Refrigeration Expert XP

Remote monitoring and maintenance solution for small stores, restaurants, refrigerated warehouses

User Manual

REX00_01EN

06/2025

www.eliwell.com

eliwell
by Schneider Electric

Legal information

Table of Contents

Safety information

Important information

Read these instructions carefully and visually inspect the equipment to familiarize yourself with the controller before installing it and/or putting it into operation or servicing it. The following warning messages may appear anywhere in this documentation or on the equipment to warn of potential dangers or to call attention to information that can clarify or simplify a procedure.

The addition of this symbol to a danger warning label “Danger” or “WARNING” indicates the existence of an electrical danger that could result in personal injury should the user fail to follow the instructions.

This is the safety warning symbol. It is used to warn the user of the potential dangers of personal injury. Observe all the safety warnings that follow this symbol to avoid the risk of serious injury or death.

DANGER

DANGER indicates a dangerous situation that, unless avoided, **will result in** death or cause serious injuries.

WARNING

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

CAUTION

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

NOTICE

NOTICE used in reference to procedures not associated with physical injuries.

Note

Electrical equipment must be installed, used and repaired by qualified personnel only. Schneider Electric and Eliwell do not accept responsibility for any consequences resulting from the use of this material.

A qualified person is someone who has specific skills and knowledge regarding the structure and the operation of electrical equipment and who has received safety training on how to avoid the inherent dangers.

Personnel qualification

Only personnel with suitable training and an in-depth knowledge and understanding of the content of this manual and other documentation relating to the product in question are authorized to work on and with this product.

The qualified employee must be capable of identifying any hazards that may arise from the parameters, changing the value of the parameters and from using mechanical, electrical and electronic equipment in general. Plus, they must be familiar with accident prevention standards, provisions and regulations, which must be observed while the system is being designed and implemented.

Permitted use

The products described or mentioned in this document, together with the software, accessories and optional extras, are controllers intended for the supervision of monitoring, recording and data handling procedures, plus remote viewing and maintenance of the connected devices for refrigeration systems used in the processing, storage and distribution of foodstuffs, in compliance with the instructions, directives, examples and safety information provided in this document and other supporting documentation.

The product may only be used in line with all applicable laws and safety directives, the specified requirements and the technical data.

Before using the product, a risk assessment in relation to the intended application must be carried out. Suitable safety measures should be implemented based on the results obtained.

Although the product is used as a component of a machine or of a general process, the safety of individuals must be guaranteed when planning this system as a whole.

Only use the product with the specified cables and accessories. Only use genuine accessories and spare parts.

Any use other than the expressly permitted use is prohibited and may present unforeseen risks.

Improper use

Any use other than that described in the previous paragraph, “Permitted use”, is strictly prohibited.

The relay contacts supplied are electromechanical and are subject to wear. The functional safety protection devices, specified by international or local laws, must be installed outside this device.

Liability and Residual Risks

Electrical equipment must be installed, used and repaired by qualified personnel only.

The liability of Schneider Electric and Eliwell is limited to the correct and professional use of the product according to the directives referred to herein and in the other supporting documents, and does not cover any damage (including but not limited to) the following causes:

- unspecified installation/use and, in particular, in contravention of the safety requirements of the legislation in force in the country of installation and/or specified in this document;
- use on equipment which does not provide adequate protection against electrocution, water and dust in the actual installation conditions;
- use on equipment which allows access to dangerous components without the use of tools and/or a keyed locking mechanism;
- installation/use on equipment that does not comply with the regulations in force in the country of installation.

Disposal

The equipment (or product) must be subjected to separate waste collection in compliance with the local legislation on waste disposal.

About the document

Document Scope

Refrigeration Expert XP is a web-based monitoring and control system for small-scale commercial refrigeration setups, supporting up to 20 devices and 200 data resources. It enables remote access, data logging, alarm management, and HACCP reporting. Users can configure devices, view real-time data, and schedule reports through a multilingual interface. The system supports Modbus RTU and Eliwell Micronet controllers, with connectivity via Ethernet, USB, and RS485. Features include customizable dashboards, parameter mapping, and firmware updates. It offers user role management, virtual alarms, and integration with email servers for notifications and report delivery. Configuration is accessible via browser without additional software.

Validity Note

This document applies to the **Refrigeration Expert XP** device.
The characteristics of the products described in this document are intended to match the characteristics that are available on www.eliwell.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.eliwell.com, consider www.eliwell.com to contain the latest information.

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 (English document).
Schneider Electric provides additional information and assistance:

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

Available Languages of this Document

This document is available in these languages:

- Italian (REX00_01IT)
- English (REX00_01EN)
- Spanish (REX00_01ES)
- German (REX00_01DE)
- French (REX00_01FR)

Related documents

Publication title	Reference code
Instruction sheet Refrigeration Expert XP	9IS54911 (5L)
Cybersecurity Best Practices	Refer to Cybersecurity Best Practices (English document)

The available technical documentation and other technical information can be downloaded from the website: www.eliwell.com.

Environmental Data

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

Information on non-inclusive or insensitive terminology

As part of a group of responsible and inclusive companies, we are currently updating our communications and products that contain non-inclusive terminology. Nevertheless, until we have completed this process, our content may still include standardized industry terminology which may be considered inappropriate by our customers.

Product related information

⚠ ⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, FIRE OR ARC FLASH

- Disconnect all power from all equipment including connected devices prior to removing any covers or doors, or installing or removing any accessories, hardware, cables or wires.
- Always use a properly rated voltage sensing device to confirm the power is off where and when indicated.
- Replace and secure all covers, accessories, hardware, cables and wires and confirm that a proper ground connection exists before restoring the unit power supply.
- Use only the specified voltage when operating this equipment and any associated products.

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

⚠ ⚠ DANGER

LOOSE WIRING CAN RESULT IN ELECTRIC SHOCK AND/OR FIRE

- Tighten the connections in compliance with the technical specifications for torque values and make sure the wiring is correct.
- Do not insert more than one cable per terminal board connector unless you are using the ends of the cables (terminals).
- Use only the recommended wire cross-sections for the current capacity of the electrical power supply.

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

⚠ ⚠ DANGER

GROUND RING CAUSING ELECTRIC SHOCK AND/OR EQUIPMENT MALFUNCTION

- Do not connect the connection to 0 V (indicated by the symbol on the power supply connector) of the power supply/transformer powering this equipment to an external earth connection (ground).
- Do not connect the connection to 0 V or earth (ground) on the sensors and actuators connected to this equipment (indicated as “GND” on the respective connector) to an external earth connection (ground).
- If necessary, use separate power supplies/transformers to power the sensors and actuators isolated from this equipment.

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

Refer to the product information at the start of this document in addition to the “Technical data” section for important information relating to installation of this specific equipment in hazardous areas.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Install and use this equipment in compliance with the conditions described in the “Technical data” section of this document.

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

⚠ WARNING

HAZARD OF OVERHEATING AND/OR FIRE

Install and use the equipment exclusively in a protected environment, to prevent direct exposure to sunlight and atmospheric agents.

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

⚠ WARNING

HAZARD OF OVERHEATING AND FIRE

- Do not connect the equipment directly to line voltage.
- Only use Class 2 transformers/power supplies with SELV isolated voltage for supplying power to the equipment.

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

Qualified individuals, being aware of the risks posed by incorrect configuration, must install the equipment in an area which can only be accessed with suitable authorization, and must avoid using the equipment in areas in which children are present.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Only install this equipment in areas with limited access.
- Do not install this equipment in areas where children are present.
- Use appropriate safety interlocks where personnel and/or equipment hazards exist.
- Install and operate this equipment in an enclosure appropriately rated for its intended environment and secured by a keyed or tooled locking mechanism.
- Power line and output circuits must be wired and fused in compliance with local and national regulatory requirements for the rated current and voltage of the equipment used.
- Do not disassemble, repair or modify this equipment.

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

⚠ WARNING

LOSS OF CONTROL

- The installation designer must consider the potential failure modes of the control circuit and, for some critical control functions, provide a means for reaching a safe condition during and after a circuit failure. Examples of critical control functions are the emergency stop and end of travel stop, power supply cut-off and restarting.
- Separate or redundant control circuits must be provided for critical control functions.
- The system control circuits can include communication connections. Keep in mind the implications of transmission delays or sudden connection failures.
- Comply with all standards regarding accident prevention and local applicable safety directives. (1).
- Every implementation of this device must be tested individually and completely in order to check its proper operation before putting it into service.

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

(1) For additional information, refer to the standards NEMA ICS 1.1 (latest edition), “Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control” and NEMA ICS 7.1 (latest edition) “Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems” or to equivalent standards that regulate your particular location.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Use appropriate safety interlocks where personnel and/or equipment hazards exist.
- Do not use this equipment for safety-critical functions.
- Install this equipment in an environment in which EMC disturbance is below the limits specified in standard EN61000-6-1 (residential, commercial and light industry environments).
- For the connection to the supervision system, use a specific shielded “twisted pair” cable (for example: BELDEN cable model 8762).

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

⚠ WARNING

HAZARD OF OVERHEATING AND/OR FIRE

Install and use the equipment exclusively in a protected environment, to prevent direct exposure to sunlight and atmospheric agents.

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

When handling the equipment, exercise caution to avoid damage caused by electrostatic discharge. In particular, contact with uncovered connectors is likely to damage the controller due to electrostatic discharge.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION DUE TO ELECTROSTATIC DISCHARGE

- Store the equipment in the protective packaging until ready for installation.
- Before handling the equipment, always discharge the static electricity from the body by touching an earthed surface or type-approved antistatic mat.

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

The pages on the website have been designed to set up and monitor the system and to access the equipment from a web browser, via a web server. Use HTTPS protocol for installation of a TLS certificate generated by a trusted CA (Certification Authority).

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Only use software approved by Eliwell when using this equipment.
- Update your application program every time you change the physical configuration of the hardware.

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

Take the suitable care and precautions when using this product as a control device, to avoid unforeseen consequences resulting from the operation of the controlled machine, variations in controller status or changes to the machine data memory or operating parameters.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Before attempting to control the application remotely, you must be perfectly familiar with the application and the machine.
- Take the necessary precautions to guarantee that you are working on the anticipated machine remotely by using clear identification documentation within the application and the corresponding remote connection.

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

Eliwell adheres to industry best practices in the development and implementation of control systems. This includes a Defense-in-Depth approach to guarantee an industrial control system. This approach protects the controller and limits access to authorized personnel only.

⚠ WARNING

UNAUTHORIZED ACCESS AND SUBSEQUENT NETWORK INTRUSION

- Assess whether the room or the machines are connected to a critical infrastructure and, if so, take suitable preventative measures, based on “Defense-In-Depth ” strategy, before connecting the automation system to any network.
- Minimize the number of devices connected to a network.
- Isolate your industrial network from other networks within the company.
- Protect any network from unintentional access using firewalls, VPNs or other proven security measures.
- Monitor activity within the systems.
- Prevent direct access or direct connection to the devices by unauthorized individuals or unauthorized actions.

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

NOTICE

LOSS OF APPLICATION DATA

- Do not remove the micro SD card.
- When accessing the USB stick, do not turn off or reset the controller.
- Do not insert or remove the USB stick while accessing it.
- Make sure at least one email recipient has been configured for the transmission of generated reports.
- Back up the reports received via email (1).

Failure to follow these instructions can result in equipment damage.

(1) To satisfy the HACCP requirements and prevent the system memory from being exhausted, with a resulting loss of function, the reports should be created, emailed and then deleted.

NOTICE

UNINTENDED EQUIPMENT OPERATION

- Do not connect the power cable to the RS485 serial port terminal.
- Before switching on the controller, make sure it is not damaged and that all cables are securely fastened.
- Observe the minimum curve radius of the Ethernet cable to avoid damaging the controller (typically: eight times the overall diameter of the cable).

Failure to follow these instructions can result in equipment damage.

NOTICE

UNINTENDED EQUIPMENT OPERATION

- For connection to the power supply, use cables no longer than 10 m (32.80 ft).
- For USB connection, use cables no longer than 30 cm (11.80 in) if connected permanently within a panel.
- For Ethernet connection, use cables no longer than 100 m (328 ft).

Failure to follow these instructions can result in equipment damage.

NOTICE

UNINTENDED EQUIPMENT OPERATION

- For the RS485 network, use a special shielded "twisted-pair" cable with two conductors with cross-section 0.5 mm2 (AWG 20), plus a sheath (characteristic impedance 120 Ω) with PVC sleeve, rated capacity between conductors 36 pF/m, rated capacity between conductor and shield 68 pF/m.
- Alternatively, for the RS485 network, use a special shielded "twisted-pair" cable with two conductors with cross-section 0.5 mm2 (AWG 20), plus a sheath with PVC sleeve, rated capacity between conductors 89 pF/m, rated capacity between conductor and shield 161 pF/m. When laying cables, comply with the indications given in standard EN 50174 on information technology wiring.
- When laying and connecting cables, always observe applicable regulations. Separate the data transmission circuits from electrical lines.
- The length of the RS485 network that can be directly connected to the controller is 1200 m, with a maximum of 32 devices. The length of the network and the number of devices for each channel can be expanded using suitable repeater modules.
- The single terminal block has 3 wires: use all 3 (“+”, “-” for signal and “GS” for the sheath).
- Apply 120 Ω 1/4 W resistors between the “+” and “-” terminals of the interface and the last controller for each branch of the network.

Failure to follow these instructions can result in equipment damage.

Flammable refrigerant gases

This equipment is designed to operate in non-hazardous locations and where applications which generate (or could potentially generate) hazardous environments have been isolated. Install this equipment only in areas and with applications known to be constantly free from hazardous atmospheres.

⚠ ⚠ DANGER

HAZARD OF EXPLOSION

- Install and use this equipment in non-hazardous locations only.
- Do not install or use this equipment in applications which could generate hazardous atmospheres, such as applications which use flammable refrigerants.

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

For information regarding the use of control equipment in applications capable of generating hazardous materials, please contact the relevant national regulatory bodies or certifying authorities.

Before you start

Do not use this product on machines without effective protection for the work area.
The lack of effective protection for the work area on a machine may lead to serious injury for the machine operator.

⚠ WARNING

EQUIPMENT WITHOUT PROTECTION
Do not use this software or the relative automation equipment on a device lacking protection on the workstation.
Failure to follow these instructions can result in death, serious injury, or equipment damage.

This automation equipment and the corresponding software are used to control various industrial and commercial processes.

Only the user, the machine manufacturer or the system integrator can be up-to-date in terms of all the conditions and factors present when preparing, starting up and servicing the machine and therefore only they are able to determine which automation equipment and corresponding safety devices and interlocks can be used correctly.

When the automation and control equipment and the relative software are selected for a particular application, the applicable local and national standards and regulations must also be taken into consideration. Furthermore, the manual for accident prevention of the National Safety Council (recognized nationally in the United States of America) provides very useful information.

Before putting the equipment into service, make sure that all the safety devices and appropriate mechanical/electrical interlocks relating to the protection of the workstation have been installed. All the interlocks and safety devices relating to workstation protection must be coordinated with the corresponding software programming and automation instruments.

Start-up and testing

Before using the electric control and automation equipment for normal operation after installation, the system should be subjected to a start-up test by qualified personnel to make sure the equipment is functioning correctly.
It is important to carry out the preparations for this check and that sufficient time is provided in order to completely and satisfactorily perform the test.

⚠ WARNING

DANGER WHEN STARTING UP THE EQUIPMENT

- Check that all installation and preparation procedures have been completed.
- Before performing the operating tests, remove all the locks or other temporary retaining devices used when shipping the device components.
- Remove any tools, measuring instruments and debris from the equipment.

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

Perform all the start-up tests recommended in the equipment documentation. Conserve all equipment documentation for future consultation.

The custom software must be tested in a simulated environment as well as in the real environment.

Check that the completed system is free of short circuits and that the temporary earth system is not installed in compliance with local standards (for example the National Electrical Code in the US). If it is necessary to perform high potential voltage tests, comply with the recommendations provided in the equipment documentation in order to avoid damaging the device.

Before powering the equipment:

- Close the door in the equipment casing.
- Remove all the temporary earth systems from the incoming power supply lines.
- Perform all the start-up tests recommended by the manufacturer.

Terminology sourced from standards

The technical terms, terminology, symbols and corresponding descriptions in this manual, or which appear on the products themselves, are generally sourced from the terms or definitions used in international standards. In the context of functional safety systems, start-ups and general automation, this may include, but is not limited to, terms such as safety, safety function, protected status, fault, fault reset, malfunctioning, fault, error, error message, hazardous, etc.

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers, part 2: Equipment requirements and tests.
ISO 13849-1:2015	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2013	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction.
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements.
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection.
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design.
IEC 62061:2015	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems.
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software requirements.
IEC 61784-3:2016	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.
2006/42/EC	Machinery Directive.
2014/30/EU	Electromagnetic Compatibility Directive.
2014/35/EU	Low Voltage Directive.

Plus, the terms used in this document may be used in passing as they are sourced from other standards such as:

Standard	Description
IEC 60034 series	Rotating electrical machines.
IEC 61800 series	Adjustable speed electrical power drive systems.
IEC 61158 series	Digital data communications for measurement and control – Fieldbus for use in industrial control systems.

Finally, the term "operating area" may be used in relation to the description of specific hazards, and is defined as for a hazard area or hazardous area in the Machinery Directive (2006/42/EC) and ISO 12100:2010.

NOTE: The abovementioned standards may or may not be applicable to the specific products mentioned in this documentation. For further information concerning individual standards applicable to the products described herein, please refer to the table of characteristics for these product references.

Introduction

Contents

This section includes the following topics:

General description

Refrigeration Expert XP is a web-based monitoring and control system for small-scale commercial refrigeration setups, supporting up to 20 devices and 200 data resources. It enables remote access, data logging, alarm management, and HACCP reporting. Users can configure devices, view real-time data, and schedule reports through a multilingual interface. The system supports Modbus RTU and Eliwell Micronet controllers, with connectivity via Ethernet, USB, and RS485. Features include customizable dashboards, parameter mapping, and firmware updates. It offers user role management, virtual alarms, and integration with email servers for notifications and report delivery. Configuration is accessible via browser without additional software.

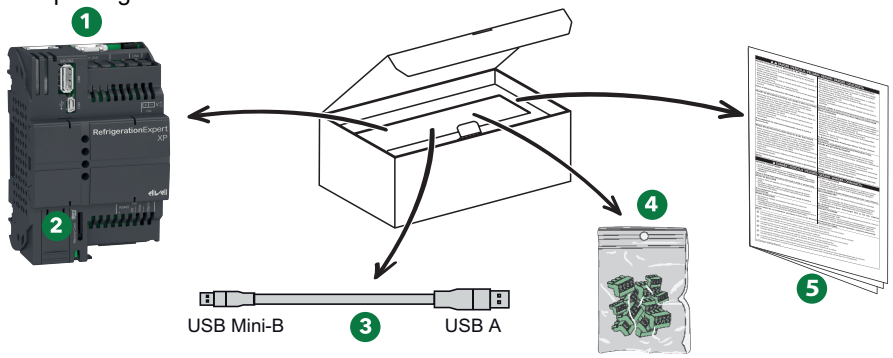
Models

The available models are listed below:

Product	Description	no. of devices (maximum)
RXB01000E0000	Refrigeration Expert XP /10	10 (20)

Package contents

The package contents include:



Label	Description
1	**Refrigeration Expert XP**
2	Micro SD (installed in the product)
3	USB A / USB Mini-B cable
4	Bag with removable terminals
5	Instruction Sheet Refrigeration Expert XP

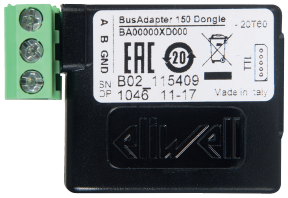
Accessories available

⚠ ⚠ DANGER

HAZARD OF ELECTRIC SHOCK, FIRE OR ARC FLASH
Only connect compatible accessories to the device.
Failure to follow these instructions will result in death or serious injury.

Contact a representative Eliwell for further information regarding compatible accessories.

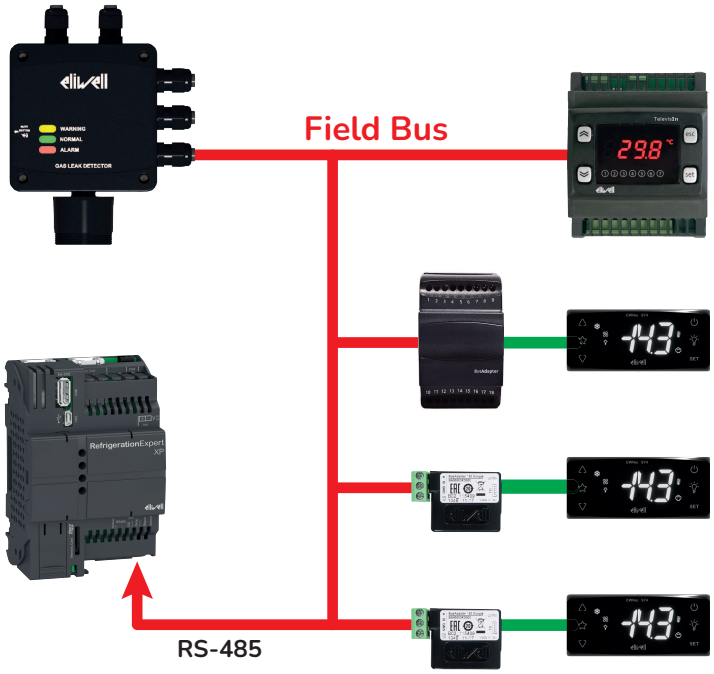
Depending on your own applications, the following accessories may be purchased separately:

Accessory	Description
	**ABLM1A24006**: POWER SUPPLY 24V 0.6A MODULAR
	**SAM4GW000AA00**: ROUTER 4G LTE W/ANT PSU RUT200 **Model**: TELTONIKA RUT2000 10000 Europe, Australia, Asia Pacific certification 9W EU PSU 2x 4G antenna 1x WiFi antenna
	**BusAdapter**: optoisolated TTL/RS485 communication interface for controllers with no RS-485 serial port. The interface requires separate mains power
	**BusAdapter 150 Dongle**: non-optoisolated TTL/RS485 communication interface for AIR series controllers with no RS-485 serial port. The interface is powered by the controller via the TTL port

Monitored network example

Refrigeration Expert XP is certified for use with RS485 networks.

Below is an example of a network:



Example of RS485 network with Refrigeration Expert XP

Languages supported

The languages included are as follows:

- Italian
- English
- Spanish
- German
- French

Browser

Browsers supported

Platform	Browser	Minimum version
Personal Computer	Google Chrome	98
	Microsoft Edge	98
	Safari	15.4
Tablet	Android browser	116
	Google Chrome for Android	116
	Safari for iOS	15.4

Browsers not supported

Platform	Browser	Minimum version
Personal Computer	Firefox	94
Tablet	Firefox for Android	116
	Samsung Internet	18
	Opera mobile	73

Updating the application

The cache settings may affect how the new system version loads.

NOTICE
INOPERABLE DEVICE After updating the application, delete the browser history used to access the system. **Failure to follow these instructions can result in equipment damage.**

Cybersecurity

Contents

This section includes the following topics:

Overview

This Eliwell product includes functions that enable Information security.
These functions come as default and can be configured according to your own installation requirements.

NOTE: deactivating or changing the settings for these individual functions can positively or negatively affect the overall posture of the device security and ultimately, the security-related behavior of the network.

It is also necessary to observe best practices in order to guarantee advanced system protection and ensure the security of the system as a whole.
For more information, please refer to: “Cybersecurity Best Practices” (English language only).

Eliwell adheres to industry best practices in the development and implementation of control systems. This includes a Defense-in-Depth approach which protects the controller by limiting access exclusively to authorized personnel and protocols.

⚠ WARNING

UNAUTHORIZED ACCESS AND SUBSEQUENT NETWORK INTRUSION

- Assess whether the room or the machines are connected to a critical infrastructure and, if so, take suitable preventative measures, based on “Defense-In-Depth ” strategy, before connecting the automation system to any network.
- Minimize the number of devices connected to a network.
- Isolate your industrial network from other networks within the company.
- Protect any network from unintentional access using firewalls, VPNs or other proven security measures.
- Monitor activity within the systems.
- Prevent direct access or direct connection to the devices by unauthorized individuals or unauthorized actions.

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

Managing users

User management is used to create groups of users with configurable authorizations.

Access can be limited to a few functions by assigning individual users to a group.

There are 3 default groups:

- **Administrators**: editing rights for all functions
- **Maintenance**: editing rights for selected functions
- **End users**: viewing rights for selected functions

Only the **admin** administrator, or a user with "User management" authorization enabled can add, edit or remove users and groups.

Note: the **admin** user represents the device owner and has special rights. They cannot configure the system - only the device, its connectivity and users.

Note: the **admin** user is the only one that can carry out the password recovery procedure.

List of protocols and ports managed

The list of device ports is shown below:

Input ports

- Port 443/TCP (HTTPS) - Non-configurable

Output ports

- Port 465/TCP (SMTP/SMTPS) - Configurable
- Port 123/UDP (NTP) - Non-configurable

  The following address must be reacheable when enabling Network Time Protocol (NTP):

  - **Primary NTP server**
    - 0.arch.pool.ntp.org
    - 1.arch.pool.ntp.org
    - 2.arch.pool.ntp.org
    - 3.arch.pool.ntp.org
  - **Fallback NTP server**
    - time1.google.com
    - time2.google.com
    - time3.google.com
    - time4.google.com

  Acronym meanings

  - **TCP**: Transmission Control Protocol
  - **SMTP**: Simple Mail Transfer Protocol
  - **SMTPS**: Simple Mail Transfer Protocol Secured
  - **UDP**: User Datagram Protocol
  - **NTP**: Network Time Protocol

Information security configuration recommendations

Recommendations

- Do not add more users than those requiring access and evaluate the system requirements before allowing users access to critical pages, for example: **Device settings**.
- Limit the number of IP addresses that can access the **Refrigeration Expert XP**.
- In Email server configuration, do not use unsecure authentication type 'none'
- In Email server configuration, do not use unsecure port 25. Use ports 465 or 587 instead.
- In Email server configuration, do not skip certificate verification

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, STATE AND SECURITY

- Change the default passwords to prevent unauthorized access to device settings and information.
- Position the network devices behind various cyber defense levels (firewalls, network segmenting and network intrusion detection and protection systems).
- Adopt cyber security best practices (for example: minimal privileges, separation of functions, secure SMTP, etc.) to prevent unauthorized exposure, loss of or changes to data and registries, the interruption of services or accidental operation.

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

NOTE: the table below contains the risks and best practices associated with unprotected protocols. We strongly recommend adhering to these best practices.

Unprotected protocols	Risks	Best practices
SMTP	• malware threat • unauthorized access to data • data loss threat • email content transferred to normal text	For publication: • Select Login configuration, SMTP with SSL/TLS or Smart TLS (port 465, 587) and do not skip certificate verification for publication

Mechanical installation

Contents

This section includes the following topics:

Before you start

Before installing your system, read this chapter carefully.
Only the user, the machine manufacturer or the integrator can be familiar with all the conditions and factors present during installation and set up, preparing, starting-up and servicing the machine and therefore only they are able to determine which automation equipment and relative safety devices and interlocks can be used in a correct manner.
When the automation and control equipment and any other relative equipment or software are selected for a particular application, the applicable local, regional and national standards and regulations must also be taken into consideration.
Take extra care to comply with safety standards, electrical requirements and other statutory provisions applied to your own machine.

⚠ WARNING

REGULATORY INCOMPATIBILITY
Make sure that all equipment used and the systems designed comply with all applicable local, regional and national laws.
Failure to follow these instructions can result in death, serious injury, or equipment damage.

Disconnecting from the power supply

Assemble and install all options and modules before installing the control system.
Before dismantling the equipment, remove the control system from the wall or panel.

⚠ ⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, FIRE OR ARC FLASH

- Disconnect all power from all equipment including connected devices prior to removing any covers or doors, or installing or removing any accessories, hardware, cables or wires.
- Always use a properly rated voltage sensing device to confirm the power is off where and when indicated.
- Replace and secure all covers, accessories, hardware, cables and wires and confirm that a proper ground connection exists before restoring the unit power supply.
- Use only the specified voltage when operating this equipment and any associated products.

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

Operating environment

This equipment is designed to operate in non-hazardous locations and where applications which generate (or could potentially generate) hazardous environments have been isolated. Install this equipment only in areas and with applications known to be constantly free from hazardous atmospheres.

⚠ ⚠ DANGER

HAZARD OF EXPLOSION

- Install and use this equipment in non-hazardous locations only.
- Do not install or use this equipment in applications which could generate hazardous atmospheres, such as applications which use flammable refrigerants.

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

For information regarding the use of control equipment in applications capable of generating hazardous materials, please contact the relevant national regulatory bodies or certifying authorities.

Refer to the product information at the start of this document in addition to the “Technical data” section for important information relating to installation of this specific equipment in hazardous areas.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Install and use this equipment in compliance with the conditions described in the “Technical data” section of this document.

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

Installation considerations

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Use appropriate safety interlocks where personnel and/or equipment hazards exist.
- Power line and output circuits must be wired and fused in compliance with local and national regulatory requirements for the rated current and voltage of the particular equipment.
- Do not use this equipment in safety-critical machine functions.
- Do not disassemble, repair, or modify this equipment.

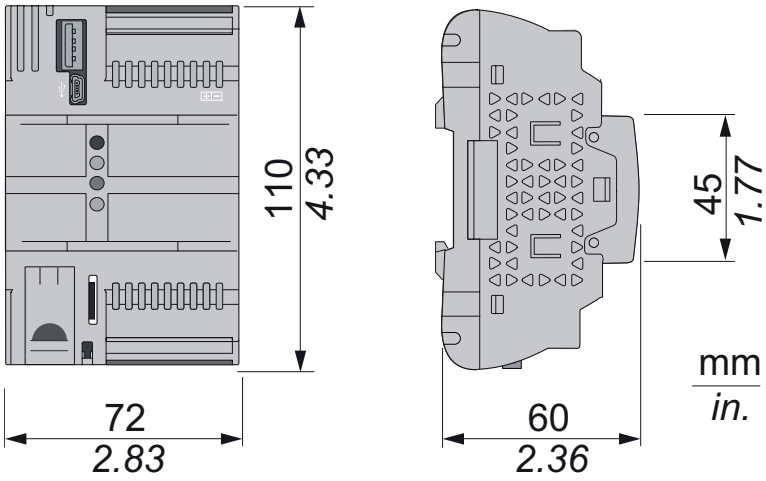
Failure to follow these instructions can result in death, serious injury, or equipment damage.

For the mechanical dimensions, refer to "Mechanical dimensions".

Mechanical dimensions

The mechanical specifications of **Refrigeration Expert XP** are:

- Width: 72 mm (2.83 in.)
- Length: 110 mm (4.33 in.)
- Height: 60 mm (2.36 in.)



Installation

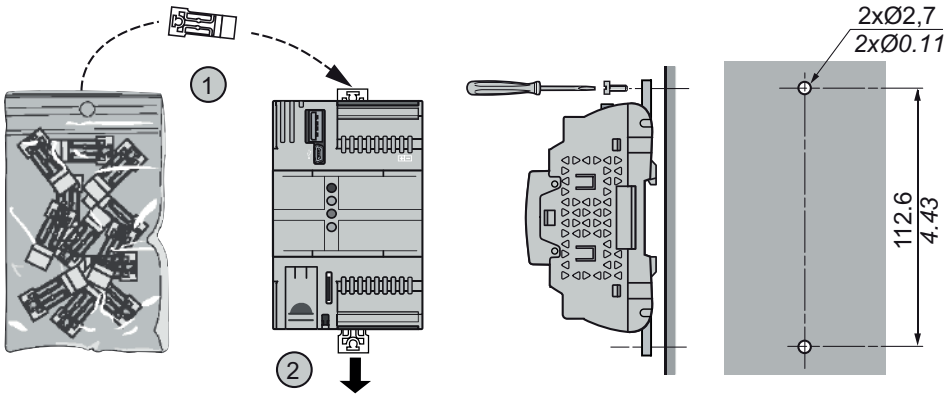
Refrigeration Expert XP is intended for wall- or panel-mounting (on a flat surface).

Note: **Refrigeration Expert XP** is only suitable for indoor use. DO NOT install it outdoors.

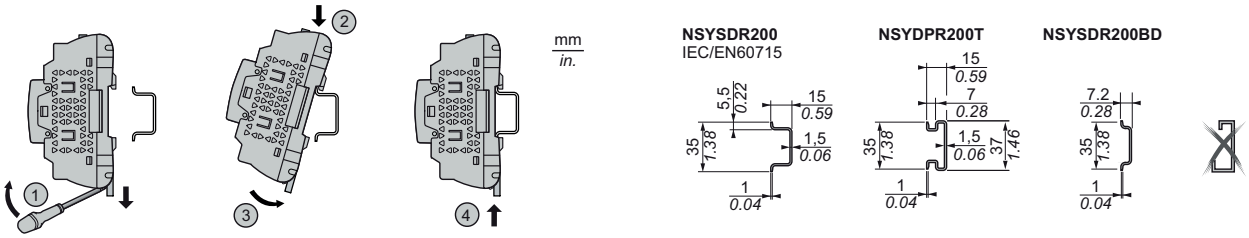
How to install/uninstall the controller

Panel mounting

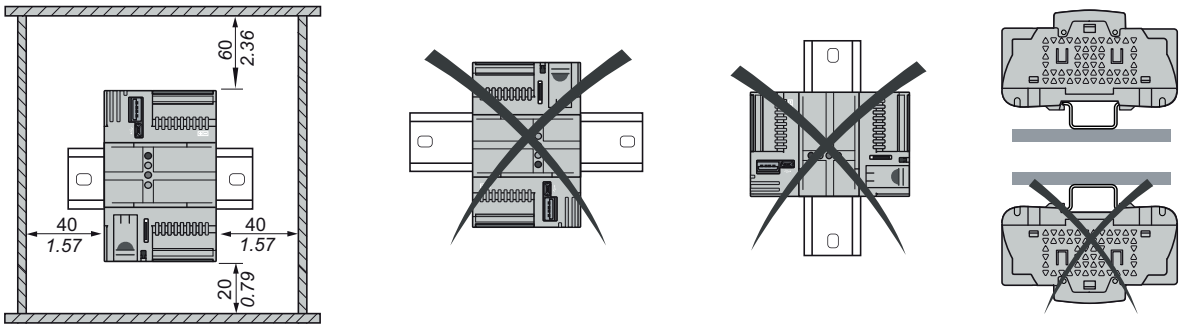
To install, secure the device to the wall/panel with 2 screws (not supplied) in line with the holes illustrated in the figure below:



Top hat section profile guide



DIN rail mount



Electrical connections

Contents

This section includes the following topics:

Best wiring practices

Warnings

The following information describes wiring guidelines and the practices to observe when using the device.

⚠ ⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, FIRE OR ARC FLASH

- Disconnect all power from all equipment including connected devices prior to removing any covers or doors, or installing or removing any accessories, hardware, cables or wires.
- Always use a properly rated voltage sensing device to confirm the power is off where and when indicated.
- Replace and secure all covers, accessories, hardware, cables and wires and confirm that a proper ground connection exists before restoring the unit power supply.
- Use only the specified voltage when operating this equipment and any associated products.

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

Qualified individuals, being aware of the risks posed by incorrect configuration, must install the equipment in an area which can only be accessed with suitable authorization, and must avoid using the equipment in areas in which children are present.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Only install this equipment in areas with limited access.
- Do not install this equipment in areas where children are present.
- Use appropriate safety interlocks where personnel and/or equipment hazards exist.
- Install and operate this equipment in an enclosure appropriately rated for its intended environment and secured by a keyed or tooled locking mechanism.
- Power line and output circuits must be wired and fused in compliance with local and national regulatory requirements for the rated current and voltage of the equipment used.
- Do not disassemble, repair or modify this equipment.

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

⚠ WARNING

HAZARD OF OVERHEATING AND/OR FIRE

Install and use the equipment exclusively in a protected environment, to prevent direct exposure to sunlight and atmospheric agents.

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

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Install Refrigeration Expert XP in an environment in which EMC disturbance is below the limits specified in standard EN61000-6-1 (residential, commercial and light industry environments).
- Configure the sending of a regular report to make sure that Refrigeration Expert XP is active. Non-receipt of the periodic email indicates a malfunction of the Refrigeration Expert XP or the email transmission service.

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

⚠ WARNING

LOSS OF CONTROL

- The installation designer must consider the potential failure modes of the control circuit and, for some critical control functions, provide a means for reaching a safe condition during and after a circuit failure. Examples of critical control functions are the emergency stop and end of travel stop, power supply cut-off and restarting.
- Separate or redundant control circuits must be provided for critical control functions.
- The system control circuits can include communication connections. Keep in mind the implications of transmission delays or sudden connection failures.
- Comply with all standards regarding accident prevention and local applicable safety directives. (1).
- Every implementation of this device must be tested individually and completely in order to check its proper operation before putting it into service.

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

(1) For additional information, refer to the standards NEMA ICS 1.1 (latest edition), “Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control” and NEMA ICS 7.1 (latest edition) “Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems” or to equivalent standards that regulate your particular location.

Wiring guidelines

Observe the following standards when wiring the device:

- Keep the communication wiring separate from the power wiring. Keep these two types of cables in separate conduits.
- Check that the operating conditions and surroundings comply with the specification values.
- Use wires of the correct diameter which are suited to the voltage and current requirements.
- Use copper conductors (required).
- Use twisted-pair shielded wires for networks and field buses.

Use shielded wires, correctly earthed, for the communication connections. If shielded wires cannot be used for these connections, the electromagnetic interference may deteriorate the signal. Deteriorated signals can result in the device, modules or attached equipment operating incorrectly.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Use shielded cables for all communication signals.
- Earth the wire shields for all communication signals in a single point.
- The signal cables (communication and relative power supplies) of the device must be laid separately from the power cables.
- Reduce the length of the connections as far as possible and avoid winding them round electrically connected parts.

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

Guidelines for screw-type terminal blocks

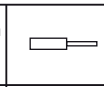
⚠ ⚠ DANGER

LOOSE WIRING CAN RESULT IN ELECTRIC SHOCK AND/OR FIRE

- Tighten the connections in compliance with the technical specifications for torque values and make sure the wiring is correct.
- Do not insert more than one cable per terminal board connector unless you are using the ends of the cables (terminals).
- Use only the recommended wire cross-sections for the current capacity of the electrical power supply.

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

Only use copper conductors.
The table below shows the type and size of permitted cables for screw terminals and the torque values:

mm / *in.* 9 / *0.35*								
mm^2	0.14…1.5	0.14…1.5	0.25…1.5	0.25…0.5	2x 0.08…0.5	2x 0.08…0.75	2x 0.25…0.34	2 x 0.5
AWG	*26…16*	*26…16*	*22...16*	*22...20*	*2x 28...20*	*2x 28...20*	*2x 24…22*	*2 x 20*

 Ø 2,5 mm (*0.1 in.*)		N•m	0.22...0.25
		lb-in	*1.95...2.21*

Specific considerations for handling

When handling the equipment, exercise caution to avoid damage caused by electrostatic discharge. In particular, contact with uncovered connectors is likely to damage the controller due to electrostatic discharge.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION DUE TO ELECTROSTATIC DISCHARGE

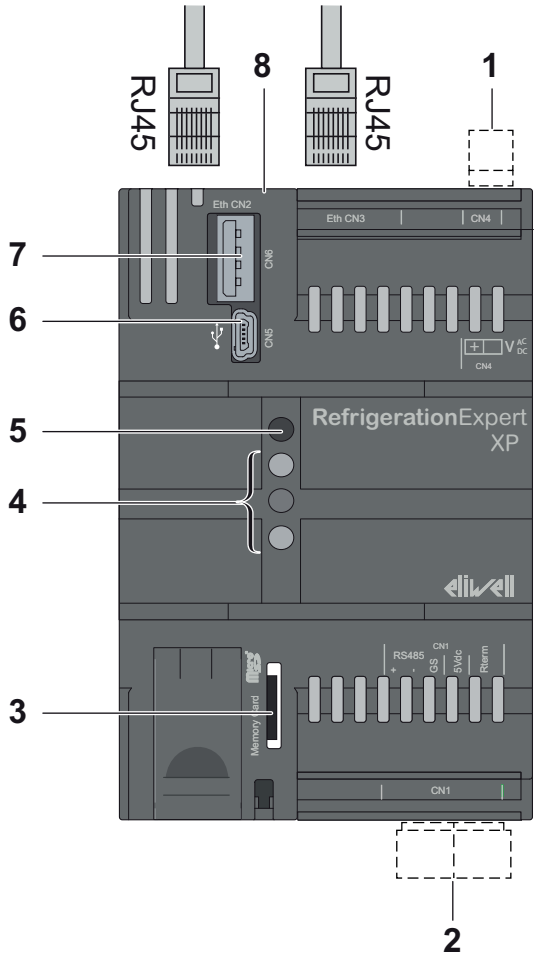
- Store the equipment in the protective packaging until ready for installation.
- Before handling the equipment, always discharge the static electricity from the body by touching an earthed surface or type-approved antistatic mat.

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

Before starting any operations, check that the device is connected to a suitable external power supply. Please refer to "Power supply".

Hardware Refrigeration Expert XP

The **Refrigeration Expert XP** connectors are as follows:



Number	Label	Description
1	CN4	Power supply
2	CN1	Serial port (RS485)
3	Memory Card	Slot for memory card (Micro SD)
4	LED	LEDs not used
5	LED ON	Power supply LED (green)
6	CN5	Mini-B USB port
7	CN6	Type A USB port
8	CN2, CN3	Ethernet port (RJ45). **Note**: the Ethernet connectors have the same MAC address.

NOTICE

LOSS OF APPLICATION DATA

- Do not remove the micro SD card.
- When accessing the USB stick, do not turn off or reset the controller.
- Do not insert or remove the USB stick while accessing it.
- Make sure at least one email recipient has been configured for the transmission of generated reports.
- Back up the reports received via email (1).

Failure to follow these instructions can result in equipment damage.

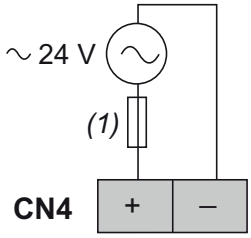
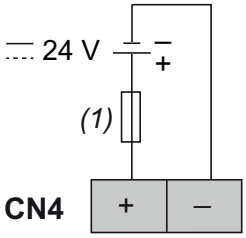
(1) To satisfy the HACCP requirements and prevent the system memory from being exhausted, with a resulting loss of function, the reports should be created, emailed and then deleted.

Power supply

The table for the type of power supply and the corresponding consumption is:

Power supply characteristics	Absorbed power (maximum)
24 Vac (+/- 10 %) - 50/60 Hz	11 VA
20…38 Vdc (UL / CSA)	8 W
24 Vdc (IEC)	8 W

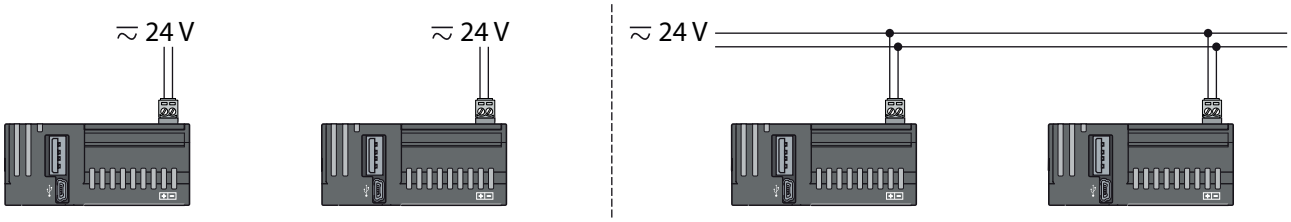
Power supply connection diagram

24 Vac	24 Vdc
	
(1) Fuse type T 3 A ~ 3.15 A	

The DC power supply connection negative terminal and the reference signal for the RS485 port (indicated as GS) are not connected internally.

Terminal block spacing	Wiring length
3.50 mm (0.14 in.)	10 m (32.8 ft)

The power supply connections may be isolated or non-isolated, as per the image below:



⚠ ⚠ DANGER

GROUND RING CAUSING ELECTRIC SHOCK AND/OR EQUIPMENT MALFUNCTION

- Do not connect the connection to 0 V (indicated by the symbol on the power supply connector) of the power supply/transformer powering this equipment to an external earth connection (ground).
- Do not connect the connection to 0 V or earth (ground) on the sensors and actuators connected to this equipment (indicated as “GND” on the respective connector) to an external earth connection (ground).
- If necessary, use separate power supplies/transformers to power the sensors and actuators isolated from this equipment.

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

In all cases, if the specified voltage interval is not maintained, the products may not work as intended. Use suitable safety interlocks and voltage monitoring circuits.

⚠ WARNING

HAZARD OF OVERHEATING AND FIRE

- Do not connect the equipment directly to line voltage.
- Only use Class 2 transformers/power supplies with SELV isolated voltage for supplying power to the equipment.

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

Communication

Refrigeration Expert XP has the following communication ports:

- 1x RS485 serial port (CN1)
- 2x RJ45 Ethernet ports (CN2, CN3)
- 1x USB mini-B port (CN5)
- 1x USB A port (CN6)

Take extra care when performing serial line connections.
Incorrect wiring may lead to faulty operation or breakdown of the equipment.

NOTICE
UNINTENDED EQUIPMENT OPERATION • Do not connect the power cable to the RS485 serial port terminal. • Before switching on the controller, make sure it is not damaged and that all cables are securely fastened. • Observe the minimum curve radius of the Ethernet cable to avoid damaging the controller (typically: eight times the overall diameter of the cable). **Failure to follow these instructions can result in equipment damage.**

NOTICE
UNINTENDED EQUIPMENT OPERATION • For connection to the power supply, use cables no longer than 10 m (32.80 ft). • For USB connection, use cables no longer than 30 cm (11.80 in) if connected permanently within a panel. • For Ethernet connection, use cables no longer than 100 m (328 ft). **Failure to follow these instructions can result in equipment damage.**

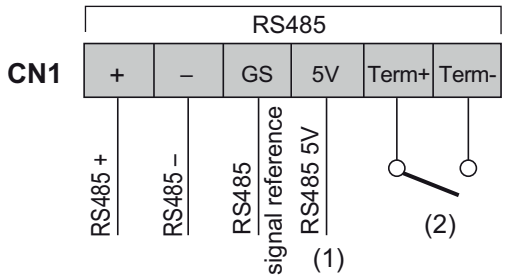
RS485 serial port

Overview

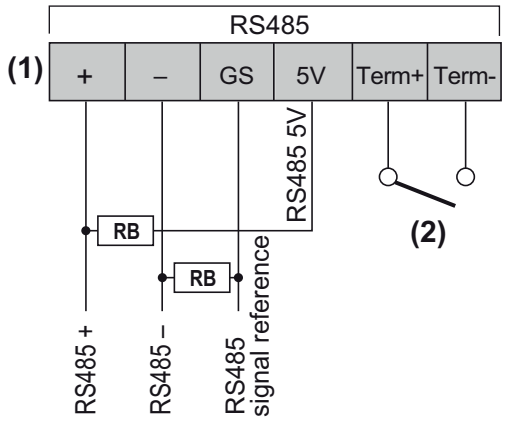
This port offers the user communication between controllers by means of a Modbus RTU connection.

Connector

Refrigeration Expert XP is equipped with an RS485 serial port (CN1):



NOTE: the GS pin is not directly connected to the DC power supply connection of the “-” pin for the power supply unit.



(1) (**CN1**) 5 V power supply for any external polarizing resistors (RB). Maximum current: 10 mA.

(2) (**CN1**) On closing the circuit between the terminals Term+ and Term- (using a switch or a jumper), a 120 Ohm internal terminal resistor should be applied to the positive (RS485+) and negative (RS485-) terminals of the RS485 port. Apply the resistor if it is the last bus device.

Wiring

NOTICE

UNINTENDED EQUIPMENT OPERATION

- For the RS485 network, use a shielded "twisted-pair" cable with two conductors with cross-section 0.5 mm^2 (AWG 20) plus a sheath (typical impedance 120 Ω) with PVC sleeve, rated capacity between conductors 36 pF/m, rated capacity between conductor and shield 68 pF/m.
- Alternatively, for the RS485 network, use a shielded "twisted-pair" cable with two conductors with cross-section 0.5 mm^2 (AWG 20) plus a sheath with PVC sleeve, rated capacity between conductors 89 pF/m, rated capacity between conductor and shield 161 pF/m. When laying cables, comply with the indications given in standard EN 50174 on information technology wiring.
- When laying and connecting cables, always observe applicable regulations. Separate the data transmission circuits from electrical lines.
- The length of the RS485 network that can be directly connected to the controller is 1200 m, with a maximum of 32 devices. The length of the network and the number of devices for each channel can be expanded using suitable repeater modules.
- The single terminal block has 3 wires: use all 3 (“+”, “-” for signal and “GS” for the sheath).
- Apply 120 Ω 1/4 W resistors between the “+” and “-” terminals of the interface and the last controller for each branch of the network.

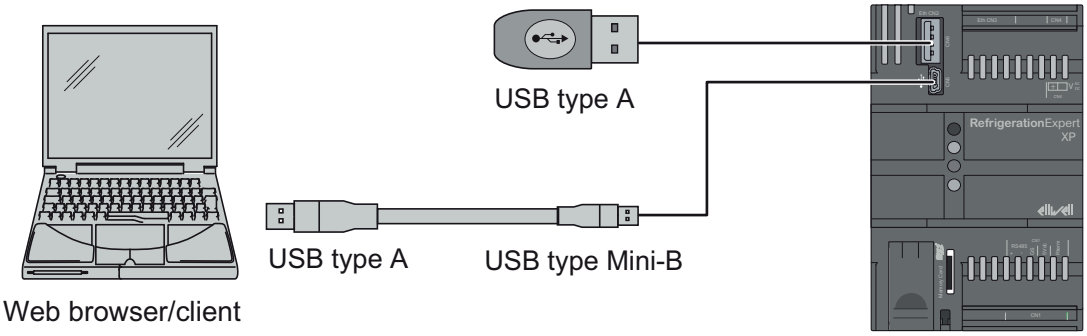
Failure to follow these instructions can result in death, serious injury, or equipment damage.

USB serial port

Overview

The Mini-B type USB connector (DEVICE) is used to connect **Refrigeration Expert XP** to a PC via Mini-B/A USB cable for debugging, commissioning and downloading.

The type A USB connector (HOST) is used to connect a USB memory stick.



Power supply

Refrigeration Expert XP does not allow power supply via the Mini-B USB cable.

Compatibility

The Mini-B type USB connection is configured to emulate an Ethernet port in devices equipped with Microsoft USB/RNDIS drivers.

RJ45 Ethernet port

Overview

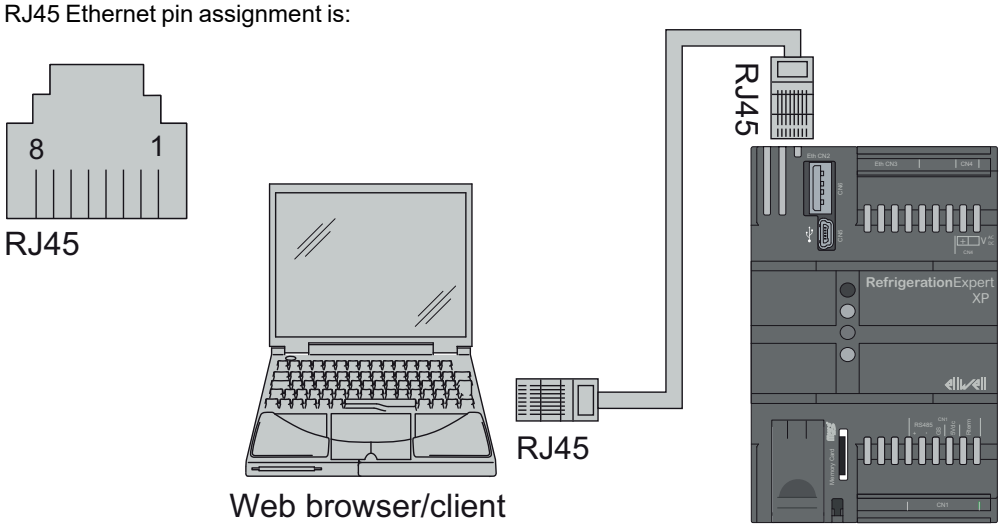
Refrigeration Expert XP has two 10 M / 100 M Ethernet ports with auto-negotiation, which share the same MAC address, and therefore can be used alternately for the same functions.
The Ethernet connection allows:

- the user to connect via HTTPS web browser
- the **Refrigeration Expert XP** to communicate by means of TCP/IP protocol
- the **Refrigeration Expert XP** to connect to an SMTP/SMTPS server

Simultaneous communication of different protocols that use the same Ethernet port is permitted (for example, using a Web browser in addition to the SMTPS mail server).

Connector

RJ45 Ethernet pin assignment is:

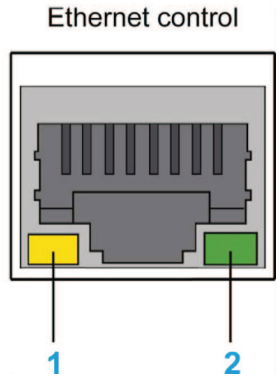


Pin number	Signal
1	TX_D1+
2	TX_D1-
3	RX_D2+
4	BI_D3-
5	BI_D3+
6	RX_D2-
7	BI_D4+
8	BI_D4-
Wiring length (maximum): 100 m (328 ft)	

NOTE: the controller supports the MDI/MDIX automatic crossover cable function. It is not necessary to use special crossed Ethernet cables to connect the devices directly to this port (connections without hub or Ethernet switch).

Status LED

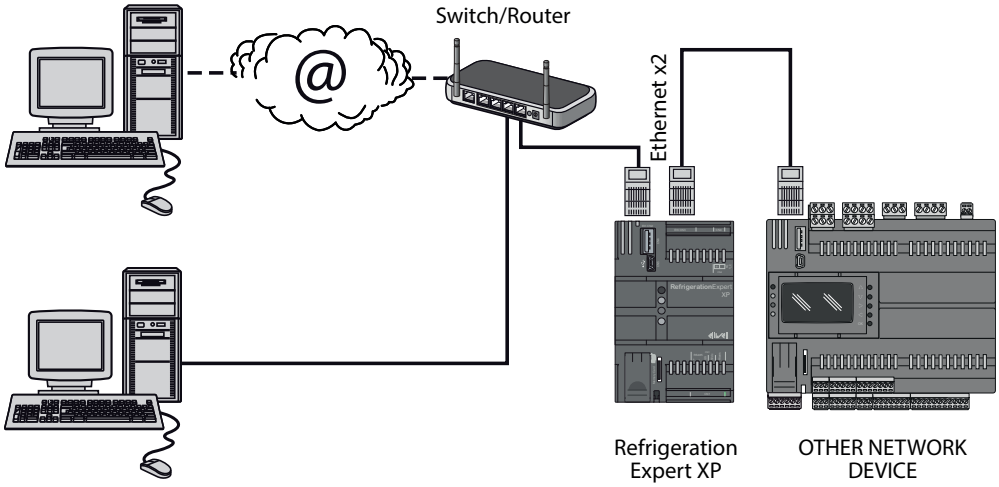
The RJ45 Ethernet LEDs indicate:



Label	Signal	LED		
		Color	Status	Description
1	Ethernet Activity	Yellow	Off	No activity
			Flashing	Active
2	Ethernet Link	Green	Off	No Link
			Green LED on	Linked

Ethernet connection

The Ethernet connectors have the same MAC address and can be used to perform connections in series:



Network connection example

The connection between **Refrigeration Expert XP** and the network devices should take place using conductors with a cross-section of 0.5 mm^2 (see "Best wiring practices").

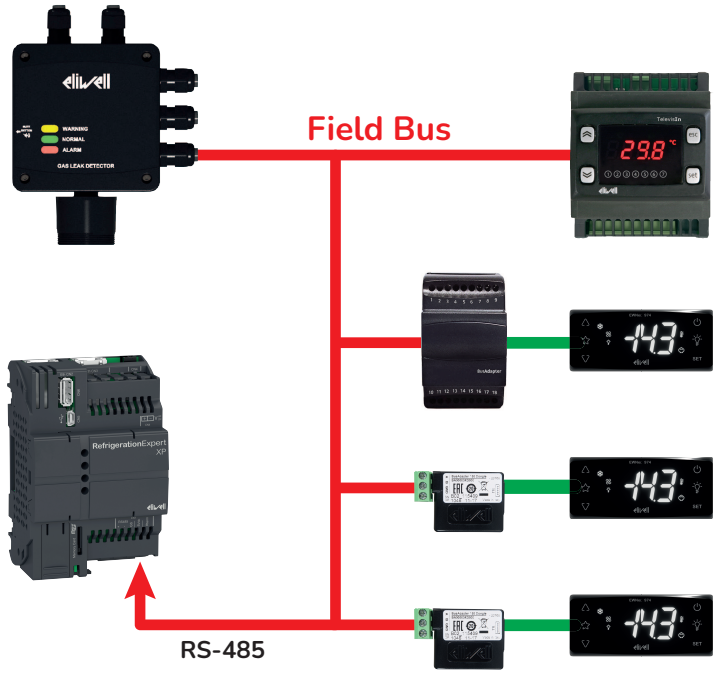
Device configuration

Before configuring a network using the **Refrigeration Expert XP**, each device within the system should be assigned a unique code in the context of the serial port by setting - depending on the on-board device protocol - the following parameters:

- Device with Micronet protocol: parameters “**FAA**” (0...14) and “**dEA**” (0...14).
- Device with Modbus protocol: parameter “**Adr**” (1...247).

RS485 network example

The connection of an RS485 network takes place as follows:



In the example the following devices were used:

- 1x **Refrigeration Expert XP**
- 1x LKDNext
- 1x **Bus**Adapter
- 2x **Bus**Adapter 150 Dongle
- 3x EWNext
- 1x Televis**In**

Signal propagation in an Ethernet network depends on bus traffic, making access times non-deterministic and potentially influencing **Refrigeration Expert XP** access time to the various resources with possible No-Link.

NOTICE
INOPERABLE DEVICE If connection proves difficult, check if the right profile has been assigned to the network; if not, change it accordingly. **Failure to follow these instructions can result in equipment damage.**

Technical data

Contents

This section includes the following topics:

Technical data

Feature	Description
The product also complies with the following harmonized standards:	EN 62368-1
Product group:	End product
Classified for use by:	Qualified personnel
Equipment mobility:	Fixed installation
Mounting method:	see Mechanical installation
Protection rating provided by outer casing:	IPX0
Pollution class:	2
Insulation class:	III
Power supply:	24 Vac ± 10 % 50/60 Hz 20...38 Vdc (UL/CSA) - 24 Vdc (IEC)
Absorbed power (maximum):	8 W / 11 VA
Power supply connection type:	Not connected directly to the mains power (ES1)
Environmental operating conditions:	Temperature: -20...55 °C (-4...131 °F) Humidity: 5...95% RH (non-condensing)
Transportation and storage conditions:	Temperature: -30...70 °C (-22...158 °F) Humidity: 5...95% RH (non-condensing)
Tma specified by the manufacturer (°C):	55°C
Power system:	Not at AC mains voltage
Software class:	A
Altitude during operation (maximum):	2000 m (6560 ft)
Mass of equipment:	0.160 kg
Special installation site:	Area with limited access
RS485 connection:	The RS485 serial bus is not isolated.
Maximum number of devices connectable:	20
Data storage:	1 year with maximum 200 resources and 20 alarm event per day.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION
Do not exceed any of the rated values specified in the “Technical data” table.
Failure to follow these instructions can result in death, serious injury, or equipment damage.

Installing and starting up the system

Contents

This section includes the following topics:

Initial configuration Refrigeration Expert XP

Considerations

- After every maintenance procedure, all USB devices should be removed.
- The default time zone is **GMT+1**. Select the correct option in **System > Plant > Date and time**.
- The mini-B USB connection emulates an Ethernet port with DHCP server.
- **Refrigeration Expert XP** is always accessible with a web browser:
  - via DHCP connection at the address **https://192.168.254.254**
  - by entering the credentials of your user
- At first power-up, only the **admin** user is present, whose credentials are:
  - user: **admin**
  - password: **EW_RefrigerationExpert**

Note: at first power-up, you will be redirected to the password change screen.

Note: **Refrigeration Expert XP** requires the creation of secure passwords for all users.

⚠ WARNING
UNAUTHORIZED ACCESS Do not give the password to unauthorized individuals or non-qualified personnel. **Failure to follow these instructions can result in death, serious injury, or equipment damage.**

Carefully consider the implications of giving access to other people.

NOTICE
LOSS OF FUNCTION Loss of the admin user password prevents access to system configuration. **Failure to follow these instructions can result in equipment damage.**

Note: if a password is forgotten, the only user that can recover it is the **admin** user via the “Password recovery” procedure.

Note: a secure password is one that has not been shared with or given to unauthorized personnel, and that does not contain personal or otherwise obvious information. Do not exceed 50 characters and only use alphanumeric characters.

Password criteria: The password must have at least:

- 8 characters
- 1 numerical digit (0, 1, ... , 9)
- 1 uppercase letter (A, B, ... , Z)
- 1 lowercase letter (a, b, ... , z)
- 1 special character (\|¬¦`!" £$%^&*()_+-=[]{};:'@#~<>,./?)

Installation procedure

Requirements

Hardware:

- **Refrigeration Expert XP**
- USB A / USB mini-B cable
- Personal computer with USB A port and compatible web browser (see Compatible browsers)
- Network of compatible devices connected (see Network connection example)

Software:

- email account and relevant SMTP server settings
- familiarity with the network settings if the device is connected to a LAN (IP, gateway)

Procedure

1. Power up the **Refrigeration Expert XP** (green LED lit steadily).
2. Connect the mini-B USB connector to the **Refrigeration Expert XP**.
3. Connect the USB A connector to the PC.
4. Wait for the driver to auto-configure.
5. Open the browser.
6. In the status bar, enter the address "**192.168.254.254**" and press RETURN. **NOTE**: if the browser opens a window showing “Your connection is not private”, continue by clicking "**Advanced**” and then "Proceed on 192.168.254.254 (not secure).”
7. On the Login page that opens, enter the default user (see Login):
    - Username: **admin**
    - Password: **EW_RefrigerationExpert**
8. Click **Log in**.
9. The system will show the password change screen (see Changing the password the first time you log in).
10. Enter the new password twice as requested and click **Save**.
11. The **SYSTEM** page for device configuration will appear.
12. Proceed with setting the following essential information (for further information see System):
    - **Plant**:
        - **Info**: set the Plant name which will appear in the top left-hand corner (), in reports and in notifications
        - **Localization**:
            - optionally upload language translation (see Manage language translations)
            - set the system language and the date/time format
        - **Date and time**: set the time zone and the clock update methods (see Setting and updating the clock)
    - **History**: set the data recording interval for the historical and quick log
    - **Connectivity**:
        - **Ethernet**: set the connection to the LAN or the router for Internet access and/or remote access to **Refrigeration Expert XP**
        - **Email**: set the SMTP / SMTPS server to send emails and carry out a transmission test
    - **Backup and restore**: set the key protecting the backup files. **NOTE**: the key can only be viewed by the **admin** user
    - **Controller drivers**: optionally upload updated or customized controller drivers (see Manage controller drivers)
    - **Users**:
        - **Users**: add at least one new user by assigning them to the Administrators group. Copy the temporary password assigned by the system
13. Click the (user) icon.
14. In the drop-down menu, select "**Logout**".
15. Access the system through the new User in the Administrators group and the temporary password copied previously.
16. If the password is valid, the system will show the password change screen (see Changing the password the first time you log in).
17. Make sure the device network is connected to **Refrigeration Expert XP**

18. Click “**Add equipment**“ (see Equipment and controllers)
19. Access an instrument by clicking on the relative card
20. Click **Edit** () to edit the device.
21. Configure the network by setting:
    - **groups**: create groups for viewing charts
    - **colors**: assign colors to the resources to identify them in the charts
    - **resources**: add resources to the “Foreground” () and/or "Overview" () screen
22. Configure the device parameters (see Parameters).
23. Configure alarm notification transmission (see Configuring alarm notifications and categories).
24. Configure the schedule of HACCP reports (see Configuring regular HACCP reports).

Note: Alternatively to the mini-B USB port, at the first power-on, it is possible to connect via the Ethernet port to the static IP address **192.168.1.3**.

Changing the password the first time you log in

Requirements

- be connected to the IP address of the **Refrigeration Expert XP**
- have entered the default user credentials (User: **admin**; Password: **EW_RefrigerationExpert**) (see Login section)
- have an Internet connection with a strong signal or be connected via USB.

Procedure

1. on the Login page, enter the default user (see Login).
2. click **Log in**.
3. on the page that opens:
   - **New password**: enter the new password
   - **Confirm password**: enter the new password again.
4. click **Save**.

Note: = show/hide the password entered.
Note: if the password does not meet the criteria, you will not be able to save it.
Password criteria: the password must have at least:

- 8 characters
- 1 numerical digit (0, 1, ... , 9)
- 1 uppercase letter (A, B, ... , Z)
- 1 lowercase letter (a, b, ... , z)
- 1 special character (\|¬¦`!" £$%^&*()_+-=[]{};:'@#~<>,./?)

Remote connectivity

Contents

This section includes the following topics:

Remote connectivity

To make **Refrigeration Expert XP** accessible remotely, it needs to be connected to a suitably configured device enabled for Internet services.
For example, you can use:

A. A router for an xDSL line (Very High-Speed Digital Subscriber Line) with:
   - public static IP
   - DMZ service (demilitarized zone) at the local IP address assigned to **Refrigeration Expert XP**

B. A router for an xDSL line (Very High-Speed Digital Subscriber Line) with:
   - public static IP
   - NAT (Network Address Translation) service from port 443 over the public IP address, at port 443 of the local IP address assigned to **Refrigeration Expert XP**

C. A mobile router with VPN (Virtual Private Network) service that manages the HTTPS service for **Refrigeration Expert XP**

Page structure

Contents

This section includes the following topics:

Page structure

All pages in the web application have the same structure, i.e.:

- Status bar
- Navigation menu
- Work area

Status bar

The status bar is always shown at the top of the window, providing important system status information.
The Status bar contains the following icons and text:

Plant name:		Shows the system name.
Resources Used:		Shows the number of resources used and the total number of resources available (for example: 110/200).
System status:		**Operative**: the system is working properly.
		**In error**: the system is working properly, potentially causing data acquisition to be interrupted. **NOTE**: in the event of a serious error, the system sends a notification containing details of the error to the recipient entered in **SYSTEM > System notifications**.
Alarm status:		**Active**: indicates that active alarms are present.
		**Not active**: indicates that no active alarms are present.
Username and number of users connected:		Indicates the name of the connected user. The following appear in the drop-down menu: • **User management** = redirect to the User configuration page (**SYSTEM > Users**) • **Change password** = edit the password for the current user • **Disconnection** = end the session for the current user and return to the Login screen

Navigation menu

The navigation menu is shown at the top of the page and contains the hypertext links to the different sections of the application:

EQUIPMENT	Used to: • view network devices • filter by description of the individual devices • configure individual devices • add new devices • show alarms for the various devices
HACCP	Used to: • view HACCP resources over a 24-hour period • view HACCP resources for a specific day • schedule the period and time for sending regular reports
HISTORY	Used to: • view the alarm history with the relevant status • view and save reports in table or chart format • schedule the sending of saved reports
SYSTEM	Used to: • set system data • set Users and Groups (if they have authorization) • set the mail for sending System notifications • set connectivity (Ethernet, USB, Email, Devices) • view the software version and load any updates • manage SSL/TLS (Transport Layer Security) certificates (see Certificate management) • set, reload and protect backup files • set data acquisition intervals

Work area

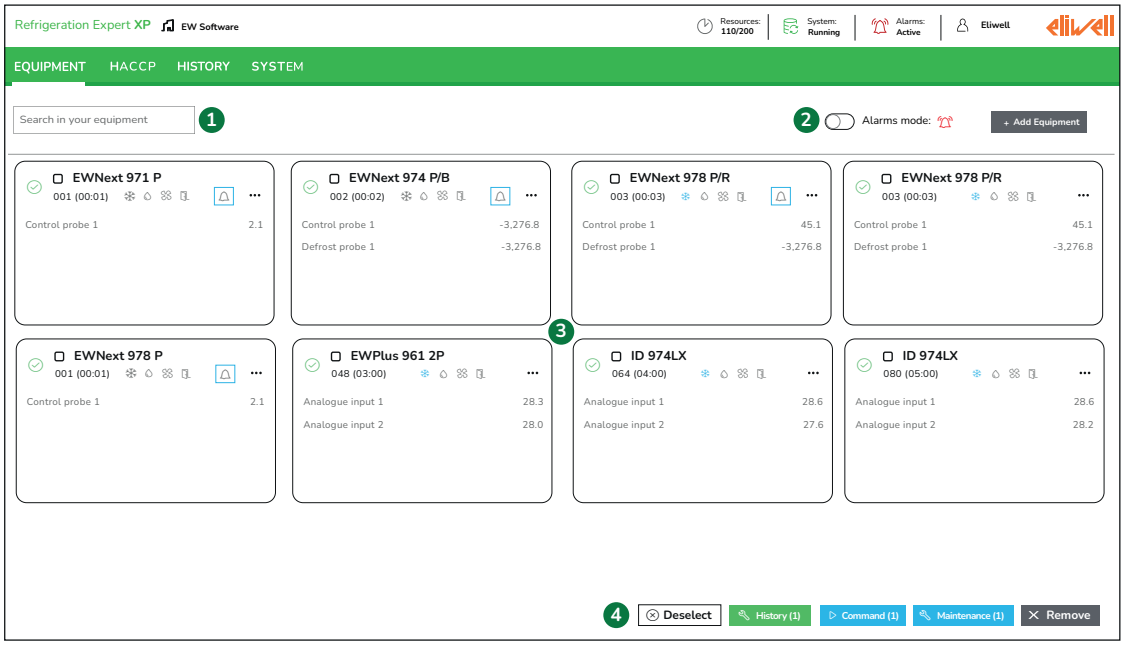
Central area of the page, where the information is shown.

Equipment panel

Access the **EQUIPMENT** page.

The screen components are as follows:

1. **Search**: filter the list of devices by product name or model
2. **Alarm view**: when the selector switch ( ) is activated, devices in alarm mode will be shown (see Alarm status)
   Note: show "device panels" with active/confirmed alarms and the list of alarms
3. **Device panels**: show panels for devices belonging to the network with:
   - ☐: select/deselect box for carrying out procedures on one or more devices using the buttons (**4**), which are only shown when a selection is active
   - **Name**: Name, model and network address (in Modbus format) of the device.
     Note: click on the panel heading to view the device Overview
   - **List**: list resources and alarms selected using the icon in the relevant panels with the relevant values
   - **Icons**: show, if configured, the resources: cooling request, defrost status, fan status and door open status
     Note: the resources are active (colored icons) or inactive (gray icons)
   - **Alarms**: if at least one alarm is active, the alarm status is displayed ( ) . The icon acts as a shortcut to the Alarms panel for individual Devices
4. **Select buttons**: if at least one box ( ) has been selected, the following buttons will be shown:
   - **Deselect**: cancel any selections made
   - **History**: used to access the alarm history
   - **Command**: used to carry out a command
   - **Maintenance**: used to place one or more devices in Maintenance mode
   - **Remove**: used to delete one of the associated devices.



Add equipment panel

Requirements

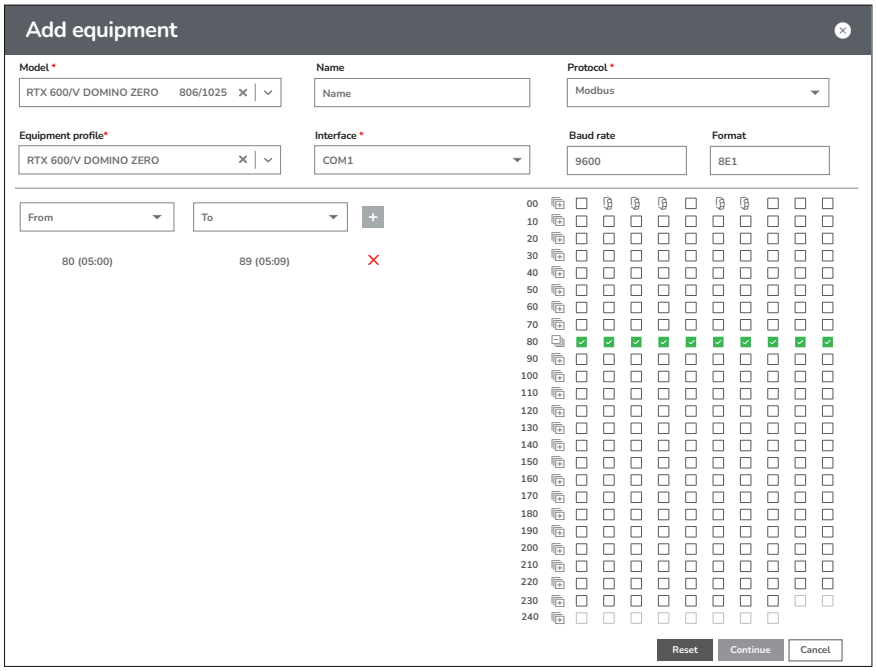
- the user must be authorized to configure the network of controllers

Procedure

1. Access the page **EQUIPMENT**.
2. Select **Add equipment**.
3. Select the device **Model**. Options are:
   - **Manual**: by entering the controller model
   - **Automatic**: by entering “Auto-Discovery Mode”

   Note: while typing, the models corresponding to the entered text appear.
4. Assign a **Name** to the controller. If not specified, the address will be assigned automatically, followed by the model name.
5. Confirm or edit the **Equipment profile**. The drop-down menu will only show profiles which are compatible with the model selected/found.
6. Confirm or edit the fieldbus **Interface** to which the controller is connected (for example: COM1). The system automatically sets the **Baud rate** and **Format**. The system provides information relating to protocol and to the network settings required for communication with the controllers. Depending on the protocol, some addresses may be disabled (gray box).
7. **From-To**: set the range of addresses to scan in order to detect the controller. Click "**+**” to add it
8. **From-To list**: show the list of saved address ranges
9. **Address table**: show the following information:
   - **Address**: identify addresses that can be set
   - : select all non-blocked addresses in the selected group of ten
   - : deselect all free addresses in the selected group of ten
   - : free location in which a device can be added
   - : location occupied by a device
10. **Reset**: delete the data entered on the page and begin the entry process again
11. **Continue**: once one or more devices have been selected with the relevant data, continue with the configuration procedure
12. **Cancel**: exit without saving the settings

Note: all fields with a red asterisk (*) are compulsory and must be completed.



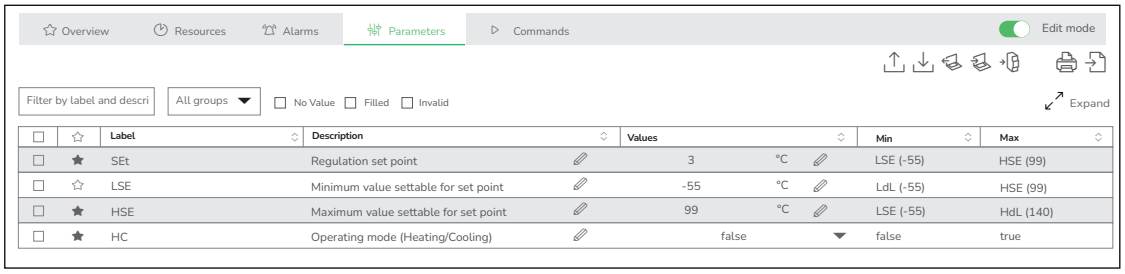
Parameters panel

Procedure

1. Access the **EQUIPMENT** page.
2. Click on the card of an equipment.
3. Access the **Parameters** panel.
4. Activate the **Edit** selector switch.
5. **Filter by label and description**: filter by parameter label and description
6. **All groups**: filter by all parameter groups or by specific codes
7. **Missing value**: filter the parameters to which a value has not been assigned
8. **Valid**: filter the parameters which meet the validity criteria
9. **Not valid**: filter the parameters with a value outside the range between the minimum and maximum values. This condition can arise when editing the value of a parameter which acts as a limit for another parameter (for example, **SEt**)
10. : save the controller parameters as a default parameter map
11. : load and show the default parameter map
12. : save the parameter map to a file
13. : load the parameter map from a file
14. : write onto the device
15. : create PDF document
16. : export .xlsx file
17. **Parameters table**: shows the following information:
    - : tick the box to select/deselect one or more parameters
    - : used to add the parameter to the "overview" panel (only visible in **Edit**)
    - **Label**: shows the label for the controller parameters (filtered or not)
    - **Description**: shows the parameter description; allows editing by clicking the icon
    - **Value**: shows the value read for the controller parameters (filtered or not) with the corresponding unit of measure (UM); allows instant editing by clicking the icon
    - **Min**: shows the minimum value the parameter can assume and any reference to other parameters.
    - **Max**: shows the maximum value the parameter can assume and any reference to other parameters.

Note: if the controller has not been recognized or is in No-Link, or the model is incorrect/does not correspond, the TAB is not enabled

Note: values change is only permitted if the current user is authorized to write the device parameters.



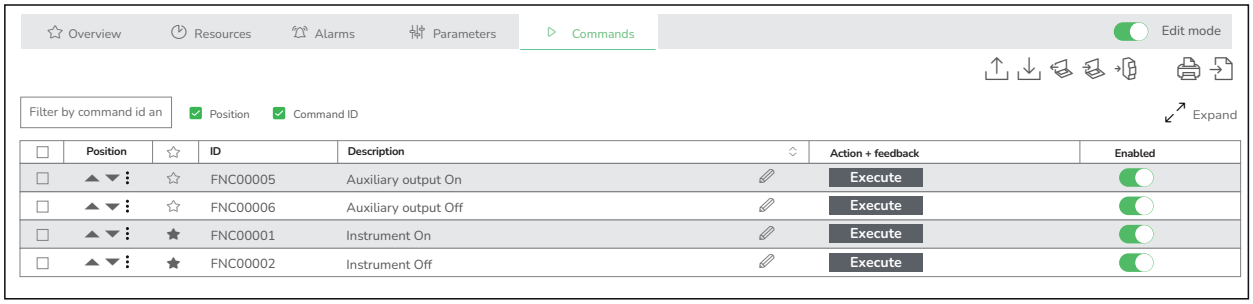
Commands panel

Procedure

1. Access the **EQUIPMENT** page.
2. Click on the card of an equipment.
3. Access the **Commands** panel for the device.
4. Activate the **Edit** selector switch.
5. **Filter by code and description**: filter by command code and description
6. **Position**: activate a column containing the commands to move the resource higher or lower
7. **Alarm code**: show/hide the column containing the alarm code
8. **Command table**: show the following information:
    - ☐: tick the box to select/deselect one or more parameters
    - **Position**: show the commands to move the resource higher or lower (shown if activated in step 2)
    - ☆: used to add the parameter to the "overview" panel (only visible in **Edit**)
    - **Code**: show the code linked to the command (shown if activated in step 3)
    - **Description**: shows the parameter description; allows editing by clicking the icon
    - **Action and result**: show the **Execute** button for carrying out the command
    - **Enabled** ( ): the selector switch enables/disables the command.

Note: if the controller has not been recognized or is in No-Link, or the model is incorrect/does not correspond, the TAB is not enabled

Note: command execution is only permitted if the current user is authorized to execute equipment commands.



Managing users

Contents

This section includes the following topics:

Accessing the system (login)

Requirements

- have a registered account with **Refrigeration Expert XP**
- use a compatible browser (see Compatible browsers)
- have an Internet connection with a strong signal or be connected via USB.

Procedure

1. Open the browser.
2. In the status bar, enter the **Refrigeration Expert XP** IP address and click ENTER.
   Note: if the browser opens a window showing “Your connection is not private”, continue using the "**Advanced**" options.
3. In the **Username** box, enter the "Name" of the registered user.
4. In the **Password** box, enter the current password for your account. **Note**: use  to show/hide the password.
5. In the **Language** box, enter the user interface language (the browser language is set by default).
6. Click **Log in** to access **Refrigeration Expert XP**
7. Click the link **Forgot password?** to start the password recovery procedure.
   Note: the only user authorized to recover passwords is the "**admin**" user (see User management).

Note: if the user enters an incorrect password, the message “Wrong password” will appear.

Note: if the an incorrect password is entered 3 times in a row, the message “The user is temporarily disabled” will appear. The user will be locked out for 10 minutes. At the end of this period the user can attempt login again.

Editing the password for the current user

Requirements

- Be connected, with an active user, to **Refrigeration Expert XP**

Procedure

1. Click the (user) icon.
2. In the drop-down menu, select "**Change password**".
3. Fill in the following fields:
   - **Old password**: enter the current password
   - **New password**: enter the new password
   - **Repeat password**: enter the new password again.
4. Click **Save** to save the new password or **Back** ( ) to exit without changing the password.

Note: : show/hide the password entered.
Note: if the password does not meet the criteria, you will not be able to save it.
Password criteria: The password must have at least:

- 8 characters
- 1 numerical digit (0, 1, ... , 9)
- 1 uppercase letter (A, B, ... , Z)
- 1 lowercase letter (a, b, ... , z)
- 1 special character (\|¬¦`!" £$%^&*()_+-=[]{};:'@#~<>,./?)

Resetting a user password

Requirements

- be the **admin** user or a user in the **Administrator** group.

Procedure

1. On the screen **SYSTEM > Users > Users**:
2. Search for the User whose password needs to be reset.
3. Click in the icon in the user **password** column.
4. Click **Cancel** to exit without saving the changes.
5. Click **Reset** to reset the password.
6. Give the user a temporary password created by the system.

Note: the password should also be reset whenever the password expiry settings are changed.

Note: the first time the user logs in, they will be asked to change the password (see Changing the password the first time you log in).

Creating/editing a user

Requirements

- Be connected to the IP address of the **Refrigeration Expert XP**
- Have an Internet connection with a strong signal or be connected via USB.

Procedure

1. On the screen **SYSTEM > Users > Users**:
2. Click "**Add user**" to create a new user, or **Username** to edit an existing user.
3. In the window which appears:
    - **Username**: enter the username.
    - **Group**: enter the group to which the user belongs
      Note: the groups Administrator, Maintenance and End Users are listed by default.
    - **Description**: description of the user.
    - **Password expiration**: select the password expiry period from the drop-down menu.
4. Click **Add** to save the new user, or **Change** to save the changes to an existing user.
5. Click **Cancel** to exit without saving the changes.
6. Click **Remove user** to remove an existing user.

Note: an active user cannot be edited.

Note: if the group or expiry period is changed, the password should be reset (see Changing the password the first time you log in).

Creating/editing a group

Requirements

- Be connected to the IP address of the **Refrigeration Expert XP**
- Have an Internet connection with a strong signal or be connected via USB.

Procedure

1. On the screen **SYSTEM > Users > Groups**:
2. Click "**Add group**" to create a new group, or the  icon to edit an existing group.
3. In the window which appears:
   - **Group name**: enter the name of the group.
   - **Description**: description of the group.
   - **Select permissions**: select the permissions to assign to the group.
4. Click **Add** to save the new group, or **Change** to save the changes to an existing group.
5. Click **Cancel** to exit without saving the changes.
6. Click **Remove group** to remove an existing group.

Note: changing group permissions will affect all individuals belonging to the group.

Alarms

Contents

This section includes the following topics:

Viewing alarm status

Description

You can view the status of alarms by accessing the **EQUIPMENT** page:

A. In the individual device panels, by clicking the alarm icon ( ).
Note: the icon is only shown if there are active alarms.
B. By activating the **Alarm view** selector switch.

Procedure A (Individual panels)

1. Click the alarm symbol ( ) for a device; the **Alarms** panel containing the relevant details will appear.
2. Click the **Edit** selector switch.
3. **Filter by code and description**: filter by alarm code or description.
4. **Active**: show/hide active alarms.
5. **Confirmed**: show/hide confirmed alarms.
6. **Alarms table**: show:
   - **Description**: description of the alarm
   - **Status**: whether the alarm is active ( ) or confirmed ( ) and for how long
   - **Delay**: show any delays in alarm activation
   - **Colors**: show the color used to represent the alarm in charts

Procedure B (Alarm view)

1. Activate the **Alarm view** selector switch; the screen will be updated to show only the devices in alarm mode with the corresponding alarms. **Note**: both active and confirmed alarms are shown by default.
2. Select the flag "**Show confirmed alarms**" (**1**).
3. View the **Alarms** panel for the device by clicking the alarm icon ( )(**2**).
4. Click the **Edit** selector switch.
5. Select one or more devices/alarms.
6. The following buttons will appear:
   - **Deselect**: to cancel the selections made.
   - **Confirm**: to change the status of the “confirmed” alarms.

Note: confirming one or more alarms only changes the displayed information on the alarms page. Its history is tracked but it does not affect the actions.

Example: it does not change the behavior of an alarm relay. You will need to wait for the alarm condition to actually end for the relay output to be disabled.

Viewing the alarm history

Procedure

1. Access **History > Alarms**
2. The page contains:
    - **Date and time**: select the date and time to be analized
    - **Select period**: select the time interval to use from the options in the drop-down menu (for example: 24 hours)
    - **Select devices**: select one or more devices for which to view the alarms
    - **Filter by alarm description**: search for one or more alarms based on their description
    - **Active**: show/hide active alarms
    - **Confirmed**: show/hide confirmed alarms
    - : print the alarm history in PDF format
    - : export the alarm history in xlsx format
    - **Alarms table**: show the following information:
        - **Devices**: show the device associated with the alarm and the corresponding address
        - **Alarm description**: show the description of the alarm with the corresponding code
        - **Date and time**: show the date and time
        - **Status**: show whether the alarm is active ( ) or confirmed ( )
        - **Time**: show for how long the alarm has been active

Viewing alarm and action details

Description

You can view alarm details by accessing the **EQUIPMENT** page:

A. : **Method 1**

- In the individual device panels, by clicking the alarm icon ( ).
  Note: the icon is only shown if there are active alarms
- By clicking the alarm start time in the **Status** column

B. : **Method 2**

- By activating the **Alarm view** selector switch
- By clicking the alarm start time in the panels for the individual devices

The information shown is:

1. **Alarm detail**: show the following information:
   - **Updates**: show the date and time of the most recent alarm update
   - **Plant name**: show the name assigned to the system
   - **Devices**: show the name of the device in alarm mode
   - **Alarm**: show the color used to represent the alarm in charts
   - **Current status**: identify whether the alarm is **active**, **inactive** or **confirmed**
   - **Alarm start**: show the date and time at which the alarm started
   - **Duration**: show how long the alarm has been active
2. **Event list**: show a list with the following information:
   - **Date and time**: show the date and time of the event
   - **Event**: identify the type of event/action which took place
3. **Notes**: empty box in which to enter any relevant notes

Configuring device alarms

Procedure

1. On the page **EQUIPMENT > Device panel > Alarms**
2. Click the **Edit** selector switch.
3. **Filter by code and description**: used to filter resources based on the alarm code and the description.
4. **Position**: show/hide the column containing the commands to move the resource higher or lower.
5. **Alarm code**: show/hide the column containing the alarm code.
6. **Active**: filter alarms and only show those which are active.
7. **Acknowledged**: filter alarms and only show those which are confirmed.
8. **Resources table**: show the following information:
   - **Position**: show the commands to move the resource higher or lower (shown if activated in step 2)
   - : used to add the alarm to the list "in the foreground"
   - **Alarm code**: show the code linked to the alarm (shown if activated in step 5)
   - **Description**: show the alarm description; allows editing by clicking the icon
   - **State**: whether the alarm is active ( ) or confirmed ( ) and for how long
   - **Delay**: show/set any delays in alarm activation
   - **Colors**: used to link a color to the resource. The color is black by default
   - **Enabled** ( ): the selector switch is used to activate/deactivate the resource.

Creating virtual alarms

Procedure

1. On the page **EQUIPMENT > Device panel > Resources**
2. Activate the **Edit** ( ) selector switch.
3. In the **Alarms** column, enter a low and high threshold.

Example of Setting virtual alarms

When a low and/or high threshold is entered in the **Alarm** box for an analog resource, the system will generate the corresponding "**virtual alarms**".
If, for example, you set:

Resource	Low	High
Analog input 1	(**A**) 30	(**B**) 60
Analog input 2	-	-
Dew point	-	(**C**) 45
Valve opening percentage	-	-
Door opening status	(**D**) 1	(**E**) 0

the following “virtual alarms” will be generated:

Resource	Alarm due to...	Description
(**A**) Low alarm (Analog input 1)	Low	Activated when the value of analog input 1 is < 30
(**B**) High alarm (analog input 1)	High	Activated when the value of analog input 1 is > 60
(**C**) High alarm (Dew point)	High	Activated when the value of the Dew point is > 45
(**D**) Low alarm (Door opening status)	Low	Activated when the value becomes 0
(**E**) High alarm (Door opening status)	High	Activated when the value becomes 1

The new alarms will inherit all the properties of the instrument to which they refer (option of putting them offline, choice of infill/color inside graphs and any activation delays).

If the analogue resource to which the “**virtual alarms**” refer is no longer present, the alarms will be deleted.

Configuring alarm notifications and categories

Description

The alarm categories can be used to define a series of actions to be carried out when specific conditions arise within set time bands.

If an alarm condition is identified, the system associates the first category in order of priority level that meets the configured criteria. If a specific category does not exist, the condition is associated with the “Universal” category.
The **levels** can be set from 1 to 100 (1 represents the most critical level).
The categories will be assessed starting from the lowest level and increasing.
Available **actions** are: sending notifications via email and activating an output on the alarm module.

Requirements

- to have configured one or more devices.

Procedure

1. Access the **EQUIPMENT** page.
2. Activate **Alarm view** ( ) selector switch.
3. Open the **Device management** drop-down menu and select the **Categories** option.
4. Activate the **Edit** ( ) selector switch.
5. Create or edit a category:
   - select + Add category to add a new alarm category.
   - Click the name of an existing category to edit it (the list is underneath the + Add category button).
     Note: the categories are listed in increasing level order and upon first access there is a "Universal" category at level 100 (the lowest).
6. Enter the **Information relating to the category**:
   - **Name**: name linked to the alarm category
   - **Level**: level associated with the alarm category
   - **Enabled**: flag enabling/disabling (/) the alarm category
7. Select **Equipment and alarms**:
   - **Devices**: select the devices to which the alarm category should be applied
   - **Device list**: show the selected devices underneath the selection menu
   - **Alarms**: select the alarms to which the alarm category should be applied
   - **Alarm list**: show the selected alarms underneath the selection menu
8. Enter the **Time bands**:
   - **Add time band**: select a time band from the configured options. By default only "Always” is present
   - **Time band manager**: used to set a new time band
   - **Selected time band**: show the selected time band underneath the selection menu
9. Set the **Actions**:
   - **Add action**: used to set the actions to be carried out, from those available, in the event that an alarm category is activated
   - **Action list**: configured actions are listed underneath the action selection menu, with the corresponding details and a "Remove" button for deleting the action.
   - **Alarms**: select the alarms to which the alarm category should be applied
   - **Alarm list**: show the selected actions underneath the selection menu
10. **Create**: save the alarm category (only present while creating).
11. **Delete category**: delete the category shown (only present while editing).
12. **Update**: save any changes made to the alarm category (only present while editing).

Temporarily suspending alarm notifications during maintenance

Requirements

- have the necessary permissions to manage the network devices.

Procedure

When one or more devices are in maintenance, the corresponding alarm notifications are temporarily silenced for the duration of the maintenance period.
The system will continue to save data but will only begin sending alarm notifications again once the maintenance period is over.
The exception is the **Offline** value setting, where data is no longer saved (see Device maintenance).

Equipment and controllers

Contents

This section includes the following topics:

Automatically searching for devices connected to the network

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. Access the page **EQUIPMENT**
2. Click “**Add equipment**”
3. In the **Model** box, enter "Auto-Discovery Mode"
4. Select one or more address intervals within which to search
   Note: entering a range of addresses instead of performing a full search reduces the search time
5. Carry out one of the available commands:
   - **Reset**: delete the data entered on the page and begin the entry process again
   - **Continue**: once one or more devices have been selected with the relevant data, continue with the configuration procedure
   - **Cancel**: exit without saving the settings
6. A window will open showing the devices which have already been found and the corresponding addresses. You can:
   - **Stop and Continue**: stop the search and show the instruments which have already been identified
   - **Cancel**: cancel the search and return to the **Add equipment** page
7. If **Stop and Continue** is selected, a new window opens showing the list of instruments found and you will be able to decide whether to add them or not. You can:
   - **Add devices**: add the instruments found
   - **Cancel**: cancel the save procedure and return to the **Add equipment** page
8. Access the panel for the added device and customize its resources (see Customizing device resources)

Manually adding devices to the network

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. Access the page **EQUIPMENT**
2. Click “**Add equipment**”
3. Enter the model of the connected device in the **Model** box
4. Enter the controller profile in the **Equipment profile** box. The drop-down menu will only show profiles which are compatible with the model selected/found
5. Enter the fieldbus interface to which the controller is connected in the **Interface** box (for example: COM1)
6. The **Protocol** box identifies the protocol used by the controller to communicate and should be filled in based on the selected profile
7. Select the addresses where the instruments are to be added
8. Carry out one of the available commands:
   - **Reset**: delete the data entered on the page and begin the entry process again
   - **Continue**: once one or more devices have been selected with the relevant data, continue with the configuration procedure
   - **Cancel**: exit without saving the settings
9. A window opens showing the list of instruments found and you will be able to decide whether to add them or not. You can:
   - **Add and continue with configuration**: add the instruments found and return to the "**Add equipment**” page
   - **Add equipment**: add the instruments found and exit
   - **Cancel**: cancel the save procedure and return to the "**Add equipment**" page

   Note: the instruments, if selected, will be added and the system will not check whether the instrument is present or not. Once the system tries to communicate with the device, it will be highlighted as not reachable (“?” icon).

   When the instrument is available, the icon will become ⓥ
10. Access the panel for the added device and customize its resources (see Customizing device resources)

Removing a device from the network

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. Access the **EQUIPMENT** page.
2. Select the equipment to remove by clicking the box to the left of the name.
3. Click the **Remove** button in the bottom right-hand corner.
4. In the dialog box that appears, click **Remove** to confirm your selection or **Cancel** to cancel the removal process.

Setting an equipment to “Offline” mode

Requirements

- have the necessary permissions to manage the network devices.

Procedure

If a device is disconnected for a long period of time, it can be set to “Offline” mode, preventing alarm notifications from being sent and data from being gathered.
You can proceed in two ways:

1. In the **Device panel**:
   - On the page **EQUIPMENT > Device panel**
   - Activate the **Maintenance** selector switch
   - In the dialog box that opens, set the value “offline” as the duration and click **Confirm**
   - The background of the box **Maintenance** box will turn red.

     Note: on the **EQUIPMENT** page, the panel will now appear with a gray background and the ? icon.
2. On the **EQUIPMENT** page:
   - Access the **EQUIPMENT** page
   - Select the equipment to set as “Offline” by clicking the box to the left of the name
   - Click the **Maintenance** button at the bottom of the page
   - In the dialog box that opens, set the value “offline” as the duration and click **Confirm**
   - The icon to the left of the name of the devices in **Offline** mode will change from ⊘ to ?

Editing the name and attributes of an equipment

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. Access the page **EQUIPMENT**
2. To edit the attributes of a device, proceed as follows:
   - In the "Device panel", select the ••• icon and click **Configure** (one of the shortcut functions) or
   - Access the "Device panel" and click **Edit**.
3. In the window which appears:
   - **Device Name**: used to change the name of the device which appears in the device panel
   - **Product model**: used to enter the device model (Optional)
   - **Serial number**: used to add the serial number of the device (Optional)
   - **External link**: used to enter a reference to a website, a telephone number or an email address
   - **Connection label**: assign a name to the entered link
   - **Add a new category**: list of the categories linked to the device. New categories can be entered by pressing “Add new category”
   - **Remove device**: button for removing the device
   - **Save**: save any changes you have made
   - **Cancel**: cancel and exit without saving the changes

Note: the only required information is "Device name".

Customizing equipment resources

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. On the page **EQUIPMENT > Device panel**
2. Enter editing mode by activating the **Edit** selector switch in the top right-hand corner.
3. The **Resources** panel can be used to:
    - : add a resource to the "foreground" view
    - : add a resource to the "overview" view
    - **UM**: add the unit of measure
    - **HACCP**: add a resource to the HACCP resources
    - **History**: add a resource to the log
    - **Color**: add a color to the resource in chart view mode
    - **Group**: add a resource to a group of resources
    - **Enable**: enable a resource
4. The **Alarms** panel can be used to:
    - : add an alarm to the "foreground" view
    - **Delay**: add a delay in activating alarm indication to the specific alarm
    - **Color**: add a color to the alarm in chart view mode
    - **Enable**: enable an alarm
5. The **Parameters** panel can be used to:
    - : add a parameter to the "overview" view
    - **Value**: edit the value of a parameter by clicking the icon and save it by clicking the icon.
      Note: if the value entered is outside the permitted interval (Min...Max), it will be highlighted in red and you will not be able to save it.
      Note: editing a value could affect other parameters with related values. Always make sure that one or more parameters have not been highlighted in red due to no longer being valid and correct their values as necessary.
6. The **Commands** panel can be used to:
    - : add a command to the "overview" view
    - **Action + Feedback**: carry out a command
    - **Enable**: enable a command

Selecting the resources shown in the device panel

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. On the page **EQUIPMENT > Device panel**
2. Enter editing mode by activating the **Edit** selector switch in the top right-hand corner.
3. In the **Resources** panel, click to add a resource to the “foreground” view (device panel)
4. In the **Alarms** panel, click to add an alarm to the “foreground” view (device panel)

Selecting the resources shown in the overview panel

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. On page **EQUIPMENT > Device panel**
2. Enter editing mode by activating the **Edit** selector switch in the top right-hand corner.
3. In the **Resources** panel, click to add a resource to the "overview” panel
4. In the **Parameters** panel, click to add a parameter to the "overview” panel
5. In the **Commands** panel, click to add a command to the "overview” panel:

Controller parameters

Contents

This section includes the following topics:

Introduction

Parameters can be viewed in two separate panels:

- **Overview**
- **Parameters**

Parameters visible in the “Overview” panel

This panel only shows parameters configured with the ★ icon in the **Parameters** panel
To edit their value:

1. On the page **EQUIPMENT > Device panel > Overview** (☆)
2. click the ✎ icon in the "value” box
3. edit the parameter value
4. save the changes by clicking the icon ✓

Parameters visible in the “Parameters” panel

All visible controller parameters will be shown in this panel.
To edit their value:

1. On the page **EQUIPMENT > Device panel > Parameters** (⚙)
2. click the ✎ icon in the "value” box
3. edit the parameter value
4. save the changes by clicking the icon ✓

Editing parameters (value/description)

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. On page **EQUIPMENT > Device panel > Parameters** (⚙)
2. Activate the **Edit** (⬭) selector switch.
3. Click the ✎ icon in the “value” box for the parameter.
4. Edit the parameter value.
   Note: If the value entered is outside the parameter range, it will be shown in red and you will not be able to save the change.
5. save the changes by clicking the icon ✓
6. Click the ✎ icon in the “description” box for the parameter
7. Edit the parameter description.
8. save the changes by clicking the icon ✓

Saving default parameters

The default map for the various controllers can be saved so that it can be reloaded in the event of a malfunction.

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. On page **EQUIPMENT > Device panel > Parameters** ( )
2. Activate the **Edit** ( ) selector switch.
3. Change the parameter values, if necessary, according to your equipment
4. Click the icon
5. The system will save the controller parameters as a default parameter map

Note: the process saves all instrument parameters regardless of the selections made.

Note: a default map can be saved for each instrument belonging to the network.

Note: if a default map has already been saved, the system opens a pop-up where you can decide whether to continue or stop the process.

Restoring default parameters

The default map for the various controllers can be restored in the event of a malfunction.

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. On page **EQUIPMENT > Device panel > Parameters** ( )
2. Click the icon
3. The system will load and show the default parameter map saved
4. A new column **New value** will appear in the table, to the left of the **Value** column, showing the default values saved
5. The buttons "**Cancel**" and "**Load**" will appear in the top right-hand corner
6. Select the parameters you want to reset using the selection box in the first column.
   Note: to select all of them, click the header box in the first column or do not select any parameters
7. Click **Load** to load the default map or a selection of parameters
8. Click **Cancel** to exit without saving
9. A pop-up will appear advising the save procedure was successful, or containing a message regarding the presence of read-only parameters that cannot be overwritten and that will be highlighted in red
10. Click **Cancel** to end the procedure.

Saving the parameter map to a file

A parameter map containing one or more parameters can be saved in **.dat** format.

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. On page **EQUIPMENT > Device panel > Parameters** ( )
2. Change the parameter values, if necessary, according to your equipment
3. Select the parameters you want to export to the parameter map
4. Click the icon (Save parameter map to file)
5. A window will appear for the selection of a name to be assigned to the file and the destination folder

Loading the parameter map from a file

A previously saved parameter map containing one or more parameters can be loaded in **.dat** format.

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. On page **EQUIPMENT > Device panel > Parameters** ( )
2. Click the icon to load a parameter map from a file
3. A new column **New value** will appear in the table, to the left of the **Value** column, showing the default values saved
4. The buttons "**Cancel**" and "**Load**" will appear in the top right-hand corner
5. Parameters not included in the map you are loading will be highlighted with a red background
6. Select the parameters you want to load onto the controller
7. Click **Load** to load the default map or a selection of parameters
8. Click **Cancel** to exit without saving
9. A pop-up will appear advising the loading procedure was successful, or containing a message regarding the presence of read-only parameters that cannot be overwritten and that will be highlighted in red

Copying parameters to other controllers

One or more parameters can be copied from one instrument to another.

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. On page **EQUIPMENT > Device panel > Parameters** ( )
2. Select with the check-boxes the parameters you want to copy to one or more other controllers. Leave check-boxes unchecked to select the whole parameter map
3. Click the (write on) icon
4. A selection box will open, showing a list of equipment highlighted in various colors:
   - **Green**: instrument compatible (same firmware version (MSK) and model (poles))
   - **Gray**: instrument partially compatible (same firmware version (MSK) and different model (poles))
   - **Orange**: instrument incompatible (different firmware version (MSK)) and not available for selection
5. Select one or more instruments on which to copy the parameters
6. If the instrument is compatible (green) it will proceed with writing the new values. If the instrument is partially compatible (gray) the system will attempt to write the various parameters and will highlight any that are not present or cannot be changed
7. Click **Write on** and wait for the procedure to end.

Printing the parameter map

A **.PDF** file containing all the map parameters can be created.

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. On page **EQUIPMENT > Device panel > Parameters** ( )
2. Click the icon to create a file in PDF format
3. A window will appear for the selection of a name to be assigned to the file and the destination folder
4. The system will confirm creation of the file

Exporting the parameter map

An **.xlsx** file containing all the map parameters can be exported.

Requirements

- have the necessary permissions to manage the network devices.

Procedure

1. On page **EQUIPMENT > Device panel > Parameters** ( )
2. Click the icon to export the file in .xlsx format
3. A window will appear for the selection of a name to be assigned to the file and the destination folder
4. The system will confirm creation of the file

Controller commands

Contents

This section includes the following topics:

Sending a command to a single controller

Procedure

1. Access the **EQUIPMENT** page.
2. Carry out a command in one of the following ways:
   A. Click the menu icon (⋮):
      - scroll through the menu (list of functions and commands)
      - carry out one of the commands by clicking **Execute**

        Note: only the commands selected with the ★ icon in the **Commands** panel appear in the list

   B. Access the panel for the network device:
      - select the **Overview** panel (☆)
      - carry out one of the commands by clicking **Execute**

        Note: only the commands selected with the ★ icon in the **Commands** panel appear in the list

   C. Access the panel for the network device:
      - select the **Commands** panel (▷)
      - carry out one of the available commands.

Sending a command to several controllers

Procedure

1. Access the **EQUIPMENT** page
2. Select the devices to set in maintenance mode by clicking the relevant flags to the left of the device name
3. Click the **Commands** button in the bottom right-hand corner
4. the "**Execute command on...**" window opens
5. In the "**Select a command**" drop-down menu, select the command you want to send
6. In the list of selected commands, the controllers that cannot execute this command will be labeled
7. Click ▷ **Execute** to carry out the command
8. Click **Cancel** to exit without carrying out the command
9. Click **Exit** to exit the window after carrying out one or more commands

Configuring the commands shown and available for use

Procedure

1. On the page **EQUIPMENT > Device panel > Commands** (▷)
2. Activate the **Edit** ( ) selector switch
3. Use the ★ icon to select the commands to be shown in the Overview panel and in the menu (⋮)

Equipment Maintenance and Offline status

Contents

This section includes the following topics:

Setting an equipment to maintenance mode

Requirements

- have the necessary permissions to manage Device maintenance.

Procedure

In maintenance mode, alarm notifications are temporarily silenced for the duration of the maintenance period.
The system will continue to save data but will only begin sending alarm notifications again once the maintenance period is over.
The exception is the **Offline** value setting, where data is no longer saved.
You can proceed in two ways:

1. On the page **EQUIPMENT > Device panel**:
   - activate the **Maintenance** selector switch ( ).
   - in the dialog box that opens, set the anticipated duration and **Confirm**.
     Note: Periods are pre-set and range from 10 minutes to 24 hours. There is also the **Offline** option, which assumes disconnection of the controller.
   - the background of the box **Maintenance** box will turn orange and the text will show the remaining time.
     Note: on the **EQUIPMENT** page, the panel will now show the icon.
2. On the **EQUIPMENT** page:
   - select the devices to set to “Maintenance” by clicking the box to the left of the name
   - click the **Maintenance** button at the bottom of the page
   - in the dialog box that opens, set the anticipated duration and **Confirm**.
     Note: Periods are pre-set and range from 10 minutes to 24 hours. There is also the **Offline** option, which assumes disconnection of the controller.
   - the icon to the left of the name of the devices will change from to

Ending the maintenance period of an equipment

Requirements

- have the necessary permissions to manage Device maintenance.

Procedure

1. On the page **EQUIPMENT > Device panel**
2. Deactivate the **Maintenance** selector switch ( ).
3. The background of the **Maintenance** box will turn white again.
4. The icon associated with the equipment will change from to .

Setting an equipment to “Offline” mode for an unspecified period of time

Requirements

- have the necessary permissions to manage Device maintenance.

Procedure

When one or more devices need to be set as “Offline” for an extended period of time, you can proceed in one of two ways:

1. On page **EQUIPMENT > Device panel**:
   - activate the **Maintenance** selector switch ( ).
   - in the dialog box that opens, set the value “Offline” as the duration and **Confirm**
   - the background of the **Maintenance** box will turn red and the text will show "Device offline".
2. On the **EQUIPMENT** page:
   - select the devices to set as “Offline” by clicking the box to the left of the name
   - click the **Maintenance** button at the bottom of the page
   - in the dialog box that opens, set the value “Offline” as the duration and **Confirm**
   - the background of the devices set as “Offline” will turn gray and the icon to the left of the name of the devices will change from to ?.

Note: if a device is “Offline”, the system will no longer read its data/alarms.

Bringing an equipment back online

Requirements

- have the necessary permissions to manage Device maintenance.

Procedure

1. On the page **EQUIPMENT > Device panel**
2. Deactivate the **Maintenance** selector switch ( ).
3. The background of the **Maintenance** box will turn white again.
4. The icon associated with the equipment will change from ? to .

Logged and temporary data

Contents

This section includes the following topics:

Viewing logged data in tables and charts

Procedure

All users are authorized to view historical reports.
Some functions such as “Save report”, “Edit report” or “Delete report” are only available to individuals with the relevant authorization.
Proceed as follows:

1. Logged data can be accessed:
    - On the **EQUIPMENT** page:
        - select the devices for which you want to view the data by clicking the box to the left of the name
        - click the **History** button at the bottom of the page
        - select a group of resources from those available
        - click **Generate chart** to view the data or **Cancel** to exit.
    - On the page **HISTORY > Reports**
        - click the name of the report you want to view.
2. In the window which appears, you can select:
    - the start date (for example: 24/07/2024 09:02)
    - the time interval to show (instant or with fixed values between one hour and one week)
    - whether to view the data in Table or Chart form
    - whether to view Short-term or Long-term logged data
    - any additional resources (if authorized)
    - whether to show/hide resources by clicking the relevant icon.
3. Click the icon to save a new report that can be reused
4. Click the icon to save changes to the report
5. Click the icon to delete a report
6. Click the icon to print the report in .pdf file format
7. Click the icon to export the report in .xlsx file format

Saving a reusable report

Requirements

- be authorized to configure and program historical reports.

Procedure

To create a reusable report, you can proceed in two ways:

1. On the **EQUIPMENT** page:
   - select the devices for which you want to view the data by clicking the box to the left of the name
   - click the **History** button at the bottom of the page
   - select a group of resources from those available
   - click **View chart** to view the data or **Cancel** to exit.
   - Configure the view as table or chart (see Viewing log data)
   - Click the  icon to create a reusable report
   - Enter the "report name" and click **Save**
2. On page **HISTORY > Reports**:
   - Activate the **Edit** () selector switch
   - Click the  icon to view a new report
   - In the “Add resources” window:
     - select the devices for which you want to view the resources and click **Confirm**
     - select the resources to include in the report from those available
       Note: **Filter resources by description**: used to view resources according to their description
     - click **Add** to confirm or **Cancel** to exit without saving
   - Configure the view as table or chart (see Viewing log data)
   - Click the  icon to create a reusable report
   - Enter the "report name" and click **Save**

Schedule reports

Requirements

- be authorized to configure and program historical reports.
- have configured the server for sending emails (see email servers)
- have an Internet connection with a strong signal.

Procedure

1. On the page **HISTORY > Reports**
2. Activate the **Edit** ( ) selector switch
3. Click the icon in the "Report name" column to edit it
4. Click the icon in the “Scheduling” column
5. In the “Scheduling” window:
   - **Type**: select the report sending frequency from: daily, weekly or monthly
   - **Send on**: select the day of the week on which to send the report (weekly report only).
     Note: the monthly report is always sent on the first day of the month
   - **At**: select the time at which the report will be sent
   - **Send to**: enter the email address to which the report should be sent
   - click **Confirm** to save the changes and **Close** to exit without saving
6. Enable report sending using the **Enable** selector switch ( ) and the date on which the next report is due to be sent will be shown.

Configuring groups of resources for charts and tables

Requirements

- be authorized to configure and program devices.

Procedure

1. On the page **EQUIPMENT > Device panel > Resources**
2. Activate the **Edit** ( ) selector switch
3. Click the icon in the “Groups” column
4. In the box that opens, link the resource with the groups to which it belongs
5. Click the icon to save the changes.
6. Click the **Color** column and assign a different color to each resource for its representation on the chart

Note: one or more groups can be associated with a resource, or an association can be removed.

Note: an existing group can be selected or a new one created simply by entering its name.

Configuring the data recording interval

Requirements

- be authorized to configure and program historical reports.

Information

The system reports the current total number of days of historical data it can store. When the memory is filled, it report also the number of days remaining before deleting the oldest data.

Procedure

1. access the page **SYSTEM > History**
2. enter the **Short recording interval** (short-term data recording frequency) from the relevant drop-down menu
3. click **Historical recording interval** (long-term data recording frequency) in the relevant drop-down menu
4. click **Save** to save the data entered

HACCP

Contents

This section includes the following topics:

HACCP daily dashboard

Requirements

- Have configured one or more HACCP resources (see HACCP configuration)

Procedure

1. On the **HACCP > Dashboard** page
2. The table shows the following information:
   - **Devices**: show the device for which the resource has been selected.
   - **Resource**: show the HACCP resource.
   - **00...23**: show the values of the resources at various times of the current day.

     Note: the icon appears alongside the value if a defrost was active at the moment the reading was taken.

     Note: the icon appears alongside the value if the instrument was in Maintenance mode (but not "Offline") when the reading was taken.
   - **Min**: show the minimum value read.
   - **Max**: show the maximum value read.
   - **Average**: show the average of the read values.
3. Click the icon to change the day for which you want to consult data.
4. Use **Select devices** to filter the read values by instrument.
5. Use **Filter resources by description** to filter the read values according to the resource description.
6. Use **Reset** to cancel any filters set.
7. Use to print the values read for the highlighted day in **.pdf** format.

Schedule HACCP reports

Requirements

- have configured the server for sending emails (see email servers).
- have an Internet connection with a strong signal.
- be authorized to configure and program HACCP reports.

Procedure

1. On the **HACCP > Reports** page
2. Activate the **Edit** () selector switch
3. Click the  icon in the **Scheduling** box and:
   - **Type**: select the report sending frequency from: daily, weekly or monthly
   - **Send on**: select the day of the week on which to send the report (weekly report only).
     Note: the monthly report is always sent on the first day of the month
   - **At**: select the time at which the report will be sent
   - **Send to**: enter the email address to which the report should be sent
   - Click **Confirm** to save the changes and **Close** to exit without saving
4. Click the  **Enabled** selector switch to activate/deactivate report transmission.

HACCP configuration

Requirements

- have configured the server for sending emails (see email servers).
- have an Internet connection with a strong signal.
- have set the HACCP report interval and recipients (see Configuring regular reports).

Procedure

1. On page **EQUIPMENT > Device panel > Resources** ( )
2. Activate the **Edit** selector switch ( ).
3. Click the resource in the **HACCP** column. If selection was successful, the icon will turn green.
   Note: the icon identifies analog resources, asterisks digital resources.
4. Make sure the resource is enabled (**Enable** selector switch active).
5. Make sure the resource **history** is enabled (green tick in the **History** column).

System settings

Contents

This section includes the following topics:

Setting the system and updating the clock

Requirements

- have the necessary permissions to manage system data.

Procedure

1. Access the **SYSTEM** page
2. Click **Information**:
    - In the **Site** part, enter:
        - **Name**: device name (visible in the **EQUIPMENT** panel)
        - **Description**: description identifying the system
        - **Address (Line1/Line2)**: system address
        - **City**: city in which the system is installed
        - **Country**: country in which the system is installed
        - **ZIP/postal code**: postal code for the area in which the system is installed

      Click **Save** to save the data entered
    - In the **Installer contact** part, enter:
        - **Installer name**: name of the person who installed the device
        - **Email address**: email address of the person who installed the device

      Click **Save** to save the data entered
3. Click **Localization**:
    - **System language** system language used to send reports
    - **Import** import new or customized languages (see Manage language translations)
    - **Date format** format used to write the date and time (DD/MM/YYYY HH:mm or MM/DD/YYYY HH:mm)

    Click **Save** to save the data entered
4. Click **Date and time**:
    - select the **time zone** from the drop-down menu (for example: Europe/Rome) and click **Set**
    - enable/disable date and time syncing with an NTP (Network Time Protocol) server

    Click **Sync** to sync with the current device (only active if syncing with an NTP server is disabled).

Note: time updating takes place through connection to a public NTP (Network Time Protocol) server by default.

Note: if **Refrigeration Expert XP** is not connected or will not have access to the Internet, disable NTP mode and sync the clock with the PC clock regularly using the **Sync** button.

Manage language translations

Requirements

- have the necessary permissions to manage languages.
- have the ZIP file with new or customized language translation.

Upload custom language translation

1. On the page **SYSTEM > Localization > Manage Languages**
2. Click "Select file" to load a ZIP file with a new language or a customization of an existing one
    - If the ZIP file is valid and the content does not exceed the available quota for language translations, the system provides a summary of the language file content.
    - Modify the selection of items to upload (frontend: user interface; backend: messages and reports; extra: controller resources descriptions) and continue.
    - The uploaded translation will replace the ones eventually present in the system for the same language.
    - In case the language translation is partial, the system will use, for the missing translation, the system translation for the same language, when available, or English as a backup.
3. The customized language is immediately available and can be configured as System Language.

Remove custom language translation

1. On the page **SYSTEM > Localization > Manage Languages.**
2. Identify the language to from the list and click on the Remove button ( ).
3. Confirm the deletion.

Note: In case the removed language is the one in use, the system will revert to the original language translation, where available, or to English as a backup.

Note: In case the removed language is the System language and there is not an original translation for the same language, the system will switch the System language configuration to English.

System backup and restore

Requirements

- Be the **admin** user or a user in the **Administrator** group.
- Know the password used in the backup process.

Note: the backup password can only be set by the **admin** user.
Note: the backup files are protected and can only be reset via **Refrigeration Expert XP** once the reset key has been confirmed.

Data and system settings backup

1. On the page **SYSTEM > Backup and restore**
2. Click **Generate backup**.
3. This process overwrites any backup file present in the memory of the micro SD for the system; the date and time of the last backup will be shown in the box.
4. Click **Download** to save the backup file in a different location.

Restoring data and system settings

1. Access the page **SYSTEM > Backup and restore**
2. Click **Restore** to restore the file on the memory card.
3. Click "Select file" in the **Load backup file to restore** to load a file in the current system.

Note: when a backup file is loaded, this overwrites anything already saved in the system micro SD card memory.

Note: backup includes the custom languages and custom drivers in use for one or more equipment.

System notification emails

Description

The system sends notification emails to the indicated address in the event of serious errors which could compromise data recording or system operation in general.

If the problem persists, the system will send a new notification every day.

Requirements

- have the necessary permissions to manage system notifications.
- have configured the SMTP server for sending emails (see Configuring the email server).
- have an Internet connection with a strong signal.

Procedure

1. On the page **SYSTEM > System notifications**
2. Enter the **email address** to which alarm indications should be sent
3. Click **Verify email** to make sure it is working properly
4. Click **Save** to save the data entered

Configuring the SMTP email server

Requirements

- have the necessary permissions to manage system data.
- know the email server connection data.
- have read the Cybersecurity Email server recommendation (see Information security configuration recommendations)

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, STATE AND SECURITY

- Change the default passwords to prevent unauthorized access to device settings and information.
- Position the network devices behind various cyber defense levels (firewalls, network segmenting and network intrusion detection and protection systems).
- Adopt cyber security best practices (for example: minimal privileges, separation of functions, secure SMTP, etc.) to prevent unauthorized exposure, loss of or changes to data and registries, the interruption of services or accidental operation.

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

Procedure

1. On page **SYSTEM > Connectivity > Email server**.
2. In the **email** part, enter:
   - **Authentication**: if access to emails requires authentication (None, Simple, Login, Cram-MD5)
   - **Address**: email server address (for example: smtp.gmail.com)
   - **Port**: port used
   - **Sender's email address**: email address of the sender
   - **Name**: username
   - **Password**: user password
   - **Security**: type of security used (None, SSL or StartTLS)
   - **Skip certificate verification**: disable the flag (☐)

   Click **Save** to save the data entered
3. In the **Send test email** part, enter:
   - **Address**: test email address
   - Click **Verify email** to send a test email
     Note: make sure that the message has arrived in the recipient's inbox.

Configuring connectivity

Requirements

- Have the necessary permissions to manage system data.

Procedure

1. On the page **SYSTEM > Connectivity**
2. Click **Ethernet** to:
    - **DHCP**: if DCHP is enabled, all other network parameters can no longer be edited
    - **IP address**: IP address (for example: 192.168.0.52)
    - **Subnet mask**: the subnet mask (for example: 255.255.255.0)
    - **Gateway**: gateway address (for example: 192.168.0.1)
    - **DNS 1**: main DNS address (for example: 8.8.8.8)
    - **DNS 2**: secondary DNS address (for example: 4.4.4.4)

    Click **Apply** to save the data entered
3. Click **mini USB/RNDIS** to view the information for connection via USB
4. Click **Utilities** to check whether there is a network connection:
    - **IP address**: via IP address and then clicking **Ping**
    - **Network name**: via network address and then clicking **Check name resolution**

Manage controller drivers

A controller driver describes how the system reads and writes data to a series of controllers. Each family of controllers is identified by a Firmware MSK.
The system is provided with a large number drivers but new controller, PLC application or third party modbus controllers may require a newer version of an existing driver or a completely new driver.

Requirements

- have the necessary permissions to manage drivers.
- BIN file with the new or updated driver.

Upload custom or updated controller driver

1. On the page **SYSTEM > Software > Drivers**
2. Use the upload button to load the driver BIN file
    - If the BIN file is valid and the new driver does not exceed the driver space of the system, the system prompts with a summary of the new driver and possible replacement of existing one with the same firmware MSK.
    - Continue the upload procedure if the driver upload is not impacting current operations.
    - The new driver will eventually replace the one in the system for the same firmware MSK.
3. The driver is immediately available without further actions.

Remove custom controller driver

1. On the page **SYSTEM > Software > Drivers.**
2. Identify the driver from the list and click on the Remove button ( ).
    - If the driver is currently in use, the system will provide a message and the operation must be aborted.
3. Confirm the deletion.

Updating the software

Requirements

- Have a version of the software (file with ".raucb" extension) that is more recent than the current version.
- Be logged in as the **admin** user or a user belonging to the **Administrator** group.
- Have performed a backup, saving the file to an device external to the **Refrigeration Expert XP** and making sure a backup protection key is provided as this is required for the reset process.

Procedure

1. On the page **SYSTEM > Software > Upgrade**
2. Select the file to upload using the "Select file" button.
3. Select the file destination in the memory (for example: microSD card).
4. Start uploading the file with "Select this memory device".
5. Identify the version you want to install from the list of available software.
6. Click the button "Install this software version" to begin the update.
7. Leave the "Skip data migration" () selector switch disabled if you want to carry out an installation, retaining the current data and configurations.
8. Enable the "Skip data migration" () selector switch if you want to carry out an installation, with the complete deletion of data and configurations.
9. Confirm your selection.
10. Once the update has finished, the system will restart.

Note: it may take several minutes to complete the steps.
Note: the system will retain settings relating to the network IP address and **admin** user password, to allow reconnection to the system with the same network address.
Note: when upgrading the system, Refrigeration Expert restores from the previous version the custom languages and custom drivers in use for one or more Equipment. A newer version of custom languages may be needed to cover new functionalities.

SSL/TLS security certificate management

Description

The controller is provided with a self-signed certificate, which is by default not accepted by the browser.

Requirements

- have the necessary permissions to manage system connectivity network.

Show currently installed SSL/TLS certificate

1. On page **SYSTEM > Connectivity > Certificates**.
2. Click on "**Show CRT certificate**" to display the content of current certificate.

Generate and upload a SSL/TLS certificate

1. On page **SYSTEM > Connectivity > Certificates**.
2. Click on **Generate CSR** to generate and download the current machine unique* Certificate Signing Request file including the required network configuration.
3. Submit the CSR file to the certification authority (either a private network or public certification authority depending on the network configuration). The certification authority will return a valid SSL/TLS certificate (CRT).
4. Click on **Upload CRT** to upload the CRT certificate provided.

Restore self-signed SSL/TLS certificate

1. On page **SYSTEM > Connectivity > Certificates**.
2. Click on **Restore self-signed CSR certificate** to remove and invalidate* any uploaded CRT certificate and re-generate a self-signed certificate for the current Refrigeration Expert.

Note: CSR certificates are unique. Each time a new CSR file is generated, any previous CRT certificate will be invalidated and not reusable.

Support from Eliwell Technical Support

Requirements

- have the Admin permissions.

Description

In case of unexpected operation of the system it is strongly recommend collecting the following information:

1. On page **SYSTEM > Backup and restore**
2. Click on **Generate backup**
3. Click on **Download** to retrieve a complete copy of the system. Not that is it necessary to know the Backup key to use the downloaded file.
4. On page **SYSTEM > Support**
5. Click on **Download trace files** to retrieve a ZIP file containing logs of recent system operation for debugging purposes.

When contacting Eliwell Technical support you may be required to provide the above information.

Eliwell Controls srl
Via dell'Industria, 15 Z.I. Paludi
32016 Alpago (BL) Italy
Telephone +39 (0) 437 166 0000
www.eliwell.com

Customer Technical Support
Telephone +39 (0) 437 166 0005
E techsuppeliwell@se.com

Sales office
Telephone +39 (0) 437 166 0060 (Italy)
Telephone +39 (0) 437 166 0066 (other countries)
E saleseliwell@se.com

REX00_01EN - Refrigeration Expert XP - EN - 06/2025