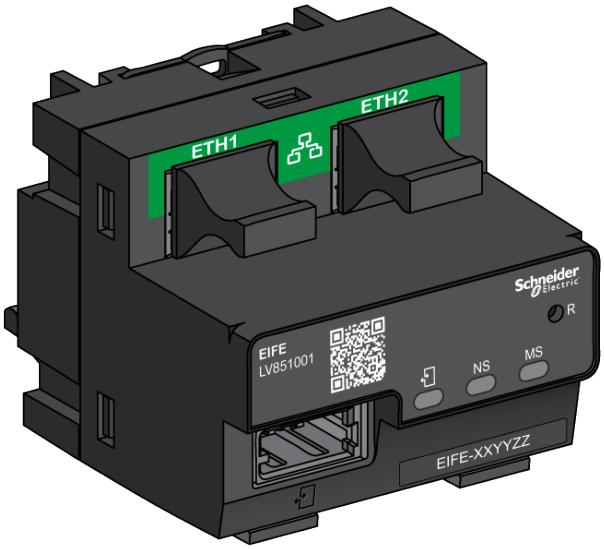
Enerlin’X EIFE

Embedded Ethernet Interface for One MasterPacT MTZ Drawout Circuit Breaker

User Guide

DOCA0106EN-15
10/2025



www.se.com

Legal Information

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

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

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

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

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

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

Table of Contents

Safety Information

Important Information

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

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

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

Please Note

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

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

About the Document

Document Scope

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 EIFE Embedded Ethernet interface for MasterPacT™ MTZ drawout circuit breakers.

Validity Note

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

- MasterPacT MTZ circuit breakers with MicroLogic X control unit
- MasterPacT MTZ circuit breakers with MicroLogic Active control unit

Online Information

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

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

General Cybersecurity Information

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

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

Schneider Electric provides additional information and assistance:

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

Product Related Cybersecurity Information

⚠WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- 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 (DOCA0106EN), original language
- Spanish (DOCA0106ES)
- French (DOCA0106FR)
- Chinese (DOCA0106ZH)

Related Documents

Title of the Documentation	Reference Number
Enerlin'X EIFE – Embedded Ethernet Interface for One MasterPacT MTZ Drawout Circuit Breaker – Instruction Sheet	NVE23550
Enerlin'X IFE/EIFE - Ethernet Interface - Firmware Release Notes	DOCA0147EN
ULP (Universal Logic Plug) System - User Guide	DOCA0093EN DOCA0093ES DOCA0093FR DOCA0093ZH
MasterPacT, ComPacT, PowerPacT Circuit Breakers - Modbus Communication - User Guide	DOCA0384EN DOCA0384ES DOCA0384FR DOCA0384ZH
MasterPacT MTZ - MicroLogic X Control Unit - User Guide	DOCA0102EN DOCA0102ES DOCA0102FR DOCA0102ZH

Title of the Documentation	Reference Number
MasterPacT MTZ - MicroLogic Active Control Unit - User Guide	DOCA0265EN DOCA0265ES DOCA0265ZH
Breaker Communication and Isolation Module (BCIM) for MicroLogic Active Control Unit - User Guide	DOCA0387EN DOCA0387ES DOCA0387ZH
MasterPacT MTZ Circuit Breakers with MicroLogic X Control Units - IEC 61850 Communication Guide	DOCA0162EN DOCA0162ES DOCA0162FR DOCA0162ZH
CET850 IEC 61850 Configuration Software – User Manual	SEPED306025EN
Enerlin'X IO - Input/Output Application Module for One Circuit Breaker - User Guide	DOCA0055EN DOCA0055ES DOCA0055FR DOCA0055ZH
MasterPacT, ComPacT, PowerPacT - Cybersecurity Guide	DOCA0122EN DOCA0122ES DOCA0122FR DOCA0122ZH
EcoStruxure Cybersecurity Admin Expert Guide	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.

EIFE Interface Presentation

What's in This Part

Introduction

Overview

The EIFE embedded Ethernet interface for one MasterPacT MTZ drawout circuit breaker (or EIFE interface) enables one MasterPacT MTZ drawout circuit breaker to be connected to an Ethernet network.

The EIFE interface provides digital access to the data delivered by the MicroLogic X or MicroLogic Active control unit of the MasterPacT MTZ circuit breaker. It provides information about the Intelligent Modular Unit (IMU) system.

> **NOTE:** The EIFE interface is only compatible with the MasterPacT MTZ drawout circuit breaker with MicroLogic Active control unit and BCIM module.
>
> For more information, refer to the DOCA0387•• *Breaker Communication and Isolation Module (BCIM) for MicroLogic Active Control Unit - User Guide*, page 7.

The EIFE interface monitors the three positions of the circuit breaker when inserted in its cradle:

- Cradle connected
- Cradle disconnected
- Cradle test position

EIFE Interface Features

The main features of EIFE interface are:

- Dual 10/100 Mbps Ethernet port for simple daisy chain connection
- Device profile web service for discovery of the EIFE interface on the local area network (LAN)
- Ethernet interface for MasterPacT MTZ drawout circuit breakers with MicroLogic Active or MicroLogic X control units
- Embedded settings webpages
- Embedded monitoring and control webpages
- Embedded diagnostics webpages
- Embedded security webpages
- Cradle status management (CE, CD, and CT)
- Built-in email alarm notification
- IEC 61850 interface for MasterPacT MTZ drawout circuit breakers with MicroLogic X control units
- Machine-to-Machine (M2M) communication
- Role-Based Access Control (RBAC) for users accessing the webpages

EIFE Webpage Sessions

Maximum of 8 HTTP sessions are supported. Once the HTTPS is enabled, only 4 HTTPS sessions are supported at the same time.

EIFE Interface Firmware Versions

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

- EIFE Interface Webpages from Firmware Version 005, page 36, describes the EIFE interface webpages for the firmware version 005 and later.
- EIFE Interface Webpages up to Firmware Version 003, page 92, describes the EIFE interface webpages for the firmware versions up to 003.

EIFE Interface Supported Protocols

The EIFE interface supports the following Ethernet protocols:

- **Modbus TCP/IP:** Modbus TCP/IP is a protocol, which provides client/server communication between devices and Modbus TCP/IP that provides communications over an Ethernet connection. Modbus TCP/IP is used to exchange data between EIFE 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 EIFE 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 EIFE 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 EIFE interface. It provides web server functionality through TCP port 443.
- **File Transfer Protocol (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 EIFE interface.

  NOTE: For EIFE 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 Intelligent Electronic Devices (IEDs). These systems 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 EIFE interface firmware version higher than version 005.000.000.

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

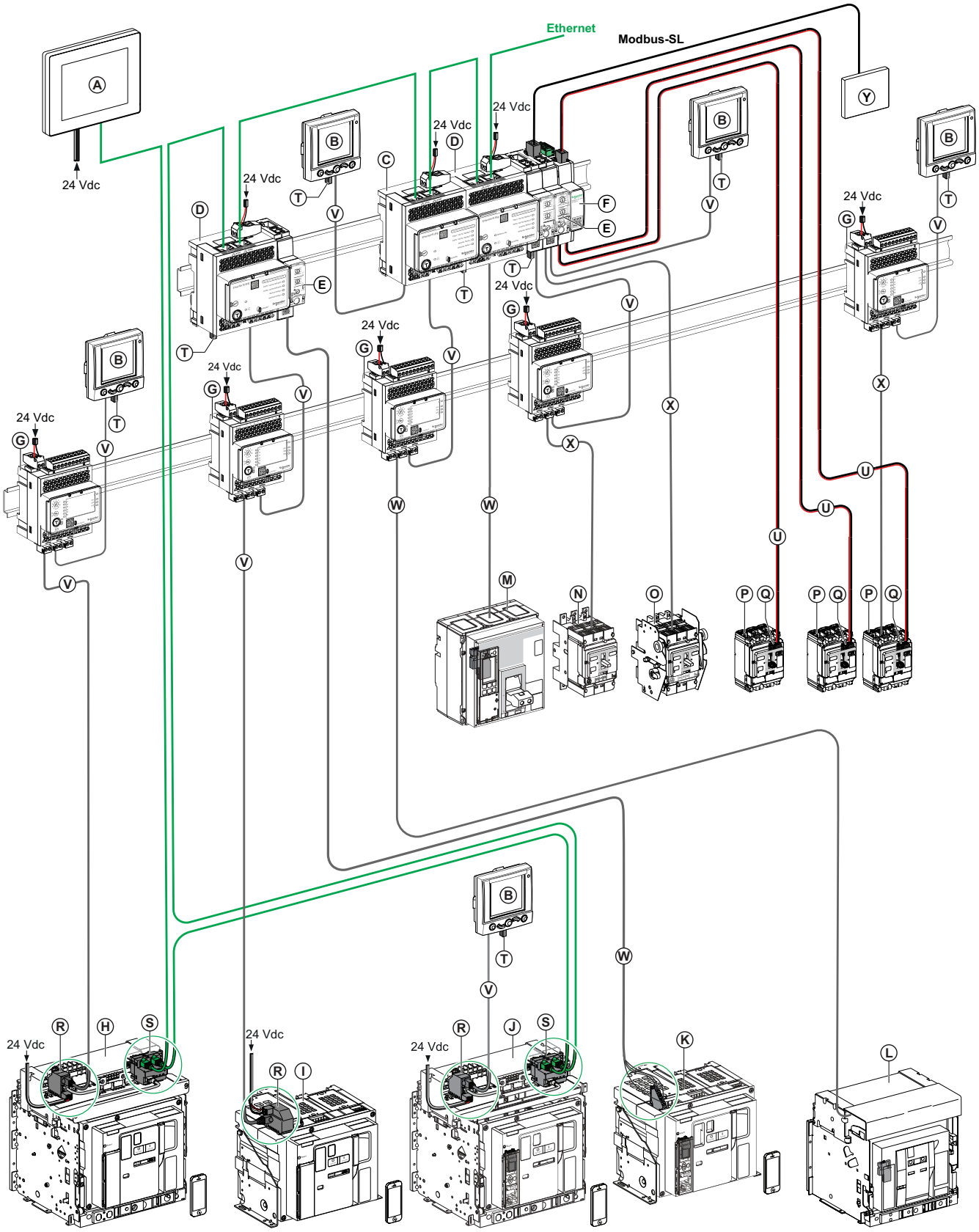
The following table lists the compatible ULP modules for each range of circuit breakers.

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

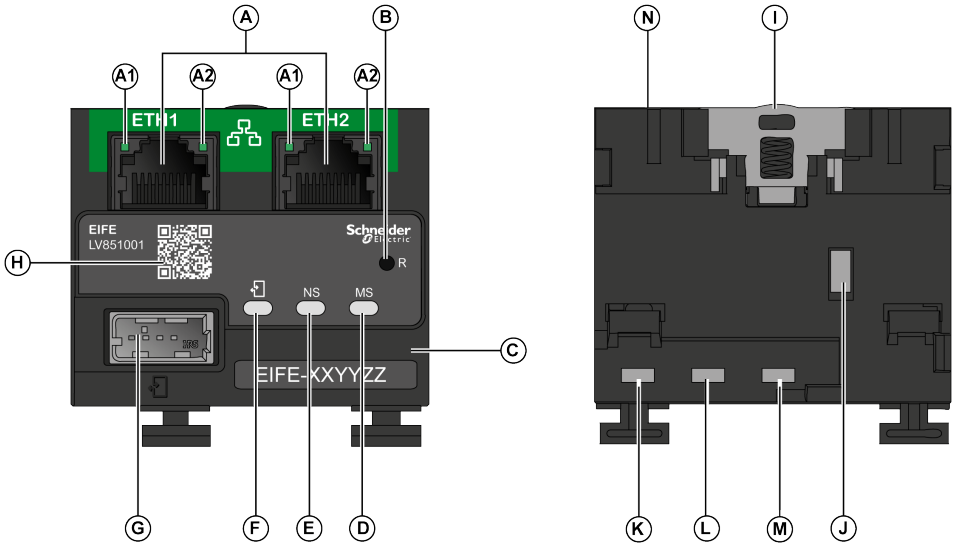
Remote Controller

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 Two RJ45 Ethernet ports

A1 OFF: 10 Mbps

Steady green: 100 Mbps

A2 Steady green: link

Blinking green: activity

B Reset button

C Device identification label

D Module status LED

E Network status LED

F ULP status LED

G USB mode ULP port

H QR code to product information

I DIN clip

J Grounding connection

K CT limit switch

L CE limit switch

M CD limit switch

N MAC ID

For information on installation, refer to the instruction sheet – NVE23550.

Mounting

The EIFE interface is embedded in the cradle of the MasterPacT MTZ circuit breaker.

Power Supply

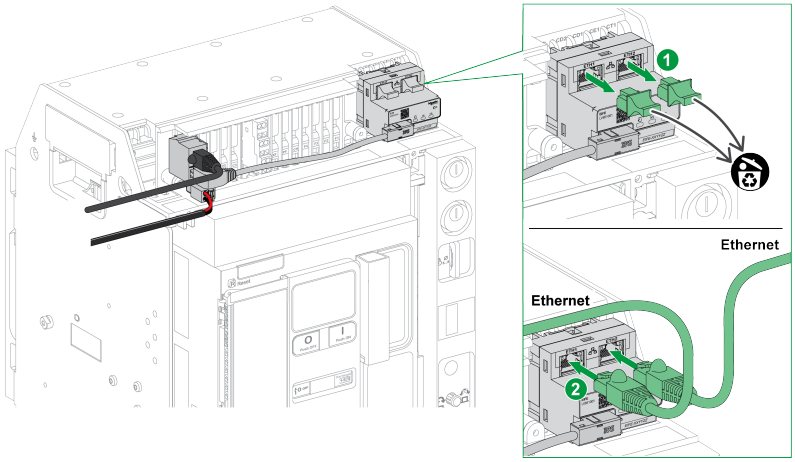
The EIFE interface is powered by the ULP port module.

For more information, refer to *ULP System User Guides* in Related Documents, page 7.

It is recommended to use an UL listed and 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.

Ethernet Connection



Module Status LED

The module status dual color LED, indicates the EIFE interface status.

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

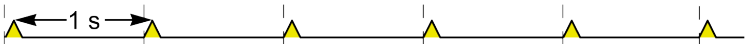
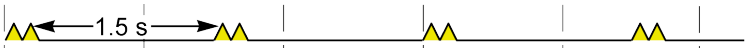
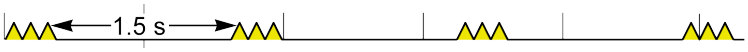
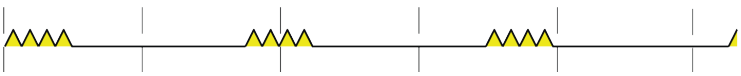
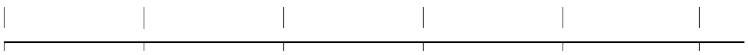
Network Status LED

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 detected in IP configuration

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 EIFE interface at the next maintenance operation
	Test	None
	Non-critical firmware discrepancy	Use the 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 the EcoStruxure Power Commission software to check the firmware and hardware compatibility and follow the recommended actions
	Critical hardware discrepancy	
	Stop	Replace EIFE interface
	Power OFF	Check power supply

Modbus Address

The EIFE interface accepts the Modbus address of the IMU to which it is connected. The Modbus address is 255 and cannot be changed.

Intrusive Command Mode

The EIFE interface intrusive command mode can be configured with EcoStruxure Power Commission software. This software can enable or disable the ability to send the remote control commands over the Ethernet network to the EIFE interface, and to the other modules of the connected IMU.

- If the intrusive command mode is Locked, the remote control commands are disabled.
- If the intrusive command mode is Unlocked (default setting), the remote control commands are enabled.

  NOTE: Whatever is the intrusive command mode, the only remote control command that is always enabled is the **Set Absolute Time** command.

Reset Button

The **Reset** button has three functions, according to the duration of the button pressed.

Time Range	Function
1 s	Resets the IP acquisition mode to its default setting (DHCP).
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 EIFE interface to its factory default settings.

Security Administrator Password Reset

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

1. Press the reset button (**R**) on the EIFE interface for 5 s. 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 reset button (**R**), the EIFE 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 reset button (**R**) on the EIFE 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.

EIFE Interface Factory Reset

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

1. Press the reset button (**R**) on the EIFE interface for 10 s. The LED will rapidly flash in red with a 100 millisecond ON and 100 ms OFF interval.

2. On releasing the reset button (**R**), the EIFE 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 reset button (**R**) on the EIFE interface to confirm or wait for 30 s to cancel the reset.
4. Once the reset to factory default settings is confirmed, the EIFE interface reboots and all the device settings are reset to their factory default values.

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

Parameter	Default Value
Date & Time	• Date and time setting mode: Manual • Date: yyyy-mm-dd • Time: hh:mm:sec
NTP	• NTP server setting mode: Manual • Primary SNTP: time.windows.com • Secondary SNTP: time.nist.com
Time zone	• Time zone offset :UTC • Day light saving: Disabled
Preferences	• Real time sample rate : 5 s • Communications check rate: 15 min
Ethernet	Frame format: Auto
	Port control • ETH1 mode: Auto-negotiation • ETH2 mode: Auto-negotiation
	Broadcast storm protection • Enable: Enabled • Level: Medium-Low • Committed information rate: 4000 s
IP configuration	**IPv4** • 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 • Enable IPv6: Enabled • IPv6 address: Unavailable
	DNS • DNS address: Automatic
Email service	Email service: Disabled
Data publishing	Logging interval: Disabled
RSTP	RSTP: Disabled
SNMP	SNMPV1 agent: Disabled
Devices	• 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	• Modbus TCP: Enabled • Secure commissioning: Disabled • Secure Modbus for M2M: Disabled • FTPS server: Disabled

Parameter	Default Value
	• Discovery: Enabled • HTTP/Web: Disabled • HTTPS: Enabled
Modbus TCP/IP filtering	• Modbus TCP/IP filtering: Disabled • IP filtering exception list cleared
Certificates	Certificate type: Self signed
User management	• User name: SecurityAdmin • Roles: SECADM, Viewer, Operator, Engineer, Installer • Password: AAAAAAAA
Syslog service	Syslog logging service: Disabled

Cradle Position Contacts

To identify the cradle position of the circuit breaker, the EIFE interface has three limit switches.

Limit Switch	Description
CE	Cradle connected position contact
CD	Cradle disconnected position contact
CT	Cradle test position contact

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.

The EcoStruxure Power Commission software enables the configuration of the MasterPacT MTZ devices with:

- MicroLogic X control unit
- MicroLogic Active control unit
- Communication interface modules such as IFE, EIFE, and IFM interfaces
- IO application modules
- M2C output module

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

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

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).

Cradle Management Function

Presentation

The cradle management function is used to:

- Record and check the position of drawout circuit breakers in the cradle.
- Provide information about the preventive maintenance actions.
- Notify the remote controller about the position of the drawout circuit breaker.

  NOTE: When the circuit breaker is detected as being in the disconnected position, the remote controller quits polling the MicroLogic control unit. If the remote controller does not quit polling, the remote controller receives the time-out response as long as the circuit breaker is disconnected.

The cradle information is available on:

- Remote controller using the communication network.
- EIFE interface webpages.

Compatible Devices

Range	Minimum Hardware Configuration Required
MasterPacT MTZ circuit breaker	• Drawout circuit breaker + MicroLogic X control unit + EIFE interface + ULP port module • Drawout circuit breaker + MicroLogic Active control unit + BCIM module + EIFE interface + ULP port module

Cradle Position Status

The cradle position status is defined by the position of the limit switches.

Cradle Position Status	CE Limit Switch	CT Limit Switch	CD Limit Switch
Cradle in connected position	ON	OFF	ON
Cradle in test position	OFF	ON	ON
Cradle in disconnected position	OFF	OFF	OFF

Cradle Position Counters

The cradle position counters are:

- Cradle connected position counter
- Cradle disconnected position counter
- Cradle test position counter

A counter is linked to each cradle position state. The counter is incremented each time the linked state is activated.

The cradle position counters have the following properties:

- Counters are saved in non-volatile memory to prevent loss of data in case of power outage.
- Counters are incremented from 0 to 65534.

Predefined Events

The following events are generated by the cradle management function.

Code	Description	Type	Priority	Reset
2304 (0x0900)	Cradle position discrepancy.	Alarm	Medium	Manual or remote
2308 (0x0904)	Disconnection of the circuit breaker from cradle is overdue.	Alarm	Medium	Manual or remote
2309 (0x0905)	Cradle has reached its maximum number of operations.	Alarm	High	Manual or remote
2310 (0x0906)	Remaining service life of cradle is below alarm threshold.	Alarm	Medium	Manual or remote
2311 (0x0907)	New MicroLogic control unit has been detected.	Alarm	High	Manual or remote

Cradle Position Discrepancy

The EIFE interface detects the cradle position discrepancy and generates an alarm when the cradle position contacts indicate that the circuit breaker is not in one of the allowable positions, connected, disconnected, or test.

Disconnection of the Circuit Breaker from Cradle is Overdue

The alarm is generated after 11 months without disconnecting the circuit breaker, to remind the user to operate the cradle at least once in every year by moving the circuit breaker from connected position to disconnected position and from disconnected position to connected position.

Recommended action: Disconnect the circuit breaker from cradle and connect it back.

Cradle Has Reached Its Maximum Number of Operations

The cradle is designed to connect 500 times and must be replaced before that number is reached. The alarm is generated when the cradle connected position counter reaches 450.

Recommended action: Plan to replace the cradle. Contact your local Schneider Electric service team for support.

Remaining Service Life of Cradle Is Below Alarm Threshold

Regrease the cradle and clusters. The cradle needs a comprehensive check-up when:

- Cradle is in operation for five years,
- Cradle position counter reaches 250.

Recommended action: Plan to replace the cradle. Contact your local Schneider Electric service team for support.

New MicroLogic Detection

A time-stamped alarm is generated when the EIFE interface detects that the MicroLogic control unit of the circuit breaker has been replaced. The detection is based on the MicroLogic control unit serial number.

Time-Stamped Information

The following time-stamped information is recorded:

- Last connection of the cradle
- Last disconnection of the cradle
- Last cradle in test position

The stamped information can be read by a remote controller using the communication network.

Technical Characteristics

Environmental Characteristics

Characteristics		Value
Conforming to standards		• IEC 60947-2 • IEC 61000-6-2 • IEC 61000-6-4
Certification		CE
Ambient temperature	Storage	-40 °C...+85 °C (-104 °F...+185 °F)
	Operation	-20 °C...+70 °C (-68 °F...+158 °F)
Relative humidity		5...85 %
Protective treatment		ULV0, conforming to IEC/EN 60068-2-30
Pollution		Level 3

Mechanical Characteristics

Characteristics	Value
Shock resistance	Same as MasterPacT MTZ circuit breakers.
Resistance to sinusoidal vibrations	Same as MasterPacT MTZ circuit breakers.

Electrical Characteristics

Characteristics		Value
Power supply		24 Vdc, -20%/+10% (19.2...26.4 Vdc)
Consumption		24 Vdc, 100 mA at 25 °C
Resistance to electrostatic discharge	Conforming to IEC/EN 61000-4-2	8 kV AD
Immunity to radiated fields	Conforming to IEC/EN 61000-4-3	10 V/m
Immunity to surges	Conforming to IEC/EN 61000-4-13	Class 2

Physical Characteristics

Characteristics	Value
Dimensions	51 x 51 x 52.5 mm (2.01 x 2.01 x 2.07 in)
Mounting	Embedded in the cradle of the circuit breaker
Weight	75 g (0.17 lb)
Degree of protection of the installed module	• Connectors: IP20 • Other parts: IP30
Connections	• RJ45 for Ethernet • Industrial USB type connector for ULP

Firmware Update

What's in This Chapter

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

- Firmware update to version 005 is recommended when all the features available in firmware version 004 are also available in firmware version 005.
- Firmware update to version 005 is not recommended when any of the features currently used by the application in firmware version 003 is not available in firmware version 005.

  NOTE: To use EIFE interface with MicroLogic Active control unit, you must update the EIFE interface firmware to version 005.003.000 or later.

Description

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

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

For more information on EIFE interface firmware versions, refer to the DOCA0147EN *Enerlin'X IFE/EIFE - Ethernet Interface - Firmware Release Notes*, page 7.

NOTICE

LOSS OF DATA

- Ensure that you take backup of the data log files before updating the firmware. The data log entries of the EIFE interface may be lost when the EIFE interface firmware is updated.
- Ensure that you take backup of data present in User Accounts and Email Events sections of EIFE webpages.
- Ensure that after firmware upgrade, you restore the User Accounts and Email Events configuration on EIFE 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.

Signed Firmware

All firmware designed for the *MasterPacT MTZ* IMU is signed using the Schneider Electric public key infrastructure.

The digital certificates used to authenticate genuine Schneider Electric firmware and software must be regularly verified to ensure that they are still valid. Digital certificates that are no longer valid are published on the certificate revocation list (CRL) available on the Schneider Electric Cybersecurity Support Portal.

NOTE: Each time you connect to the MicroLogic X or MicroLogic Active control unit using EcoStruxure Power Commission software, the digital signature of the control unit is automatically verified.

For more information on cybersecurity for the MasterPacT MTZ circuit breakers, refer to the *MasterPacT MTZ – Cybersecurity Guide* in Related Documents, page 7.

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

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

Recover EIFE Interface from Boot Mode

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

1. Connect EIFE 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 EIFE interface in boot mode.
4. Open the EcoStruxure Power Commission software.
5. Sign in to EcoStruxure Power Commission software.
6. Discover the EIFE interface, which is in the boot mode.

   NOTE: The current firmware version of EIFE interface is displayed as **EIFEBOOT**.
7. Initiate the firmware update process.

   After the firmware update, the EIFE interface reverts to its original IP address.
8. Restore the PC network settings.

Security Features

What’s in This Part

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 EIFE interface enables the protection of Modbus TCP communication by ensuring its confidentiality. When this feature is activated through the EIFE webpages, the communication between a Modbus TCP client and the EIFE interface is encrypted using the TLS protocol on port number 802. For information about enabling secure Modbus for M2M on the EIFE webpages, refer to IP Network Services Parameter, page 65.

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.

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

- EIFE interface 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 Parameter, page 65.

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 EIFE interface users.

The security administrator can manage the users of EIFE interface:

- On the EIFE interface webpages
- With the EcoStruxure Cybersecurity Admin Expert (CAE) software

EcoStruxure Cybersecurity Admin Expert Software

Cybersecurity Admin Expert (CAE) software is used for security configuration of the EIFE interface with firmware version 004.009.000 and later.

The security administrator can use CAE software to:

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

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

NOTE:

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

CAE Software Settings

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

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

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

CAE Device Specific Settings

The Device Specific Settings (DSS) is unique to the EIFE 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 EIFE interface while leaving it inactive on others.

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

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

Permission for Each Role

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

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

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

Permission	Roles				
	Viewer	**Engineer**	**Operator**	**Installer**	**Security Administrator**
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 EIFE 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 EIFE webpage. For more information, refer to Export to CSV, page 73.
- Configuring the Syslog parameters in the EIFE 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 73.

EIFE Interface Webpages from Firmware Version 005

What's in This Part

Webpage Access and User Interface

What's in This Chapter

Access to EIFE 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 EIFE Webpages

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

When the EIFE 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 EIFE 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 local area network (LAN) and switch off Wi-Fi.
2	Connect an Ethernet cable from the computer to the EIFE interface or to the Ethernet switch inside the panel.
3	Open File Explorer.
4	Click **Network** and the EIFE-**XXYYZZ** appears in the list of devices. **NOTE:** If the EIFE interface name is not displayed in the list of devices in File Explorer, check if the PC and the EIFE interface are not connected through the router.
5	Double-click the selected EIFE-**XXYYZZ**, the login page automatically opens in the browser. **NOTE:** Default browser must be Microsoft Edge.
6	Enter `SecurityAdmin` as the user name and `AAAAAAAA` as the password, the home page automatically opens in the browser. **NOTE:** The user name and password are case-sensitive.
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 EIFE-XXYYZZ, click **Device Location** on the header. The ULP LED of the selected EIFE-XXYYZZ blinks for 15 seconds (test mode).

Step	Action
11	To name the EIFE-**XXYYZZ**, select the **SETTINGS** menu, go to **DEVICES** submenu, enter the device name and click **Apply Changes.**
12	Write the EIFE 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

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

Step	Action
1	Connect the EIFE interface or the Ethernet switch inside the panel to the local area network (LAN).
2	Connect the computer to the local area network (LAN).
3	Open File Explorer.
4	Click **Network**, the EIFE interface name is displayed in the list of devices. **NOTE:** If the EIFE interface name is not displayed in the list of devices in File Explorer, check if the PC and the EIFE interface are not connected through the router.
5	Double-click the EIFE interface name which is written on the device label located on the front face of the selected EIFE 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 EIFE interface or the Ethernet switch inside the panel to the local area network (LAN).
2	Connect the computer to the local area network (LAN).
3	Start the web browser, page 38.
4	In the address text box, enter the EIFE interface name which is written on the device label located on the front face of the selected EIFE interface.
5	Press **Enter**, the login page automatically opens in the browser. **NOTE:** If the EIFE interface does not appear in the list of devices in File Explorer, check if the PC and the EIFE interface are not connected through the router.

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

IP Address Browsing

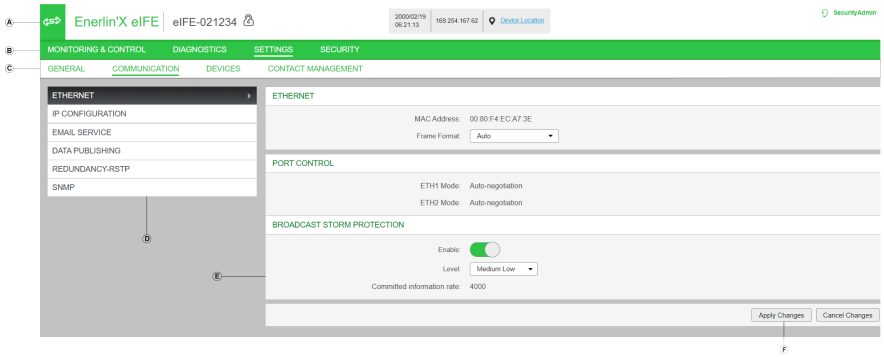
IP static configuration has to be set.

Step	Action
1	Connect the EIFE interface or the Ethernet switch inside the panel to the local area network (LAN).
2	Connect the computer to the local area network (LAN).
3	Start the web browser, page 38.
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 EIFE webpage user interface layout.



A Header

B Menu bar

C Submenu bar

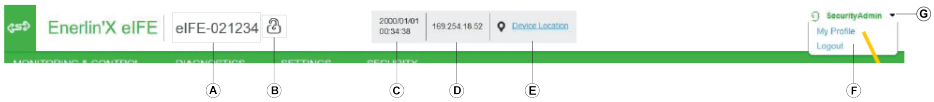
D Webpages

E Display zone

F Action button

Header

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



A EIFE 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
EIFE interface name	Device name of the EIFE interface.
Intrusive command mode , page 20	• : 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.

Header Part	Description
Device Location	Click **Device Location** to locate the selected interface in your equipment: • 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 EIFE webpage session, or close your browser. It is recommended to log out from the EIFE 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 Buttons

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

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

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

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

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

Display Zone

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

Webpage Description

MONITORING & CONTROL Webpage

Submenu	Webpage	Description
CIRCUIT BREAKERS, page 75	–	• 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 79	-	• Displays data from the IO modules. • Allows you to control the IO modules. • Displays Input/Output configuration for IO modules connected to the EIFE interface.

DIAGNOSTICS Webpage

Submenu	Webpage	Description
COMMUNICATION	**STATUS**, page 81	Displays diagnostic data used to troubleshoot the network-related problems.
	ETHERNET, page 82	Displays the diagnostic data of Ethernet global statistics and Ethernet port characteristics.
	MODBUS, page 83	Displays the global statistics of TCP/IP and TCP port connections.
	ULP, page 84	Displays the global statistics of ULP port connection.
	REDUNDANCY-RSTP BRIDGE, page 85	Displays the diagnostic data of RSTP bridge.
	REDUNDANCY-RSTP PORTS, page 86	Displays the diagnostic data of RSTP ports.
	SNMP, page 87	Displays the diagnostic data of SNMPV1 Agent.
	Read Device Registers, page 88	Displays register data connected locally to the EIFE interface.
EIFE, page 89	–	• Displays the EIFE interface basic information. • Displays the EIFE interface parameters and characteristics.
DEVICES	**CIRCUIT BREAKERS**, page 91	• 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 **COMMUNICATION**	**DATE & TIME**, page 46	Sets the date and time manually or sets the EIFE interface time automatically using an NTP source or configures the device connected to EIFE interface to synchronize their time with the EIFE interface time automatically.
	TIME ZONE, page 47	Sets the time zone for the region and sets the daylight saving time.
	ETHERNET, page 49	Sets the Modbus TCP/IP communication interface.
	IP CONFIGURATION, page 51	Sets the IP parameters.
	EMAIL SERVICE, page 53	Sets the configuration of SMTP server for mailing purpose.
	DATA PUBLISHING, page 55	Sets data generation and publishing parameters.

Submenu	Webpage	Description
	REDUNDANCY-RSTP, page 56	Sets the RSTP bridge and RSTP port details.
	SNMP, page 58	Sets the SNMPV1 agent parameters.
DEVICES, page 60	-	• Sets the EIFE interface name. • Sets circuit breaker name and data logging.
CONTACT MANAGEMENT	**EMAILS**, page 63	• 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 65	-	Configures the settings and activates the IP network services.
MODBUS TCP/IP FILTERING, page 66	-	Configures the IP addresses that can access the EIFE interface through Modbus TCP/IP.
CERTIFICATES, page 68	-	Displays the EIFE interface certificate with expiration date and validity period.
USER MANAGEMENT, page 70	-	Manages the existing and newly added user accounts.
SYSLOG SERVICE, page 73	-	Configures the Syslog server address.

Settings Pages

What's in This Chapter

Date and Time

Description

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

- Manually set the date and time of the MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.
- Automatically synchronize the date and time of the MasterPacT MTZ drawout circuit breaker to the EIFE 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 MasterPacT MTZ drawout circuit breaker and its IMU devices: • Check **Manual** (default setting) to set manually the date and time in the dedicated fields. • Check **Network Synchronization via NTP** to set automatically the date and time by an external time server (NTP server).
Date	Allows you to set the present date manually in the format yyyy-mm-dd.
Time	Allows you to set the present time manually in the format hh:mm:sec.

NTP Settings

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

NOTE:

- When both the NTP servers are not reachable by EIFE interface and another IMU device is setting the date and time, the EIFE 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**.

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 EIFE 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 pop-up message is displayed for confirmation to restart the interface to apply the new settings:

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

Navigation to the Ethernet Page

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

Ethernet Settings

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

Port Control Settings

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

Broadcast Storm Protection Settings

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

IP Configuration

Description

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

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

Navigation to the IP Configuration Page

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

IPv4 Settings

Parameter	Description
Configuration	Allows you to select the IPv4 configuration mode: • Check **Automatic** (default setting) to set IPv4 parameters automatically by using **DHCP** or **BOOTP**. • Check **Manual** to set manually the IPv4 parameters (IP address, Subnet mask, and Gateway).
Mode	Allows you to select the mode for assigning the IPv4 parameters by using: • DHCP (default setting) • BOOTP **NOTE:** While using a legacy DHCP server, the device name must be limited to 16 characters.
IP address	Used to enter manually the static IP address of an EIFE 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 pop-up message is displayed for confirmation to restart the interface to apply the new settings:

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

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

DNS Settings

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

Email Service

Description

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

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

Navigation to the Email Service Page

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

Email Service

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

Email SMTP Server Settings

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

Email Sender Address Settings

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

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

- Use the **From Address** as a context provider: If you do not want to receive any reply, and only notify the recipient, use **From Address** as contextual information. The **From Address** syntax includes “no-reply”, “device name”, “site name”, @a validated domain.com, .net, and so on.
- Create an alias in the **From Address** to allow replies to be sent to the person in charge of an alarm: An email can be sent to multiple people who are responsible for a specific appliance. This feature allows the receivers to reply to follow up with the responsible person.

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

Email Language Settings

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

Email Test Settings

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

The **Email Test** feature enables connection from the EIFE interface to the service.

Click the **Test** button 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 EIFE 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, ÿ, and ç are not shown correctly in the email. However, the generic text message is shown correctly.

Data Publishing

Description

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

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

Navigation to the Data Publishing Page

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

Data Generation Setting

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

Data Publishing Settings

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

Manual Export

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

Redundancy-RSTP

Description

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

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

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

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

Navigation to the Redundancy-RSTP Page

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

RSTP Settings

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

RSTP Bridge Settings

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

RSTP Port 1 and 2 Settings

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

SNMP

Description

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

The EIFE interface supports SNMP, allowing a network administrator to access remotely an EIFE interface with an SNMP manager and to view the networking status and diagnostics of the EIFE 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.	• Setting range: 1...65534 • Default setting: 161
Notification Port	Allows you to enter notification port number.	• Setting range: 1...65534 • Default setting: 162

System Objects Settings

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

Community Names Settings

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

Enabled Traps Settings

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

Setting	Description
Cold Start Trap	Generates a trap when the EIFE 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 EIFE 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 EIFE interface to publish (24 data maximum).The way to publish the data is set on the **DATA PUBLISHING** page. For more information, refer to Data Publishing, page 55.

The device connected to the EIFE interface ULP port is automatically detected and added to the EIFE 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	Allows you to enter the EIFE interface name. **NOTE:** • The LV breaker system is uniquely identified over possible interfaces such as HMI, Modbus/TCP, DPWS, and DHCP. • EIFE interface name is common across all interfaces. Thus, changing EIFE interface name by any means has direct impact on all the connected interfaces.	The EIFE interface name can have up to 63 ASCII characters. The allowed characters are **A–Z**, **a–z**, **0–9**, and **-**. However, **-** is not allowed at the beginning or at the end of the name. **NOTE:** • EIFE interface name should be unique. • EIFE interface names for different devices may have impact on web applications, logging, and export features.
Device Type	Displays the device type. **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. **NOTE:** • 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.	The device name can have up to 45 ASCII characters. The allowed characters are **A–Z**, **a–z**, **0–9**, **Space**, and **-**. However, **Space** and **-** is not allowed at the beginning or at the end of the name.
IP Address/Server ID	Displays the device IP address and the local address of the device connected to the EIFE interface or remote device. • For EIFE 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	Allows you to enable the publication of data from the device connected to the EIFE interface (disabled by default). The data is selected to publish while **Data Publishing** is enabled.	There are eight categories for data publishing Default values: • Apparent Energy (kVAh) • Active Energy (kWh) • Reactive Energy (kVARh)
Select Data Publishing	Click **Select Data Publishing** to open the **Data Publishing** window, where you can select the data to publish.	–

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 EIFE interface.

A maximum of 24 data can be selected for publication, out of which the following 3 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 54
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. For more information, refer to Devices, page 60.

Notification Page

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

⚠CAUTION

EQUIPMENT INCOMPATIBILITY OR INOPERABLE EQUIPMENT

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

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

The list of events displayed contains only applicable events related to the MasterPacT MTZ circuit breaker:

- With MicroLogic X control unit and EIFE interface
- With MicroLogic Active control unit and EIFE interface
- With 1 or 2 optional IO modules connected to the ULP port module.

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

Security Pages

What's in This Chapter

IP Network Services

Description

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

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

Navigation to the IP Network Services Page

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

IP Network Services Parameters

Parameter	Description	Value
Modbus TCP	Allows you to enable/disable the Modbus/TCP service.	Default setting: Enabled
Secure Commissioning	Allows you to enable/disable the secure communication over TLS and then by RBAC mechanism between EcoStruxure Power Commission software and EIFE interface. **NOTE:** It is recommended to set it as Enabled. Once the secure commissioning is enabled, if EcoStruxure Power Commission software is connected to EIFE interface, user must start a new discovery of the EIFE interface with EcoStruxure Power Commission software.	Default setting: Disabled
	Allows you to set the port number of the secure commissioning server.	Setting range:1...65534 Default setting: 49152
Secure Modbus for M2M	Allows you to enable/disable the secure Modbus for machine-to-machine service. **NOTE:** Machine-to-Machine secure communication requires components that connect to the EIFE 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/disable the FTPS server.	Default setting: FTPS server is disabled
Discovery	Allows you to enable/disable the discovery (DPWS) of the EIFE 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/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 EIFE 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: • **Read only**: The following Modbus TCP/IP function codes are allowed: ◦ 1 (0x01) ◦ 2 (0x02) ◦ 3 (0x03) ◦ 4 (0x04) ◦ 7 (0x07) ◦ 8 (0x08) ◦ 11 (0x0B) ◦ 12 (0x0C) ◦ 17 (0x11) ◦ 20 (0x14) ◦ 24 (0x18) ◦ 43 (0x2B), with subfunction codes 14 (0x0E), 15 (0x0F), and 16 (0x10). ◦ 100 (0x64) • **None**: The access to the IP address is blocked. • **Read/Write**: Full access is provided.

IP Filtering Exception List Parameters

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

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

Certificates

Description

The **CERTIFICATE** page allows you to create, modify, and import the EIFE 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 EIFE 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** button 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 EIFE interface is Self-Signed.
Validity Period (UTC)	Validity period of the certificate. The certificate generated by the EIFE 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 by using the EcoStruxure Cybersecurity Admin Expert Software, page 32.

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, EIFE 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 new user. • User name is composed of 4 to 16 characters. • User names are case-sensitive and can contain special characters.
Password	Enter the password for the new user , page 71. The password entered must be confirmed.
Role	Select one or multiple roles for the new user in the predefined list of roles , page 32.
Email ID	Enter a valid email address for the entered user name.

User Account Edition

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

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

User Account Details

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

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

Password Syntax

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

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

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

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

Password Update

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** window.

Password Reset

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

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

The EIFE interface logs 2048 security events before the oldest events are over written by newer events.

Ensure the security logs are exported on a regular basis from the EIFE interface by:

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

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

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

Test Connection

Click the **Test Connection** button to verify the connection between the EIFE interface and Syslog server. During the test, the EIFE 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

Description

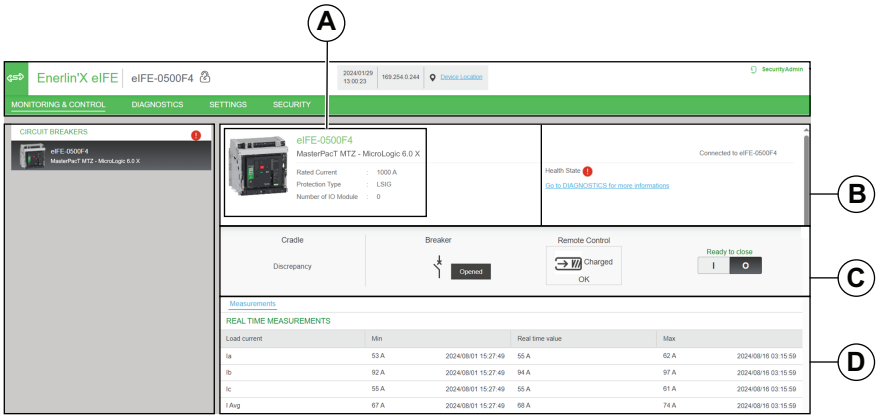
The **CIRCUIT BREAKERS** page allows you:

- 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 the Page

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

Page Layout



A Circuit breaker identification data

B Circuit breaker health status

C Circuit breaker monitoring and control panel

D Monitoring of measurements

Circuit Breaker Identification Data

The circuit breaker is identified by the following data:

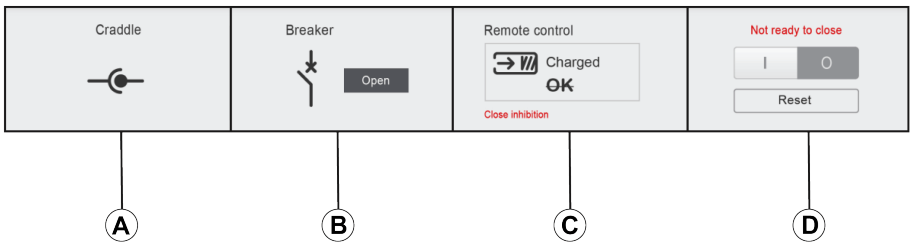
- Rated current
- Protection type
- Number of IO modules connected
- Additional data according to the range of the circuit breaker

Circuit Breaker Health Status

The health status of the MasterPacT MTZ drawout 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 buttons

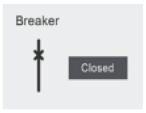
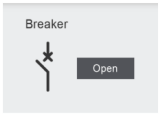
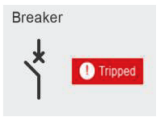
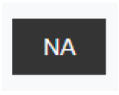
Drawout Circuit Breaker Position in the Cradle

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:

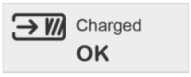
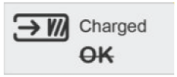
Icon	Description
	The main contacts of the circuit breaker are closed.
	The main contacts of the circuit breaker are opened.
	The main contacts of the circuit breaker are opened and the circuit breaker is tripped. The circuit breaker must be reset.
	The circuit breaker position is unknown in case of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

Circuit Breaker Control Mode

The circuit breaker control mode is:

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

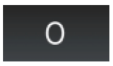
The circuit breaker control status is indicated by the following icons:

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 Buttons

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

Control Button	Description
	Click the button to open the circuit breaker.
	Click the button to close the circuit breaker. The circuit breaker will close only if it is ready to close.

For each control action:

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

  NOTE: The message in the dialog box 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 control unit of the circuit breaker.

Measurement are shown in the following order:

- Real time measurements with minimum and maximum values. For MasterPacT MTZ drawout 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.	• 1 • 0
Forced	Displays the six digital inputs and three digital outputs are forced or not.	• **FORCED** • –

Diagnostics Pages

What's in This Chapter

Status

Description

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

While browsing the real-time data views, the EIFE 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 EIFE 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 change 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 EIFE interface.
Device Type	Type of the device connected to EIFE interface.
Connection	Displays the connection type: Type 1: ULP
Communication	Status of communication: • Passed: EIFE interface successfully connected to the devices. • Failed: EIFE interface not connected to the devices.

Ethernet

Description

The **ETHERNET** page displays:

- Ethernet global statistics accumulated since the EIFE interface was last activated.
- Ethernet port characteristics.

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

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 EIFE 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 change the Diagnostics page settings.

Navigation to the Modbus Page

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

Global Statistics Parameters

Global Statistics	Parameter	Description
TCP/IP	**Frames Received**	Number of frames received
	Frames Transmitted	Number of frames transmitted
	Port Status	Status of the connected Ethernet port: • **Operational** • **Idle** If **MODBUS TCP/IP** is disabled, the Port Status value is displayed as **Idle**.
	Opened Connections	Number of active connections
Serial	**Frames Received**	Number of frames received
	Frames Transmitted	Number of frames transmitted
	Error Messages	Number of error messages
Click **Reset Counters** to reset the statistics values to 0. If the EIFE 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 change 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 change 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 EIFE 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 change 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:** The below points are provided for understanding the usage of port priority (port identifier). • Port that carries packets to root bridge is root port. When there are multiple such ports exist, one with least Port Identifier becomes the root port, and others will become alternate ports. • Port Number: Port number cannot be configured. In the device the port Number (interface number) for port-1 is 1 and port number for port-2 is 2.
Port Path Cost	The contribution of this port to the path cost of paths towards the Root bridge which includes this port.
Received RST (BPDUs)	Total number of RSTP BPDUs received by this port since the last reset counters.
Transmitted RST (BPDUs)	Total number of RSTP BPDUs transmitted by this port since the last reset counters.
Received TCN (BPDUs)	Total number of Topology Change BPDUs received by this port since the last reset counters.
Transmitted TCN (BPDUs)	Total number of Topology Change BPDUs transmitted by this port since the last reset counters.
Click **Reset Counters** to reset to 0 the statistics values. If the EIFE 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 change 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 EIFE 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.	• **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)

EIFE

Description

The EIFE page displays the information of the EIFE interface connected to the circuit breakers.

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

Navigation to the EIFE Page

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

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

System Parameters

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

EIFE Interface Operating Time Parameters

Statistic	Description
Operating Time	Operating time of EIFE interface

Devices

Description

The **DEVICES** page gives the information about the MicroLogic control unit connected to the ULP port of the EIFE interface.

NOTE: The users with installer or engineer roles can change 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.
Number of IO Module	Displays the number of IO modules connected to 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.

EIFE Interface Webpages up to Firmware Version 003

What's in This Part

NOTE: The information provided in this part is only applicable for EIFE interface connected to MasterPacT MTZ with MicroLogic X control unit.

Webpage Access and User Interface

What's in This Chapter

Access to EIFE 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 EIFE Webpages

The EIFE interface name must be configured during the first access to the EIFE 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 EIFE 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 EIFE interface or to the Ethernet switch inside the panel.
3	Open File Explorer.
4	Click **Network** and the EIFE-**XXYYZZ** appears in the list of devices. **NOTE:** If the EIFE interface name is not displayed in the list of devices in File Explorer, check if the PC and the EIFE interface are not connected through the router.
5	Double-click the selected EIFE-**XXYYZZ**, the login page automatically opens in the browser.
6	Enter `Administrator`as the user name and `Gateway` as the default password, the home page automatically opens in the browser. **NOTE:** The user name and password are case-sensitive. The *Administrator* user name cannot be changed as it is 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 *Administrator* user name.
8	To locate the EIFE-XXYYZZ, select the **Configuration & Settings** menu, go to **General** submenu, click **Device Physical Location**, and click **Blink ON**. The ULP LED of the selected EIFE-XXYYZZ blinks for 15 seconds (test mode).
9	To name the EIFE-**XXYYZZ**, select the **Configuration & Settings** menu, go to **Device Configuration** submenu, click **Device List** and then click **Name**. Click EIFE-**XXYYZZ** to set the EIFE interface name.
10	Write the EIFE 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

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

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

Name Browsing

DNS server is mandatory.

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

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

IP Address Browsing

IP static configuration has to be set.

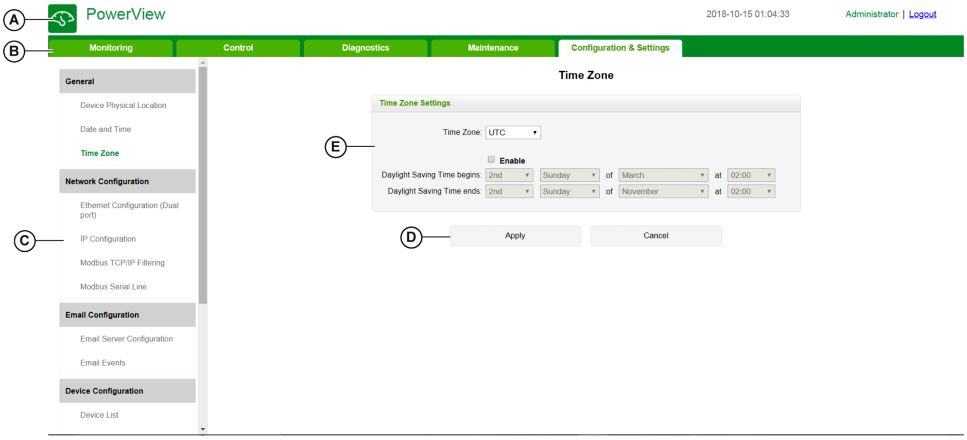
Step	Action
1	Connect the EIFE interface or the Ethernet switch inside the panel to the local area network (LAN).
2	Connect the PC to the local area network (LAN).

Step	Action
3	Start the web browser.
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 EIFE webpage user interface layout.



A Banner

B Menu tabs

C Subtabs

D Action button

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 EIFE webpage session, click **Logout** or close your browser. It is recommended to log out from the EIFE 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 Buttons

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

The following table describes the interface buttons:

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

Display Zone

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

Webpage Description

Monitoring Webpage

Monitoring Submenu	Webpage	Description
Real Time Data	**Single Device Pages**, page 130	The single device pages provide basic readings of the MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.
	Summary Device Pages, page 130	The summary device pages provide summaries of the MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.
	Trending, page 130	The trending page view provides real-time graphic and table trending of the MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.
Device Logging	**Single Device Pages**, page 132	The single device pages provide the graphic and table trending logs of user-selectable quantities for the MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.
	Summary Device Pages, page 134	The summary device pages provide graphic trending logs of MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.

Control Webpage

Control Submenu	Webpage	Description
Device Control	**Device Control**, page 137	Resets and controls the MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.
Set Device Time	**Set Device Time**, page 139	Displays the time of the MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.

Diagnostics Webpage

Diagnostics Submenu	Webpage	Description
General	**Statistics**, page 141	Displays diagnostic data used to troubleshoot the network-related problems.
Product Information	**Device Identification**, page 144	• Displays the EIFE interface basic information to set the EIFE 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 145	Displays the list of the IMU devices connected to the ULP port.
Device Health Check	**Read Device Registers**, page 146	Displays register data connected locally to the EIFE interface.
	Communications Check, page 147	Verifies the communication health of the MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.
IO Readings	**IO Readings**, page 148	Displays the status of IO module connected to the MasterPacT MTZ drawout circuit breaker. Displays **No IO modules connected** if the MasterPacT MTZ drawout circuit breaker is not connected to a IO module. **NOTE: IO Module** refers to the MasterPacT MTZ drawout circuit breaker name defined in the **Device List** page.

Maintenance Webpage

Maintenance Submenu	Webpage	Description
Indicators	**Indicators**, page 149	Displays the maintenance counters of the MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.

Configuration & Settings Webpage

Configuration & Settings Submenu	Webpage	Description
General	**Device Physical Location**, page 102	• Locate the EIFE-XXYYZZ interface. • Click **Blink ON**. • The ULP LED of the EIFE-XXYYZZ interface blinks and is active for 15 s (Test mode: 1 s ON, 1 s OFF).
	Date and Time, page 103	Sets the date and time manually or sets the EIFE interface time automatically using an SNTP source or configures the ULP devices connected to EIFE interface to synchronize their time with the EIFE interface time automatically.
	Time Zone, page 104	Configures the time zone for the region and sets the daylight saving time.
Network Configuration	**Ethernet Configuration (Dual port)**, page 105	Configures the Ethernet.
	IP Configuration, page 106	Configures the IP parameters.
	Modbus TCP/IP Filtering, page 107	Configures the maximum number of Modbus TCP/IP server connections. Configures the IP addresses that can access the EIFE interface through Modbus TCP/IP.
Email Configuration	**Email Server Configuration**, page 108	Configures the alarms to be emailed. Configures the SMTP parameter for mailing purpose.
	Email Events , page 110	Configures the alarms to be sent through email.
Device Configuration	**Device List**, page 118	Configures MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.
	Device Logging, page 119	Configures device logging parameters.
	Device Log Export, page 121	Configures device logging export options.
Other Configuration	**SNMP Parameters**, page 123	Configures Simple Network Management Protocol (SNMP).
	Preferences, page 124	Configures EIFE interface preferences.
	Advanced Services Control, page 125	Configures the advanced service control parameters.
	User Account, page 126	Creates and edits groups and users. Configures email accounts.
	Webpage Access, page 128	Configures webpage access rights for each user group.

Configuration & Settings Webpages

What's in This Chapter

General

Device Physical Location

Step	Action	Result
1	From the EIFE webpage menu bar, click **Configuration & Settings**.	Opens the **Configuration & Settings** menu.
2	From the **Configuration & Settings** menu, in the **General** submenu, click **Device Physical Location**.	Opens the **Device Physical Location** page.
3	In **Device Physical Location** webpage, click **Blink ON**.	Sets the EIFE 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 MasterPacT MTZ drawout circuit breaker connected to the EIFE interface
- To automatically synchronize the date and time of the MasterPacT MTZ drawout circuit breaker to the EIFE 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 MasterPacT MTZ drawout circuit breaker. This option is disabled when **Automatic** 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:sec.
Automatic (SNTP)	Allows you to enable the automatic time setting of the MasterPacT MTZ drawout circuit breaker. 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 MasterPacT MTZ drawout circuit breaker connected to the EIFE interface with the EIFE interface time.
Cancel	Allows you to clear the synchronization of the MasterPacT MTZ drawout circuit breaker connected to the EIFE interface.

Time Zone

Time Zone Configuration

Step	Action
1	From the EIFE webpage 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.

Ethernet Configuration (Dual Port)

Ethernet

Parameter	Description	Settings
MAC address	A unique media access control address of an EIFE interface. The MAC address is written on the label which is placed on the side of the EIFE 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.	• **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: • **1**: Highest (1000) • **2**: High (2000) • **3**: Medium-High (3000) • **4**: Medium-Low (4000), Default setting • **5**: Low (5000) • **6**: Lowest (6000) **NOTE:** The level value corresponds to the committed information rate.
Committed information rate	Defines the read-only value of the broadcast storm protection level.	–

IP Configuration

IPv4 Configuration

Parameter	Description	Settings
Obtain an IP address automatically using	Used to select the mode for assigning the IPv4 parameters set. Obtain IPv4 parameters automatically using BOOTP or DHCP. **NOTE:** While using a legacy DHCP server, the device name must be limited to 16 characters.	• **DHCP** (default setting) • **BOOTP**
Manual IP address	Used to enter the static IP address of an EIFE 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 EIFE 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.	–

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 EIFE 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.	• Enabled • Disabled (No filtering)
IP Address	Filters the required IP address entered by you.	10 addresses (Maximum allowed IP addresses)
Access level	Defines the access level for the corresponding IP address.	• Read: The following Modbus TCP/IP function codes are allowed: ◦ 1 (0x01) ◦ 2 (0x02) ◦ 3 (0x03) ◦ 4 (0x04) ◦ 7 (0x07) ◦ 8 (0x08) ◦ 11 (0x0B) ◦ 12 (0x0C) ◦ 17 (0x11) ◦ 20 (0x14) ◦ 24 (0x18) ◦ 43 (0x2B), with subfunction codes 14 (0x0E), 15 (0x0F), and 16 (0x10). ◦ 100 (0x64) • **None**: The access to the IP address is blocked. • **Read/Write**: Full access is provided.
Allow Anonymous IP	Allows all Modbus TCP/IP clients to have the read-only access.	• Enabled • Disabled (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 must 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 EIFE interface by default. If you have configured SMTP profile for the previous version of the EIFE 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.	• 25 (default setting) • 465: TLS • 587: STARTTLS
Authentication	If the SMTP server requires login information, enable the **Authentication Enable** check box.	• **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.	• **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 events displayed contain only applicable events related to the MasterPacT MTZ circuit breaker with:

- with MicroLogic X control unit and EIFE interface
- with 1 or 2 optional IO modules connected to the ULP port module.

  NOTE: If an email SMTP server is not located on the same Ethernet network segment as EIFE interface, ensure that the EIFE 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 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
	IDMTG Ig 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
	Overvoltage on all 3 phases start
	Overvoltage on all 3 phases operate
	Reverse Power start
	Reverse Power operate

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

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

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

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

Events from IO Modules

Device connected	Events
IO module 1	Threshold overrun on Input 1 counter (#1)
	Threshold overrun on Input 2 counter (#1)
	Threshold overrun on Input 3 counter (#1)
	Threshold overrun on Input 4 counter (#1)
	Threshold overrun on Input 5 counter (#1)
	Threshold overrun on Input 6 counter (#1)

Device connected	Events
	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	Discrepancy with ERMS orders
	Earth leakage trip signal contact (SDV) alarm
	Control voltage presence contact alarm
	Surge protection status contact alarm
	Surge failure contact alarm
	Switch disconnector ON/OFF indication alarm contact (OF)
	Fuse blown indication contact alarm
	Emergency Stop alarm
	Switchboard temperature contact alarm
	Switchboard ventilation contact alarm
	Switchboard door contact alarm

Events from EIFE Interface

Device connected	Events
EIFE interface	Disconnection of the circuit breaker from cradle is overdue
	Remaining service life of cradle is below alarm threshold
	Cradle has reached its maximum number of operations
	New MicroLogic unit has been detected
	Cradle Position Discrepancy
	Cradle connected position status (CE)
	Cradle disconnected position status (CD)
	Cradle test position status (CT)
	Cradle replacement within 6 month
	Regrease cradle to be performed
	Drawer Position Discrepancy
	Cradle Connected Contact Change
	Cradle Disconnected Contact Change
	Cradle Test Contact Change
	Password of service user profile for EIFE interface was changed
	Password of engineer user profile for EIFE interface was changed
	Password of operator user profile for EIFE interface was changed
	Password of administrator user profile for EIFE interface was changed
	All the passwords for EIFE interface were changed

Device List

Description

The MasterPacT MTZ circuit breaker connected to the EIFE interface is automatically detected. Click the **Apply** button 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 EIFE interface.	–
Address	Displays the Modbus address of the EIFE interface. **NOTE:** The **Address** text box is unavailable to edit.	255 (fixed)
Name	Allows you to enter the name for EIFE interface. **NOTE:** • The LV breaker system is uniquely identified over possible interfaces such as HMI, Modbus/TCP, DPWS, and DHCP. • EIFE interface device name is common across all interfaces. Thus, changing EIFE interface device name by any means has direct impact on all the connected interfaces.	The EIFE interface device name can have up to 64 ASCII characters with the following characters: **A–Z**, **a–z**, **0–9**, and **-**. However, **-** cannot be used at the end of the name. **NOTE:** • EIFE interface device 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: • 59 ASCII characters for MasterPacT MTZ devices • 64 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 EIFE 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 118. 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 EIFE interface can log data received at predefined intervals (5, 10, 15, 20, 30, and 60 minutes). Below is an explanation of how the EIFE 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 EIFE interface provides this data logging at predefined intervals.

The features of EIFE interface data logging are:

- 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 EIFE 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 MasterPacT MTZ drawout 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 132 in **Monitoring** menu.

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

Logging

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

Purge Data

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

Customize

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

Device Log Export

Description

The **Device Log Export** page is used to export the device logs automatically by EIFE interface. The device log export allows you to configure EIFE 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 EIFE interface, ensure that the EIFE 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:** • If the transport is scheduled for **Hourly** or **Logging Interval**, the incremental check box is selected automatically and is unavailable to be cleared. • If the **Incremental** check box is not selected, the complete log file is sent through an email as an attachment on each scheduled interval.	–
Manual Export	Allows you to export the accumulated log files manually.	–

Schedule

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

To Addresses

Parameter	Description	Setting
To Addresses	Lists the email recipients configured in the EIFE 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 EIFE interface supports SNMP, allowing a network administrator to access remotely an EIFE interface with an SNMP manager and to view the networking status and diagnostics of the EIFE 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 EIFE 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 EIFE 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 setting: 5 s
Communications Check Rate	Controls how often a communications check is performed while the browser is displaying real-time readings in the standard monitoring table views. This function attempts to bring any out-of-service devices back into service automatically.	5...30 min Default setting: 15 min

Advanced Services Control

Industrial Protocol

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

Services Configuration

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

User Accounts

Description

The EIFE interface users are assigned with user names and passwords. Each user belongs to a group, and each group has access rights to the EIFE webpages assigned by the EIFE 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 stars (**********) is not allowed.

Users

Parameter	Description
Name	Enter a name (1 to 15 characters) for a new user. **NOTE:** User names are case-sensitive and can contain only alphanumeric characters.
Password	Enter a password (0 to 11 characters) for a new user.
Email ID	Enter a valid email address for the selected name.
Group	Select a group for the new user.
Language	Select the language for the new user and click the **Apply** button 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.

EIFE 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: • **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

Description

The **Real Time Data** page provides:

- The basic readings of the circuit breaker connected to the EIFE 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 EIFE 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 EIFE webpage menu bar, click **Monitoring**.	Displays 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 MasterPacT MTZ drawout circuit breaker connected to the EIFE 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.	Displays 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 EIFE webpage menu bar, click **Monitoring**.	Displays 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**.	Displays 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.	Displays 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 EIFE interface. For more details on configuring device logging, refer to Device Logging, page 119.

Single Device Pages

Step	Action	Result
1	From the EIFE webpage 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: • **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
EIFE interface FTPS server	Comma-separated variable (CSV)
Export to an external FTPS server	CSV
Data point button	HTML
Email	CSV

To view the list of all the available log files, follow steps 2 to 4 in the section Getting an Interval Data Log using FTPS, page 134. Files are in the format: *Device Name.csv* where the device name is the name given to the MasterPacT MTZ drawout circuit breaker. For example, a device named building 1 utility entrance is *Building 1 Utility Entrance.csv*.

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

NOTE:

- The circuit breaker status in log file is coded by numbers. For information on circuit breaker status, refer to the description of the Modbus register 12001 in the *Modbus Communication Guides* in Related Documents, page 7.
- The device log file may contain invalid values (-9999, -99999, 32768) for electrical parameters based on the data read from the device.

Log Format

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

Row	Data in CSV Format	Description
1	EIFE interface name, EIFE interface serial number, EIFE 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	EIFE 555, 23227,157.198.184.116, building1 utility entrance, 893, MasterPacT MTZ,15	This row contains the information about the EIFE 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. EIFE 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 EIFE interface FTPS Server

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

NOTE: If you want the EIFE 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 EIFE interface data log.
2	Launch Windows Explorer, enter `ftps://` and the IP address of the EIFE interface in the address text box (for example, `ftps://169.254.0.10`), press **Enter**.	Opens the **Log On As** dialog box.
3	Enter the user name as `Administrator` and password as `Gateway` in the text boxes, click **Log On**.	Opens an FTPS session with the EIFE interface and displays the files stored in the EIFE interface.
4	Navigate to the directory*/logging/data* on the EIFE interface.	Opens the data logging directory on the EIFE 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 Button

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 EIFE interface must be configured to deliver data logs to an email address. For more information, refer to Email Export, page 121.

Summary Device Pages

The summary device view provides the summary of the circuit breaker connected to the EIFE 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

Reset Commands

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

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.

This feature is always enabled.

Application Control

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

- Breaker application
- IO application

Password Management

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

The password is required for MasterPacT MTZ circuit breaker with MicroLogic control units.

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

Control	Operation	Availability
Breaker	Open/Close	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

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	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 MasterPacT MTZ drawout circuit breaker connected to the EIFE interface to EIFE interface date and time. The time is set automatically. This page is used to get the MasterPacT MTZ drawout circuit breaker time.

List of Parameters in Set Device Time

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

Setting the Device Time

Step	Action	Table
1	From the EIFE webpage 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 MasterPacT MTZ drawout circuit breaker gets synchronized with the EIFE interface date and time, and the status is updated as successful. **NOTE:** If the synchronization fails, then the status is updated as unsuccessful.

Diagnostics Webpages

What's in This Chapter

Statistics

Description

The **Statistics** page shows the readings accumulated since the EIFE interface was last activated. If the power to the EIFE 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 EIFE webpage 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 EIFE 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: • Nominal • Degraded • Out of service
Boot Memory	Healthiness of the boot memory
EEPROM	Healthiness of EEPROM
File System	Healthiness of the file system
Ethernet PHY 1	Healthiness of PHY 1 hardware
Ethernet PHY 2	Healthiness of PHY 2 hardware
DDR	Healthiness of the execution memory

Interpreting Date and Time Statistics

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

Interpreting Date /Time Synchronization

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

Interpreting ULP Statistics

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

Interpreting File System Statistics

Statistic	Description
Total Size	Total amount of the EIFE interface disk size in kilobytes
Used Size	Total amount of used disk size on the EIFE interface disk in kilobytes
Free Size	Total amount of unused disk space on the EIFE interface disk in kilobytes
Bad Size	Amount of corrupted disk space on the EIFE 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 EIFE webpage 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 EIFE 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 EIFE interface. The devices connected are:

- MicroLogic X control unit
- IO module IO 1
- IO module IO 2

Read Device Registers

Description

Read device registers allows the EIFE interface to read Modbus registers from the devices of the MasterPacT MTZ IMU:

- MicroLogic X control unit
- EIFE interface
- IO modules

Read Procedure

Step	Action	Result
1	From the EIFE webpage 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.

EIFE 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 EIFE 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.	• **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 EIFE interface has an automated communication check that runs every 15 minutes by default. To change the timing, refer to Preferences, page 124. This check verifies the communication health of all the devices configured on the EIFE 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 EIFE webpage menu bar, click **Diagnostics**.	Opens the **Diagnostics** menu.
2	From the **Diagnostics** menu, in the **Device Health Check** submenu, click **Communications Check**.	Opens the **Communications Check** page.
3	Click **Check Device Status**.	Runs a communications check. The communicating device displays: • **Passed** in the **Communications** column. • **In Service** in the **Status** column. A device that is not communicating display: • **Failed** in the **Communications** column. • **Out of Service** in the **Status** column if it has failed multiple times.

IO Readings

Description

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

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

Step	Action	Result
1	From the EIFE webpage 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	• 1 • 0
Force/Unforce	Displays the six digital inputs and three digital outputs are forced or unforced	• **UNFORCED** • **FORCED**

Maintenance Webpages

What's in This Chapter

Indicators

Description

The **Indicators** page provides the maintenance counter information for the MasterPacT MTZ drawout circuit breaker connected to the EIFE 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 EIFE webpage 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.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

www.se.com

DOCA0106EN-15