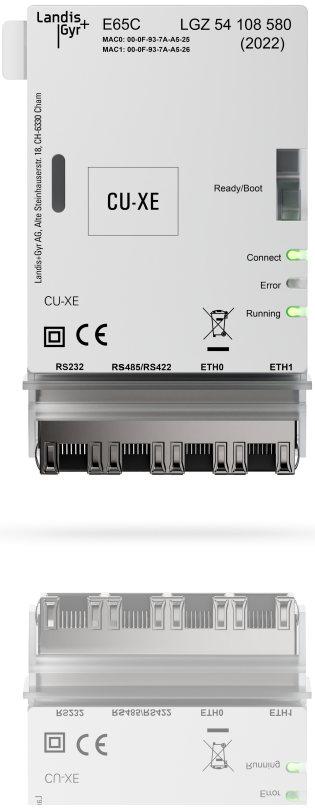
Communication

Industrial and commercial

Communication module

E65C CU-XE

User manual



Date: 15.03.2022
D000062528 f en 1.8

© Landis+Gyr

Revision history

Version	Date	Comments
a	10.07.2018	First edition. Release 1.
b	27.08.2018	Second edition. Updated Landis+Gyr Root Certificate Authority link.
c	06.12.2018	Third edition.
d	06.08.2019	Updated section *5.1 "Installation in a meter"*.
e	31.03.2020	Adaptations for Release 2. Sections *2.4.1, 2.4.2, 5.1, 5.3, 5.4,* and *9* updated. Sections *5.4 "Updating the CU-XE from release 1 to release 2"*, and 10 "Third-party software used and open source (OS) software licenses" added.
f	15.03.2022	Adaptations for release 2.3.1. Manual structure and layout updated. Event log, data log, protocol conversion and routing added.

Although the information contained within this document is provided in good faith, Landis+Gyr (including its affiliates, agents and employees) repudiates any and all liability for any errors, inaccuracies or incompleteness relating to the product. Landis+Gyr provides no warranty, representation or guarantee with regard to the performance, quality, lifetime or suitability of the products for any particular purpose. To the fullest extent permitted by law, Landis+Gyr disclaims (1) any and all liability arising out of or in connection with the use of the product, and (2) any and all liability, including, but without limitation, special, consequential and indirect damages and losses, and (3) any and all implied warranties, including, but without limitation to, fitness for purpose and merchantability.

All images, drawings, diagrams, technical descriptions, information and specifications contained in this document (the “Content”) constitute the intellectual property of Landis+Gyr. All rights are reserved. Any distribution, duplication, amendment, and any other kind of use of the Content or its reproduction in whole or in part is only permitted with the prior written consent of Landis+Gyr. The Content is strictly confidential and intended solely for the addressee.

All product information may be changed at any time without prior notification.

Table of contents

1 About this document

Range of validity

This User Manual applies to E65C CU-XE communication modules hereinafter referred to as “CU-XE”.

Purpose

This User Manual supplements the operating instructions of the electricity meter and is incomplete without the data contained therein. Together with the meter operating instructions, the User Manual contains all the information necessary for the operation of the CU-XE communication module for its intended purpose. This includes:

- Provision of knowledge concerning the characteristics, construction and function of the CU-XE communication module
- Information about possible dangers, their consequences and measures to prevent any danger
- Details concerning the performance of all work throughout the service life of the CU-XE communication module (installation, commissioning, operation, maintenance, decommissioning and disposal)

Target group

The contents of this User Manual are intended for technically qualified personnel of energy supply companies responsible for system planning, installation and commissioning, as well as the operation, maintenance, decommissioning and disposal of the communication modules.

Reference documents

The Technical Data and the Functional Description of the CU-XE communication module can be found in the following documents:

- D000062527 E65C CU-XE Technical data en
- D000062529 E65C CU-XE Functional description en

Terms and abbreviations

A list of terms and abbreviations used in this User Manual is available at the end of this document.

© Landis+Gyr

2 Safety

This section describes the safety information used in this manual, outlines the responsibilities and lists the safety regulations to be observed.

2.1 Safety information

The following symbols are used to draw your attention to the relevant danger level, i.e. the severity and probability of any danger, in the individual sections of this document.

Warning
Used to indicate a dangerous situation that could cause bodily injury or death.

Caution
Used to indicate a situation/action that could result in material damage or loss of data.

Note
Used to indicate general guidelines and other useful information.

In addition to the danger level, safety information also describes the type and source of the danger, its possible consequences and measures for avoiding the danger.

2.2 Responsibilities

The owner of the communication modules – usually the utility company – is responsible for assuring that all persons engaged in working with meters and communication modules:

- Have read and understood the relevant sections of the user manual.
- Are appropriately qualified for the work to be performed in accordance with national regulations (see ISSA "Guideline for Assessing the Competence of Electrically Skilled Persons").
- Strictly observe the safety regulations (laid down in section Safety regulations and the operating instructions as specified in the individual sections.

In particular, the owner of the meters and communication modules bears responsibility for the protection of persons, prevention of material damage and the training of personnel.

For this purpose, Landis+Gyr provides training on a variety of products and solutions. Contact your local Landis+Gyr representative for more information.

2.3 Safety regulations

The following safety regulations must be observed at all times:

- Only appropriate tools shall be used for the job. This means, e.g. that the screwdriver must be of the correct size for the screws, and the handle of the screwdriver must be insulated.
- Devices that have been dropped must not be installed even if no damage is apparent, but must be returned to an authorised service and repair centre (or the manufacturer) for testing. Internal damage may result in malfunctions or short-circuits.

- Communication modules must not be cleaned under running water or with compressed air. Water ingress can cause short-circuits or damage components.

In addition, the safety instructions given in the User Manuals for the meter are also applicable.

Landis+Gyr hereby declares that the radio equipment type CU-XE is in compliance with Directive 2014/53/EU. The full text of the EU Declaration of Conformity is available at the following internet address: https://www.landisgyr.eu/product/landisgyr-e65c-cu-series/.

© Landis+Gyr

3 Device description

3.1 Field of application

The CU-XE communication module can be installed in and uninstalled from the following Landis+Gyr meters without opening the calibration seal:

- E650 ZxD300/400xT industrial and commercial meters
- E850 ZxQ high-precision meters
- S650 SxA300/400xT and SMA500 Smart Grid Terminals
- E65C CU-ADPx adapters

3.2 Characteristics

The CU-XE communication module contains two independent Ethernet interfaces, one RS-232 serial interface and one RS-422/RS-485 serial interface . The device also contains a powerful application processor for networking, security and data processing functionalities.

3.3 Type designation

The type designation of the CU-XE communication module is added to that of the meter (see meter User Manual), but is not shown on the main faceplate of the meter. The type designation is inscribed on the case of the communication module and can be seen through the front door of the meter through an opening in the tariff faceplate.

The CU-XE communication module is available in the following versions:

Type	Ethernet	RS-485/RS-422	RS-232
E65C CU-XE	•	•	•

3.4 Functions

The Functional Description of the CU-XE communication module is provided separately. The main functions are briefly summarised below.

3.4.1 Ethernet interfaces

The communication module offers two Ethernet interfaces supporting 100BASE-TX and 10BASE-TX. Depending on the Ethernet interface used, the communication module offers various services. The two Ethernet interfaces can be configured independently. This configuration is defined during the ordering process and can be changed during operation.

3.4.2 RS-485/RS-422 interface

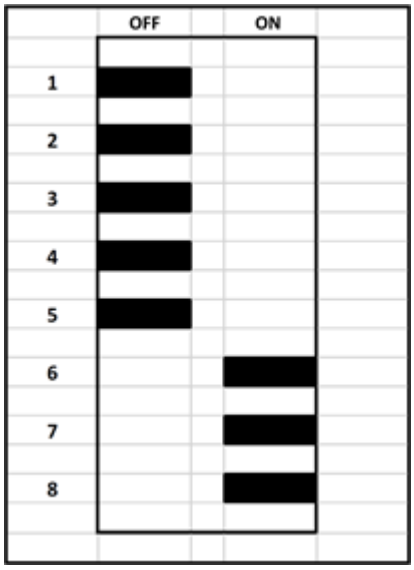
The RS-485/RS-422 interface is a serial, bi-directional, differential interface. The interface includes user configurable bias and termination resistors. A typical application is to create a multi-drop bus, where multiple devices can share the communication channel. For example, up to 31 E650 meters can be connected to the RS-485 bus configured as the bus master, and they can be read remotely using the Ethernet interface.

To configure the RS-485/RS-422 operational mode as well as the bias and termination resistors, DIP switches on the backside of the PCB can be used. The DIP switches are accessible only when the CM is removed from the meter.

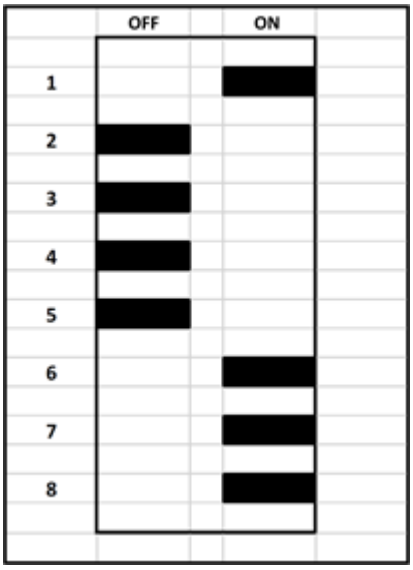
Legends for the scenarios below:

DIP switch	Function
Position 1	ON = rx termination enabled, 120 Ω
Position 2	ON = tx termination enabled, 120 Ω
Position 3	ON = bias enabled
Position 4	ON = bias enabled
Position 5	ON = Manufacturer access
Position 6	ON = used as RS485 (half-duplex); OFF = used as RS422 (full-duplex)
Position 7	ON = used as RS485 (half-duplex); OFF = used as RS422 (full-duplex)
Position 8	ON = used as RS485 (half-duplex); OFF = used as RS422 (full-duplex)

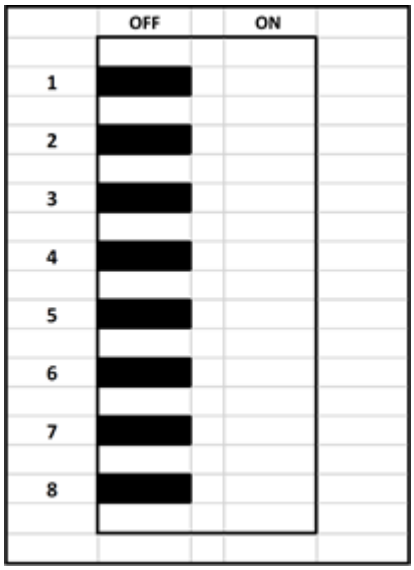
RS-485 Half-duplex not terminated:



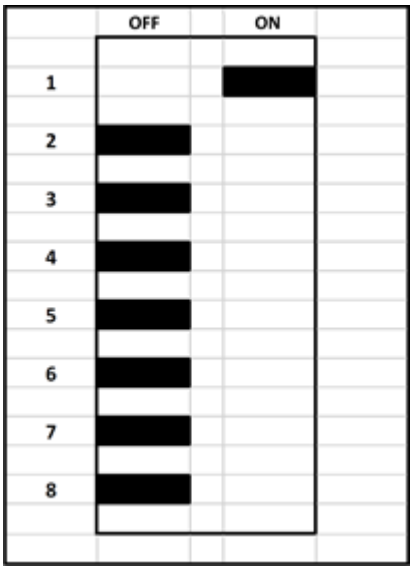
RS-485 Half-duplex terminated:



RS-422 Full-duplex not terminated:



RS-422 Full duplex terminated:



3.4.3 RS-232 interface

The RS232 interface is a serial, bi-directional, full-duplex interface.

3.4.4 Base meter interface

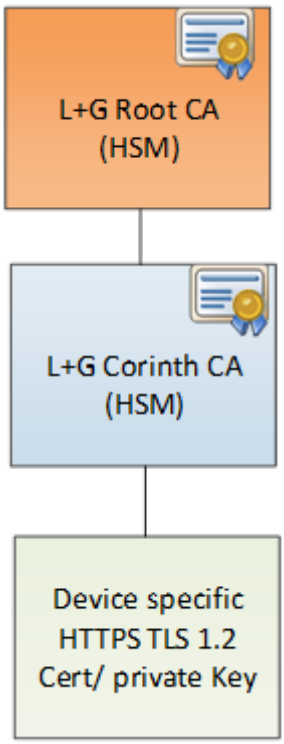
The communication module has a two-channel interface to connect to the base meter that is hosting the communication module.

3.5 Security features

The communication module is configured from production with certificates from the Landis+Gyr root certificate authority. The Landis+Gyr Root CA is available under the Landis+Gyr EMEA Root Certificate RSA-4096 at:

https://www.landisgyr.com/webfoo/wp-content/uploads/2013/12/rsa4096-root-ca-cert.pem

Add this certificate to the root certificates of your system to be able to verify the server in a TLS connection to the communication module.



4 Mechanical construction

4.1 Overview

The CU-XE communication module is a complete unit with its own plastic case.

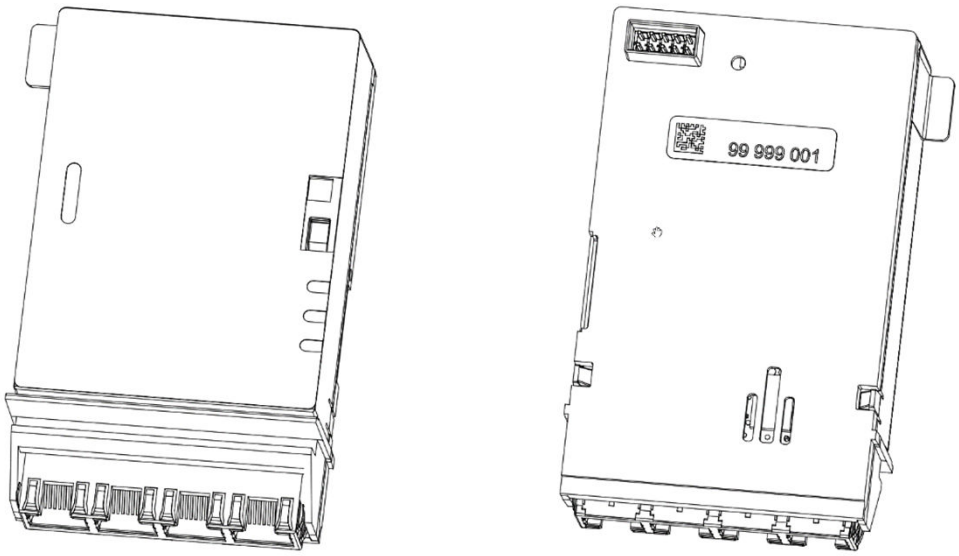


Figure 1: Front and back of the communication module

The faceplate of the communication module installed in the meter is visible when the meter front door is open.

External connections are situated underneath the unit, while a 10-pin connecting plug at the rear provides a connection to the meter electronics.

Four LEDs on the circuit board indicate when the communication module is booting or ready, when it is connected, when there is an error and when the communication module is running properly.

The communication module has no seal of its own. It is secured by the utility seal of the meter.

4.2 Antenna and interface connections

4.2.1 CU-XE connections

The CU-XE communication module has the following four interface connections:

#1: Ethernet port 1

#2: Ethernet port 0

#3 RS-485/RS-422

#4: RS-232

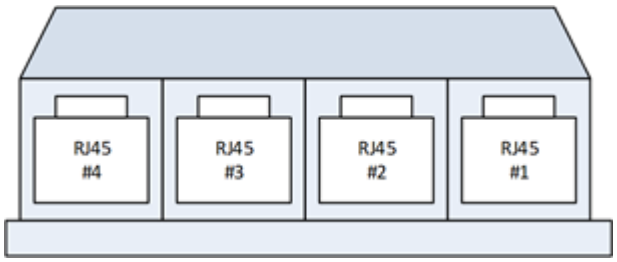
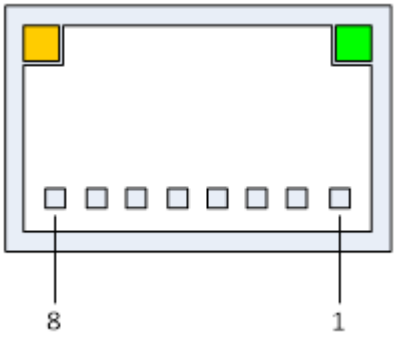


Figure 2: CU-XE interface connections

The RJ45 sockets of Ethernet ports 1 and 0 have the following pin assignment:

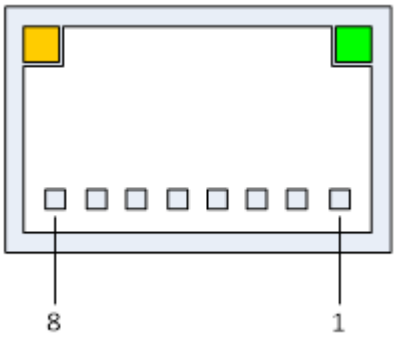


1	TxD+
2	TxD-
3	RxD+
4	not used
5	not used
6	RxD-
7	not used
8	not used
green	link

The orange led shows the speed of the connection and if it is on then it is indicating the 100Mbit connection, otherwise it is referring to 10Mbit connection.

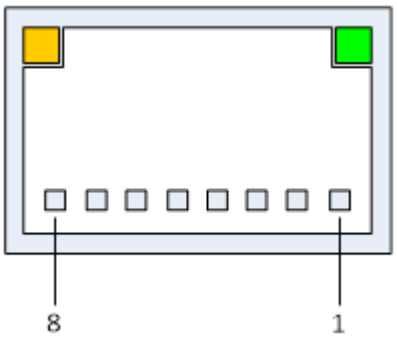
The green led is showing the link activity on the RJ45 socket. On status indicates the link is on and is blinking when data transmitted or received.

The RJ45 socket of the RS485/RS422 interface has the following pin assignment:



1	not used
2	GND
3	Tx+
4	Tx-
5	Rx-
6	Rx+
7	GND
8	not used
green	link

The RJ45 socket of the RS232 interface has the following pin assignment:



1	DSR
2	DCD
3	DTR
4	GND
5	RxD
6	TxD
7	CTS
8	RTS
orange	speed
green	link

4.3 Faceplate

The faceplate of the E65C CU-XE communication module:

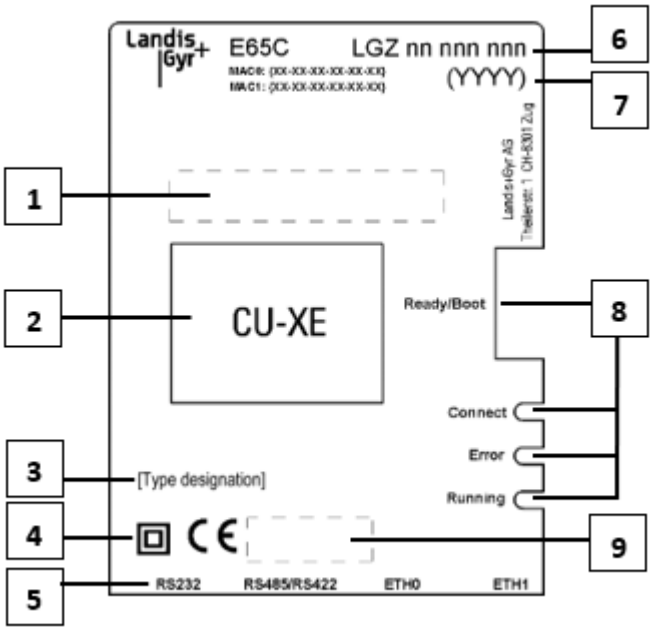


Figure 3: Faceplate of the CU-XE communication module

1. Warning plate (country-specific)
2. Type designation
3. Type designation (property information
4. Insulation class and CE mark
5. Interface inscriptions
6. Serial number
7. Year of manufacture
8. LEDs and LED inscriptions
9. Certification information

The faceplate may also contain customer-specific and country-specific data, e.g. warnings.

4.4 LED status descriptions

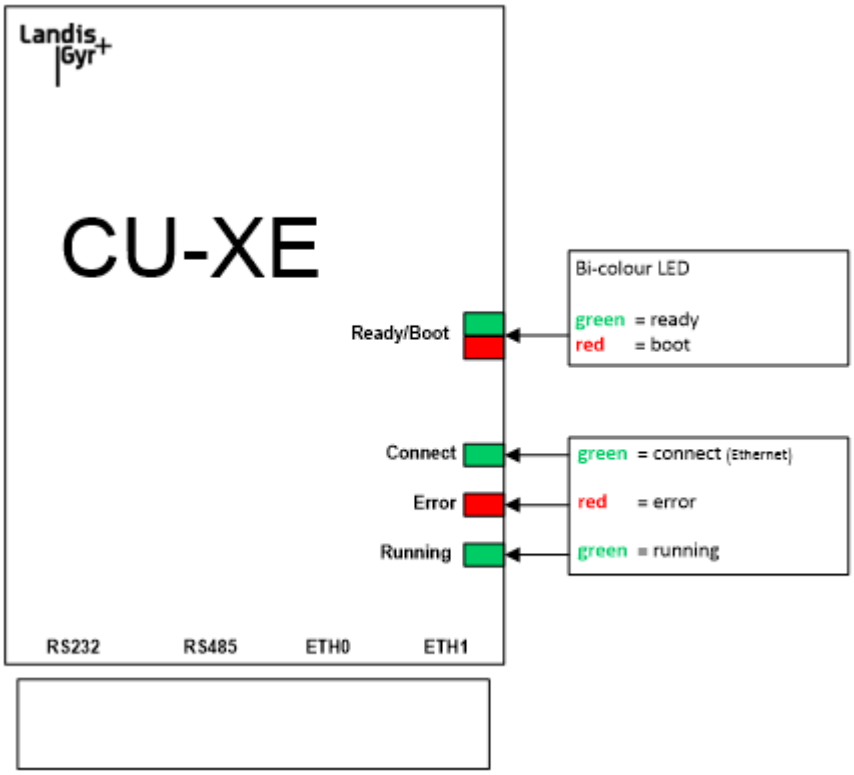


Figure 4: LEDs on the communication module

4.4.1 Power-up

During power-up, all LEDs are switched on. If the system is running, the LEDs display the behaviour described in sections below.

4.4.2 Connect LED

The Connect LED can be viewed by the user with meter cover closed. It is switched on when one or more application level TCP connections are established. This applies to all components that are used for transporting process data (SCADA protocols and the passthrough mechanism are examples) but excludes transient TCP connections like the main or management connections and VPN tunnels.

4.4.3 Boot LED

The Boot LED is the red part of the bi-colour Ready/Boot LED. It is switched on when the CU is booting and switched off during normal operation

4.4.4 Ready LED

The Ready LED is the green part of the bi-colour Ready/Boot LED. It is switched off during start-up and blinks in pulses once the application has fully started.

4.4.5 Ethernet LEDs

The orange and green Ethernet LEDs indicate speed and link state.

5 Installation/uninstallation

5.1 Installation in a meter

Warning

No voltage to the meter during installation

In order to avoid hazardous electric shocks, make sure that there is no voltage applied to the meter when installing the communication module. Contact with live parts is dangerous to life. Disconnect the meter from the power supply as described in the meter User Manual.

Note

Excessive number of power failures reduces life of product

The CM writes to its internal flash memory every time there is a power failure. This type of memory has a life expectancy of approximately 100,000 write cycles. This is not a guaranteed value. During a lifespan of 15 years this would amount to approximately 15 power failures per day. Exceeding this number may shorten the useful life of the product.

Note

E65C CU-XE communication modules can be used in E650 (from Series 3 FW version B30 upwards), S650 and E850 electricity meters or in CU-ADPx adapters

The CM is designed to be operable with meters mentioned above. The CM should not be operated with other devices even if it can be inserted to the device. Compatibility with other devices cannot be guaranteed.

Install the communication module in a meter as follows:

1. Make sure that no voltage is applied to the meter.
2. Remove the utility seals on the front door and terminal block cover.
3. Open the front door and remove the terminal block cover.

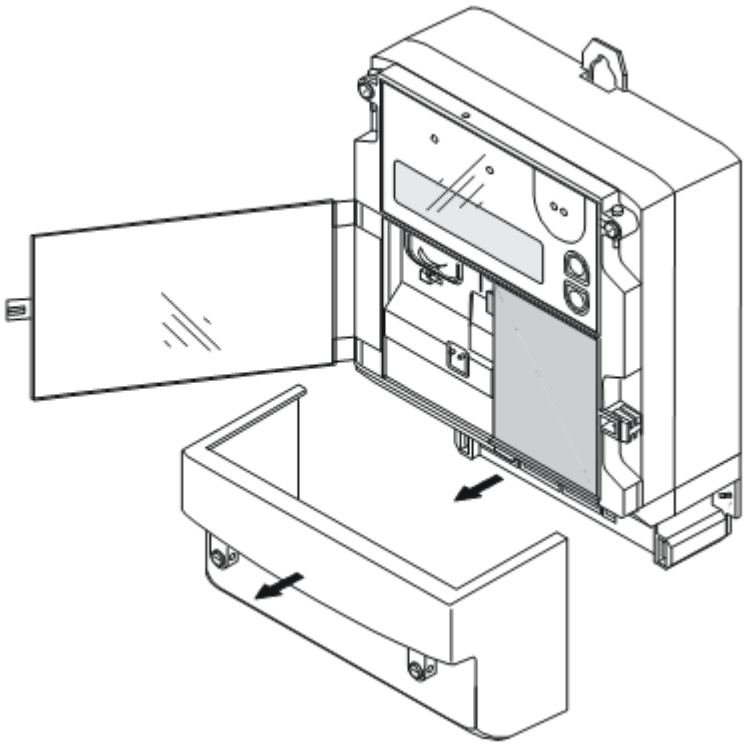


Figure 5: Preparing the meter for the installation of the communication module

4. Remove the built-in dummy communication module.
5. Insert the communication module carefully into the space provided in the meter. Ensure correct fitting of the connector.

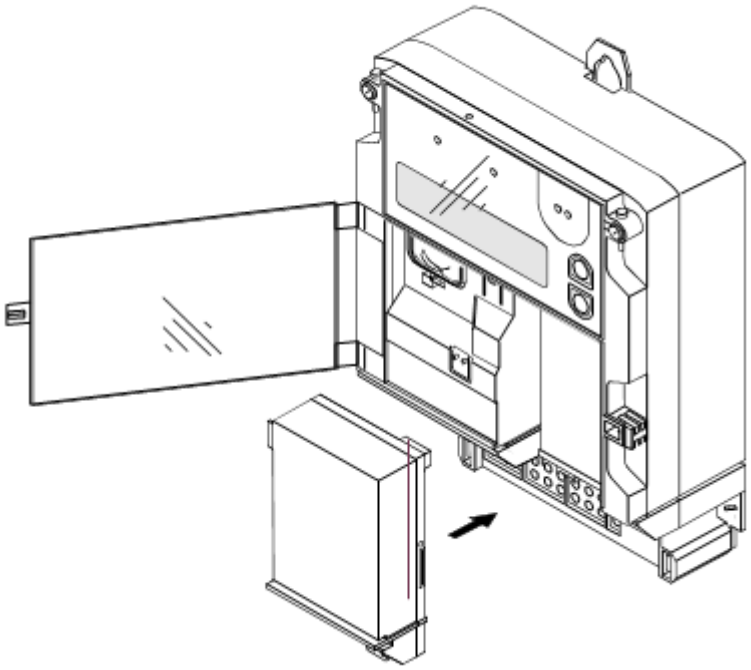


Figure 6: Installing the communication module in the meter

6. Close and seal the front door.
7. Connect to the Web UI, see section Accessing the Web UI on page 19 for more information.

8. Change the initial password that was specified prior to order confirmation. See section My settings / password on page 52.

5.2 Connecting the communication module

5.2.1 Connecting the RS-485 interface

1. Insert the connecting cable with the RJ12 connector to the socket labelled RS-485/RS-422 in the communication module until the connector engages.
2. Connect the other end of the cable to the nearest unit of the RS-485 multiple connection.

   The RS-485 interface of the CU-XE is provided with one RJ12 socket. Extensions for the RS-485 must therefore be formed with an external splitter.

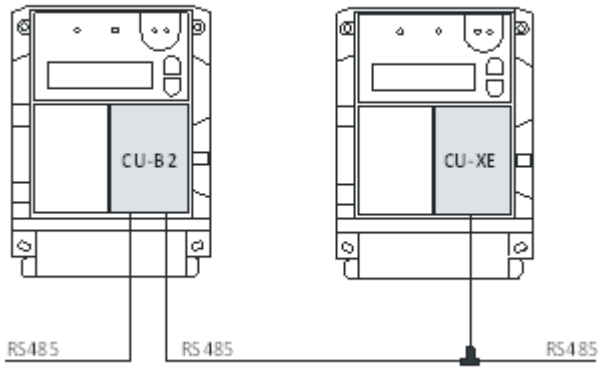


Figure 7: Connecting multiple communication modules

Caution

External wiring of RS-485

In order to function correctly, all 3 wires (data a, data b and common GND) must be connected. RS-485 operation with only 2 wires (without common GND) is forbidden as the RS-485 interface may not function correctly or may even get damaged.

5.2.2 Resealing the meter

After all connections have been made and the device is properly configured, you can replace the covers and reseal the meter with a utility seal.

5.3 Commissioning and functional check

The CU-XE communication module should be taken into operation as follows (see also section Operation on page 19 for a detailed description of LED states):

1. After switching on the mains voltage, a red boot LED is blinking. When the communication module is ready for operation, the LED switches to green. When the Ethernet connection is made, the running LED is illuminated.
2. A remote readout of meter data via Ethernet should be performed as a functional check if the CU has been appropriately configured.
3. If a multiple connection to further devices is used, check that they are working as expected.

5.4 Removal or exchange of communication module

The communication module is exchanged or removed from the meter in reverse order of the installation (see sections Installation in a meter on page 15 and Connecting the communication module on page 17).

6 Operation

The CU-XE communication module features four LEDs to display operational status information. These LEDs are visible through the transparent plastic housing on the right side of the faceplate. Refer to LED status descriptions on page 14 for more information.

Note

After configuration change the power cannot be cut off for 10 seconds, otherwise the CM can be damaged.

6.1 Accessing the Web UI

To ease installation and maintenance, the communication module features a Web UI. The Web UI is accessible on the ethernet interface ETH1 and/or ETH0 and modem, depending on the configuration, using a standard, up-to-date web browser (e.g. Chrome, Firefox or Edge).

Note

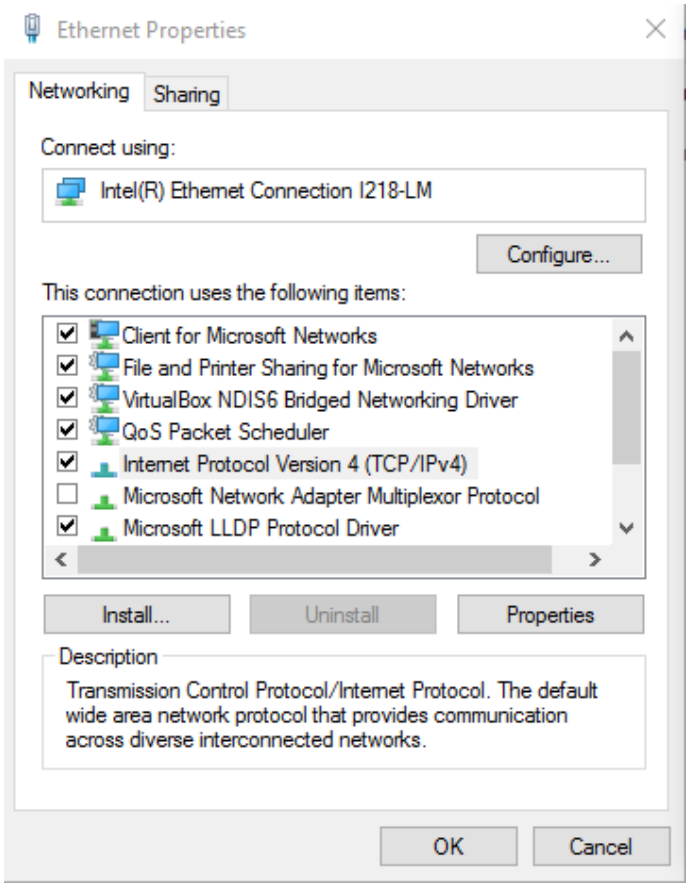
The Web UI is not accessible over the optical port nor the RS485 interface

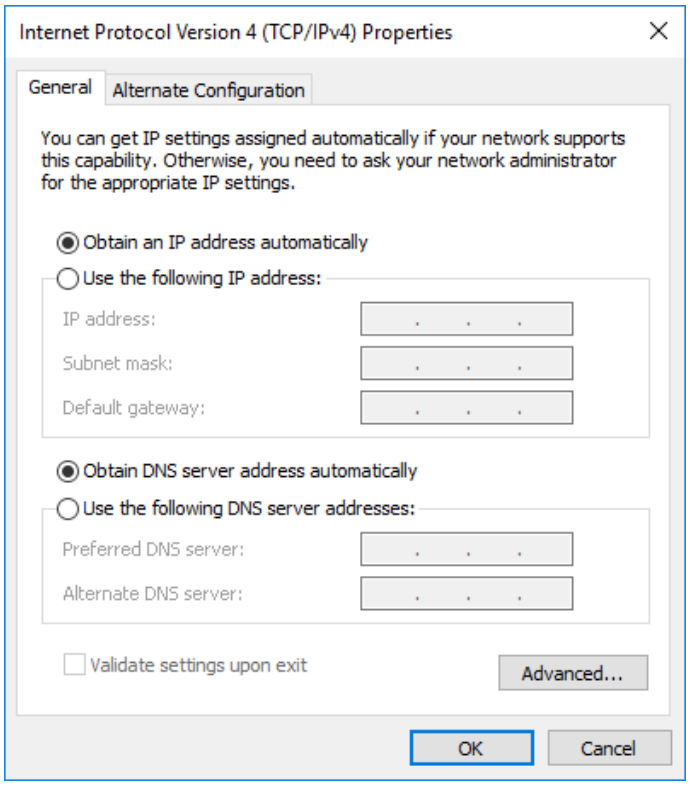
The Web UI is only accessible over ethernet interfaces.

The ethernet interfce ETH0 and ETH1 can be configured in multiple ways, refer to Ethernet ports on page 32 for more information.

6.1.1 Management port on ETH1

If the management port is enabled, it is accessible on the ETH1 interface at IP address 172.16.0.1 or at https://hostname.landis. The management port features a DHCP and DNS server. Establishing the connection is easier if the ethernet interface of the PC is set in DHCP mode. See the example below from Windows 10 settings (click **Start** > **Settings** > **Network & Internet** > **Ethernet** > **Change adapter options**).





How to access communication module with, for example, manufacturer serial number 58703388 and management port enabled:

1. Configure the ethernet interface to DHCP mode.
2. Connect to the ethernet interface ETH1 of the communication module.

3. Enter either the IP address of the management port or use https://hostname.landis to access the Web UI login page.
   a) IP address: https://172.16.0.1
   b) Hostname: https://LGZ58703388.landis
4. Provide your username and password at the login page.

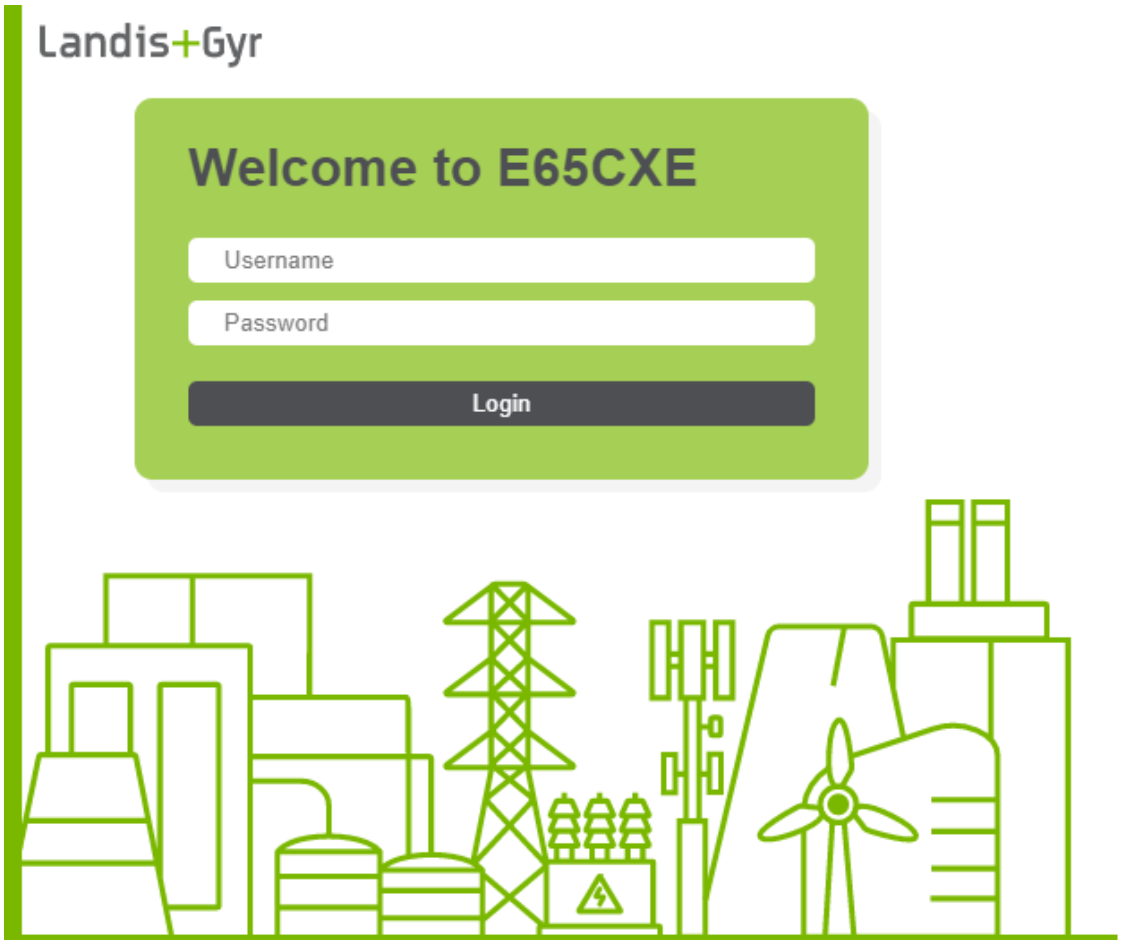


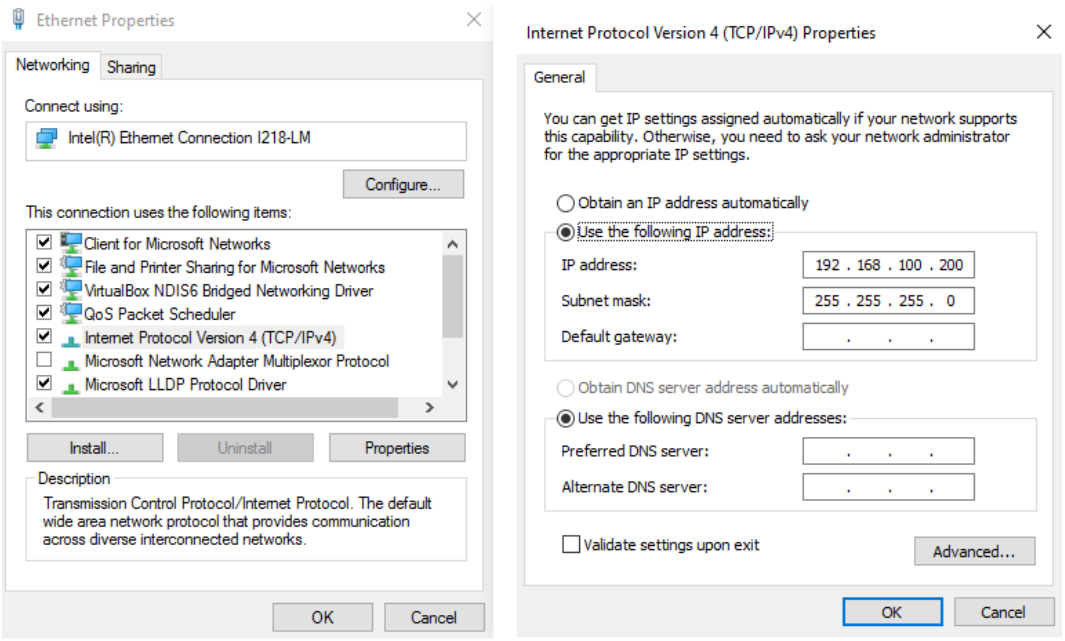
Figure 8: Login page

6.1.2 Static IPv4 address

This section explains how to access the Web UI when ethernet interfaces (ETH0, ETH1 or bridged as BR0) are configured with a static IP address.

Example: Communication module with ETH0 configured to a static IP address 192.168.100.100.

1. Configure the ethernet interface to an IP adress in the same range as ETH0, e.g. 192.168.100.200.



2. Connect to the ethernet interface ETH0 of the communication module.
3. Enter the IP address of ETH0 into the web browser: https://192.168.100.100.
4. Enter your username and password on the login page.

For more information about the different configuration options of the ethernet interfaces, refer to Ethernet ports on page 32.

6.1.3 Dynamically assigned IPv4 address

This section explains how to access the Web UI when the communication module is connected to a network where the IP address is assigned by a DHCP server from the network.

For more information about the different configuration options of the ethernet interfaces, refer to Ethernet ports on page 32.

Example: a communication module with manufacturer serial number 58703388, and ETH0 configured to DHCP and connected to a LAN where the assigned IP address is 10.41.4.34.

1. Make sure the PC is connected to the LAN.
2. Enter the IP address of ETH0 into the web browser: https://10.41.4.34.
3. Enter your username and password on the login page.

Depending on the IT network infrastructure settings, the device may be accessible over the hostname and domain (DNS suffix the network assigns): Instead of entering the IP address you could use https://LGZ58703388.example.net.

6.2 Device information, status and configuration

After accessing the Web UI, you can log in using the username and password.

In order to make changes on the configuration:

1. Click **Enter configuration mode** at the top of the page.

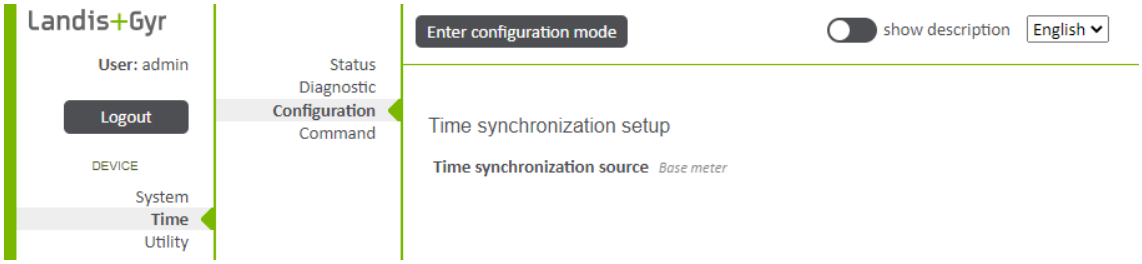


Figure 9: Configuration mode

2. Make your configuration change.
3. Click **Save**.

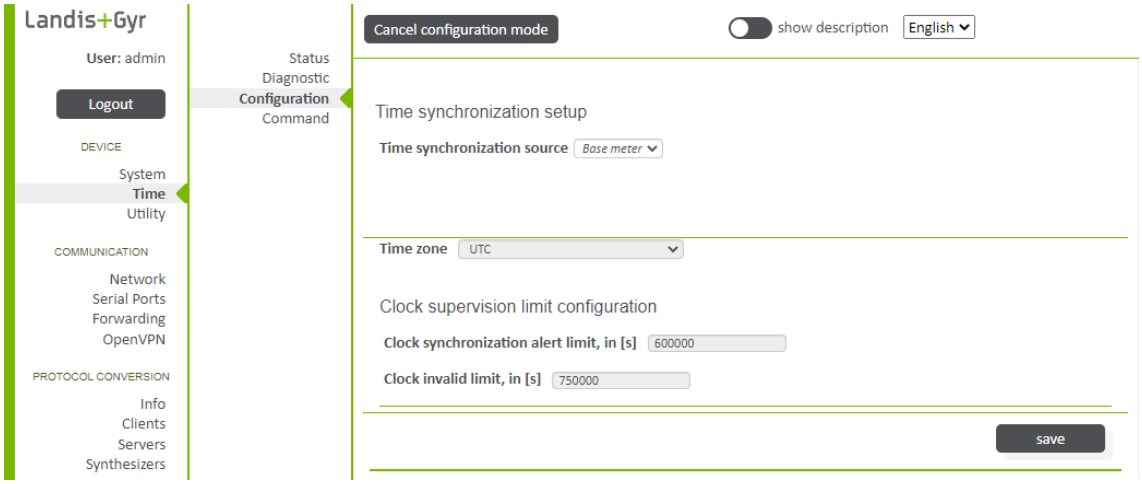


Figure 10: Configuration mode - Save

4. Repeat steps 2 and 3 on each menu page you would like to change.
5. Click **Apply configuration change** at the top of the page to confirm the changes.

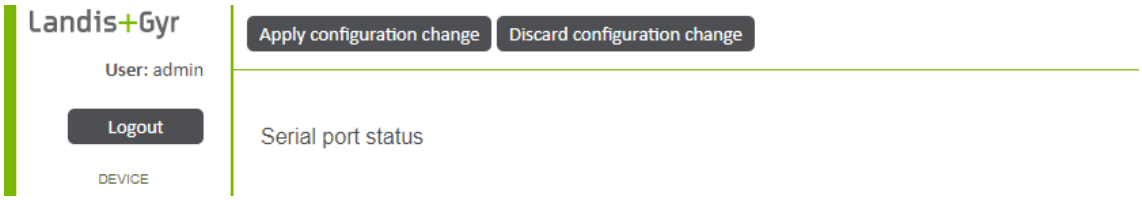


Figure 11: Apply/Discard configuration change

Note

Additional description

Every menu page on the Web UI provides an additional description of the functions to be configured. This additional description can be enabled by clicking the **Show description** slider at the top of the Web UI.

Note

Entering configuration mode simultaneously by several users is not possible. The button "Cancel configuration mode of user '*username*'" discards all changes made by '*username*'.

Note

Applying configuration changes might cause components in the device to be stopped and restarted. Depending on the components this might take a few minutes.

6.2.1 System

6.2.1.1 System information

Under **Device** > **System** > **Info** the manufacturer serial number, firmware version, installed feature licenses and the operation status of the communication module are shown.

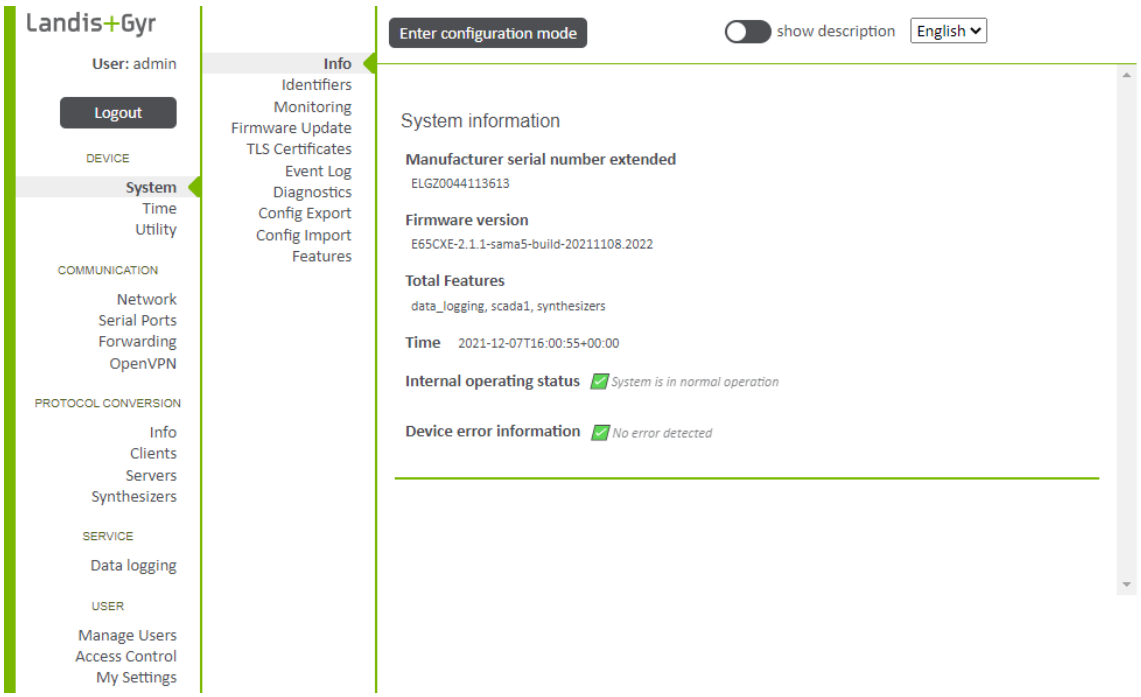


Figure 12: Device > System > Info

The system information page is updated automatically approximately every 3 seconds.

6.2.1.2 Device identifiers communication module

Under **Device** > **System** > **Identifiers**, you can view all the device identifiers, firmware package versions, hardware identifiers and production information.

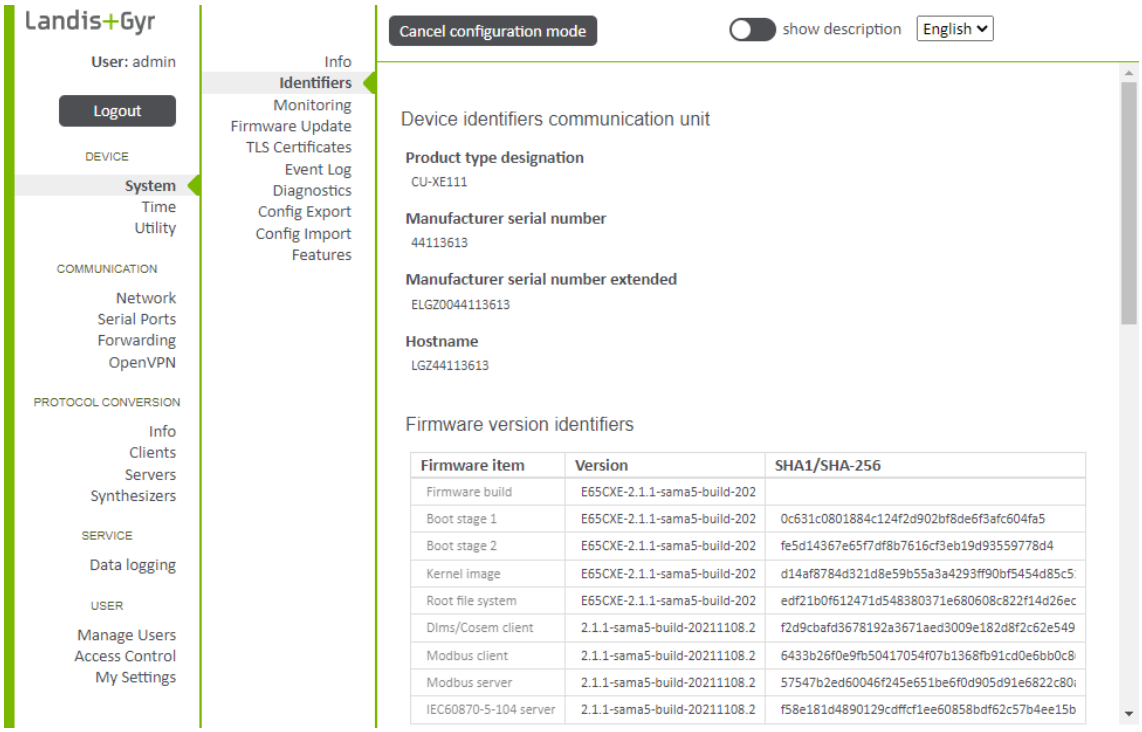


Figure 13: Device > System > Identifiers

6.2.1.3 System monitoring

Under **Device** > **System** > **Monitoring** you can view the system load, resource usage, device traffic, actual system temperature and the time since last system start.

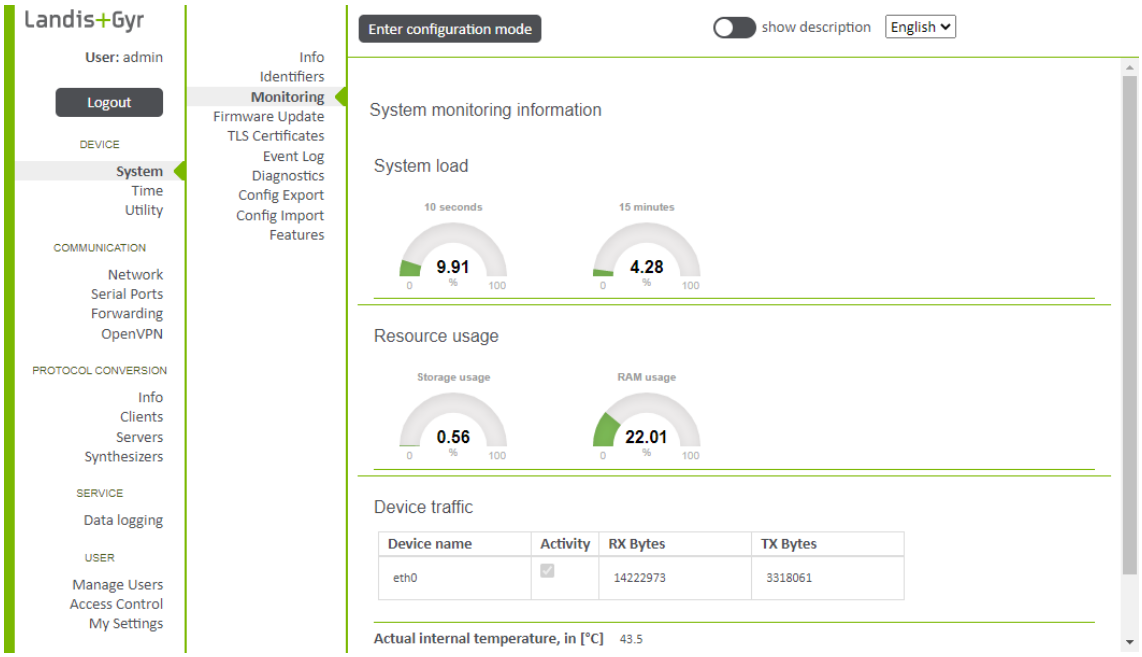


Figure 14: Device > System > Monitoring

The system information page is updated automatically approximately every 3 seconds.

6.2.1.4 Firmware update

Note

Check firmware update compatibility

Make sure that the update package is compatible with the device and the installed firmware. If you are not sure about the compatibility, contact Landis+Gyr before update.

The current firmware versions of the communication module are displayed on the identifiers page (**Device** > **System** > **Identifiers**).

The firmware can be updated using one of two update packages:

Regular update package	Consists of all the files of the new version.	Used when the update is done over higher bandwidth channel. Faster installation process.
Delta update package	Consists of only the files that have changed from the previous version.	Used when the update is done over lower bandwidth channels.

Independent of uploading a regular package or a delta package it is possible to upload either the full file (**Network type** > “High speed and reliable”) or smaller chunks (**Network type** > “Typical speed” or “Low speed”). A chunked upload has the advantage that it is resumable if the upload gets interrupted. Already uploaded chunks are persistently stored in the device.

1. To update the firmware of the respective communication module, go to **Device** > **System** > **Firmware Update**. In the Firmware upload section, two options are offered:
   - Drag and drop the firmware package into the grey box or
   - Click **Choose file** to open the **File Select** window.
2. Select the appropriate speed from **Network type** drop-down list.
   a) **High speed and reliable**, with this option the full file is uploaded. The upload is not resumable, if interrupted. Recommended option when the upload is done over higher bandwidth channel.
   b) **Typical speed**(default), with this option the file is uploaded in small chunks. The upload is resumable, if interrupted. Recommended option if there is no reason to use the high or low speed options.
   c) **Low speed or unreliable**, with this option the file is uploaded in small chunks. The upload is resumable, if interrupted. Recommended option when the upload is done over lower bandwidth channel and/or weak reception quality.
3. Click **Upload**. After a successful firmware package upload, the package is validated (integrity, authenticity, compatibility), unpacked and installed. Depending on the size of the update, this might take up to 15 minutes. The version and progress of the update are displayed.
4. To activate the new firmware, click **Activate**, or alternatively, configure an activation scheduler.

   The communication module will only execute the update after the successful validation of the firmware. The communication module restarts automatically to activate the new firmware. After activation, the new firmware version will be indicated under the **Info** and **Identifiers** sections of the Web UI.

Note
Log in again after the communication module restarts. Then make sure that the new firmware version has been activated.

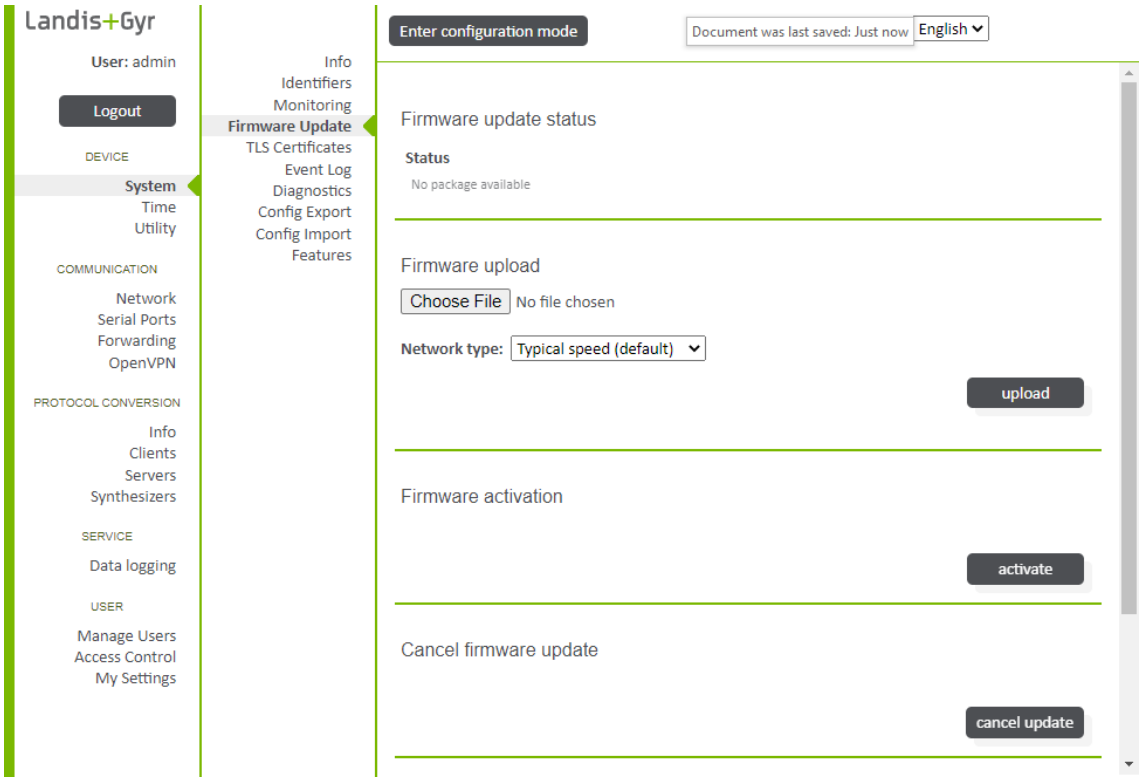


Figure 15: Device > System > Firmware Update

6.2.1.5 HTTP TLS key and certificate in use

In the HTTP TLS key and certificate section (**Device** > **System** > **TLS Certificates**), you can upload a new certificate and private key for TLS. After the new certificate or private key has been applied, reload the Web UI as the new certificates are used immediately.

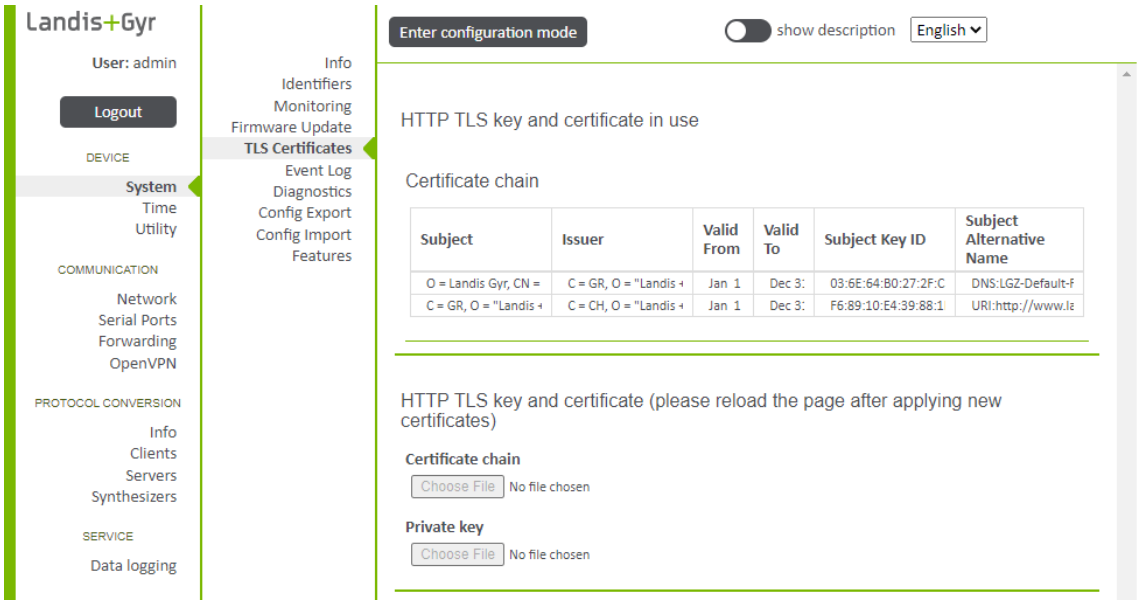


Figure 16: Device > System > TLS Certificates

Note
Restricted use of fallback certificate on the Web UI

In very rare cases (in which the configured certificate is not valid), a fallback certificate will be used on the Web UI. Such cases can be detected by a warning in the browser about an unsecure connection. Landis+Gyr cannot guarantee the security of the connection in such cases and therefore a new certificate should be installed immediately.

6.2.1.6 Event log

In the event log section (**Device** > **System** > **Event log**), you can view or download logs of events. The logs show timestamps, event IDs, clock status at the time of the event, severity of the event and event description among other information. Events can also be filtered from the logs. The following log files are available for viewing or download:

- Event Log System
- Event Log User Authentication
- Even Log Access Rights and User Management
- Event Log Communication
- Event Log Firmware Update and Licenses
- Event Log Security
- Event Log Critical Error
- All Events Log
- Diagnostics Log
- All Events and Diagnostics Log

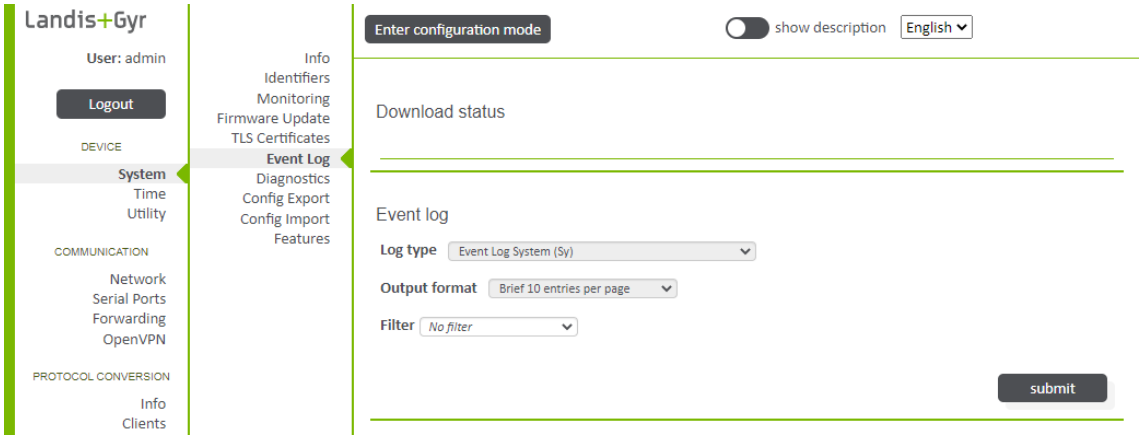


Figure 17: Device > System > Event log

6.2.1.7 Diagnostics download

In the diagnostics section (**Device** > **System** > **Diagnostics**), you can download support dumps for correspondence with L+G customer support.

Device reboot can be activated by clicking **reboot**. Triggering a reboot is normally not necessary.

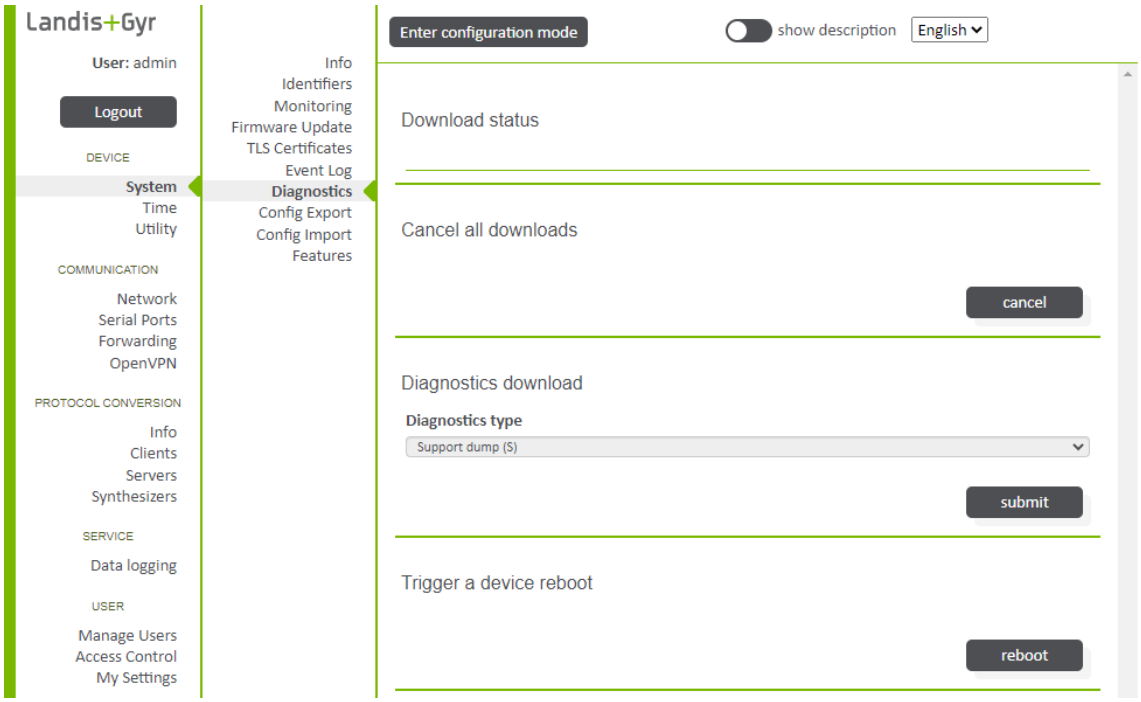


Figure 18: Device > System > Diagnostics

6.2.1.8 Feature license

In section **Device** > **System** > **Features**, feature licenses can be activated for additional functionality on the device. A file can be uploaded for feature licenses by entering configuration mode and clicking **Choose file** and selecting a file. Apply the configuration after installing new licenses and before making any further changes.

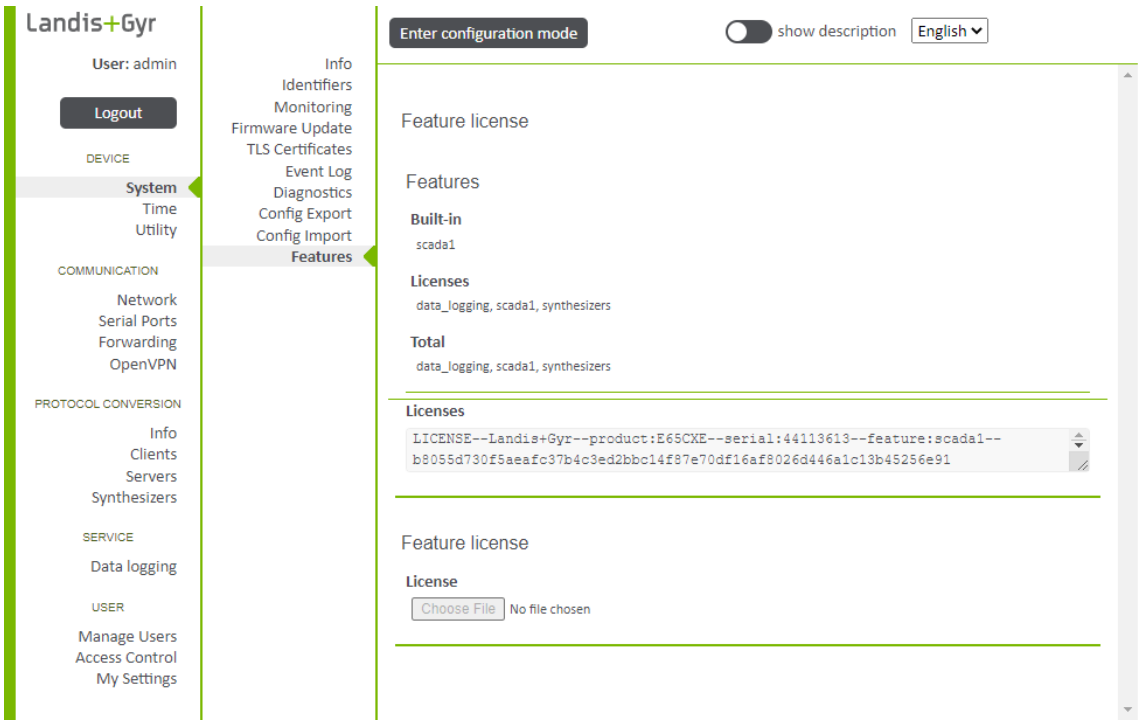


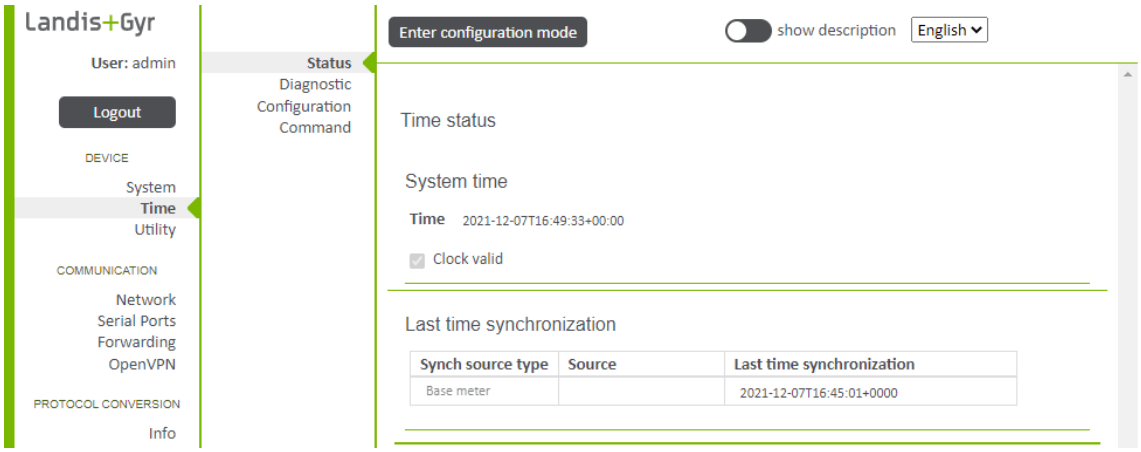
Figure 19: Device > System > Features

6.2.2 Time

6.2.2.1 Time status and diagnostic

Go to **Device** > **Time** > **Status** to view the current system time and date in local time. Clock status (valid/invalid) and the last time synchronisation are also shown. The status page is updated automatically approximately every 3 seconds.

Figure 20: Device > Time > Status



Additional diagnostic information is available under **Device** > **Time** > **Diagnostic**.

6.2.2.2 Time synchronisation setup

Time synchronisation can be found under **Device** > **Time** > **Configuration**. You can configure clock synchronisation based on the base meter clock or NTP. With NTP, the device synchronizes its time on a periodical interval to a NTP server or servers. Up to 6 NTP servers or pools can be configured, using either an IP address or a hostname. The number of server addresses per pool is limited to 4. NTP offers improved reliability and accuracy by using multiple servers in time synchronisation.

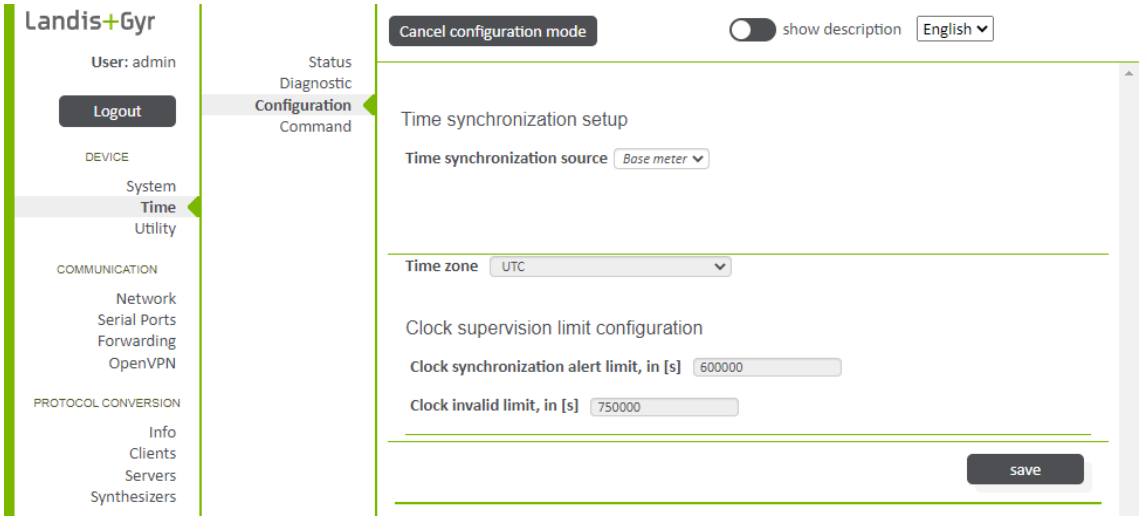


Figure 21: Device > Time > Configuration

Note
Always configure the correct time zone to show local time.

6.2.2.3 Force a time synchronisation

Under **Device** > **Time** > **Command** you can force the device to synchronise its time with the configured synchronisation source. Click **force a time sync** to execute the synchronisation.

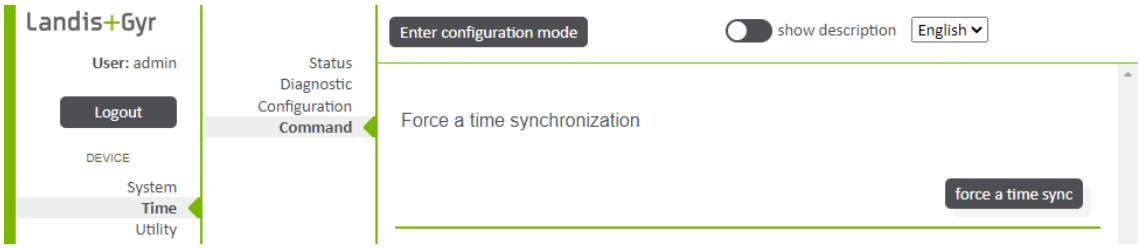


Figure 22: Device > Time > Command

Note
In case of large time offsets while forcing a time synchronisation, resulting in large time jumps, certain operations on communication protocols (such as HTTP, Modbus, IEC 60870-5-104) may time out and must be executed again.

6.2.3 Utility

6.2.3.1 Utility owned identifiers

Additional system identification information can be added in section **Device** > **Utility** > **Config Idents** and the information is shown in section **Device** > **Utility** > **Identifiers**. This information can include the installation location, the customer property numbers of the module and the server name.

Utility serial numbers and identifiers are free-purpose identification numbers. They are owned and handled by the utility, and the utility decides how to use and compile the numbers.

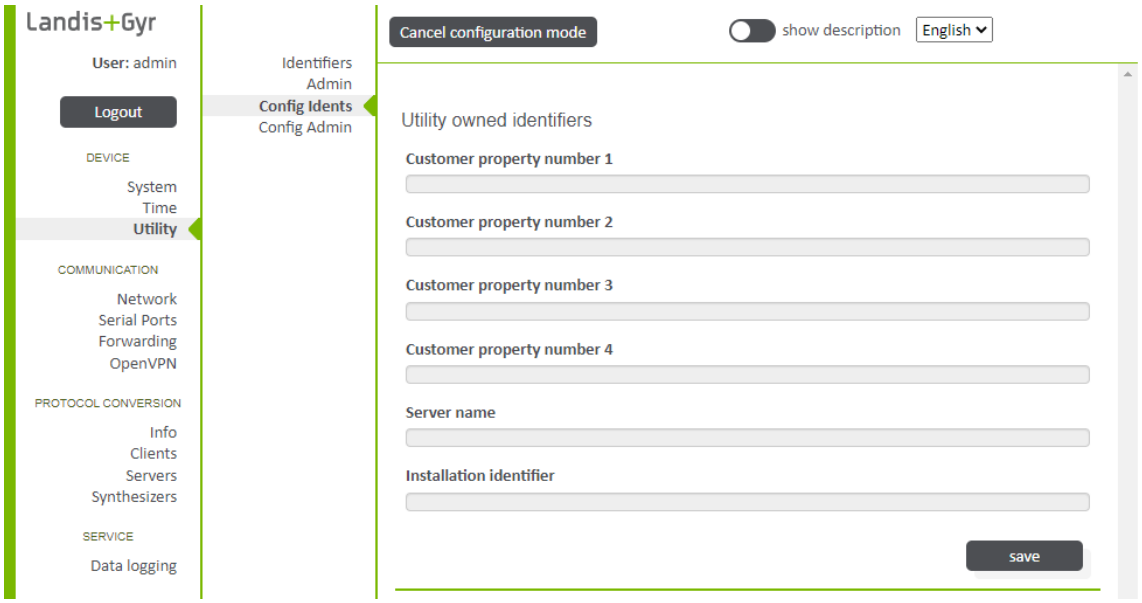


Figure 23: Device > Utility > Identifiers

6.3 Communication

6.3.1 Network

6.3.1.1 Ethernet ports

Figure 24: Communication > Network > Status

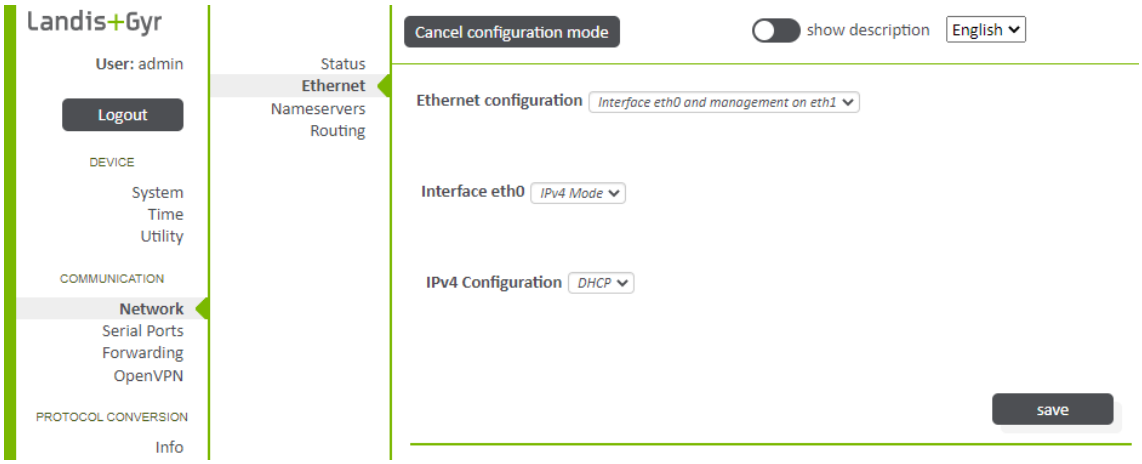


Figure 25: Communication > Network > Ethernet

Configuration of the Ethernet ports is available under **Communication** > **Network**. The upper part of the status screen (**Communication** > **Network** > **Status**) indicates the current address information including MAC, IP address and Gateway. Settings can be changed on the Ethernet page (**Communication** > **Network** > **Ethernet**).

Ethernet interfaces are named ETH0 and ETH1. Port ETH0 can be disabled if required. ETH1 is always enabled and commonly used with fixed IPv4 settings as local management access. However, if needed, ETH1 is also freely configurable.

Basic functionality can be selected from the following configuration options:

- **Interface ETH0 and management on eth1**
  - eth0 is freely configurable
    - mode: IPv4
    - IPv4 config: static/ DHCP
    - default gateway
  - ETH1 is mapped as management interface with IPv4 172.16.0.1 and as DHCP server.
- **Management ETH1**
  - ETH0 is disabled
  - ETH1 is mapped as management interface with IPv4 172.16.0.1 and as DHCP server.
- **Bridge between ETH0 and ETH1**
  - bridge BR0 is freely configurable
    - mode: IPv4
    - IPv4 config: static/ DHCP
    - default gateway
    - optionally: recovery IP (IPv4 172.16.0.1) on BR0 without DHCP server
- **Interface ETH0 and ETH1**
  - ETH0 is freely configurable
    - mode: IPv4
    - IPv4 config: static/ DHCP
    - default gateway
  - ETH1 is freely configurable
    - mode: IPv4
    - IPv4 config: static/ DHCP
    - optionally: recovery IP (IPv4 172.16.0.1) on BR0 without DHCP server

The IP address can be configured either manually by the user or automatically using the dynamic address assignment functionalities. For the main port, the manually inserted IP address cannot refer to the same subnet as the one used for the management port.

6.3.1.2 Bridging

An ethernet bridge represents the software analogue to a physical ethernet switch while sharing a single IP subnet.

Bridging of the two ethernet interfaces ETH0 and ETH1 allows you to connect several communication modules transparently, without using an external switch. Therefore, it is a cost competitive option for meter room applications or other use-cases where the ethernet interfaces are kind of daisy chained. Bridging has been tested with up to 20 communication modules.

The network is a linear topology and a loop must be avoided since there is no spanning tree protocol support implemented in the bridges.

6.3.1.3 Nameservers

The **Communication** > **Network** > **Nameservers** section allows you to configure the name(s) of the DNS server(s). The addresses of up to 3 DNS servers can be configured.

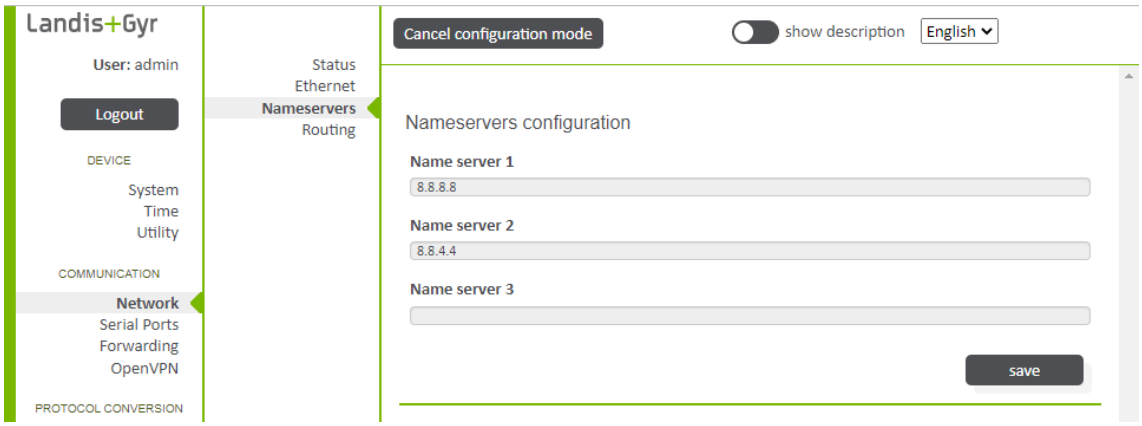


Figure 26: Communication > Network > Nameservers

Note

If the IP address is obtained automatically via DHCP, the servers configured above will be used as secondary nameservers, otherwise as primary.

6.3.2 Serial ports

The CU-XE communication module features several serial ports. For the usage of the serial and internal ports, go to **Communication** > **Serial ports**.

6.3.2.1 RS-485/RS-422

The RS485/RS422 interface can be used for virtual bus (forwarding). The port can be configured according to the peer. The CM supports a maximum transmission speed of 115.2 kbps. To configure the termination resistor, refer to RS-485/RS-422 interface on page 8. To switch between RS485 and RS422, DIP switch settings have to be applied according to tables shown in section RS-485/RS-422 interface on page 8.

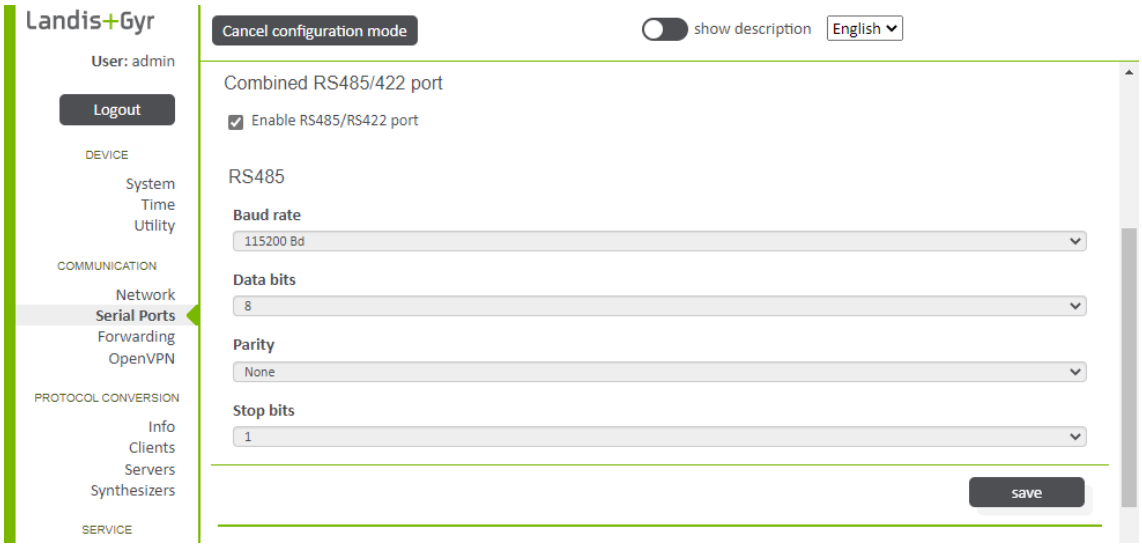


Figure 27: Communication > Serial Ports

6.3.2.2 RS-232

The RS232 interface can be used for virtual bus (forwarding). The port can be configured according to the peer. The CM supports a maximum transmission speed of 115.2 kbps.

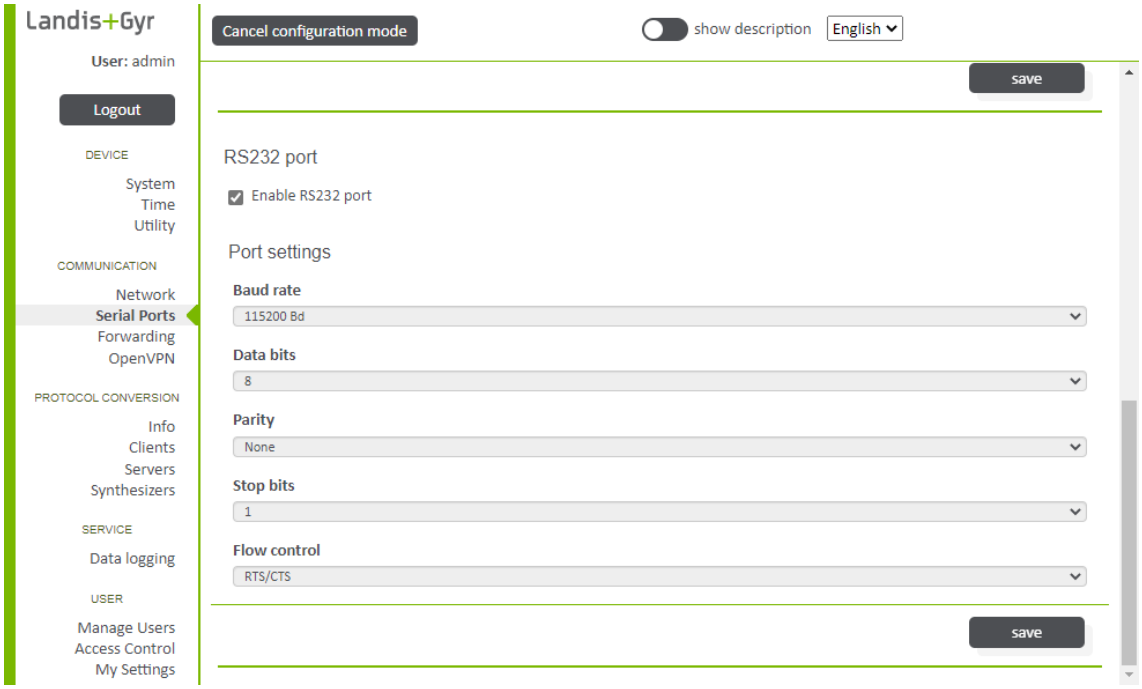


Figure 28: Communication > Serial Ports

6.3.3 Forwarding

Under **Communication** > **Forwarding**, you can view the use of the serial ports and configure forwarding rules between interfaces.

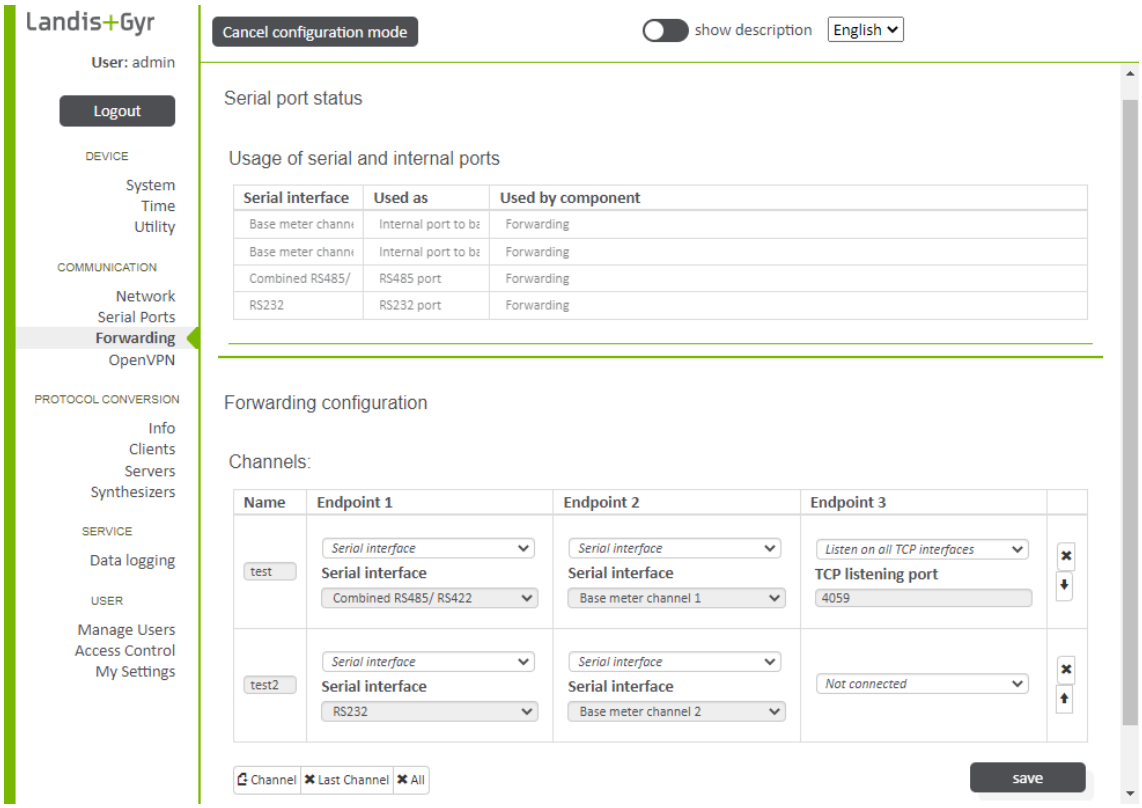


Figure 29: Communication > Forwarding

To be able to establish a direct connection between devices on different interfaces (serial and/or TCP/IP), the communication module provides a forwarding functionality. Application level data received on one interface is forwarded to one or more other interfaces (and vice versa). Using this approach, the device is capable of handling every data transmission on the configured interfaces independent of any protocol language. In this sense, the forwarding component acts as a fully transparent media converter.

The communication module contains several different ports that can be used for forwarding:

- TCP ports
- Serial ports (combined RS485/RS422 or RS232)
- Internal channels to the base meter (base meter channel 1 or 2)

Up to maximum 10 channels can be defined in the forwarding configuration.

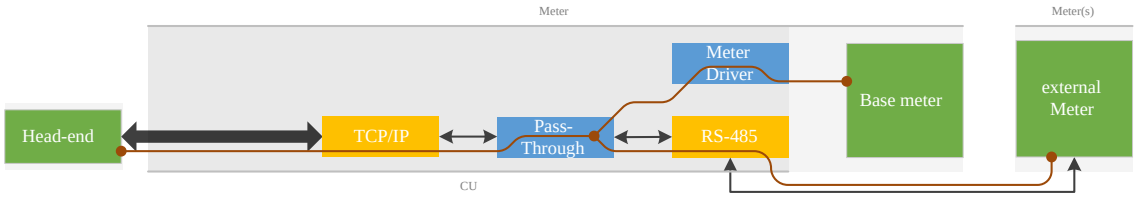
Using the buttons below the channels table you can add new channels or delete the last channel or all channels.

With the arrow buttons in the last column of the channels table you can move the table entries up and down for sorting purposes.

To delete a specific channel from the channels table click on the “x” button in the last column of the channels table.

Ethernet bridging is meant to be used for forwarding using Ethernet ports (forwarding from Ethernet to Ethernet is not possible).

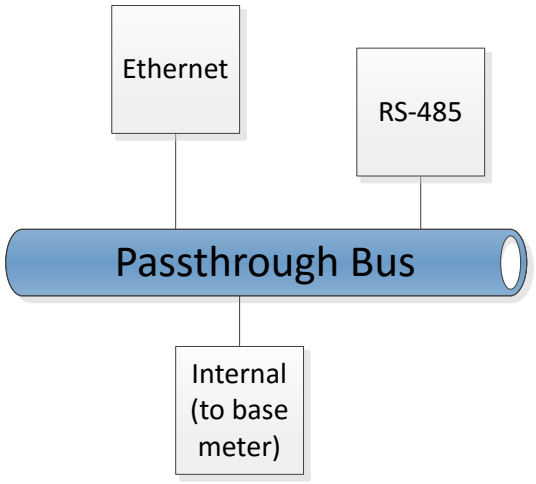
The forwarding feature can be used in a number of different ways. See the example below.



Note

Forwarding is not protocol-aware, i.e. every use case that does not require actions on the communication module itself is supposed to be supported. Every protocol requiring actions (such as transmission speed switch at HDLC Mode E) is not supported.

Forwarding works like a bus with several attached ports. The number of ports attached to a bus is only limited by the number of available ports. Traffic received from one of the connected ports is forwarded to every other port. This also implies that the slowest port defines the bus speed, which may have an impact on the timing behaviour.



Note

It is possible to have up to 4 virtual busses configured to work in parallel. If forwarding is being used to read out the base meter, DLMS and IEC 62056-21 protocols are supported by the meter.

6.3.4 OpenVPN

OpenVPN is an open source software that implements virtual private network (VPN) techniques to create a secure encrypted point-to-point TSL connection. More information on OpenVPN is available at: https://openvpn.net/. In the **Communication** > **OpenVPN** > **Status** section of the Web UI you can see the overview of the currently enabled OpenVPN connections and the status of the current OpenVPN sessions.

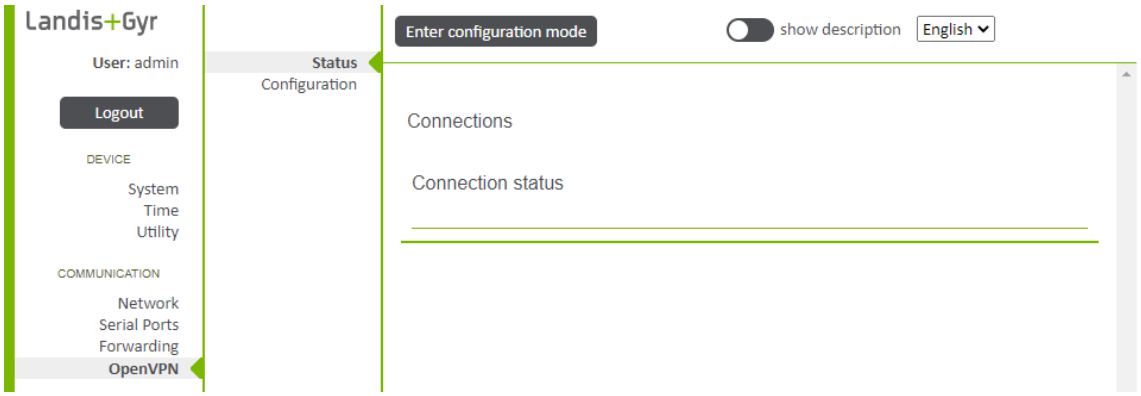


Figure 30: Communication > OpenVPN > Status

For the OpenVPN credentials, configuration and channels, go to **Communication** > **OpenVPN** > **Configuration**.

Following parameters can be configured:

- **Network type:** Currently only TUN is supported
- **Protocol:** OpenVPN can utilize TCP or UDP. Use UDP for better performance.
- **OpenVPN server:** The hostname or IP address of the OpenVPN server.
- **Port:** Port of the OpenVPN server.
- **Local address of the TUN/TAP device:** IP address of the local device. Can be left empty if the OpenVPN server configures the client.
- **Remote address or netmask:** For TUN devices in point-to-point mode, this is the IP address of the remote VPN endpoint. The proper usage of ifconfig is to use two private IP addresses which are not a member of any used, existing subnet. The IP addresses may be consecutive and should have their order reversed on the remote peer. Can be left empty if the OpenVPN server configures the client.
- **Encryption algorithm:** With Static key authentication only use AES CBC.
- **Authentication method:** Can be set to existing credentials, certificates, username/password with certificates, and static key.
- **Ping:** Configure to enable ping and set the interval for sent pings. Purpose of these pings is to maintain the connection if no packets are sent.
- **Ping restart:** Configure the time after which OpenVPN connection is restarted if no data is received.
- **Compression:** Enable and choose a compression algorithm. LZO and LZ4 are different compression algorithms, with LZ4 generally offering the best performance with least CPU usage. For backwards compatibility with OpenVPN versions before v2.4, use "LZO".

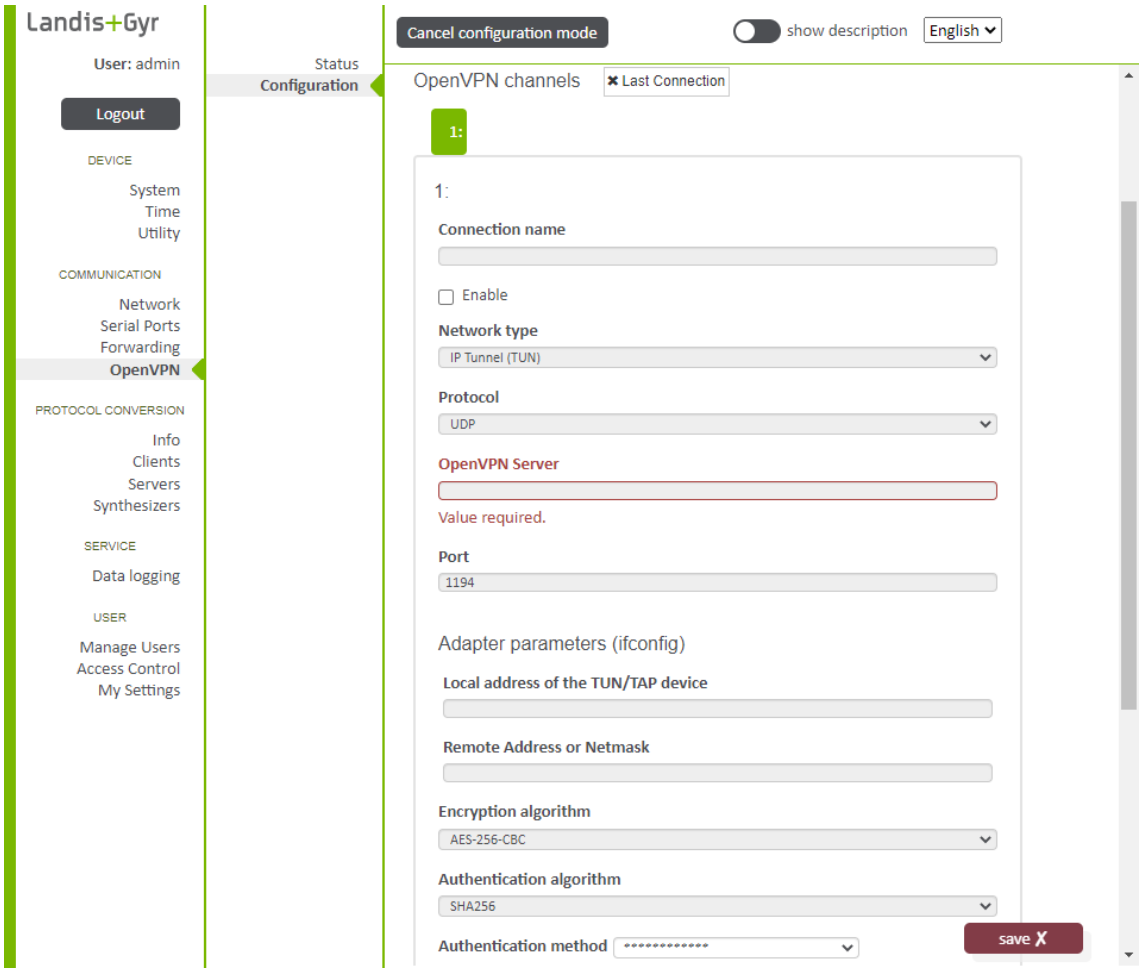


Figure 31: Communication > OpenVPN > Configuration

6.4 Protocol conversion

One of the core features of the firmware is the ability to convert between communication protocols. Protocol conversion process includes several components, including clients, servers and the datahub. The datahub acts as a mediator between data producing and consuming components. The data that travels through the datahub is modelled streams of atoms called data points. Each data point contains a value, a timestamp, some quality information, and a unique data-point identification number.

For protocol conversion the client mapping with server must be configured. The data read by the DLMS/COSEM and/or the Modbus clients can be mapped to either or both of the Modbus and IEC 60870-5-104 servers.

The proper configuration can be verified using any Modbus Master and SCADA 104 test tool.

6.4.1 Checking the protocol conversion status of all clients and servers

The status of protocol components, the clients and servers, can be checked on the **Protocol Conversion** > **Info** > **Status** page. Green colour indicates the client/server is properly configured and running.

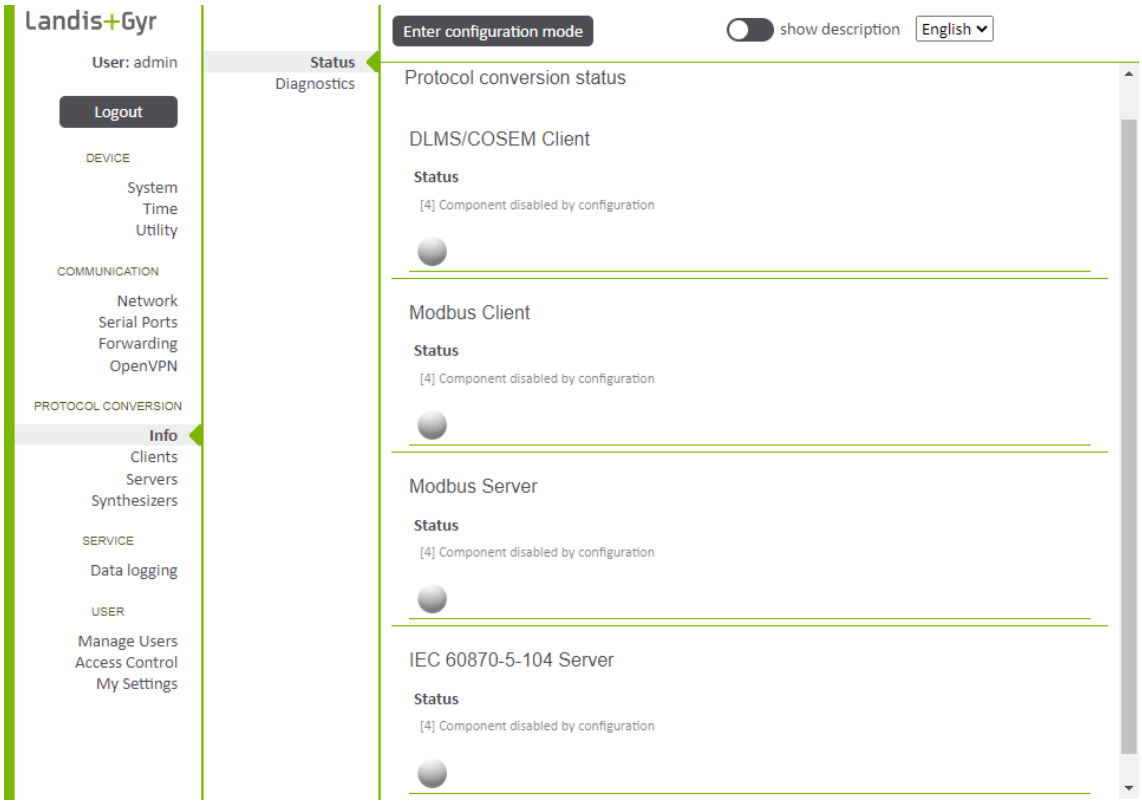


Figure 32: Protocol Conversion > Info > Status

Additional information is displayed on the Protocol conversion diagnostics and monitoring information screen:

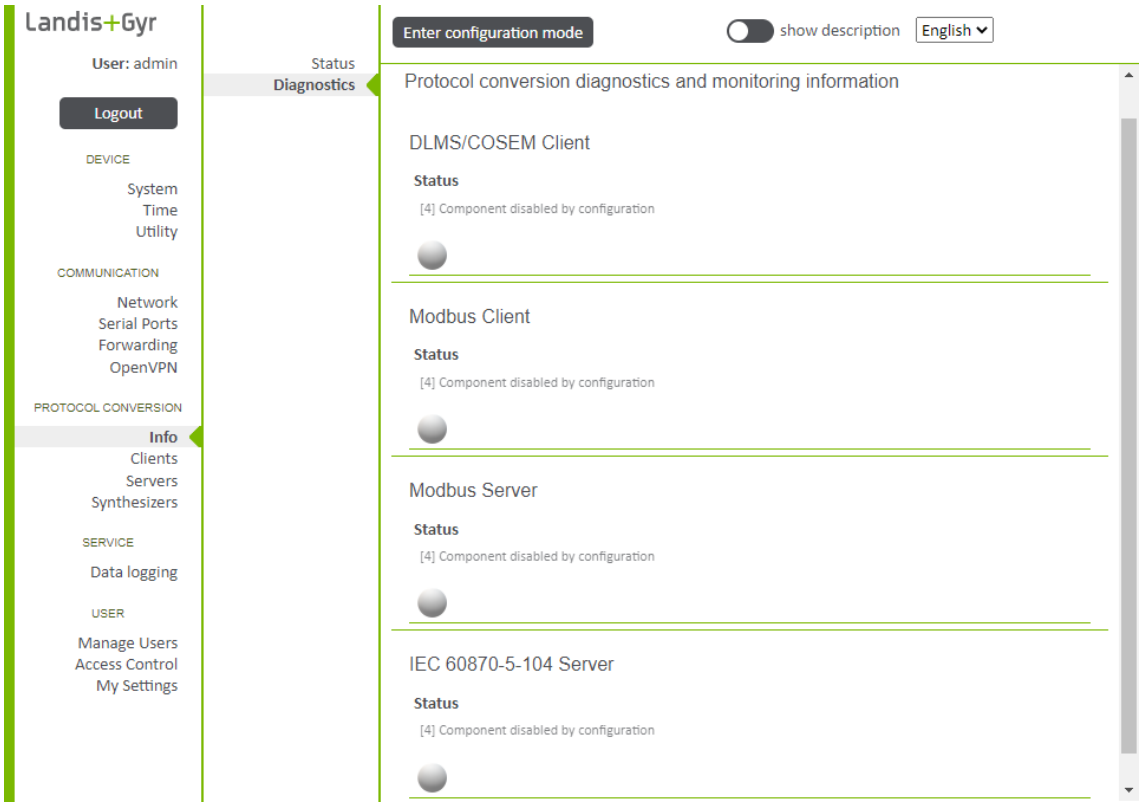


Figure 33: Protocol Conversion > Info > Diagnostics

6.4.2 DLMS/COSEM client configuration

The CU-XE communication module features a DLMS/COSEM client. It can connect to and read various types of data from devices that utilize the DLMS/COSEM protocol. The data is read using a polling mechanism. The DLMS/COSEM client can communicate with multiple devices via the serial port.

DLMS/COSEM client configuration requires a base meter channel that is available for use and does not have forwarding rules in place.

If the needed base meter channel is used in a forwarding rule, the forwarding rule must be removed before DLMS/COSEM configuration (see section Forwarding on page 35).

The usage of serial and internal ports is displayed in the serial port status area.

The DLMS/COSEM client must be enabled in the checkbox for the client to work. In the same section time synchronization interval and offset (deviation that triggers a synchronization) can be configured as well as the delay until reconnecting to a device if a communication failure occurs. Slow, fast, and normal polling group intervals are also configurable. Slow polling is used for data that is static, such as serial number or firmware version. Fast polling is used for limited number of high-priority values, and normal polling for all the remaining values.

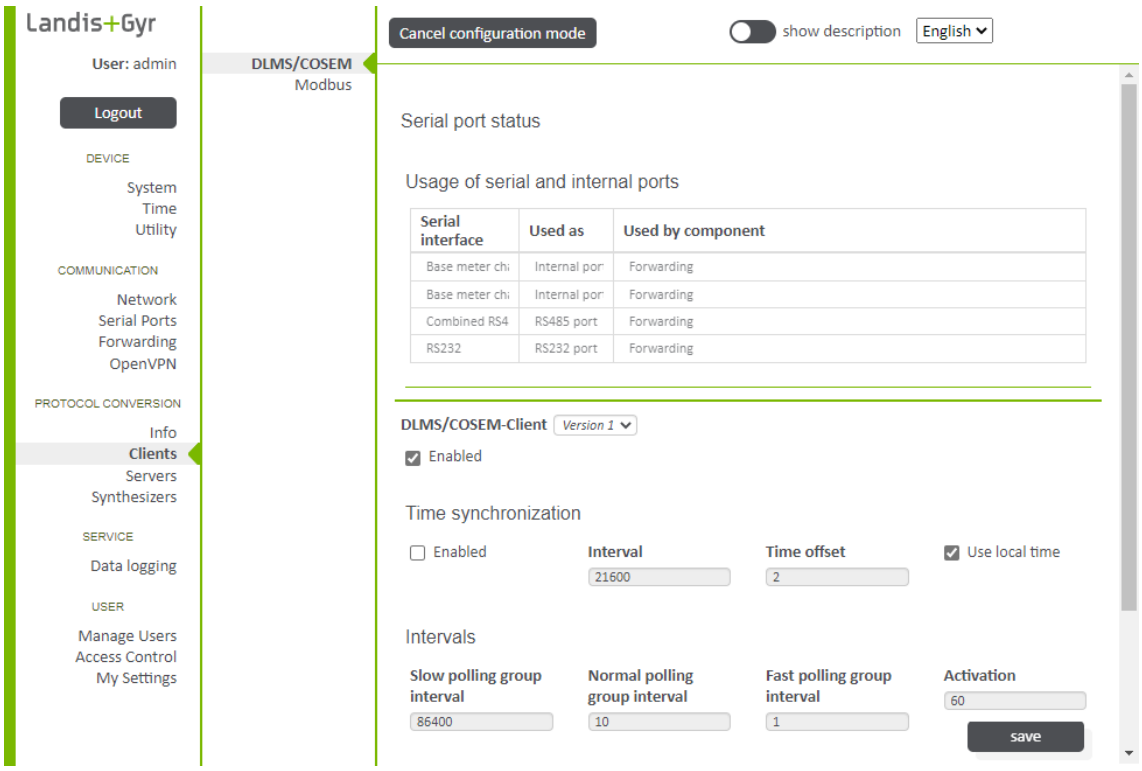


Figure 34: Protocol Clients > Clients > DLMS/COSEM

Then a meter can be configured in the Meter Configuration area as follows:

1. Enter the configuration mode.
2. Click on the **Device** button to display device definition.
3. Enter device label.
4. Choose serial interface.
5. Enter address information.
6. Click on the **row** button to display the first mapping.
7. Enter a name and a logical name (OBIS code) and select the type (e.g. Register).

8. Click on the **save** button. If the mapping definition is correct, the **Valid** checkbox is activated.
9. Define the next rows until the meter mapping is complete.

Note

Please note that there is no verification, whether the entered OBIS codes are configured accordingly in the base meter.

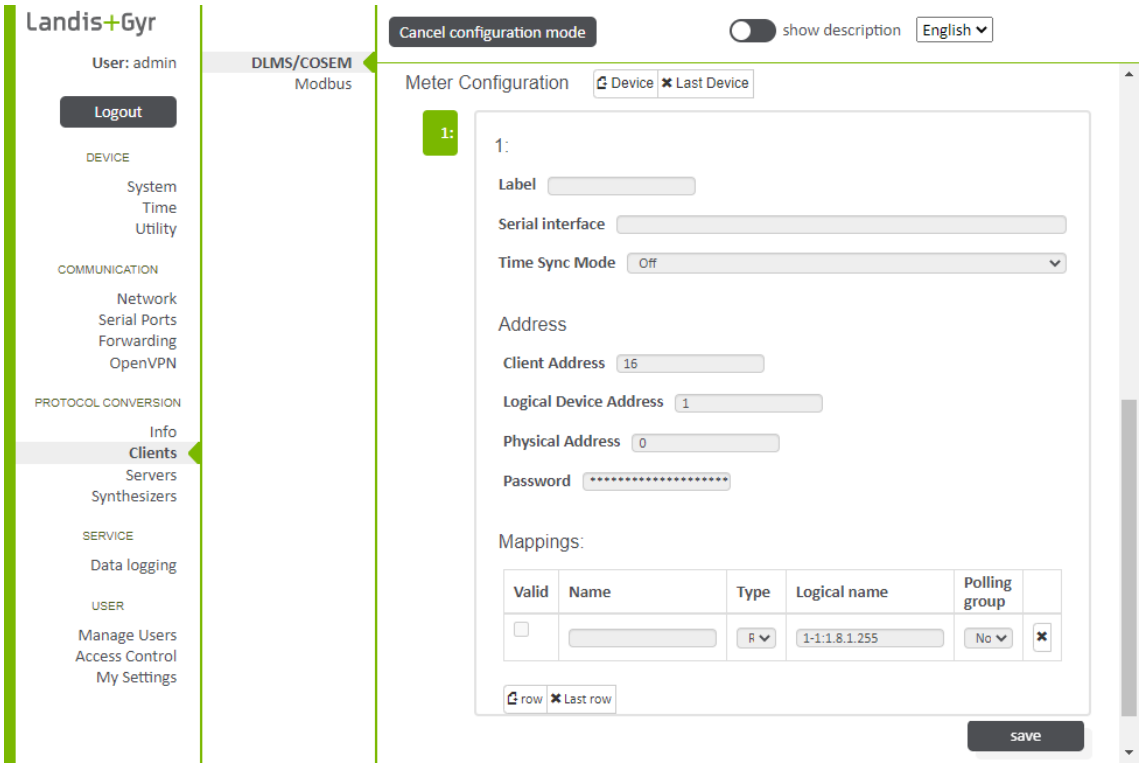


Figure 35: Protocol Conversion > Clients > DLMS/COSEM

6.4.3 Modbus client configuration

The CU-XE communication module features a Modbus client. It can communicate with multiple devices using serial and TCP/IP connections. The Modbus client can read values from registers. Reading is done using a polling mechanism, on a configurable schedule.

For the Modbus client to work, it must enabled in the checkbox on **Protocol Conversion** > **Clients** > **Modbus** page.

On the same page polling optimization can be enabled. User can also configure the starting time for first poll and further polling intervals for slow, fast, and normal polls. Slow polling is used for data that is static, such as serial number or firmware version. Fast polling is used for limited number of high-priority values, and normal polling for all the remaining values.

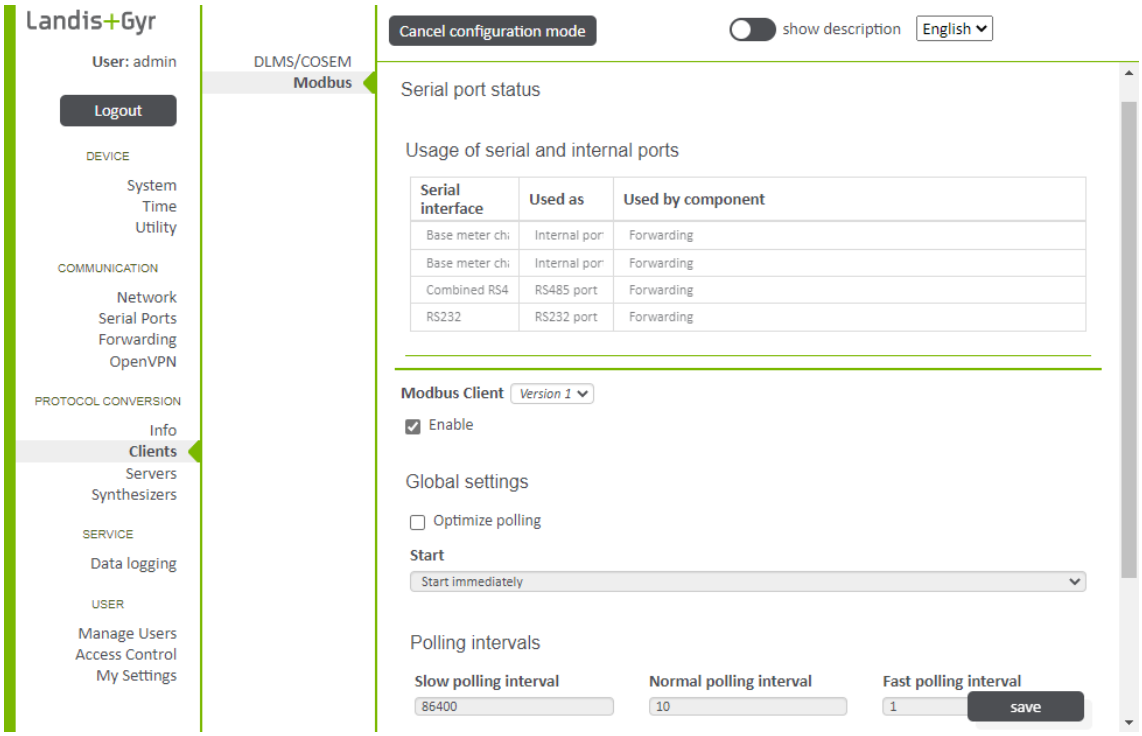


Figure 36: Protocol Conversion > Clients > Modbus

Then a device can be configured in the Device Configuration area as follows:

1. Enter the configuration mode.
2. Click on the **Device** button to display a device definition.
3. Enter device label.
4. Choose interface.
5. Enter the hostname, TCP port and unit identifier.
6. Click on the **row** button to display the first entry of the register list.
7. Enter an ID and an index and select the bank (coils, contact, input or holding), the type and the polling group (normal, fast or slow).
8. Click on the **save** button.
9. Define the next rows until the register list is complete.

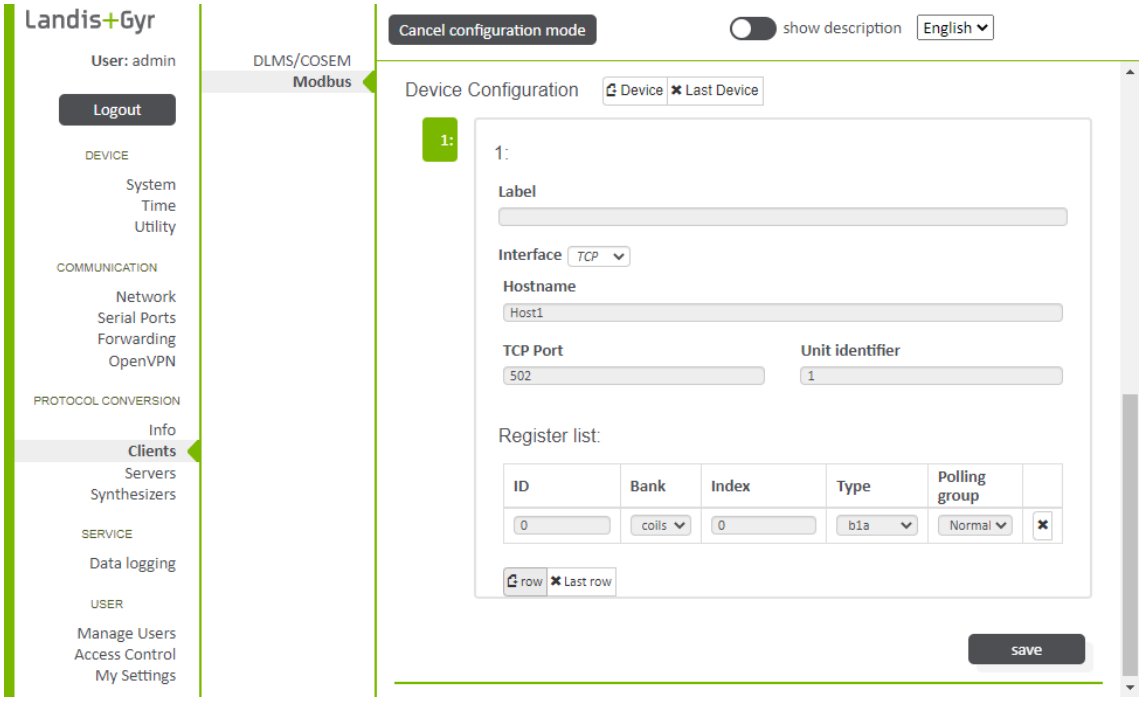


Figure 37: Protocol Conversion > Clients > Modbus

6.4.4 Modbus server configuration

The CU-XE communication module features a Modbus server. Modbus is a protocol based on request, reply. The client requests operations from the server. The server then replies. The Modbus server supports the server side of the RTU and TCP variants of the Modbus protocol over serial- and TCP/IP network links, respectively.

The Modbus server must enabled in the checkbox and configured for the server to work.

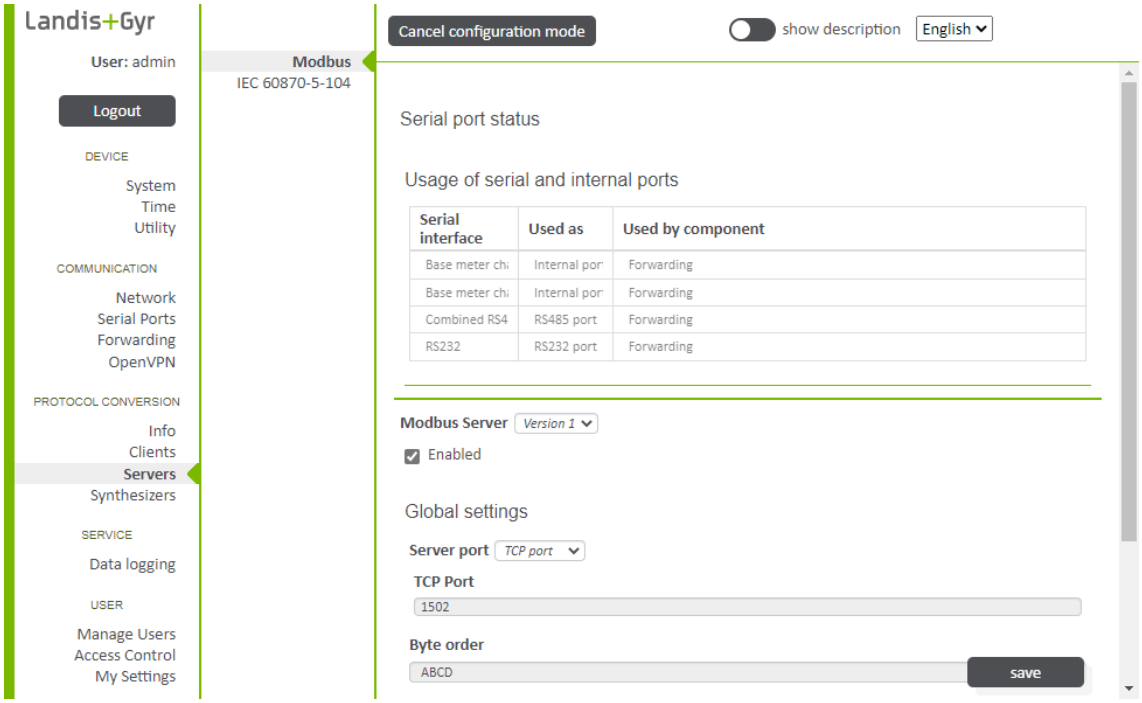


Figure 38: Protocol Conversion > Servers > Modbus

Once the Modbus server is enabled, both the Modbus TCP port and the Modbus serial port (RTU mode) can be selected and configured. In the example above the TCP port with port 1502

is selected. Byte order can also be selected from one of the four endianness modes for 32-bit data types: ABCD, DCBA, CDAB or BACD.

Then the mapping to a client can be defined in the Mapping groups area as follows:

1. Make sure that you are in configuration mode.
2. Click on the **Group** button to display a group definition.
3. Enter a label.
4. Click on the **row** button to display the first mapping.
5. Select a data point, the bank (coils, contact, input or holding) and the format (bool, i16, i32 or float) and enter the address and the scaling.
6. Click on the **save** button.
7. Define the next rows until the mapping is complete.

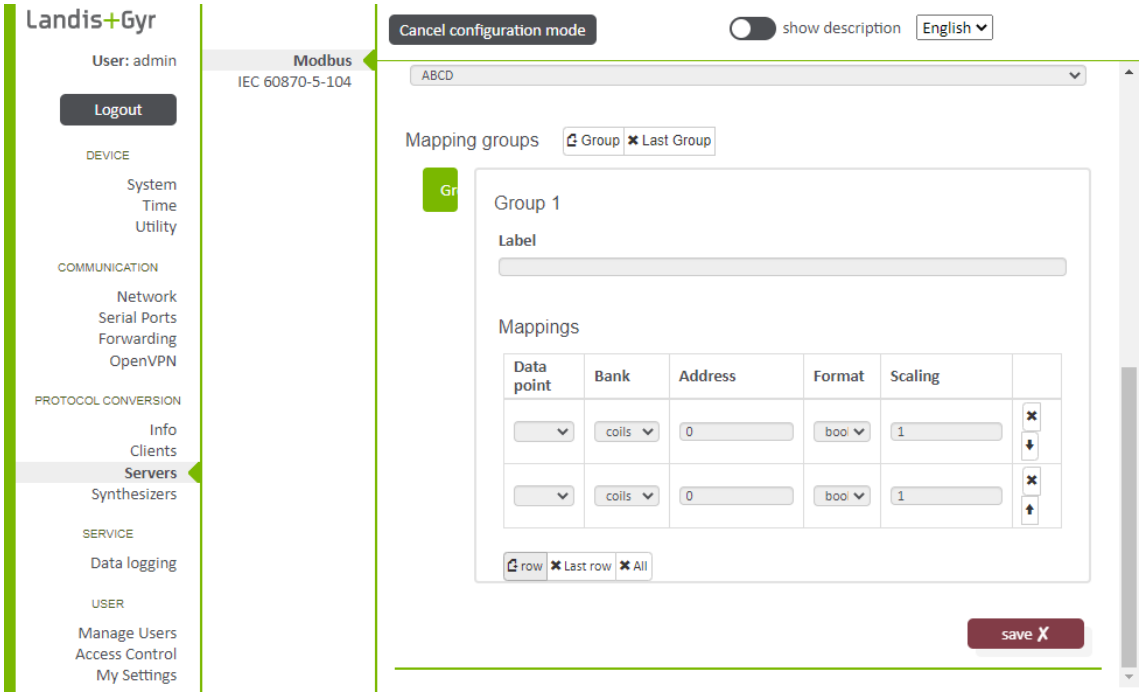


Figure 39: Protocol Conversion > Servers > Modbus

Please note that once the activated DLMS/COSEM client is selected for mapping with any server, only the previously activated OBIS objects can be used for mapping any data point.

6.4.5 IEC 60870-5-104 server configuration

The IEC 60870-5-104 standard describes the communication between server device and a client device on an IP network. The client monitors process data coming from the server and may instruct server to perform some action with a command. A server can elect to transmit data spontaneously or it can transmit data in response to an interrogation or read command. The IEC 60870-5-104 server spends most of its time waiting for changes in the data set it has been configured to use. Once a value changes it will store the new value and potentially (pending on evaluation of a value based deadband) do a spontaneous transmission of this new value.

The deadband mechanism looks at the value of a given data point and can be specified using either an absolute or relative change. For each data-point two values are stored: the most recent value, and the last value which caused a spontaneous transmission. Whenever the most recent value changes, the system compares the last value transmitted spontaneously with the

most recent value. If it finds that the deadband has been exceeded it triggers a spontaneous transmission.

The IEC 60870-5-104 Server must first be enabled in the checkbox for the server to work.

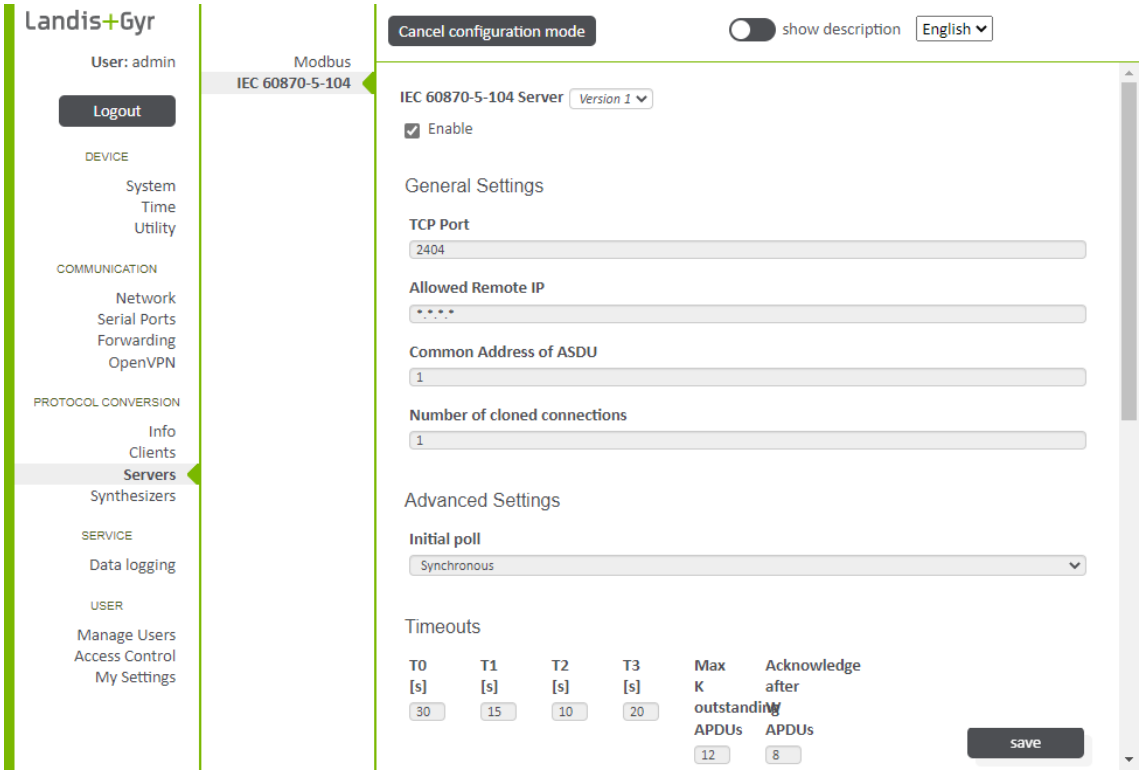


Figure 40: Protocol Conversion > Servers > IEC 60870-5-104

Then the server can be configured as follows:

1. Make sure that you are in configuration mode.
2. Enter necessary information in the **TCP Port** , **Allowed Remote IP**, **Common Address of ASDU** and **Number of cloned connections** fields.
3. Select synchronous (connections accepted only after all mapped data points are polled) or asynchronous (connections accepted before all data points are polled) mode for the initial poll.
4. Configure the different timeouts if necessary:
   - T0: Interval at which offline session attempts reconnecting.
   - T1: Time waited for ACK to a transmitted APDU.
   - T2: Time before sending supervisory APDU ACK. Must be lower than T1.
   - T3: Idle time before sending TEST APDU.
   - Maximum unacknowledged transmitted APDUs.
   - Maximum unacknowledged received APDUs
5. Enable or disable time-tagged commands.
6. Configure maximum command age and maximum command derivation ahead of time.
7. Enable or disable direct command transmission. If enabled, direct executing is possible.
8. Enter time that a select will remain valid for.
9. Enable or disable sending of ACT TERM upon completion of commands.
10. Enable or disable timestamps for measured values.
11. Click on the **Group** button to display a group definition.
12. Enter a label.

13. Click on the **Mapping** button to display the first mapping.
14. Select a type, the data point 1 and 2 and the push mode (always, on change or deadband) and enter the IOA, the deadband and the scaling.
15. Click on the **save** button.
16. Define the next row until the mapping is complete.

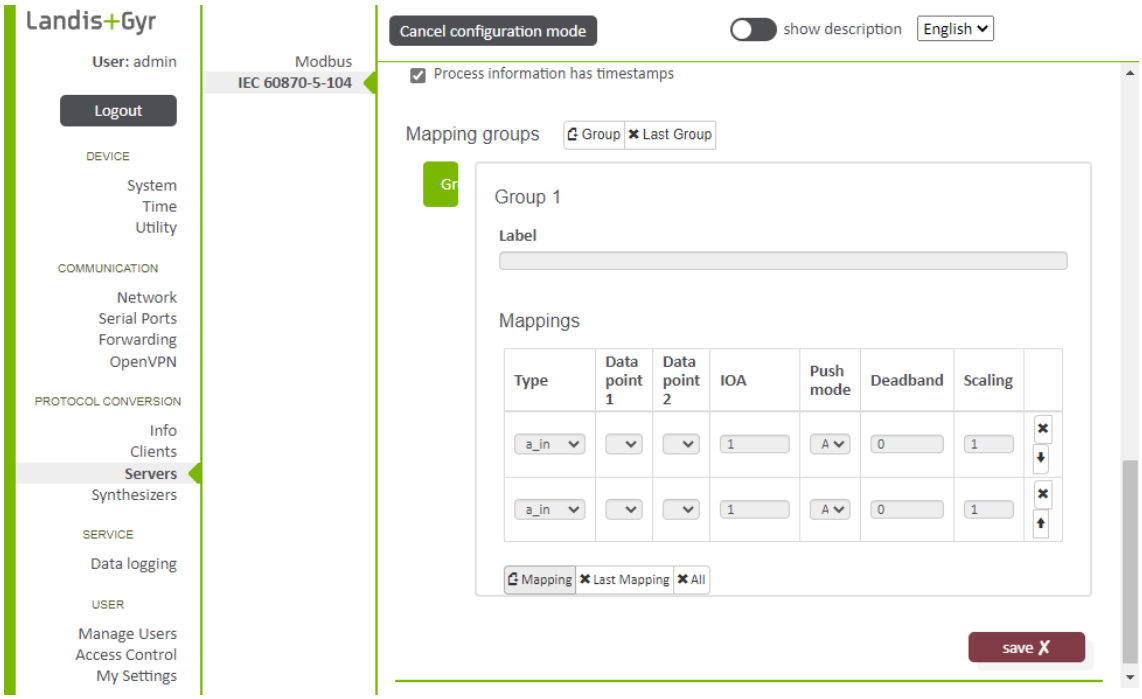


Figure 41: Protocol Conversion > Servers > IEC 60870-5-104

6.4.6 Synthesizers

The functionality of the firmware of Adventure based devices can be extended by uploading synthesizers. These synthesizers can fulfil special customer needs. The synthesizers take data from the datahub, perform processing, and inject the result back into the Datahub.

Out of security reasons every synthesizer must be written by Landis+Gyr. The synthesizer files are signed like firmware files. The signature is verified during upload of the synthesizers to the device.

Synthesizers can be uploaded and deleted on **Protocol Conversion** > **Synthesizers** > **Manage** page.

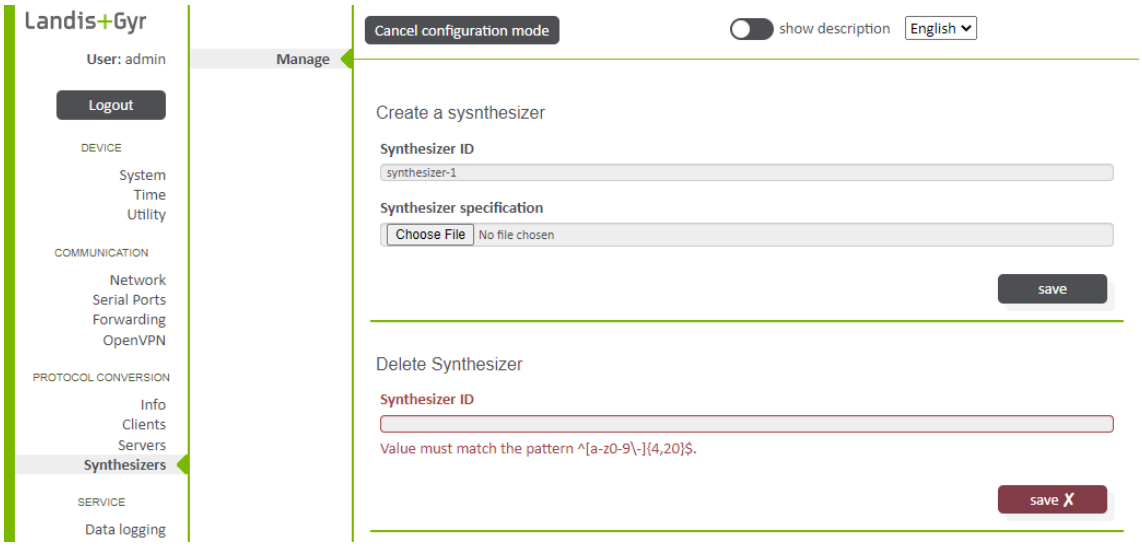


Figure 42: Protocol Conversion > Synthesizers > Manage

6.5 Service

6.5.1 Data logging

The communication module features a data logger that logs values from various sources and process, including the base meter, externally connected devices, other components and internal processes (CPU usage, temperature etc.)

The communication module stores configurable number of data log entries, up to one million. If the number is exceeded, entries are removed until the number of entries is within the configured limit. Entries are removed in chronological order, starting from the oldest.

The data logger stores following information for every value:

- Timestamp
- Value and type
- Validity of the value
- Validity of the timestamp

Under **Service** > **Data logging** > **Query data** you can view or download data logs containing the logged events and data.

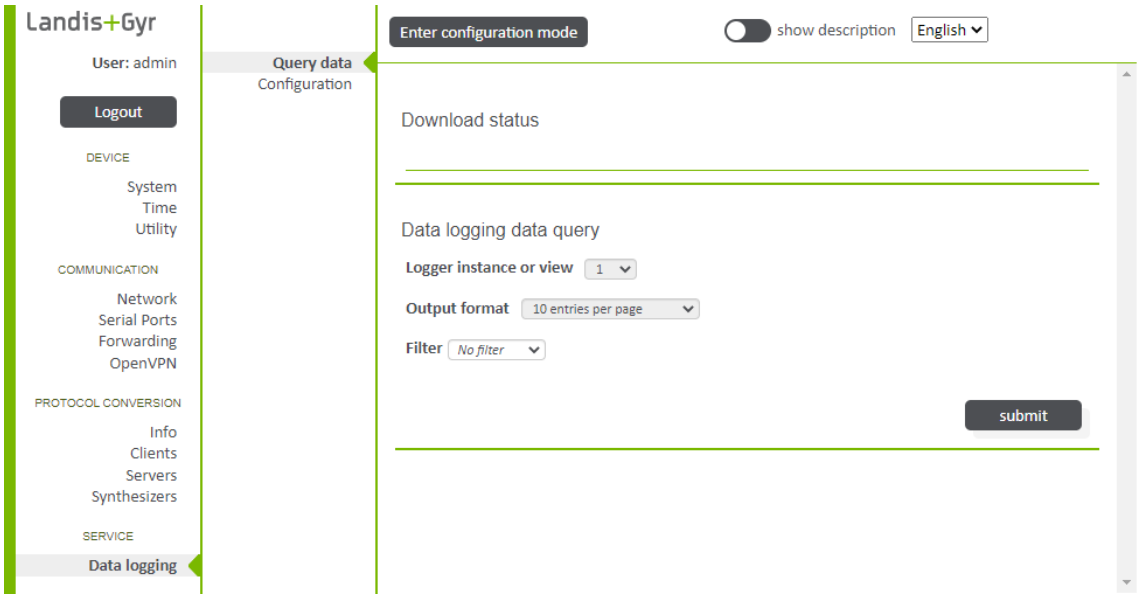


Figure 43: Service > Data logging > Query data

Data loggers can be configured under **Service** > **Data logging** > **Configuration**. You can create mappings and scalers. Scalers can be applied to mappings to scale and influence the measured values. Scalers can also be chained and used together. Following scalers are available:

- **Round:** Rounds the value to configured maximum number of digits.
- **Add:** Adds a configured value to the value of the scaling operation.
- **Multiply:** Multiplies the value with a configured factor.
- **Polynomial:** The value is used within a polynomial, which is defined in increasing order.
- **Linear interpolation:** The value is used as input for linear interpolation. This is based on a set of datapoints; interpolation is done between each pair of datapoints.

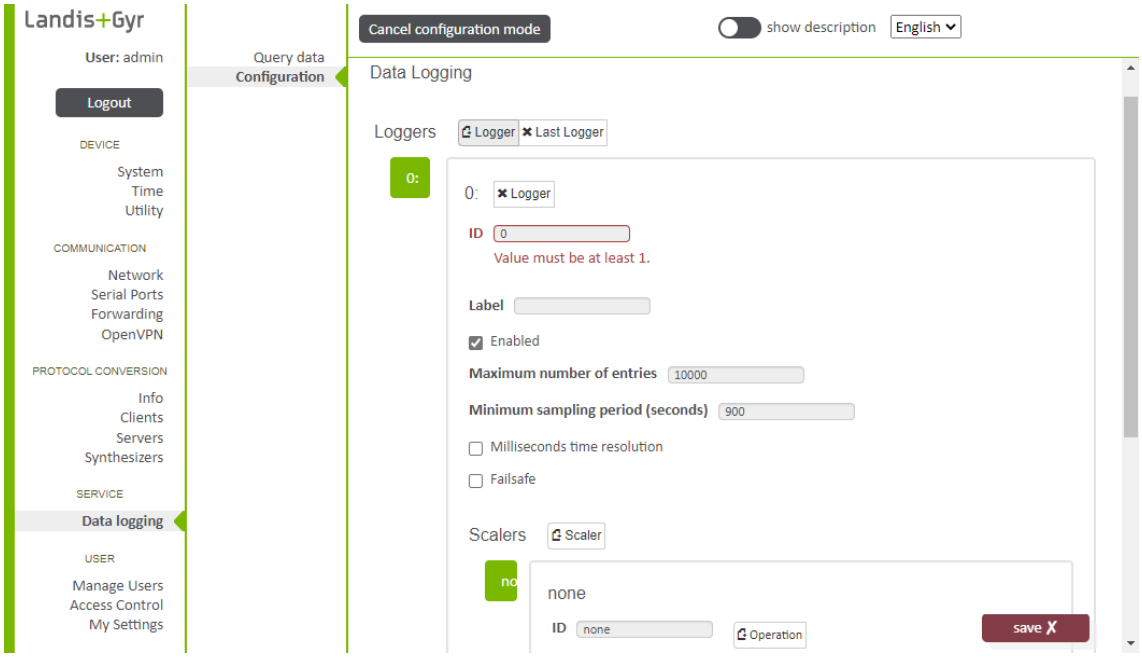


Figure 44: Service > Data logging > Query data

6.6 User configuration

The CU-XE provides data access protection via a Role-Based Access Control (RBAC) system. The access control is highly configurable. The RBAC as defined and described here only applies to the communication module and the RESTful/web interface. The base meter, for forwarding access, has its own RBAC configuration.

6.6.1 Management of users

Users are managed in the **User** > **Manage Users** section. There are 9 configurable roles. Users are instantiated, and assigned to roles, granting them access rights. The maximum number of user profiles the device supports is 32.

A new user first needs to be added, assigned one or more role(s), and activated with credential (username/password) settings.

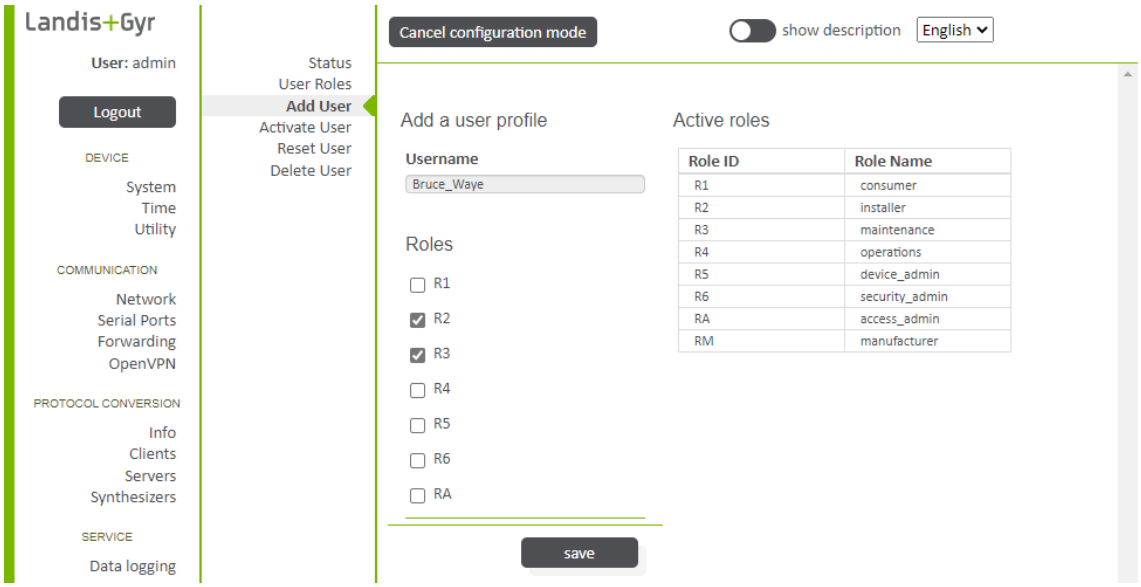


Figure 45: User > Manage users > Add user

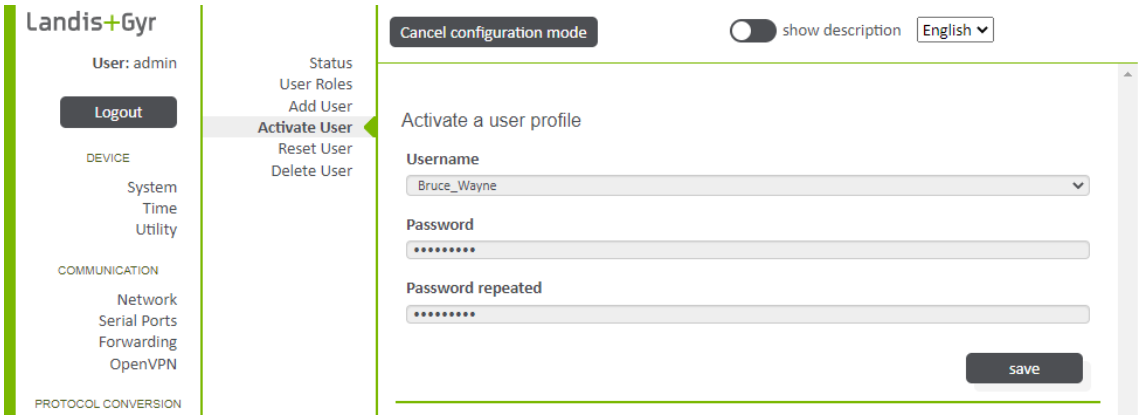


Figure 46: User > Manage users > Activate user

Table 1: User management actions

Action	Description
Add user	Add a user profile, consisting of the username and the assignments to the roles. An added user profile is inactive until a password is assigned.

Action	Description
Activate user	After adding a user profile to the device, the user must be activated before permitting access to the device. User activation is done by assigning a password to the user profile.
Reset user	Reset the user password.
Delete user	Delete a user profile.
Change user to roles assignment	When a user profile is added, the user is assigned to roles. This can be changed at any point.
Change user password	A logged in user can change the password.

6.6.2 Access and session management

The access rights of roles to resources (paths) are changeable for user roles. Go to **User** > **Access Control** > **Configuration**.

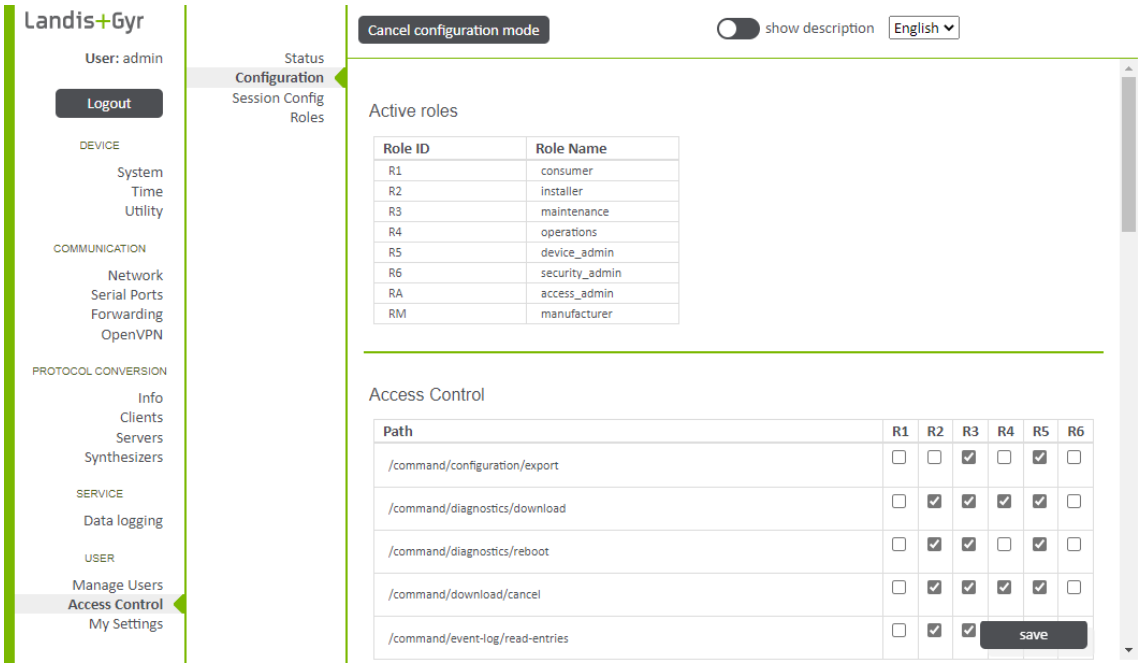


Figure 47: Access Control > Configuration

Login supervision and user session timeout are also configurable, under **User** > **Access control** > **Session config**.

With login supervision, further login attempts with the same username from the same source IP address can be blocked for a specified time after a number of failed login attempts.

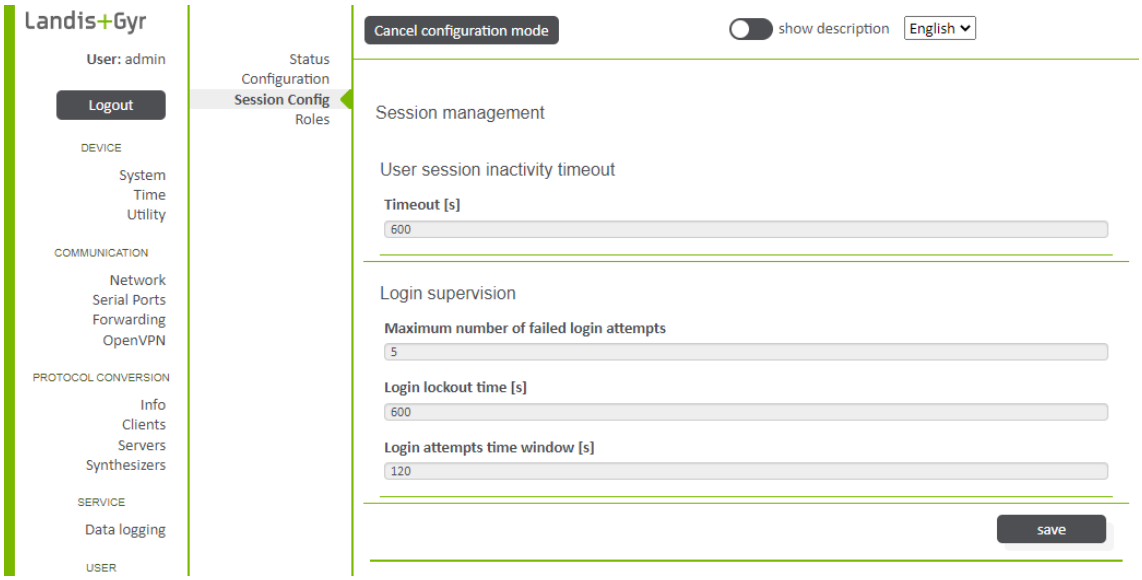


Figure 48: User > Access control > Session config

6.6.2.1 My settings / password

To change the current password, go to **User** > **My settings** > **Password**. Type the **Old password** and the **New password** in the respective fields.

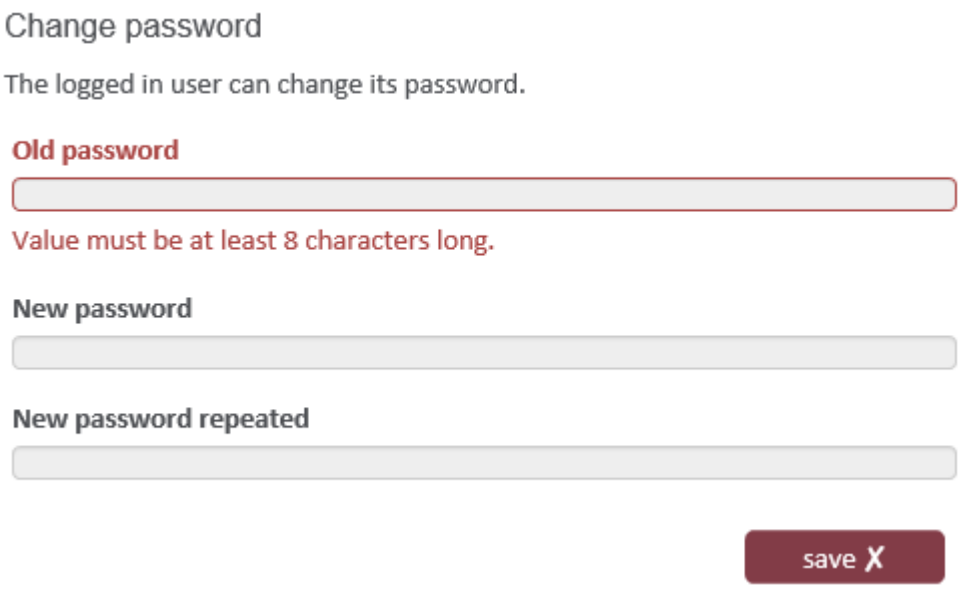


Figure 49: User > My Settings > Password

7 Service

7.1 Troubleshooting

When a fault has been detected in the system, check the following points regarding the interfaces. If you contact Landis+Gyr customer support, the support team may ask for a diagnostic export. See Diagnostics download on page 28 for more information on downloading it.

- Is the mains voltage present (meter LCD is working)?
- Has the maximum permissible ambient temperature been exceeded?
- Is there any visible damage to the installation?
- Check the status of the LEDs according to section LED status descriptions on page 14

  If none of these steps resolves the problem, the communication module should be removed and sent to the designated service and repair centre.

7.2 Repairing the communication module

Communication modules can only be repaired by authorised service and repair centres or by the manufacturer.

Note

Meter data cannot be read without a communication module

The meter data cannot be read without a communication module because the communication module provides the functionality for reading.

If repairing the communication module is necessary, use the following procedure:

1. Describe the problem as accurately as possible and state the name and telephone number of the contact person in case of inquiries.
2. Pack the communication module carefully to ensure it will not suffer any further damage during transport. Use the original packing materials, if available. Do not enclose any loose components.
3. Send the communication module to the designated service and repair centre.

8 Maintenance

The CU-XE communication module requires no maintenance.

Caution

Never use running water for cleaning

Communication modules must not be cleaned under running water or with compressed air. Water ingress can cause short-circuits or damage components.

9 Decommissioning and disposal

Note

Electronic waste treatment

This product must not be disposed of in regular waste. Use a professional electronic waste treatment process.

The components used to manufacture the device can, in the main, be broken down into constituent parts and sent to an appropriate recycling or disposal facility. When the product is removed from use, the whole product must be sent to a professional electronic waste treatment process. The waste treatment and disposal plants must be approved by local regulatory authorities.

The end processing of the product and recycling of its components must always be carried out in accordance with the rules and regulations of the country where the end processing and recycling are done.

On request, Landis+Gyr will provide more information about the environmental impact of the product.

Note

Disposal and environmental protection regulations

The following are general guidelines and should NOT take priority over local disposal and environmental policies which should be adhered to without compromise.

Components	Disposal
Printed circuit boards	Delivered to recycling plants
Metal components	Sorted and delivered to metal recycling plants
Plastic components	Sorted and delivered to re-granulation if possible

© Landis+Gyr

10 Terms and abbreviations

The following terms and abbreviations are used in this document.

Term	Definition
10-BASE-TX	Ethernet standard for transmitting data at the nominal speed of 10 Mbit/s.
100-BASE-TX	Fast Ethernet standard for transmitting data at the nominal speed of 100 Mbit/s.
DHCP	Dynamic Host Configuration Protocol.
DLMS	Device Language Message Specification is a set of standards developed by the DLMS User Association.
IEC 62056-21	IEC 62056-21 is a standard for Electricity metering - Data exchange for meter reading, tariff and load control - Part 21: Direct local data exchange.
IEC 60870-5-104	IEC 60870-5-104 is a standard for telecontrol (SCADA) in electrical engineering and power system automation applications.
IPv4	Internet Protocol version 4. An internet protocol.
SCADA	Supervisory Control and Data Acquisition Control system architecture comprising computers, networked data communications and graphical user interfaces for high-level process supervisory management.
TLS	Transport Layer Security is a cryptographic protocol for secure Internet communications.
UI	User Interface

11 Third-party software used and open source (OS) software licenses

A document containing all information related to the licensing of open source software packages and third-party software for the E65C CU-XE communication module and its associated software components:

https://www.landisgyr.com/webfoo/wp-content/uploads/2012/12/LandisGyr-Third-Party-Open-Source-Licensing-for-E65C-and-E66C-Devices.pdf

© Landis+Gyr

Contact:
Landis+Gyr AG
Alte Steinhauserstrasse 18
CH-6330 Cham
Switzerland
Phone: +41 41 935 6000
www.landisgyr.com

Landis+Gyr
manage energy better