
	Ground-fault pre-alarm
	Long-time overcurrent pre-alarm
	45% rated current alarm
	50% rated current alarm
	80% rated current alarm
	Overcurrent pre-alarm
	Overvoltage pre alarm
	Test pushbutton trip alarm

NOTE:

- 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**.

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 wireless device.

The communication loss happens if the gateway has not received packets for a period of time equal to 6 times the communication period of the device.

The alarm will automatically disappear 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 alarm 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 alarm 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).

Notifications (Advanced Model)

Presentation

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.

The list of notifications displays the following information for each alarm:

- Date of alarm
- Severity icon
- Name of device which triggered alarm
- Alarm name
- Status of alarm

Availability

This function is available on Panel Server Advanced webpages, at **Notifications**.

Display Settings




The time period of alarms notifications to display can be selected from a list of options:




- Last 24 hrs
- Last 7 days
- 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.

Icon	Description
	Medium-severity alarm. Disappearance.
	Low-severity alarm. Appearance.
	Low-severity alarm. Disappearance.

Firmware Update

Presentation

Update the Panel Server to the latest version to obtain the latest features and keep up-to-date with security patches.

Use the latest version of EcoStruxure Power Commission to update your product to the latest available version. It is also possible to perform a firmware update using the embedded webpages.

All firmware designed for the Panel Server is signed using the Schneider Electric public key infrastructure to provide integrity and authenticity of the firmware running on the Panel Server.

For more information about Panel Server firmware versions, 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*

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 the Panel Server webpages at **Settings > General**

The latest security patch is also available on the EcoStruxure Panel Server webpages. It is the lowest firmware revision that the Panel Server can be downgraded to, without removing currently installed security patches.

Updating the Firmware

To update Panel Server firmware, use one of the following:

- EcoStruxure Power Commission software (recommended)
- 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*

User Management

Presentation

The default user account has administrator rights such as reading and changing the product configuration, pairing or unpairing wireless devices, accessing system logs. The user name of the user account is **SecurityAdmin**.

Availability

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

Changing the User Account Password

The user account password can be changed as follows:

- With EcoStruxure Power Commission software
- On the home page of Panel Server webpages.
 1. Click the arrow next to the user 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 incorporates password requirements.

A password must conform to the following rules:

- 6 to 32 characters
- At least one character in uppercase
- At least one character in lowercase
- Must not contain special characters other than: ! " # \$ % & ' () * + - , . ; : / ~ < > = ? @ [] \ ^ _ ` { } |
- The space character is permitted

Password Lockout

After 10 invalid attempts to login to the EcoStruxure Panel Server, the user account is locked out.

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

The user account is locked for 60 minutes each time there are 5 more invalid attempts.

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

Digital Inputs (PAS600L, PAS600LWD, PAS800L)

Presentation

The two embedded digital inputs on Panel Server Universal PAS600L and Advanced PAS800L are used to monitor the state of an external contact or as a pulse counter.

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 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.

Examples:

- If each pulse delivered by an active energy meter corresponds to 10 kWh, and the pulse unit is set to Wh, the pulse weight must be set to 10,000 (Wh).
- If each pulse delivered by a volume meter corresponds to 125 liters, and the pulse unit is set to m³, the pulse weight must be set to 0.125 m³.
- If each pulse delivered by a volume meter corresponds to 1 gallon, and the pulse unit is set to m³, the pulse weight must be set to 0.003785 m³.

Setting the Parameters

The digital inputs are set as follows:

- With EcoStruxure Power Commission software
- On the Panel Server webpages, at **Settings > Embedded Input Management**

Digital Input Settings

The following table describes the settings of **Embedded input 1 (DI01)** and **Embedded input 2 (DI02)** digital inputs.

Parameter	Description
Type	Used to select the type of each digital input (Embedded input 1 (DI01) / Embedded input 2 (DI02)): <ul style="list-style-type: none"> • Not connected • Standard I/O • Pulse counter

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**:

Parameter	Description
Name	Enter the input name.
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.
Meaning of status	Enter the label for the threshold: <ul style="list-style-type: none"> • Meaning of status when Input is high. • Meaning of status when Input is low.

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**:

Parameter	Description
Name	Enter the input name of the device.
Label	Enter the input label as per the name plate in the network.
Type	Type of digital input NOTE: Setting not editable.
Consumption meter elements	Select either a meter element or Custom in the pre-defined list. NOTE: If a meter element is selected, the consumption unit, flow element, and flow unit are displayed.
Consumption meter element name	Enter the name of the custom meter element. NOTE: Displayed when Custom is selected.
Consumption unit	Enter the consumption unit of the meter element. NOTE: Displayed when Custom is selected.
Custom flow element name	Enter the name of the flow the meter element is intended for. NOTE: Displayed when Custom is selected.
Custom flow unit name	Enter the unit of the meter element flow (calculated on a per hour basis). NOTE: Displayed when Custom is selected.
Pulse weight	Enter the pulse weight to be calculated according to the characteristics of the pulses delivered by the meter.

Parameter	Description
Preset meter consumption value	Set a value to the consumption meter element if any, taking into account the pulse weight value.
Commodity	Select the commodity type in the list, as contextualization data.
Usage	Select the commodity usage in the list, as contextualization data.

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 > Devices communication**, device diagnostics:
 - Panel Server, page 131
 - Modbus Devices, page 132
 - Wireless Devices, page 132
- At **Maintenance > System monitoring**, system diagnostics, page 133

EcoStruxure Panel Server Diagnostics

Parameter	Description
Ethernet information	Ethernet information switched port <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Number of active connections • Maximum number of connections allowed • Maximum number of simultaneous connections occurred

Parameter	Description
	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Received messages Transmitted messages Protocol errors Reset counters button allows you to reset the counters to zero.
Wireless (802.15.4) identification⁴	Displays identification of IEEE 802.15.4 wireless network: <ul style="list-style-type: none"> RF-id Personal Area Network (PAN) identifier Extended PAN identifier Network address
Wireless (802.15.4) network status⁴	Displays status of the IEEE 802.15.4 wireless network <ul style="list-style-type: none"> Network status

Modbus Devices Diagnostics

Parameter	Description
Modbus information	Displays identification and diagnostics counters for Modbus devices: <ul style="list-style-type: none"> Server identifier historical data (1–254)⁵ 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.
Internal temperature⁵	Displays temperature records for Modbus devices: <ul style="list-style-type: none"> Current temperature Minimum temperature Maximum temperature

Wireless Devices Diagnostics

Parameter	Description
Wireless (802.15.4) identification⁵	Displays identification of the wireless network: <ul style="list-style-type: none"> Address PAN identifier Extended PAN identifier⁵ Network address⁵
Modbus identification⁵	Displays Modbus identification: <ul style="list-style-type: none"> Virtual server identifier (1–254) (if virtualization of device is supported).

4. Depending on the model

5. Depending on device.

Parameter	Description
Wireless network indicator ⁶ For more information, see Appendix C, page 214.	Displays connection information of the wireless devices: <ul style="list-style-type: none"> • Signal quality level • Device indicator <ul style="list-style-type: none"> ◦ Device received signal strength indicator (RSSI)⁶ ◦ Device link quality indicator (LQI)⁶ ◦ Device packet error rate (PER)⁶ • Panel Server indicator <ul style="list-style-type: none"> ◦ Device received signal strength indicator (RSSI) ◦ Device link quality indicator (LQI) ◦ Device packet error rate (PER) • Link indicator <ul style="list-style-type: none"> ◦ Device received signal strength indicator (RSSI) ◦ Device link quality indicator (LQI) ◦ Device packet error rate (PER)
Status	Battery information ⁶ Displays power information of the wireless devices: <ul style="list-style-type: none"> • Power source • Power source backup • Battery voltage • Battery percentage remaining
	Internal temperature ⁶ Displays temperature records of the wireless devices: <ul style="list-style-type: none"> • Current temperature⁶ • Minimum temperature • Maximum temperature

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: <ul style="list-style-type: none"> • Nominal • Degraded
Global performance	Displays Panel Server performances: <ul style="list-style-type: none"> • CPU usage (in %) • Memory usage (in %)

6. Depending on device.

Diagnostics Logs

Presentation

The EcoStruxure 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**.

Exporting All Logs

In **Collecting all logs** click **Export all logs** to export a .zip file containing all logs (audit, diagnostic and system) to your PC.

Logs Configuration Settings

The logs 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

To change the level of a log, proceed as follows:

1. Select a log level in **Global log level**.

IMPORTANT: Exporting **Debug** logs 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 **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 limited logs**.
3. Wait until the .zip file is downloaded on your PC.
4. Unzip the .zip file to access the detailed logs.

Backup and Restore Panel Server Configuration

Presentation

At any moment after commissioning, 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, or the same Panel Server.

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 S-L, 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:

- Permanent deactivation of wireless networks, page 60
- Logs including diagnostics counters, page 131 and diagnostics logs, page 134
- Alarms, page 119
- Sampled data, page 104
- 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 the EcoStruxure Panel Server webpages, at **Maintenance > Backup & restore**

Panel Server Configuration Backup Settings

The following table describes the settings and where they are available.

Parameter	Description	EPC software	Webpages
Backup	Used to save the Panel Server configuration.	✓	✓
Backup settings	Used to name the backup file and help secure backup data by encrypting the backup file with a password. 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	EPC software	Webpages
Restore	Used to restore configuration from a backup file. Check that the Panel Server receiving the backup has a firmware revision equal to or greater than the firmware revision of the Panel Server used to create the backup file. 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. NOTE: When the configuration is restored, existing logged data is 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 60.
Data is restored in the same Panel Server	Wireless networks remain deactivated.

Cybersecurity Recommendations

What's in This Part

Security Capabilities	139
Security Recommendations for Commissioning	141
Security Recommendations for Operation	142
Security Recommendations for Decommissioning	143

Security Capabilities

General Cybersecurity Recommendations

⚠ WARNING
<p>POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY</p> <ul style="list-style-type: none"> • 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. <p>Failure to follow these instructions can result in death, serious injury, or equipment damage.</p>

For detailed information about cybersecurity for the EcoStruxure Panel Server, see DOCA0211•• *EcoStruxure Panel Server - Cybersecurity Guide*, page 10. For a general introduction to cybersecurity threats and how to address them, see *How Can I Reduce Vulnerability to Cyber Attacks?*.

For more information about cybersecurity, visit [Schneider Electric Cybersecurity Support Portal](#).

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 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

Two 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	<p>Modbus and some IT protocols (NTP, DHCP, DNS, and DPWS) are unsecure.</p> <p>The device does not have the capability to transmit data encrypted using these protocols.</p>	If a malicious user gained access to your network, they could intercept communications.	<p>If transmitting data over an internal network, physically or logically segment the network.</p> <p>If transmitting data over an external network, encrypt protocol transmissions over all external connections using a VPN (Virtual Private Network) or a similar solution.</p> <p>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.</p>
Wireless radio communication	During the pairing 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).	<p>Reduce commissioning window to limit exposure.</p> <p>Once the pairing is performed, consult the list of paired devices in EcoStruxure Panel Server configuration using EcoStruxure Power Commission software and make sure that the list of devices contains no unexpected or rogue devices.</p>

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.

Once the pairing is performed, it is recommended to periodically verify the list of paired 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.

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.

Secure Communication with Wireless Devices

It is recommended to periodically verify the list of paired 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 EcoStruxure 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 EcoStruxure 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.

<i>NOTICE</i>
<p>HAZARD OF IP ADDRESS CONFLICT</p> <p>Disconnect the EcoStruxure Panel Server from any Ethernet networks before resetting the IP settings to factory values.</p> <p>Failure to follow these instructions can result in impaired communications.</p>

To reset the EcoStruxure Panel Server completely, follow this procedure to set all configuration settings to factory values:

1. Unpair all wireless devices from the EcoStruxure Panel Server.
2. Power up the EcoStruxure Panel Server while pressing the Restart 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 EcoStruxure Panel Server to restart completely:
 - a. The status LED turns steady orange while the EcoStruxure Panel Server is booting.
 - b. The status LED turns steady green when the EcoStruxure Panel Server is in normal operation.

IMPORTANT: After performing a reset to factory setting on a Panel Server that has been previously connected to the Schneider Electric cloud, contact the Schneider Electric Customer Care Center to allow the reset Panel Server to connect again to the Schneider Electric cloud or to enable a Panel Server Advanced used as a local energy server to send e-mails again.

General Principle to Commission an EcoStruxure Panel Server

Overview

The commissioning of an Panel Server can be performed using one of the following tools:

- EcoStruxure Power Commission software, page 145. See *EcoStruxure Power Commission Online Help*.

Use the software for a system-focused, global approach to configure the Panel Server 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 150.

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

During commissioning of the Panel Server, update the firmware of the Panel Server, page 126.

Pre-requisites to Commissioning

To commission the Panel Server, connect it to Ethernet (see *Connection to a PC*, page 30).

Getting Started with EcoStruxure Power Commission Software

What's in This Part

- First Connection with EcoStruxure Power Commission Software 146
- Non-Selective Pairing of Wireless Devices 147
- Selective Pairing of Wireless Devices 148
- Device Configuration with EcoStruxure Power Commission Software 149

First Connection with EcoStruxure Power Commission Software

EcoStruxure Power Commission software supports self-discovery of EcoStruxure Panel Server and connected devices.

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 29).
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 191.

Non-Selective Pairing of Wireless Devices

Presentation

Non-selective pairing of wireless devices is available on EcoStruxure Power Commission software: all wireless devices in the network and in pairing phase are discovered by the EcoStruxure Panel Server. The feature enables you to pair a large number of wireless devices at the same time.

Procedure

To commission the EcoStruxure Panel Server with 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 29).
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 68).
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 pairing and filled information 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 Pairing of Wireless Devices

Presentation

It is possible to achieve a selective pairing by using EcoStruxure Power Commission software. To pair the wireless devices with EcoStruxure Panel Server, define and upload a pairing list to EcoStruxure Power Commission software. The Panel Server will pair only the wireless devices belonging to the list.

Device Configuration with EcoStruxure Power Commission Software

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*.

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 146.
2. Set the date and time for the Panel Server at **Settings > General**. Refer to [Date and Time](#), page 102.
3. Configure the network settings, page 46.
4. Discover Modbus devices, page 170 and/or pair wireless devices, page 174.
5. Configure the connected devices:
 - Modbus devices: at **Settings > Modbus Devices**. Refer also to [Custom Models](#), page 116.
 - Wireless devices: at **Settings > Wireless Devices**. Refer also to sections on configuring wireless devices in [Pairing/Unpairing of Wireless Devices Through Webpages](#), page 174.
 - Configure embedded digital inputs, page 128, if relevant.
 - Set up data sampling, page 104.
 - Set up data publishing and/or cloud services, page 87.

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.

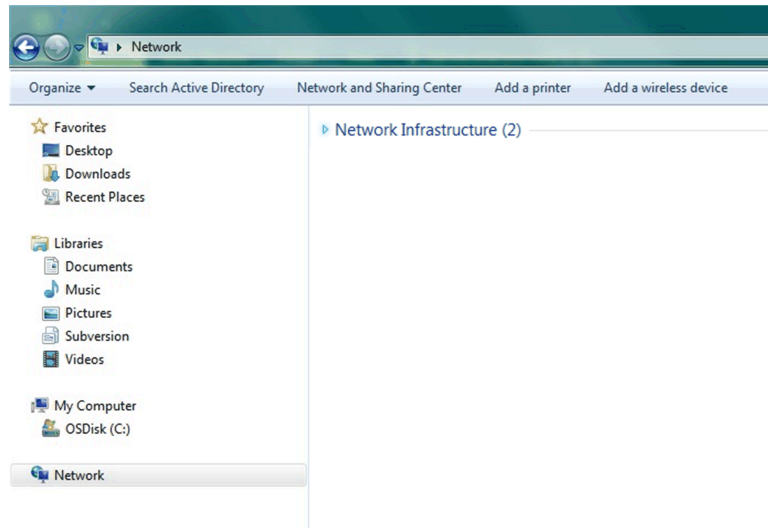
Connecting to a Panel Server on a PC

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:

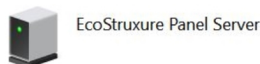
1. Disconnect the PC from the local area network (LAN) and switch off Wi-Fi, if any.
2. Connect an Ethernet cable from the PC to the Panel Server (see [Connection to Ethernet](#), page 29).

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 EcoStruxure Panel Server icon.
- Result:** The Panel Server webpages open.
6. If the Panel Server is not displayed under **Network**:
- 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**.
 - Go to step 1 and do the procedure again.
 - If the Panel Server is still not displayed under **Network**, see *Troubleshooting*, page 191.
7. You are prompted to change the password when logging in for the first time to help prevent unauthorized access to the application. Change the default password (see *Password Requirements*, page 127).

8. 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).

Using EcoStruxure Panel Server Webpages

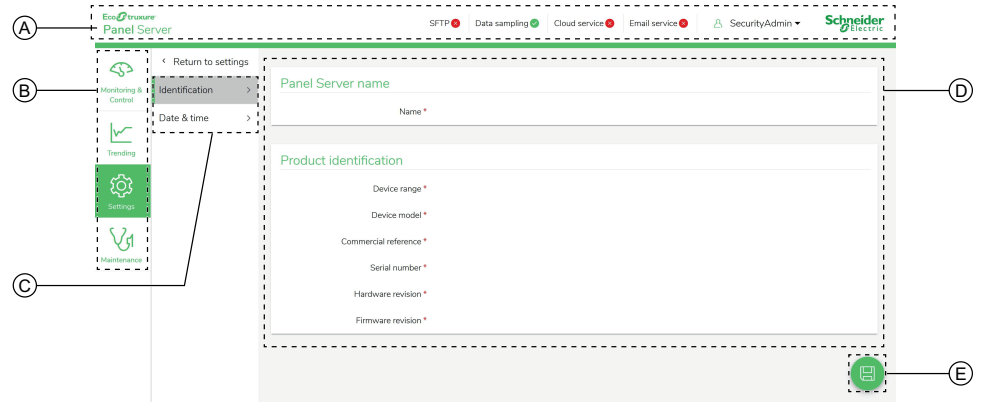
What's in This Part

EcoStruxure Panel Server User Interface Layout	155
EcoStruxure Panel Server Webpage Menus.....	159
Addition and Removal of Modbus Devices.....	170
Pairing/Unpairing of Wireless Devices Through Webpages.....	174

EcoStruxure Panel Server User Interface Layout

Overview

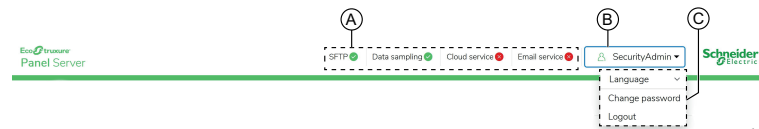
The illustration shows the Panel Server user interface layout.



- A. Header
- B. Main menus
- C. Sub menus
- D. Display zone
- E. Icon for contextual menu






Header

The header displays the following information at the top of every page.



- A. Services and associated status
- B. User name
- C. Drop-down list (language, change password, logout)

Header part	Description
User name	The user name is SecurityAdmin , a user account with administrator rights such as reading and changing the product configuration, pairing or unpairing wireless devices, accessing system logs.
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 127).
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 a certain time of no activity.

Header part	Description
Service names	<p>Services are displayed depending on the Panel Server model:</p> <ul style="list-style-type: none"> • SFTP • HTTPS • Data sampling • Cloud service • Control scheduling • Email service (Advanced model) • Data maintenance
Service status	<p>The icon displays the service status:</p> <ul style="list-style-type: none"> •  Service activated and operative •  Service activated but inoperative •  (Cloud service only): <ul style="list-style-type: none"> ◦ Initial configuration of the Panel Server is complete, however these additional actions are needed: publish the topology and associate the Panel Server on the cloud application side. ◦ The remote configuration sent by the cloud application is invalid and is rejected by the Panel Server. An error is logged in the <code>auto-dignostic</code> log file to assist with troubleshooting, page 131. 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. •  (All services): A restart was initiated. The icon will change to green after a successful publication cycle. •  Data maintenance operation in progress. The service name and status icon will disappear when the data maintenance operation is completed.

Main Menus

The main menus are:

- **Home** (Advanced model), page 161
- **Notifications** (Advanced model), page 124
- **Monitoring and Control**, page 162
- **Trending** (Advanced model), page 166
- **Settings**, page 167
- **Maintenance**, page 169

Cards and Sub-menus












The cards and sub-menus display the sub-levels available under the selected main menu. Fields with a red star icon should be filled in to help ensure the proper behavior of the gateway and devices.

Display Zone




The display zone shows the selected card or sub-menu in detail with all related fields.

Icons

The context-specific function icons displayed depend on the selected menu.



Icon	Action
	Open the contextual menu.
	Close 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. <ul style="list-style-type: none"> • 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.
	In Settings pages, save the setting changes without applying the configuration on the Panel Server.
	Contextual icon: <ul style="list-style-type: none"> • 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.
	Go to the maintenance page of the selected device.
	Go to the settings page of the selected device.
	Go to the real-time data page of the selected device.
	Go to the data management page of the selected device.
	Go to the trending page.
	Go to the monitoring and control page of the selected device.

Monitoring and Control Icons







Icon	Description
	The device is connected.
	The device is not connected.
	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.

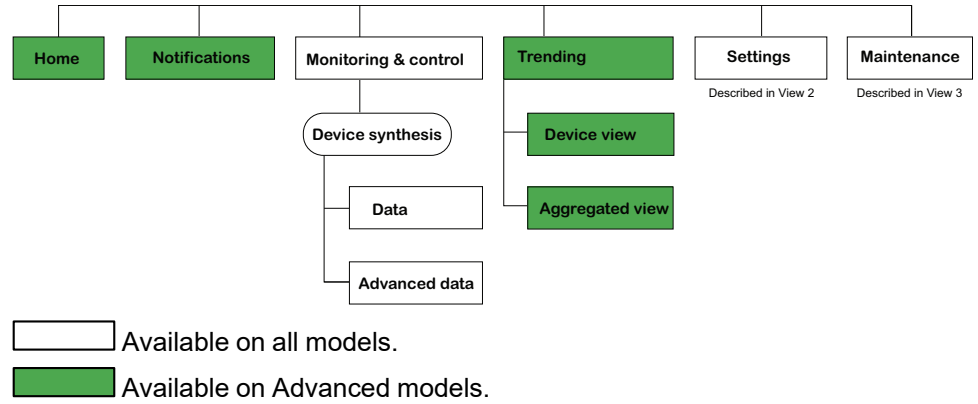
Alarm Icons

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

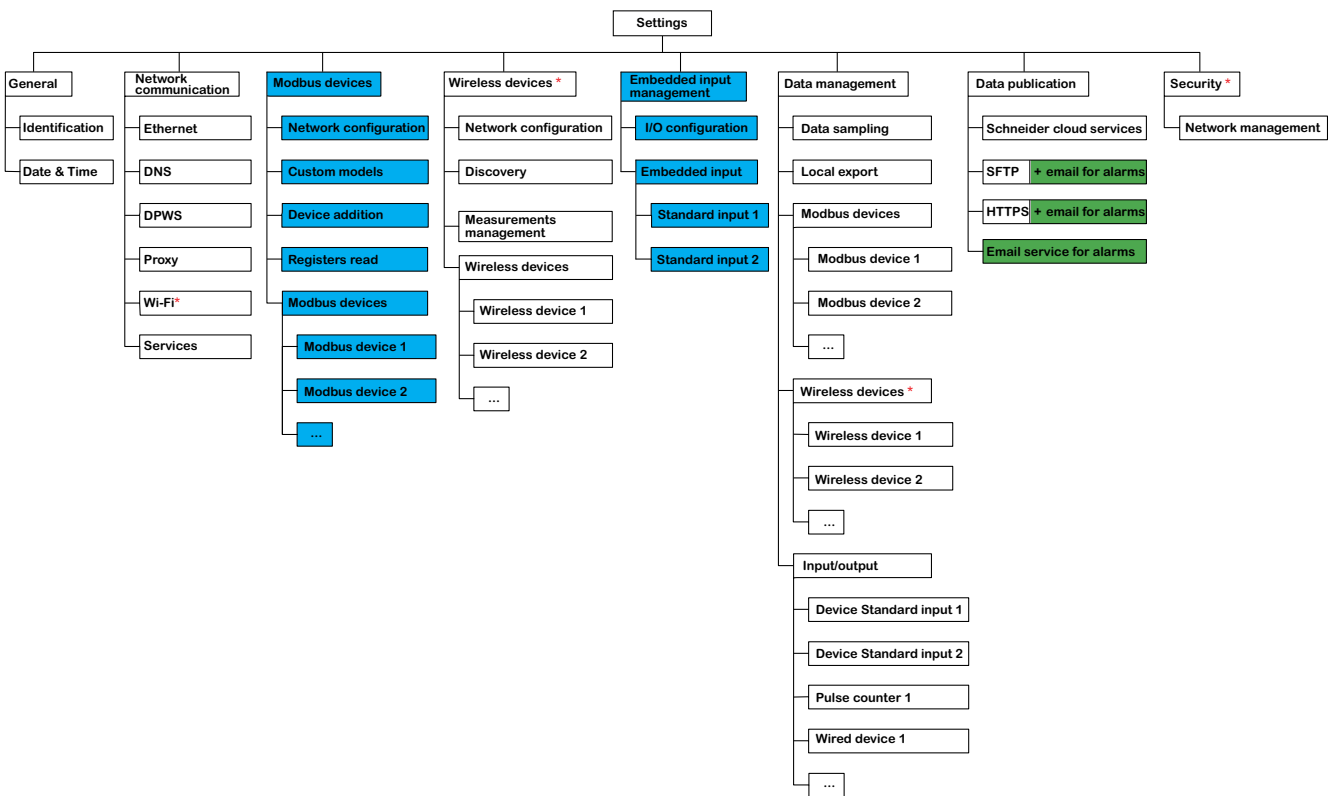
Overview

The following diagram gives an overview of the structure of webpages.



Settings Menu Structure

View 2



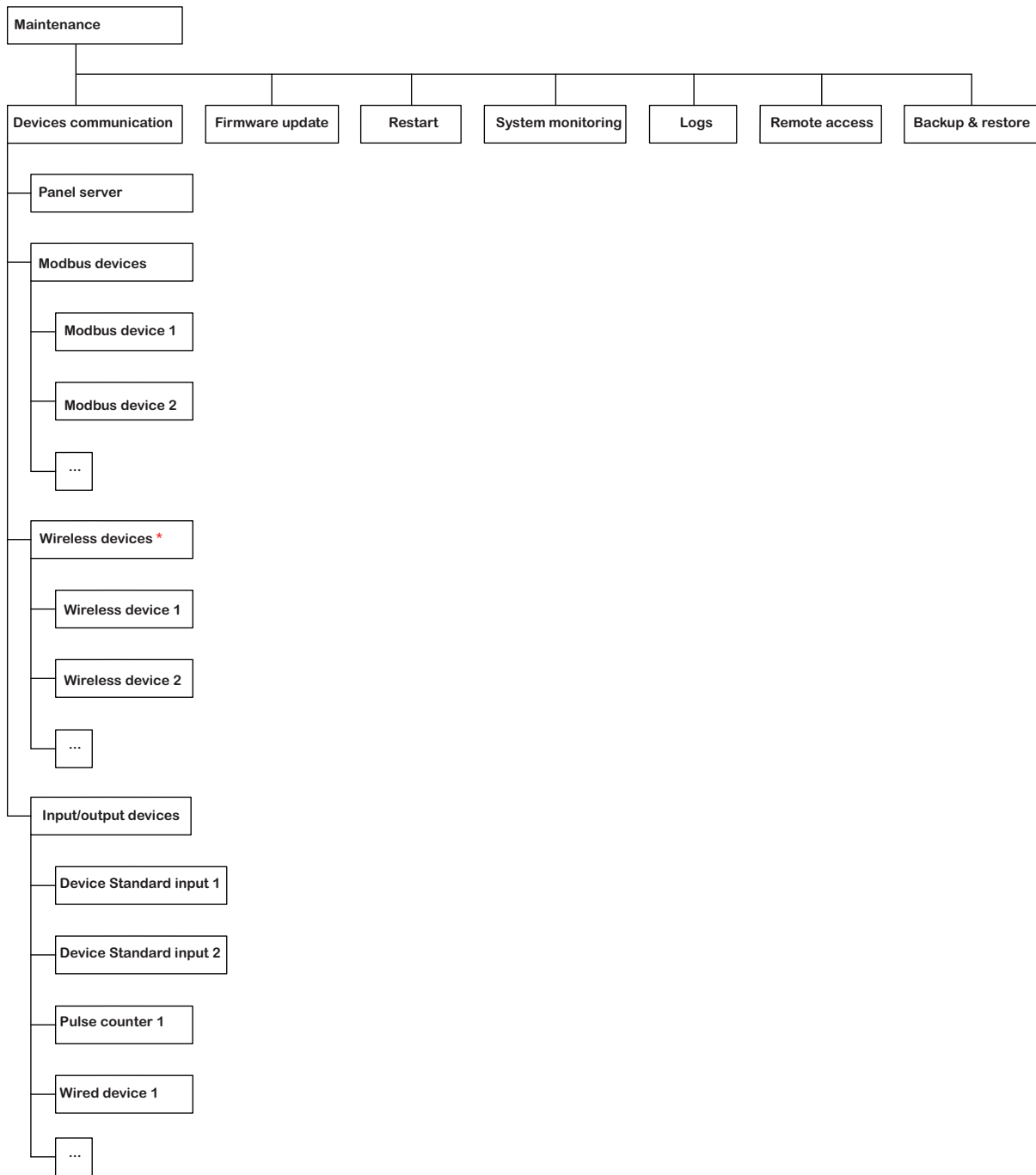
* Not available on Wired by Design models.

Available on all models.
 Available on Universal and Advanced models.
 Available on Advanced models.

For more information, refer to **Settings** menu, page 167.

Maintenance Menu Structure

View 3



* 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 169.

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), and organized by usage. Other commodities and periods can be selected.


The top five types of usage (plus any other type of usage that is also consuming the selected commodity) are displayed, arranged from highest to lowest consumption.

A pie-chart shows the distribution of the top five consumers. The webpage displays for each usage:

- 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)

In the **Home** page the user can select a different commodity (for example, gas) and a different period (one day, one week, or 4 weeks). For more information about filtering, see [Data Trending](#), page 110.

When the user is logged in the Panel Server webpages, the Home page automatically displays if historized data is available.

For more information about the trending data, click the  **Trending** icon on the right-hand side of the **Home** webpage to go to **Trending > Aggregated view**.

Notifications Menu (Advanced Model)

The webpage for the **Notifications** menu displays a list of alarms for a selected period.

For more information, refer to [Notifications](#), page 124.

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.

General information is displayed for each device (for example, name and type of the device communicating with the Panel Server). The **Data type selection** button can be used to display specific information, depending on the device type (for example, energy, environment, or voltage). If the button is not visible, scroll to the right.

In a large electrical distribution system, filtering enables you to display selected devices by using one or several of the following filters:

- Device family
- Commodity
- Usage
- Zone in which the device is installed.





Example: To display **Energy** consumption for **Power meter** devices,

- Select **Power Meter** in the Device family list.
- Scroll to the right of the screen and select **Energy** in the **Data type selection** list.

Result: The columns display the different energy parameters for the devices selected. Scroll to the bottom of the page to check for other devices on subsequent pages.

Displaying Data by Device

Click on a device name to see information specific to that device:

- Information about the device:
 - Device model
 - Device firmware version
 - Device serial number
 - Device connection status
- Real-time data of the device:
 - The displayed data depends on the device 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.
 - Data is displayed per family.
- Advanced data, page 164
- 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 .

Device Real-time Data

In the **Monitoring and Control** menu, the **Advanced data** page of the selected device shows the exhaustive list of data related to this device.

The following table presents data available per measurement family. The availability of measurements depends on the type of connected device.

Data family	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
Digital input	Digital input 1 status
	Digital input 1 name
	Digital input 2 status
	Digital input 2 name
	Digital output status
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

Data family	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 current N
	Harmonic current alarm
IGBT temperature	Temperature board in device
	Temperature IGBT A
	Temperature IGBT B
	Temperature IGBT C
Insulation	Insulation ground
	Earth coupling capacity
Motor	Motor trip indicator
	Motor running
	Motor operating mode
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)

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.

For information about trending graphs, see [Data Trending](#), page 110.

Settings Menu

<i>NOTICE</i>
<p>IMPAIRED NETWORK PERFORMANCE</p> <p>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.</p> <p>Failure to follow these instructions can result in equipment damage.</p>

The webpage for the **Settings** menu displays the sub-menus for configuration and communication settings. The menus and sub-menus on the webpages depend on the Panel Server model.

Settings menu	Navigation menu webpage	Description
General	Identification	Information about the Panel Server identification: <ul style="list-style-type: none"> • Device name • Device range • Device model • Commercial reference • Serial number • Hardware revision • Firmware revision
	Date & Time , page 102	Used to set the date and time manually or via NTP (Network Time Protocol).
Network communication	Ethernet , page 53	Allows you to configure the Panel Server Ethernet mode including ports and IP parameters (IPv4 and IPv6)
	DNS , page 61	Allows you to configure the DNS server.
	DPWS , page 63	Allows you to configure the IP network discovery.
	Proxy , page 62	Allows you to configure the Internet proxy settings.
	Wi-Fi , page 57	Allows you to configure the Wi-Fi settings.
	Services	Allows you to deactivate services per interface (ETH1 port, ETH2 port, and Wi-Fi)
Modbus devices	Modbus configuration , page 70	Allows you to define the Modbus-SL and Modbus TCP/IP network.
	Custom models , page 116	Allows you to upload Modbus-SL and Modbus TCP/IP devices that are not natively managed by the Panel Server built-in models.
	Modbus addition , page 170	Allows you to discover the Modbus-SL and Modbus TCP/IP devices by using a selective list.
	Modbus registers read , page 172	Allows you to troubleshoot the addition of Modbus devices
	Modbus devices	Detailed information about each device 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.

Settings menu	Navigation menu webpage	Description
Wireless devices, page 67	Wireless (802.15.4) configuration	Allows you to define the IEEE 802.15.4 network when activated.
	Wireless (802.15.4) discovery	Allows you to discover the wireless devices in the IEEE 802.15.4 network by using a selective list or non-selective discovery.
	Wireless devices	Detailed information about each wireless device in the IEEE 802.15.4 network. Information (for example, device identification, 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 128	Allows you to configure the Panel Server digital inputs.
	Input/Output	Allows you to configure inputs/outputs of I/O devices associated with Panel Server.
Data Management	Data sampling , page 104	Allows you to define data sampling of the connected devices.
	Local export , page 113	Allows you to export the data sampled locally in a .csv file. (Available in Advanced model only.)
	Modbus devices	Detailed information about sampling for each device in the Modbus network. Measurements and alarms depend on the device type.
	Wireless devices	Detailed information about sampling for each wireless device in the IEEE 802.15.4 network. Measurements and alarms depend on the device type.
	Input/Output	Detailed information about sampling for devices connected to the embedded inputs of the Panel Server. Measurements and alarms depend on the device type.
Data Publication , page 87	Data Publication	Allows you to set the means used to publish data and to enable the email of alarms service
Security	Network management , page 60	Allows you to configure the security feature to permanently disable the wireless networks.

Maintenance Menu

Webpage for the **Maintenance** menu displays the sub-menus for maintenance and diagnostic functions, based on diagnostic counters.

Maintenance main menu	Navigation menu webpage	Description
Devices communication, page 131	Communication data about the Modbus and wireless devices in the network.	Allows you to check the communication status of the Panel Server with downstream devices (Modbus-SL and wireless devices).
	Modbus devices	Displays information about and status of the selected device.
	Wireless devices	Allows you to delete a previously paired or associated downstream device.
	Embedded Input (PAS600L, PAS600LWD, PAS800L)	Displays information about and status of the embedded inputs.
Firmware update	–	Allows you to perform a local firmware update of the Panel Server.
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 133	–	Displays Panel Server health status indicators.
Logs, page 134	–	Allows you to: <ul style="list-style-type: none"> • Change the log level and download the 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.
Remote access	–	<ul style="list-style-type: none"> • The Remote access section allows you to provide the Schneider Electric Customer Care Center with a temporary remote access to the Panel Server webpages: <ul style="list-style-type: none"> ◦ When you have contacted the Schneider Electric Customer Care Center, you can give access to Schneider Electric local support to the Panel Server. ◦ A password is displayed that you communicate to the Schneider Electric local support. ◦ The support connects to the Panel Server. ◦ As soon as you click the disconnection button on the webpages or after 3 hours maximum, the password is no longer active and remote access is terminated. • The Remote operation 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: <ul style="list-style-type: none"> ◦ Enable the toggle button to proceed. <p>For information about the cloud infrastructure, see Schneider Electric cloud services, page 88.</p>
Backup & restore, page 133	–	Allows you to save the Panel Server current configuration and restore it.

Addition and Removal of Modbus Devices

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 List

In the **Settings > Modbus devices > Modbus addition > Modbus TCP/IP > Discovery > Selective list** webpage, create a list of devices to be discovered by entering the IP address for each device. The port is always 502 (see Ethernet Communication, page 53) and unit ID 255 (see Modbus Gateway Function, page 76).

Result: The table shows the following information for each device discovered on the Modbus TCP/IP network:

- Picture
- Device name

NOTE: If applicable, for example for a third-party device, **unknown device** is displayed. In this case, data not displayed in the webpages.

- IP address
- Port
- Unit ID

The device is displayed in the **Modbus devices** section.

Manual Addition of Modbus TCP/IP Devices

In the **Settings > Modbus devices > Modbus addition > Modbus TCP/IP > Manual addition > IP address** webpage, enter the following information for each device:

- IP address
- Port
- Unit ID
- Device type

NOTE: If the device type is not available in the drop-down list, for example for a third-party device, select **unknown device**. In this case, data is not displayed in the Panel Server webpages.

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 > Modbus Addition > Modbus TCP/IP > Manual Addition** then:

- Type the value for **Physical Server ID**.
- Select the custom device model name in **Device**.

Discovery of Modbus-SL Devices With a List

In the **Settings > Modbus devices > Modbus addition > Modbus serial > Discovery > Selective list** webpage, 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.

Result: The table shows the following information for each device discovered on the Modbus-SL network:

- Picture
- Device name

NOTE: If applicable, for example for a third-party device, **unknown device** is displayed. In this case, data is not displayed in the Panel Server webpages.

- Virtual server ID (**Server ID**)

The device is displayed in the **Modbus devices** section.

Manual Addition of Modbus-SL Devices

In the **Settings > Modbus devices > Modbus addition > Modbus Serial > Manual addition > Server ID** webpage, enter the physical server ID of the device to be added and select the device type.

NOTE: If the device type is not available in the drop-down list, for example for a third-party device, select **unknown device**.

Result: Once the device is discovered, 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 > Modbus 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 86), navigate to **Settings > Modbus devices > Modbus 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

NOTE: If the device type is not available in the drop-down list, for example for a third-party device, select **unknown device**. In this case, data is not displayed in the Panel Server webpages.

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 > 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 device	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: <ul style="list-style-type: none"> • FC01 Read coils status • FC02 Read inputs status • FC03 Read holding registers • FC04 Read input registers
Starting register	✓	✓	Enter the number of the first register 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	✓	✓	Enter the total number of consecutive registers to be read.
Result format	✓	✓	For function codes FC03 and FC04, select from the list the format to display the results: <ul style="list-style-type: none"> • 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.

Removal of Modbus Devices

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.

Pairing/Unpairing of Wireless Devices Through Webpages

What's in This Chapter

Selective Pairing of Wireless Devices Through Webpages	175
Controlled Pairing of Wireless Devices (PowerTag Energy, HeatTag) Through Webpages	176
Configuration of Wireless Energy Devices Through Webpages	177
Configuration of PowerTag Control Devices Through Webpages.....	182
Configuration of Ambient Sensors Through Webpages	185
Unpairing Wireless Devices Through Webpages	187
Adding Wireless Devices Paired Under a Child Gateway (Universal and Advanced Models).....	189

Selective Pairing of Wireless Devices Through Webpages

Presentation

It is possible to achieve a selective pairing through the EcoStruxure Panel Server webpages. To pair the wireless devices installed in the EcoStruxure Panel Server system, define and type a pairing list to EcoStruxure Panel Server webpages. The Panel Server will pair only the wireless devices belonging to the list.

Procedure to Pair Wireless Devices Through Webpages

To generate the file that lists the selective wireless devices to be uploaded on the Panel Server webpages:

- List the devices to be paired with Panel Server by typing the RF-id (unique radio frequency identification code) of each wireless device.
The format of RF-id code is alphanumeric.
- It is mandatory to add 0x before each RF-id code printed on the device.
- In the list of devices, separate each RF-id by a comma and no space after the comma.

A virtual ID address will be applied during the pairing process with the Panel Server. The first virtual server address ID is allocated to the first discovered device. If you need to apply virtual ID addresses in a defined order, follow the procedure of [controlled pairing, page 176](#). By default, Modbus virtual server IDs allocated to wireless devices start from 100.

To perform selective pairing of wireless devices through webpages, proceed as follows:

1. Log in to the Panel Server webpages (see how to [access the webpages, page 151](#)).
2. Navigate to **Settings > Wireless devices > Wireless configuration**.
3. If specified in the radio frequency plan, choose the correct communication channel in **Wireless network settings**.
4. In **Wireless communication**, set the communication period for each of the 3 types of devices.
5. Navigate to **Settings > Wireless devices > Wireless discovery > Selective list** and type the RF-id of each wireless device in the field, separating RF identifiers with a comma, and no space after the comma. **Example:**
0xFF900A59,0xFF900A58

All and only the wireless devices in the selective list can be paired with the Panel Server.

6. Click **Start** to scan the environment to discover the list of imported wireless devices.

Result: Once pairing is completed you can view the list of paired wireless devices.

NOTE: A popup message indicates if the network is overconfigured and suggests solutions. To check the network occupancy, navigate to **Settings > Wireless devices > Wireless configuration**.

Controlled Pairing of Wireless Devices (PowerTag Energy, HeatTag) Through Webpages

1. All the wireless devices in the EcoStruxure Panel Server system must be powered on.
2. Launch the EcoStruxure Panel Server webpage in the web browser.
3. Log in to the webpages (see how to [access the webpages](#), page 151).
4. Navigate to **Settings > Devices > Wireless devices**.
5. Click **Start Scanning**.
6. Power on the wireless devices, one by one, in the required order.
7. Stop scanning when all the devices are discovered, or click **Start Scanning** again to complete the scanning process.
A list of paired devices is displayed according to the required order (Modbus address plan).
8. Select the wireless device to configure and click **Locate** to find the device in the panel.
Result: The status LED of the selected device blinks fast green in the panel.
9. If one of the located wireless devices is not part of your selection, click **Delete** to reject the device.
10. Once pairing is completed you can view the list of the paired wireless devices in webpage **Settings > Devices > Wireless devices**.
11. Configure the wireless devices.
NOTE: The Modbus address assigned to the wireless devices can be changed after the pairing process is done.

Configuration of Wireless Energy Devices Through Webpages

To configure wireless energy devices, for example, PowerTag Energy devices, with Panel Server webpages, proceed as follows:

1. Navigate to **Settings > Wireless Devices > Wireless Devices** to view the list of the paired wireless devices.

Result: The list of paired 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. Click **Apply Changes** to save the settings

or

Click **Cancel Changes** to revert the settings.

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 for the configuration of wireless devices.

The fields displayed depend on the type of device.

Parameter Tables

Identification

Parameter name	Description
Name	Enter the name of the wireless device.
Label (optional)	Enter the label of the wireless device .
RF-id	For display only
Device range	For display only
Commercial reference	For display only
Hardware revision	For display only
Device family	For display only

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: <ul style="list-style-type: none"> • Available • Not available
Mounting position	Select the mounting position from the list: <ul style="list-style-type: none"> • 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.

Electrical characteristics (Continued)

Parameter name	Description
Current flow	Select the Current flow to define the convention for PowerTag Energy device to count energies. See the section Current Flow , page 179 for more information about filling this parameter.
Power factor sign convention	Select the power factor sign convention from the list. The setting has an influence on the convention used to sign the power factor. <ul style="list-style-type: none"> • IEC • IEEE For more information, see the section Power Factor Sign Convention , page 179.

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. Select a value of between 2 and 120 seconds from the list (default setting 5 seconds). <p>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).</p> <p>NOTE: Use a maximum setting of 90 seconds if power demand calculation is required. .</p>

Modbus virtual

Parameter name	Description
Virtual server ID	Enter the ID of the Modbus virtual server.

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 I _{max} of the device.
	Rated Voltage (V) (optional)	Enter the value of the rated voltage for the associated circuit breaker. <ul style="list-style-type: none"> • LN rated voltage for 3P4W installation. • LL rated voltage for 3P3W installation.
Load information	Load zone (optional)	The Load operating time counter increments only when the power is greater or equal to the value set. You can set the value between 10 W and 15000 W.

Contextualization data

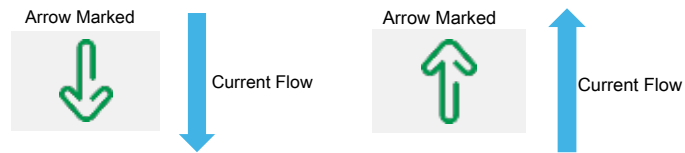
Parameter name	Description
Commodity (optional)	Select the commodity required from the list to indicate the main purpose of the device.
Usage (optional)	Select the usage required from the list to indicate the precise function of the device, for example, the type of lighting to be monitored: Lighting (Exterior and Park) or Lighting (Interior)

Current Flow

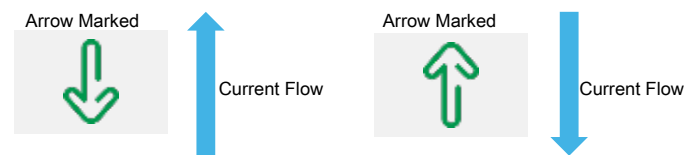
For PowerTag Energy devices F160 and Rope, selecting the current flow defines the convention for the PowerTag Energy device to count energies.

The current flow can be **Direct** or **Reverse**:

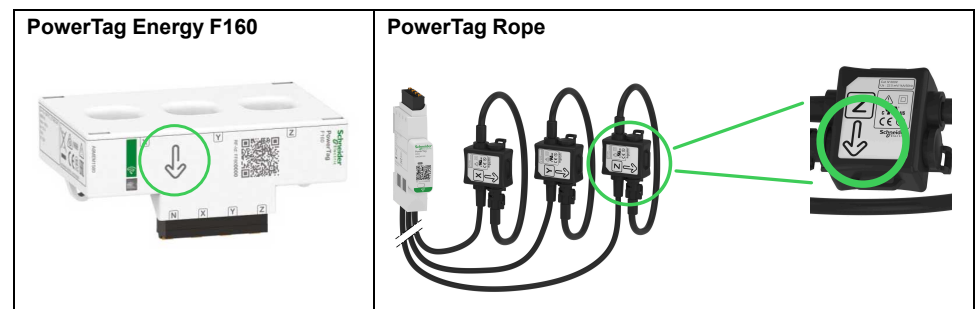
- **Direct:** If the arrow marked on the PowerTag Energy device is in the same direction as the current flow.



- **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:

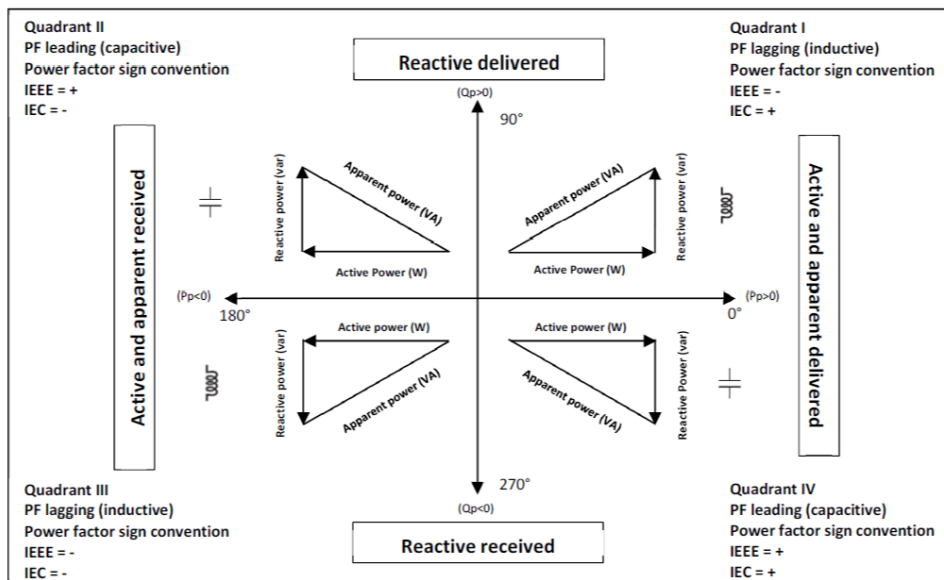


Power Factor Sign Convention

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 > Measurements management**. 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.

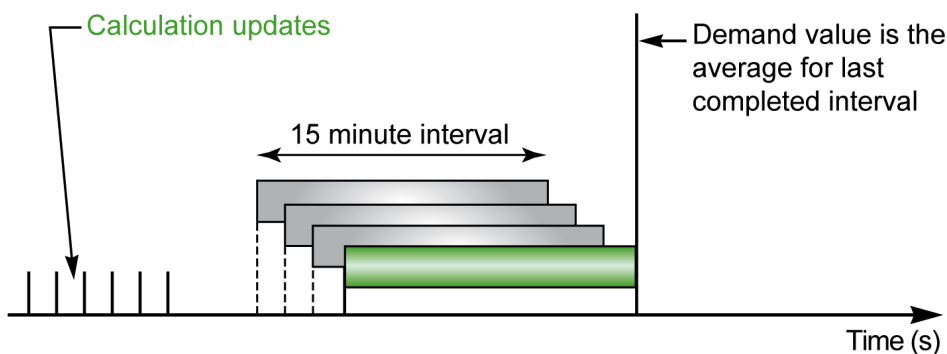
You can reset the peak power demand value to 0 for:

- All PowerTag devices connected to the Panel Server, including PowerTag Rope on the Panel Server webpages at **Settings > Wireless devices > Measurements management**
- 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 PowerTag Control Devices Through Webpages

To configure PowerTag Control devices with EcoStruxure Panel Server webpages, proceed as follows:

1. Navigate to **Settings > Wireless Devices > Wireless Devices** to view the list of the paired wireless devices.

Result: The list of paired devices is displayed (with **Connected** written in green under the device name).

2. Select the required PowerTag Control device to modify the configuration.

Result: The parameters of the PowerTag Control device are displayed.

3. If necessary, in **Locate**, click **Start** to identify the specific device in its location. The PowerTag Control device LED blinks for 30 seconds.

4. Enter the data in the fields, referring to the following tables for more information about the parameters.

5. Click **Apply Changes** to save the settings

or

Click **Cancel Changes** to revert the settings.

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.

Parameter Tables

Identification

Parameter name	Description
Name	Enter the name of the wireless device.
Label (optional)	Enter the label of the wireless device.
RF-id	For display only
Device range	For display only
Commercial reference	For display only
Hardware revision	For display only
Device family	For display only

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. Select a value of between 5 and 120 seconds from the list.

Modbus virtual

Parameter name	Description
Virtual server ID	Enter the ID of the Modbus virtual server.

Input/Output Settings

Parameter name	Description
Local Control	Toggles local control on or off.
Configuration Type	Select from the list: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.
	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.
Input	I/O Type	Select from the list: <ul style="list-style-type: none"> • 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.

Parameters for Contactor with feedback loop and for Impulse Relay

Parameter name		Description
I/O Type		Select from the list: <ul style="list-style-type: none"> • Standard I/O • Not connected <p>NOTE: No parameters are displayed if Not connected is selected.</p>
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.
	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. <p>NOTE: Clicking the double arrow icon on the right allows you to swap the meanings of outputs 0 and 1.</p>
	Meaning of output = 1	Displayed values depend on selection of I/O Contextualization . Enter your custom values if you select Custom as contextualization option. <p>NOTE: Clicking the double arrow icon on the right allows you to swap the meanings of outputs 0 and 1.</p>

Configuration of Ambient Sensors Through Webpages

To configure ambient sensors with EcoStruxure Panel Server webpages, proceed as follows:

1. Navigate to **Settings > Wireless Devices > Wireless Devices** to view the list of the paired wireless devices.

Result: The list of paired devices is displayed (with **Connected** written in green under the device name).

2. Select the required ambient sensor to modify the configuration.

Result: The parameters of the sensor are displayed.

3. If necessary, in **Locate**, click **Start** to identify the specific sensor in its location. The sensor LED blinks for 30 seconds.

4. Enter the data in the fields, referring to the following tables for more information about the parameters.

5. Click **Apply Changes** to save the settings

or

Click **Cancel Changes** to revert the settings.

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.

Parameter Tables

Identification

Parameter name	Description
Name	Enter the name of the wireless device.
Label (optional)	Enter the label of the wireless device.
RF-id	For display only
Device range	For display only
Commercial reference	For display only
Hardware revision	For display only
Device family	For display only

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. Select a value of between 60 and 600 seconds from the list.

Modbus virtual

Parameter name	Description
Virtual server ID	Enter the ID of the Modbus virtual server.

Contextualization

Parameter name	Description
Commodity	Select from the list the commodity to be monitored.

Unpairing Wireless Devices Through Webpages

Unpairing of Wireless Devices Through Webpage

To unpair one or several wireless devices through EcoStruxure Panel Server webpages, follow the procedures in the subsequent sections, as applicable:

- Unpairing all connected wireless devices
- Unpairing one connected wireless device
- Forcing unpairing of one or several connected wireless devices

Some wireless devices have a local method to unpair 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.

Unpairing of all Wireless Devices Through Webpage

1. Navigate to **Settings > Wireless devices > Wireless Configuration** to view the list of paired wireless devices.
2. In the **Wireless device management** section, click the **Unpair all devices** button.
Result: A message displays to confirm the removal of the wireless devices from the configuration.
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 unpairing order. The process duration depends on the device. It may take up to 10 minutes.

Result: Once a wireless device is successfully unpaired with the Panel Server, it is no longer visible in the list of wireless devices discovered.

Unpairing of one Wireless Device Through Webpage

1. Navigate to **Settings > Devices > Wireless devices > Wireless Devices** to view the list of paired wireless devices.
2. Select the device to be removed from the configuration.
3. Click the bin icon on the right side of the webpage.
4. Click **Yes** to initiate the removal process.
5. Wait until unpairing is completed. The process duration depends on the devices. It may take up to 10 minutes.

Result: Once the wireless device is successfully unpaired with the Panel Server, it is no longer visible in the list of wireless devices discovered.

Forcing Unpairing of Wireless Devices Through Webpage

It is possible that the unpairing process does not succeed with one or several devices when a device is not powered or is out of order. If a device has not been unpaired 10 minutes after the unpairing process has begun, 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, open the webpage for the selected device and click the **Force remove** button.

Result: Once the wireless device is successfully deleted from the Panel Server configuration, it will not be visible in the list of devices discovered.

If you want to pair the forced unpaired device with a new Panel Server, reset and power off this device.

Adding Wireless Devices Paired Under a Child Gateway (Universal and Advanced Models)

Presentation

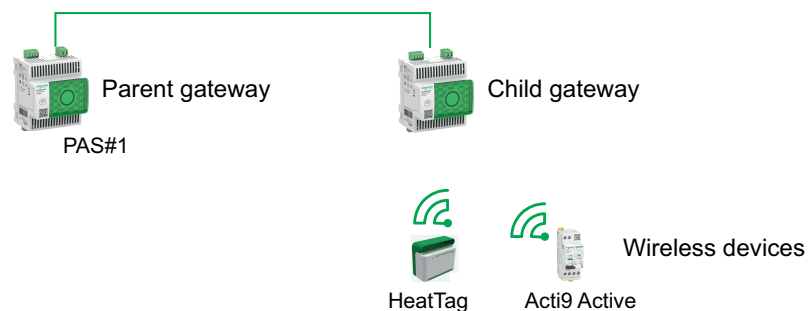
The Panel Server Universal allows you to display and publish data from wireless devices connected to a child gateway. In addition, the Panel Server Advanced can log the data, display them in the trending screens and export them in a csv file.

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 able 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 embedded webpages
2. Pair all the wireless devices to the child gateway.
3. Connect to the parent gateway using the embedded webpages.

4. Each wireless device is added to the parent gateway using the Modbus/TCP manual addition procedure by accessing the **Settings > Modbus devices > Modbus discovery > 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 53). If the Panel Server Entry is connected in DHCP mode, follow the procedure in *Appendix G*, page 223 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 of 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.	MAC address (printed on the Panel Server front face nose) not recognized.	Follow the procedure to convert the hexadecimal value of the MAC address to the decimal value to get the IP address, page 192.
On first connection to the Panel Server from a PC, the Panel Server is not displayed under Network .	You need to convert the hexadecimal value of the MAC address to a decimal value to get the Panel Server IP address.	
The status LED is not lit.	Source power not applied or not stable.	Apply power or check power source.
Panel Server status LED blinking orange	Panel Server in degraded health state.	<p>See the Panel Server Diagnostics webpages, page 131.</p> <p>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:</p> <ul style="list-style-type: none"> • If Modbus is identified, then a Modbus-SL device may have been powered off or removed from EcoStruxure Power Commission software, 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.

Procedure to Convert MAC Address to IP Address

- Follow the procedure to convert the hexadecimal value of the MAC address to the decimal value to get the IP address:
 - For Panel Server serial number starting with 54-21-44 or lower**

If...	Then...	Example with MAC address 00-00-54-01-07-70
The Panel Server is in Ethernet switch mode (default setting).	Y is equal to the last digits of the Panel Server MAC address converted into decimal value + 1.	Hexadecimal 70 converted to decimal is 112.
The Panel Server is in Ethernet separated mode and the PC is connected to Panel Server ETH1 port.		Y = 112 + 1 = 113 Therefore IPV4 address will be 169.254.7.113.
The Panel Server is in Ethernet separated mode and the PC is connected to Panel Server ETH2 port.	Y is equal to the last digits of the Panel Server MAC address converted into decimal value + 2.	Hexadecimal 70 converted to decimal is 112. Y = 112 + 2 = 114 Therefore IPV4 address will be 169.254.7.114.

- For Panel Server serial number starting with 54-21-45 or higher**

If...	Then...	Example with MAC address 00-00-54-02-07-10
The Panel Server is in Ethernet switch mode (default setting).	Y is equal to the last digits of the Panel Server MAC address converted into decimal value.	Hexadecimal 10 converted to decimal is 16.
The Panel Server is in Ethernet separated mode and the PC is connected to Panel Server ETH1 port.		Therefore IPV4 address will be 169.254.7.16.
The Panel Server is in Ethernet separated mode and the PC is connected to Panel Server ETH2 port.	Y is equal to the last digits of the Panel Server MAC address converted into decimal value + 1.	Hexadecimal 10 converted to decimal is 16. Y = 16 + 1 = 17 Therefore IPV4 address will be 169.254.7.17.

- Launch one of the recommended web browser on your PC.
- In the address field, type the IPv4 address starting with `https://` and press **Enter** to access the login page `https://169.254.XX.YY`.

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.

Troubleshooting of Webpages and 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 143.
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

Problem	Diagnostics	Action
		Commission software or Panel Server webpages.
A wireless device is not discovered by the Panel Server.	Panel Server does not recognize this type of wireless devices.	<p>Verify that the device is in the list of supported devices. See the respective release notes, page 10s:</p> <ul style="list-style-type: none"> DOCA0249•• <i>EcoStruxure Panel Server Entry - Firmware Release Notes</i> DOCA0178•• <i>EcoStruxure Panel Server Universal - Firmware Release Notes</i> DOCA0248•• <i>EcoStruxure Panel Server Advanced - Firmware Release Notes</i>
Status of wireless devices (for example, Easergy TH110) does not update in Panel Server webpages or EcoStruxure Power Commission software.	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 the webpages .	<ul style="list-style-type: none"> Verify that the device is powered on. Verify that the wireless device is not installed out of range of the Panel Server.
A Modbus device is not discovered by the Panel Server.	Incorrect device configuration settings.	<ul style="list-style-type: none"> Verify that the device is in the list of supported devices. Verify that the device settings are set according to the Panel Server (see Serial Configuration Settings, page 71).
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 76 to correct conflicts by using EcoStruxure Power Commission software.
Alarms are not displayed in the Monitoring & Control page of the Panel Server webpages.	The device may be associated with a custom model.	<ol style="list-style-type: none"> 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. In the webpage Settings > Data management, select the device and enable the alarms to be displayed in the Alarm widget.
<p>The Panel Server cannot reach the Schneider Electric cloud.</p> <p>Network unreachable is displayed in Connection diagnostics.</p>	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 102).
The Panel Server is not recognized by the Schneider Electric cloud services.	–	<p>Check that port 443 has been opened to cloud services (see parameters for cloud connection and services, page 88).</p> <p>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.</p>

Appendices

What's in This Part

Appendix A: Details of Modbus Functions	195
Appendix B: Data Availability	207
Appendix C: Wireless Device Network Indicators	214
Appendix D: SFTP and HTTPS Publication File Formats	215
Appendix E: SSH Key Exchange and Cipher	218
Appendix F: Certificate Authorities	219
Appendix G: Retrieve the DHCP IP Address of a PAS400 Panel Server	223

Appendix A: Details of Modbus Functions

What's in This Chapter

Modbus TCP/IP Functions	196
Modbus-SL Functions.....	198
Modbus TCP/IP and Modbus-SL Exception Codes	199
Modbus Registers Tables.....	201
Function 43-14: Read Device Identification.....	202
Function 100-4: Read Non-Adjacent Registers	204
Setting Message Timeout for Modbus Client and Modbus Server	205

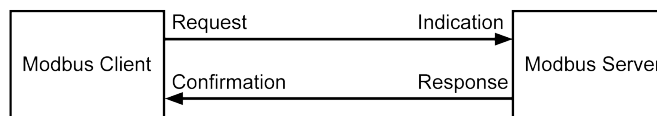
Modbus TCP/IP Functions

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:

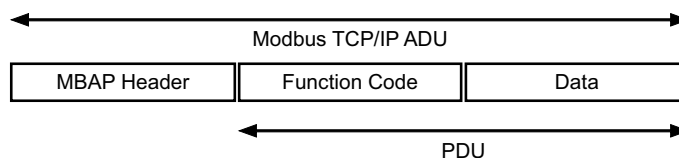
- Modbus Request, the message sent on the network by the client to initiate a transaction.
- Modbus Indication, the request message received on the server side.
- Modbus Response, the response message sent by the server.
- Modbus Confirmation, the response message received on the client side.



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 Modbus TCP/IP devices supported by the EcoStruxure Panel Server:

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 202)
100-4	Read non-adjacent words where $n \leq 100$ (refer to Function 100-4: Read Non-Adjacent Registers, page 204)

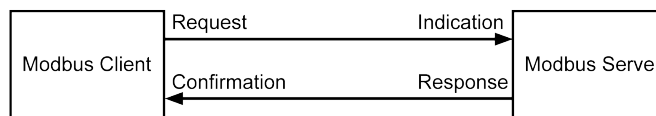
Modbus-SL Functions

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).

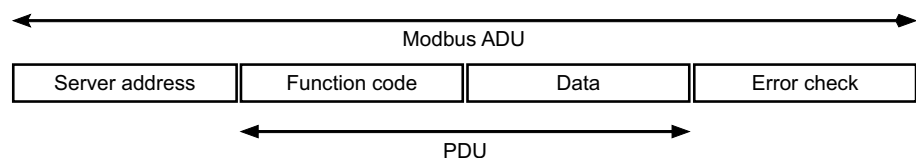


Table of Modbus Functions

The following table describes in detail the functions supported by the Modbus-SL devices supported by the EcoStruxure Panel Server:

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 202)
100-4	Read non-adjacent words where $n \leq 100$ (refer to Function 100-4: Read Non-Adjacent Registers, page 204)

IMPORTANT: Function codes 1 and 2 are not supported.

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 wireless devices of 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.

For detailed information about these Modbus registers, refer to DOCA0241EN *EcoStruxure Panel Server - Modbus File*.

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

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

NOTE: The table above describes how to read the ID of an EcoStruxure Panel Server.

Function 100-4: Read Non-Adjacent Registers

Structure of Modbus Read n Non-Adjacent Registers Messages Where $n \leq 100$

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 will be dropped.

The message timeout for the Modbus TCP server is called **Upstream timeout**, set in ms (see [Modbus TCP/IP Server Settings](#), page 66).

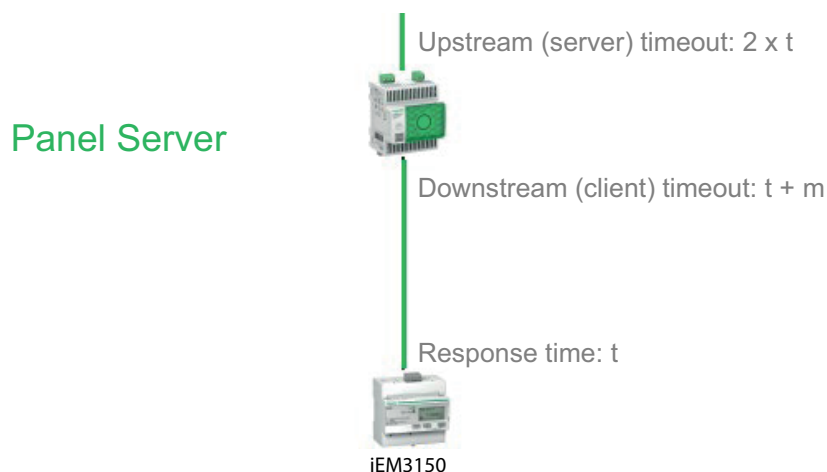
The message timeout for the Modbus client is called **Downstream timeout**, set in s (see [Modbus TCP/IP Client Settings](#), page 65).

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

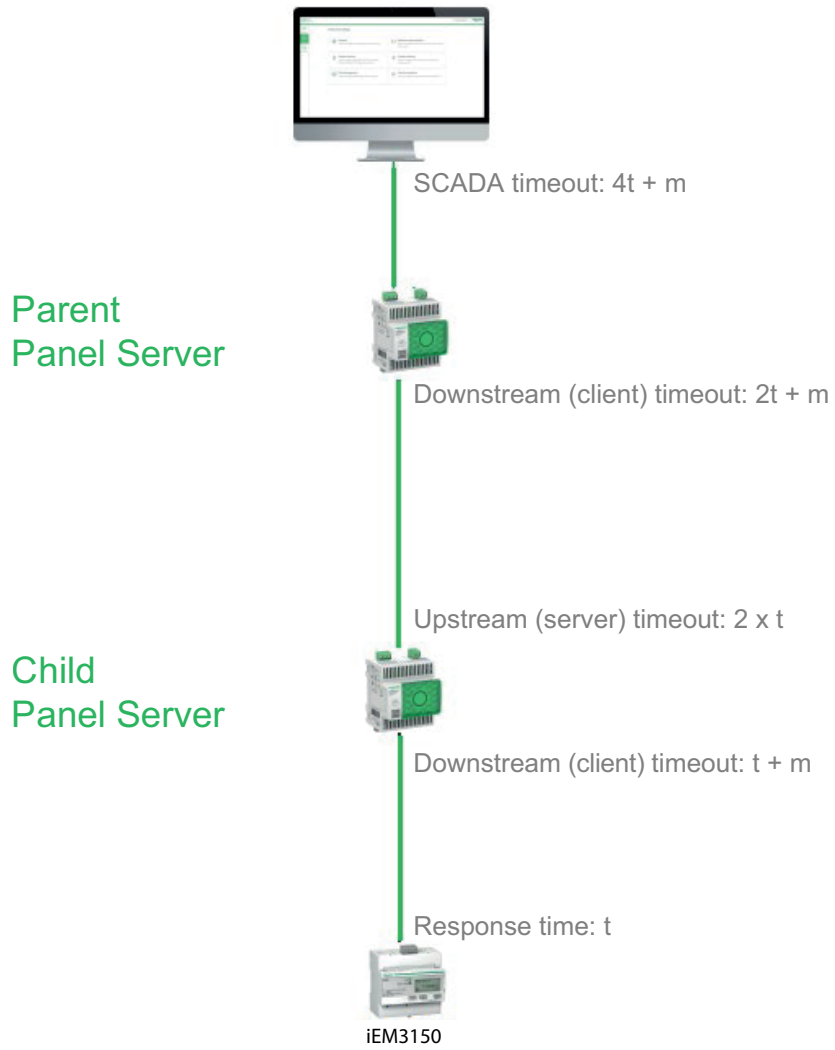
m: margin to add

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	208
Environmental Sensor Data Availability	213

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
- 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 ⁷	✓	✓	NA ⁷	✓	✓ ⁸	✓ ⁸	✓	✓ ⁸	✓	✓ ⁸	✓
Total reactive power	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Per phase reactive power	–	–	–	–	–	–	✓ ⁸	–	–	–	–	✓ ⁸	–
Total apparent power	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

7. Not applicable because there is no neutral voltage on the PowerTag Energy sensors.

8. 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	–	–	–	–	–	–	√ ⁹	–	–	–	–	√ ⁹	–
Total factor power	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Per phase factor power	–	–	–	–	–	–	√ ⁹	–	–	–	–	√ ⁹	–
Active power demand	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Active power peak demand (Resettable, page 180)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Energy

Data	PowerTag M63, PowerLogic Tag QO, PowerLogic Tag E-Frame		PowerTag P63	PowerTag F63			Power-Tag F160	PowerTag M250		PowerTag M630		PowerTag Rope, PowerLogic Tag Rope	Acti9 Active
	A1	A2	P1	F1	F2	F3	FL	M0	M1	M2	M3	R1	C
Total resettable active energy delivered	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Total non resettable active energy delivered	✓	✓	✓	✓	✓	✓	√ ⁹	✓	✓	✓	✓	√ ⁹	√ ⁹
Per phase resettable active energy delivered	–	–	–	–	–	–	√ ⁹	–	–	–	–	√ ⁹	√ ⁹
Per phase non resettable active energy delivered	–	–	–	–	–	–	√ ⁹	–	–	–	–	√ ⁹	√ ⁹
Total resettable active energy received	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Total non resettable active energy received	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Per phase resettable active energy received	–	–	–	–	–	–	√ ⁹	–	–	–	–	√ ⁹	√ ⁹
Per phase non resettable active energy received	–	–	–	–	–	–	√ ⁹	–	–	–	–	√ ⁹	√ ⁹

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	PowerTag M250		PowerTag M630		PowerTag Rope, PowerLogic Tag Rope	Acti9Active
	A1	A2	P1	F1	F2	F3	FL	M0	M1	M2	M3	R1	C
Total resettable active energy delivered and received	✓	✓	✓	✓	✓	✓	NA ¹⁰	N-A ¹⁰	N-A ¹⁰	N-A ¹⁰	N-A ¹⁰	NA ¹⁰	NA ¹⁰
Total non resettable active energy delivered and received	✓	✓	✓	✓	✓	✓	NA ¹⁰	N-A ¹⁰	N-A ¹⁰	N-A ¹⁰	N-A ¹⁰	NA ¹⁰	NA ¹⁰
Per phase resettable active energy delivered and received	-	-	-	-	-	-	NA ¹⁰	-	-	-	-	NA ¹⁰	NA ¹⁰
Per phase non resettable active energy delivered and received	-	-	-	-	-	-	NA ¹⁰	✓ ¹¹	✓	✓ ¹¹	✓	NA ¹⁰	NA ¹⁰
Total resettable reactive energy delivered	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓	✓
Total non resettable reactive energy delivered	-	-	-	-	-	-	✓ ¹¹	-	-	-	-	✓ ¹¹	✓ ¹¹
Per phase resettable reactive energy delivered	-	-	-	-	-	-	✓ ¹¹	-	-	-	-	✓ ¹¹	✓ ¹¹
Per phase non resettable reactive energy delivered	-	-	-	-	-	-	✓	-	-	-	-	✓	✓
Total resettable reactive energy received	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓	✓
Total non resettable reactive energy received	-	-	-	-	-	-	✓	-	-	-	-	✓	✓
Per phase resettable reactive energy received	-	-	-	-	-	-	✓ ¹¹	-	-	-	-	✓ ¹¹	✓ ¹¹
Per phase non resettable reactive energy received	-	-	-	-	-	-	✓ ¹¹	-	-	-	-	✓ ¹¹	✓ ¹¹
Total resettable	-	-	-	-	-	-	✓	-	-	-	-	✓	✓

10. Not applicable because energy is individually cumulated in received and delivered counters.

11. 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	PowerTag M250		PowerTag M630		PowerTag Rope, PowerLogic Tag Rope	Acti9Active
	A1	A2	P1	F1	F2	F3	FL	M0	M1	M2	M3	R1	C
apparent energy delivered and received													
Total non resettable apparent energy delivered and received	-	-	-	-	-	-	✓	-	-	-	-	✓	✓
Per phase resettable apparent energy delivered and received	-	-	-	-	-	-	✓ ¹²	-	-	-	-	✓ ¹²	✓ ¹²
Per phase non resettable apparent energy delivered and received	-	-	-	-	-	-	✓ ¹²	-	-	-	-	✓ ¹²	✓ ¹²

Alarms

Data	PowerTag M63, PowerLogic Tag QO, PowerLogic Tag E-Frame		PowerTag P63	PowerTag F63			Power-Tag F160	Power-Tag M250		PowerTag M630		PowerTag Rope, PowerLogic Tag Rope	Acti9 Active
	A1	A2	P1	F1	F2	F3	FL	M0	M1	M2	M3	R1	C
Voltage loss	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Overcurrent at voltage loss	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Load current 45%	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Load current loss	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Over voltage 120%	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Undervoltage 80%	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
RMS current on phase A, B, C at voltage loss	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

12. The values are significant only if the neutral voltage picking is connected.

Other Measurements

Data	PowerTag M63, PowerLogic Tag QO, PowerLogic Tag E-Frame		Power-Tag P63	PowerTag F63			Power-Tag F160	Power-Tag M250		PowerTag M630		PowerTag Rope, Power-Logic Tag Rope	Acti9 Active
	A1	A2	P1	F1	F2	F3	FL	M0	M1	M2	M3	R1	C
Phase current (measured)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Neutral current (calculated)	–	–	–	–	–	–	✓	–	–	–	–	✓	
Phase-to-phase voltage	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Phase-to-neutral voltage	✓	NA ¹³	✓	✓	NA ¹³	✓	✓ ¹⁴	✓ ¹⁴	✓	✓ ¹⁴	✓	✓	✓ ¹⁴
Frequency	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	
Quadrant	1	1	1	1	1	1	4	4	4	4	4	4	
Internal temperature	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓	✓
Load operating time counter	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

13. Not applicable because there is no neutral voltage on the PowerTag Energy sensors

14. The values are significant only if the neutral voltage picking is connected.

Environmental Sensor Data Availability

Presentation

The data transmitted by the environmental sensors to the Panel Server depends on the type of environmental sensor. The following 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 sensors are:

- CL110 (Contact your Schneider Electric representative for information about commercial references.)
- TH110 (Contact your Schneider Electric representative for information about commercial references.)
- 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	✓	✓	✓	✓
Ambient humidity	✓	–	✓	✓
Ambient CO ₂ level	–	–	–	✓

For a full list of measurements transmitted by environmental sensors, refer to DOCA0241EN *EcoStruxure Panel Server - Modbus File*.

Appendix C: Wireless Device Network Indicators

The following table describes the network indicators of wireless devices.

Information type	Description
RSSI	Displays the power level of the wireless signal. <ul style="list-style-type: none">• Good: 0 to -65 dbm• Average: -65 to -75 dbm• Poor (with risk of outage): < -75 dbm
LQI	Displays the measurement of the strength and/or the quality of the received frames. NOTE: It is recommended to use this indicator as the main indicator of acceptance.
PER	Displays the ratio of the packet that does 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: <ul style="list-style-type: none">• Device indicator: provided by the device.• Panel Server indicator: calculated over a 10-minute sliding window, and refreshed every 30 seconds.• Link indicator: displays the higher of the two previous indicators.

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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 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": {
    "remoteld": "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 Panel Server provides secure SFTP data publication based on the following elements:

Key Exchange

- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

Cipher

- blowfish-cbc
- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr
- 3des-ctr
- arcfour
- arcfour128
- arcfour256

Appendix F: Certificate Authorities

- actalisauthenticationrootca
- addtrustclass1ca
- addtrustexternalca
- addtrustqualifiedca
- affirmtrustcommercialca
- affirmtrustnetworkingca
- affirmtrustpremiumca
- affirmtrustpremiumeccca
- amazonrootca1
- amazonrootca2
- amazonrootca3
- amazonrootca4
- baltimorecybertrustca
- buypassclass2ca
- buypassclass3ca
- camerfirmachambersca
- camerfirmachamberscommerceca
- camerfirmachamberssignca
- 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_esign_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
- comodoecca
- comodorsaca
- digicertassuredidg2
- digicertassuredidg3
- digicertassuredidrootca
- digicertglobalrootca
- digicertglobalrootg2
- digicertglobalrootg3
- digicerthighassuranceevrootca
- digicertrustedrootg4
- 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
- swissigngoldg2ca
- swissignplatinumg2ca
- swissignsilverg2ca
- teliasonerarootcav1
- thawtepremiumserverca
- thawteprimaryrootca
- thawteprimaryrootcag2
- thawteprimaryrootcag3
- ttelesecglobalrootclass2ca
- ttelesecglobalrootclass3ca
- usertrustecca
- usertrustsaca
- verisignclass2g2ca
- verisignclass3ca

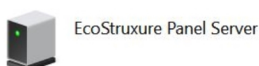
- verisignclass3g2ca
- verisignclass3g3ca
- verisignclass3g4ca
- verisignclass3g5ca
- verisigntsaca
- verisignuniversalrootca
- xrampglobalca

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.

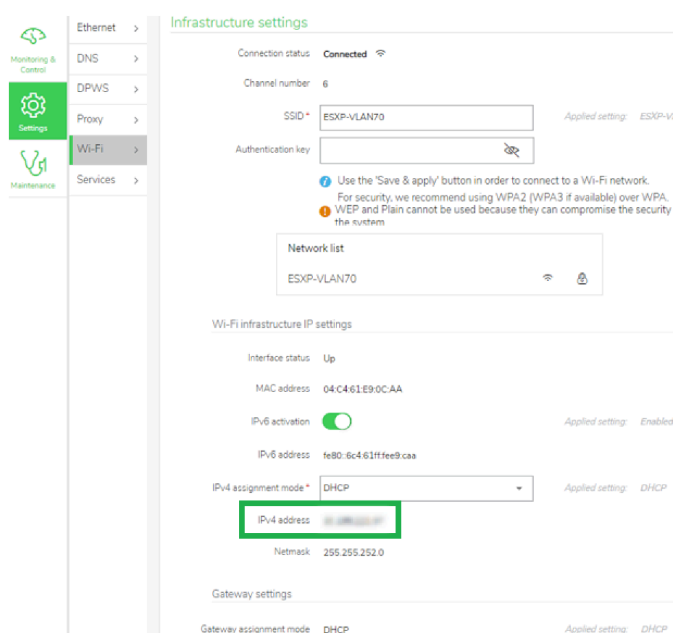
Result: The EcoStruxure Panel Server icon that displays under **Network** is as follows:



5. Double-click the EcoStruxure Panel Server icon.

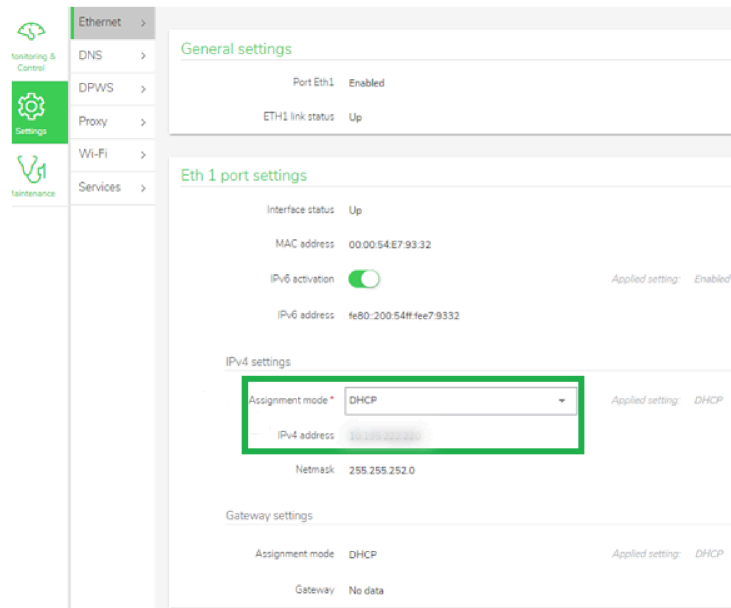
Result: The Panel Server webpages open.

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.

- At **Settings > Network configuration > Ethernet > Eth 1 port settings**, retrieve the DHCP IP address, as indicated in the following screenshot:



- Return to Panel Server webpages at **Settings > Network configuration** to deactivate the Wi-Fi.
- Disconnect your PC from your smartphone Wi-Fi network and switch off the Wi-Fi access point on your smartphone.

Glossary

A

Aggregated data :

Integrated data which is summed up in order to present a view. It is applicable only in the **Home** and **Trending** menus

C

Continuous data: A measurement, for example Active power A, Apparent power C, Temperature.

Custom model: Panel Server supports several native device models. It is also possible to create and import a custom model 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. The custom model is defined using the EPC Web tool.

D

Data publication: The sampled data can be exported to a dedicated server.

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.

E

EWP: EcoStruxure Panel Server embedded webpages

H

Hardware version:

The new models of EcoStruxure Panel Server, PAS600LWD and PAS600PWD are released with hardware version 002.000.000 (HW: V02).

To identify the hardware version of your device, use one of the following methods:

- On the front face of the product check the laser marking which includes the MAC ID and serial number of the device. For hardware version 002.000.000 devices, an additional line indicates HW: V02.
- On the Panel Server webpages, navigate to **Settings > General > Identification** or to **Maintenance > Firmware update**. Check the **Hardware revision** line for the hardware version of your device.

I

IEEE 802.15.4: Standard defined by the IEEE and used by the EcoStruxure Panel Server to communicate with wireless devices.

Integrated data: A measurement calculated over a period of time, for example Reactive energy received measured in KWh. Available for Energy only.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

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

© 2024 – Schneider Electric. All rights reserved.

DOCA0172EN-13