Enerlin'X IFE

Ethernet Switchboard Server

User Guide

DOCA0084EN-11
05/2024

Schneider Electric

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

Cybersecurity Safety Notice

> ### ⚠ WARNING
>
> **POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY**
>
> - Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.
> - Disable unused ports/services and default accounts to help minimize pathways for malicious attackers.
> - Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
> - Use cybersecurity best practices (for example, least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, or interruption of services.
>
> **Failure to follow these instructions can result in death, serious injury, or equipment damage.**

About the Book

Document Scope

The aim of this document is to provide the users, installers, and the maintenance personnel with the technical information and procedure needed to access and maintain the IFE Ethernet switchboard server webpages.

Validity Note

This guide is valid for the IFE server for use with:

- MasterPacT™ MTZ circuit breakers (with MicroLogic X control unit)
- MasterPacT™ NT/NW circuit breakers
- ComPacT™ NS 1600b - 3200 circuit breakers
- ComPacT™ NS 630b - 1600 circuit breakers
- PowerPacT™ P- and R-frame circuit breakers (with MicroLogic A/E/P/H trip unit)
- ComPacT™ NSX circuit breakers (with MicroLogic 5/6/7 trip unit)
- PowerPacT™ H-, J-, and L-frame circuit breakers (with MicroLogic 5/6 trip unit)

  NOTE:

  - The information related to the new generation of ComPacT NS and PowerPacT P- and R-frame circuit breakers in this guide applies to ComPact NS and PowerPact P- and R-frame circuit breakers also. The exceptions are mentioned wherever applicable.

    The new ComPacT NS and PowerPacT P- and R-frame ranges are based on the same technical and dimensional architecture as that of ComPact NS and PowerPact P- and R-frame circuit breakers. The electrical and mechanical performances of these ranges are identical.

  - The information related to the new generation of ComPacT NSX and PowerPacT H-, J-, and L--frame circuit breakers in this guide applies to ComPact NSX and PowerPact H-, J-, and L-frame circuit breakers also. The exceptions are mentioned wherever applicable.

    The new ComPacT NSX and PowerPacT H-, J-, and L-frame ranges are based on the same technical and dimensional architecture as that of ComPact NSX and PowerPact H-, J-, and L-frame circuit breakers. The electrical and mechanical performances of these ranges are identical.

Online Information

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

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/

Related Documents for IEC Devices

Title of Documentation	Reference Number
Enerlin'X IFE - Ethernet Switchboard Server - Instruction Sheet	QGH13473
Enerlin'X IFE Server Firmware Release Note	DOCA0148EN
ULP System (IEC Standard) - User Guide	DOCA0093EN DOCA0093ES DOCA0093FR DOCA0093ZH
MasterPacT MTZ Modbus Communication Guide	DOCA0105EN DOCA0105ES DOCA0105FR DOCA0105ZH
MasterPacT NT/NW, ComPacT NS Modbus Communication Guide	DOCA0054EN DOCA0054ES DOCA0054FR DOCA0054ZH
ComPacT NS Modbus Communication Guide	DOCA0220EN DOCA0220ES DOCA0220FR DOCA0220ZH
ComPacT NSX Modbus Communication Guide	DOCA0213EN DOCA0213ES DOCA0213FR DOCA0213ZH
Enerlin'X IO Input/Output Application Module (IEC Standard) - User Guide	DOCA0055EN DOCA0055ES DOCA0055FR DOCA0055ZH
MasterPacT, ComPacT, PowerPacT - Cybersecurity Guide	DOCA0122EN DOCA0122ES DOCA0122FR DOCA0122ZH
EcoStruxure Cybersecurity Admin Expert Guide	CAE_UM_EN

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

Related Documents for UL/ANSI Devices

Title of Documentation	Reference Number
Enerlin'X IFE - Ethernet Switchboard Server - Instruction Sheet	QGH13473
Enerlin'X IFE Server Firmware Release Note	DOCA0148EN
ULP System (UL Standard) - User Guide	0602IB1503EN 0602IB1504ES 0602IB1505FR 0602IB1506ZH
MasterPacT MTZ Modbus Communication Guide	DOCA0105EN

Title of Documentation	Reference Number
	DOCA0105ES DOCA0105FR DOCA0105ZH
MasterPacT NT/NW, PowerPacT P- and R-frame Modbus Communication Guide	0613IB1313EN 0613IB1314ES 0613IB1315FR 0613IB1316ZH
PowerPacT H-, J-, and L-Frame Modbus Communication Guide	0611IB1302EN 0611IB1303ES 0611IB1304FR 0611IB1305ZH
Enerlin'X IO Input/Output Application Module (UL Standard) - User Guide	0613IB1317EN 0613IB1318ES 0613IB1319FR 0613IB1320ZH
MasterPacT MTZ - Cybersecurity Guide	DOCA0122EN DOCA0122ES DOCA0122FR DOCA0122ZH
EcoStruxure Cybersecurity Admin Expert Guide	CAE_UM_EN

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

IFE Server Presentation

What's in This Part

Introduction

Overview

The IFE Ethernet switchboard server (or IFE server) enables an intelligent modular unit (IMU) with a ComPacT, PowerPacT, or MasterPacT circuit breaker to be connected to an Ethernet network. Each circuit breaker has its own IFE server and a corresponding IP address.

NOTE: The IFE server with part number LV434002 completely replaces the IFE server with part number LV434011. The part number LV434002 comes with the Real Time Clock (RTC) feature and allows ULP connections up to 20 m (65.6 ft). The part number LV434011 had a theoretical limitation of 5 m (16.4 ft) over the life of the IFE server.

The IFE server with part number LV434002 is an Ethernet switchboard server for ComPacT, PowerPacT, and MasterPacT circuit breakers and a Modbus client for Modbus-SL (serial line) connected devices.

IFE Server Features

The main features of IFE server are:

- Dual 10/100 Mbps Ethernet port for simple daisy chain connection
- Device profile web service for discovery of the IFE server on the local area network (LAN)
- ULP compliant for location of the IFE server in the switchboard
- Ethernet interface for ComPacT, PowerPacT, and MasterPacT circuit breakers
- Server for Modbus-SL connected devices
- Embedded setup webpages
- Embedded monitoring webpages
- Embedded control webpages
- Built-in email alarm notification for circuit breaker connected to IFE server.

  NOTE: The built-in switch of IFE server does not support the ring topology as it does not have the feature of the loop back protection.

IFE Firmware Versions

This guide describes the webpages for two different firmware versions of IFE server:

- , describes the IFE server webpages for the firmware version 005 and later.
- , describes the IFE server webpages for the firmware versions up to 003.

IFE Server Supported Protocols

The IFE server supports the following Ethernet protocols:

- **Modbus TCP/IP:** Is a protocol, which provides client/server communication between devices and TCP/IP that provides communications over an Ethernet connection. Modbus TCP/IP is used to exchange data between IFE server and other compatible Modbus TCP/IP devices through TCP port 502.

- **Secure Modbus TCP/IP:** is a secure protocol, which provides client/server communication between devices and TCP/IP that provides communications over an Ethernet connection. Secure Modbus TCP/IP is used to exchange data between IFE server and other compatible Modbus TCP/IP devices through TCP port configured by user through IFE webpage. By default this protocol will be disabled.

- **Hypertext Transfer Protocol (HTTP):** HTTP is a network protocol that handles delivery of files and data on the World Wide Web (WWW). It provides web server functionality through TCP port 80. Remote configuration of IFE server and viewing of diagnostic data is possible using a web browser.

- **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 Transport Layer Security (TLS) protocol connection. HTTPS enables encrypted communication and secure connection between a remote user and the IFE server.

- **File Transfer Protocol Secure (FTPS):** FTPS is a variant of the standard File Transfer Protocol (FTP) that adds a layer of security on the data in transit through a TLS protocol connection. FTPS enables encrypted communication and secure connection between a remote user and the IFE server.

- **Simple Network Management Protocol (SNMP):** Based on MIB2 format, SNMP provides the ability to store and send identifying and diagnostic information used for network management purposes through UDP port 161.

- **Rapid Spanning Tree Protocol (RSTP EcoStruxure Power Commission Software):** RSTP is a network protocol that ensures a loop-free topology for Ethernet networks. It is the advanced version of Spanning Tree Protocol, is a link layer protocol executed within bridges or switches.

- **Devices Profile for Web Services (DPWS):** DPWS defines a minimal set of implementation constraints to enable secure web service messaging, discovery, description, and eventing on resource-constrained devices.

- **Network Time Protocol (NTP):** NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

- **IEC 61850 Protocol:** IEC 61850 is a standard for communication networks and systems in substations. Based on Ethernet protocol, it is a standardized method of communication developed to support integrated systems, composed of multi-vendor, self-describing IEDs (Intelligent Electronic Devices) that are networked together to perform real-time protection, control, measurement, and monitoring functions.

   NOTE: IEC 61850 protocol is compatible with IFE server only if the MasterPacT MTZ circuit breaker with MicroLogic X control unit is connected directly to IFE server. IEC 61850 protocol is not compatible with IFE server if the MasterPacT MTZ circuit breaker is connected under an IFM interface stacked to the IFE server.

   NOTE: HTTPS, FTPS, RSTP, NTP, and IEC 61850 protocols are applicable only from IFE server firmware version 005.001.000.

Intelligent Modular Unit

Definition

A modular unit is a mechanical and electrical assembly containing one or more products to perform a function in a switchboard (incoming protection, motor command, and control).

The circuit breaker with its internal communicating components (MicroLogic control unit or MicroLogic trip unit) and external ULP modules (IO module) connected to one communication interface is called an Intelligent Modular Unit (IMU).

An IMU is composed around a circuit breaker from the following ranges:

- MasterPacT MTZ circuit breakers
- MasterPacT NT/NW circuit breakers
- ComPacT NS 1600b-3200 circuit breakers
- ComPacT NS 630b-1600 circuit breakers
- PowerPacT P- and R- frame circuit breakers
- ComPacT NSX circuit breakers
- PowerPacT H-,J-, and L- frame circuit breakers

ULP Modules Per Circuit Breaker Range

The following table lists the compatible ULP modules for each range of circuit breakers.

ULP Module	Part Number	MasterPacT MTZ with ULP Port Module and MicroLogic X Control Unit	MasterPacT NT/NW or ComPacT or PowerPacT P- and R-Frame with BCM ULP Module and MicroLogic Trip Unit	ComPacT NSX or PowerPacT H-, J-, and L-frame with BSCM or BSCM Modbus SL/ULP Module and/or MicroLogic Trip Unit
IFE Ethernet interface for one circuit breaker	LV434001 LV434010	✓	✓	✓
IFE Ethernet switchboard server	LV434002 LV434011	✓	✓	✓
EIFE Embedded Ethernet interface for one MasterPacT MTZ drawout circuit breaker	LV851001	✓	–	–
Spare part kit EIFE for one MasterPacT MTZ1 drawout circuit breaker	LV851100SP	✓	–	–
Spare part kit EIFE for one MasterPacT MTZ2/MTZ3 drawout circuit breaker	LV851200SP	✓	–	–
IFM Modbus-SL interface for one circuit breaker	TRV00210 STRV00210	–	✓	✓
IFM Modbus-SL interface for one circuit breaker	LV434000	✓	✓	✓
FDM121 front display module for one circuit breaker	TRV00121 STRV00121	–	✓	✓

ULP Module	Part Number	MasterPacT MTZ with ULP Port Module and MicroLogic X Control Unit	MasterPacT NT/NW or ComPacT or PowerPacT P- and R-Frame with BCM ULP Module and MicroLogic Trip Unit	ComPacT NSX or PowerPacT H-, J-, and L-frame with BSCM or BSCM Modbus SL/ULP Module and/or MicroLogic Trip Unit
IO input/output application module for one circuit breaker	LV434063	✓	✓	✓
USB maintenance interface or Universal Test Adapter (UTA) module	TRV00911 STRV00911	–	✓	✓

For more information on the ULP System and its components, refer to the *ULP System User Guides* in Related Documents, page 7.

Communication Architecture
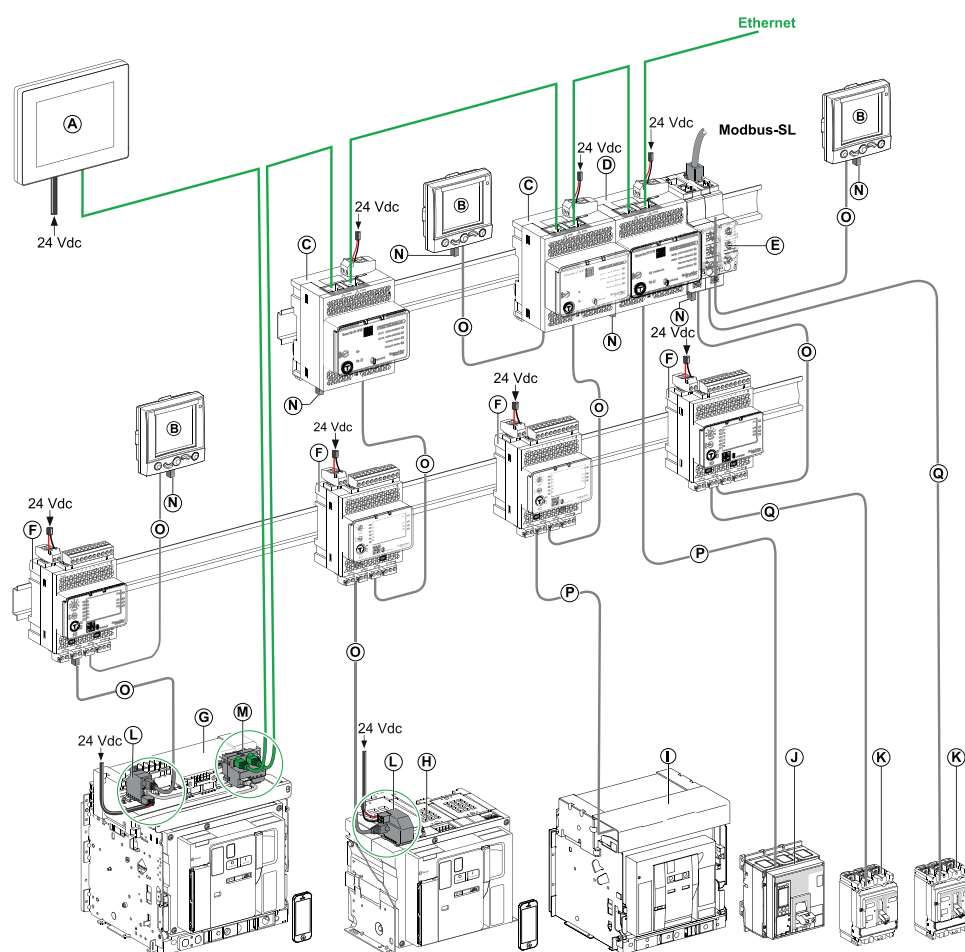
A   FDM128 Ethernet display for eight devices

B   FDM121 front display module for one circuit breaker

C   IFE Ethernet interface for one circuit breaker

D   IFE Ethernet switchboard server

E   IFM Modbus-SL interface for one circuit breaker

F   IO input/output application module for one circuit breaker

G   MasterPacT MTZ1 or MTZ2/MTZ3 drawout circuit breaker

H   MasterPacT MTZ1 or MTZ2/MTZ3 fixed circuit breaker

I   MasterPacT NT/NW circuit breaker

J   ComPacT NS/PowerPacT M-,P,- and R-frame circuit breaker

K   ComPacT NSX/PowerPacT H-, J-, and L-frame circuit breaker

L   ULP port module

M   EIFE Embedded Ethernet Interface for one MasterPacT MTZ drawout circuit breaker

N   ULP line termination

O   RJ45 plug/plug ULP cord

P   Circuit breaker BCM ULP cord

Q   NSX cord

Remote Controller

A remote controller is a device that is able to communicate with an IMU using a communication interface, such as the IFE server. For example, FDM128 Ethernet display for eight devices, supervisor, PLC, BMS, SCADA system, and so on, are remote controllers.

For more information on Modbus registers and commands, refer to the *Modbus Communication Guides* in Related Documents, page 7.

Hardware Description

Description
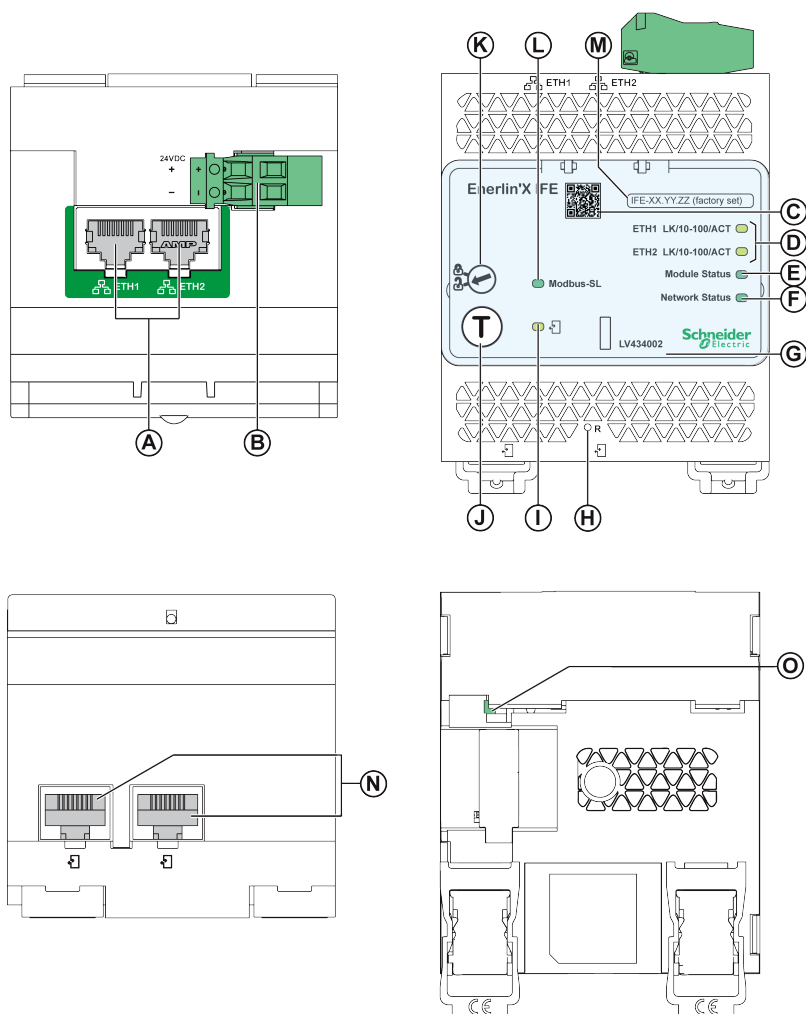
A   Ethernet 1 and Ethernet 2 RJ45 communication ports

B   24 Vdc power supply terminal block

C   QR code to product information

D   Ethernet communication LEDs

E   Module status LED

F   Network status LED

G   Sealable transparent cover

H   Reset button

I   ULP status LED

J   Test button (accessible even with closed cover)

K   Locking pad

L   Modbus traffic status LED (IFE server only)

M   Device name label

N   Two RJ45 ULP ports

0   Grounding connection

For information on installation, refer to the instruction sheet available on the Schneider Electric website: QGH13473.

Mounting

The IFE server mounts on a DIN rail. The stacking accessory enables the connection of several IFM interfaces to an IFE server without additional wiring.

Power Supply

The IFE server must always be supplied with 24 Vdc. The power to the IFM interfaces stacked to an IFE server are supplied by the IFE server and it is not necessary to supply power to them separately.

It is recommended to use an UL listed and recognized limited voltage or limited current or a class 2 power supply with a 24 Vdc, 3 A maximum.

> **NOTE:** For 24 Vdc power supply connection, use copper conductors only.
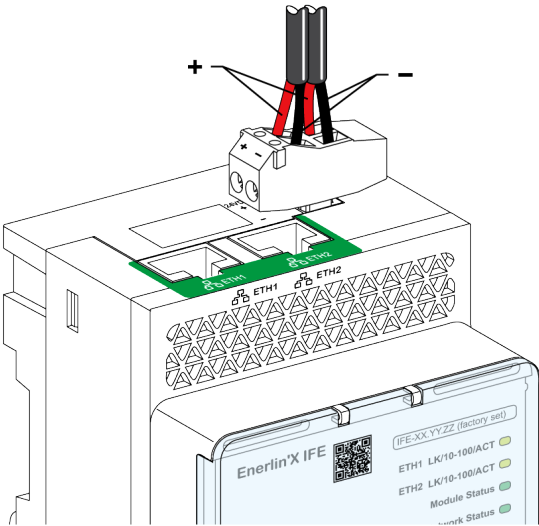
Ethernet Communication LEDs

The Ethernet communication dual color LEDs, indicate the status of the Ethernet ports **ETH1** and **ETH2**.

LED Indication	Status Description
OFF	No power or no link
Steady yellow	10 Mbps, link established, and no activity
Blinking yellow	10 Mbps, ongoing activity
Steady green	100 Mbps, link established, and no activity
Blinking green	100 Mbps, ongoing activity

Module Status LED

The module status dual color LED, indicates the IFE server status.

LED Indication	Status Description	Action
OFF	No power	None
Steady green	IFE server operational	None
Blinking green (250 ms ON, 250 ms OFF)	Hidden control webpage available	None
Blinking green (500 ms ON, 500 ms OFF)	IFE server firmware corrupted	Contact your local Schneider Electric service team for support.
Blinking red (500 ms ON, 500 ms OFF)	IFE server in degraded mode	Replace ULP module at the next maintenance operation.
Steady red	IFE server out of service	None
Blinking green/red (1 s green, 1 s red)	Firmware update in progress	None
Blinking green/red (250 ms green, 250 ms red)	Self-test in progress	None

Network Status LED

The network status dual color LED, indicates the Ethernet network status.

LED Indication	Status Description
OFF	No power or no IP address
Steady green	Valid IP address
Steady red	Duplicated IP address
Blinking green/red (250 ms green, 250 ms red)	Self-test in progress
Steady amber	Error in IP configuration

Modbus Serial Line Traffic LED

The Modbus serial line traffic yellow LED, indicates that the traffic is being transmitted or received over the Modbus serial line network through the IFE server.

The LED is ON during the transmission and reception of the messages. The LED is OFF otherwise.

Modbus Address

The IFE server accepts the Modbus address of the IMU to which it is connected.

The Modbus address is 255 and cannot be changed.

Locking Pad

The locking pad on the front panel of the IFE server enables or disables the ability to send the remote control commands over the Ethernet network to the IFE server, and to the other modules of the IMU.
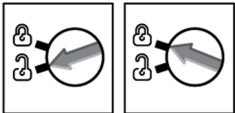
- If the arrow points to the open padlock (factory setting), remote control commands are enabled.

- If the arrow points to the closed padlock, remote control commands are disabled.

  The only remote control command that is enabled even if the arrow points to the closed padlock, is the set absolute time command.

Test Button

The test button has two functions, according to the duration of the button pressed.

Time Range	Function
1–5 s	Tests the connection between all the ULP modules for 15 s.
10–15 s	Activates the hidden configuration mode. **NOTE:** The hidden configuration is not activated if the button is pressed for more than 15 s.

Reset Button

When the reset button is pressed for 1–5 s, it forces the IP acquisition mode to the factory default setting (DHCP).

ULP Status LED

The yellow ULP status LED describes the mode of the ULP module.

ULP LED	Mode	Action
	Nominal	None
	Conflict	Remove extra ULP module
	Degraded	Replace ULP module at the next maintenance operation
	Test	None
	Non-critical firmware discrepancy	Use EcoStruxure Power Commission software to check the firmware and hardware compatibility and follow the recommended actions
	Non-critical hardware discrepancy	
	Configuration discrepancy	Install missing features

ULP LED	Mode	Action
	Critical firmware discrepancy	Use EcoStruxure Power Commission software to check the firmware and hardware compatibility and follow the recommended actions
	Critical hardware discrepancy	
	Stop	Replace ULP module
	Power OFF	Check power supply

EcoStruxure Power Commission Software

Overview

EcoStruxure ™ Power Commission software helps you to manage a project as part of testing, commissioning, and maintenance phases of the project life cycle. The innovative features in it provide simple ways to configure, test, and commission the smart electrical devices.

EcoStruxure Power Commission software automatically discovers the smart devices and allows you to add the devices for an easy configuration. You can generate comprehensive reports as part of Factory Acceptance Test and Site Acceptance Test to replace your heavy manual work. Additionally, when the panels are under operation, any change of settings made can be easily identified by a yellow highlighter. This indicates the difference between the project and device values, and hence provides a system consistency during the operation and maintenance phase.

EcoStruxure Power Commission software enables the configuration of the following circuit breakers, modules, and accessories:

Circuit breaker ranges	Modules	Accessories
MasterPacT MTZ circuit breakers	• MicroLogic X control units • Communication interface modules: IFM interface, IFE interface, IFE server, and EIFE interface • ULP modules: IO module	M2C output module
• MasterPacT NT/NW circuit breakers • ComPacT NS circuit breakers • PowerPacT P- and R-frame circuit breakers	• MicroLogic trip units • Communication interface modules: BCM module, CCM module, BCM ULP module, IFM interface, IFE interface, IFE server • ULP modules: IO module, FDM121 display [1]	M2C and M6C output modules
• ComPacT NSX circuit breakers • PowerPacT H-, J- and L-frame circuit breakers	• MicroLogic trip units • Communication interface modules: BSCM or BSCM Modbus SL/ULP module, IFM interface, IFE interface, IFE server • ULP modules: IO module, FDM121 display [1]	SDTAM and SDx output modules

For more information, refer to the *EcoStruxure Power Commission Online Help*.

Click here to download the latest version of EcoStruxure Power Commission.

---

1.   For FDM121 display, only the firmware and language download are supported.

Key Features

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

- Create projects by device discovery
- Save the project in the EcoStruxure Power Commission cloud for reference
- Upload settings to the device and download settings from the device
- Compare the settings between the project and the device
- Perform control actions in a secured way
- Generate and print the device settings report
- Perform a communication wiring test on the entire project and generate and print test report
- View the communication architecture between the devices in a graphical representation
- View the measurements, logs, and maintenance information
- Export Waveform Capture on Trip Event (WFC)
- View the status of device and IO module
- View the alarm details
- Buy, install, remove, or retrieve the Digital Modules
- Check the system firmware compatibility status
- Update to the latest device firmware
- Perform force trip and automatic trip curve tests

Schematics with MasterPacT MTZ Circuit Breakers

Description

The IFE server is connected to the MasterPacT MTZ circuit breaker with MicroLogic X control unit through its ULP port module.

For more information on the ULP System and its components, refer to the *ULP System User Guides* in Related Documents, page 7.

ULP Connection

NOTICE
HAZARD OF EQUIPMENT DAMAGE
• Never connect an Ethernet device to an RJ45 ULP port.
• The RJ45 ULP ports of IFE server are for ULP modules only.
• Any other use can damage the IFE server or the device connected to the IFE server.
• To check if an ULP module is compatible with the RJ45 ULP ports of IFE server, refer to the *ULP System User Guides* in Related Documents, page 7.
Failure to follow these instructions can result in equipment damage.

All the connection configurations require the RJ45 plug/plug ULP cord.

When the second RJ45 ULP port is not used, it must be closed with an ULP line termination.
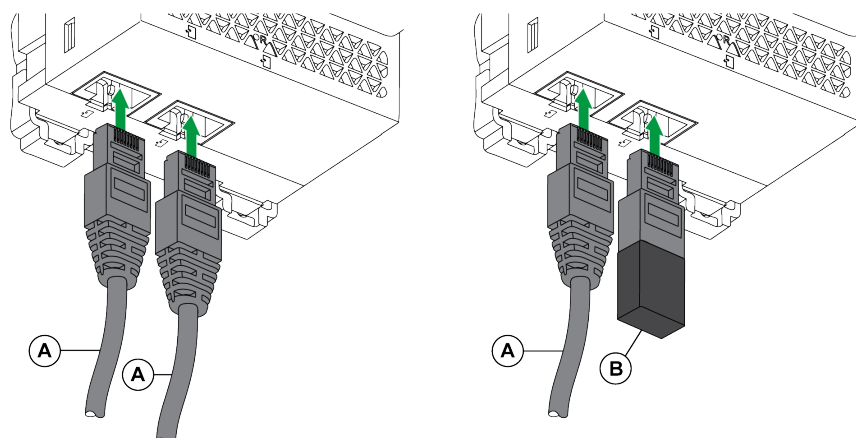
A   RJ45 plug/plug ULP cord

B   ULP line termination

Connection of the IFE Server to a MasterPacT MTZ Circuit Breaker with MicroLogic X Control Unit

Connect the IFE server to the ULP port module on a MasterPacT MTZ circuit breaker with MicroLogic X control unit by using the ULP cord.
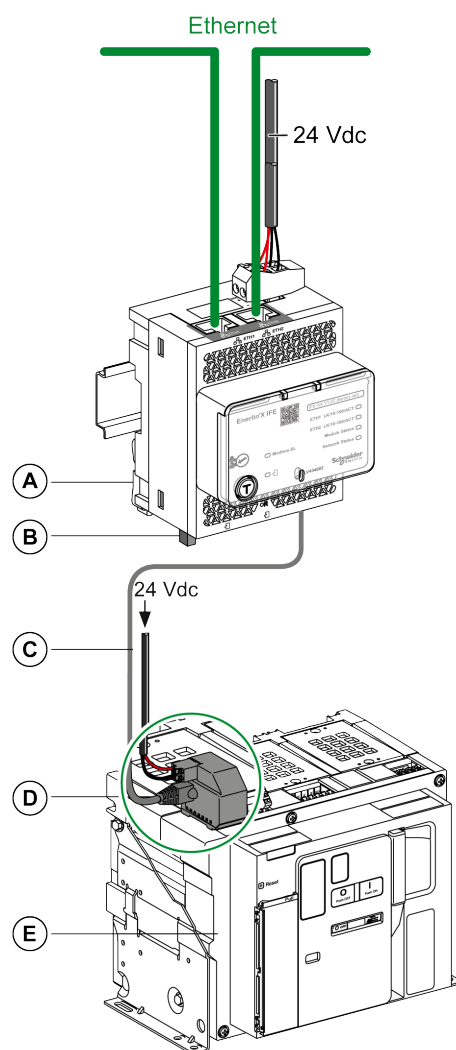
A   IFE Ethernet switchboard server

B   ULP line termination

C   RJ45 plug/plug ULP cord

D   ULP port module

E   MasterPacT MTZ fixed circuit breaker with MicroLogic X control unit

Schematics with MasterPacT NT/NW, ComPacT NS, PowerPacT P- and R-Frame Circuit Breakers

Description

Depending on the type of circuit breaker used, connect the IFE server to the circuit breaker using one of the following configurations:

- Connection of the IFE server to a fixed manually-operated circuit breaker with a BCM ULP module:
  - ComPacT NS 630b-3200 circuit beakers
  - PowerPacT P- or R-Frame circuit breakers
- Connection of the IFE server to a fixed electrically-operated circuit breaker with a BCM ULP module:
  - MasterPacT NT/NW circuit beakers
  - ComPacT NS 630b-1600 circuit beakers
  - PowerPacT P-Frame circuit breakers
- Connection of the IFE server to a drawout circuit breaker with a BCM ULP module and its respective IO module:
  - MasterPacT NT/NW circuit beakers
  - ComPacT NS 630b-1600 circuit beakers
  - PowerPacT P-Frame circuit breakers

For more information on the ULP System and its components, refer to the *ULP System User Guides* in Related Documents, page 7.

ULP Connection

<table>
<tr><td colspan="2" align="center">NOTICE</td></tr>
<tr><td colspan="2">HAZARD OF EQUIPMENT DAMAGE

- Never connect an Ethernet device to a RJ45 ULP port.
- The RJ45 ULP ports of IFE server are for ULP modules only.
- Any other use can damage the IFE server or the device connected to the IFE server.
- To check if a ULP module is compatible with the RJ45 ULP ports of IFE server, refer to the *ULP System User Guides* in Related Documents, page 7.

Failure to follow these instructions can result in equipment damage.</td></tr>
</table>

All connection configurations require the BCM ULP cord.

When the second RJ45 ULP port is not used, it must be closed with a ULP line termination.
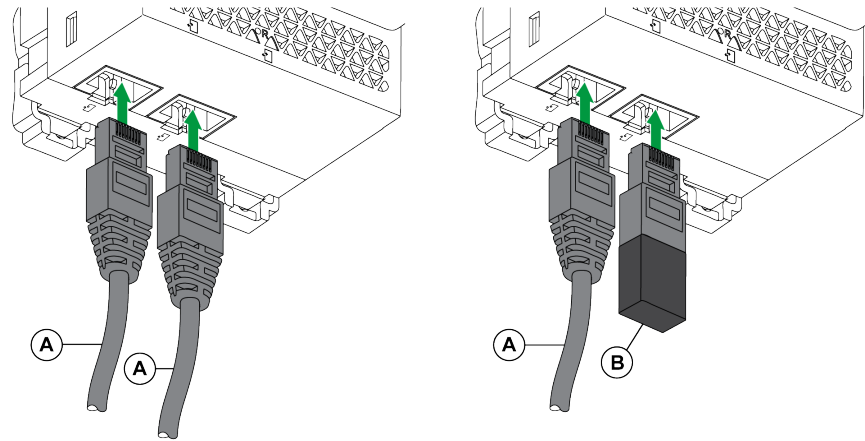
A Circuit breaker BCM ULP cord or RJ45 plug/plug ULP cord

B ULP line termination

Connection of the IFE Server to a Fixed Manually-Operated Circuit Breakers

Applicable for:

- ComPacT NS 630b-3200 circuit beakers
- PowerPacT P- or R-Frame circuit
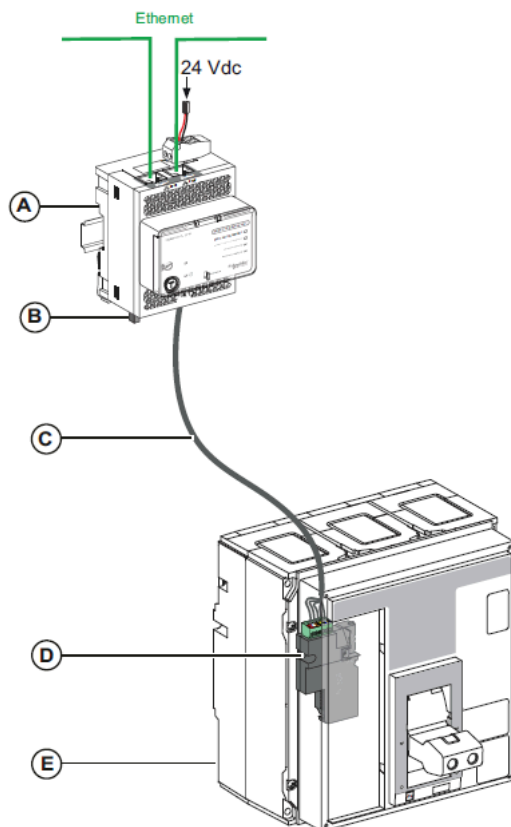
A	IFE Ethernet switchboard server
B	ULP line termination
C	Circuit breaker BCM ULP cord
D	BCM ULP circuit breaker communication module
E	Fixed manually-operated circuit breaker

Connection of the IFE Server to a Fixed Electrically-Operated Circuit Breakers

Applicable for:

- MasterPacT NT/NW circuit beakers
- ComPacT NS 630b-1600 circuit beakers
- PowerPacT P-Frame circuit breakers
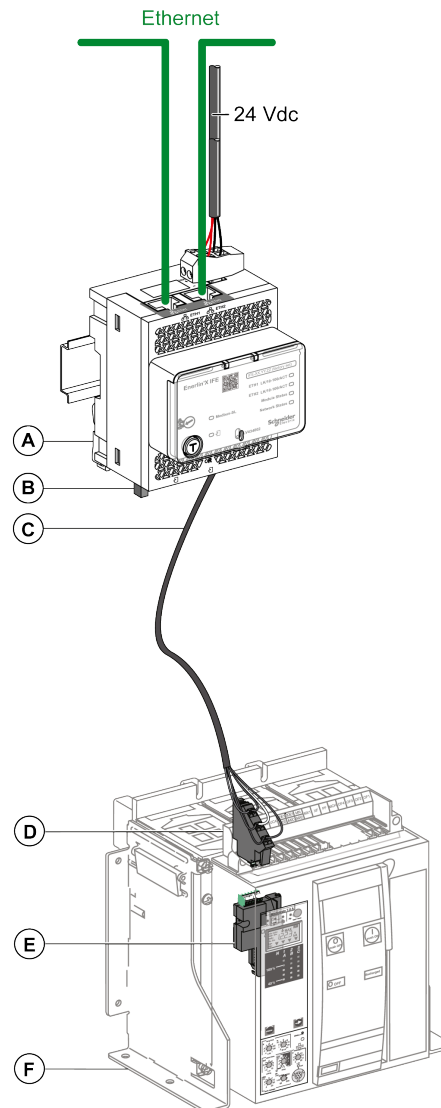
A	IFE Ethernet switchboard server
B	ULP line termination
C	Circuit breaker BCM ULP cord
D	Fixed terminal block
E	BCM ULP circuit breaker communication module
F	Fixed electrically-operated circuit breaker

Connection of the IFE Server to the Drawout Circuit Breakers

Applicable for:

- MasterPacT NT/NW circuit beakers
- ComPacT NS 630b-1600 circuit beakers
- PowerPacT P-Frame circuit breakers
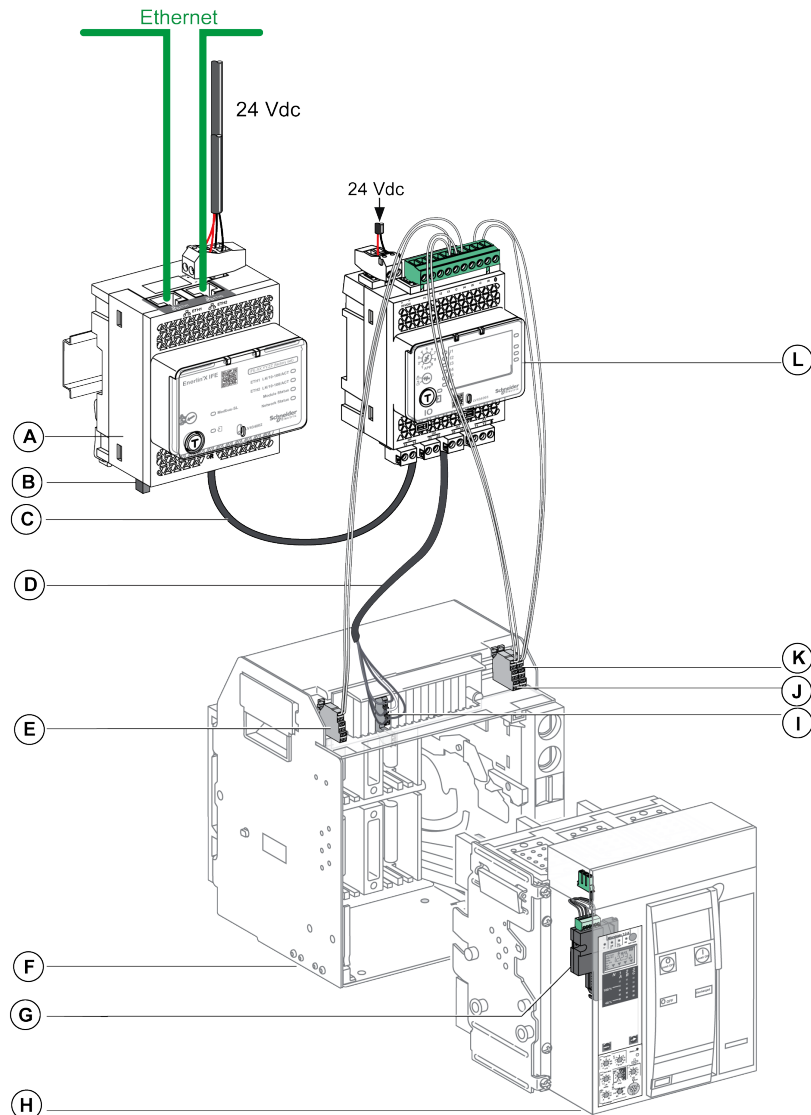
A	IFE Ethernet switchboard server
B	ULP line termination
C	RJ45 plug/plug ULP cord
D	Circuit breaker BCM ULP cord
E	Circuit breaker disconnected position contact (CD)
F	Circuit breaker cradle
G	BCM ULP circuit breaker communication module
H	Drawout circuit breaker
I	Drawout terminal block
J	Circuit breaker connected position contact (CE)
K	Circuit breaker test position contact (CT)
L	IO input/output application module for one circuit breaker

Schematics with ComPacT NSX and PowerPacT H-, J-, and L-Frame Circuit Breakers

General Description

Depending on the configuration of the ComPacT NSX and PowerPacT H-, J-, and L-Frame circuit breakers, connect the IFE server to the circuit breaker using one of the following configurations:

- Connection of the IFE server to the MicroLogic trip unit
- Connection of the IFE server to the BSCM module
- Connection of the IFE server to the BSCM module and to the MicroLogic trip unit

For more information on the ULP System and its components, refer to the *ULP System User Guides* in Related Documents, page 7.

ULP Connection

| ⚠ **WARNING** |
|---|
| **HAZARD OF ELECTRIC SHOCK** |
| For system voltage greater than 480 Vac: |
| • Use the insulated NSX cord LV434204, S434204, S434303, or S434303BS. |
| • Do not use NSX cords LV434200, LV434201, LV434202, S434201, and S434202. |
| **Failure to follow these instructions can result in death, serious injury, or equipment damage.** |

NOTICE
HAZARD OF EQUIPMENT DAMAGE
• Never connect an Ethernet device to an RJ45 ULP port.
• The RJ45 ULP ports of IFE server are for ULP modules only.
• Any other use can damage the IFE server or the device connected to the IFE server.
• To check if an ULP module is compatible with the RJ45 ULP ports of IFE server, refer to the *ULP System User Guides* in Related Documents, page 7.
Failure to follow these instructions can result in equipment damage.

All connection configurations require the NSX cord. The insulated NSX cord is mandatory for system voltages greater than 480 Vac.

When the second RJ45 ULP port is not used, it must be closed with an ULP line termination.
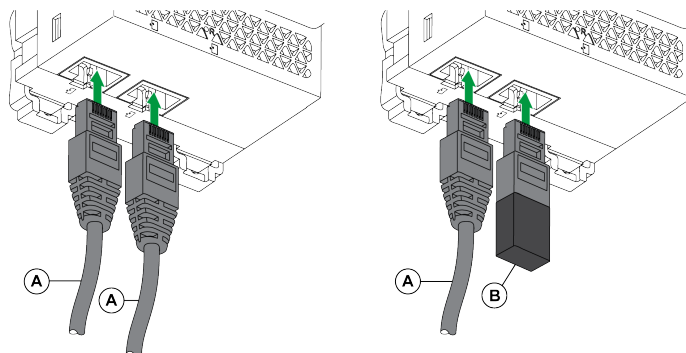
A   NSX cord or RJ45 plug/plug ULP cord

B   ULP line termination

Connection of the IFE Server to the MicroLogic Trip Unit
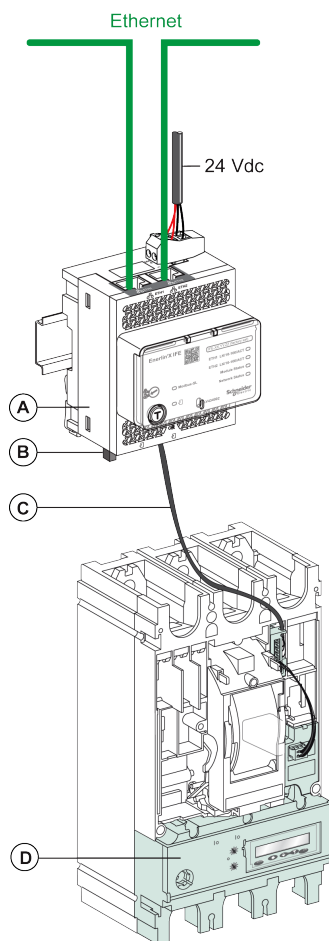
A   IFE Ethernet switchboard server

B   ULP line termination

C   NSX cord

D   MicroLogic trip unit
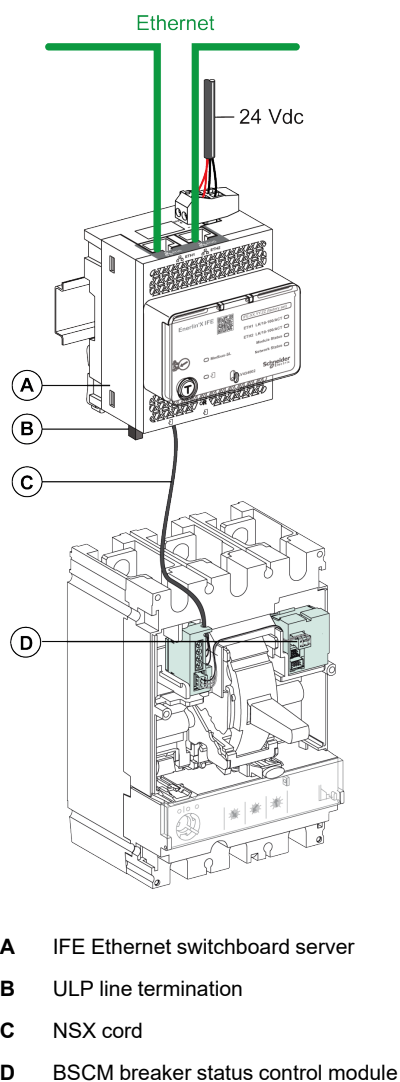
Connection of the IFE Server to the BSCM Module

A   IFE Ethernet switchboard server

B   ULP line termination

C   NSX cord

D   BSCM breaker status control module

Connection of the IFE Server to the BSCM Module and to the MicroLogic Trip Unit

A   IFE Ethernet switchboard server

B   ULP line termination

C   NSX cord

D   BSCM breaker status control module

E   MicroLogic trip unit

Connection of the IFE Server to a Circuit Breaker for System Voltage Greater Than 480 Vac
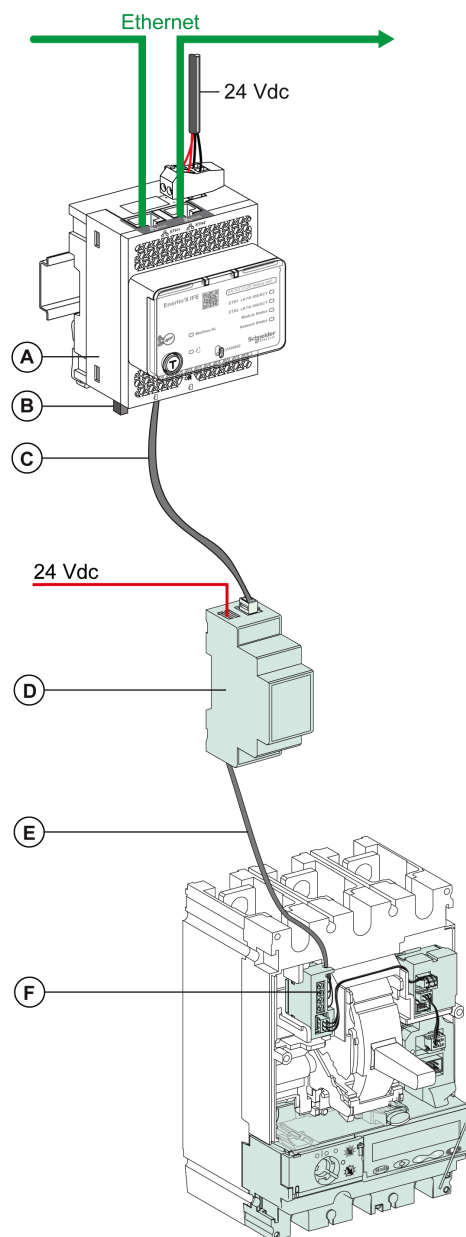
A   IFE Ethernet switchboard server

B   ULP line termination

C   RJ45 plug/plug ULP cord

D   Insulated ULP module for system voltage greater than 480 Vac

E   Insulated ULP cord for system voltage greater than 480 Vac

F   ComPacT NSX internal connection

Technical Characteristics

Environmental Characteristics

Characteristics		Value
Conforming to standards		• IACS E10 • EN 61326-1 • CSA C22.2 • IEC/UL 61010-2-201 • IEC61000-6-2 Ed.2
Certification		cULus, CE, EAC, and FCC marking
Ambient temperature	Storage	-40 °C to +85 °C (-40 °F to +185 °F)
	Operation	-25 °C to +70 °C (-13 °F to +158 °F)
Protective treatment		ULV0, conforming to IEC/EN 60068-2-30
Pollution		Level 3

Mechanical Characteristics

Characteristics	Value
Shock resistance	Conforming to IEC 60068-2-27 15 g/11 ms, 1/2 sinusoidal
Resistance to sinusoidal vibrations	Conforming to IEC/EN 60068-2-6

Electrical Characteristics

Characteristics		Value
Power supply		24 Vdc, -20%/+10% (19.2–26.4 Vdc)
Consumption	Typical	24 Vdc, 120 mA at 20 °C (68 °F)
	Maximum with server	19.2 Vdc, 140 mA at 60 °C (140 °F)

Physical Characteristics

Characteristics	Value
Dimensions	72 x 105 x 71 mm (2.83 x 4.13 x 2.79 in)
Mounting	DIN rail
Weight	187 g (0.41 lb)
Degree of protection of the installed module	• On the front panel (wall-mounted enclosure): IP4x • Connectors: IP2x • Other parts: IP3x
Connections	Screw type terminal blocks

24 Vdc Power Supply Characteristics

It is recommended to use an UL listed/UL recognized limited voltage/limited current or a class 2 power supply with a 24 Vdc, 3 A maximum.

NOTE: For 24 Vdc power supply connection, use copper conductors only.

For more information on the ULP System and its components, refer to the *ULP System User Guides* in Related Documents, page 7.

Characteristics	Value
Power supply type	Regulated switch type
Rated power	72 W
Input voltage	100–120 Vac for single phase
	200–500 Vac phase-to-phase
PFC filter	With IEC 61000-3-2
Output voltage	24 Vdc
Power supply output current	3 A

Firmware Update

Read the following instructions carefully before performing the firmware update to version 005:

- Firmware update to version 005 is recommended when all the features available in firmware version 003 are also available in firmware version 005.

- Firmware update to version 005 is not recommended when any of the features currently used by the application in firmware version 003 is not available in firmware version 005.

The firmware version 005 does not support the following features as compared to the firmware version 003:

- Firmware version 005 supports less devices as compared to the firmware version 003. For more information, refer to the list of supported devices with the firmware version 005 and the firmware version 003. Refer to List of IFE Supported Device Types, page 176

- Display of the IO module input/output configuration, refer to IO Readings, page 170

- Adding remote devices, refer to Device List Parameters, page 136

- Trending graphs, refer to Trending Parameters, page 152

- Data logging for serial devices, refer to Device Logging, page 153

Description

Use the latest version of EcoStruxure Power Commission software for all firmware updates.

The latest version of IFE firmware and IFE webpages are updated in a single operation through EcoStruxure Power Commission software.

For more information on IFE firmware versions, refer to the *Enerlin'X IFE Server Firmware Release Note* in Related Documents, page 7.

NOTICE

LOSS OF DATA

- Ensure that you take backup of the data log files before updating the firmware. The data log entries of the IFE server may be lost when the IFE firmware is updated.

- Ensure that you take backup of data present in User Accounts and Email Events sections of IFE webpages.

- Ensure that after firmware upgrade, you restore the User Accounts and Email Events configuration on IFE webpages.

Failure to follow these instructions can result in permanent loss of data.

After updating the firmware of one device in the IMU, use the latest version of EcoStruxure Power Commission software to check the firmware compatibility between the IMU devices. The **Firmware Update** table helps you to diagnose and identify all discrepancy issues between the IMU devices. This table also provides the recommended actions relevant to the detected discrepancies.

Checking the Firmware Version

You can find the firmware version of the devices in the IMU by using:

- EcoStruxure Power Commission software, refer to the *EcoStruxure Power Commission Online Help*.

• For IFE webpages, see the following procedure.

Step	Action	Result
1	Open the web browser and log in to the IFE webpage.	Opens the IFE home page.
2	Locate the firmware version on **Device Information** page on the **Diagnostics** menu , page 166. **NOTE:** If you have updated the firmware recently, press **F5** to refresh the webpage and update the displayed firmware number.	Determines the firmware version of the IFE server.

Updating the Firmware and Webpages using EcoStruxure Power Commission Software

Click here to download the latest version of EcoStruxure Power Commission.

For more information, refer to the *EcoStruxure Power Commission Online Help*.

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: • 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.

IFE Server Webpages from Firmware Version 005

What's in This Part

Security Features

What's in This Chapter

Machine to Machine Communication

M2M Definition

The Machine to Machine (M2M) communication feature allows communication and data exchange between devices or machines without the need for human intervention. This means that machines can communicate with each other, share information, and make decisions based on that information without human assistance.

The secure M2M communication feature available in the IFE server enables the protection of Modbus TCP communication by ensuring its confidentiality. When this feature is activated through the IFE webpages, the communication between a Modbus TCP client and the IFE server is encrypted using the TLS protocol on port number 802. For information about enabling secure Modbus for M2M on the IFE webpages, refer to IP Network Services, page 79.

> **NOTE:** For secure M2M communication to work, the Modbus TCP client must also support the Modbus TCP over TLS. If the client does not support this, then the standard Modbus TCP on port 502 must be used instead.

Role Based Access Control

RBAC Definition

Role-based Access Control (RBAC) is a way to assign different levels of access to the users that define the features they can access.

RBAC is supported only by:

- MasterPacT MTZ circuit breakers with MicroLogic X control unit.
- ComPacT NSX circuit breakers.
- PowerPacT H-, J- and L-frame circuit breakers.

Access to the IFE server is checked by RBAC mechanism when the connection is made through:

- IFE server webpages
- EcoStruxure Power Commission (EPC) software

  For information about enabling RBAC when the connection is made through EPC software, refer to IP Network Services, page 79.

Role Definition

The following roles are defined for remote access by default:

- Security Administrator (SECADM)
- Engineer
- Installer
- Operator
- Viewer

The security administrator assigns a role to each of the users. Each role includes a set of permissions for the IFE server users.

The security administrator can manage the users of IFE server:

- On the IFE server webpages
- With the EcoStruxure Cybersecurity Admin Expert (CAE) software

EcoStruxure Cybersecurity Admin Expert Software

Cybersecurity Admin Expert (CAE) software is used for security configuration of the IFE server with firmware version 005.001.000 and later.

The security administrator can use CAE software to:

- Manage the users of IFE server
- Define the security policy of the IFE server
- Upload security configurations to multiple IFE servers
- Change Device Specific Settings (DSS) of each IFE server independently

For more information, refer to the *EcoStruxure Cybersecurity Admin Expert Guide* in Related Documents, page 7.

NOTE:

- Enable HTTPS for secure transfer of configurations from CAE software to IFE server.
- Enable DPWS for discovery of the IFE server on CAE software.

CAE Software Settings

The security administrator can set the following parameters in the CAE software:

Parameter	Description	Value
Minimum inactivity period	After this duration without any action from the user, IFE server webpages are locked.	• Range: 1–3600 s • Default value: 600 s
Maximum login attempts	The maximum login attempts	• Range: 1–32 • Default value: 3
Locking period duration	After this duration the locked user account will be unlocked.	• Range: 0–3600 s • Default value: 60 s
LoggingPolicy	**Enabled** to enable the user account	Default setting: Disabled
	SyslogServerIPAddress to enter the server IP address of the Syslog server.	–
	SyslogServerport to enter the Syslog server port number.	• Range: 1–65534 • Default value: 601
Device measure read permission	**Enabled** while creating a role.	Default setting: Disabled

NOTE: CAE software supports a maximum of 12 users and 10 user roles for the IFE server.

CAE Device Specific Settings

The Device Specific Settings (DSS) is unique to the IFE server which enables the configuration to be tailored for each individual device. For example, by using this feature it is possible to activate Modbus secure on a specific IFE server while leaving it inactive on others.

The following device specific settings are available on the CAE software:

Parameter	Description	Default Setting
DPWS Discovery Status	Activates DPWS discovery on the IFE server.	Enabled
FTP Server Status	Activates FTP server on the IFE server.	Disabled
Modbus Secure Status	Activates Modbus secure on the IFE server.	Disabled
Modbus TCP Status	Activates Modbus TCP on the IFE server.	Enabled

Permission for Each Role

The security administrator can modify the permissions for each role using the CAE software.

The following table describes the permissions allowed for each role by default:

Permission	Roles				
	Viewer	Engineer	Operator	Installer	Security Administrator
Maintenance Information Read	–	✓	✓	✓	–
Maintenance Settings Write	–	✓	–	✓	–
Maintenance Control Write	–	✓	✓	✓	–
Public Information Read	✓	✓	✓	✓	✓
Device Measures Information Read	✓	✓	✓	✓	✓
Device Measures Settings Write	–	✓	–	✓	–
Device Measures Control Write	–	–	✓	–	–

Permission	Roles				
	Viewer	Engineer	Operator	Installer	Security Administrator
Device Settings Write	–	✓	–	✓	–
Device Information Read	✓	✓	✓	✓	✓
Communication Information Read	–	✓	✓	✓	–
Communication Settings Write	–	✓	–	✓	–
Communication Control Write	–	✓	–	✓	–
Date and Time Settings Write	–	✓	–	✓	–
Date and Time Information Read	✓	✓	✓	✓	✓
Security Information Read	–	–	–	–	✓
Security Settings Write	–	–	–	–	✓
Security Control Write	–	–	–	–	✓
Breaker Control Write	–	–	✓	–	–
Breaker Settings Write	–	✓	–	✓	–
Breaker Information Read	–	✓	✓	✓	–
Protection Information Read	–	✓	✓	✓	–
Protection Settings Write	–	✓	–	✓	–
Protection Control Write	–	✓	–	✓	–
Input Output Information Read	–	✓	✓	✓	–
Input Output Settings Write	–	✓	–	✓	–
Input Output Control Write	–	✓	–	✓	–
Security Logs Information Read	–	–	–	–	✓
Security Logs Settings Read	–	–	–	–	✓
Security Logs Settings Write	–	–	–	–	✓

Security Logs

Description

The security log feature of the IFE server enables the generation of security related events such as successful or failed login attempts, user configuration, object access, and firmware updates. These events are recorded in security logs which provide information that can be used to monitor activities carried out on the system. The security team can use this information to detect and respond in the event of a security compromise.

The security team can retrieve the generated security logs by:

- Using the manual export option on the IFE webpage. For more information, refer to Export to CSV, page 87.

- Configuring the Syslog parameters in the IFE webpage. In this case, the generated security logs will be automatically sent to the configured Syslog server. For more information, refer to Syslog Service Parameters, page 87.

Webpage Access and User Interface

What's in This Chapter

Access to IFE Webpages

Supported Web Browsers

Browser	Version with Windows XP	Version with Windows Vista	Version with Windows 7 and later
Microsoft Internet Explorer	IE 9.0	IE 9.0	IE 10.0, IE11.0
Microsoft Edge	–	–	81.0.416.58 and later
Mozilla Firefox	15.0	20.0	20.0, 45.0
Google Chrome	24.0 and later	24.0 and later	24.0 and later

First Access to the IFE Webpages

The IFE name must be configured during the first access to the IFE webpages.

NOTICE

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.

Failure to follow these instructions can result in equipment damage.

When the IFE server is accessed for the first time with **SecurityAdmin** user name (Security Administrator role), the user will be asked to change the default password.

The procedure to access the IFE webpages for the first time depends on the operating system of the computer:

- Windows Vista, Windows 7 and later, or newer operating systems
- Windows XP or older operating systems

    NOTE: On upgrade of IFE server before accessing the webpages for the first time, delete the browser cache.

First Access Through PC with Windows Vista or Windows 7 and Later

Step	Action
1	Disconnect the PC from the local area network (LAN) and switch off Wi-Fi.
2	Connect an Ethernet cable from the computer to the IFE server or to the Ethernet switch inside the panel.
3	Open **Windows Explorer**.
4	Click **Network** and the IFE-**XXYYZZ** appears in the list of devices. **NOTE:** If the IFE name is not displayed in the list of devices in **Windows Explorer**, check if the PC and the IFE server are not connected through the router.
5	Double-click the selected IFE-**XXYYZZ**, the login page automatically opens in the browser. **NOTE:** Default browser must be Microsoft Internet Explorer or Microsoft Edge.

6	Enter `SecurityAdmin` as the user name and `AAAAAAAA` as the password, the home page automatically opens in the browser.
	    NOTE: The user name and password are case-sensitive.
	    NOTE: When the IFE server is accessed for the first time with **SecurityAdmin** user name (Security Administrator role), the user will be asked to change the default password.

Step	Action
7	To change the default password, select **My Profile** from the **SecurityAdmin** user name arrow on the header. The **Account Details Modification** page is displayed.
8	Enter **Old Password**, **Password**, **Confirm Password**, **EmailId**, and **Phone** to change the default password.
9	Select the language from the **Language** box and then click **Apply Changes**.
10	To locate the IFE-XXYYZZ, click **Device Location** on the header. The ULP LED of the selected IFE-XXYYZZ blinks for 15 seconds (test mode).
11	To name the IFE-**XXYYZZ**, select the **SETTINGS** menu, go to **DEVICES** submenu, enter the device name and click **Apply Changes.**
12	Write the IFE name on a blank device name label and stick it on the existing one.

NOTE:

- XXYYZZ is the last 3 bytes of the MAC address in hexadecimal format.
- Check the firewall settings if DPWS is not enabled.

First Access Through PC with Windows XP

Step	Action
1	Disconnect the computer from the local area network (LAN) and switch off Wi-Fi.
2	Connect an Ethernet cable from the computer to the IFE server.
3	Start the web browser, page 49. **NOTE:** The computer automatically uses the default IP address 169.254.#.# (#=0–255) and the default subnet mask 255.255.0.0.
4	In the address text box, enter `169.254.YY.ZZ`, where YY and ZZ are the last 2 bytes of the IFE server MAC address (to be found on the IFE server side label), then press **Enter**: the home page opens in the browser. Example: For an IFE with MAC address 00-B0-D0-86-BB-F7 or 0-176-208-134-187-247 in decimal, enter 169.254.187.247 in the address text box.
5	Press **Enter**, the login page automatically opens in the browser.
6	Enter `SecurityAdmin` as the user name and `AAAAAAAA` as the password, the home page automatically opens in the browser. **NOTE:** The user name and password are case-sensitive. **NOTE:** When the IFE server is accessed for the first time with **SecurityAdmin** user name (Security Administrator role), the user will be asked to change the default password.
7	To change the default password, select **My Profile** from the **SecurityAdmin** user name arrow on the header. The **Account Details Modification** page is displayed.
8	Enter **Old Password**, **Password**, **Confirm Password**, **EmailId**, and **Phone** to change the default password.
9	Select the language from the **Language** box and then click **Apply Changes**.
10	To locate the -XXYYZZ, click **Device Location** on the header. The ULP LED of the selected -XXYYZZ blinks for 15 seconds.
11	To name the -XXYYZZ, select the **SETTINGS** menu and click **DEVICES** submenu, and enter the device name and then click **Apply Changes**.
12	Write the IFE name on a blank device name label and stick it on the existing one.

NOTE: XXYYZZ is the last 3 bytes of the MAC address in hexadecimal format.

Access to Webpages

Follow the Network Discovery, Name Browsing, and IP Address Browsing process to access the webpages.

The webpage access depends on the IT infrastructure.

Network Discovery

Perform the following procedure to access the IFE webpages once the IFE name has been configured.

Step	Action
1	Connect the IFE server or the Ethernet switch inside the panel to the local area network (LAN).
2	Connect the computer to the local area network (LAN).
3	Open **Windows Explorer**.
4	Click **Network**, the IFE name is displayed in the list of devices. **NOTE:** If the IFE name is not displayed in the list of devices in **Windows Explorer**, check if the PC and the IFE server are not connected through the router.
5	Double-click the IFE name which is written on the device label located on the front face of the selected IFE server, the login page automatically opens in the browser. **NOTE:** Default browser must be Microsoft Internet Explorer or Microsoft Edge.

Name Browsing

DNS server is mandatory.

Step	Action
1	Connect the IFE server or the Ethernet switch inside the panel to the local area network (LAN).
2	Connect the computer to the local area network (LAN).
3	Start the web browser, page 49.
4	In the address text box, enter the IFE name which is written on the device label located on the front face of the selected IFE server.
5	Press **Enter**, the login page automatically opens in the browser. **NOTE:** If the IFE server does not appear in the list of devices in **Windows Explorer**, check if the PC and the IFE server are not connected through the router.

NOTE: The IFE IP address is mapped to the device label in the DNS server.

IP Address Browsing

IP static configuration has to be set.

Step	Action
1	Connect the IFE server or the Ethernet switch inside the panel to the local area network (LAN).
2	Connect the computer to the local area network (LAN).
3	Start the web browser, page 49.
4	In the address text box, enter IP address given by the IT administrator.
5	Press **Enter**, the login page automatically opens in the browser. **NOTE:** If the login page in the web browser does not open or does not display correctly, check if **Internet Explorer \Tools\Compatibility View Settings\Display Intranet sites in Compatibility View** in Internet Explorer is checked.

User Interface Layout

Overview

This graphic shows the IFE server user interface layout.
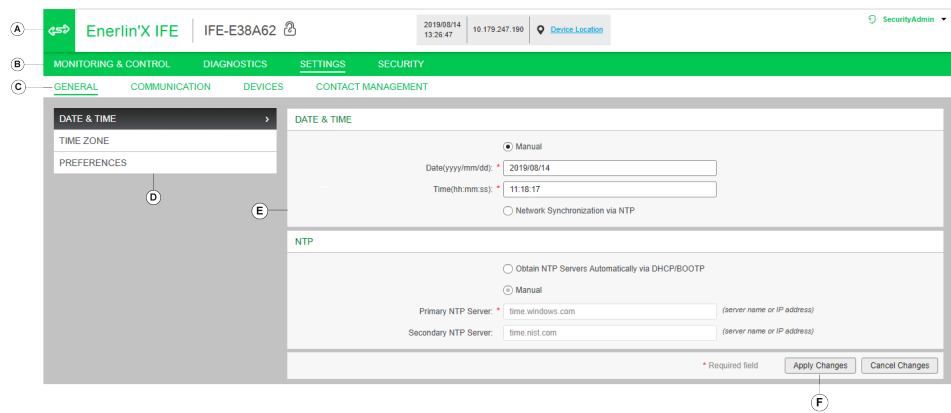
A	Header
B	Menu bar
C	Submenu bar
D	Webpages
E	Display zone
F	Action fields

Header

The header displays the following information at the top of all the pages.

A	IFE name
B	Intrusive command mode
C	Date and time
D	IP address
E	Device Location
F	My Profile Logout
G	User name

Header Part	Description
IFE name	Device name of the IFE server.
Intrusive command mode	• 🔒 : The intrusive command mode is Locked, the remote control commands are disabled. • 🔓 : The intrusive command mode is Unlocked (default setting), the remote control commands are enabled.
Date and time	Current date in yyyy-mm-dd format. Current time in hh-mm-sec format.

Header Part	Description
IP address	IPv4 address of the server.
Device Location	Click **Device Location** to locate the selected server in your equipment: • The ULP LED of the selected server blinks for 15 seconds (test mode). • The icon 📍 blinks 1 second ON and 1 second OFF when the device location is activated.
My Profile	Click to change your account password in the **Accounts Details Modification** window.
Logout	Click to log out from the IFE session, or close your browser. It is recommended to log out from the IFE session when it is not in use.
User name	Name of the user who has logged in.

Menu Bar

The main tabs in the menu bar are:

- **MONITORING & CONTROL**
- **DIAGNOSTICS**
- **SETTINGS**
- **SECURITY**

Submenu Bar

The subtabs in the submenu bar display the submenus under the selected main tab.

Webpages

The navigation menu under each subtab lists the webpages for the selected submenu.

Action Fields

The action fields correspond to the selected tab and it varies.

The following table describes the generic action fields on Setting and Security webpages:

Action Fields	Action
Apply Changes	Applies the setting changes.
Cancel Changes	Cancels the setting modifications and returns to the last saved settings.

For some settings, after clicking **Apply Changes**, a pop-up message is displayed for confirmation to restart the IFE server to apply the new settings:

- Click **Yes** to restart and apply the setting changes.
- Click **No** to cancel the setting modifications and return to the last saved settings.

Display Zone

The display zone shows the selected subtab in detail with all the related fields.

Webpage Description

MONITORING & CONTROL Webpage

Submenu	Webpage	Description
CIRCUIT BREAKERS, page 89	–	• Displays data from the circuit breaker and its IO modules. • Allows to reset of minimum and maximum values. • Allows to control the circuit breaker and the IO application.

DIAGNOSTICS Webpage

Submenu	Webpage	Description
COMMUNICATION	**STATUS**, page 95	Displays diagnostic data used to troubleshoot the network-related problems.
	ETHERNET, page 96	Displays the diagnostic data of Ethernet global statistics and Ethernet port characteristics.
	MODBUS, page 97	Displays the global statistics of TCP/IP and TCP port connections.
	ULP, page 98	Displays the global statistics of ULP port connection.
	REDUNDANCY-RSTP BRIDGE, page 99	Displays the diagnostic data of RSTP bridge.
	REDUNDANCY-RSTP PORTS, page 100	Displays the diagnostic data of RSTP ports.
	SNMP, page 101	Displays the diagnostic data of SNMPV1 Agent.
	READ DEVICE REGISTERS, page 102	Displays the list of devices to read device registers according to the selected device.
IFE, page 103	–	• Displays the IFE server basic information. • Displays the IFE server parameters and characteristics.
DEVICES	**DEVICES**, page 105	• Displays the list of the IMU devices connected to the ULP port. • Displays the maintenance counter information of the selected device. • Displays the IO module input/output configuration. • Displays the details of circuit breaker communication component.

SETTINGS Webpage

Submenu	Webpage	Description
GENERAL	**DATE & TIME**, page 57	Sets the date and time manually or sets the IFE time automatically using an NTP source or configures the device connected to IFE server to synchronize their time with the IFE time automatically.
	TIME ZONE, page 59	Sets the time zone for the region and sets the daylight saving time.
	PREFERENCES, page 60	Sets IFE preferences for data refreshment.
COMMUNICATION	**ETHERNET**, page 62	Sets the Modbus TCP/IP communication interface.
	IP CONFIGURATION, page 64	Sets the IP parameters.
	EMAIL SERVICE, page 66	Sets the configuration of SMTP server for mailing purpose.
	DATA PUBLISHING, page 68	Sets data generation and publishing parameters.
	REDUNDANCY-RSTP, page 69	Sets the RSTP bridge and RSTP port details.
	SNMP, page 71	Sets the SNMPV1 agent parameters.

Submenu	Webpage	Description
	MODBUS SERIAL CONFIGURATION, page 73	Sets the Modbus serial communication parameters.
DEVICES, page 74	-	• Sets the IFE name. • Sets circuit breaker name and data logging.
CONTACT MANAGEMENT	**EMAILS**, page 77	• Sets the email address for the events notification and data publishing. • Sets the events to be notified.

SECURITY Webpage

Submenu	Webpage	Description
IP NETWORK SERVICES, page 79	-	Configures the settings and activates the IP network services.
MODBUS TCP/IP FILTERING, page 80	-	Configures the IP addresses that can access the IFE server through Modbus TCP/IP.
CERTIFICATES, page 82	-	Displays the IFE certificate with expiration date and validity period.
USER MANAGEMENT, page 84	-	Manages the existing and newly added user accounts.
SYSLOG SERVICE, page 87	-	Configures the Syslog server address.

Settings Pages

What's in This Chapter

Date & Time

Description

The **DATE & TIME** page allows you to:

- Manually set the date and time of the circuit breaker connected to the IFE server.
- Automatically synchronize the date and time of the circuit breaker to the IFE time.
- Periodically check the synchronization at specified interval of time.

The users with Installer or Engineer role can change the date and time settings.

Navigation to the Date and Time Page

To view the **DATE & TIME** page, click **SETTINGS > GENERAL > DATE & TIME**.

Date and Time Settings

Parameter	Description
Date and time setting mode	Allows you to select the date and time setting mode of the circuit breaker and its IMU devices: • Check **Manual** (default setting) to set manually the date and time in the dedicated fields. • Check **Network Synchronization via NTP** to set automatically the date and time by an external time server (NTP server).
Date	Allows you to set the present date manually in the format YYYY-MM-DD.
Time	Allows you to set the present time manually in the format hh:mm:ss.

NTP Settings

Parameter	Description
NTP server setting mode	Allows you to select the NTP server setting mode: • Check **Obtain Servers Automatically via DHCP/BOOTP** (default setting) to set the NTP servers automatically. • Check **Manual** to set manually the NTP servers names or addresses.
Primary NTP server	Allows you to enter manually the primary NTP server address.
Secondary NTP server	Allows you to enter manually the secondary NTP server address.

NOTE:
- When both the NTP servers are not reachable by IFE server and another IMU device is setting the date and time, the IFE server date and time setting mode falls back to Manual automatically.
- When the time setting mode is set to Manual, Time Zone Offset is reset to 0.
- IPv6 is not supported for NTP server address.

Time Spreading

Follow this procedure to set the date and time of Modbus server devices of IFE server.

Step	Action	Result
1	From the IFE menu bar, click **Settings**.	Opens the **Settings** menu.
2	In the **General** submenu, click **Date and Time**.	The selection of server devices and **Every** box is available.
2	In **Date and Time: Periodic Spreading**, select **Every** check box and enter the time interval (you can enter value between 1 to 63 hours).	Allows you to enter the time interval in hours.
3	Select the server devices from the device list which supports date and time setting from external source.	The server devices get selected.
8	Click **Apply Changes**.	The date and time of the selected server devices get synchronized with the IFE time immediately and also periodically as per the selected time interval.

Time Zone

Description

The **TIME ZONE** page allows you to set the time zone of a particular region.

The users with Installer or Engineer roles can change the time zone settings.

Navigation to the Time Zone Page

To view the **TIME ZONE** page, click **SETTINGS > GENERAL > TIME ZONE**.

Real Time Clock

The IFE server has a Real Time Clock (RTC) to maintain date and time during power outage. The expected life time of the RTC is 15 years when operated at intermediate mode (in this mode, the battery is operated continuously for 4 days with an interval of 45 times over a period of 10 years).

The IFE server must maintain a crystal tolerance of ±20 ppm (typical)/±150 ppm (maximum) during the period of 15 years at -25 °C (-13 °F) to 85 °C (185 °F). The time drift by RTC chip varies from -16 s/day to +2 s/day. During power recycle, the RTC is able to maintain the date and time settings.

Time Zone Settings

Parameter	Description
Time Zone Offset	Allows you to select the time zone of a particular region.
Enable	Enables the daylight saving time.
Daylight Savings Time begins	Allows you to set the beginning time of daylight saving.
Daylight Savings Time ends	Allows you to set the end time of daylight saving.

NOTE: The settings of **Time Zone** is applicable only when **DATE & TIME** is in **Network Synchronization via NTP** mode.

Preferences

Description

The **PREFERENCES** page allows you to set the IFE server preferences for data refreshment rate.

The users with installer or engineer roles can change the preferences settings.

Navigation to the PREFERENCES Page

To view the **PREFERENCES** page, click **SETTINGS > GENERAL > PREFERENCES**.

Preferences Settings

Parameter	Description	Value
Real Time Sample Rate	Sets how often data is read from the device in the standard monitoring table views.	Setting range: 5–60 s Default setting: 5 s
Communications Check Rate	Sets how often a communications check is performed while the browser is displaying real-time readings in the standard monitoring table views. This function attempts to bring any out-of-service devices back into service automatically.	Setting range: 5–30 min Default setting: 15 min

Set Device Time

Description

The **SET DEVICE TIME** page allows you to synchronize the date and time of the IMU devices connected to the IFE server to IFE date and time. It also allows you to get the device time and set device time that are connected to the IFE server. This page lists the IMU devices that are stacked to the IFE server to set their date and time.

List of Parameters in Set Device Time

Parameter	Description
Device Selection	Allows you to select the device from the list for synchronizing, getting, and synchronizing the time.
Localized Time	Displays the time of the selected device.
Status	Displays the status of the selected device.
Get Time	Allows you to get the time of the selected device.
Set Device Time	Allows you to set the time of the selected device.

Setting the Device Time

Step	Action	Table
1	From the IFE menu bar, click **Settings**.	Opens the **Settings** menu.
2	From the **Settings** menu go to **General** and click **Set Device Time**.	Opens the **Set Device Time** page.
3	Select the devices from the **Set Device Time** page, and then click **Set Device Time**.	The selected server device date and time gets synchronized with the IFE time and the status is updated as successful. **NOTE:** If the selected device fails to synchronize with IFE date and time, then the status is updated as unsuccessful. **NOTE: Set Device Time** feature is not applicable for IFE's own IMU and shows the set status as **NA** (Not Applicable).

Ethernet

Description

The **ETHERNET** page allows you to define the physical Ethernet connection speed and transmission rate for the Ethernet ports.

The users with Installer or Engineer roles can change the Ethernet settings.

For Ethernet settings, after clicking **Apply Changes**, a pop-up message is displayed for confirmation to restart the server to apply the new settings:

- Click **Yes** to restart and apply the setting changes.
- Click **No** to cancel the setting modifications and return to the last saved settings.

Navigation to the ETHERNET Page

To view the **ETHERNET** page, click **SETTINGS > COMMUNICATION > ETHERNET**.

Ethernet Settings

Parameter	Description	Value
MAC Address	A unique media access control address of an IFE server. The MAC address is written on the label which is placed on the side of the IFE server.	–
Frame Format	Used to select the format for data sent over an Ethernet connection.	• Ethernet II • 802.3 • Auto (default setting)

Port Control Settings

Parameter	Description	Value
ETH1 Mode	Used to define the physical Ethernet connection speed and transmission mode for Ethernet port 1.	Auto-negotiation (default setting)
ETH2 Mode	Used to define the physical Ethernet connection speed and transmission for Ethernet port 2.	Auto-negotiation (default setting)

Broadcast Storm Protection Settings

Parameter	Description	Value
Enable	Enables the Broadcast Storm Protection (enabled by default).	–
Level	Allows you to select the broadcast storm protection level. The level value corresponds to a committed information rate (CIR) value, that is, the amount of traffic entering the switch port from which the storm protection drops entering the broadcast traffic.	Broadcast storm protection level: • **1**: Highest (1000) • **2**: High (2000) • **3**: Medium-High (3000) • **4**: Medium-Low (4000), Default setting • **5**: Low (5000) • **6**: Lowest (6000) **NOTE:** The level value corresponds to the committed information rate.
Committed information rate	Displays the read-only value of the broadcast storm protection level.	–

IP Configuration

Description

The **IP CONFIGURATION** page allows you to set the IP parameters.

The users with Installer or Engineer roles can change the IP configuration settings.

Navigation to the IP CONFIGURATION Page

To view the **IP CONFIGURATION** page, click **SETTINGS > COMMUNICATION > IP CONFIGURATION**.

IPv4 Settings

Parameter	Description
Configuration	Allows you to select the IPv4 configuration mode: • Check **Automatic** (default setting) to set IPv4 parameters automatically by using **DHCP** or **BOOTP**. • Check **Manual** to set manually the IPv4 parameters (IP address, Subnet mask, and Gateway).
Mode	Allows you to select the mode for assigning the IPv4 parameters by using: • DHCP (default setting) • BOOTP **NOTE:** While using a legacy DHCP server, the device name must be limited to 16 characters.
IP address	Used to enter manually the static IP address of an IFE server.
Subnet mask	Used to enter manually the Ethernet IP subnet mask address of your network.
Gateway	Used to enter manually the gateway (router) IP address used for wide area network (WAN) communication.

IPv6 Settings

For IPv6 Configuration settings, after clicking **Apply Changes**, a pop-up message is displayed for confirmation to restart the server to apply the new settings:

• Click **Yes** to restart and apply the setting changes.

• Click **No** to cancel the setting modifications and return to the last saved settings.

Parameter	Description
Enable IPv6	Enables IPv6 (Default setting: Enable).
IPv6 address	Static IP address of IFE server. **NOTE:** In the URL address box, use [ ] brackets to enter the link local address.

DNS Settings

Parameter	Description
DNS address	Allows you to select the IPv4 configuration mode: • Check **Automatic** (default setting) to obtain the IP address from the DNS server automatically. • Check **Manual** to set manually the primary and secondary server addresses. NOTE: Domain name system (DNS) is the naming system for computers and devices connected to a local area network (LAN) or the Internet.
Primary server address	Used to enter manually the IPv4 address of the primary DNS server.
Secondary server address	Used to enter manually the IPv4 address of the secondary DNS server. Used to perform a DNS resolution when the resolution fails with the primary DNS server.

Duplicate IP Address Detection

While connected to your network, the IFE server publishes its IP address. To avoid any duplicate IP address conflicts, the IFE server uses the address resolution protocol (ARP) to see if any other device on your network is using the same IP address. The following table explains how the IFE server handles a duplicate IP address when it is detected.

Duplicate IP Address Scenario

Scenario	Duplicate IP Detected	Network Status LED
Ethernet link detected	Reverts to the default IP address, subnet mask, and gateway address. ARP requests are sent every 15 seconds until the IP address is available. IFE server uses the IP address when it is available,	Steady red
Manual address change	Reverts to the default IP address, subnet mask, and gateway address. The ARP requests are sent every 15 seconds until the IP address is available. The IFE server uses the IP address when it is available.	Steady red
Receives an ARP request	If more than one ARP is detected within 10 seconds, initiate the process to reacquire the IP.	OFF

Email Service

Description

The **EMAIL SERVICE** page allows you to activate email service and to set the Simple Mail Transfer Protocol (SMTP) server settings. The SMTP is a set of communication guidelines that allow the software to transmit an electronic mail over the Internet. It is a program used for sending messages to other computer users based on email addresses.

The users with Installer or Engineer roles can change the email service settings.

Navigation to the EMAIL SERVICE Page

To view the **EMAIL SERVICE** page, click **SETTINGS > COMMUNICATION > EMAIL SERVICE**.

Email Service

Parameter	Description
Email Service	Enables the Email service (disabled by default).

Email SMTP Server Settings

Parameter	Description	Value
SMTP Server Address	Allows you to enter an email server address (SMTP server). **NOTE:** Contact your network administrator to know the IP address or the name of the SMTP server.	–
Connection Security Mode	Allows you to select the connection security mode.	• None (default setting) • TLS • STARTTLS
SMTP Server Port	Allows you to enter the SMTP server port.	• 25 (default setting) • 465: TLS • 587: STARTTLS
Authentication	Allows you to enable Authentication if the SMTP server requires login information (disabled by default).	-
SMTP Account login	Allows you to enter the SMTP account login name.	–
SMTP Account Password	Allows you to enter the SMTP account password.	–

Email Sender Address Settings

Parameter	Description
From Address	Allows you to enter the email address of the administrator.

The **From Address** can be used in different ways:

- Use the **From Address** as a context provider: If you do not want to receive any reply, and only notify the recipient, use **From Address** as contextual information. The **From Address** syntax includes "no-reply", "device name", "site name", @a validated domain.com, .net, and so on.

- Create an alias in the **From Address** to allow replies to be sent to the person in charge of an alarm: An email can be sent to multiple people who are responsible for a specific appliance. This feature allows the receivers to reply to follow up with the responsible person.

  For example, the facility manager would receive an email from an alarm. Facility manager can send a reply email to the maintenance contractor to follow up on the action.

Email Language Settings

Parameter	Description	Setting
Language	Allows you to select the language of the email body.	• **English** (default setting) • **French**

Email Test Settings

Parameter	Description
Recipient Address for Test	Allows you to enter the email address of the recipient to test the delivery of the email.

The **Email Test** feature enables connection from the IFE server to the service.

Click **Test** to send the test email to the recipient address for test. If the test emails are not received, the Internet connection needs to enable the email ports (port 25 or 465 or 587). The required setting of the port is done in accordance between the IFE server that sends the email and the site router settings.

NOTE: The email with custom text that uses characters such as à, è, ù, é, â, ê, î, ô, û, ë, ï, ü, ÿ, and ç are not shown correctly in the email. However, the generic text message is shown correctly.

Data Publishing

Description

The **DATA PUBLISHING** page allows you to export the data selected on the **Devices** page in email or FTPS mode.

The users with Installer or Engineer roles can change the data publishing settings.

Navigation to the DATA PUBLISHING Page

To view the **DATA PUBLISHING** page, click **SETTINGS > COMMUNICATION > DATA PUBLISHING**.

Data Generation Setting

Setting	Description	Value
Logging Interval	Allows you to select the time interval for logging the data.	–

Data Publishing Settings

Setting	Description
Export Activated	Allows you to enable the export activation of data publishing (disabled by default).
Mode	Allows you to select the mode for data publishing by: • **Email** • **FTPS**
FTPS Server Address	Allows you to enter the FTPS server address.
Port	Allows you to enter the FTPS port number.
Directory	Allows you to enter the FTPS directory name.
User Name	Allows you to enter the user name.
Password	Allows you to enter the password.
Export Interval	Allows you to select the export interval time for: • **Logging Interval** • **Hourly** • **Daily** • **Weekly** • **Monthly**
Time of Day	Allows you to select the time for data export (Default time: 00:00).
Day of the Week	Allows you to select the day for weekly export of data (Default day: Sunday).
Day of the Month	Allows you to select the day for monthly export of data (Default day: 1st day of the month).

Manual Export

Click the **Manual Export** to manually export the data by Email or FTPS according to the data publishing settings.

Redundancy-RSTP

Description

The **REDUNDANCY-RSTP** page allows you to set the RSTP bridge and RSTP port details.

The users with Installer or Engineer roles can change the Redundancy-RSTP settings.

For REDUNDANCY-RSTP settings, after clicking **Apply Changes**, a pop-up message is displayed for confirmation to restart the server to apply the new settings:

- Click **Yes** to restart and apply the setting changes.
- Click **No** to cancel the setting modifications and return to the last saved settings.

Navigation to the REDUNDANCY-RSTP Page

To view the **REDUNDANCY-RSTP** page, click **SETTINGS > COMMUNICATION > REDUNDANCY-RSTP**.

RSTP Settings

Setting	Description
Enable	Allows you to enable RSTP feature (disabled by default).

RSTP Bridge Settings

Setting	Description	Value
Bridge Priority	Allows you to select bridge priority.	• Setting range: 0-61440 • Default setting: 32768
Bridge Hello Time	Allows you to enter bridge hello time.	• Setting range: 1-2 s • Default setting: 2 s
Bridge Max Age Time	Allows you to enter bridge maximum age time.	• Setting range: 6-40 s • Default setting: 40 s
Transmit Hold Count	Allows you to enter the transmit hold count.	• Setting range: 3-100 s • Default setting: 6 s
Bridge Forward Delay	Allows you to enter bridge forward delay.	• Setting range: 4-30 s • Default setting: 21 s

RSTP Port 1 and 2 Settings

Settings	Description	Value
RSTP setting mode	Allows you to select the RSTP setting mode: • Check **Automatic** (default setting) to set RSTP port 1 and 2 automatically. • Check **Manual** to set manually the RSTP port 1 and 2 parameters (port priority and port cost).	–
Port 1 and 2 Priority	Allows you to select manually port 1 and 2 priority.	• Setting range: 0-240 • Default setting: 128
Port 1 and 2 Cost	Allows you to enter manually the port 1 and 2 cost.	• Setting range: 1-200000000

SNMP

Description

The **SNMP** page allows you to set the Simple Network Management Protocol (SNMP) settings.

The IFE server supports SNMP, allowing a network administrator to access remotely an IFE server with an SNMP manager and to view the networking status and diagnostics of the IFE server in the MIBII format.

The users with Installer or Engineer role can change the SNMP settings.

Navigation to the SNMP Page

To view the **SNMP** page, click **SETTINGS > COMMUNICATION > SNMP**.

SNMPV1 Agent Settings

Setting	Description	Value
Enable	Allows you to enable or disable the SNMP agent.	–
Listening Port	Allows you to enter listening port number at which the SNMP agent listens for network traffic.	• Setting range: 1 -65534 • Default setting: 161
Notification Port	Allows you to enter notification port number.	• Setting range: 1 -65534 • Default setting: 162

System Objects Settings

Setting	Description
System Location	Allows you to enter system location.
System Contact	Allows you to enter system contact person name.
System Name configuration mode	Allows you to select the System Name configuration mode: • Check **Automatic Configuration of System Name** to set the system name automatically. • Check **Manual Configuration of System Name** (default setting) to set manually the system name.
System Name	Allows you to enter the system name manually.

Community Names Settings

Setting	Description
Get Community Name	Allows you to enter get community name.
Set Community Name	Allows you to enter set community name.
Trap Community Name	Allows you to enter trap community name.

Enabled Traps Settings

Enabled Traps allows you to select any of the following traps, which are disabled by default:

Setting	Description
Cold Start Trap	Generates a trap when the IFE server is powered ON.
Warm Start Trap	Generates a trap when SNMP is enabled.
Link Down Trap	Generates a trap when an Ethernet port communication link is disconnected.
Link Up Trap	Generates a trap when an Ethernet port communication link is reconnected.
Authentication Failure Trap	Generates a trap when an SNMP manager is accessing the IFE server with incorrect authentication.

SNMP Managers Settings

Setting	Description
Manager#1	Allows you to enter name or IP address of SNMP manager one.
Manager#2	Allows you to enter name or IP address of SNMP manager two.

Modbus Serial Configuration

Description

The **MODBUS SERIAL CONFIGURATION** page allows you to modify Modbus serial communication parameters.

Navigation to the MODBUS SERIAL CONFIGURATION Page

To view the MODBUS SERIAL CONFIGURATION page, click **SETTINGS > COMMUNICATION > MODBUS SERIAL CONFIGURATION**.

Modbus Serial Line Settings

Parameter	Settings
Baud Rate	• 9600 bps • 19200 bps (Factory setting) • 38400 bps
Parity	• **Even** (Factory setting) • **Odd** • **None**
Nb bits of Stop	• **Auto** (Factory setting) • 1 bit • 2 bits
Serial line termination	• **Enabled** (Factory setting) • **Disabled**
Modbus SL timeout	• 1 s (Factory setting) • 0.1–0.5 s • 1–10 s

NOTE: When **Nb bits of Stop** parameter is set to **Auto**, the actual value is based on the parity chosen.

Devices

Description

The **DEVICES** page allows you to discover or add the list of devices connected to the IFE server (ULP port, serial port). In the device list you can delete the previously discovered devices.

The list of connected devices is defined by either of the following:

- Automatically, by clicking **Discover**. Device Discovery Procedure, page 75
- Manually, by clicking **Add Serial Device**. Adding a Device Manually, page 76

    NOTE: The webpages are supported only for the devices added in the device list.

For more information on devices that are supported in firmware version 005, refer to List of IFE Supported Device Types, page 176
.

Navigation to the Devices Page

To view the **DEVICES** page, click **SETTINGS > DEVICES**.

Number of Modbus Server Devices

Under each IFE server or remote Modbus client device, a maximum of 11 IFM interfaces can be added.

The application dictates the maximum Modbus server devices or IFM interfaces that can be used. The following general guidelines can be used to size the application:

- Maximum of 11 IFM interfaces can be physically connected to one IFE server. This can be used for applications that have the lowest performance requirement and are recommended for simple applications.
- Maximum of 8 IFM interfaces should be used for applications that requires regular access via the IFE webpages or that have other Modbus clients communicating, such as FDM128 display. This normally provides a reasonable response time for up to three Modbus clients.
- The number of IFM interfaces that can be stacked in a more complex environment, for example, with SCADA or Building Management Systems must be scaled to the performance needs in the application.

Device List Parameters

Parameters	Description	Settings
Name	Allows you to enter the names for IFE server and remote device. **NOTE:** - The LV breaker system is uniquely identified over possible interfaces such as HMI, Modbus/TCP, DPWS, and DHCP. - IFE device name is common across all interfaces. Thus, changing IFE device name by any means has direct impact on all the connected interfaces.	The IFE name can have up to 63 ASCII characters with the following characters: **A–Z**, **a–z**, **0–9**, and **-**. However, **-** cannot be used at the end of the name. **NOTE:** - IFE name should be unique within the device list. - Duplicate IFE names for different devices may have impact on web applications, logging, and export features.
Device Type	Allows you to select the server devices from the list of supported devices, page 176.	–

Parameters	Description	Settings

Device Name	Allows you to enter the name for the discovered devices.
	
	• For **ULP** port: Enter the device name in the device type text box.
	    NOTE:
	    ◦ Applicable only for devices other than MasterPacT MTZ circuit breaker.
	    ◦ For MasterPacT MTZ circuit breaker, user application name and device name are the same.
	• For **Serial port**: Enter the device name.
	    NOTE: Delete and edit operations are not allowed if the device is selected for logging.
		The device name can have up to:
		
		• 63 ASCII characters for MasterPacT MTZ devices
		• 45 ASCII characters for other devices
		
		The allowed characters are: **A–Z**, **a–z**, **0–9**, and **-**. However, **-** cannot be used at the end of the name.

Server ID	Displays the local address of the device connected to the IFE server or remote device.	• For **ULP** port: 255 (Fixed) • For **Serial port** and remote device: 1–247
Apply Changes	Allows you to save device list configuration.	–
Delete 🗑	Allows you to delete the selected server devices. **NOTE:** Delete operation is not allowed if the device is selected for logging.	–
Discover	Allows you to discover the server devices. **NOTE:** The discover option for the device type BCM-OF/SD is available only on IFE's own IMU.	–
+ Add Serial Devices	Allows you to add a new server device to the device list.	–

Adding Device to the Device List for the First Time

Step	Action	Result
1	Server device to IFE server: Add the server devices to the IFE server manually, page 76 or by device discovery, page 75.	Adds the server device to IFE server.

Device Discovery Procedure

When you start device discovery, the IFE server queries the ULP port, serial port, and Ethernet port using a user-defined address range. Modbus RTU protocol is used for discovery on the serial port. If the device replies to the query, the local ID is set to the current discovery address, and the device is given a default device name. The IFE server, then tries to identify the device type. If the IFE server recognizes the device type of the discovered device, the IFE server sets the recognized device type in the **Device Type** field. If the IFE server does not recognize the **Device Type** of the discovered device, the IFE server sets to Modbus in the **Device Type** field.

The list of devices supported by the IFE server is in Appendix, page 175.

The table shows the steps to add device using device discovery procedure:

Step	Action	Result
1	From the IFE menu bar, click **Settings**.	Opens the **Settings** menu.
2	From the **Settings** menu, click **Devices** .	Opens the **Devices** page.
3	To discover locally connected devices, click **Discover**.	Opens the **Device Discovery** page.
4	Enter **Start Modbus ID** and **Stop Modbus ID**.	Enters the discovery address range.
6	Click **Start Discover**. (Click **Stop Discover** to stop the process).	Begins to discover all connected devices.

Step	Action	Result
	NOTE: Discovery only finds local serial Modbus devices connected to the IFE server. The device on the ULP port is discovered automatically.	
7	Enter a new device name in the **Name** text box.	Renames the device.
8	Click **Apply Changes** in the **Device Discovery** page.	Displays the saved device list.

Device Discovery Parameters

Parameters	Description	Setting
Start/Stop Modbus ID	Defines the Modbus server address range that is to be used to discover devices on the IFE serial port.	• **Start Modbus ID:** 1–247 (Factory setting: 1) • **Stop Modbus ID:** 1–247 (Factory setting: 10)
Apply Changes	Allows you to save the selected device to the **Device List**.	–
IP Address	Displays the IP address of the IFE server or the remote device.	–
Defined	Lists the device type that was defined for this device.	–
Assigned	Allows you to assign the device type from the drop-down list.	–
Name	Displays a default name (combination of user application name or IFE name and the server ID).	–
Local ID	The server address of the device connected to the IFE server.	–

Adding a Device Manually

Step	Action	Result
1	From the IFE menu bar, click **Settings**.	Opens the **Settings** menu.
2	From the **Settings** menu, click **Devices**.	Opens the **Devices** page.
3	Click **Add Serial Devices** to add a new device.	Allows you to add device in the device list.
4	Choose the supported device from the **Device Type** list.	Selects the device type selected from the list.
5	Enter a new device name in the **Device Name** text box.	Renames the device.
6	Enter the local address of the device in the **Local ID** text box.	Displays the local address of the device.
7	Click **Apply Changes**.	A new device is added to the list.

Emails

Description

The **EMAILS** page allows you to set the list of recipients of emails for:

- Event notification
- Data publishing

A maximum of 15 users or email recipients can be declared.

The users with Installer or Engineer roles can change the Emails settings.

Navigation to the EMAILS Page

To view the **EMAILS** page, click **SETTINGS > CONTACT MANAGEMENT > EMAILS**.

List of Settings

Setting	Description
Email	Allows you to enter the email address of the recipient.
Language	Displays the name selected language.
Notification	Allows you to select the events from the list to notify the user through email.
Data Publishing	Allows you to enable publication through email of the data selected on the **DEVICES** page .

Notification Page

The **NOTIFICATION** page allows the selection of the events to notify through email among a list of events.

⚠ CAUTION
EQUIPMENT INCOMPATIBILITY OR INOPERABLE EQUIPMENT
Do not rely solely on the notification of the emails for maintaining your equipment.
Failure to follow these instructions can result in injury or equipment damage.

The list of event displayed contains only applicable events related to the devices connected to the ULP port of the IFE server.

> **NOTE:** If an email SMTP server is not located on the same Ethernet network segment as IFE server, ensure that the IFE default gateway is properly configured.

Security Pages

What's in This Chapter

IP Network Services

Description

The **IP NETWORK SERVICES** page allows you to set and activate the IP network services.

The users with Security Administrator role can edit the IP network services parameters.

Navigation to the IP NETWORK SERVICES Page

To view the **IP NETWORK SETTINGS** page, click **SECURITY > IP NETWORK SERVICES**.

IP Network Services Parameters

Parameter	Description	Value
Modbus TCP	Allows you to enable/disable the Modbus/TCP service.	Default setting: Enabled
Secure Commissioning	Allows you to establish the secure communication over TLS and then by RBAC mechanism between EPC software and IFE server. **NOTE:** It is recommented to set it as Enabled. Once the secure commissioning is enabled, if EPC software is connected to IFE server, user must start a new discovery of the IFE server with EPC software.	Default setting: Disabled
	Allows you to set the port number of the secure commissioning server.	Setting range:1–65534 Default setting: 49152
Secure Modbus for M2M	Allows you to enable/disable the secure Modbus for machine-to-machine service. **NOTE:** Machine-to-Machine secure communication requires components that connect to the IFE server to support the Secure Modbus communication.	Default setting: Disabled
	Allows you to set the port number of the secure Modbus server.	Setting range:1–65534 Default setting: 802
	Allows you to set the number of sessions for the secure Modbus server.	Setting range:1–8 Default setting: 2
Internal FTPS Server	Allows you to enable/disable the FTPS server.	Default setting: FTPS server is disabled
Discovery	Allows you to enable/disable the discovery (DPWS) of the IFE server automatically.	Default setting: Enabled
HTTP/Web Port	Allows you to set the port number of the HTTP/Web server.	Setting range:1–65534 Default setting: 80
HTTPS Port	Allows you to enable/disable the HTTPS service and to set the port number of the HTTPS server. **NOTE:** After disabling the HTTPS, you should clear the browser cookies before authenticating it again.	Setting range:1–65534 Default setting: Enabled (value: 443)

Modbus TCP/IP Filtering

Description

The **MODBUS TCP/IP FILTERING** page allows you to set the level of access for Modbus TCP/IP clients connected to IFE server.

The users with Security Administrator role can edit the Modbus TCP/IP filtering parameters.

Navigation to the MODBUS TCP/IP FILTERING Page

To view the **MODBUS TCP/IP FILTERING** page, click **SECURITY > MODBUS TCP/IP FILTERING**.

Modbus TCP/IP Filtering Parameters

Parameters	Description
Modbus TCP/IP Filtering	Enables the Modbus TCP/IP address filtering (disabled by default). The list of IP addresses available in the table is granted access.

IP Filtering Global Access List Parameters

Click the ✎ icon to edit the **IP Filtering Rules** and set the access level.

Setting	Description
IP Range	Filters the required IP address you entered. A maximum of 10 IP addresses are allowed.

Access level	Displays the access level for the corresponding IP address:
	• **Read only**: The following Modbus TCP/IP function codes are allowed:
	  ◦ 1 (0x01)
	  ◦ 2 (0x02)
	  ◦ 3 (0x03)
	  ◦ 4 (0x04)
	  ◦ 7 (0x07)
	  ◦ 8 (0x08)
	  ◦ 11 (0x0B)
	  ◦ 12 (0x0C)
	  ◦ 17 (0x11)
	  ◦ 20 (0x14)
	  ◦ 24 (0x18)
	  ◦ 43 (0x2B), with subfunction codes 14 (0x0E), 15 (0x0F), and 16 (0x10).
	  ◦ 100 (0x64)
	• **None**: The access to the IP address is blocked.
	• **Read/Write**: Full access is provided.

IP Filtering Exception List Parameters

Click **Add Exception** and set additional **IP Filtering Rules** parameters.

Setting	Description
IP Address/IP Range	Filters the required IP address you entered. A maximum of 10 IP addresses are allowed.
Access level	Displays the access level for the corresponding IP address: • **Read**: The following Modbus TCP/IP function codes are allowed: 　◦ 1 (0x01) 　◦ 2 (0x02) 　◦ 3 (0x03) 　◦ 4 (0x04) 　◦ 7 (0x07) 　◦ 8 (0x08) 　◦ 11 (0x0B) 　◦ 12 (0x0C) 　◦ 17 (0x11) 　◦ 20 (0x14) 　◦ 24 (0x18) 　◦ 43 (0x2B), with subfunction codes 14 (0x0E), 15 (0x0F), and 16 (0x10). 　◦ 100 (0x64) • **None**: The access to the IP address is blocked. • **Read/Write**: Full access is provided.

Certificates

Description

The **CERTIFICATE** page allows you to create, modify, and import the IFE server certificate. This page also displays the details of the certificate and expiration date of the certificate.

The users logged with Security Administrator role can edit the certificate parameters.

> **NOTE:** For IFE server with firmware version 005.001.000 and later, only the certificate format **.pem** is supported.

Navigation to the CERTIFICATES Page

To display the **CERTIFICATES** page, click **SECURITY > CERTIFICATES**

Product Certificate Parameters

Parameter	Description
Certificate Type	Displays type of certificate.
Subject	Displays subject of the certificate.
Issuer	Displays the issuer name of the certificate.
Expiration Date	Displays expiration date of the certificate.
Create Certificate	Allows you to create new certificate for the product.
Import Certificate	Allows you to import the existing certificate for the product.
Delete Certificate	Allows you to delete the product certificate. NOTE: **Delete Certificate** option is enabled only in case of a customized certificate.

Import Certificate Parameters

Parameter	Description
Certificate Package	Name of the certificate package.
Browse	Allows you to navigate and locate the required certificate package.
Password	Allows you to enter the password.

Product Certificate Details

Parameters	Description
Certificate Type	Certificate generated by IFE server is Self-Signed.
Validity Period (UTC)	Validity period of the certificate. The certificate generated by the IFE server is automatically renewed one month before end of validity period.

Certificate Renewal

When the self-signed certificate is renewed, the session is closed automatically and you have to login again.

The self-signed certificate is renewed in the following cases:

- Deletion of imported certificate
- Self-signed certificate regeneration
- Expiration date is overdue
- Change in IP address

User Management

Description

The **USER MANAGEMENT** page is only accessible to the user with Security Administrator (SECADM) role.

The users with Security Administrator role can:

- Create, edit, and delete user accounts.
- Assign a role and a password to the users.

    NOTE: User accounts can also be managed using the EcoStruxure Cybersecurity Admin Expert Software.

Navigation to the USER MANAGEMENT Page

To view the **USER MANAGEMENT** page, click **SECURITY > USER MANAGEMENT**.

Security Administrator Role

The Security Administrator user account is created by default with all the roles. Therefore, IFE server helps to ensure that at least one user with SECADM role is always present in the users list.

⚠ **WARNING**
POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY
Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.
Failure to follow these instructions can result in death, serious injury, or equipment damage.

The security administrator default password is AAAAAAAA.

User Account Parameters

Parameter	Description
User Name	Enter a name for a new user. • User name is composed of 4 to 16 characters. • User names are case-sensitive and can contain special characters.
Password	Enter the password for the new user , page 85. The password entered must be confirmed.
Role	Select one or multiple roles for the new user in the predefined list of roles .
Email ID	Enter a valid email address for the entered user name.

User Account Edition

Once the user account is created, click the ✎ icon to edit and complete it with the following parameters.

Parameter	Description
User Name	Edit the user name.
Role	Change the role.
EmailID	Edit the email address of the user.
Phone	Enter the phone number of the user.
Language	Select the user language in the predefined list of languages.
Unlock	Unlock the user account locked after entry of 3 incorrect passwords.
Enabled	Turn on to enable the user account.

User Account Details

Once the user account is created, click the 🛈 icon to view the following parameters.

Parameter	Description
User Name	Displays name of the user.
EmailID	Displays the email address of the user.
Language	Displays the selected language of the user.
Phone	Displays the phone number of the user.
UserStatus	Displays the user status.
PasswordExpiryTime	Displays the expiration time of user password.
LockedUntil	Displays the user account locked status.

Password Syntax

A password is composed of 8 to 16 characters. It is case-sensitive and the allowed characters are:

- Digits from 0 to 9
- Letters from a to z
- Letters from A to Z
- Special characters as *, /, \, etc.

To be accepted by IFE server, a password must contain one letter lowercase, one letter uppercase, one digit and one non-alphanumeric character.

NOTE: Password with eleven stars (***********) is not allowed. While editing a user password, the three previous passwords of this user cannot be used.

Password Customization

After created by the user with Security Administrator role, the credentials are shared by Security Administrator with the new user.

┌───┐
│   ⚠ **WARNING**   │
├───┤
│ **POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND**   │
│ **CONFIDENTIALITY**   │
│   │
│ Change default passwords at first use to help prevent unauthorized   │
│ access to device settings, controls, and information.   │
│   │
│ **Failure to follow these instructions can result in death,**   │
│ **serious injury, or equipment damage.**   │
└───┘

The new user will be prompted to change his password at first connection. The password can be changed anytime by the user in the **MyProfile** page.

Password Reset

A user with Security Administrator role can reset another user password by pressing the **Reset** in the webpage. The new password is generated automatically and is shown in a pop-up message. Once generated, the new password is shared by Security Administrator with the user. The user must customize his new password at the first connection.

For more information about resetting the Security Administrator password, refer to .

In the case that all passwords with Security Administrator roles are lost or forgotten, contact your local Schneider Electric Customer Care Center.

Syslog Service

Description

The **SYSLOG SERVICE** page allows you to configure the Syslog server settings for the security logs generated by the IFE server.

The IFE server logs 2048 security events before the oldest events are over written by newer events.

Ensure the security logs are exported on a regular basis from the IFE server by:

- Manual log export in **CSV** format.
- Automatic export of the security logs using the **Export Interval** parameter.

   NOTE: Syslog server can also be configured using the CAE software. For more information, refer to the *EcoStruxure Cybersecurity Admin Expert Guide* in Related Documents, page 7.

Navigation to the SYSLOG SERVICE Page

To view the **SYSLOG SERVICE** page, click **SECURITY > SYSLOG SERVICE**.

Syslog Service Parameters

Parameter	Description	Value
Syslog Logging Service	Allows you to enable/disable the Syslog service.	Default setting: Disabled
SysLog Server Address	Allows you to enter the server name or IP address of the Syslog server.	–
Connection Mode	Allows you to select the connection type.	Default setting: TCP
SysLog Server Port	Allows you to enter the Syslog server port number.	Setting range:1–65534 Default setting: 801
Export Interval	Allows you to set the interval for the export of Syslog logging file.	Setting range:10–3600 s Default setting: 300 s

Export to CSV

Click **Export to CSV** to export the security log files in CSV format. The content of the security logs comply with the Syslog standard.

Test Connection

Click the **Test Connection** to verify the connection between the IFE server and Syslog server. During the test, the IFE server will connect with the Syslog server and the user will be notified if the connection is established or not.

Monitoring and Control Pages

What's in This Chapter

Circuit Breakers

Description

The **CIRCUIT BREAKERS** page allows:

- All users with any role to monitor data from the circuit breaker and its IO modules.
- The users with Installer or Engineer role to reset minimum and maximum values of the energy and demand measurements.
- The users with Operator role to control the circuit breaker and the IO application.

Navigation to the CIRCUIT BREAKERS Page

To view the **CIRCUIT BREAKERS** page, click **MONITORING & CONTROL > CIRCUIT BREAKERS**.

Page Layout
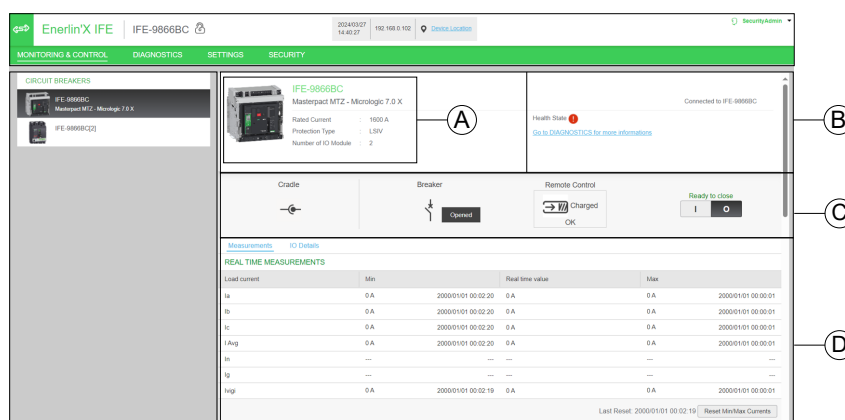
A   Circuit breaker identification data

B   Circuit breaker health status

C   Circuit breaker monitoring and control panel

D   Monitoring of measurements or IO details

Circuit Breaker Identification Data

The circuit breaker is identified by the following data:

- Rated current
- Protection type
- Number of IO modules connected
- Additional data according to the range of the circuit breaker

Circuit Breaker Health Status

The health status of a circuit breaker is indicated by one of the following icons:

Icon	Description
	OK
	Medium severity detected alarm that requires non-urgent action.
	High severity detected alarm that requires immediate corrective action.

Circuit Breaker Monitoring and Control Panel
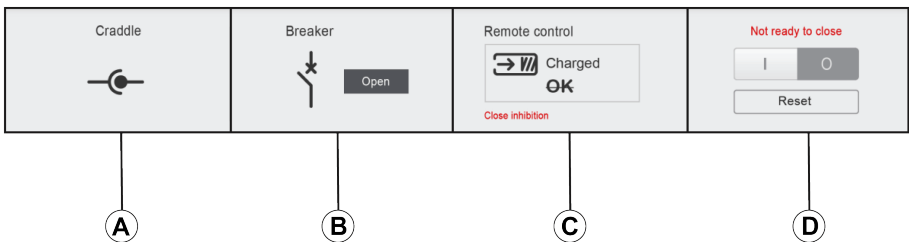
A	Drawout circuit breaker position in the cradle
B	Circuit breaker main contact position
C	Circuit breaker control mode and control status
D	Circuit breaker control options
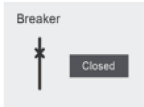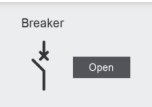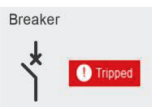
Drawout Circuit Breaker Position in the Cradle

The position of the drawout circuit breaker in the cradle is indicated by the following icons:

Icon	Description
	Drawout circuit breaker is in connected position.
	Drawout circuit breaker is in test position.
	Drawout circuit breaker is in disconnected position.

Circuit Breaker Main Contact Position

The position of the main contacts of the circuit breaker is indicated by the following icons:
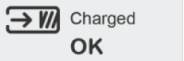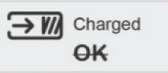
Icon	Description
	The main contacts of the circuit breaker are closed.
	The main contacts of the circuit breaker are opened.
	The main contacts of the circuit breaker are opened and the circuit breaker is tripped. The circuit breaker must be reset.
	The circuit breaker position is unknown in case of contact position discrepancy.

Circuit Breaker Control Mode

The circuit breaker control mode is:

- **Remote control**: The control options on the webpage can be used to control the circuit breaker remotely.
- **Local control**: The control options are not available on the webpage. The circuit breaker is controlled locally through manual operation.

The circuit breaker control status is indicated by the following icons:

Icon	Description
	The closing spring is charged and the circuit breaker is ready to close.
	The closing spring is charged and the circuit breaker is not ready to close.
	The closing spring is discharged and the circuit breaker is not ready to close.

Close inhibition indicates that the circuit breaker closing is inhibited by the EcoStruxure Power Commission software or IO modules or a remote controller through the communication network.

Circuit Breaker Control Options

When the circuit breaker is in remote control mode, the following control options are available:

Control Options	Description
O	Click this option to open the circuit breaker.
I	Click this option to close the circuit breaker. The circuit breaker will close only if it is ready to close.
Reset	Click this option to reset ComPacT NSX or PowerPacT H-, J-, and L-frame circuit breakers.

For each control action:

- A safety message is displayed in a pop-up window.
  - Read the message and click **I understand** to confirm the action.
  - Click **Cancel** to cancel the action.
  - The result of the action (successful or failed) is displayed in a pop-up window.

  NOTE: Pop-up message confirms that the command is successfully sent or not. It does not confirm whether the complete action is successful.

Measurements

The list of measurements displayed depends on the type of MicroLogic of the circuit breaker.

Measurement are shown in the following order:

- Real time measurements with minimum and maximun values. For circuit breaker, the time stamp of the minimum and maximum values is also displayed.
- Energy measurements
- Demand measurements

The minimum and maximum values of the energy and the demand measurements can be reset by users with Installer or Engineer role.

IO Details Layout

If the circuit breaker is connected to 1 or 2 IO modules, the IO module details are displayed.
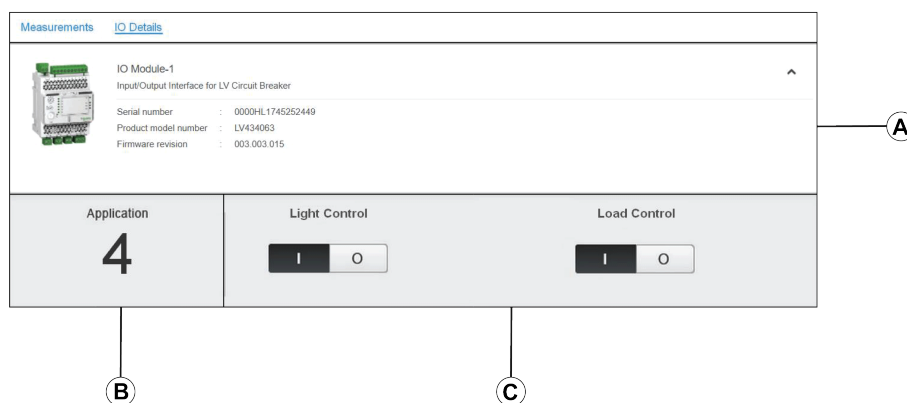
A   IO module identification data

B   Selected predefined application

C   Light and load control options, available if the selected predefined application is 4.

Selected Predefined Application

The number of the predefined application selected by the application rotary switch on the IO module is indicated in the following table:

Application Rotary Switch Position	Predefined Application	Description
1	Cradle management	Monitors the position of the circuit breaker in the cradle.
2	Circuit breaker operation	Controls the opening and closing of the circuit breaker by using the control mode (local or remote) and the inhibit close order.
3	Cradle management and Energy Reduction Maintenance Setting (ERMS)	Monitors the position of the circuit breaker in the cradle and monitors the position of inputs and controls the ERMS mode of the circuit breaker.
4	Light and load control	Controls the light and load application.
5–8	Spare	–
9	Custom	Performs the user-defined applications with the IO module.

For more information, refer to the *IO Module User Guide* in Related Documents, page 7.

Diagnostics Pages

What's in This Chapter

Status

Description

The **STATUS** page displays the IFE server communication status.

While browsing the real-time data views, the IFE server has an automated communication check that runs every 15 minutes by default. This check verifies the communication health of all the devices configured on the IFE server, and attempts to re-establish the communication to any device marked out of service within the current browser session.

The users with installer or engineer roles can make changes to the Diagnostics page settings.

Navigation to the STATUS Page

To view the **STATUS** page, click **DIAGNOSTICS > COMMUNICATION > STATUS**.

Status Parameters

Data	Description
Device Name	Name of the devices connected to IFE server.
Device Type	Type of the devices connected to IFE server.
Connection	Displays the connection type: • Type 1: ULP • Type 2: Serial
Communication	Status of communication: • Passed: IFE server successfully connected to the devices. • Failed: IFE server not connected to the devices.

Ethernet

Description

The **ETHERNET** page displays:

- Ethernet global statistics accumulated since the IFE server was last activated.
- Ethernet port characteristics.

The users with installer or engineer roles can make changes to the Diagnostics page settings.

Navigation to the ETHERNET Page

To view the **ETHERNET** page, click **DIAGNOSTICS > COMMUNICATION > ETHERNET**.

Ethernet Port Characteristics

Statistics	Description
ETH1 Link Speed	Operational speed (10 Mbps or 100 Mbps)
ETH1 Mode	Current mode of operation (full duplex or half duplex)
ETH2 Link Speed	Operational speed (10 Mbps or 100 Mbps)
ETH2 Mode	Current mode of operation (full duplex or half duplex)

Ethernet Global Statistics

Data	Description
Frames Received	Number of frames received
Frames Transmitted	Number of frames transmitted
Click **Reset Counters** to reset to 0 the statistics values.	
If the IFE server is switched off or if it is reset due to a configuration change or another event, the statistics values are reset to 0.	

Modbus

Description

The **MODBUS** page displays the global statistics of TCP/IP and TCP port connections.

The users with installer or engineer roles can make changes to the Diagnostics page settings..

Navigation to the MODBUS Page

To view the **MODBUS** page, click **DIAGNOSTICS > COMMUNICATION > MODBUS**.

Global Statistics Parameters

Global Statistics	Parameter	Description
TCP/IP	**Frames Received**	Number of frames received
	Frames Transmitted	Number of frames transmitted
	Port Status	Status of the connected Ethernet port: • **Operational** • **Idle** If **MODBUS TCP/IP** is disabled, the Port Status value is displayed as **Idle**.
	Opened Connections	Number of active connections
Serial	**Frames Received**	Number of frames received
	Frames Transmitted	Number of frames transmitted
	Error Messages	Number of error messages
Click **Reset Counters** to reset the statistics values to 0.		
If the IFE server is switched off or if it is reset due to a configuration change or another event, the statistics values are reset to 0.		

Modbus TCP Port Connections Parameters

Parameter	Description
Index	Serial number
Remote IP	Remote IP address
Remote Port	Remote port number
Local Port	Local port number
Transmitted Messages	Number of messages transmitted
Received Messages	Number of messages received
Sent Errors	Number of error messages sent

ULP

Description

The **ULP** page displays the global statistics of **ULP** port connection.

The users with installer or engineer roles can make changes to the Diagnostics page settings.

Navigation to the ULP Page

To view the **ULP** page, click **DIAGNOSTICS > COMMUNICATION > ULP**.

ULP Global Statistics

Statistic	Description
Frames Received	Number of CAN frames received successfully
Frames Transmitted	Number of CAN frames transmitted successfully
Max Receive Error	Maximum number of CAN received errors (REC)
Max Transmit Error	Maximum number of CAN transmitted errors (TEC)
Bus off	CAN Bus off count
Max Bus off	Maximum number of bus off counts

Redundancy-RSTP Bridge

Description

The **REDUNDANCY-RSTP BRIDGE** page displays the diagnostic data of RSTP bridge.

The users with installer or engineer roles can make changes to the Diagnostics page settings.

Navigation to the REDUNDANCY-RSTP BRIDGE Page

To view the **REDUNDANCY-RSTP BRIDGE** page, click **DIAGNOSTICS > COMMUNICATION > REDUNDANCY-RSTP BRIDGE**.

General Parameters

Parameter	Description
Bridge Status	Status of RSTP feature. It is either enabled or disabled based on the configuration.
Bridge ID	Unique identifier of this Bridge. It is a combination of MAC address and Bridge Priority of this device.
Root ID	Unique identifier of the Root Bridge. Combination of MAC address and Root Bridge Priority of the Root device
Root Port	The port number that offers the lowest cost path from this bridge to the root bridge. **NOTE:** For the Root Bridge, the value is always 0. For other devices, either 1 or 2.
Root Path Cost	The cost of the path to the root as seen from this bridge.
Total Topology Changes	Total number of topology changes detected by this bridge since the last reset counters.
Click **Reset Counters** to reset the statistics values to 0.	
If the IFE server is switched off or if it is reset due to a configuration change or another event, the statistics values are reset to 0.	

Configured/Learned Parameters

Parameter	Description
Configured Bridge Hello Time	The value of Hello Time configured at this Bridge.
Learned Bridge Hello Time	The actual Hello Time used by the bridge currently. This is the configured Hello Time of the Root Bridge.
Configured Bridge Forward Delay	The value of Forward Delay configured at this Bridge.
Learned Bridge Forward Delay	The actual Forward Delay used by the bridge currently. This is the configured Forward Delay of the Root Bridge.
Configured Bridge Max Age Time	The value of Max Age Time configured at this Bridge.
Learned Bridge Max Age Time	The actual Max Age Time used by the bridge currently. This is the configured Max Age Time of the Root Bridge.

Redundancy-RSTP Ports

Description

The **REDUNDANCY-RSTP PORTS** page displays the diagnostic data of RSTP ports.

The users with installer or engineer roles can make changes to the Diagnostics page settings.

Navigation to the REDUNDANCY-RSTP PORTS Page

To view the **REDUNDANCY-RSTP PORTS** page, click **DIAGNOSTICS > COMMUNICATION > REDUNDANCY-RSTP PORTS**.

Port 1 and Port 2 Parameters

Parameter	Description
State	Current state of the port. By default, it is disabled, blocking, and forwarding. **NOTE:** Other states like listening, learning are intermediate states which are not visible to the user.
Role	Current role of the port in the ring. If the port state is disabled, the role can be either Root or Designated. If the port state is disabled (Ethernet link is down) then the Role is Unknown.
Priority	The value of the port priority is contained in Port Identifier. All ports of a bridge will have a port identifier with format: [1 byte port number][1 byte port priority]. **NOTE:** Following points are provided for understanding the usage of port priority (port identifier). • Port that carries packets to root bridge is root port. When there are multiple such ports exist, one with least Port Identifier becomes the root port, and others will become alternate ports. • Port Number: Port number cannot be configured. In the device the port Number (interface number) for port-1 is 1 and port number for port-2 is 2.
Port Path Cost	The contribution of this port to the path cost of paths towards the Root bridge which includes this port.
Received RST (BPDUs)	Total number of RSTP BPDUs received by this port since the last reset counters.
Transmitted RST (BPDUs)	Total number of RSTP BPDUs transmitted by this port since the last reset counters.
Received TCN (BPDUs)	Total number of Topology Change BPDUs received by this port since the last reset counters.
Transmitted TCN (BPDUs)	Total number of Topology Change BPDUs transmitted by this port since the last reset counters.
Click **Reset Counters** to reset to 0 the statistics values.	
If the IFE server is switched off or if it is reset due to a configuration change or another event, the statistics values are reset to 0.	

SNMP

Description

The **SNMP** page displays the diagnostic data of SNMPV1 Agent parameters.

The users with installer or engineer roles can make changes to the Diagnostics page settings.

Navigation to the SNMP Page

To view the **SNMP** page, click **DIAGNOSTICS > COMMUNICATION > SNMP**.

SNMPV1 Agent Parameters

Parameter	Description
State	Displays the state of SNMPV1 agent.
Received Packets	Number of packets received from the network.
Emitted Packets	Number of packets transmitted from the network.
Emitted Traps	Number of traps transmitted on detection of a change as asynchronous notification from agent to manager.
Received Bad Community Names	Number of received bad community names.
Emitted Bad Community Names	Number of transmitted bad community names.
Click **Reset Counters** to reset the statistics values to 0. If the IFE server is switched off or if it is reset due to a configuration change or another event, the statistics values are reset to 0.	

Read Device Registers

Description

The **READ DEVICE REGISTERS** page allows you to read Modbus registers from the selected device.

Read Procedure

Step	Action	Result
1	From the IFE menu bar, click **Diagnostics**.	Opens the **Diagnostics** menu.
2	From the **Diagnostics** menu, in the **Communication** submenu, click **Read Device Registers**.	Opens the **Read Device Registers** page.
3	From the **Device Name**, select the device.	Selects the device from the drop-down list.
4	Enter **Local ID** (or choose from the defined device list), **Starting Register**, and the **Number of Registers** to read.	Enters the registers to read from the specified device.
5	Select the data type from **Data Type** drop-down list.	Selects the appropriate data type.
6	To change how Modbus data is displayed in the **Value** column, select **Decimal**, **Hexadecimal**, **Binary**, or **ASCII**.	Selects how the data values are displayed.
7	Click **Read**.	Reads the device registered according to the selected configuration.

IFE Read Device Register Parameters

Parameter	Description	Settings
Device Name	Selects a device to read from the list of previously added devices. A Modbus server device of a Modbus client IFE server not defined in the device list can be read by entering its local ID number. **NOTE:** The server device of a remote device not defined in the device list cannot be read by entering its local ID number.	–
Local ID	The address (local ID) of the device that is to be read.	1–247 Factory setting: 1
Starting Register	Register number in decimal.	0–65535 Factory setting: 1000
Number of Registers	The number of registers to read.	1–125 Factory setting: 10
Register	Lists the register numbers in decimal.	–
Value	Lists the data stored for a register. Values retrieved depend on the device connected to the IFE server. Refer to the documentation for the connected device for more information about stored register values.	–
Data Type	Lists the data types available for the device.	• **Holding Registers** (Factory setting) • **Input Registers** • **Output Coils** • **Input Coils**
Decimal, Hexadecimal, Binary, or ASCII options	Select an option to specify how the value column data is displayed.	**Decimal** (Factory setting)

IFE

Description

The IFE page displays the information of the IFE server connected to the circuit breakers.

The users with Installer or Engineer roles can consult the Diagnostics pages.

Navigation to the IFE Page

To view the IFE page, click **DIAGNOSTICS > IFE**.

IFE Server Parameters

Parameter	Description
Serial Number	Device serial number
Commercial Reference Number	Device commercial reference number
Firmware Revision	Current firmware version
Unique Identifier	Combination of MAC address and the time
MAC Address	Unique MAC address
IPv4 Address	IPv4 address of the IFE server
IPv6 Link-local Address	IPv6 address used to communicate on the local network

Date and Time Parameters

Parameter	Description
Time Source	Source of time with which the last synchronization has happened
Last Synchronization	Elapsed time from last synchronization
NTP Synchronization Status	Status of NTP Synchronization
NTP Stratum	Describes the accuracy of NTP time. It can take values from 1 to 15 or as NA (not applicable) if NTP server is not reachable.

File System Parameters

Parameter	Description
Total Size	Total amount of the IFE server disk size in kilobytes
Used Size	Total amount of used disk size on the IFE server disk in kilobytes
Free Size	Total amount of unused disk space on the IFE server disk in kilobytes
Bad Size	Amount of corrupted disk space on the IFE server disk in kilobytes

System Parameters

Parameter	Description
CPU	Status of the CPU: • Nominal • Degraded • Out of service
Boot Memory	Status of the boot memory
EEPROM	Status of EEPROM
File System	Status of the file system
Ethernet PHY 1	Status of PHY 1 hardware
Ethernet PHY 2	Status of PHY 2 hardware
DDR	Status of the execution memory

IFE Operating Time Parameters

Statistic	Description
Operating Time	Operating time of IFE server

Device Name Configuration Procedure

Step	Action	Result
1	From the IFE menu bar, click **Diagnostics**.	Opens the **Diagnostics** page.
2	From the **Diagnostics** menu, in the **Product Information** submenu, click **Device Identification**.	Opens the **Device Identification** page.

List of Parameters in Device Identification

Parameter	Description
Device name	Device name which is updated in the device name field
Product name	Name of the product
Serial number	Device serial number
Product model number	Device model number
Firmware version	Current firmware version
Unique Identifier	Combination of MAC address and the time
MAC address	Unique MAC address
IPv4 address	IP address of the IFE server
IPv6 link local address	Address used to communicate on the local network

Devices

Description

The following devices can be connected under IFE server. However, the Device webpage only displays the connected devices.

- BCM ULP module
- MicroLogic trip unit
- BSCM module
- BSCM Modbus SL/ULP module
- FDM121 display
- IO module IO 1
- IO module IO 2
- USB maintenance interface or Universal Test Adapter (UTA) module

    NOTE: The webpages are supported only for the devices added in the device list.

Navigation to the Devices Page

To view the **DEVICES** page, click **DIAGONASTICS > DEVICES**.

Circuit Breakers Parameters

Parameter	Description
Rated Current	Displays the rated current of the circuit breaker.
Protection Type	Displays the protection type of the circuit breaker.
Number of IO Module	Display the number of IO modules connected to the circuit breaker.
Remaining service life indicator	Display the service life of the circuit breaker.
Contact wear indicators	Display the contact wear counters of the circuit breaker.
Indication contacts (OF) operation since last reset	Display the indication of contact operation of circuit breaker since last reset.
Fault trip indication contact (SDE) operation	Display the indication of fault trip contact operation of circuit breaker.
Cradle connected	Display the status of cradle in connected position.
Cradle disconnected	Display the status of cradle in disconnected position.
Cradle test	Display the status of cradle in test position.

Components Parameters

Device	Parameters	Description
Circuit Breaker	**Product Range**	Name of the device type.
	Product Model	Device model number.
	Serial Number	Device serial Number.

	Commercial Reference Number	Device commercial reference number.
	Firmware Revision	Current firmware version.
IO Module	Serial Number	Device serial number.
	Commercial Reference Number	Device commercial reference number.
	Firmware Revision	Current firmware version.

IFE Server Webpages up to Firmware Version 003

What's in This Part

Webpage Access and User Interface

What's in This Chapter

Access to IFE Webpages

Supported Web Browsers

Browser	Version with Windows XP	Version with Windows Vista	Version with Windows 7 and later
Internet Explorer	IE 9.0	IE 9.0	IE 10.0, IE11.0
Firefox	15.0	20.0	20.0, 45.0
Chrome (recommended)	24.0 and later	24.0 and later	24.0 and later

First Access to the IFE Webpages

The IFE name must be configured during the first access to the IFE webpages.

<table>
<tr><td align="center">⚠ WARNING</td></tr>
<tr><td>POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.

Failure to follow these instructions can result in death, serious injury, or equipment damage.</td></tr>
</table>

The procedure to access the IFE webpages for the first time depends on the operating system of the PC:

- Windows Vista, Windows 7 and later, or newer operating systems
- Windows XP or older operating systems

  NOTE: After updating the IFE server, delete the browser cache before accessing the webpages for the first time.

First Access Through PC with Windows Vista or Windows 7 and Later

Step	Action
1	Disconnect the PC from the local area network (LAN) and switch off Wi-Fi.
2	Connect an Ethernet cable from the PC to the IFE server or to the Ethernet switch inside the panel.
3	Open **Windows Explorer**.
4	Click **Network** and the IFE-**XXYYZZ** appears in the list of devices. **NOTE:** If the IFE name is not displayed in the list of devices in **Windows Explorer**, check if the PC and the IFE server are not connected through the router.
5	Double-click the selected IFE-**XXYYZZ**, the login page automatically opens in the browser.
6	Enter `Administrator` as the user name and `Gateway` as the default password, the home page automatically opens in the browser. **NOTE:** The user name and password are case-sensitive. The `Administrator` user name cannot be changed as it is default user name for administrator role.
7	To change the default password, select the **Configuration and settings** menu, go to **Other Configuration** submenu, click **User Accounts** and enter new password for `Administrator` user name.
8	To locate the IFE-XXYYZZ, select the **Configuration & Settings** menu, go to **General** submenu, click **Device Physical Location**, and click **Blink ON**. The ULP LED of the selected IFE-XXYYZZ blinks for 15 seconds (test mode).

Step	Action
9	To name the IFE-**XXYYZZ**, select the **Configuration & Settings** menu, go to **Device Configuration** submenu, click **Device List** and then click **Name**. Click IFE-**XXYYZZ** to set the IFE name.
10	Write the IFE name on a blank device name label and stick it on the existing one.

NOTE:

- XXYYZZ is the last 3 bytes of the MAC address in hexadecimal format.
- Check the firewall settings if DPWS is not enabled.

First Access Through PC with Windows XP

Step	Action
1	Disconnect the PC from the local area network (LAN) and switch off Wi-Fi.
2	Connect an Ethernet cable from the PC to the IFE server.
3	Start the web browser, page 109. **NOTE:** The PC automatically uses the default IP address 169.254.#.# (#=0–255) and the default subnet mask 255.255.0.0.
4	In the address text box, enter `169.254.YY.ZZ`, where YY and ZZ are the last 2 bytes of the IFE server MAC address (to be found on the IFE server side label), then press **Enter**: the home page opens in the browser. Example: For an IFE with MAC address 00-B0-D0-86-BB-F7 or 0-176-208-134-187-247 in decimal, enter 169.254.187.247 in the address text box.
5	Press **Enter**, the login page automatically opens in the browser.
6	Enter `Administrator` as the user name and `Gateway` as the default password. The homepage automatically opens in the browser. **NOTE:** The user name and password are case-sensitive. The `Administrator` user name cannot be changed as it is default user name for administrator role.
7	To change the default password, select the **Configuration and settings** menu, go to **Other Configuration** submenu, click **User Accounts** and enter new password for `Administrator` user name.
8	To locate the -XXYYZZ, select the **Configuration & Settings** menu, go to **General** submenu, click **Device Physical Location**, go to **Device Physical Location,** and click **Blink ON**. The ULP LED of the selected -XXYYZZ blinks for 15 seconds.
9	To name the -XXYYZZ, select the **Configuration & Settings** menu, go to **Device Configuration** submenu, click **Device List** and then click **Name** to set the IFE name.
10	Write the IFE name on a blank device name label and stick it on the existing one.

NOTE: XXYYZZ is the last 3 bytes of the MAC address in hexadecimal format.

Access to Webpages

Follow the Network Discovery, Name Browsing, and IP Address Browsing process to access the webpages.

The webpage access depends on the IT infrastructure.

Network Discovery

Follow the below procedure to access the IFE webpages once the IFE name has been configured.

Step	Action
1	Connect the IFE server or the Ethernet switch inside the panel to the local area network (LAN).
2	Connect the PC to the local area network (LAN).
3	Open **Windows Explorer**.
4	Click **Network**, the IFE name is displayed in the list of devices. **NOTE:** If the IFE name is not displayed in the list of devices in **Windows Explorer**, check if the PC and the IFE server are not connected through the router.
5	Double-click the IFE name which is written on the device label located on the front face of the selected IFE server, the login page automatically opens in the browser.

Name Browsing

DNS server is mandatory.

Step	Action
1	Connect the IFE server or the Ethernet switch inside the panel to the local area network (LAN).
2	Connect the PC to the local area network (LAN).
3	Start the web browser, page 109.
4	In the address text box, enter the IFE name which is written on the device label located on the front face of the selected IFE server.
5	Press **Enter**, the login page automatically opens in the browser. **NOTE:** If the IFE server does not appear in the list of devices in **Windows Explorer**, check if the PC and the IFE server are not connected through the router.

NOTE: The IFE IP address is mapped to the device label in the DNS server.

IP Address Browsing

IP static configuration has to be set.

Step	Action
1	Connect the IFE server or the Ethernet switch inside the panel to the local area network (LAN).
2	Connect the PC to the local area network (LAN).
3	Start the web browser, page 109.
4	In the address text box, enter IP address given by the IT administrator.
5	Press **Enter**, the login page automatically opens in the browser. **NOTE:** If the login page in the web browser does not open or does not display correctly, check if **Internet Explorer \Tools\Compatibility View Settings\Display Intranet sites in Compatibility View** in Internet Explorer is checked.

User Interface Layout

Overview

This graphic shows the IFE user interface layout.
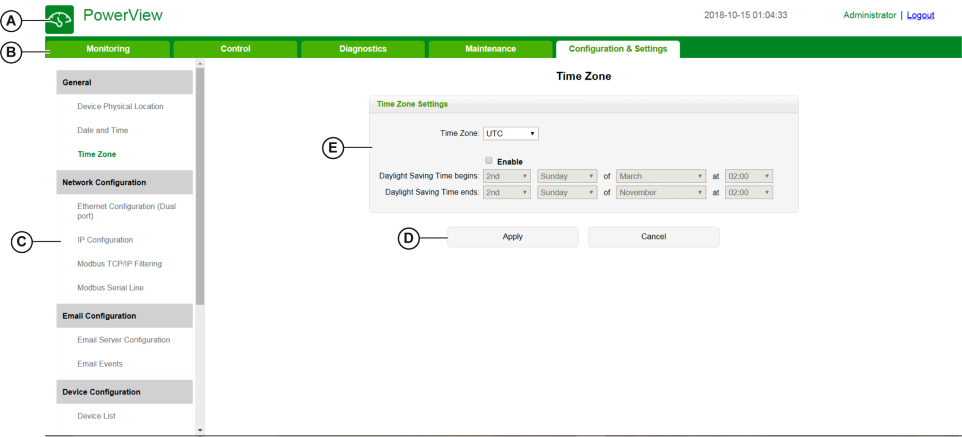
A	Banner
B	Menu tabs
C	Subtabs
D	Action fields
E	Display zone

Banner

The banner displays the following information at the top of all the pages.

Generic Information	Description
Date and time	Current date and time in the format yyyy-mm-dd hh-mm-sec
User name checked	Name of the user who has logged in
Logout	To log out the IFE session, click **Logout** or close your browser. It is recommended to log out from the IFE session when it is not in use.

Main Tabs

The main tabs are:
- **Monitoring**
- **Control**
- **Diagnostics**
- **Maintenance**
- **Configuration & Settings**

Subtabs

The subtabs display the submenus under the selected main tab.

Action Fields

The action fields correspond to the selected tab and it varies.

The following table describes the action fields on user interface layout:

Action Fields	Action
Apply	Applies the changes.
Cancel	Cancels the modifications to return to the last saved settings.

Display Zone

The display zone shows the selected subtab in detail with all the related fields.

Webpage Description

Monitoring Webpage

Monitoring Submenu	Webpage	Description
Real Time Data	**Single Device Pages**, page 151	The single device pages provide basic readings of the selected devices.
	Summary Device Pages, page 151	The summary device pages provide summaries of one or more selected devices.
	Trending, page 152	The trending page view provides real-time graphic and table trending of common topics across multiple devices.
Device Logging	**Single Device Pages**, page 153	The single device pages provide the graphic and table trending logs of user-selectable quantities for selected devices.
	Summary Device Pages , page 156	The summary device pages provide graphic trending logs of multiple devices with a common topic.

Control Webpage

Control Submenu	Webpage	Description
Device Control	**Device Control**, page 158	Resets and controls the connected server devices.
Set Device Time	**Set Device Time**, page 161	Sets the server device time to synchronize with the IFE time and displays the server device time of the selected device.

Diagnostics Webpage

Diagnostics Submenu	Webpage	Description
General	**Statistics**, page 163	Displays diagnostic data used to troubleshoot the network-related problems.
Product Information	**Device Identification**, page 166	• Displays the IFE basic information to set the IFE device name and helps in the device physical location. • Contains information about the product name, serial number, model number, firmware version, unique identifier, MAC address, IPv4 address, and IPv6 link local address.
	IMU Information, page 167	Displays the list of the IMU devices connected to the ULP port.
Device Health Check	**Read Device Registers**, page 168	Displays register data connected locally to the IFE server.
	Communications Check, page 169	Verifies the communications health of all the server devices connected to IFE server.
IO Readings	**IO Readings**, page 170	Displays the status of IO module of the selected device. Displays **No IO modules connected** if the selected device is not connected to a IO module. **NOTE: IO Module** refers to the server device name defined in the **Device List** page.

Maintenance Webpage

Maintenance Submenu	Webpage	Description
Indicators	**Indicators**, page 172	Displays the maintenance counters of the connected ULP devices.

Configuration & Settings Webpage

Configuration & Settings Submenu	Webpage	Description
General	**Device Physical Location**, page 117	- Locate the IFE-XXYYZZ server - Click **Blink ON**. - The ULP LED of the selected IFE-XXYYZZ server blinks and is active for 15 s (Test mode: 1 s ON, 1 s OFF).
	Date and Time, page 118	Sets the date and time manually or sets the IFE time automatically using an SNTP source or configures the server device connected to IFE server to synchronize their time with the IFE time automatically.
	Time Zone, page 120	Configures the time zone for the region and sets the daylight saving time.
Network Configuration	**Ethernet Configuration (Dual port)**, page 121	Configures the Ethernet.
	IP Configuration, page 122	Configures the IP parameters.
	Modbus TCP/IP Filtering, page 124	Configures the maximum number of Modbus TCP/IP server connections. Configures the IP addresses that can access the IFE server through Modbus TCP/IP.
	Modbus Serial Line, page 125	Configures serial communication parameters.
Email Configuration	**Email Server Configuration**, page 126	Configures the alarms to be emailed. Configures the SMTP parameter for mailing purpose.
	Email Events, page 128	Configures the alarms to be sent through email.
Device Configuration	**Device List**, page 136	Configures local serial devices on the Modbus serial daisy chain and IMU core product connected to the ULP port of the IFE server.
	Device Logging, page 140	Configures device logging parameters.
	Device Log Export, page 142	Configures device logging export options.
Other Configuration	**SNMP Parameters**, page 144	Configures Simple Network Management Protocol (SNMP).
	Preferences, page 145	Configures IFE preferences.
	Advanced Services Control, page 146	Configures the advanced service control parameters.
	User Account, page 147	Creates and edits groups and users. Configures email accounts.
	Webpage Access, page 149	Configures webpage access rights for each user group.

Configuration & Settings Webpages

What's in This Chapter

General

Device Physical Location

Step	Action	Result
1	From the IFE menu bar, click **Configuration & Settings**.	Opens the **Configuration & Settings** menu.
2	From the **Configuration & Settings** menu, in the **General** submenu, click **Device Physical Location**.	Opens the **Device Physical Location** page.
3	In **Device Physical Location** webpage, click **Blink ON**.	Sets the IFE server in test mode and the LED blinks in ULP pattern with 1 second ON and 1 second OFF.

Date and Time

Description

The **Date and Time** page allows you:

- To manually set the date and time of the circuit breaker connected to the IFE server
- To automatically synchronize the date and time of the circuit breaker to the IFE time
- To periodically check the synchronization at specified interval of time

List of Parameters in Date and Time Configuration

Parameter	Description
Manual	Allows you to select the manual date and time setting of server devices. This option is disabled when **Automatic (SNTP)** is selected.
Date	Allows you to set the present date manually in the format YYYY-MM-DD.
Time	Allows you to set the present time manually in the format hh:mm:ss.
Automatic (SNTP)	Allows you to select an external time server (SNTP server) for IFE server and synchronize the time of its server devices automatically.
Poll Interval	Allows you to enter the poll interval in hours that ranges from 1 through 63.
Obtain Servers Automatically via DHCP/BOOTP	Allows you to enable the check box that obtains the server address from DHCP or BOOTP.
Primary SNTP/NTP server	Allows you to enter the primary SNTP server address.
Secondary SNTP/NTP server	Allows you to enter the secondary SNTP server address.
Apply	Allows you to automatically synchronize the selected device with the IFE time.
Cancel	Allows you to clear the synchronization of the selected device.

Setting the IFE Date and Time Manually

Step	Action	Result
1	From the IFE menu bar, click **Configuration & Settings**.	Opens the **Configuration & Settings** menu.
2	In the **General** submenu, click **Date and Time** and then select **Manual** from the **Date/Time Settings**.	The parameters for date and time settings is available.
3	Enter the date in the format YYYY-MM-DD.	Sets the date of the IFE server manually.
4	Enter the time in the format hh:mm:ss.	Sets the time of the IFE server manually.
5	Click **Apply**.	The date and time of IFE server is set.

Setting the IFE Date and Time Automatically with SNTP

Step	Action	Result
1	From the IFE menu bar, click **Configuration & Settings**.	Opens the **Configuration & Settings** menu.
2	In the **General** submenu, click **Date and Time** and then select **Automatic (SNTP)** from the **Date/Time Settings**.	The server devices of IFE server are selected by default for date and time synchronization.
3	Enter the poll time in the **Poll Interval** box.	The entered time is updated.
4	Select to obtain SNTP server automatically via DHCP/BOOTP.	The SNTP server address is obtained automatically.
5	Enter the primary and secondary server address in the **Primary SNTP/NTP server** and **Secondary SNTP/NTP server** box.	The entered SNTP server address is updated.
8	Click **Apply**.	The date and time of the selected server devices get synchronized with the IFE time.

Setting the Date and Time of Server Devices

Follow this procedure to set the date and time of server devices of IFE server.

Step	Action	Result
1	From the IFE menu bar, click **Configuration & Settings**.	Opens the **Configuration & Settings** menu.
2	In the **General** submenu, click **Date and Time**.	The selection of server devices and **Every** box is available.
2	In **Date and Time: Periodic Spreading**, select the **Every** check box and enter the time interval.	Allows you to enter the time interval in hours.
3	Select the server devices from the device list which supports date and time setting from external source.	The server devices get selected.
8	Click **Apply**.	The date and time of the selected server devices get synchronized with the IFE time immediately and also periodically as per the selected time interval.

Time Zone

Time Zone Configuration

Step	Action
1	From the IFE menu bar, click **Configuration & Settings**.
2	From the **Configuration & Settings** menu, in the **General** submenu, click **Time Zone**.
3	In **Time Zone Configuration** webpage, select the time zone of your region from the **Time Zone** list.
4	Select the **Enable** check box if you have to set the daylight saving time.
5	Select the beginning and end time of daylight saving from the **Daylight Saving Time begins** and the **Daylight Saving Time ends** list.
6	Click **Apply** to save the settings.

NOTE: The settings of **Time Zone** is applicable only when **Date and Time** is in **Automatic** mode.

Real Time Clock

The IFE server has a real time clock (RTC) to maintain date and time during power outage. The expected life time of the RTC is 15 years when operated at intermediate mode (in this mode, the battery is operated continuously for 4 days with an interval of 45 times over a period of 10 years).

The IFE server must maintain a crystal tolerance of ±20 ppm (typical)/±150 ppm (maximum) during the period of 15 years at -25 °C (-13 °F) to 85 °C (185 °F). The time drift by RTC chip varies from -16 s/day to +2 s/day. During power recycle, the RTC is able to maintain the date and time settings.

Ethernet Configuration (Dual Port)

Ethernet

Parameter	Description	Settings
MAC address	A unique media access control address of an IFE server. The MAC address is written on the label which is placed on the side of the IFE server.	–
Frame format	Used to select the format for data sent over an Ethernet connection. **NOTE:** Whenever the frame format settings are changed, restart the device to implement the changes.	• **Ethernet II** • **802.3** • **Auto** (Factory setting)

Ethernet Port Control

Parameter	Description	Settings
Speed and mode for Port #1	Used to define the physical Ethernet connection speed and transmission mode for Ethernet port 1.	**Auto-negotiation** (Factory setting)
Speed and mode for Port #2	Used to define the physical Ethernet connection speed and transmission for Ethernet port 2.	**Auto-negotiation** (Factory setting)

Broadcast Storm Protection

Parameter	Description	Settings
Level	Defines the broadcast storm protection level. The level value corresponds to a committed information rate (CIR) value, that is, the amount of traffic entering the switch port from which the storm protection drops entering the broadcast traffic. **NOTE:** If the level value is changed, you are prompted to restart the device to implement changes.	Broadcast storm protection level: • **1**: Highest (1000) • **2**: High (2000) • **3**: Medium-High (3000) • **4**: Medium-Low (4000), Default setting • **5**: Low (5000) • **6**: Lowest (6000) **NOTE:** The level value corresponds to the committed information rate.
Committed information rate	Defines the read-only value of the broadcast storm protection level.	–

IP Configuration

IPv4 Configuration

Parameter	Description	Settings
Obtain an IP address automatically using	Used to select the mode for assigning the IPv4 parameters set. Obtain IPv4 parameters automatically using BOOTP or DHCP. **NOTE:** While using a legacy DHCP server, the device name must be limited to 16 characters.	• **DHCP** (Factory setting) • **BOOTP**
Manual IP address	Used to enter the static IP address of an IFE server.	–
Manual Subnet mask	Used to enter the Ethernet IP subnet mask address of your network.	–
Manual Default gateway	Used to enter the gateway (router) IP address used for wide area network (WAN) communication.	–

IPv6 Configuration

Parameter	Description	Settings
Enable IPv6	Defines the IPv6 configuration.	**Enabled** (Factory setting) **NOTE:** The setting is unavailable to edit.
Link local address	Used to open the IFE webpage for future use. **NOTE:** In the URL address box, use [ ] brackets to enter the link local address.	–

DNS

Parameter	Description	Setting
Obtain DNS address automatically	Defines the dynamic behavior of the DNS server address configuration. Used to obtain the IP address from the DNS server automatically. **NOTE:** Domain name system (DNS) is the naming system for computers and devices connected to a local area network (LAN) or the Internet.	Disabled when manual setting is selected.
Manual Primary server address	Defines the IPv4 address of the primary DNS server.	–
Manual Secondary server address	Defines the IPv4 address of the secondary DNS server. Used to perform a DNS resolution when the resolution fails with the primary DNS server.	–

Duplicate IP Address Detection

While connected to your network, the IFE server publishes its IP address. To avoid any duplicate IP address conflicts, the IFE server uses the address resolution protocol (ARP) to see if any other device on your network is using the same IP address. The following table explains how the IFE server handles a duplicate IP address when it is detected.

Duplicate IP Address Scenario

Scenario	Duplicate IP Detected	Network Status LED
Ethernet link detected	Reverts to the default IP address, subnet mask, and gateway address. ARP requests are sent every 15 seconds until the IP address is available. IFE server uses the IP address when it is available,	Steady red
Manual address change	Reverts to the default IP address, subnet mask, and gateway address. The ARP requests are sent every 15 seconds until the IP address is available. The IFE server uses the IP address when it is available.	Steady red
Receives an ARP request	If more than one ARP is detected within 10 seconds, initiate the process to reacquire the IP.	OFF

Duplicate IP Address Scenario

Modbus TCP/IP Filtering

Description

The **Modbus TCP/IP Filtering** page allows you to define the level of access for Modbus TCP/IP clients connected to IFE server.

Block Connections

You can select the maximum number of IP connections allowed, 8 or 16. Each connection can have 12 concurrent transactions simultaneously.

NOTE: When the maximum number of IP connections is changed, a message pops-up on the screen **Max Connection is changed. Restart the Device to Take Effect** and prompts to restart the device.

If IP Filtering is enabled, you must configure the IP address of the PC in the list of allowed addresses with read/write permission for using the EcoStruxure Power Commission software.

IP Filtering

Parameter	Description	Setting
Enable IP Filtering	Activates the IP address filtering. The list of IP addresses available in the table is granted access.	• Enabled • Disabled (No filtering)
IP Address	Filters the required IP address entered by you.	10 addresses (Maximum allowed IP addresses)

Access level	Defines the access level for the corresponding IP address.	• Read: The following Modbus TCP/IP function codes are allowed:
		   ◦ 1 (0x01)
		   ◦ 2 (0x02)
		   ◦ 3 (0x03)
		   ◦ 4 (0x04)
		   ◦ 7 (0x07)
		   ◦ 8 (0x08)
		   ◦ 11 (0x0B)
		   ◦ 12 (0x0C)
		   ◦ 17 (0x11)
		   ◦ 20 (0x14)
		   ◦ 24 (0x18)
		   ◦ 43 (0x2B), with subfunction codes 14 (0x0E), 15 (0x0F), and 16 (0x10).
		   ◦ 100 (0x64)
		• **None**: The access to the IP address is blocked.
		• **Read/Write**: Full access is provided.

Allow Anonymous IP	Allows all Modbus TCP/IP clients to have the read-only access.	• Enabled • Disabled (Factory setting)

Modbus Serial Line

Modbus Serial Line Settings

Parameter	Settings
Baud Rate	• 9600 bps • 19200 bps (Factory setting) • 38400 bps
Parity	• **Even** (Factory setting) • **Odd** • **None**
Nb bits of Stop	• **Auto** (Factory setting) • 1 bit • 2 bits
Serial line termination	• **Enabled** (Factory setting) • **Disabled**
Modbus SL timeout	• 1 s (Factory setting) • 0.1–0.5 s • 1–10 s

NOTE: When **Nb bits of Stop** parameter is set to **Auto**, the actual value is based on the parity chosen.

Email Server Configuration

Introduction

The built-in email alarm notifications are sent through emails when the connected devices trigger an alarm. The alarms are notifications that occur in response to a status change or when a value exceeds a threshold value. The administrator selects and configures several alarm notifications. The recipient list is configurable to notify the several users of the same alarm.

The email alarm notifications require unfiltered Internet access. This level of service is suited for small or mid-sized non-critical buildings. The device sends the emails when Internet access is available through a dedicated connection or through a local area network (LAN) with Internet access.

> **NOTE:** The email alarm notifications should not be used if email services are managed internally by a customer IT domain administrator.

Email Service

Parameter	Description	Setting
My Own SMTP Server	Sets **My Own SMTP Server** profile as the email service in IFE server by default. If you have configured SMTP profile for the previous version of the IFE server, on updating to a newer version, you can still retrieve the saved configuration under **My Own SMTP Server** profile.	–

Email SMTP Server Settings

Parameter	Description	Setting
SMTP server address	Allows you to enter an email server address (SMTP server). **NOTE:** Contact your network administrator to know the IP address or the name of the simple mail transfer protocol (SMTP) server.	–
SMTP server port	Allows you to enter the SMTP server port.	• 25 (default setting) • 465: TLS/SSL • 587: STARTTLS
Authentication	If the SMTP server requires login information, enable the **Authentication Enable** check box.	• **Enabled** • **Disabled** (factory setting)
SMTP account login	Allows you to enter the SMTP account login name.	–
SMTP account password	Allows you to enter the SMTP account password.	–

Email Sender Address

Parameter	Description	Setting
From address	In the **From Address** box, enter the email address of the administrator.	–

The **From address** can be used in different ways:

- Use the **From address** as a context provider: If you do not want to receive any reply, and only notify the recipient, use **From address** as contextual information. The **From address** syntax includes "no-reply", "device name", "site name", @a validated domain .com, .net, and so on.

- Create an alias in the **From address** to allow replies to be sent to the person in charge of an alarm: An email can be sent to multiple people who are responsible for a specific appliance. This feature allows the receivers to reply to follow up with the responsible person.

  For example, the facility manager would receive an email from an alarm. Facility manager can send a reply email to the maintenance contractor to follow up on the action.

Email Language

Parameter	Description	Setting
Language	Allows you to select the language of the email body.	• **English** (factory setting) • **French**

Email Test

Parameter	Description	Setting
Recipient address for test	Allows you to enter the email address of the recipient to test the delivery of the email.	–

The **Email Test** feature enables connection from the device to the service. If the test emails are not received, the Internet connection needs to enable the email ports (port 25 or 587 or 2525). The required setting of the port is done in accordance between the device that sends the email and the site router settings.

NOTE: The email with custom text that uses characters such as à, è, ù, é, â, ê, î, ô, û, ë, ï, ü, ÿ, and ç are not shown correctly in the email. However, the generic text message is shown correctly.

Email Events

Description

The **Email Events** page allows the selection of the events to notify through email among a list of events.

⚠ **CAUTION**

EQUIPMENT INCOMPATIBILITY OR INOPERABLE EQUIPMENT

Do not rely solely on the notification of the emails for maintaining your equipment.

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

The list of event displayed contains only applicable events related to the devices connected to the ULP port of the IFE server.

NOTE: If an email SMTP server is not located on the same Ethernet network segment as IFE server, ensure that the IFE default gateway is properly configured.

Parameter	Description
Events	List of events for configuration
Add Event	A check box to enable to add events.
Email Recipients	Allows you to choose from a list of email recipients. **NOTE:** You can choose a maximum of 12 recipients.
Custom Text	Allows you to enter a custom text. **NOTE:** You can enter a maximum of 63 characters in the custom text area.

Events from ComPacT NSX or PowerPacT H-, J-, and L- Frame Circuit Breakers

Device Connected	Events
ComPacT NSX or PowerPacT H-, J-, and L-frame circuit breaker with BSCM module	Circuit breaker indicator status (OF)
	Fault trip indicator status (SDE)
	Trip indicator status (SD)
ComPacT NSX or PowerPacT H-, J-, and L-frame circuit breaker with MicroLogic 5, 6, or 7 trip unit	Long time protection Ir pre-alarm (PAL Ir)
	Long time protection Ir
	Short time protection Isd
	Instantaneous protection Ii
	Ground fault protection Ig
	Earth leakage (Vigi) protection IΔn
	Integrated Instantaneous protection
	STOP (trip unit internal failure)
	Instantaneous with earth leakage protection
	Reflex tripping protection
	Unbalance motor protection
	Jam motor protection

Device Connected	Events
	Underload motor protection
	Long start motor protection
	User-defined alarm 1
	User-defined alarm 2
	User-defined alarm 3
	User-defined alarm 4
	User-defined alarm 5
	User-defined alarm 6
	User-defined alarm 7
	User-defined alarm 8
	User-defined alarm 9
	User-defined alarm 10

Events from MasterPacT NT/NW, ComPacT NS, or PowerPacT P- and R-Frame Circuit Breakers

Device Connected	Events
MasterPacT NT/NW, ComPacT NS, or PowerPacT P- and R-frame circuit breaker with BCM ULP module	Long time protection Ir pre-alarm (PAL Ir)
	Long time protection Ir
	Short time protection Isd
	Instantaneous protection Ii
	Ground fault protection Ig
	Earth leakage (Vigi) protection IΔn
	Integrated Instantaneous protection
	STOP (trip unit internal failure)
	Reflex tripping protection
	Instantaneous with earth leakage protection
	Unbalance motor protection
	Jam motor protection
	Underload motor protection
	Long start motor protection
	Iunbal protection
	I1 Max protection
	I2 Max protection
	I3 Max protection
	IN Max protection
	Vmin protection
	Vmax protection
	Vunbal protection
	Reverse power protection
	Fmin protection
	Fmax protection
	Phase rotation

	Ready to close status (PF)
	Wear on contacts
	Arc reduction state engaged

Events from MasterPacT MTZ Circuit Breaker

Device connected	Events
MasterPacT MTZ circuit breaker with MicroLogic X control units	Ir trip
	Isd trip
	Ii trip
	Ig trip
	IΔn trip
	Ultimate self-protection trip (SELLIM)
	Self diagnostic trip
	Ultimate self-protection trip (DIN/DINF)
	IΔn/Ig test trip
	Undervoltage on 1 phase trip
	Overvoltage on 1 phase trip
	Reverse power trip
	Undervoltage on all 3 phases trip
	Overvoltage on all 3 phases trip
	Optional protection trip
	Ultimate self-protection (DIN/DINF) operate
	Ultimate self-protection (SELLIM) operate
	Thermal memory reset order
	Ir prealarm (I > 90% Ir)
	Ir start (I > 105% Ir)
	Ir operate
	Isd start
	Isd operate
	Ii operate
	Ig alarm
	Ig start
	Ig operate
	IΔn alarm
	IΔn start
	IΔn operate
	Undervoltage on 1 phase start
	Undervoltage on 1 phase operate
	Undervoltage on all 3 phases start
	Undervoltage on all 3 phases operate
	Overvoltage on 1 phase start
	Overvoltage on 1 phase operate

Device connected	Events
MasterPacT MTZ circuit breaker with MicroLogic X control units	Overvoltage on all 3 phases start
	Overvoltage on all 3 phases operate
	Reverse Power start
	Reverse Power operate
	ERMS engaged
	ERMS engaged for more than 24 hours
	ESM (ERMS switch module) self diagnostic alarm
	Communication lost with ESM (ERMS switch module)
	Request to unlock ERMS by Smartphone
	B curve active
	Optional protections inhibited by IO
	Circuit breaker opened
	Circuit breaker closed
	Closing order sent to XF
	Opening order sent to MX
	Circuit Breaker did not open or close
	Manual mode enabled
	Local mode enabled
	Allow control by Digital input is disabled (by EcoStruxure Power Commission)
	Closing inhibited by communication
	Closing inhibited through IO module
	Alarm reset
	M2C output 1 is forced
	M2C output 2 is forced
	Protection settings change by display enabled
	Remote protection settings change enabled
	Protection settings changed by display
	Protection settings changed by Bluetooth/USB/IFE
	Communication lost with IO#1 module
	Communication lost with IO#2 module
	Config error IO/CU: dual settings or inhibit cls.
	Config error IO/CU: optional protection Inhibit
	Config. error IO and CU - Local/Remote mode
	Date and time set
	Digital module license installed
	Digital module license uninstalled
	Digital module license expired
	Digital module license rejected
	Digital module License expires in 30 days
	Digital module License expires in 20 days
	Digital module License expires in 10 days
	Connection on USB port
	Injection test in progress

Device connected	Events
MasterPacT MTZ circuit breaker with MicroLogic X control units	Ig function inhibited for test propose
	Test aborted by user
	Ig protection in OFF mode
	Control unit self test major malfunction 1
	Control unit self test major malfunction 2
	Control unit self test major malfunction 3
	Control unit self test major malfunction 4
	Control unit self test major malfunction 5
	Internal current sensor disconnected
	External neutral current sensor disconnected
	Internal Current Power Supply (CPS) sensors malfunction
	Partial internal Current Power Supply (CPS) sensors malfunction
	Partial Internal Current Power Supply (CPS) sensors major malfunction
	Earth leakage (Vigi) sensor disconnected
	Protection settings reset to factory values
	Protection settings no accessible # 1
	Protection settings no accessible # 2
	Protection settings no accessible # 3
	Protection settings no accessible # 4
	Protection settings no accessible # 5
	Control unit self test # 1
	Control unit self test # 2
	Control unit self test # 3
	Control unit self test # 4
	Control unit self test # 5
	Invalid measurement and optional protection # 1
	Invalid measurement and optional protection # 2
	Invalid measurement and optional protection # 3
	Invalid optional protection self test
	NFC invalid communication #1
	NFC invalid communication #2
	NFC invalid communication #3
	Invalid display screen or wireless communication # 1
	Invalid display screen or wireless communication # 2
	Invalid display screen or wireless communication # 3
	Loss of IEEE 802.15.4 communication
	Loss of Bluetooth communication
	Replace Battery
	No battery detected
	Control Unit alarm reset
	Self diagnostic test - firmware
	Unable to read sensor plug
	Invalid Control Unit factory config #1

Device connected	Events
MasterPacT MTZ circuit breaker with MicroLogic control units	Invalid Control Unit factory config #2
	Critical hardware modules discrepancy
	Critical firmware modules discrepancy
	Non-critical hardware modules discrepancy
	Non-critical firmware modules discrepancy
	Firmware discrepancy within control unit
	IΔn/Ig test - no trip
	IΔn/Ig test button pressed
	ZSI test in progress
	Contact wear is above 60% Check contacts
	Contact wear is above 95% Plan for replacement
	Contacts 100% worn out CB needs to be replaced
	Less than 20% CB operation remaining
	CB has reached the max number of operations
	Invalid self test - MX1 shunt trip
	MX1 shunt trip not detected
	MCH charging operations above threshold
	MCH has reached the max number of operations
	Invalid self test - XF shunt close
	XF shunt close not detected
	Invalid self test - MN undervoltage release
	MN undervoltage release not detected
	Voltage loss on MN undervoltage release
	Communication loss on MN undervoltage release
	Invalid self test - MX2 shunt trip
	MX2 shunt trip not detected
	Presence of external 24V power supply
	Loss of voltage and CB is closed
	Events in history log have been erased
	Reset Min/Max currents
	Reset Min/Max voltages
	Reset Min/Max power
	Reset Min/Max frequency
	Reset Min/Max harmonics
	Reset Min/Max power factor
	Reset current demand
	Reset power demand
	Reset energy counters
	Bluetooth communication enabled
	ZigBee communication enabled
	Connection on Bluetooth port
	Underfrequency trip
	Overfrequency trip

Device connected	Events
MasterPacT MTZ circuit breaker with MicroLogic control units	Underfrequency start
	Overfrequency start
	Underfrequency operate
	Overfrequency operate
	Diagnostic data (link)
	Last event sequence number
	voltage release operation counter is above alarm threshold
	voltage release has reached the max number of operations
	MX2 voltage release operation counter above alarm threshold
	MX2 voltage release reached the max number of operations
	MX1 voltage release operation counter above alarm threshold
	MX1 voltage release reached the max number of operations
	MN undervoltage release operation counter is above alarm threshold
	MN undervoltage voltage release reached the max number of operations
	Schedule basic maintenance within one month
	Schedule standard maintenance within one month
	Schedule manufacturer maintenance within three months
	After 6 months of commissioning protection settings still set to factory default
	Remaining service life of MicroLogic below alarm threshold
	MicroLogic control unit reached the max service life
	Last modification of protection settings not completely applied
	Frequency based protection
	IDMTL long time trip
	IDMTL long time start
	IDMTL long time operate
	Forward directional overcurrent trip
	Reverse directional overcurrent trip
	Forward directional overcurrent start
	Reverse directional overcurrent start
	Forward directional overcurrent operate
	Reverse directional overcurrent operate
	Forward directional overcurrent received
	Reverse directional overcurrent received
	Forward directional overcurrent sent
	Reverse directional overcurrent sent

Events from IO Modules

Device connected	Events
IO module 1	Threshold overrun on Input 1 counter (#1)
	Threshold overrun on Input 2 counter (#1)
	Threshold overrun on Input 3 counter (#1)
	Threshold overrun on Input 4 counter (#1)

Device connected	Events
	Threshold overrun on Input 5 counter (#1)
	Threshold overrun on Input 6 counter (#1)
	Switchboard Temperature threshold 1(#1)
	Switchboard Temperature threshold 2 (#1)
	Switchboard Temperature threshold 3 (#1)
	IO module Failure (STOP mode) (#1)
	IO module Failure (ERROR mode) (#1)
IO module 2	Threshold overrun on Input 1 counter (#2)
	Threshold overrun on Input 2 counter (#2)
	Threshold overrun on Input 3 counter (#2)
	Threshold overrun on Input 4 counter (#2)
	Threshold overrun on Input 5 counter (#2)
	Threshold overrun on Input 6 counter (#2)
	Switchboard Temperature threshold 1(#2)
	Switchboard Temperature threshold 2 (#2)
	Switchboard Temperature threshold 3 (#2)
	IO module Failure (STOP mode) (#2)
	IO module Failure (ERROR mode) (#2)
IO module 1 or IO module 2	Disconnection of the circuit breaker from cradle is overdue
	Cradle has reached its maximum number of operations
	Remaining service life of cradle is below alarm threshold
	New MicroLogic unit has been detected
	Discrepancy with ERMS orders
	Earth leakage trip signal contact (SDV) alarm
	Control voltage presence contact alarm
	Surge protection status contact alarm
	Surge failure contact alarm
	Switch disconnector ON/OFF indication alarm contact (OF)
	Fuse blown indication contact alarm
	Emergency Stop alarm
	Switchboard temperature contact alarm
	Switchboard ventilation contact alarm
	Switchboard door contact alarm
	Cradle connected position status (CE)
	Cradle disconnected position status (CD)
	Cradle test position status (CT)

Device List

Description

The **Device List** page is used to define the list of devices connected to the IFE server (ULP port, serial port) and remote Modbus/TCP server devices. In the device list, you can add, delete and/or discover devices.

The list of connected devices is defined by either of the following:

- Automatically, by using the device discovery procedure.
- Manually, by adding the devices one by one.

  NOTE: The webpages are supported only for the devices added in the device list.

Number of Modbus Server Devices

A maximum of 20 server devices can be added in the device list. Under each IFE server or remote Modbus client device, a maximum of 11 IFM interfaces can be added.

The application dictates the maximum server devices or IFM interfaces that can be used. The following general guidelines can be used to size the application:

- Maximum of 20 server devices are technically supported via the IFE webpages.
- Maximum of 11 IFM interfaces can be physically connected to one IFE server. This can be used for applications that have the lowest performance requirement and are recommended for simple applications.
- Maximum of 8 IFM interfaces should be used for applications that requires regular access via the IFE webpages or that have other Modbus clients communicating, such as FDM128 display. This normally provides a reasonable response time for up to three Modbus clients.
- The number of IFM interfaces that can be stacked in a more complex environment, for example, with SCADA or Building Management Systems must be scaled to the performance needs in the application.

Device List Parameters

Parameters	Description	Settings
IP Address	Displays the device IP address. • For IFE server: The **IP Address** box is unavailable to edit. • For remote device: Allows you to enter IP address in the **IP Address** box.	–
Gateway	Indicates if the IP device is a gateway or not. • For IFE server: The **Gateway** check box is always selected. • For remote device: Allows you to add/discover the server devices of remote device when you select the **Gateway** check box.	**Gateway** check box is always selected.
Address	Displays the Modbus server address of the IFE server and the remote device. • For IFE server: The **Address** box is unavailable to edit. • For remote device: Allows you to enter the Modbus server address of the remote device in the **Address** box.	• For IFE server: 255 (fixed) • For remote device: (1–247 or 255)

Parameters	Description	Settings
Name	Allows you to enter the names for IFE server and remote device. **NOTE:** • The LV breaker system is uniquely identified over possible interfaces such as HMI, Modbus/TCP, DPWS, and DHCP. • IFE device name is common across all interfaces. Thus, changing IFE device name by any means has direct impact on all the connected interfaces.	The IFE name can have up to 63 ASCII characters with the following characters: **A–Z**, **a–z**, **0–9**, and **-**. However, **-** cannot be used at the end of the name. **NOTE:** • IFE name should be unique within the device list. • Duplicate IFE names for different devices may have impact on web applications, logging, and export features.
Connection	Displays the connection type. It is unavailable to edit.	The 2 types of port are: • **ULP** port • **Serial port**
Device Type	Allows you to select the server devices from the list of supported devices, page 176.	–
Device Name	Allows you to enter the name for the discovered devices. • For **ULP** port: Click **edit**, and then click **Device Name** to edit the device name, • For **Serial port**, remote device, and its servers: Click **Device Name** to edit the device name. **NOTE:** Delete and edit operations are not allowed if the device is selected for logging.	The device name can have up to: • 63 ASCII characters for MasterPacT MTZ devices • 45 ASCII characters for other devices The allowed characters are: **A–Z**, **a–z**, **0–9**, and **-**. However, **-** cannot be used at the end of the name.
Server ID	Displays the local address of the device connected to the IFE server or remote device.	• For **ULP** port: 255 (Fixed) • For **Serial port** and remote device: 1–247
Add Remote Devices	Allows you to add remote devices. Using this feature, you can also add PowerTag energy sensors in the **Device List**. These PowerTag energy sensors are preconfigured with Smartlink SI B or Smartlink SI D device. For more information, refer to *Smartlink SI B User Manual* or *Smartlink SI D User Manual* accordingly.	–
Apply	Allows you to save device list configuration.	–
Delete	Allows you to delete the selected server devices. **NOTE:** Delete operation is not allowed if the device is selected for logging.	–
Discover	Allows you to discover the server devices. **NOTE:** The **Discover** option for the remote device is available only if you click the **Apply** button. **NOTE:** The discover option for the device type BCM-OF/SD is available only on IFE's own IMU.	–
⊞	Allows you to add a new server device to the device list.	–
Delete Remote Device	Allows you to delete the remote device. **NOTE:** Delete operation is not allowed if the device is selected for logging.	–

Adding Device to the Device List for the First Time

Step	Action	Result
1	server device to IFE server: Add the server devices to the IFE server manually, page 139 or by device discovery, page 138.	Adds the server device to IFE server.
2	Remote device: In the **Device List** page, click **Add Remote Devices** to add a remote device.	Adds the remote device in the **Device List** page.
3	Server device to remote device: Add the server device for remote device by device discovery. **NOTE:** The **Discover** option for the remote device is available only if you click the **Apply** .	Adds the server device to remote device.
4	Repeat step 2 and 3 to add more remote devices to **Device List** page. Click **Apply** to save the modified changes.	–

Device Discovery Procedure

When you start device discovery, the IFE server queries the ULP port, serial port, and Ethernet port using a user-defined address range. Modbus RTU protocol is used for discovery on the serial port. If the device replies to the query, the local ID is set to the current discovery address, and the device is given a default device name. The IFE server, then tries to identify the device type. If the IFE server recognizes the device type of the discovered device, the IFE server sets the recognized device type in the **Device Type** field. If the IFE server does not recognize the **Device Type** of the discovered device, the IFE server sets to Modbus in the **Device Type** field.

The list of devices supported by the IFE server is in Appendix, page 175.

The table shows the steps to add device using device discovery procedure:

Step	Action	Result
1	From the IFE menu bar, click **Configuration & Settings**.	Opens the **Configuration & Settings** menu.
2	From the **Configuration & Settings** menu, in the **Device Configuration** submenu, click **Device List** .	Opens the **Device List** page.
3	To discover locally connected devices, click **Discover**.	Opens the **Device Discovery** page.
4	Enter **Start Modbus ID** and **Stop Modbus ID**.	Enters the discovery address range.
5	Select **Discover Wireless Devices**. **NOTE:** This option is available if the selected remote device is Smartlink SI B or Smartlink SI D and the device is selected by default.	• If **Discover Wireless Devices** option is selected, the PowerTag energy sensors with Modbus server ID range150...169 is searched in addition to the server devices given in the **Start Modbus ID** and **Stop Modbus ID**. • If the **Start Modbus ID** and **Stop Modbus ID** range overlaps with PowerTag energy sensor Modbus ID range (150...169), then **Discover Wireless Devices** option is ignored during discovery. Only the devices in the given range of the **Start Modbus ID** and **Stop Modbus ID** is searched. • If the selected remote device is Smartlink SI D, then the **Start Modbus ID** and **Stop Modbus ID** is preset with values 150 and 169 respectively and is disabled. The **Discover Wireless Devices** option is selected and disabled.
6	Click **Start Discover**. (Click **Stop Discover** to stop the process).	Begins to discover all connected devices.

Step	Action	Result
	NOTE: Discovery only finds local serial Modbus devices connected to the IFE server. The device on the ULP port is discovered automatically.	
7	Enter a new device name in the **Name** text box.	Renames the device.
8	Select the **Save** check box for the device to be saved in the device list.	Selects or deselects a device entry to be saved or removed.
9	Click **Apply** in the **Device Discovery** page.	Displays the saved device list.

Device Discovery Parameters

Parameters	Description	Setting
Start/Stop Modbus ID	Defines the Modbus server address range that is to be used to discover devices on the IFE serial port.	• **Start Modbus ID:** 1–247 (Factory setting: 1) • **Stop Modbus ID:** 1–247 (Factory setting: 10)
Save	Allows you to save the selected device to the **Device List**.	–
IP Address	Displays the IP address of the IFE server or the remote device.	–
Defined	Lists the device type that was defined for this device.	–
Assigned	Allows you to assign the device type from the drop-down list.	–
Name	Allows you to enter a custom name for the device.	–
Local ID	The server address of the device connected to the IFE server.	–
Status	Displays the discovery or validation status.	• Attempting (trying to determine the device type that matches in the device list.) • Discovering (query attempt of device which is not in the device list.) • Found (device found but the device type does not match what is defined in the device list.) • Unknown (device found but the device type is unknown.) • Valid (device type identified and matches what is defined in the device list.) • Failed (failed to communicate with the device.)

Adding a Device Manually

Step	Action	Result
1	From the IFE menu bar, click **Configuration & Settings**.	Opens the **Configuration & Settings** menu.
2	From the **Configuration & Settings** menu, in the **Device Configuration** submenu, click **Device List**.	Opens the **Device List** page.
3	Click the icon to add a new device.	Allows you to add device in the device list.
4	Choose the supported device from the **Device Type** list.	Selects the device type selected from the list.
5	Enter a new device name in the **Device Name** text box.	Renames the device.
6	Enter the local address of the device in the **Local ID** text box.	Displays the local address of the device.
7	Click **Apply**.	A new device is added to the list.

Device Logging

Description

Logging is available for the devices which are in the device list, page 136. The logging contents can be customized using topics. Topics are the parameters for a device that can be selected to have the desired logging content. The number of log entries per device is fixed irrespective to the number of topics selected for that device. The IFE server can log data received at predefined intervals (5, 10, 15, 20, 30, and 60 minutes). Below is an explanation of how the IFE server logs data and how to set up logging for a device.

NOTE: Device information in the **Device List** page cannot be edited if the device logging for that device is selected.

Logging Interval

Many devices in a power monitoring system do not have the ability to record data in non-volatile memory. The IFE server provides this data logging at predefined intervals for up to 13 devices.

The features of IFE data logging are:

- The maximum number of log entries per device is fixed to 12960.
- Select maximum of 13 devices for data logging.
- Select maximum of 24 topics per device for data logging (topics are kVAh, kWh, kVARh, and so on).
- Select the desired device and list of topics for data logging.

  NOTE: Number of days of logging is impacted only by the log interval selected. It is independent of number of devices selected, number of topics selected per device, and type of topic selected.

Logging interval is a predefined time for the IFE server to log data received from the device. The logging capacity of a device is calculated by multiplying the log capacity factor with the logging interval set in the **Device Logging** page.

Logging capacity (in days) = Log capacity factor * logging interval (in minutes)

The log capacity factor is 9 and is calculated as follows:

Log capacity factor = 12960/1440

Where:

- 12960 is the maximum number of log entries per device
- 1440 is the number of minutes per day

Example: If the **Logging Interval** in the **Device Logging** page is set to 5 minutes, then the logging capacity is 45 days.

The table shows the logging capacity for the corresponding logging interval:

Logging Interval (Minutes)	Logging Capacity (Days)
5	45
10	90
15	135
20	180
30	270
60	540

Interval Logging Setting Procedure

Each device (except Smartlink Ethernet and Smartlink Modbus) in the device list may be independently enabled for logging. Topics to log are unique to each device. To view interval data logs, refer to Device Logging, page 153 in **Monitoring** menu.

> **NOTE:** To enable the **Device Logging** feature, there must be a time value selected from the **Logging Interval** drop-down list. It is recommended to disable the logging feature for the specific device being configured. To do this, clear the logging check box for the device being selected.

Logging

To disable logging, select the logging interval as **Disabled**, ensure that the logging selections are cleared, then click **Apply**.

Purge Data

To delete a data log, check **Purge Data** for the topics to be deleted.

Customize

To customize logging content, enable device logging. Click **Topics** under **Customize** for the device to be configured.

Device Log Export

Description

The **Device Log Export** page is used to export the device logs automatically by IFE server. The device log export allows you to configure IFE server to export device logs periodically. You can choose to export the device log files through email or FTP.

NOTE: If the email and the FTP servers are not located on the same Ethernet network segment as the IFE server, ensure that the IFE default gateway is properly configured.

Transport

Parameter	Description	Setting
Disabled	When **Disabled** is selected, either email or FTP is enabled.	–
Email	Allows you to choose the way of exporting the log files through email.	–
FTP	Allows you to choose the way of exporting the log files through FTP. **NOTE:** When **FTP** is selected, **Test FTP** is enabled.	–
Test FTP	Sends the text file to the FTP server configured in the FTP parameters. The text file contains the device information, and the device name with the date and time.	–
Incremental	Selects only the new interval data logged since the last successful data export. **NOTE:** • If the transport is scheduled for **Hourly** or **Logging Interval**, the incremental check box is selected automatically and is unavailable to be cleared. • If the **Incremental** check box is not selected, the complete log file is sent through an email as an attachment on each scheduled interval.	–
Manual Export	Allows you to export the accumulated log files manually.	–

Schedule

Parameter	Description	Setting
Logging Interval	Selects how often the data logs are sent.	• **Hourly** • **Daily** • **Weekly** • **Monthly** • **Logging Interval**

To Addresses

Parameter	Description	Setting
To Addresses	Lists the email recipients configured in the IFE user accounts.	–

FTP Parameters

Parameter	Description	Setting
Server IP Addresses	Allows you to enter the FTP server IP address.	–
Server TCP Port	Allows you to enter the server port number.	–
Directory	Allows you to select the directory where you want the files to be saved.	–
Username	Allows you to enter the FTP username.	–
Password	Allows you to enter the FTP password.	–
Passive	Allows you to select the mode of FTP operation. **NOTE: Passive** mode is enabled by default.	–

SNMP Parameters

Manage IP Parameters

The IFE server supports SNMP, allowing a network administrator to access remotely an IFE server with an SNMP manager and to view the networking status and diagnostics of the IFE server in the MIB-II format.

Parameter	Description	Setting
Manager One	Allows you to configure the IP address of SNMP manager one.	−
Manager Two	Allows you to configure the IP address of SNMP manager two.	−
System Contact	Allows you to configure the SNMP system contact name.	−
System Name	Allows you to configure the system name.	−
System Location	Allows you to configure the SNMP system location.	−
Read-only Community Name	Allows you to configure the SNMP read-only community name.	**Public** (Factory setting)
Read-write Community Name	Allows you to configure the SNMP read-write community name.	**Private** (Factory setting)
Trap	Allows you to trap the community name.	**Alert** (Factory setting)

NOTE: Only SNMP version 1 is supported.

Enabled Traps

Parameter	Description	Setting
Coldstart Trap	Generates a trap when the IFE server is powered ON.	−
Warmstart Trap	Not supported	−
Linkdown Trap	Generates a trap when an Ethernet port communication link is disconnected.	−
Linkup Trap	Generates a trap when an Ethernet port communication link is reconnected.	−
Authentication Failure Trap	Generates a trap when an SNMP manager is accessing the IFE server with incorrect authentication.	−

Preferences

General Settings

Parameter	Description	Setting
Equipment Name	Displays the equipment name. This name is used in the web interface banner. **NOTE:** The device name can be updated in the **Name** field of the **Device Configuration** submenu in the **Configuration & Settings** menu.	–
Real Time Sample Rate	Controls how often data is read from the device in the standard monitoring table views.	5–60 s Factory setting: 5 s
Communications Check Rate	Controls how often a communications check is performed while the browser is displaying real-time readings in the standard monitoring table views. This function attempts to bring any out-of-service devices back into service automatically.	5–30 min Factory setting: 15 min

Advanced Services Control

Industrial Protocol

Parameter	Description	Setting
Enable Modbus/TCP	Allows you to enable/disable the Modbus/TCP service.	• Enabled (Factory setting) • Disabled

Services Configuration

Parameter	Description	Setting
Enable FTP server	Allows you to enable/disable the FTP service.	• Enabled (Factory setting) • Disabled
Enable device announcement	Allows you to enable/disable the DPWS service.	• Enabled (Factory setting) • Disabled
Enable SNMP	Allows you to enable/disable the SNMP service.	• Enabled • Disabled (Factory setting)

User Accounts

Description

The IFE users are assigned with user names and passwords. Each user belongs to a group, and each group has access rights to the IFE webpages assigned by the IFE administrator.

NOTE: There are two pre-defined user accounts:

- Administrator (the default password is `Gateway`)
- Guest (the default password is `Guest`)

Groups

To change the group name, enter a new name in one of the group text boxes.

NOTE: The administrator group name cannot be changed.

Password

⚠ **WARNING**
POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY
Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.
Failure to follow these instructions can result in death, serious injury, or equipment damage.

A password can be changed on the User Accounts webpage.

A password is composed of 0 to 11 characters. It is case-sensitive and the allowed characters are:

- Digits from 0 to 9
- Letters from a to z
- Letters from A to Z
- Special characters as *, /, \, etc.

NOTE: The password with eleven stars (***********) is not allowed.

Users

Parameter	Description
Name	Enter a name (1 to 15 characters) for a new user. **NOTE:** User names are case-sensitive and can contain only alphanumeric characters.
Password	Enter a password (0 to 11 characters) for a new user.
Email ID	Enter a valid email address for the selected name.
Group	Select a group for the new user.
Language	Select the language for the new user and click **Apply** to view the webpages in the selected language. **NOTE:** When the administrator switches to a different language for the user account, make sure to refresh the webpage manually to display the webpages in a selected language.

NOTE: The maximum number of user-defined accounts are 11.

IFE Accounts and Passwords

Accounts	Password
Administrator	Gateway
Guest	Guest
User-defined accounts (11 accounts possible)	User-defined passwords

NOTE:

- You can change your password.

- If you forget the password, contact your local Schneider Electric service team for retrieving the password.

Webpage Access

Group Access

Group	Access
Administrator	Full access to all webpages.
	NOTE: It is recommended to change the default administrator password for system security the first time you log in.
Guest	Read-only access to selected webpages.
User-defined groups	Choosing from the following options, the administrator assigns webpage access for each group. The access levels are as follows:
	• **None**: A group has no access to selected webpage
	• **Read-Only**: The password grants a group read-only access to the selected webpage
	• **Full**: A group has the same access as the administrator group to the selected webpage

NOTE:

- The **Webpage Access** is available for the **Administrator** only.
- The **Administrator** has full access to all the webpages.

Monitoring Webpges

What's in This Chapter

Real Time Data

Description

The **Real Time Data** page provides:

- the basic readings of the selected devices in real time on **Single Device Pages**.
- the device summaries on **Summary Device Pages**.
- the real-time trending for the selected device for the selected topics on **Trending**.

  NOTE: Refresh the webpage by action on the function key **F5** when out of service is displayed.

Single Device Pages

This page displays the basic readings of the selected devices on real-time basis. This includes circuit breaker health status with green, orange, and red indication, cradle status, load current, power, power factor, voltage, and so on.

The table shows the steps to monitor the real-time data of a device:

Step	Action	Result
1	From the IFE menu bar, click **Monitoring**.	Opens the **Monitoring** menu.
2	From the **Monitoring** menu, in the **Real Time Data** submenu, select a device from **Single Device Pages**.	Displays the real-time data of the selected device.

For BCPM devices, the auxiliary and branch circuit parameters can be monitored for real-time values. If you have Administrator privilege, you can modify or configure the circuit names for BCPM devices.

Summary Device Pages

The summary device table views provide summary of one or more selected devices.

Step	Action	Result
1	From the **Monitoring** menu, in the **Real Time Data** submenu, click **Summary Device Pages**.	Expands the tree for summary page selection choices.
2	Select the **Summary Page** to be viewed.	Opens the device selection list.
3	Select the devices from the **Available Devices**, then click **Apply**. **NOTE:** Click **select all** to select all the available devices. Click **clear all** to clear all the selected devices.	Summary of the selected device appears. **NOTE:** Click **New selection** to navigate back to the device selection list.

Trending

Step	Action	Result
1	From the IFE menu bar, click **Monitoring**.	Opens the **Monitoring** menu.
2	From the **Monitoring** menu, in the **Real Time Data** submenu, select **Trending**.	Expands the data tree for real-time data option selection and the time trending option selection.
3	Select **Real Time Trending**.	Opens the real-time trending setup page.
4	Select up to 4 devices from the **Available Devices** list.	Selects devices for trending.
5	Select the topics from the **Available Topics** list. **NOTE:** Only topics common to all selected devices are available for trending. The maximum number of topics to trend is dependent on the number of devices selected.The multiplication (product) of the selected devices and the selected topics must be 8 or less.	Selects topics for trending.
6	Click **Apply** to open the **Real Time Trending** display page.	Opens the real-time trending display page.
7	Set the trending parameters.	Allows trending parameters to be set.

Trending Parameters

Step	Action	Result
1	Select **Absolute** or **Relative** trending. **NOTE: Absolute** redraws the x-axis in the graph after each sample, filling it with all the data collected since the start of the trend. The **Relative** updates the graph with the latest data after each sample while the x-axis stays constant to show the overall trend time selected.	Selects graph mode.
2	Choose a trend time from 1–15 minutes. This is the duration of the trend. **NOTE:** Data samples are taken as fast as possible but may take longer depending on the communications load on the Modbus-SL port.	Selects the amount of time of the trend.
3	Select **Start Sampling** to start the trending of the selected device topics. **NOTE:** Trending may be stopped before reaching the trend time by clicking **Stop Sampling**. If **Start Sampling** is pressed after stopping the sampling, a new trend is started.	Starts trending.
4	Press **Data Points** to view a log of all the sampled topics recorded during the trend time.	Displays a log of all topic values sampled during the trend.
5	Press **New Selection** to reselect the devices and topics to trend.	Navigates back to the real-time trending setup page.

Device Logging

Introduction

The **Device Logging** page provides the graphic and table representations of the selected device log data. For more details on configuring device logging, refer to Device Logging, page 140.

Single Device Pages

Step	Action	Result
1	From the IFE menu bar, click **Monitoring**.	Opens the **Monitoring** menu.
2	From the **Monitoring** menu, click **Device Logging**.	Expands tree to show available device logging choices.
3	From the **Device Logging**, click **Single Device Pages**.	Expands tree to show available devices that have logged data available for viewing.
4	Select a device from the **Device List**.	Displays the device log for the selected device.
5	To view a data range, select a period range from the period range drop-down list: • **Last Full Day** • **Last Full Week** • **Last Full Month** • **All**	Plots the selected period range.
6	Hold the left mouse button and drag a selection box around a graph area to zoom in on it.	Zooms in on the selected graph area.
7	To return to the original full view, enter **Z** on your keyboard, or double-click the graph.	The view zooms out.
8	Click **Data Points** to view the selected interval data log table.	Opens the selected **Interval Data Log** table.
9	To view different topics, click **New Topic(s)**. Enable the check boxes of the topics to be displayed, and click **Apply**.	Enables the display of the selected topics.

The data logged from each device is displayed in a webpage in a time-trend chart format. The time-trend chart is preconfigured to display data from the **Last Full Day**, **Last Full Week**, **Last Full Month**, or **All**.

Energy parameters are logged as accumulating values but are displayed as incremental values on an interval basis. All other parameters are logged and displayed as the actual value recorded.

Retrieving a Data Log

Interval data logs can be retrieved using the methods given in the following table:

Retrieval Method	File Format Retrieved
IFE FTP server	Comma-separated variable (CSV)
Export to an external FTP server	CSV
Data point button	HTML
Email	CSV

To view the list of all the available log files, follow steps 2 to 4 in the section Getting an Interval Data Log using FTP, page 155. Files are in the format: *Device Name.csv* where the device name is the name given to the server device. For example, a device named building 1 utility entrance is *Building 1 Utility Entrance. csv*.

When the log files are exported, the date and time are appended to the file name in the following format: _YYYYMMDDHHMMSS. For example, *Building 1 Utility Entrance_20100218115216.csv*. This indicates that the file was exported on 2010 February 18 at 11:52:16 AM.

NOTE:

- The circuit breaker status in log file is coded by numbers. For information on circuit breaker status, refer to the description of the Modbus register 12001 in the .

- The device log file may contain invalid values (-9999, -99999, 32768) for electrical parameters based on the data read from the device.

Log Format

Data is logged in the CSV file with the following format:

Row	Data in CSV Format	Description
1	IFE name, IFE serial number, IFE address, device name, device local ID, device type name, logging interval.	This row contains the column headings for the information in row 2.
2	IFE 555, 23227,157.198.184.116, building1 utility entrance, 893, MasterPacT MTZ,15	This row contains the information about the IFE server and the logged device.
3	This row is blank.	–
4	,,,topic id 1,topic id 2,topic id 3	This row contains the column headings for the topic IDs in row 5. A topic ID is a numerical reference to the quantity being logged. Topic IDs are used to identify the quantity, regardless of the device or language. The first three commas are used for layout purposes in a spreadsheet application.
5	,,,1617,1621,1625	This row contains the topic IDs of the values logged.
6	This row is blank.	–
7	Error, UTC offset (Minutes), local time stamp, apparent energy (kVAh), real energy (kWh), reactive energy (kVARh)	This row contains the column headings for the data logged in rows 8 and higher.
8 and higher	These rows contain the logged data. 0,-300,2008-10-09 14:15:00,1400738.219,1201962.707,647069.906,15 0,-300,2008-10-09 14:20:00,1400758.260,1201980.725,647078.602,15 0,-300,2008-10-09 14:25:00,1400778.198,1201998.661,647087.233,15	

If a spreadsheet application is used to view the CSV file, data should look similar to the interval data log opened in a spreadsheet application.

Error Codes for Data Logs

The following error codes may be seen when troubleshooting data logs:

Error Code	Definition
19	Communication error occurred (for example: CRC, protocol, or exception).
25	Timeout occurred when a request was sent without receiving a corresponding response within the allowed time.
38	Invalid data.
100	Interval time expired before data could be recorded.
101	Invalid local time stamp. IFE is not set with absolute time.

Contact technical support if you need assistance in resolving these or other error conditions.

Retrieving Data Log Using IFE FTP Server

You can use IFE FTP server to retrieve a data log file by connecting to the IFE server via FTP and transferring the .csv file, as shown in the steps below.

NOTE: If you want the IFE server to send the data log file via FTP automatically, the device log export must be configured for FTP.

Step	Action	Result
1	Create a folder on your computer, such as `C\:file_ logs.`	Creates a folder to store the IFE data log.
2	Launch Windows Explorer, enter `ftp://` and the IP address of the IFE server in the address text box (for example, `ftp://169.254.0.10`), press **Enter**.	Opens the **Log On As** dialog box.
3	Enter the user name as `Administrator` and password as `Gateway` in the text boxes, click **Log On**.	Opens an FTP session with the IFE server and displays the files stored in the IFE server.
4	Navigate to the directory*/logging/data* on the IFE server.	Opens the data logging directory on the IFE server.
5	Copy the log file and paste it into the folder created in step 1.	Copies the data log to the folder.

Retrieving Data Log Using the Data Points Option

Step	Action	Result
1	From the **Device Logging** webpage, click **Data Points**.	Opens a new window displaying the logged data.
2	Press **CTRL+A**, then press **CTRL+C**.	Selects all of the data and copies the data to the clipboard.
3	Open Excel, then press **CTRL+V**.	Pastes the data into an Excel spreadsheet.

Retrieving Data Log Using Email

The IFE server must be configured to deliver data logs to an email address. For more information, refer to Email Export, page 142.

Summary Device Pages

The summary device view provides the summary of one or more selected devices.

Step	Action	Result
1	From the **Monitoring** menu, click **Device Logging**.	Expands the tree for device logging choices.
2	Under **Device Logging**, click **Summary Device Page**.	–
3	Under **Summary Device Pages**, click **Single Topic for Multiple Devices**.	Opens the setup page for the multiple devices, and single topic page for multiple devices.
4	Select a device from the **Available Devices** list. **NOTE:** A maximum of four devices may be selected.	Selects the devices for the summary options.
5	Select a topic from the **Available Topics** list. **NOTE:** Only topics that are common between the selected devices are available.	Selects the topic to display for each selected device.
6	Select **Next**.	Displays the **Single Topic for Multiple Devices** page.
7	Hold the left mouse button and drag a selection box around a graph area to zoom in on it.	Zooms in on the selected graph area.
8	To return to the original full view, enter **Z** on the keyboard, or double-click the graph.	The view zooms out.

The topic logged from the selected devices is displayed in a webpage in a time-trend chart format. The time-trend chart is preconfigured to display data from the last full day, last full week, last full month, or last 6 weeks.

Energy parameters are displayed as incremental values on an interval basis. All other parameters are logged and displayed as the actual value recorded.

Control Webpages

What's in This Chapter

Device Control

Reset Commands

The **Device Control** page allows you to execute one or more reset commands per device type.

From the **Control** menu, in the **Device Control** submenu, on the device list, select the device and click **Reset**. Select an **Operation** in the **Resets** list to reset.

Application Control

The **Device Control** page allows you to control the following applications remotely:

*   Breaker application
*   IO application

By default, this feature is disabled in IFE server.

Password Management

When the application control operation is performed, an **Authorization Required** dialog box appears in the IFE webpage. Enter the password in the **Authorization Required** dialog box to perform the application control operation.

The password is required for:

*   MasterPacT MTZ circuit breaker with MicroLogic X control units.
*   MasterPacT NT/NW, PowerPacT P- and R-frame, or ComPacT NS circuit breaker with BCM ULP.
*   ComPacT NSX or PowerPacT H-, J-, and L-frame circuit breaker with BSCM.

The following operations in the **Device Control** page require a password:

Control	Operation	Availability
Breaker/Switch disconnector (BCM-OF/SD)	Open/Close/Reset	ComPacT NSX or PowerPacT H-, J-, and L-frame circuit breaker with BSCM
	Open/Close	• MasterPacT MTZ circuit breaker with MicroLogic X control units • MasterPacT NT/NW, ComPacT NS, or PowerPacT P- and R-frame circuit breakers with BCM ULP
Light	On/Off	IO 1 or IO 2
Load	On/Off	IO 1 or IO 2
Reset input counters	I1 I2 I3 I4 I5 I6	IO 1
	#I1 #I2 #I3 #I4 #I5 #I6	IO 2
Reset output counters	O1 O2 O3	IO 1
	#O1 #O2 #O3	IO 2
User-defined output control	On/Off	IO 1 or IO 2

Enable Application Control in IFE Server

Follow the below procedure to enable the **Application Control** feature in IFE server.

NOTE: The application control feature can only be enabled when the user is logged in as an administrator.

Step	Action	Result
1	Press the test button on the front face of the IFE server for 10–15 s. **NOTE:** Do not press the test button less than 10 s or more than 15 s.	Initiates the application control feature.
2	After 15 s, IFE server initiates the application control feature.	The feature disclaimer window is available continuously for 5 min. The module status LED starts blinking continuously for 5 min (1 s ON, 1 s OFF) once the test button is released.
3	Access the IFE webpage and login as an administrator.	The administrator login to the IFE webpage.
4	From the **Configuration & Settings** menu, click **Webpage Access**.	The **Administrator** reads the disclaimer and chooses either the option **I Understand the risks/Apply** or **Continue to disable**. The application control feature disclaimer is: *By accepting this disclaimer, you are directed to webpage access which enables you to control several applications remotely. It is highly recommended that the administrator modify the default administrator password. By using, you are agreeing to indemnify and hold harmless Schneider Electric for and from any claims, losses, demands, lawsuits, and damages that are a result of direct or indirect use of this application control feature by reason of any act or emission which the user commits.* The disclaimer page is available in the language selected by the administrator.
5	Select **I Understand the risks/Apply**.	The application control feature is now enabled for the administrator. The breaker application and IO application are enabled in the webpage access for providing access to the other user groups.
6	Select **Continue to disable**.	The application control feature is disabled. The breaker application and IO application are disabled in the webpage access.

Breaker Application

From the **Device Control** page, in the **Breaker Application**, the authorized group can perform the following operations:

Control	Status	Operation	Availability
Breaker	Open/Close/Tripped/NA	Open/Close/Reset	ComPacT NSX or PowerPacT H-, J-, and L- circuit breaker with BSCM
		Open/Close	• MasterPacT MTZ circuit breaker with MicroLogic X control units • MasterPacT NT/NW, ComPacT NS, or PowerPacT P- and R-frame circuit breaker or switch disconnector with BCM ULP

NOTE: Pop-up message confirms that the command is successfully sent. It does not confirm whether the complete operation is successful.

IO Application

From the **Device Control** page, in the **IO Application**, the authorized group can perform the following operations:

Control	Status	Operation	Availability
Reset input counters	–	I1 I2 I3 I4 I5 I6	IO 1
		#I1 #I2 #I3 #I4 #I5 #I6	IO 2
Reset output counters	–	O1, O2, O3	IO 1
		#O1 #O2 #O3	IO 2
Light control	ON or OFF	ON / OFF	IO 1 or IO 2
Load control	ON or OFF	ON / OFF	IO 1 or IO 2
User-defined output control	ON or OFF	ON / OFF	IO 1 or IO 2

NOTE:

- The IO application control is possible only when the IO module is connected to a circuit breaker.

- The light and the load control are available when the application rotary switch of IO 1 or IO 2 is in position 4.

- The user-defined output control is available only when the user-defined output has been assigned with Ecoreach software.

- If the input is assigned as a pulse counter, the operation is P1, P2, P3, P4, P5, and P6 for IO 1. For IO 2, the pulse counter operation is #P1, #P2, #P3, #P4, #P5, and #P6.

Set Device Time

Description

The **Set Device Time** page allows you to synchronize the date and time of the server devices connected to the IFE server to IFE date and time. It also allows you to get the device time that are connected to the IFE server. This page lists the server devices that require an external interface to set their date and time.

List of Parameters in Set Device Time

Parameter	Description
Device Selection	Allows you to select the device from the list for synchronizing, getting, and synchronizing the time.
Localized Time	Displays the time of the selected device.
Status	Displays the status of the selected device.
Get Time	Allows you to get the time of the selected device.
Set Device Time	Allows you to set the time of the selected device.

Setting the Device Time

Step	Action	Table
1	From the IFE menu bar, click **Control**.	Opens the **Control** menu.
2	From the **Control** menu, click **Set Device Time**.	Opens the **Set Device Time** page.
3	Select the devices from the **Set Device Time** page, and then click **Set Device Time**.	The selected server device date and time gets synchronized with the IFE time and the status is updated as successful. **NOTE:** If the selected device fails to synchronize with IFE date and time, then the status is updated as unsuccessful. **NOTE: Set Device Time** feature is not applicable for IFE's own IMU and shows the set status as **NA** (Not Applicable).

DOCA0084EN-11   161

Diagnostics Webpages

What's in This Chapter

Statistics

Description

The **Statistics** page shows the readings accumulated since the IFE server was last activated. If the power to the IFE server is terminated or the device is reset due to a configuration change or other event, all cumulative values are reset to 0.

Reset Procedure

Step	Action	Result
1	From the IFE menu bar, click **Diagnostics**.	Opens the **Diagnostics** menu.
2	From the **Diagnostics** menu, in the **General** submenu, click **Statistics**.	Opens the **Statistics** page.
3	View the data.	See the statistics for each group.
4	Click **Reset Counters**.	Resets the IFE cumulative diagnostic data to 0.

Interpreting Ethernet Statistics

Global Statistic	Description
Received Frames	Number of frames received
Transmitted Frames	Number of frames transmitted
Reset Counters	Resets the transmitted and received frames

Statistic Per Port	Description
Link Speed	Operational speed (10 Mbps or 100 Mbit/s)
Duplex mode	Current mode of operation (full duplex or half duplex)

Interpreting Modbus TCP/IP Statistics

Statistic	Description
Port status	Status of the connected Ethernet port
Opened TCP connections	Number of active connections
Received messages	Number of messages received
Transmitted messages	Number of messages transmitted
Reset counters	Resets the received and transmitted messages

Interpreting System Statistics

Statistic	Description
CPU	Status of the CPU: • Nominal • Degraded • Out of service
Boot Memory	Healthiness of the boot memory
EEPROM	Healthiness of EEPROM
File System	Healthiness of the file system
Ethernet PHY 1	Healthiness of PHY 1 hardware
Ethernet PHY 2	Healthiness of PHY 2 hardware
DDR	Healthiness of the execution memory

Interpreting Date and Time Statistics

Statistic	Description
Date	Current date
Time	Current time
Uptime	Run time during the system power-up

Interpreting Date /Time Synchronization

Statistic	Description
Last Synchronization	
Last Synchronization Since	Time elapsed since the last synchronization has happened
Time Source	Source of time with which the last synchronization has happened
Date	Last synchronization date
Time	Last synchronization time
Synchronization with SNTP	
Status	The following is the status of synchronization with SNTP: • If SNTP is disabled, the status is displayed as "–" • If SNTP is enabled but not synchronized, then the status is displayed as "NOK" • If SNTP is enabled and successfully synchronized, then the status is displayed as "OK"

Interpreting Modbus Serial Statistics

Statistic	Description
Transmitted Message	A counter that increments each time a frame is sent.
Received Message	A counter that increments each time a frame is received.
Error Message	An error marked from the server or the response timeout.

Interpreting ULP Statistics

Statistic	Description
Frames Transmitted	Number of CAN frames transmitted successfully
Frames Received	Number of CAN frames received successfully
Max Transmit Error	Maximum number of CAN transmitted errors (TEC)
Max Receive Error	Maximum number of CAN received errors (REC)
Bus off	CAN Bus off count
Max Bus off	Maximum number of bus off counts

Interpreting File System Statistics

Statistic	Description
Total Size	Total amount of the IFE disk size in kilobytes
Used Size	Total amount of used disk size on the IFE disk in kilobytes
Free Size	Total amount of unused disk space on the IFE disk in kilobytes
Bad Size	Amount of corrupted disk space on the IFE disk in kilobytes

Interpreting TCP Port Connections Statistics

Statistics	Description
Remote IP	Remote IP address
Remote Port	Remote port number
Transmitted messages	Number of messages transmitted
Received message	Number of messages received
Sent Errors	Number of error messages sent
Reset Counters	Resets the transmitted and received messages

Device Identification

Device Name Configuration Procedure

Step	Action	Result
1	From the IFE menu bar, click **Diagnostics**.	Opens the **Diagnostics** page.
2	From the **Diagnostics** menu, in the **Product Information** submenu, click **Device Identification**.	Opens the **Device Identification** page.

List of Parameters in Device Identification

Parameter	Description
Device name	Device name which is updated in the device name field
Product name	Name of the product
Serial number	Device serial number
Product model number	Device model number
Firmware version	Current firmware version
Unique Identifier	Combination of MAC address and the time
MAC address	Unique MAC address
IPv4 address	IP address of the IFE server
IPv6 link local address	Address used to communicate on the local network

IMU Information

Description

The **IMU Information** page gives the information about the devices which are connected to the ULP port of the IFE server. The devices connected are:

- BCM ULP module
- MicroLogic trip unit
- BSCM module
- FDM121 display
- IO module IO 1
- IO module IO 2
- UTA module

Read Device Registers

Description

The Read Device Registers page allows you to read Modbus registers from the selected device.

Read Procedure

Step	Action	Result
1	From the IFE menu bar, click **Diagnostics**.	Opens the **Diagnostics** menu.
2	From the **Diagnostics** menu, in the **Device Health Check** submenu, click **Read Device Registers**.	Opens the **Read Device Registers** page.
3	From the **Device Name**, select the device.	Selects the device from the drop-down list.
4	Enter **Local ID** (or choose from the defined device list), **Starting Register**, and the **Number of Registers** to read.	Enters the registers to read from the specified device.
5	Select the data type from **Data Type** drop-down list.	Selects the appropriate data type.
6	To change how Modbus data is displayed in the **Value** column, select **Decimal**, **Hexadecimal**, **Binary**, or **ASCII**.	Selects how the data values are displayed.
7	Click **Read**.	Reads the device registered according to the selected configuration.

IFE Read Device Register Parameters

Parameter	Description	Settings
Device Name	Selects a device to read from the list of previously added devices. A Modbus server device of a Modbus client IFE server not defined in the device list can be read by entering its local ID number. **NOTE:** The server device of a remote device not defined in the device list cannot be read by entering its local ID number.	–
Local ID	The address (local ID) of the device that is to be read.	1
Starting Register	Register number in decimal.	0–65535 Factory setting: 1000
Number of Registers	The number of registers to read.	1–125 Factory setting: 10
Register	Lists the register numbers in decimal.	–
Value	Lists the data stored for a register. Values retrieved depend on the device connected to the IFE server. Refer to the documentation for the connected device for more information about stored register values.	–
Data Type	Lists the data types available for the device.	• **Holding Registers** (Factory setting) • **Input Registers** • **Input Coils** • **Output Coils**
Decimal, Hexadecimal, Binary, or ASCII options	Select an option to specify how the value column data is displayed.	**Decimal** (Factory setting)

Communication Check

Automated Communication Check

While browsing the real-time data views, the IFE server has an automated communication check that runs every 15 minutes by default. To change the timing, refer to Preferences, page 145. This check verifies the communication health of all the devices configured on the IFE server, and attempts to re-establish the communication to any device marked out of service within the current browser session.

Manual Communication Check

In certain cases, there is no need to wait for the automated communications check interval and need to force the check to run manually.

Step	Action	Result
1	From the IFE menu bar, click **Diagnostics**.	Opens the **Diagnostics** menu.
2	From the **Diagnostics** menu, in the **Device Health Check** submenu, click **Communications Check**.	Opens the **Communications Check** page.
3	Click **Check Device Status**.	Runs a communications check. The communicating device displays: • **Passed** in the **Communications** column. • **In Service** in the **Status** column. A device that is not communicating display: • **Failed** in the **Communications** column. • **Out of Service** in the **Status** column if it has failed multiple times.

IO Readings

Description

The **IO Readings** page shows the IO module input/output configuration. It displays six digital inputs, three digital outputs, and one analog input. The IO application control is possible only when the IO module is connected to a circuit breaker.

The table shows the steps to access the **IO Readings** page:

Step	Action	Result
1	From the IFE menu bar, click **Diagnostics**.	Opens the **Diagnostics** page.
2	From the **Diagnostics** menu, select a device from **IO Readings** submenu.	Opens the **IO Readings** page for the selected device.

List of Parameters in IO Module

Parameter	Description	Setting
Inputs	Displays the six digital inputs configured in the IO module.	–
Outputs	Displays the three digital outputs configured in the IO module.	–
Analog Inputs	Displays the analog input assigned in the IO module.	–
Label	Displays the assigned functions of the corresponding inputs or outputs.	–
Value	Displays the value of the six digital inputs and three digital outputs	• 1 • 0
Force/Unforce	Displays the six digital inputs and three digital outputs are forced or unforced	• **UNFORCED** • **FORCED**

Maintenance Webpages

What's in This Chapter

Indicators

Description

The **Indicators** page provides the maintenance counter information for the selected device. The page displays the information about the remaining service life of the circuit breaker, contact wear counters, circuit breaker operation counters, and the cradle counters.

Viewing Maintenance Counters

Step	Action	Result
1	From the IFE menu, click **Maintenance**.	Opens the **Maintenance** page.
2	From the **Indicators** menu, select the device from the device list. NOTE: This feature is available for circuit breakers only.	Displays the information about the remaining service life of the circuit breaker, contact wear counters, circuit breaker operation counters, and the cradle counters.

Restore the Smartlink Modbus Devices

Description

The **Restore** submenu allows you to move the configuration settings from the IFE server to the Smartlink Modbus device. The page displays the information about the device name, device type, and device status.

NOTE: The **Restore** submenu is available only for:

- IFE firmware versions that are less than or equal to V001.009.008.
- Smartlink Modbus devices and the IFE firmware versions that are equal to or greater than the versions listed in the system compatibility table for Smart Panels 1.1 and later.

Restore Page Parameters

Parameter	Description	Settings
Check box	Allows you to select the desired Smartlink Modbus device to restore the configuration in the Smartlink Modbus device.	• Selected • Cleared **NOTE:** The check box is unavailable if the Smartlink Modbus device is not connected or the Smartlink Modbus device has incompatible firmware version
Remote Gateway Name	Displays the name of the IFE server.	−
Name	Displays the name of the Smartlink Modbus device entered in the device list.	−
Device Type	Displays the device type selected for the Smartlink Modbus device in the device list.	−
Status	Displays the restore status of the Smartlink Modbus device.	• **OK** • **Not OK : Incompatible version** • **Not OK : Communication Failure**
Restore	Allows you to restore the configuration in the Smartlink Modbus devices.	−

Restoring the Smartlink Modbus Device Configuration

Step	Action	Result
1	From the IFE menu bar, click **Maintenance**.	Opens the **Maintenance** menu.
2	From the **Maintenance** menu, click **Restore the Smartlink's** submenu.	Displays the **Device to be restored** page.
3	From the **Device to be restored** page, select the Smartlink Modbus devices to restore the configuration.	Selects the desired Smartlink Modbus devices to restore the configuration.
4	Click **Restore**.	**Restoration Confirmation** dialog box appears.
5	Click **OK**.	Configuration is restored in Smartlink Modbus devices from IFE server.

Appendices

What's in This Part

What's in This Part

Appendix A - List of IFE Supported Devices

What's in This Chapter

List of IFE Supported Device Types

IFE Server Supported Devices

The following table gives the list of devices that can be connected as Modbus servers on an IFM interface stacked to the IFE server. This list of supported devices was accurate at the time this document was published.

Device Group	List of devices supported by IFE server from firmware version 005	List of devices supported by IFE server up to firmware version 003
MasterPacT NT/NW, ComPacT NS, and PowerPacT P- and R-frame circuit breakers with MicroLogic trip units	MicroLogic A	MicroLogic A
	MicroLogic E	MicroLogic E
	MicroLogic P	MicroLogic P
	MicroLogic H	MicroLogic H
MasterPacT MTZ circuit breaker with MicroLogic X control units	MicroLogic X	MicroLogic X
	MicroLogic Xi	MicroLogic Xi
ComPacT NSX and PowerPacT H-, J-, and L-frame circuit breakers with MicroLogic trip units	ComPacT NSX - E	ComPacT NSX - E
	PowerPacT - E	PowerPacT - E
ComPact NSX and PowerPact H-, J-, and L-frame circuit breakers with MicroLogic trip units	ComPact NSX - A	ComPact NSX - A
	ComPact NSX - E	ComPact NSX - E
	PowerPact - A	PowerPact - A
	PowerPact - E	PowerPact - E
Insulation monitoring devices	Not supported	Vigilohm IM20
	Not supported	Vigilohm IM20-H
Monitoring and protection relay	Not supported	VigiPacT RHU
Monitoring relay	Not supported	VigiPacT RMH
Power factor controller	Not supported	Varlogic
Power meters	Not supported	PM1200
	Not supported	PM3250
	Not supported	PM3255
	Not supported	PM5000
	Not supported	PM5100/PM5300
	Not supported	PM5350
	Not supported	PM5560
	Not supported	PM800
	Not supported	PM800 A-S1/A-S2
	Not supported	PM9C

Device Group	List of devices supported by IFE server with Firmware 005 and more	List of devices supported by IFE server with Firmware up to 003
Energy meters	Not supported	EM3550
	Not supported	EM3555
	Not supported	EM6400
	Not supported	EM6430
	Not supported	EM6433
	Not supported	EM6434
	Not supported	EM6436
	Not supported	EM6436D
	Not supported	EM6438
	Not supported	EM6459
	Not supported	iEM3150
	Not supported	iEM3155
	Not supported	iEM3250
	Not supported	iEM3255
	Not supported	iEM3350
	Not supported	iEM3355
Non-communicating MasterPacT NT/NW and ComPacT NS circuit breakers and switch disconnectors	BCM-OF/SD	BCM-OF/SD
Non-communicating ComPacT NSX and PowerPacT H-, J-, and L-frame circuit breakers and switch disconnectors	BSCM-OF/SD	BSCM-OF/SD
Others	Not supported	Smartlink Modbus
	Not supported	Smartlink Ethernet
	Not supported	Smartlink SI B
	Not supported	Smartlink SI D
	Not supported	PowerTag energy sensors (iEM1520, iEM1521, iEM1522, iEM1540, iEM1541, and iEM1542) IFE server reads PowerTag energy sensor configuration from Smartlink SI B and Smartlink SI D device.
	Not supported	BCPM A/E
	Not supported	BCPM B
	Not supported	BCPM C

DOCA0084EN-11