

Enerlin'X IFE

Ethernet Interface for One Circuit Breaker

User Guide

DOCA0142EN-12
04/2026



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.....	5
About the Document.....	6
IFE Interface Presentation.....	10
Introduction.....	11
Intelligent Modular Unit.....	13
Hardware Description.....	17
EcoStruxure Power Commission Software.....	23
Schematics with MasterPacT MTZ Circuit Breakers.....	25
Schematics with MasterPacT NT/NW, ComPacT NS, PowerPacT P- and R-frame Circuit Breakers.....	28
Schematics with ComPacT NSX Circuit Breakers.....	34
Technical Characteristics.....	38
Firmware Update.....	40
Recover IFE Interface from Boot Mode.....	41
Security Features.....	42
Machine to Machine Communication.....	43
Role Based Access Control.....	44
Security Logs.....	47
IFE Webpages from Firmware Version 005.....	48
Webpage Access and User Interface.....	49
Access to IFE Webpages.....	50
User Interface Layout.....	52
Webpage Description.....	54
Settings Pages.....	56
Date and Time.....	57
Time Zone.....	58
Preferences.....	59
Ethernet.....	60
IP Configuration.....	62
Email Service.....	64
Data Publishing.....	66
Redundancy-RSTP.....	67
SNMP.....	69
Devices.....	71
Emails.....	74
Security Pages.....	75
IP Network Services.....	76
Modbus TCP/IP Filtering.....	77
Certificates.....	79
User Management.....	81
Syslog Service.....	84
Monitoring and Control Pages.....	85
Circuit Breakers.....	86
IO Modules.....	90
Diagnostics Pages.....	91
Status.....	92
Ethernet.....	93

Modbus.....	94
ULP	95
Redundancy-RSTP Bridge	96
Redundancy-RSTP Ports	97
SNMP	98
Read Device Registers.....	99
IFE	100
Devices.....	102
IFE Webpages up to Firmware Version 003	104
Webpage Access and User Interface	105
Access to IFE Webpages	106
User Interface Layout.....	109
Webpage Description.....	111
Configuration & Settings Webpages.....	113
General.....	114
Date and Time	115
Time Zone	117
Ethernet Configuration (Dual Port)	118
IP Configuration.....	119
Modbus TCP/IP Filtering	121
Email Server Configuration	122
Email Events	124
Device List	133
Device Logging.....	134
Device Log Export.....	136
SNMP Parameters	138
Preferences.....	139
Advanced Services Control.....	140
User Accounts	141
Webpage Access.....	143
Monitoring Webpages	144
Real Time Data.....	145
Device Logging.....	147
Control Webpages.....	151
Device Control.....	152
Set Device Time	155
Diagnostics Webpages	156
Statistics	157
Device Identification.....	160
IMU Information	161
Read Device Registers.....	162
Communication Check	163
IO Readings	164
Maintenance Webpages	165
Indicators	165
Appendices	166
Appendix A - List of IFE Interface Supported Devices	167
List of IFE Interface Supported Device Types	167

Safety Information

Important Information

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



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



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

DANGER

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

WARNING

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

CAUTION

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

NOTICE

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

Please Note

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

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

About the Document

Document Scope

The aim of this 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 interface for one circuit breaker webpages.

Validity Note

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

- MasterPacT™ MTZ circuit breakers with MicroLogic Active control unit
- 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 and ComPacT NSX 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/.

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the [Cybersecurity Best Practices](#) document.

Schneider Electric provides additional information and assistance:

- Subscribe to the [Schneider Electric security newsletter](#).
- Visit the [Cybersecurity Support Portal](#) web page to:
 - Find Security Notifications.
 - Report vulnerabilities and incidents.
- Visit the [Schneider Electric Cybersecurity and Data Protection Posture](#) web page to:
 - Access the cybersecurity posture.
 - Learn more about cybersecurity in the cybersecurity academy.
 - Explore the cybersecurity services from Schneider Electric.

Product Related Cybersecurity Information

▲ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- 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.

Environmental Data

For product compliance and environmental information, refer to the [Schneider Electric Environmental Data Program](#).

Available Languages of the Document

The document is available in these languages:

- English (DOCA0142EN), original language
- Spanish (DOCA0142ES)
- French (DOCA0142FR)
- Chinese (DOCA0142ZH)

Related Documents for IEC Devices

Title of Documentation	Reference Number
<i>Enerlin'X IFE – Ethernet Interface for One Circuit Breaker – Instruction Sheet</i>	QGH13473
<i>Enerlin'X IFE/EIFE - Ethernet Interface - Firmware Release Notes</i>	DOCA0147EN
<i>ULP (Universal Logic Plug) System - User Guide</i>	DOCA0093EN DOCA0093ES DOCA0093FR DOCA0093ZH
<i>MasterPacT, ComPacT, PowerPacT Circuit Breakers - Modbus Communication - User Guide</i>	DOCA0384EN DOCA0384ES DOCA0384FR DOCA0384ZH
<i>MasterPacT MTZ - MicroLogic Active Control Unit - User Guide</i>	DOCA0265EN DOCA0265ES DOCA0265ZH
<i>Breaker Communication and Isolation Module (BCIM) for MicroLogic Active Control Unit - User Guide</i>	DOCA0387EN DOCA0387ES DOCA0387ZH
<i>MasterPacT MTZ - MicroLogic X Control Unit - User Guide</i>	DOCA0102EN DOCA0102ES DOCA0102FR DOCA0102ZH
<i>MasterPacT MTZ Circuit Breakers with MicroLogic X Control Units - IEC 61850 Communication Guide</i>	DOCA0162EN DOCA0162ES DOCA0162FR DOCA0162ZH
<i>CET850 IEC 61850 Configuration Software - User's Manual</i>	SEPED306025EN
<i>Enerlin'X IO - Input/Output Application Module for One Circuit Breaker - User Guide</i>	DOCA0055EN DOCA0055ES DOCA0055FR DOCA0055ZH
<i>MasterPacT, ComPacT, PowerPacT - Cybersecurity Guide</i>	DOCA0122EN DOCA0122ES DOCA0122FR DOCA0122ZH
<i>EcoStruxure Cybersecurity Admin Expert Guide</i>	CAE_UM_EN

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Related Documents for UL/ANSI Devices

Title of Documentation	Reference Number
<i>Enerlin'X IFE – Ethernet Interface for One Circuit Breaker – Instruction Sheet</i>	QGH13473
<i>Enerlin'X IFE/EIFE - Ethernet Interface - Firmware Release Notes</i>	DOCA0147EN
<i>ULP (Universal Logic Plug) System - User Guide</i>	DOCA0093EN DOCA0093ES DOCA0093FR DOCA0093ZH
<i>MasterPacT, ComPacT, PowerPacT Circuit Breakers - Modbus Communication - User Guide</i>	DOCA0384EN DOCA0384ES DOCA0384FR DOCA0384ZH
<i>MasterPacT MTZ - MicroLogic X Control Unit - User Guide</i>	DOCA0102EN DOCA0102ES DOCA0102FR DOCA0102ZH
<i>MasterPacT MTZ Circuit Breakers with MicroLogic X Control Units - IEC 61850 Communication Guide</i>	DOCA0162EN DOCA0162ES DOCA0162FR DOCA0162ZH
<i>CET850 IEC 61850 Configuration Software - User's Manual</i>	SEPED306025EN
<i>Enerlin'X IO - Input/Output Application Module for One Circuit Breaker - User Guide</i>	DOCA0055EN DOCA0055ES DOCA0055FR DOCA0055ZH
<i>MasterPacT, ComPacT, PowerPacT - Cybersecurity Guide</i>	DOCA0122EN DOCA0122ES DOCA0122FR DOCA0122ZH
<i>EcoStruxure Cybersecurity Admin Expert Guide</i>	CAE_UM_EN

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

IFE Interface Presentation

What's in This Part

Introduction.....	11
Intelligent Modular Unit	13
Hardware Description	17
EcoStruxure Power Commission Software	23
Schematics with MasterPacT MTZ Circuit Breakers	25
Schematics with MasterPacT NT/NW, ComPacT NS, PowerPacT P- and R- frame Circuit Breakers	28
Schematics with ComPacT NSX Circuit Breakers	34
Technical Characteristics	38
Firmware Update	40

Introduction

Overview

The IFE Ethernet interface for one circuit breaker (or IFE interface) 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 interface and a corresponding IP address.

The IFE interface with part number LV434001 is an Ethernet interface for ComPacT, PowerPacT, and MasterPacT circuit breakers.

NOTE: The IFE interface with part number LV434001 completely replaces the IFE interface with part number LV434010. The part number LV434001 comes with the Real Time Clock (RTC) feature and allows ULP connections up to 20 m (65.6 ft) with the MasterPacT MTZ circuit breakers (part number LV434010 had a theoretical limitation of 5 m (16.4 ft) over the life of the IFE interface).

IFE Interface Features

The main features of IFE interface are:

- Dual 10/100 Mbps Ethernet port for simple daisy chain connection
- Device profile web service for discovery of the IFE interface on the Local Area Network (LAN)
- ULP compliant for location of the IFE interface in the switchboard
- Ethernet interface for ComPacT, PowerPacT, and MasterPacT circuit breakers
- Embedded settings webpages
- Embedded monitoring and control webpages
- Embedded diagnostics webpages
- Embedded security webpages
- Built-in email alarm notification for circuit breaker connected to IFE interface.
- IEC 61850 interface for MasterPacT MTZ circuit breakers with MicroLogic X control units
- Machine-to-Machine compliance
- Role-Based Access Control (RBAC) for users accessing the webpages

IFE Firmware Versions

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

- IFE Interface Webpages from Firmware Version 005, page 48, describes the IFE interface webpages for the firmware version 005 and later.
- IFE Interface Webpages up to Firmware Version 003, page 104, describes the IFE interface webpages for the firmware versions up to 003.

IFE Interface Supported Protocols

The IFE interface supports the following Ethernet protocols:

- **Modbus TCP/IP:** 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 interface 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 interface 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. It provides web server functionality through TCP port 80. Remote configuration of IFE interface 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 interface.
- **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 interface.
NOTE: For IFE interface with firmware version 004.006.000 and later, use a FTPS client, such as FileZilla or WinSCP to transfer the IEC 61850 configuration files.
- **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: HTTPS, FTPS, RSTP, NTP, and IEC 61850 protocols are applicable only from IFE interface firmware version 004.001.000.

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 with MicroLogic Active control unit
- 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
- ComPacT NSX circuit breakers
- PowerPacT H-, J-, and L-frame circuit breakers

ULP Modules Per Circuit Breaker Range

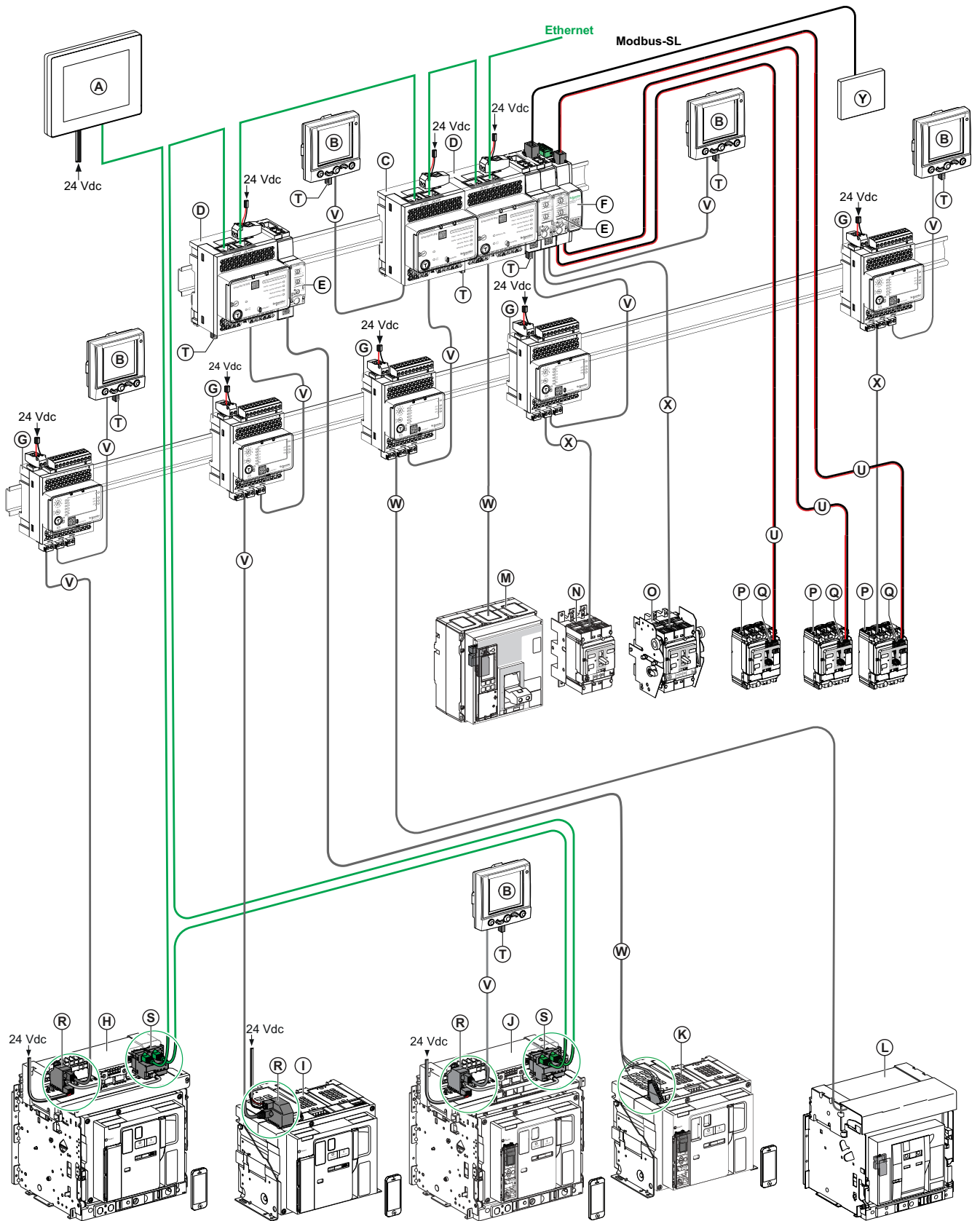
The following table lists the compatible ULP modules for each range of circuit breakers.

ULP Module	Part Number	MasterPacT MTZ circuit breaker with BCIM Module and MicroLogic Active Control Unit	MasterPacT MTZ circuit breaker with ULP Port Module and MicroLogic X Control Unit	MasterPacT NT/NW or ComPacT NS or PowerPacT P- and R-frame circuit breaker with BCM ULP Module and MicroLogic Trip Unit	ComPacT NSX or PowerPacT H-, J-, and L-frame circuit breaker 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 circuit breaker with BCIM Module and MicroLogic Active Control Unit	MasterPacT MTZ circuit breaker with ULP Port Module and MicroLogic X Control Unit	MasterPacT NT/NW or ComPacT NS or PowerPacT P- and R-frame circuit breaker with BCM ULP Module and MicroLogic Trip Unit	ComPacT NSX or PowerPacT H-, J-, and L-frame circuit breaker 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 DOCA0093•• *ULP (Universal Logic Plug) System - User Guide* in Related Documents section at the beginning of the guide.

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	Modbus-SL hub
G	IO input/output application module for one circuit breaker
H	MasterPacT MTZ drawout circuit breaker with MicroLogic X control unit
I	MasterPacT MTZ fixed circuit breaker with MicroLogic X control unit
J	MasterPacT MTZ drawout circuit breaker with MicroLogic Active control unit and BCIM module
K	MasterPacT MTZ fixed circuit breaker with MicroLogic Active control unit and BCIM module
L	MasterPacT NT/NW circuit breaker with MicroLogic trip unit and BCM ULP module
M	ComPacT NS/PowerPacT P- and R-frame circuit breaker with MicroLogic trip unit and BCM ULP module
N	ComPacT NSX/PowerPacT H-, J-, and L-frame plug-in circuit breaker
O	ComPacT NSX/PowerPacT H-, J-, and L-frame drawout circuit breaker
P	ComPacT NSX/PowerPacT H-, J-, and L-frame fixed circuit breaker
Q	BSCM Modbus SL/ULP module
R	ULP port module
S	EIFE Embedded Ethernet Interface for one MasterPacT MTZ drawout circuit breaker
T	ULP line termination
U	BSCM Modbus-SL cord
V	RJ45 ULP cord
W	Breaker ULP cord
X	NSX cord
Y	Modbus-SL server

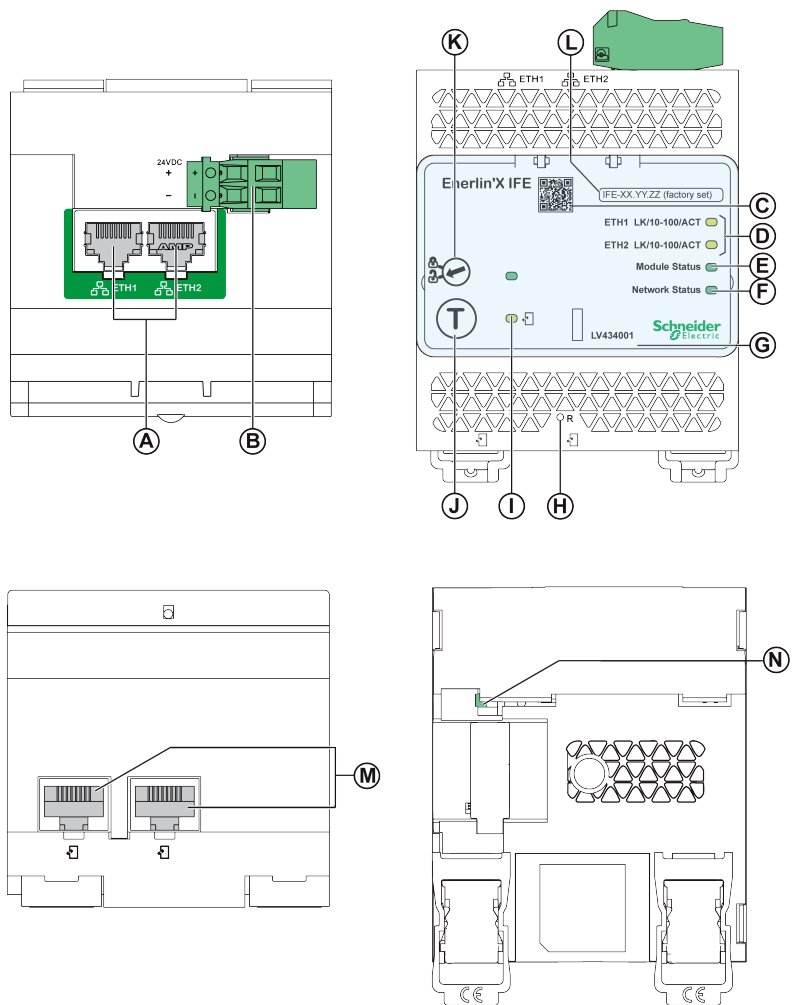
Remote Controller

A remote controller is a device that is able to communicate with an IMU using a communication interface, such as the IFE server, IFE interface, and EIFE interface. For example, FDM121 and FDM128 display modules, supervisor, PLC, BMS, SCADA system, and so on.

For more information on Modbus registers and commands, refer to the DOCA0384•• *MasterPacT, ComPacT, PowerPacT Circuit Breakers - Modbus Communication - User Guide* in Related Documents section at the beginning of the guide.

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** Device name label
- M** Two RJ45 ULP ports
- N** Grounding connection

For information on installation, refer to QGH13473 *Eterlin'X IFE – Ethernet Interface for One Circuit Breaker – Instruction Sheet*, page 8.

Mounting

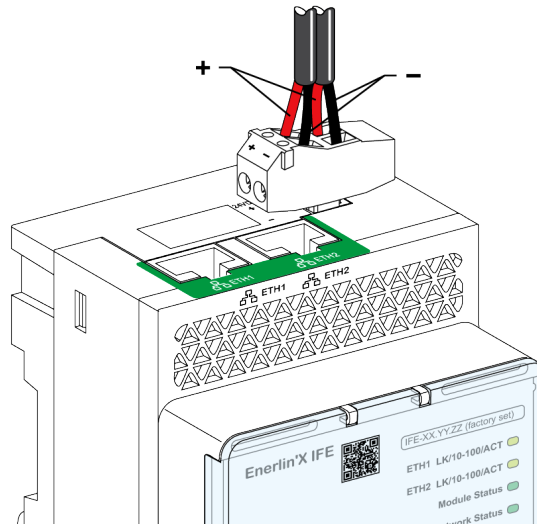
The IFE interface mounts on a DIN rail.

Power Supply

The IFE interface must always be supplied with 24 Vdc power supply.

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 interface status.

LED Indication	Status Description	Action
OFF	No power	None
Steady green	IFE interface operational	None
Blinking green (250 ms ON, 250 ms OFF)	Hidden control webpage available	None
Blinking green (500 ms ON, 500 ms OFF)	IFE interface firmware corrupted	Contact your local Schneider Electric service team for support.
Blinking red (500 ms ON, 500 ms OFF)	IFE interface in degraded mode	Replace ULP module at the next maintenance operation.
Steady red	IFE interface 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.

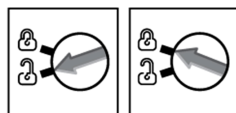
LED Indication	Status Description
OFF	No power or no IP address
Steady green	Valid IP address
Steady red	Duplicated IP address
Blinking green/red (250 ms green, 250 ms red)	Self-test in progress
Steady amber	Error in IP configuration

Modbus Address

The IFE interface 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 interface enables or disables the ability to send the remote control commands over the Ethernet network to the IFE interface, and to the other modules of the IMU.



- If the arrow points to the open padlock (default setting), remote control commands are enabled.
- If the arrow points to the closed padlock, remote control commands are disabled.

NOTE: 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 the following functions, according to the duration of the button pressed:

Time Range	Function
1 s	Tests the connection between all the ULP modules for 15 s.
5 s	Resets the security administrator password to its default setting (AAAAAAAA). NOTE: If a security administrator role does not already exist, executing this action will create a new security administrator role.
10 s	Resets the IFE interface to its factory default settings.

Reset Button

Press the **Reset** button for 1 s, to reset the IP acquisition mode to its default setting (DHCP).

Security Administrator Password Reset

The following procedure describes the steps to reset the security administrator password to its default setting:

1. Press the test button (**T**) on the IFE interface for 5 s.
Result: The LED light will flash rapidly in a pattern alternating between red and green, with each color displayed for 100 ms.
2. On releasing the test button (**T**), the IFE interface will enter reset mode for a duration of 30 s and prompts the user to reset the password to its default setting. The LED light will flash rapidly in a pattern alternating between red and green, with each color displayed for 100 ms.
3. Press the test button (**T**) on the IFE interface to confirm or wait for 30 s to cancel the reset.
4. Once the reset of the security administrator password is confirmed, either the password is reset to the default setting (AAAAAAAA) or a new security administrator role is added.

NOTE: Every time a reset operation is successfully performed, the reset administrator password counter increments by one.

IFE Interface Factory Reset

The following procedure describes the steps to reset the IFE interface to its factory default settings:

1. Press the test button (**T**) on the IFE interface for 10 s.
Result: The LED will rapidly flash in red with a 100 ms ON and 100 ms OFF interval.
2. On releasing the test button (**T**), the IFE interface will enter reset mode for a duration of 30 s and prompts the user to reset the device to its factory default settings. The LED will rapidly flash in red with a 100 ms ON and 100 ms OFF interval.
3. Press the test button (**T**) on the IFE interface to confirm or wait for 30 s to cancel the reset.
4. Once the reset to factory default settings is confirmed, the IFE interface reboots and all the device settings are reset to their factory default values.

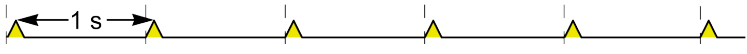

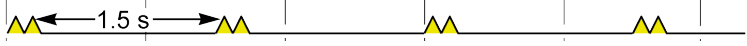

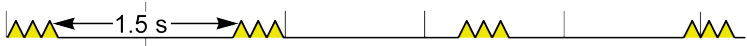
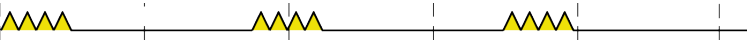
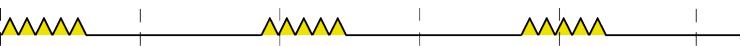



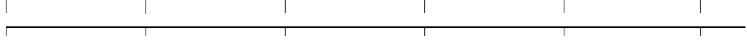
After reset, the IFE interface restarts and restores the following settings to their factory default values:

Parameter	Default Value
Date & Time	<ul style="list-style-type: none"> Date and time setting mode: Manual Date: yyyy-mm-dd Time: hh:mm:sec
NTP	<ul style="list-style-type: none"> NTP server setting mode: Manual Primary SNTP: time.windows.com Secondary SNTP: time.nist.com
Time zone	<ul style="list-style-type: none"> Time zone offset: UTC Day light saving: Disabled
Preferences	<ul style="list-style-type: none"> Real time sample rate: 5 s Communications check rate: 15 min
Ethernet	Frame format: Auto
	Port control <ul style="list-style-type: none"> ETH1 mode: Auto-negotiation ETH2 mode: Auto-negotiation
	Broadcast storm protection <ul style="list-style-type: none"> Enable: Enabled Level: Medium-Low Committed information rate: 4000 s
IP configuration	IPv4 <ul style="list-style-type: none"> Configuration: Automatic Mode: DHCP IP address: 169.254.xxx.yyy (xxx.yyy = last 6 bytes of MAC address) Subnet mask: 255.255.0.0 Gateway: 0.0.0.0
	IPv6 <ul style="list-style-type: none"> Enable IPv6: Enabled IPv6 address: Unavailable
	DNS <ul style="list-style-type: none"> DNS address: Automatic
Email service	Email service: Disabled
Data publishing	Logging interval: Disabled
RSTP	RSTP: Disabled
SNMP	SNMPV1 agent: Disabled
Devices	<ul style="list-style-type: none"> Name: Last 6 digits of MAC ID IP address: Default Breaker unit name field is empty. Data publishing: Disabled
Contact management	Empty user email list
IP network services	<ul style="list-style-type: none"> Modbus TCP: Enabled Secure commissioning: Disabled Secure Modbus for M2M: Disabled FTPS server: Disabled Discovery: Enabled HTTP/Web: Disabled HTTPS: Enabled
Modbus TCP/IP filtering	<ul style="list-style-type: none"> Modbus TCP/IP filtering: Disabled IP filtering exception list cleared
Certificates	Certificate type: Self signed

Parameter	Default Value
User management	<ul style="list-style-type: none"> User name: SecurityAdmin Roles: SECADM, Viewer, Operator, Engineer, Installer Password: AAAAAAAA
Syslog service	Syslog logging service: Disabled

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
	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	<ul style="list-style-type: none"> MicroLogic Active control units Communication interface modules: BCIM module, IFM interface, IFE interface, IFE server, and EIFE interface ULP modules: FDM121 display ⁽¹⁾ 	–
MasterPacT MTZ circuit breakers	<ul style="list-style-type: none"> MicroLogic X control units Communication interface modules: IFM interface, IFE interface, IFE server, and EIFE interface ULP modules: IO module and FDM121 display ⁽¹⁾ 	M2C output module
<ul style="list-style-type: none"> MasterPacT NT/NW circuit breakers ComPacT NS circuit breakers PowerPacT P- and R-frame circuit breakers 	<ul style="list-style-type: none"> MicroLogic trip units Communication interface modules: BCM module, CCM module, BCM ULP module, IFM interface, IFE interface, and IFE server ULP modules: IO module and FDM121 display ⁽¹⁾ 	M2C and M6C output modules
<ul style="list-style-type: none"> ComPacT NSX circuit breakers PowerPacT H-, J-, and L-frame circuit breakers 	<ul style="list-style-type: none"> MicroLogic trip units Communication interface modules: BSCM or BSCM Modbus SL/ULP module, IFE interface, IFM interface, and IFE server ULP modules: IO module and FDM121 display ⁽¹⁾ 	SDTAM and SDx output modules

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

Click [here](#) to download the latest version of EcoStruxure Power Commission software.

⁽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 standard protection settings to the device and download standard protection settings from the device.
- Compare the standard protection settings between the project and the device.
- Generate and print the device standard protection settings report.
- View the logs and maintenance information.
- View the alarm details.
- Check the system firmware compatibility status.
- Update to the latest device firmware.
- Perform automatic trip curve tests with preconfigured or custom test points.
- Perform arc energy reduction tests in compliance with NEC 240.87(C).

Schematics with MasterPacT MTZ Circuit Breakers

Description

The IFE interface is connected to the MasterPacT MTZ circuit breaker with:

- MicroLogic Active control unit through its ULP port module or COM terminal block.
- MicroLogic X control unit through its ULP port module

For more information, refer to the DOCA0093•• *ULP (Universal Logic Plug) System - User Guide*, page 8.

ULP Connection

NOTICE

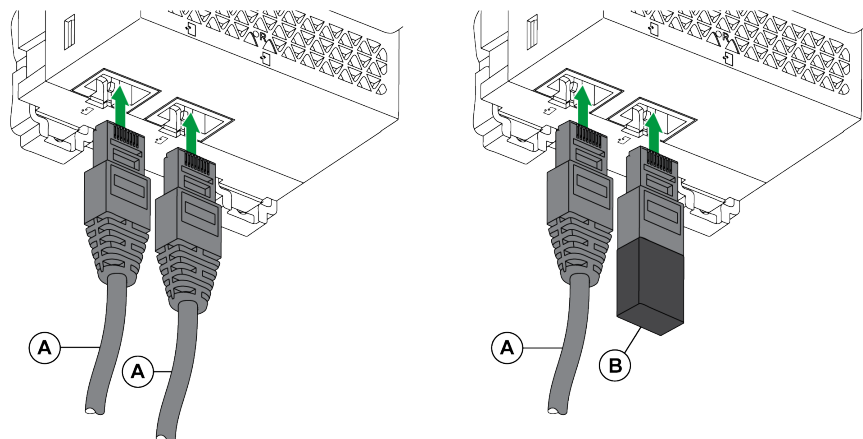
HAZARD OF EQUIPMENT DAMAGE

- Never connect an Ethernet device to a RJ45 ULP port.
- The RJ45 ULP ports of IFE interface are for ULP modules only.
- Any other use can damage the IFE interface or the device connected to the IFE interface.
- To check if a ULP module is compatible with the RJ45 ULP ports of IFE interface, refer to the DOCA0093•• *ULP (Universal Logic Plug) System - User Guide*, page 8.

Failure to follow these instructions can result in equipment damage.

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

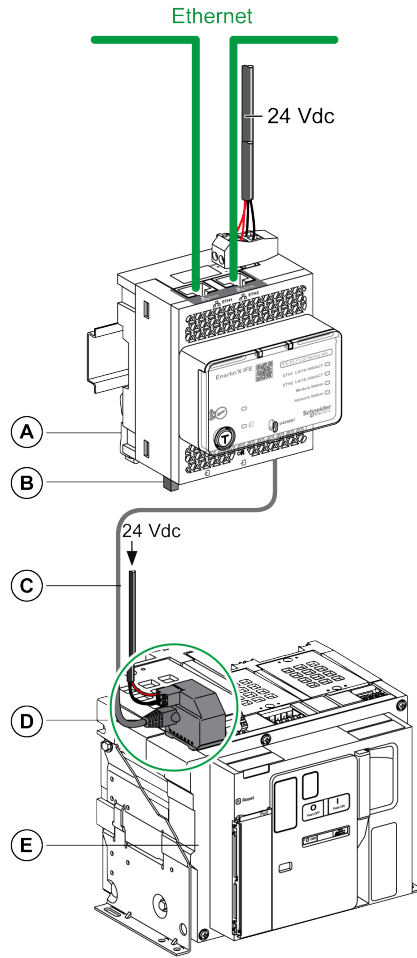
When the second RJ45 ULP port is not used, it must be closed with an ULP line termination.



- A** RJ45 plug/plug ULP cord or circuit breaker BCM ULP cord
B ULP line termination

Connection of the IFE Interface to a MasterPacT MTZ Circuit Breaker

Connect the IFE interface to the ULP port module on a MasterPacT MTZ circuit breaker by using the ULP cord.

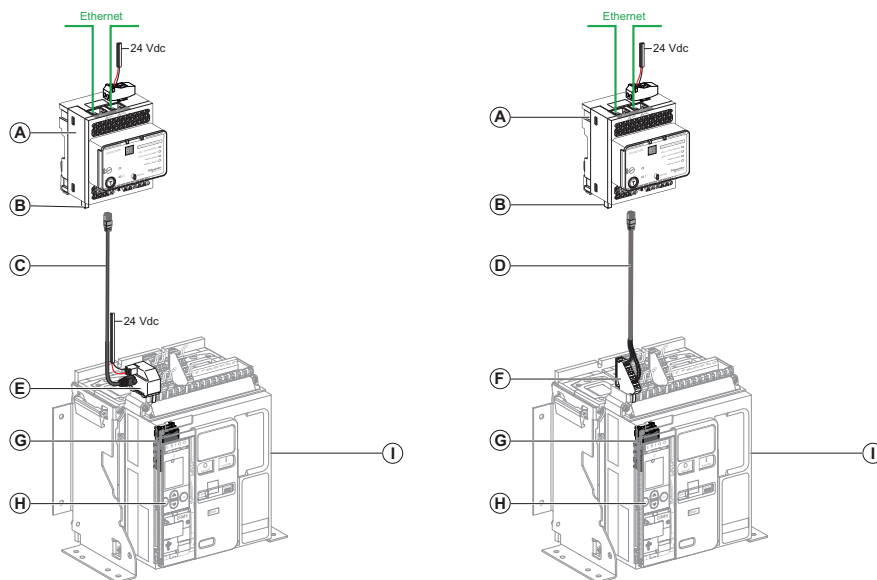


- A IFE Ethernet interface for one circuit breaker
- B ULP line termination
- C RJ45 plug/plug ULP cord
- D ULP port module
- E MasterPacT MTZ fixed circuit breaker

Connection of the IFE Interface to a MasterPacT MTZ Circuit Breaker with MicroLogic Active Control Unit

Connect the IFE interface to the MasterPacT MTZ circuit breaker with MicroLogic Active control unit through:

- ULP port module and RJ45 plug/plug ULP cord.
- COM terminal block and circuit breaker BCM ULP cord.



- A** IFE Ethernet interface for one circuit breaker
- B** ULP line termination
- C** RJ45 plug/plug ULP cord
- D** Circuit breaker BCM ULP cord
- E** ULP port module
- F** COM terminal block
- G** BCIM module
- H** MicroLogic Active control unit
- I** MasterPacT MTZ circuit breaker

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 interface to the circuit breaker using one of the following configurations:

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

For more information, refer to DOCA0093•• *ULP (Universal Logic Plug) System - User Guide*, page 8.

ULP Connection

NOTICE

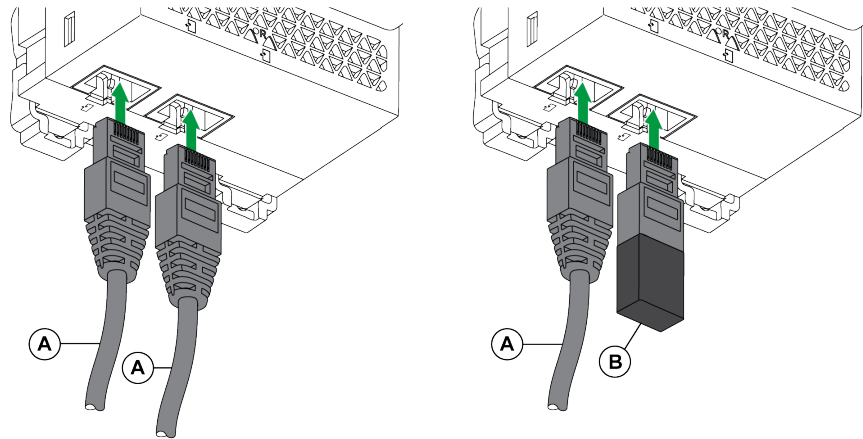
HAZARD OF EQUIPMENT DAMAGE

- Never connect an Ethernet device to a RJ45 ULP port.
- The RJ45 ULP ports of IFE interface are for ULP modules only.
- Any other use can damage the IFE interface or the device connected to the IFE interface.
- To check if a ULP module is compatible with the RJ45 ULP ports of IFE interface, refer to DOCA0093•• *ULP (Universal Logic Plug) System - User Guide*, page 8.

Failure to follow these instructions can result in equipment damage.

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.

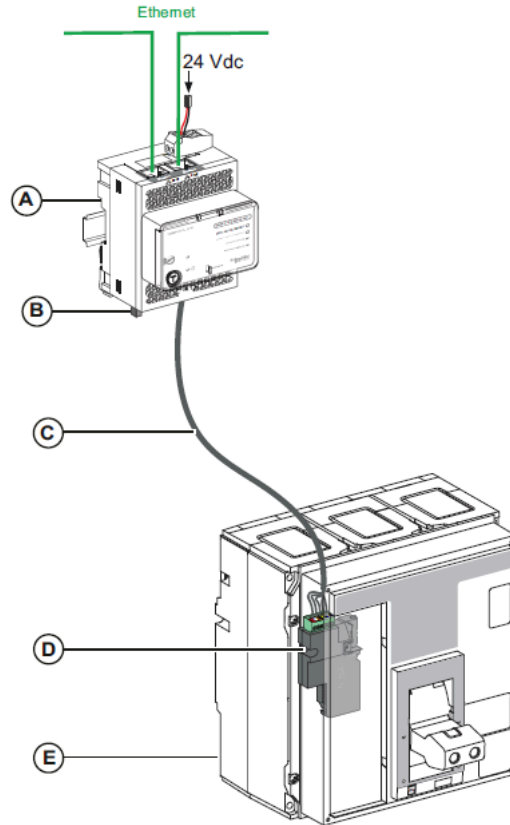


- A** Circuit breaker BCM ULP cord or RJ45 plug/plug ULP cord
- B** ULP line termination

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

Applicable for:

- ComPacT NS 630b-3200 circuit breakers
- PowerPacT P- and R-frame circuit breakers

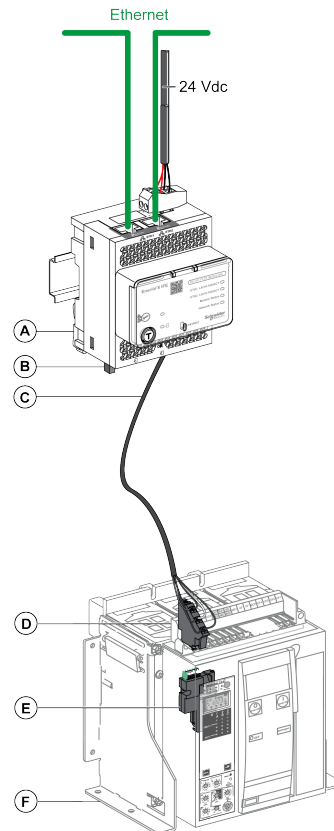


- A IFE Ethernet interface for one circuit breaker
- B ULP line termination
- C Circuit breaker BCM ULP cord
- D BCM ULP circuit breaker communication module
- E Fixed manually-operated circuit breaker

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

Applicable for:

- MasterPacT NT/NW circuit breakers
- ComPacT NS 630b-1600 circuit breakers
- PowerPacT P-frame circuit breakers

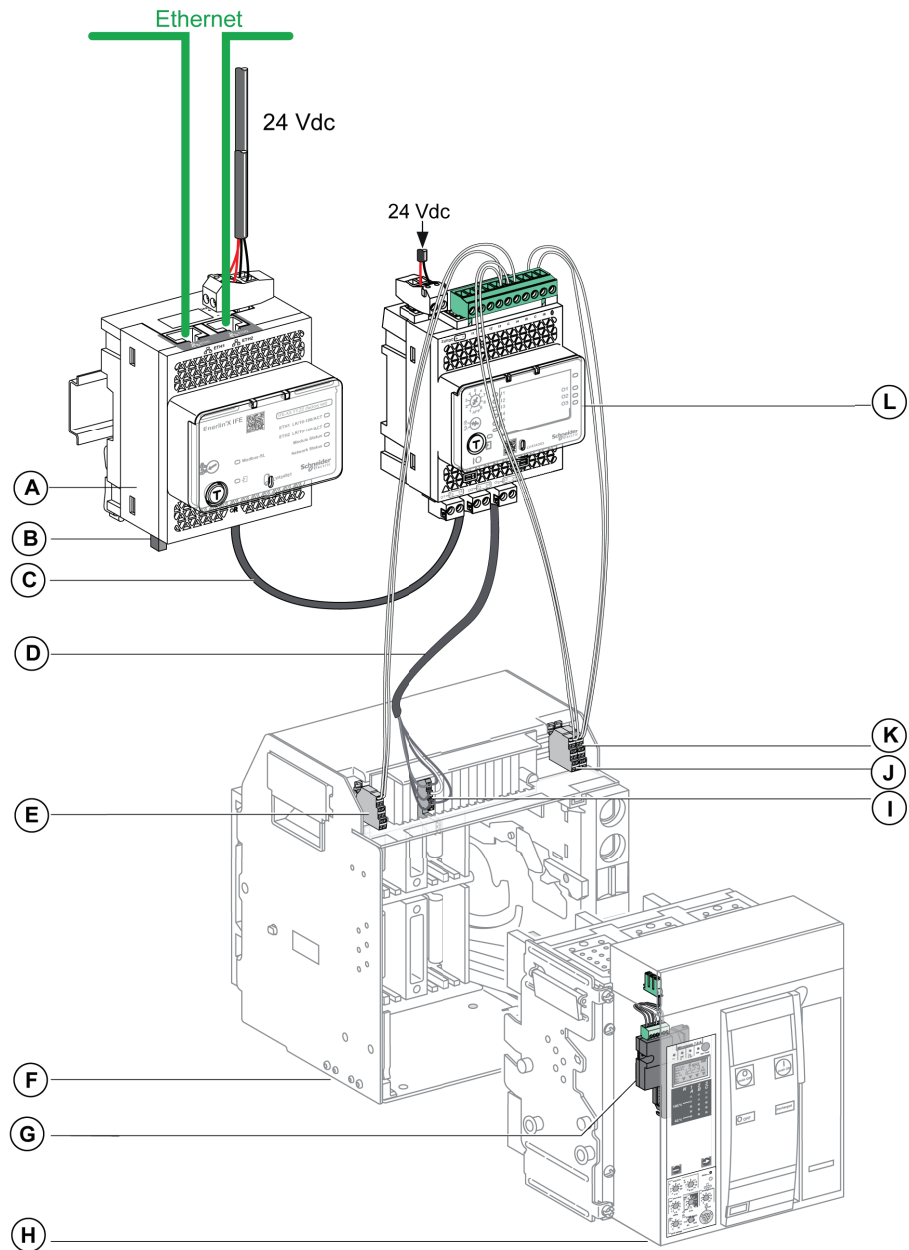


- A** IFE Ethernet interface for one circuit breaker
- B** ULP line termination
- C** Circuit breaker BCM ULP cord
- D** Fixed terminal block
- E** BCM ULP circuit breaker communication module
- F** Fixed electrically-operated circuit breaker

Connection of the IFE Interface to the Drawout Circuit Breakers

Applicable for:

- MasterPacT NT/NW circuit breakers
- ComPacT NS 630b-1600 circuit breakers
- PowerPacT P-frame circuit breakers



- A IFE Ethernet interface for one circuit breaker
- 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 Circuit Breakers

General Description

Depending on the configuration of the ComPacT NSX circuit breaker, connect the IFE interface to the circuit breaker using one of the following configurations:

- Connection of the IFE interface to the MicroLogic trip unit
- Connection of the IFE interface to the BSCM or BSCM Modbus SL/ULP module
- Connection of the IFE interface to the BSCM or BSCM Modbus SL/ULP module and to the MicroLogic trip unit

For more information, refer to DOCA0093** *ULP (Universal Logic Plug) System - User Guide*, page 8.

ULP Connection

⚠ WARNING

HAZARD OF ELECTRIC SHOCK

For system voltage greater than 480 Vac:

- Use the insulated NSX cord LV434204.
- Do not use NSX cords LV434200, LV434201, and LV434202.

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

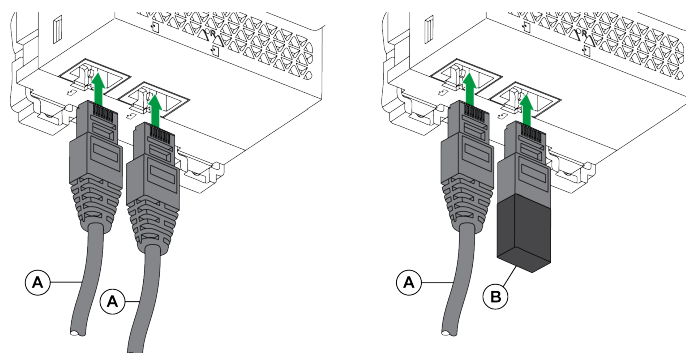
NOTICE

HAZARD OF EQUIPMENT DAMAGE

- Never connect an Ethernet device to a RJ45 ULP port.
- The RJ45 ULP ports of IFE interface are for ULP modules only.
- Any other use can damage the IFE interface or the device connected to the IFE interface.
- To check if a ULP module is compatible with the RJ45 ULP ports of IFE interface, refer to DOCA0093** *ULP (Universal Logic Plug) System - User Guide*, page 8.

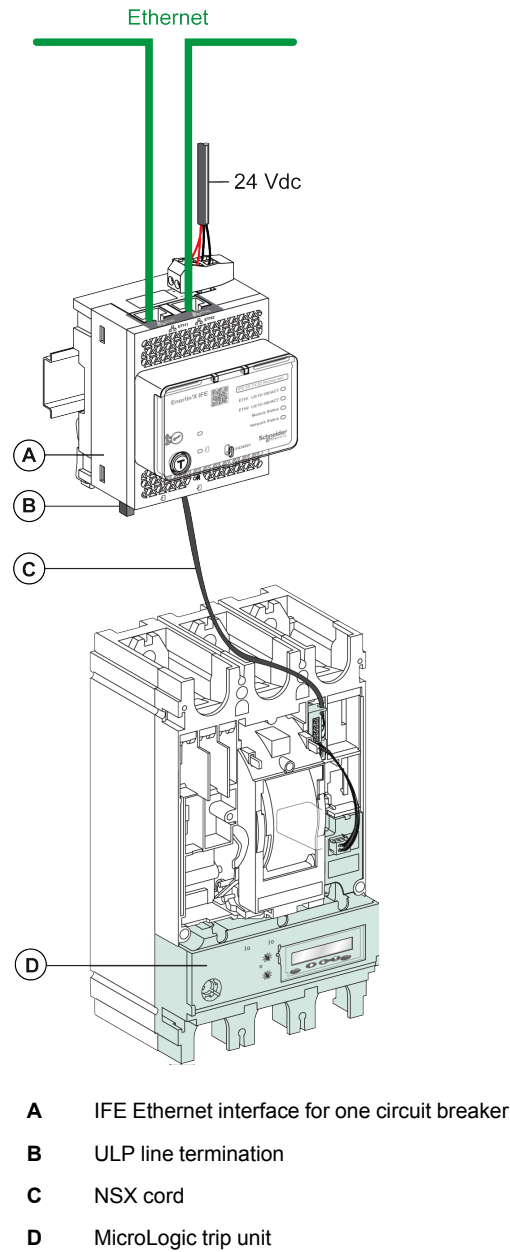
Failure to follow these instructions can result in equipment damage.

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

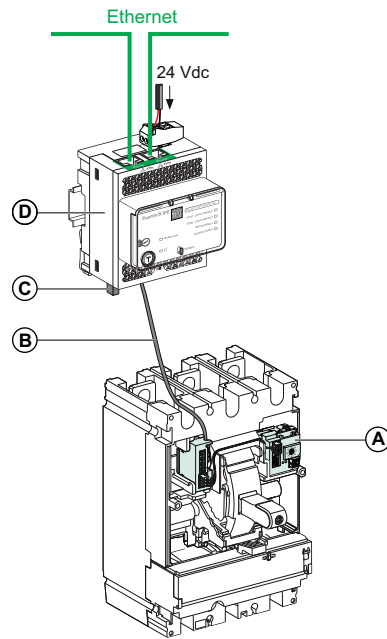


- A NSX cord or RJ45 plug/plug ULP cord
- B ULP line termination

Connection of IFE Interface to MicroLogic Trip Unit

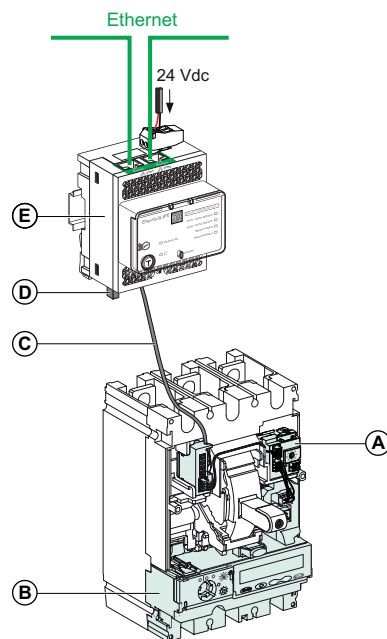


Connection of IFE Interface to BSCM or BSCM Modbus SL/ ULP Module



- A BSCM or BSCM Modbus SL/ULP module
- B NSX cord
- C ULP line termination
- D IFE Ethernet interface for one circuit breaker

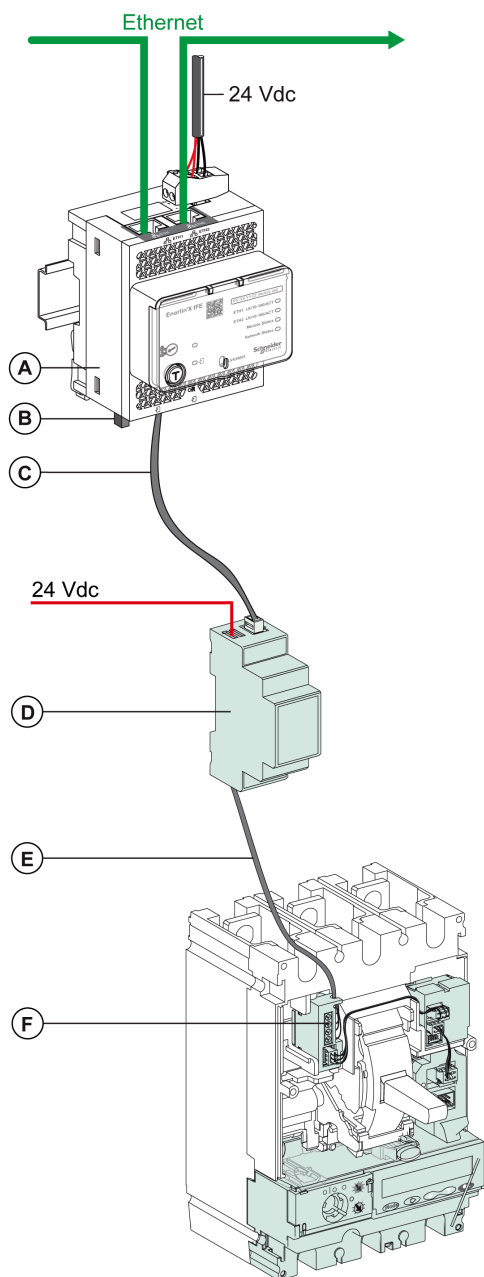
Connection of IFE Interface to BSCM or BSCM Modbus SL/ ULP Module and to MicroLogic Trip Unit



- A BSCM or BSCM Modbus SL/ULP module
- B MicroLogic trip unit
- C NSX cord

- D ULP line termination
- E IFE Ethernet interface for one circuit breaker

Connection of IFE Interface to a Circuit Breaker for System Voltage Greater than 480 Vac



- A IFE Ethernet interface for one circuit breaker
- 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 Connector for ComPacT NSX circuit breaker internal connection

Technical Characteristics

Environmental Characteristics

Characteristics		Value
Conforming to standards		<ul style="list-style-type: none"> 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...+85 °C (-40...+185 °F)
	Operation	-25...+70 °C (-13...+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		<ul style="list-style-type: none"> 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, refer to the DOCA0093•• *ULP (Universal Logic Plug) System - User Guide*, page 8.

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

What's in This Chapter

Recover IFE Interface from Boot Mode 41

All the features of the IFE interface firmware version 004 are also available for firmware version 005.

Description

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

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

For more information on IFE interface firmware versions, refer to DOCA0147** *Enerlin'X IFE/EIFE - Ethernet Interface - Firmware Release Notes*, page 8.

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 interface may be lost when the IFE interface 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.

NOTE: After updating the firmware of IFE interface from version 003 or 004 to 005, the user name and password of the IFE interface changes to default. When you access IFE interface for the first time after the firmware update, you are asked to change the default password. For more information, refer to *First Access Through PC with Windows 10 and Later*, page 50.

Checking the Firmware Version

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

- EcoStruxure Power Commission software, refer to the *EcoStruxure Power Commission Software Online Help*.
- IFE webpages, refer to the following procedure:
 1. Sign in to the IFE webpage.
 2. Do one of the following:
 - Navigate to **Diagnostics > Device Identification > Firmware version**.
 - Navigate to **Diagnostics > IFE > Firmware Revision**.

NOTE: If you have updated the firmware recently, press **F5** to refresh the webpage and update the displayed firmware number.

Updating Firmware and Webpages Using EcoStruxure Power Commission Software

Click [here](#) to download the latest version of EcoStruxure Power Commission software.

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

NOTICE

UNSUCCESSFUL FIRMWARE UPDATE

Do not update the firmware of IFE Interface (LV434010). Hardware degradation can interrupt the update process. If the update is unsuccessful, the IFE interface transitions into boot mode.

Failure to follow these instructions can result in equipment damage.

Recover IFE Interface from Boot Mode

During a firmware upgrade, if any communication disturbance occurs and files are not transferred successfully, the IFE interface can transition to boot mode.

1. Connect IFE interface to a circuit breaker using a ULP cable.
2. Change the IP address of connected PC to **169.254.XX.XX**. You can enter any value between 1 to 254 for XX.XX.
NOTE: You can refer to *Microsoft Windows Help* for performing step 2 and 3.
3. Set the subnet mask to **255.255.0.0**.
NOTE: This ensures the PC is configured within the same IP address range of the IFE interface in boot mode.
4. Open the EcoStruxure Power Commission software.
5. Sign in to EcoStruxure Power Commission software.
6. Discover the IFE interface, which is in the boot mode.
NOTE: The current firmware version of IFE interface is displayed as **IFEBOOT**.
7. Initiate the firmware update process.
After the firmware update, the IFE interface reverts to its original IP address.
8. Restore the PC network settings.

Security Features

What's in This Part

Machine to Machine Communication	43
Role Based Access Control.....	44
Security Logs.....	47

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 interface 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 interface 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 Parameter, page 76.

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 is a way to assign different levels of access to the users that define the features they can access.

RBAC is supported by MasterPacT MTZ, ComPacT NSX, and PowerPacT H-, J-, and L-frame circuit breakers only.

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

- IFE webpages
- EcoStruxure Power Commission software

For information about enabling RBAC when the connection is made through EcoStruxure Power Commission software, refer to *IP Network Services*, page 76.

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 interface users.

The security administrator can manage the users of IFE interface:

- On the IFE webpages
- With the EcoStruxure Cybersecurity Admin Expert software

EcoStruxure Cybersecurity Admin Expert Software

EcoStruxure Cybersecurity Admin Expert software is used for security configuration of the IFE interface with firmware version 004.009.000 and later.

The security administrator can use EcoStruxure Cybersecurity Admin Expert software to:

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

For more information, refer to CAE_UM_EN *EcoStruxure Cybersecurity Admin Expert Guide*, page 8.

NOTE:

- Enable HTTPS for secure transfer of configurations from EcoStruxure Cybersecurity Admin Expert software to IFE interface.
- Enable DPWS for discovery of the IFE interface on EcoStruxure Cybersecurity Admin Expert software.

CAE Software Settings

The security administrator can set the following parameters in the EcoStruxure Cybersecurity Admin Expert software:

Parameter	Description	Value
Minimum inactivity period	After this duration without any action from the user, IFE interface webpages are locked.	<ul style="list-style-type: none"> • Range: 1–3600 s • Default value: 600 s
Maximum login attempts	The maximum login attempts	<ul style="list-style-type: none"> • Range: 1–32 • Default value: 3
Locking period duration	After this duration the locked user account will be unlocked.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Range: 1–65534 • Default value: 601
Device measure read permission	Enabled while creating a role.	Default setting: Disabled

NOTE: EcoStruxure Cybersecurity Admin Expert software supports a maximum of 12 users and 10 user roles for the IFE interface.

CAE Device Specific Settings

The DSS is unique to the IFE interface 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 interface while leaving it inactive on others.

The following device specific settings are available on the EcoStruxure Cybersecurity Admin Expert software:

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

Permission for Each Role

The security administrator can modify the permissions for each role using the EcoStruxure Cybersecurity Admin Expert 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	–	–	✓	–	–
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 interface 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 84.
- 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 84.

IFE Webpages from Firmware Version 005

What's in This Part

Webpage Access and User Interface	49
Settings Pages	56
Security Pages.....	75
Monitoring and Control Pages	85
Diagnostics Pages	91

Webpage Access and User Interface

What's in This Chapter

Access to IFE Webpages	50
User Interface Layout	52
Webpage Description	54

Access to IFE Webpages

Supported Web Browsers

Browser	Version with Windows 10 and later
Microsoft Edge	81.0.416.58 and later
Mozilla Firefox	45.0 and later
Google Chrome	45.0 and later

First Access to the IFE Webpages

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

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

First Access Through PC with Windows 10 and Later

Step	Action
1	Disconnect the PC from the LAN and switch off Wi-Fi.
2	Connect an Ethernet cable from the computer to the IFE interface or to the Ethernet switch inside the panel.
3	Open File Explorer.
4	Click Network and the IFE- XXYYZZ appears in the list of devices. NOTE: If the IFE interface name is not displayed in the list of devices in File Explorer, check if the PC and the IFE interface 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 Edge.
6	Enter <i>SecurityAdmin</i> as the user name and <i>AAAAAAAA</i> as the password, the home page automatically opens in the browser. NOTE: The user name and password are case-sensitive.
7	To change the 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 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).

Step	Action
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 interface 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.

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 interface name has been configured.

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

Name Browsing

DNS server is mandatory.

Step	Action
1	Connect the IFE interface or the Ethernet switch inside the panel to the LAN.
2	Connect the computer to the LAN.
3	Start the web browser, page 50.
4	In the address text box, enter the IFE interface name which is written on the device label located on the front face of the selected IFE interface.
5	Press Enter , the login page automatically opens in the browser. NOTE: If the IFE interface does not appear in the list of devices in File Explorer, check if the PC and the IFE interface are not connected through the router.

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

IP Address Browsing

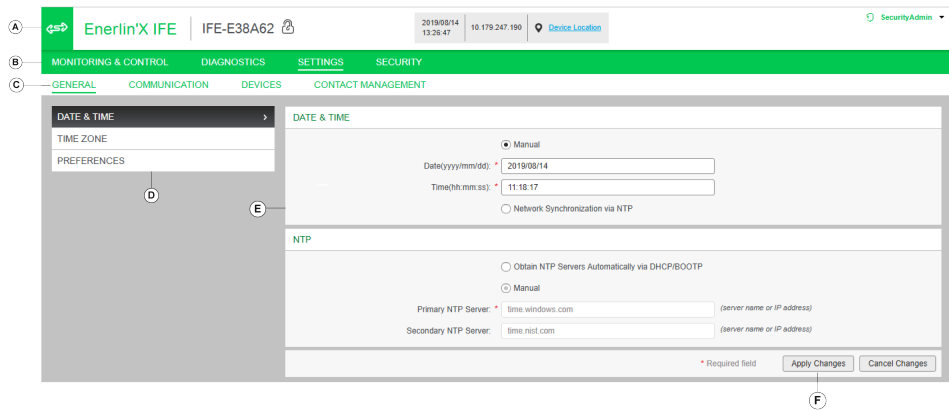
IP static configuration has to be set.

Step	Action
1	Connect the IFE interface or the Ethernet switch inside the panel to the LAN.
2	Connect the computer to the LAN.
3	Start the web browser, page 50.
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.

User Interface Layout

Overview

This graphic displays the IFE webpage user interface layout.



- A Header
- B Menu bar
- C Submenu bar
- D Webpages
- E Display zone
- F Action field




Header

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



- A IFE interface 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 interface name	Device name of the IFE interface.
Intrusive command mode	<ul style="list-style-type: none">  : 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.
IP address	IPv4 address of the interface.
Device Location	Click Device Location to locate the selected interface in your equipment: <ul style="list-style-type: none"> • The ULP LED of the selected interface 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 webpage session, or close your browser. It is recommended to log out from the IFE webpage 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 dialog is displayed for confirmation to restart the IFE interface to apply the new settings:

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

Display Zone

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

Webpage Description

MONITORING & CONTROL Webpage

Submenu	Webpage	Description
CIRCUIT BREAKERS , page 86.	–	<ul style="list-style-type: none"> • Displays data from the circuit breaker. • Allows you to reset of minimum and maximum values. • Allows you to control the circuit breaker.
IO MODULES , page 90	–	<ul style="list-style-type: none"> • Displays data from the IO modules. • Allows you to control the IO modules. • Displays Input/Output configuration for IO modules connected to the IFE interface.

DIAGNOSTICS Webpage

Submenu	Webpage	Description
COMMUNICATION	STATUS , page 92	Displays diagnostic data used to troubleshoot the network-related problems.
	ETHERNET , page 93	Displays the diagnostic data of Ethernet global statistics and Ethernet port characteristics.
	MODBUS , page 94	Displays the global statistics of TCP/IP and TCP port connections.
	ULP , page 95	Displays the global statistics of ULP port connection.
	REDUNDANCY-RSTP BRIDGE , page 96	Displays the diagnostic data of RSTP bridge.
	REDUNDANCY-RSTP PORTS , page 97	Displays the diagnostic data of RSTP ports.
	SNMP , page 98	Displays the diagnostic data of SNMPV1 Agent.
	READ DEVICE REGISTERS , page 99	Displays the list of devices to read device registers according to the selected device.
IFE , page 100	–	<ul style="list-style-type: none"> • Displays the IFE interface basic information. • Displays the IFE interface parameters and characteristics.
DEVICES , page 102	–	<ul style="list-style-type: none"> • Displays the list of the IMU devices connected to the ULP port. • Displays the maintenance counter information of the selected device. • 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 interface time automatically using an NTP source or configures the device connected to IFE interface to synchronize their time with the IFE interface time automatically.
	TIME ZONE , page 58	Sets the time zone for the region and sets the daylight saving time.
	PREFERENCES , page 59	Sets IFE interface preferences for data refreshment.
COMMUNICATION	ETHERNET , page 60	Sets the Modbus TCP/IP communication interface.
	IP CONFIGURATION , page 62	Sets the IP parameters.
	EMAIL SERVICE , page 64	Sets the configuration of SMTP server for mailing purpose.
	DATA PUBLISHING , page 66	Sets data generation and publishing parameters.
	REDUNDANCY-RSTP , page 67	Sets the RSTP bridge and RSTP port details.
	SNMP , page 69	Sets the SNMPV1 agent parameters.
DEVICES , page 71	–	<ul style="list-style-type: none"> • Sets the IFE interface name. • Sets the circuit breaker name and data publishing.
CONTACT MANAGEMENT	EMAILS , page 74	<ul style="list-style-type: none"> • 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 76	–	Configures the settings and activates the IP network services.
MODBUS TCP/IP FILTERING , page 77	–	Configures the IP addresses that can access the IFE interface through Modbus TCP/IP.
CERTIFICATES , page 79	–	Displays the IFE interface certificate with expiration date and validity period.
USER MANAGEMENT , page 81	–	Manages the existing and newly added user accounts.
SYSLOG SERVICE , page 84	–	Configures the Syslog server address.

Settings Pages

What's in This Chapter

Date and Time	57
Time Zone	58
Preferences	59
Ethernet	60
IP Configuration	62
Email Service	64
Data Publishing	66
Redundancy-RSTP	67
SNMP	69
Devices	71
Emails	74

Date and Time

Description

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

- Manually set the date and time of the circuit breaker connected to the IFE interface.
- Automatically synchronize the date and time of the circuit breaker to the IFE interface 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: <ul style="list-style-type: none"> • Select Manual (default setting) to set manually the date and time in the dedicated fields. • Select 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: <ul style="list-style-type: none"> • Select Obtain Servers Automatically via DHCP/BOOTP (default setting) to set the NTP servers automatically. • Select 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 interface and another IMU device is setting the date and time, the IFE interface 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 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 interface 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 interface 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 interface 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

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 dialog is displayed for confirmation to restart the interface to apply the new settings:

- Click **Yes** to restart the IFE interface 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 interface. The MAC address is written on the label which is placed on the side of the IFE interface.	–
Frame Format	Used to select the format for data sent over an Ethernet connection.	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none"> Select Automatic (default setting) to set IPv4 parameters automatically by using DHCP or BOOTP. Select 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: <ul style="list-style-type: none"> DHCP (default setting) BOOTP <p>NOTE: While using a legacy DHCP server, the device name must be limited to 16 characters.</p>
IP address	Used to enter manually the static IP address of an IFE interface.
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 dialog is displayed for confirmation to restart the interface to apply the new settings:

- Click **Yes** to restart the IFE interface 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 interface. <p>NOTE: In the URL address box, use [] brackets to enter the link local address.</p>

DNS Settings

Parameter	Description
DNS address	Allows you to select the IPv4 configuration mode: <ul style="list-style-type: none"> Select Automatic (default setting) to obtain the IP address from the DNS server automatically. Select Manual to set manually the primary and secondary server addresses. <p>NOTE: Domain name system (DNS) is the naming system for computers and devices connected to a local area network (LAN) or the Internet.</p>
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 interface publishes its IP address. To avoid any duplicate IP address conflicts, the IFE interface 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 interface 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 interface 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 interface 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.	<ul style="list-style-type: none"> None (default setting) TLS STARTTLS
SMTP Server Port	Allows you to enter the SMTP server port.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> • 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 interface 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 interface 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, ý, and ç are not displayed correctly in the email. However, the generic text message is displayed correctly.

Data Publishing

Description

The **DATA PUBLISHING** page allows you to export the data selected on the **Devices** page by email or FTPS. For more information, refer to *Devices*, page 71.

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: First day of the month).

Manual Export

Click **Manual Export** to start an immediate data export based on the selected data publishing settings, regardless of the scheduled interval.

Test FTPS

Click **Test FTPS** to verify the FTPS connection. The IFE interface transmits a text file to the configured FTPS server.

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 dialog is displayed for confirmation to restart the interface to apply the new settings:

- Click **Yes** to restart the IFE interface 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.	<ul style="list-style-type: none"> • Setting range: 0-61440 • Default setting: 32768
Bridge Hello Time	Allows you to enter bridge hello time.	<ul style="list-style-type: none"> • Setting range: 1-2 s • Default setting: 2 s
Bridge Max Age Time	Allows you to enter bridge maximum age time.	<ul style="list-style-type: none"> • Setting range: 6-40 s • Default setting: 40 s
Transmit Hold Count	Allows you to enter the transmit hold count.	<ul style="list-style-type: none"> • Setting range: 3-100 s • Default setting: 6 s
Bridge Forward Delay	Allows you to enter bridge forward delay.	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none">• Select Automatic (default setting) to set RSTP port 1 and 2 automatically.• Select 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.	<ul style="list-style-type: none">• Setting range: 0-240• Default setting: 128
Port 1 and 2 Cost	Allows you to enter manually the port 1 and 2 cost.	<ul style="list-style-type: none">• Setting range: 1-200000000

SNMP

Description

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

The IFE interface supports SNMP, allowing a network administrator to access remotely an IFE interface with an SNMP manager and to view the networking status and diagnostics of the IFE interface 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.	<ul style="list-style-type: none"> Setting range: 1 -65534 Default setting: 161
Notification Port	Allows you to enter notification port number.	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Select Automatic Configuration of System Name to set the system name automatically. Select 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 interface 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 interface 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.

Devices

Description

The **DEVICES** page allows you to select the data of the device connected to the IFE interface to publish (24 data maximum). The way to publish the data is set on the **DATA PUBLISHING** page , page 66.

The device connected to the IFE interface ULP port is automatically detected and added to the IFE interface in the device list.

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

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 **SETTINGS > DEVICES**.

Device Settings

Setting	Description	Value
Name	<p>Allows you to enter the IFE interface name.</p> <p>NOTE:</p> <ul style="list-style-type: none"> The LV breaker system is uniquely identified over possible interfaces such as HMI, Modbus/TCP, DPWS, and DHCP. IFE interface name is common across all interfaces. Thus, changing IFE interface name by any means has direct impact on all the connected interfaces. 	<p>The IFE interface name can have up to 63 ASCII characters.</p> <p>The allowed characters are A–Z, a–z, 0–9, and -.</p> <p>However, - is not allowed at the beginning or at the end of the name.</p> <p>NOTE:</p> <ul style="list-style-type: none"> IFE interface name should be unique. IFE interface names for different devices may have impact on web applications, logging, and export features.
Device Type	<p>Displays the device type.</p> <p>NOTE: The Device Type field is auto-detected and it is unavailable to edit.</p>	–
Device Name	<p>Allows you to enter the name for the discovered devices.</p> <p>NOTE:</p> <ul style="list-style-type: none"> You cannot change the device name for MasterPacT MTZ circuit breakers with MicroLogic X or Xi control units connected under ULP port, as the user application name and device name are the same. You can not edit or delete the device name if data publishing is enabled for the device. 	<p>The device name can have up to 45 ASCII characters.</p> <p>The allowed characters are A–Z, a–z, 0–9, Space, and -.</p> <p>However, Space and - is not allowed at the beginning or at the end of the name.</p>
IP Address/Server ID	<p>Displays the device IP address and the local address of the device connected to the IFE interface or remote device.</p> <ul style="list-style-type: none"> For IFE interface: The IP Address/Server ID box is unavailable to edit. For remote device: Allows you to enter IP address in the IP Address/Server ID box. 	For ULP port: 255 (Default setting)

Setting	Description	Value
Data Publishing	<p>Allows you to enable the publication of data from the device connected to the IFE interface (disabled by default).</p> <p>The data is selected to publish while Data Publishing is enabled.</p>	<p>There are eight categories for data publishing</p> <p>Default values:</p> <ul style="list-style-type: none">• Apparent Energy (kVAh)• Active Energy (kWh)• Reactive Energy (kVARh)
Select Data Publishing	<p>Click Select Data Publishing to open the Data Publishing window, where you can select the data to publish.</p>	—

Selection of the Data to Publish

The data to publish are listed in eight categories:

- **Current**
- **Voltage**
- **Power**
- **Energy**
- **Demand Current**
- **Demand Power**
- **Threshold Current**
- **Breaker Status**

In each category, the list of data to publish is adapted to the device connected to the IFE interface.

A maximum of 24 data can be selected for publication, out of which the following three data are selected by default:

- **Apparent Energy (kVAh)**
- **Active Energy (kWh)**
- **Reactive Energy (kVARh)**

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. , page 65
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 , page 71.

Notification Page

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

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

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

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

Security Pages

What's in This Chapter

IP Network Services	76
Modbus TCP/IP Filtering	77
Certificates	79
User Management.....	81
Syslog Service	84

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 or 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 interface. NOTE: It is recommended to set it as Enabled. Once the secure commissioning is enabled, if EPC software is connected to IFE interface, user must start a new discovery of the IFE interface 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 or disable the secure Modbus for machine-to-machine service. NOTE: Machine-to-Machine secure communication requires components that connect to the IFE interface 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 or disable the FTPS server.	Default setting: FTPS server is disabled
Discovery	Allows you to enable or disable the discovery (DPWS) of the IFE interface 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 or 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 interface.

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: <ul style="list-style-type: none"> • Read only: The following Modbus TCP/IP function codes are allowed: <ul style="list-style-type: none"> ◦ 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: <ul style="list-style-type: none">• Read: The following Modbus TCP/IP function codes are allowed:<ul style="list-style-type: none">◦ 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 interface 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 interface with firmware version 004.005.000 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 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 interface is Self-Signed.
Validity Period (UTC)	Validity period of the certificate. The certificate generated by the IFE interface 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, page 45.

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 interface 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 user. <ul style="list-style-type: none"> • User name is composed of 4 to 16 characters. • User name is case-sensitive and can contain special characters.
Password	Enter the password for the new user , page 82. The password entered must be confirmed.
Role	Select one or multiple roles for the new user in the predefined list of roles , page 44.
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.
Email Id	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.
Email Id	Displays the email address of the user.
Language	Displays the selected language of the user.
Phone	Displays the phone number of the user.
User Status	Displays the user status.
Password Expiry Time	Displays the expiration time of user password.
Locked Until	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 *, /, \, and so on.

The password must contain one letter lowercase, one letter uppercase, one digit and one special character.

NOTE: Password with 11 asterisks (******) is not allowed. While editing a user password, the three previous passwords of this user cannot be used.

Password Customization

Once 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 **Reset** in the webpage. The new password is generated automatically and is displayed in a 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 [Reset Button](#), page 20.

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 interface.

The IFE interface logs 2048 security events before the oldest events are overwritten by newer events.

Ensure the security logs are exported on a regular basis from the IFE interface 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 EcoStruxure Cybersecurity Admin Expert software. For more information, refer to CAE_UM_EN *EcoStruxure Cybersecurity Admin Expert Guide*, page 8.

Ensure that the Syslog server is installed in your monitoring PC.

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 or 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 **Test Connection** to verify the connection between the IFE interface and Syslog server. During the test, the IFE interface 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	86
IO Modules	90

Circuit Breakers

Description

The **CIRCUIT BREAKERS** page allows you:

- With any role to monitor data from the circuit breaker.
- With Installer or Engineer role to reset minimum and maximum values of the energy and demand measurements.
- With Operator role to control the circuit breaker.

Navigation to Circuit Breakers page

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

Page Layout

The screenshot shows the EnderlinX IFE web interface. The top navigation bar includes 'ENERLINX IFE', 'IFE-DataLogging', and user information. The main content area is titled 'CIRCUIT BREAKERS' and contains a 'DEVICE LIST' on the left, a 'DEVICE OVERVIEW' card in the center, a 'CONTROL PANEL' below it, and a 'REAL TIME MEASUREMENTS' table at the bottom. Callouts A, B, C, and D are placed around the interface to highlight key features.

- A Circuit breaker identification data
- B Circuit breaker health status
- C Circuit breaker monitoring and control panel
- D Monitoring of measurements




Circuit Breaker Identification Data

The circuit breaker is identified by the following data:

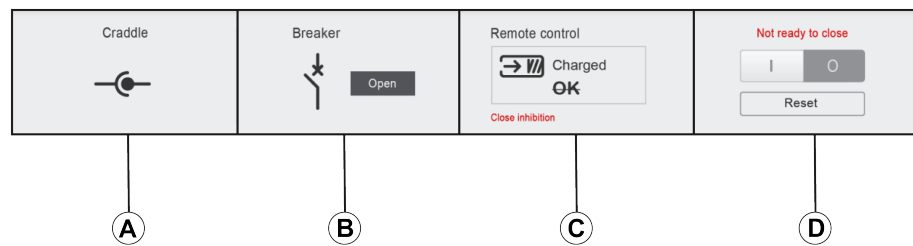
- Rated current
- Protection type
- Number of IO modules connected
- Additional data according to the range of the circuit breaker

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


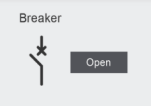
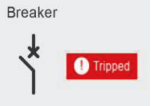
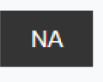
Drawout Circuit Breaker Position in the Cradle

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:

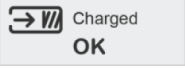
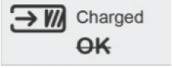

Icon	Description
	The main contacts of the circuit breaker are closed.
	The main contacts of the circuit breaker are opened.
	The main contacts of the circuit breaker are opened and the circuit breaker is tripped. The circuit breaker must be reset.
	The circuit breaker position is unknown in case of 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.


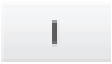

The circuit breaker control status is indicated by the following icons:

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
	Click this option to open the circuit breaker.
	Click this option to close the circuit breaker. The circuit breaker will close only if it is ready to close.
	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.
 - 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.

NOTE: The 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 trip unit or control unit of the circuit breaker.

Measurement are displayed in the following order:

- Real time measurements with minimum and maximum 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 Modules

Description

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

To open the **IO MODULES** page, navigate to **MONITORING & CONTROL > IO MODULES**.

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, 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 in DOCA0055•• *Enerlin'X IO - Input/Output Application Module for One Circuit Breaker - User Guide* in the Related Documents section at the beginning of the guide.

List of Parameters in IO Module

The **IO MODULES** page displays the following parameters:

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.	–
Label	Displays the assigned functions of the corresponding inputs or outputs.	–
Value	Displays the value of the six digital inputs and three digital outputs.	<ul style="list-style-type: none"> • 1 • 0
Forced	Displays the six digital inputs and three digital outputs are forced or not.	<ul style="list-style-type: none"> • FORCED • –

Diagnostics Pages

What's in This Chapter

Status.....	92
Ethernet	93
Modbus	94
ULP.....	95
Redundancy-RSTP Bridge.....	96
Redundancy-RSTP Ports.....	97
SNMP	98
Read Device Registers	99
IFE	100
Devices	102

Status

Description

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

While browsing the real-time data views, the IFE interface 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 interface, and attempts to re-establish the communication to any device marked out of service within the current browser session.

A manual communication check is possible by clicking **Check Device Status**.

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 device connected to IFE interface.
Device Type	Type of the device connected to IFE interface.
Connection	Displays the connection type: Type 1: ULP
Communication	Status of communication: <ul style="list-style-type: none"> Passed: IFE interface successfully connected to the devices. Failed: IFE interface not connected to the devices.

Ethernet

Description

The **ETHERNET** page displays:

- Ethernet global statistics accumulated since the IFE interface 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 interface 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: <ul style="list-style-type: none"> • 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 interface 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 interface 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). <ul style="list-style-type: none"> 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 interface 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 interface 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	Select the data type from Data Type drop-down list.	Selects the appropriate data type.
4	To change how Modbus data is displayed in the Value column, select Decimal , Hexadecimal , Binary , or ASCII .	Selects how the data values are displayed.
5	Click Read .	Reads the device registered according to the selected configuration.

IFE Interface Read Device Register Parameters

Parameter	Description	Settings
Device Name	Selects a device to read from the list of previously added devices. A Modbus interface device of a Modbus client IFE interface not defined in the device list can be read by entering its local ID number. NOTE: The interface 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.	255 NOTE: You cannot change the local ID.
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 interface. 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.	<ul style="list-style-type: none"> • 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 interface connected to the circuit breakers.

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

Navigation to the IFE Page

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

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

System Parameters

Parameter	Description
CPU	Status of the CPU: <ul style="list-style-type: none">• 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 Interface Operating Time Parameters

Statistic	Description
Operating Time	Operating time of IFE interface

Devices

Description

The **DEVICES** page gives the information about the devices which are connected to the ULP port of the IFE interface. The devices connected are:

- BCM ULP module
- MicroLogic control unit or trip unit
- BSCM module
- BSCM Modbus SL/ULP module
- FDM121 display
- USB maintenance interface or Universal Test Adopter (UTA) module

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

Navigation to the Devices Page

To view the **DEVICES** page, click **DIAGNOSTICS > 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.
Remaining service life indicator	Displays the remaining service life of circuit breaker.
Contact wear indicators	Displays the contact wear counters of the circuit breaker.
Indication contacts (OF) operation since last reset	Displays the indication of contact operation of circuit breaker since last reset.
Fault trip indication contact (SDE) operation	Displays the indication of fault trip contact operation of circuit breaker.
Cradle connected	Displays the status of cradle in connected position.
Cradle disconnected	Displays the status of cradle in disconnected position.
Cradle test	Displays the status of cradle in test position.

Components Parameters

Device	Parameter	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.

IFE Webpages up to Firmware Version 003

What's in This Part

Webpage Access and User Interface	105
Configuration & Settings Webpages	113
Monitoring Webpages.....	144
Control Webpages	151
Diagnostics Webpages	156
Maintenance Webpages	165

Webpage Access and User Interface

What's in This Chapter

Access to IFE Webpages	106
User Interface Layout	109
Webpage Description	111

Access to IFE Webpages

Supported Web Browsers

Browser	Version with Windows 10 and later
Microsoft Edge	81.0.416.58 and later
Mozilla Firefox	45.0 and later
Google Chrome	45.0 and later

First Access to the IFE Webpages

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

⚠ 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.

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

First Access Through PC with Windows 10 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 interface or to the Ethernet switch inside the panel.
3	Open File Explorer.
4	Click Network and the IFE-XXYYZZ appears in the list of devices. NOTE: If the IFE interface name is not displayed in the list of devices in File Explorer, check if the PC and the IFE interface are not connected through the router.
5	Double-click the selected IFE-XXYYZZ, the login page automatically opens in the browser.
6	Enter <code>Administrator</code> as the user name and <code>Gateway</code> as the default password, the home page automatically opens in the browser. NOTE: The user name and password are case-sensitive. The <code>Administrator</code> user name cannot be changed as it is a default user name for administrator role.
7	To change the default password, select the Configuration & Settings menu, go to Other Configuration submenu, click User Accounts and enter new password for <code>Administrator</code> 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).
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 interface name.
10	Write the IFE interface 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.

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 interface name has been configured.

Step	Action
1	Connect the IFE interface 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 File Explorer.
4	Click Network , the IFE interface name is displayed in the list of devices. NOTE: If the IFE interface name is not displayed in the list of devices in File Explorer, check if the PC and the IFE interface are not connected through the router.
5	Double-click the IFE interface name which is written on the device label located on the front face of the selected IFE interface, the login page automatically opens in the browser.

Name Browsing

DNS server is mandatory.

Step	Action
1	Connect the IFE interface 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 106.
4	In the address text box, enter the IFE interface name which is written on the device label located on the front face of the selected IFE interface.
5	Press Enter , the login page automatically opens in the browser. NOTE: If the IFE interface does not appear in the list of devices in File Explorer, check if the PC and the IFE interface are not connected through the router.

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

IP Address Browsing

IP static configuration has to be set.

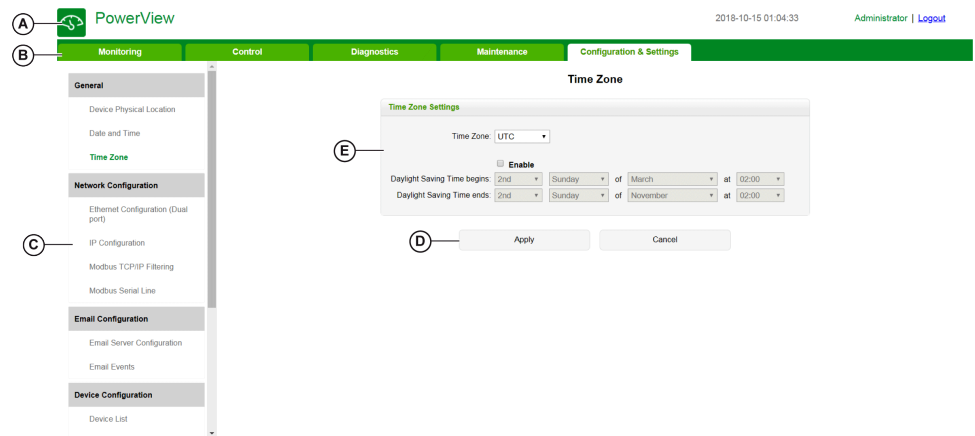
Step	Action
1	Connect the IFE interface or the Ethernet switch inside the panel to the local area network (LAN).
2	Connect the PC to the local area network (LAN).

Step	Action
3	Start the web browser, page 106.
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.

User Interface Layout

Overview

This graphic shows the IFE webpage user interface layout.



- A Banner
- B Menu tabs
- C Subtabs
- D Action field
- 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 webpage session, click Logout or close your browser. It is recommended to log out from the IFE webpage 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 interfaces:

Action Fields	Action
Apply	Applies the changes.
Cancel	Cancel 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 145	The single device pages provide basic readings of the circuit breaker connected to the IFE interface.
	Summary Device Pages, page 145	The summary device pages provide summaries of the circuit breaker connected to the IFE interface.
	Trending, page 145	The trending page view provides real-time graphic and table trending of the circuit breaker connected to the IFE interface.
Device Logging	Single Device Pages, page 147	The single device pages provide the graphic and table trending logs of user-selectable quantities for circuit breaker connected to the IFE interface.
	Summary Device Pages, page 149	The summary device pages provide graphic trending logs of the circuit breaker connected to the IFE interface.

Control Webpage

Control Submenu	Webpage	Description
Device Control	Device Control, page 152	Resets and controls the circuit breaker connected to the IFE interface.
Set Device Time	Set Device Time, page 155	Displays the time of the circuit breaker connected to the IFE interface.

Diagnostics Webpage

Diagnostics Submenu	Webpage	Description
General	Statistics, page 157	Displays diagnostic data used to troubleshoot the network-related problems.
Product Information	Device Identification, page 160	<ul style="list-style-type: none"> Displays the IFE interface basic information to set the IFE interface 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 161	Displays the list of the IMU devices connected to the ULP port.
Device Health Check	Read Device Registers, page 162	Displays register data connected locally to the IFE interface.
	Communications Check, page 163	Verifies the communication health of the circuit breaker connected to the IFE interface.
IO Readings	IO Readings, page 164	<p>Displays the status of IO module connected to the circuit breaker. Displays No IO modules connected if the circuit breaker is not connected to a IO module.</p> <p>NOTE: IO Module refers to the circuit breaker name defined in the Device List page.</p>

Maintenance Webpage

Maintenance Submenu	Webpage	Description
Indicators	Indicators, page 165	Displays the maintenance counters of the circuit breaker connected to the IFE interface.

Configuration & Settings Webpage

Configuration & Settings Submenu	Webpage	Description
General	Device Physical Location , page 114	<ul style="list-style-type: none"> Locate the IFE-XXYYZZ interface. Click Blink ON. The ULP LED of the IFE-XXYYZZ interface blinks and is active for 15 s (Test mode: 1 s ON, 1 s OFF).
	Date and Time , page 115	Sets the date and time manually or sets the IFE interface time automatically using an SNTP source or configures the device connected to IFE interface to synchronize their time with the IFE interface time automatically.
	Time Zone , page 117	Configures the time zone for the region and sets the daylight saving time.
Network Configuration	Ethernet Configuration (Dual port) , page 118	Configures the Ethernet.
	IP Configuration , page 119	Configures the IP parameters.
	Modbus TCP/IP Filtering , page 121	Configures the maximum number of Modbus TCP/IP server connections. Configures the IP addresses that can access the IFE interface through Modbus TCP/IP.
Email Configuration	Email Server Configuration , page 122	Configures the alarms to be emailed. Configures the SMTP parameter for mailing purpose.
	Email Events , page 124	Configures the alarms to be sent through email.
Device Configuration	Device List , page 133	Configures the circuit breaker connected to the IFE interface.
	Device Logging , page 134	Configures device logging parameters.
	Device Log Export , page 136	Configures device logging export options.
Other Configuration	SNMP Parameters , page 138	Configures Simple Network Management Protocol (SNMP).
	Preferences , page 139	Configures IFE interface preferences.
	Advanced Services Control , page 140	Configures the advanced service control parameters.
	User Account , page 141	Creates and edits groups and users. Configures email accounts.
	Webpage Access , page 143	Configures webpage access rights for each user group.

Configuration & Settings Webpages

What's in This Chapter

General	114
Date and Time	115
Time Zone	117
Ethernet Configuration (Dual Port)	118
IP Configuration	119
Modbus TCP/IP Filtering	121
Email Server Configuration	122
Email Events	124
Device List	133
Device Logging	134
Device Log Export	136
SNMP Parameters	138
Preferences	139
Advanced Services Control	140
User Accounts	141
Webpage Access	143

General

Device Physical Location

Step	Action	Result
1	From the IFE menu bar, click Configuration & Settings .	Displays the Configuration & Settings menu.
2	From the Configuration & Settings menu, in the General submenu, click Device Physical Location .	Displays the Device Physical Location page.
3	In Device Physical Location webpage, click Blink ON .	Sets the IFE interface 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 interface.
- To automatically synchronize the date and time of the circuit breaker to the IFE interface 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 the circuit breaker connected to the IFE interface. 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 enable the automatic time setting of the circuit breaker connected to the IFE interface. This option is disabled when Manual is selected.
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 time of the circuit breaker connected to the IFE interface with the IFE interface time.
Cancel	Allows you to clear the synchronization of the circuit breaker connected to the IFE interface.

Setting the IFE Interface 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 interface manually.
4	Enter the time in the format hh:mm:ss.	Sets the time of the IFE interface manually.
5	Click Apply .	The date and time of IFE interface is set.

Setting the IFE interface 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 circuit breaker connected to the IFE interface is 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 circuit breaker get synchronized with the IFE interface time.

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 interface 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 interface 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 interface. The MAC address is written on the label which is placed on the side of the IFE interface.	–
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.	<ul style="list-style-type: none"> • Ethernet II • 802.3 • Auto (default 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 (default setting)
Speed and mode for Port #2	Used to define the physical Ethernet connection speed and transmission for Ethernet port 2.	Auto-negotiation (default 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: <ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • DHCP (default setting) • BOOTP
Manual IP address	Used to enter the static IP address of an IFE interface.	–
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 (default 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 interface publishes its IP address. To avoid any duplicate IP address conflicts, the IFE interface 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 interface 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 interface 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 interface 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

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 interface.

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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Read: The following Modbus TCP/IP function codes are allowed: <ul style="list-style-type: none"> ◦ 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.	<ul style="list-style-type: none"> • Enabled • Disabled (default setting)

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 interface by default. If you have configured SMTP profile for the previous version of the IFE interface, 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.	<ul style="list-style-type: none"> • 25 (default setting) • 465: TLS • 587: STARTTLS
Authentication	If the SMTP server requires login information, enable the Authentication Enable check box.	<ul style="list-style-type: none"> • Enabled • Disabled (default 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.	<ul style="list-style-type: none"> • English (default 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 465 or 587). 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 interface.

NOTE: If an email SMTP server is not located on the same Ethernet network segment as IFE interface, ensure that the IFE interface 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 or 6 trip unit	Long time protection I _r pre-alarm (PAL I _r)
	Long time protection I _r
	Short time protection I _{sd}
	Instantaneous protection I _i
	Ground fault protection I _g
	Integrated Instantaneous protection
	STOP (trip unit internal failure)
	Reflex tripping protection
	Unbalance motor protection
	Jam motor protection
	Underload motor protection
Long start motor protection	

Device Connected	Events
ComPacT NSX or PowerPacT H-, J-, and L-frame circuit breaker with MicroLogic 5 or 6 trip unit	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
ComPacT NSX circuit breaker with MicroLogic 7 trip unit	Earth leakage (Vigi) protection I Δ n
	Instantaneous with earth leakage protection

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 I _r pre-alarm (PAL I _r)
	Long time protection I _r
	Short time protection I _{sd}
	Instantaneous protection I _i
	Ground fault protection I _g
	Integrated Instantaneous protection
	STOP (trip unit internal failure)
	Reflex tripping protection
	Unbalance motor protection
	Jam motor protection
	Underload motor protection
	Long start motor protection
	I _{unbal} protection
	I1 Max protection
	I2 Max protection
	I3 Max protection
	I _N Max protection
	V _{min} protection
	V _{max} protection
	V _{unbal} protection
	Reverse power protection
	F _{min} protection
	F _{max} protection
	Phase rotation
Ready to close status (PF)	
Wear on contacts	

	Arc reduction state engaged
MasterPacT NT/NW or ComPacT NS circuit breaker with BCM ULP module	Earth leakage (Vigi) protection IΔn
	Instantaneous with earth leakage protection

Events from MasterPacT MTZ Circuit Breaker

Device connected	Events
MasterPacT MTZ circuit breaker with MicroLogic 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 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 software)
	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	

Device connected	Events
MasterPacT MTZ circuit breaker with MicroLogic control units	Injection test in progress
	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	

Device connected	Events
MasterPacT MTZ circuit breaker with MicroLogic control units	Invalid Control Unit factory config #1
	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	

Device connected	Events
MasterPacT MTZ circuit breaker with MicroLogic control units	Overfrequency trip
	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 control unit 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
	IDMTG Ig trip
	IDMTG Ig start
	IDMTG Ig operate

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)
	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 disconnecter 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)	

Events from IFE Interface

Device connected	Events
IFE Interface	Password of service user profile for IFE interface was changed
	Password of engineer user profile for IFE interface was changed
	Password of operator user profile for IFE interface was changed
	Password of administrator user profile for IFE interface was changed
	All the passwords for IFE interface were changed

Device List

Description

The circuit breaker connected to the IFE interface is automatically detected. Click **Apply** to add it in the device list.

Device List Parameters

Parameters	Description	Settings
IP Address	Displays the device IP address.	–
Gateway	Indicates if the IP device is a gateway or not. NOTE: Gateway check box is always cleared for IFE interface.	–
Address	Displays the Modbus address of the IFE interface. NOTE: The Address text box is unavailable to edit.	255 (fixed)
Name	Allows you to enter the name for IFE interface. NOTE: <ul style="list-style-type: none"> The LV breaker system is uniquely identified over possible interfaces such as HMI, Modbus/TCP, DPWS, and DHCP. IFE interface name is common across all interfaces. Thus, changing IFE interface name by any means has direct impact on all the connected interfaces. 	The IFE interface 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: <ul style="list-style-type: none"> IFE interface name should be unique within the device list. Duplicate device names for different devices may have impact on web applications, logging, and export features.
Connection	Displays the connection type (ULP). NOTE: The Connection field is unavailable to edit.	ULP port
Device Type	Automatically displays the device type discovered on the ULP system. NOTE: The Device Type field is auto-detected and it is unavailable to edit.	–
Device Name	Allows you to enter the name for the discovered devices.	The device name can have up to: <ul style="list-style-type: none"> 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.
Slave ID	Displays the local address of the device connected to the IFE interface.	255 (Fixed)
Apply	Allows you to save device list configuration.	–
Delete	This operation is not available.	–
Operation	Allows you to edit the device name.	–

Device Logging

Description

Logging is available for the device which is in the device list, page 133. 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 interface can log data received at predefined intervals (5, 10, 15, 20, 30, and 60 minutes). Following is an explanation of how the IFE interface 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 interface provides this data logging at predefined intervals.

The features of IFE interface data logging are:

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

The circuit breaker in the device list can be enabled for logging. Topics to log are unique to each device. To view interval data logs, refer to [Device Logging](#), page 147 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, select **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 interface. The device log export allows you to configure IFE interface to export device logs periodically. You can choose to export the device log files through email or FTPS.

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

Transport

Parameter	Description	Setting
Disabled	When Disabled is selected, either email or FTPS is enabled.	–
Email	Allows you to export the log files through email.	–
FTPS	Allows you to export the log files through FTPS.	–
Incremental	Selects only the new interval data logged since the last successful data export. NOTE: <ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> • Hourly • Daily • Weekly • Month-ly • Log-ging Interval

To Addresses

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

FTPS Parameters

Parameter	Description	Setting
Server IP Addresses	Allows you to enter the FTPS 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 FTPS username.	–
Password	Allows you to enter the FTPS password.	–
Passive	Allows you to select the mode of FTPS operation. NOTE: Passive mode is enabled by default.	–

SNMP Parameters

Manage IP Parameters

The IFE interface supports SNMP, allowing a network administrator to access remotely an IFE interface with an SNMP manager and to view the networking status and diagnostics of the IFE interface 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 (default setting)
Read-write Community Name	Allows you to configure the SNMP read-write community name.	Private (default setting)
Trap	Allows you to trap the community name.	Alert (default setting)

NOTE: Only SNMP version 1 is supported.

Enabled Traps

Parameter	Description	Setting
Coldstart Trap	Generates a trap when the IFE interface 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 interface 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 Default settings: 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 Default settings: 15 min

Advanced Services Control

Industrial Protocol

Parameter	Description	Setting
Enable Modbus/TCP	Allows you to enable/disable the Modbus/TCP service.	<ul style="list-style-type: none">• Enabled (default setting)• Disabled

Services Configuration

Parameter	Description	Setting
Enable FTPS server	Allows you to enable/disable the FTPS service.	<ul style="list-style-type: none">• Enabled (default setting)• Disabled
Enable device announcement	Allows you to enable/disable the DPWS service.	<ul style="list-style-type: none">• Enabled (default setting)• Disabled
Enable SNMP	Allows you to enable/disable the SNMP service.	<ul style="list-style-type: none">• Enabled• Disabled (default setting)

User Accounts

Description

The IFE interface 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 interface 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 *, /, \, and so on

NOTE: Password with eleven asterisks (******) 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 Interface 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: <ul style="list-style-type: none">• 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 Webpages

What's in This Chapter

Real Time Data	145
Device Logging	147

Real Time Data

Description

The **Real Time Data** page provides:

- The basic readings of the circuit breaker connected to the IFE interface in real time on **Single Device Pages**.
- The circuit breaker summaries on **Summary Device Pages**.
- The real-time trending for the circuit breaker 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 circuit breaker connected to the IFE interface 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 the circuit breaker from Single Device Pages .	Displays the real-time data of the circuit breaker.

Summary Device Pages

The summary device table views provide summary of the circuit breaker connected to the IFE interface.

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 circuit breaker 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 circuit breaker 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 the circuit breaker from the Available Devices list.	Selects the circuit breaker for trending.
5	Select up to 8 topics from the Available Topics list.	Selects topics for trending.

Step	Action	Result
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.	Selects the amount of time of the trend.
3	Select Start Sampling to start the trending of the selected 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 log data of the circuit breaker connected to the IFE interface. For more details on configuring device logging, refer to [Device Logging](#), page 134.

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 .	Displays the available device logging choices.
3	From the Device Logging , click Single Device Pages .	Displays the available device with logged data available for viewing.
4	Select the 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: <ul style="list-style-type: none"> • 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 the circuit breaker 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 interface FTPS server	Comma-separated variable (CSV)
Export to an external FTPS server	CSV
Data point option	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 FTPS](#), page 149. Files are in the format: *Device Name.csv* where the device name is the name given to the 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 DOCA0384** *MasterPacT, ComPacT, PowerPacT Circuit Breakers - Modbus Communication - User Guide*, page 8.
- The device log file may contain invalid values (-9999, -99999, and 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 interface name, IFE interface serial number, IFE interface 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 interface 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 interface 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 interface FTPS Server

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

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

Step	Action	Result
1	Create a folder on your PC, such as C\:\file_logs.	Creates a folder to store the IFE interface data log.
2	Launch Windows Explorer, enter <code>ftps://</code> and the IP address of the IFE interface in the address text box (for example, <code>ftps://169.254.0.10</code>), press Enter .	Opens the Log On As dialog box.
3	Enter the user name as <code>Administrator</code> and password as <code>Gateway</code> in the text boxes, click Log On .	Opens an FTPS session with the IFE interface and displays the files stored in the IFE interface.
4	Navigate to the directory <code>/logging/data</code> on the IFE interface.	Opens the data logging directory on the IFE interface.
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 interface must be configured to deliver data logs to an email address. For more information, refer to [Email Export](#), page 136.

Summary Device Pages

The summary device view provides the summary of the circuit breaker connected to the IFE interface.

Step	Action	Result
1	From the Monitoring menu, click Device Logging .	Displays the available device logging choices.
2	Under Device Logging , click Summary Device Page .	–
3	Under Summary Device Pages , click Single Topic , Multiple Devices .	Opens the setup page for selecting the device and topics.
4	Select the device from the Available Devices list.	Displays the available topics for the selected device.
5	Select a topic from the Available Topics list.	Displays the selected topic for the selected device.
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 the keyboard, or double-click the graph.	The view zooms out.
8	Repeat steps 3 through 7 to display other topics of the selected device.	Displays the selected topic for the selected device.

The topic logged from the selected 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, and last full month.

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	152
Set Device Time	155

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 interface.

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:

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

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

Control	Operation	Availability
Breaker/Switch disconnecter (BCM-OF/SD)	Open/Close/Reset	ComPacT NSX or PowerPacT H-, J-, and L-frame circuit breaker with BSCM
	Open/Close	<ul style="list-style-type: none"> • MasterPacT NT/NW, ComPacT NS, or PowerPacT P- and R-frame circuit breakers with BCM ULP • MasterPacT MTZ circuit breaker with MicroLogic control units
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 Interface

Perform the following procedure to enable the **Application Control** feature in IFE interface.

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

Step	Action	Result
1	Press the test button on the front face of the IFE interface 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 interface 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 logs in 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: <i>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.</i> 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/Rest	ComPacT NSX or PowerPacT H-, J-, and L-frame circuit breakers with BSCM
		Open/Close	<ul style="list-style-type: none"> MasterPacT NT/NW, ComPacT NS, or PowerPacT P- and R-frame circuit breakers or switch disconnecter with BCM ULP MasterPacT MTZ circuit breaker with MicroLogic control units

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 EcoStruxure Power Commission 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 circuit breaker connected to the IFE interface to IFE interface date and time. The time is set automatically. This page is used to get the circuit breaker time.

List of Parameters in Set Device Time

Parameter	Description
Device Selection	Allows you to select the circuit breaker that is to be synchronized with IFE interface date and time.
Localized Time	Displays the time of the circuit breaker.
Status	Displays the status of the circuit breaker.
Get Time	Allows you to get the time of the circuit breaker.
Set Device Time	Not applicable.

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 circuit breaker from the Set Device Time page and then click Get Time .	The date and time of the circuit breaker gets synchronized with the IFE interface date and time, and the status is updated as successful. NOTE: If the circuit breaker fails to synchronize with IFE interface date and time, then the status is updated as unsuccessful.

Diagnostics Webpages

What's in This Chapter

Statistics.....	157
Device Identification	160
IMU Information	161
Read Device Registers	162
Communication Check.....	163
IO Readings.....	164

Statistics

Description

The **Statistics** page shows the readings accumulated since the IFE interface was last activated. If the power to the IFE interface 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 interface 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: <ul style="list-style-type: none"> • Nominal • Degraded • Out of service
Boot Memory	Healthiness of the boot memory

Statistic	Description
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	<p>The following is the status of synchronization with SNTP:</p> <ul style="list-style-type: none"> • 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 device 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)

Statistic	Description
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 interface disk size in kilobytes
Used Size	Total amount of used disk size on the IFE interface disk in kilobytes
Free Size	Total amount of unused disk space on the IFE interface disk in kilobytes
Bad Size	Amount of corrupted disk space on the IFE interface 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 interface
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 connected to the ULP port of the IFE interface. 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

Read device registers allows the IFE interface to read Modbus registers from the devices connected to the ULP port of the IFE interface.

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 Interface Read Device Register Parameters

Parameter	Description	Settings
Device Name	Selects a device to read from the list of previously added devices.	–
Local ID	The address (local ID) of the device that is to be read.	1
Starting Register	Register number in decimal.	0–65535 Default setting: 1000
Number of Registers	The number of registers to read.	1–125 Default 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 interface. 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.	<ul style="list-style-type: none"> • Holding Registers (Default 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 (Default setting)

Communication Check

Automated Communication Check

While browsing the real-time data views, the IFE interface has an automated communication check that runs every 15 minutes by default. To change the timing, refer to [Preferences](#), page 139. This check verifies the communication health of all the devices configured on the IFE interface, 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 .	<p>Runs a communications check.</p> <p>The communicating device displays:</p> <ul style="list-style-type: none"> • Passed in the Communications column. • In Service in the Status column. <p>A device that is not communicating display:</p> <ul style="list-style-type: none"> • 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 the circuit breaker from IO Readings submenu.	Opens the IO Readings page for the circuit breaker.

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	<ul style="list-style-type: none"> • 1 • 0
Force/Unforce	Displays the six digital inputs and three digital outputs are forced or unforced	<ul style="list-style-type: none"> • UNFORCED • FORCED

Maintenance Webpages

What's in This Chapter

Indicators..... 165

Indicators

Description

The **Indicators** page provides the maintenance counter information for the circuit breaker connected to the IFE interface. 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 circuit breaker 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.

Appendices

What's in This Part

Appendix A - List of IFE Interface Supported Devices.....	167
---	-----

Appendix A - List of IFE Interface Supported Devices

What's in This Chapter

List of IFE Interface Supported Device Types 167

List of IFE Interface Supported Device Types

IFE Interface Supported Devices

Device Group	List of devices supported by IFE interface with Firmware 005 and more	List of devices supported by IFE interface with Firmware up to 003
MasterPacT MTZ circuit breaker with MicroLogic X control units	MicroLogic X	MicroLogic X
	MicroLogic Xi	MicroLogic Xi
MasterPacT MTZ circuit breaker with MicroLogic Active control units	MicroLogic Active A	Not supported
	MicroLogic Active E	Not supported
	MicroLogic Active AP	Not supported
	MicroLogic Active Ai	Not supported
	MicroLogic Active EP	Not supported
	MicroLogic Active Ei	Not supported
BCIM	Not supported	
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
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
Non-communicating MasterPacT NT/NW, ComPacT NS, and PowerPacT P- and R-frame circuit breakers and switch disconnectors	BCM-OF/SD	BCM-OF/SD
ComPacT NSX and PowerPacT H-, J-, and L-frame circuit breakers and switch disconnectors	ComPacT NSX - A	ComPacT NSX - A
	ComPacT NSX - E	ComPacT NSX - E
	PowerPacT - A	PowerPacT - A
	PowerPacT - E	PowerPacT - E
Non-communicating ComPacT NSX and PowerPacT H-, J-, and L-frame circuit breakers and switch disconnectors	BSCM-OF/SD BSCM Modbus SL/UPLP-OF/SD	BSCM-OF/SD
Others	BCPM A/E	BCPM A/E
	BCPM B	BCPM B
	BCPM C	BCPM C

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

www.se.com

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

© 2026 Schneider Electric. All rights reserved.

DOCA0142EN-12