CMe3100
User's Manual
English
v 1.5

Content

1 DOCUMENT NOTES 6

1.1 COPYRIGHT AND TRADEMARK 6
1.2 CONTACT INFORMATION 6
1.2.1 Headquarter 6
1.2.2 Technical Support 6

2 IMPORTANT USAGE AND SAFETY INFORMATION 7

3 USING THIS MANUAL 8

3.1 PURPOSE AND AUDIENCE 8
3.2 ONLINE RESOURCES 8
3.2.1 Product information 8
3.2.2 Documentation 8
3.3 NOTATION 8
3.3.1 Navigation 8
3.4 SYMBOLS 9

4 INTRODUCTION 10

4.1 PURPOSE 10
4.2 BUILT IN DATABASES 10
4.3 APPLICATION DESCRIPTION 10
4.3.1 Applications 10
4.3.2 Quick and simple metering with integrated statistics 11
4.3.3 Metering and local integration with PLC/DCS 11
4.3.4 Full Gateway integration using DLMS or REST 12
4.4 PRODUCT FEATURES 12
4.5 COMPATIBILITY AND EXTENSIONS 13
4.5.1 Licensing scheme 13
4.5.2 Integration with other products 13
4.5.3 Wired and Wireless M-Bus 13

5 GETTING STARTED 15

5.1 PURPOSE 15
5.2 PRODUCT SPECIFICATION 15
5.3 MOUNT THE DEVICE 15
5.4 CONNECT THE DEVICE 15
5.4.1 Power supply 15
5.4.2 M-Bus Master 16
5.4.3 M-Bus slave ports 16
5.4.4 Ethernet 16
5.4.5 IR interface 16
5.4.6 USB Port 16
5.4.7 Wiring Diagram 17
5.5 START UP THE DEVICE 17
5.5.1 Start-up 17
5.5.2 Reset to factory default 17
5.5.3 LED indications 17
5.6 ACCESS THE WEB INTERFACE 18
5.6.1 Log in on the web interface from a browser 18
5.6.2 Change the default administrator password 19

6 OPERATIONS GUIDE 20

BASIC OPERATIONS 20
6.1 PURPOSE 20
6.2 USE THE INSTALLATION PANEL TO PERFORM BASIC SETUP 20
6.3 SET THE TIME 20
6.3.1 Configure time settings 20
6.4 CONFIGURE NETWORK SETTINGS 21
6.4.1 Configure IP address settings 22
6.4.2 Change the hostname (optional) 22
6.4.3 Set the Domain Name Server 23
6.5 INSTALL METERS 23
6.5.1 Create and install a list of Wired M-Bus meters 25
6.5.2 Create and install a list of Wireless M-Bus meters 26
6.5.3 Install meters through a meter search 26
6.6 DOWNLOAD A COMMISSION REPORT FOR INSTALLED METERS 27
6.6.1 Download a Commission Report 27
6.7 SCHEDULE METER READOUTS 28
6.7.1 Activate and set the meter readout schedule 28
6.8 CONFIGURE PUSH REPORT DEFAULT SETTINGS 29
6.8.1 Configure e-mail Push Report default settings 29
6.8.2 Configure FTP Push Report default settings 31
6.8.3 Configure HTTP Push Report default settings 32
6.9 SCHEDULE PUSH REPORTS AND EVENT REPORTS 33
6.9.1 Enable and configure Push Reports 34
6.9.2 Enable and configure Event Reports 35
COMMON OPERATIONS 37
6.10 PURPOSE 37
6.11 CREATE A CONFIGURATION FILE 37
6.11.1 Save non-device specific settings in a configuration file 37
6.12 CREATE A BACKUP FILE 38
6.12.1 Save meter values and device specific settings in a backup file 38
6.13 CHECK DEVICE AND METER SETTINGS 39
6.13.1 Check status through the System Panel 40
6.13.2 Check the system overview 40
6.13.3 Download a meter settings report 41
6.14 CHECK OPERATIONAL STATUS OF THE SYSTEM 42
6.14.1 Filter the System Log 42
6.14.2 Set the minimum severity level of logged events 43
6.14.3 Set when M-Bus status byte is logged in meter log 44
6.14.4 Check the readout status of an individual meter 45
6.15 INSTALL ENCRYPTION KEYS FOR WIRELESS METERS 46
6.15.1 Add an encryption key through a file upload 47
6.15.2 Add an encryption key directly in the web interface 48
6.15.3 Link an encryption key to an individual meter 49
6.16 CONFIGURE SETTINGS FOR AN INDIVIDUAL METER 51
6.16.1 Edit Measurement Object Identification of a meter 51
6.16.2 Configure communication settings of an individual meter 52
SPECIAL OPERATIONS 54
6.17 PURPOSE 54
6.18 UPDATE SOFTWARE 54
6.18.1 Perform a software update 54
6.19 ADMINISTRATE USER ACCOUNTS 55
6.19.1 Add a new user account 55
6.19.2 Edit an existing user account 56
6.19.3 Delete an existing user account 56
6.20 ADD A NEW LICENSE 57

6.20.1 Upload and save license ... *57*
6.21 PERFORM AN ADVANCED METER SEARCH ... 58
6.21.1 Customize the meter search ... *58*
6.22 PERFORM MANUAL METER READOUTS ... 59
6.22.1 Perform a manual readout of all installed meters ... *60*
6.22.2 Perform a manual readout of an individual meter ... *60*
6.23 ACTIVATE THE CONTINUOUS READOUT MODE ... 61
6.23.1 Enable continuous meter readouts ... *61*
6.24 ENABLE SECURITY FEATURES ... 62
6.24.1 Upload a certificate for device authentication ... *62*
6.24.2 Enable HTTPS to access web interface ... *63*
6.24.3 Authenticate receiving servers of HTTPS/FTPS/ Push Reports ... *64*
6.24.4 Enable HTTPS/FTPS for individual Push Reports ... *65*
6.25 CONFIGURE M-BUS SETTINGS ... 65
6.25.1 Set the way meters are searched for ... *65*
6.25.2 Configure M-Bus time and retry settings ... *67*
6.25.3 Configure M-Bus multi telegram settings ... *68*
6.25.4 Configure M-Bus settings of an individual meter ... *69*
6.26 ACCESS THE M-BUS FROM A MASTER DEVICE ... 70
6.26.1 Enable a master device to communicate directly on the M-Bus ... *71*
6.27 ACCESS METER READINGS FROM A MASTER DEVICE ... 72
6.27.1 Allow a master device to collect meter values from the database ... *72*
6.28 USE M-BUS SLAVE PORTS FOR VIRTUAL OR TRANSPARENT M-BUS ... 74
6.28.1 Activate and configure the settings of the M-Bus slave ports ... *74*
6.29 ALLOW A MASTER DEVICE TO PERFORM READOUTS OVER MODBUS ... 76
6.29.1 Enable meter readouts over Modbus ... *76*
6.30 MONITOR METERING STATUS USING SNMP ... 78
6.30.1 Enable and configure the SNMP service ... *79*
6.30.2 Set recipients of SNMP traps (optional) ... *81*
6.31 ENABLE AUTOMATIC UPDATES OF CONFIGURATION SETTINGS ... 82
6.31.1 Enable and configure the Auto Configuration service ... *82*
6.32 CONFIGURE ADVANCED PUSH REPORT SETTINGS ... 83
6.32.1 Disable Adaptive Retries ... *84*
6.32.2 Configure the Value Period ... *85*
6.32.3 Configure the Value Interval ... *86*
6.32.4 Configure the Push Report timeout settings ... *87*
6.33 CONFIGURE JOB RETRIES ... 88
6.33.1 Configure retry settings for scheduled and manual jobs ... *88*
6.34 ACCESS THE DEVICE THROUGH A CONSOLE APPLICATION ... 89
6.34.1 Enable and configure the console application ... *89*
6.35 USE ON DEMAND REPORTS ... 91
6.35.1 Enable and configure the On Demand Report ... *91*
6.36 CONFIGURE IDENTITY SETTINGS ... 93
6.36.1 Customize the Push Report identity settings ... *93*
6.36.2 Configure localization settings for Push Reports ... *94*
6.37 PERFORM A REBOOT OF THE DEVICE ... 95
6.37.1 Reboot the device ... *95*
6.38 RESET THE DEVICE TO FACTORY DEFAULT SETTINGS ... 96
6.38.1 Perform a factory reset ... *96*
6.39 CUSTOMIZE SERVICE AND JOB SCHEDULES ... 97
6.39.1 Specify schedules using cron patterns ... *97*

7 TECHNICAL SPECIFICATIONS ... 99

7.1 CHARACTERISTICS ... 99

8 TYPE APPROVALS 102

9 DOCUMENT HISTORY 103

9.1 VERSIONS 103
9.2 DOCUMENT SOFTWARE AND HARDWARE APPLIANCE 103

10 REFERENCES 104

10.1 TERMS AND ABBREVIATIONS 104

1 Document notes

All information in this manual, including product data, diagrams, charts, etc. represents information on products at the time of publication, and is subject to change without prior notice due to product improvements or other reasons. It is recommended that customers contact Elvaco AB for the latest product information before purchasing a CMe Series product.

The documentation and product are provided on an “as is” basis only and may contain deficiencies or inadequacies. Elvaco AB takes no responsibility for damages, liabilities, or other losses by using this product.

1.1 Copyright and Trademark

© 2016, Elvaco AB. All rights reserved. No part of the contents of this manual may be transmitted or reproduced in any form by any means without the written permission of Elvaco AB. Printed in Sweden.

CMe Series is a trademark of Elvaco AB, Sweden.

1.2 Contact information

1.2.1 Headquarter

Elvaco AB
Kabelgatan 2T
434 37 Kungsbacka
SWEDEN
Phone: +46 300 93 99 00
E-Mail: info@elvaco.com
Online: https://www.elvaco.se

1.2.2 Technical Support

E-Mail: support@elvaco.se
Online: https://support.elvaco.com

2 Important usage and safety information

The following safety precautions must be observed during all phases of the operation, usage, service, or repair of any CMe Series product. Users of the product are advised to convey the following safety information to users and operating personnel and to incorporate these guidelines into all manuals supplied with the product. Failure to comply with these precautions violates safety standards of design, manufacture and intended use of the product. Elvaco AB assumes no liability for customer’s failure to comply with these precautions.

The product is developed for indoor use. If the product is intended to be used outdoors, it must be protected by an enclosure of International Protection Marking (IP code) 67.

The installation of the product should be performed by a qualified electrician or another professional with the required knowledge. It is important to follow all safety information mentioned throughout the installation chapter of this manual when installing the CMe3100.

Make sure to read this manual carefully and follow it step by step to ensure a secure usage and to get the most out of your product.

3 Using this manual

3.1 Purpose and audience

This manual provides all information needed to mount, install, configure, and use the CMe3100 M-Bus Metering Gateway, and is intended for field engineers and developers. The information is based on firmware version 1.9.6. Please note that other versions may exhibit slight differences in appearance and/or functionality.

3.2 Online resources

3.2.1 Product information

information about all products and services provided by Elvaco can be found on the Elvaco website: https://www.elvaco.se

3.2.2 Documentation

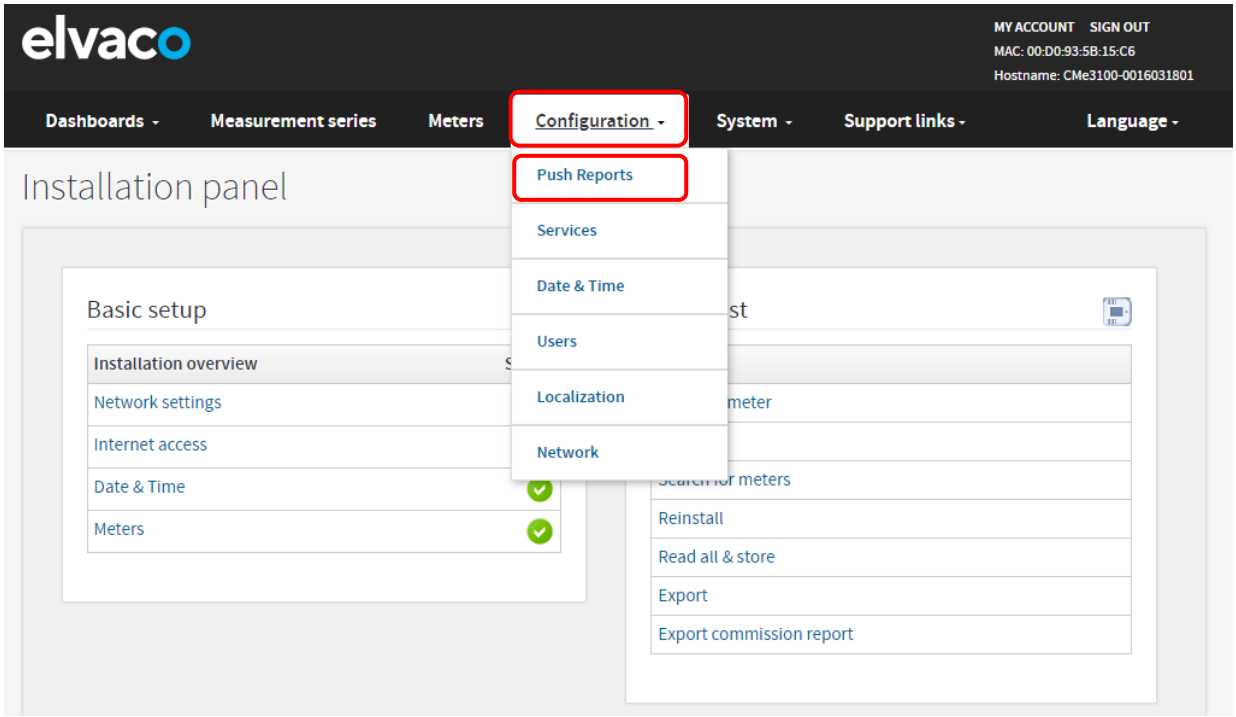
Latest versions of the CMe3100 production documentation (this manual and others) can be found on the Elvaco website:
https://www.elvaco.se/en/product/infrastructure/cme3100-m-bus-metering-gateway-for-fixed-network--CMe3100

3.3 Notation

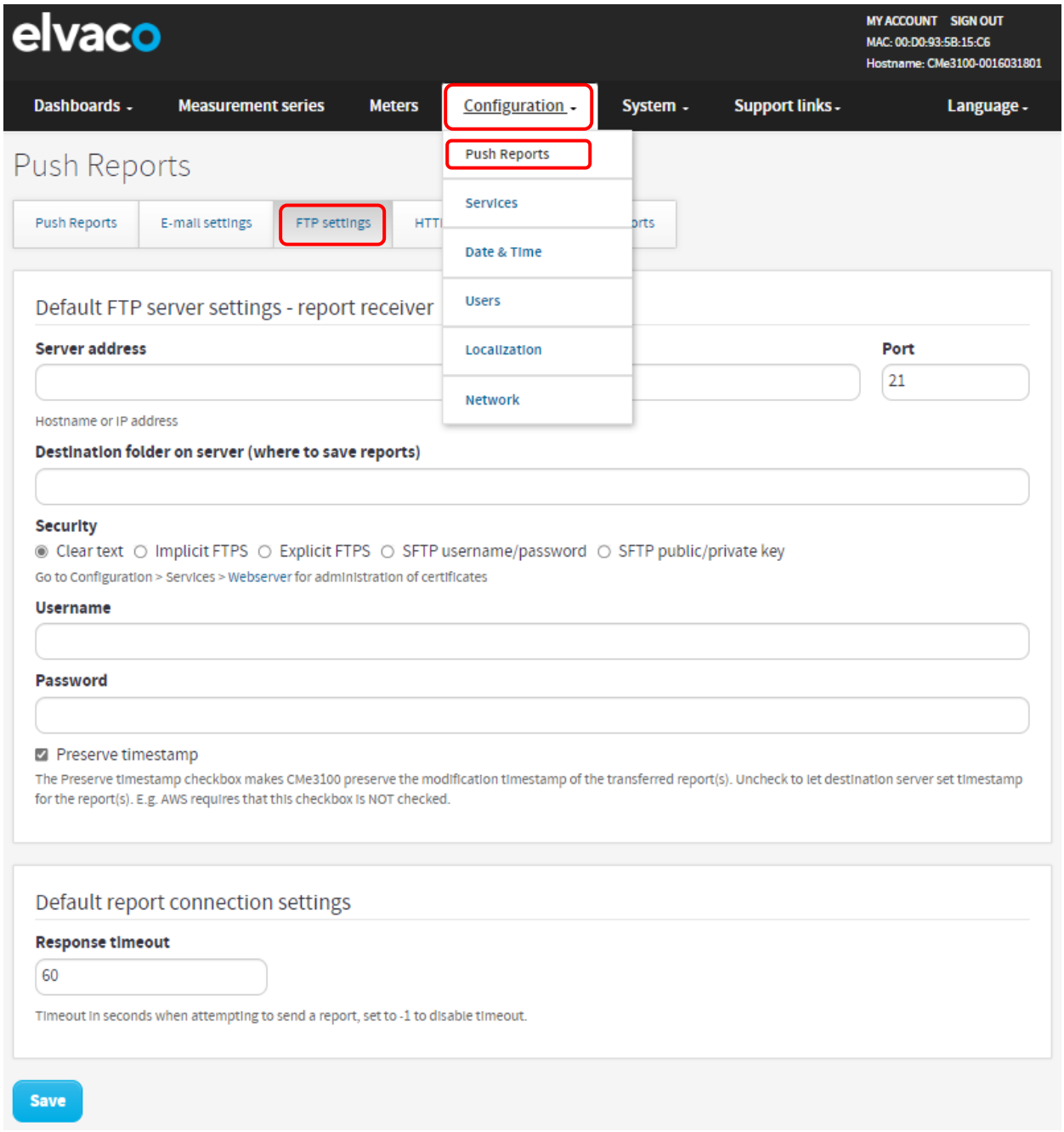
3.3.1 Navigation

All navigation in the web-interface is described referencing the **Dashboards > Installation Panel** (start page when logging in). Navigation will be noted as [**Top menu item**] > [**Sub menu item**] > [**Tab item**].

Example 1: To display Push Reports, go to **Configuration > Push Reports**.



Example 2: To configure FTP Push Report default settings, go to **Configuration** > **Push Reports** > **FTP settings**.



3.4 Symbols

The following symbols are used throughout the manual to emphasize essential information and useful tips:

The Note symbol is used to mark information that is important to take into consideration for safety reasons or to assure correct operation of the Metering Gateway.

The Tip symbol is used to mark information intended to help you get the most out of your product. It can for example be used to highlight a customization option related to the current section.

4 Introduction

4.1 Purpose

This chapter provides an initial description of the CMe3100 Metering Gateway and how it can be applied to several types of metering systems. In the next-coming sections you will get to know the product features and how to combine the CMe3100 with other products to build versatile solutions.

4.2 Built in databases

The built-in database, storing all meter values locally in the CMe3100, provides a solid base for its system robustness. This means that historical meter values can be recovered by the head-end system or locally in the CMe3100. How far back the values track depends on the resolution of meter data, see chapter 7 (data specification).

Besides the meter value database, there is also a log database, or logfile. This database stores all activities in the CMe3100 in textual form. To avoid flooding the log database with the same repeated messages, there is a one minute back off for messages with the same origin and message text. This means that when one minute has passed:

1. There is a message summarizing the log by stating the number of messages that was suppressed by the flooding protection mechanism.
2. If the same message appears again, one instance of that message will be logged again before being re-suppressed.

From FW 1.9.10 and forward, the log database has the following requirements:

- maximum size limit of 100MB
- maximum history of the log is 1 month
    - The device will continuously delete all entries older than 1 month
- At the start of a firmware update process, the log database is **always** deleted and replaced with default database
- S90 startup script always checks database size; if it is over 100MB it will be deleted and replaced with default database
    - If device detects that database has a size over 100MB during runtime the device restarts, which activates S90 startup script

4.3 Application description

4.3.1 Applications

The CMe3100 is, directly out of the box, a powerful and versatile M-Bus Metering Gateway. It can be extended in several ways using a flexible model for licence and add-on upgrades.

While there are many ways to utilize the potential in the CMe3100, its three core application areas are:

1. Quick and simple metering with integrated statistics
2. Metering and local integration with PLC/DCS
3. Full Gateway integration using e.g., DLMS or REST

Additionally, all features can be used in a mix to address application specific needs. It also fully supports all types of utility meters that are M-Bus or Wireless M-Bus compliant.

4.3.2 Quick and simple metering with integrated statistics

For small applications with a low requirement for integration, the CMe3100 is very quick to set up using its predefined readout schedules and metering reports (Push Reports). Once the meters have been installed, the device can be configured to readout meter values at specific time intervals and compile them in a suitable report format to be sent to a receiving system. If the need for integration is low, the report can be as simple as an e-mail sent at a fixed schedule.

Thanks to the device's built-in M-Bus decoder, meter values can be delivered in a human readable format with correct precision and unit. With its user-friendly web interface, the device also serves as a complete metering web service. Among various features, measurement series and calculated series, such as mean value, can be displayed as illustrative graphs.

The built-in database, storing all meter values locally in the CMe3100, provides a solid base for its system robustness. All Push Reports have an intelligent retry mechanism that automatically schedules retries for failed reports including all values for which previous transmissions have failed.

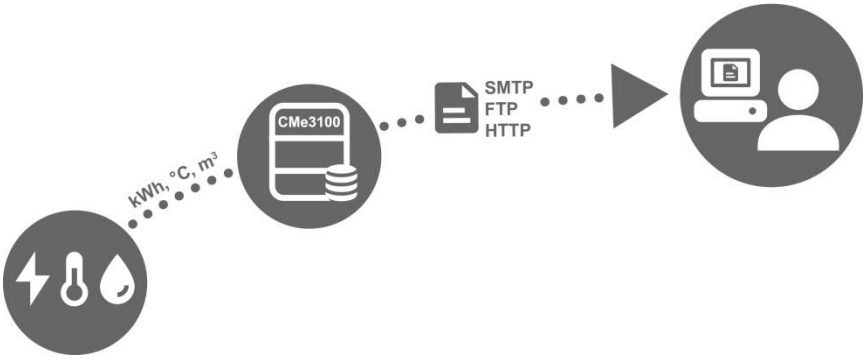


Figure 1: Quick and simple metering with integrated statistics

4.3.3 Metering and local integration with PLC/DCS

For standard applications with a medium requirement for integration, the CMe3100 is very quickly setup using its predefined readout schedules and metering reports (Push Reports). Once the meters have been installed, the device can be configured to readout meter values at specific time intervals and compile them in a suitable report format to be sent to a receiving system. Reports are transmitted using standardized internet protocols, such as SMTP (e-mail), FTP or HTTP.

Thanks to the device's built-in M-Bus decoder, meter values can be delivered in a human readable form with correct precision and unit.

The built-in database, storing all meter values locally in the CMe3100, provides a solid base for its system robustness. All Push Reports have intelligent retry mechanisms that automatically schedules retries for failed reports including all values for which previous transmissions have failed.

The built-in database also enables excellent and reliable options for local integration with a Digital Control System (DCS) or a Programmable Logic Controller (PLC). These types of system components are usually found in real-estate systems to control, for example heat and ventilation. Interfacing systems may choose to connect using Modbus, M-Bus, or JSON (TCP/IP) to retrieve meter values directly from the CMe3100 without affecting its normal operation or having to communicate with the M-Bus meters directly.

If the CMe3100 is used in a mixed application with metering reports and high demand for real-time meter values being supplied to a PLC or a DCS, there is an additional mode available, *Continuous Readout Mode.* When activated, the CMe3100 reads all meters as frequent as possible and makes the readouts available to interfacing systems *but* without affecting the reporting mechanism. This enables metering reports to be configured independently from how the interfacing system's meter value requirements.

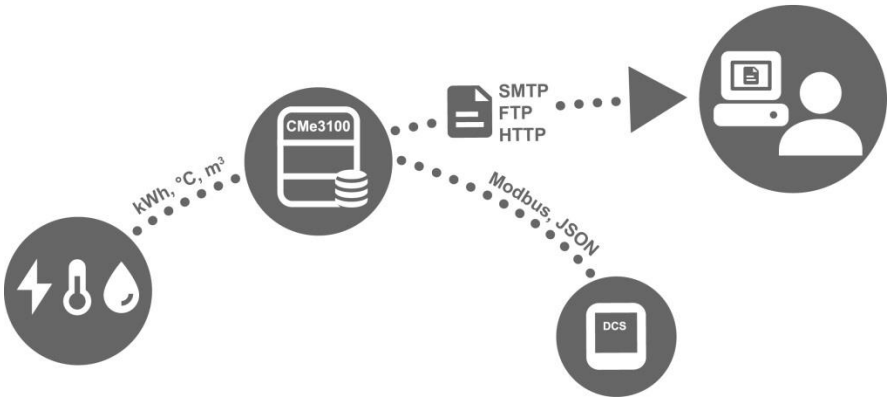


Figure 2: Metering and local integration with DCS

4.3.4 Full Gateway integration using DLMS or REST

For demanding applications that require vertical integration, the CMe3100 supports the REST or DLMS protocols. Using these protocols, meter values and configuration settings are available without having to bother about specific details of the M-Bus metering format. A head-end system may access most current readouts, historical values as well as log information, Meter Lists and change notifications. CMe3100 is certified by DLMS organization.

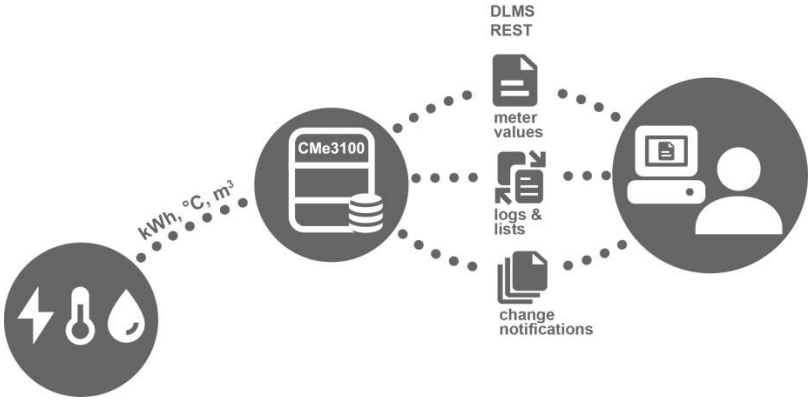


Figure 3: Full Gateway integration

4.4 Product features

The CMe3100 M-Bus Metering Gateway has the potential to read, convert and deliver meter values from all types of M-Bus meters, regardless of manufacturer. This makes the device quick and easy to integrate into an existing M-Bus system. The key features of the product include:

- An integrated M-Bus Master which can drive up to 32 unit loads (32T). By using one or two Elvaco M-Bus Master it is possible to extend this number up to 256 or 512 unit loads.
- Customized meter value reports via HTTP, FTP, and e-mail.
- A built-in web interface for easy configuring of settings.
- Remotely updatable software.
- Meter value integration via MODBUS, REST, JSON-RPC and DLMS.

A more extensive technical description of the Metering Gateway is provided in chapter 7 (Technical specifications).

4.5 Compatibility and extensions

4.5.1 Licensing scheme

The CMe3100 is equipped with a flexible licensing scheme that allows its capabilities and features to be enhanced through the addition of license files. This allows for both cost-effective customization at the purchase point as well as the possibility to later extend the product functionality without changing the hardware.

Licenses are distributed as files, bound to a specific serial number. A license file may contain several licensing options, but an individual file is always required for each product.

There are two main categories of licenses available, performance and feature licenses.

The performance licenses determine, from a software perspective, how many meters may be used with the device. Licenses range from 8 to 512 meters in steps of 8, 32, 64, 128, 255 and 512.

Feature licenses enable new services in the product, for example integration protocols such as Modbus, REST, JSON, Stream mode and DLMS.

To learn more about the different licenses available, please visit:

https://www.elvaco.se/en/product/infrastructure1/cme3100-m-bus-metering-gateway-for-fixed-network--CMe3100.

A software update is not necessary when changing the licenses, the functionality is already part of the software and just needs the correct license file to be unlocked.

Without a software license, the product is limited to 8 meters even though the integrated M-Bus master can handle up to 32 unit loads.

4.5.2 Integration with other products

The CMe3100 can be used in combination with an M-Bus Master from Elvaco to increase the number of slave devices it is able to drive (the device can by default drive up to 32 unit loads, where one load equals 1.5 mA). It can also be combined with an Elvaco Wireless M-Bus Receiver to receive meter reading from wireless meters using the Wireless M-Bus Protocol.

The CMe3100 is compatible with a wide range of meters, including:

- ABB electricity meters using IR interface communication.
- All types of M-Bus meters, regardless of manufacturer.
- The following temperature and humidity sensors, manufactured by Elvaco: CMa10, CMa10W, CMa11, CMa11W, CMa12W, CMa20, CMa20W.

4.5.3 Wired and Wireless M-Bus

The CMe3100 can be used together with Wired M-Bus meters, Wireless M-Bus meters, or a combination of both. The integrated M-Bus master can handle up to 32 unit loads so for smaller systems, the CMe3100 may operate independently. For larger systems, the number of M-Bus devices the CMe3100 can drive is easily extendable through any of Elvaco's M-Bus Masters in combination with a licence upgrade.

CMe3100 has a built-in system for wireless encryption key handling and can easily be integrated in a Wireless M-Bus metering system. To receive wireless meters, the CMe3100 needs to be complemented with an Elvaco Wireless M-Bus Receiver.

All extension devices, Wireless Receivers and M-Bus Masters from Elvaco are equipped with IR interface

to enable communication without any cabling by simply stacking the devices together.

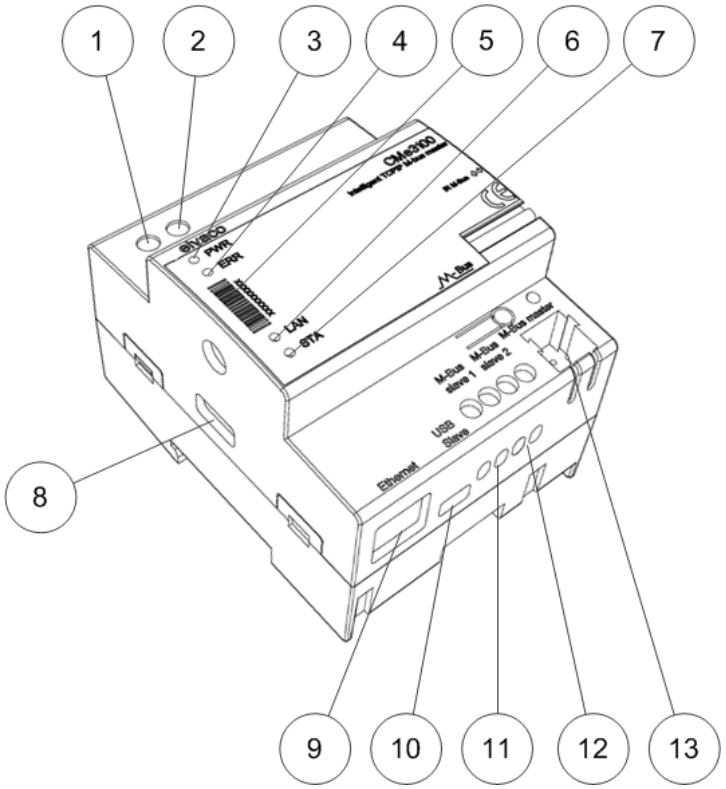
Elvaco offers box-build turnkey solutions, containing all necessary products preconfigured, directly from factory.

5 Getting started

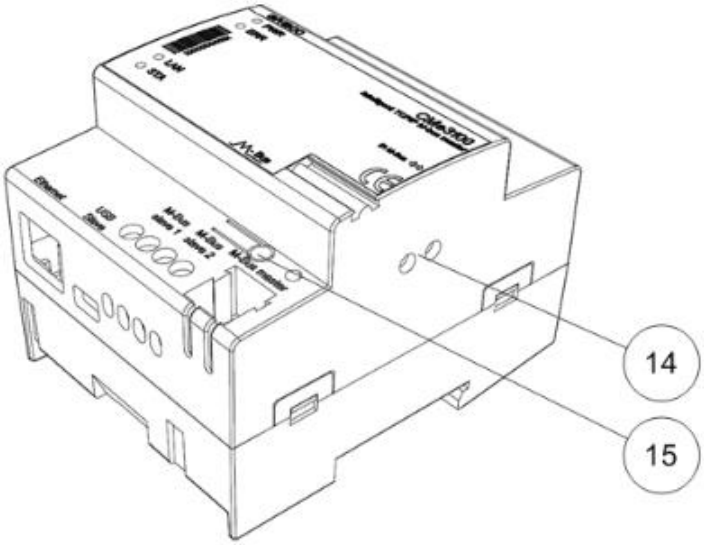
5.1 Purpose

This chapter provides instructions on how to get started with the CMe3100. After reading and carefully following each step of this chapter, the Metering Gateway will have started up, and you will have logged into its integrated web interface.

5.2 Product specification



1. Power supply L
2. Power supply N
3. Green LED
4. Red LED
5. Serial number
6. Yellow LED
7. Blue LED
8. USB Master
9. Ethernet connection
10. USB Slave
11. M-Bus slave 1
12. M-Bus slave 2
13. M-Bus master
14. IR interface
15. Push button



5.3 Mount the device

The CMe3100 is mounted on a DIN-rail. The metallic clip on the bottom is used to attach and detach the CMe3100. For safety reasons, a DIN-rail enclosure must cover the terminals.

5.4 Connect the device

5.4.1 Power supply

Screw terminal (1) and (2) are used to supply the device with power. The main supply voltage should be in the range of 100-240 VAC, with a frequency of 50/60Hz. The power needs to be connected by a clearly marked and easily accessible switch to make sure the device can be switched off during service work. On successful connection of power, the red LED and the green LED will begin to flash after undergoing a booting session of approximately 20 seconds.

⚠	The installation should be performed by a qualified electrician or another professional with the required knowledge.

⚠	The power supply must be protected with a 10 A circuit breaker of characteristics C or slow blow fuse.

5.4.2 M-Bus Master

The CMe3100 is equipped with an M-Bus master port (13), which can be used to connect (up to) 32 slave devices (32 M-Bus loads, 48mA). If more than 32 slave devices need to be connected to the CMe3100, an M-Bus Master from Elvaco can be used to extend its limit. Use a cable with a cross sectional area of 0.25-1.5 mm^2, e.g., a standard telephone cable EKKX 2x2x0.5 may be used to connect the CMe3100 with its slave devices.

⚠	Do not exceed the maximum cable length of 1000 m.

5.4.3 M-Bus slave ports

CMe3100 is equipped with two M-Bus slave ports, which are used to share meter values with another M-Bus device, for example a DCS. Connect a cable of cross-sectional area 0.25-1.5 mm^2 between the M-Bus device and port (11) or (12) of the CMe3100.

5.4.4 Ethernet

The CMe3100 is equipped with an Ethernet port to be able to connect to the local network. Use a cable of at least category 5e and connect it to the Ethernet port (9). On successful network connection, the yellow LED (6) will be permanently on or flashing, indicating active communication.

5.4.5 IR interface

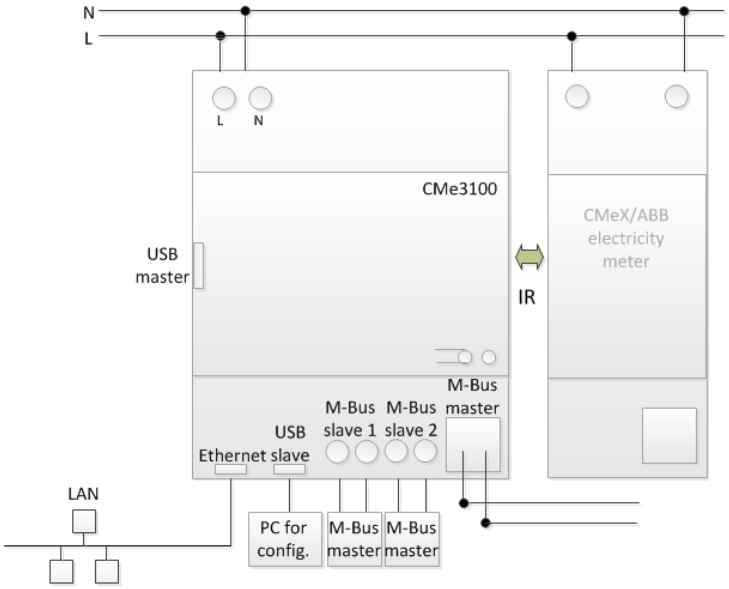
The CMe3100 supports communication with all ABB electricity meters equipped with the IR interface as well as all products from the Elvaco CMeX series. To use the IR functionality, remove the shield (14) and mount the CMe3100 right next to the device it will communicate with.

⚠	Do not remove the IR shield unless the IR interface is going to be used.

5.4.6 USB Port

The CMe3100 is equipped with a USB slave port (10) to make it able to connect to a computer and install the integrated web interface. By using the web interface, device and M-Bus settings are conveniently configured.

5.4.7 Wiring Diagram



5.5 Start up the device

5.5.1 Start-up

When connected to a power supply, the CMe3100 will undergo a boot-up for approximately 20 seconds. Thereafter, the green LED (3) and the red LED (4) will begin to flash, and the device is ready to use.

5.5.2 Reset to factory default

To reset the product configurations to factory default, press and hold the push button (15) on power-up until the green and red LED lights flashes fast. Now release the button. The product configuration will be reset to factory default and the product will restart.

5.5.3 LED indications

The product is equipped with four LED lights. The green LED displays current operations, the red LED indicates error, and the yellow LED displays the network status. Table 1-3 below provides an explanation of each LED indication.

Green LED	Product state	Visual
Permanently off	No power or boot mode	
Short flashes	Normal operation	
50 percent on/50 percent off	Booting in progress	
Permanently on	Software error indication	

Table 1: Green LED

Red LED	Product state	Visual
Permanently off	Normal operation	
50 percent on/50 percent off	Network problems or booting in progress	
Permanently On	M-Bus master short circuit protection active	

Table 2: Red LED

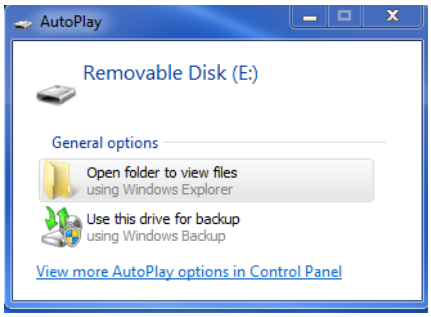
Yellow LED	Product state	Visual
Permanently off	Network connection to Ethernet port is missing	
Short flashes	Ongoing communication on network	
Permanently on	Ethernet port connected to network	

Table 3: Yellow LED

5.6 Access the web interface

5.6.1 Log in on the web interface from a browser

The CMe3100 is configured through its web interface, which is easily reached via the local USB slave port (10). Connect the included USB cable between a computer and the Metering Gateway. After approximately 30 seconds, a new removable disk will be available on the computer. Open the folder on the removable disk, run the file CMe3100-SETUP.EXE and follow the instructions.

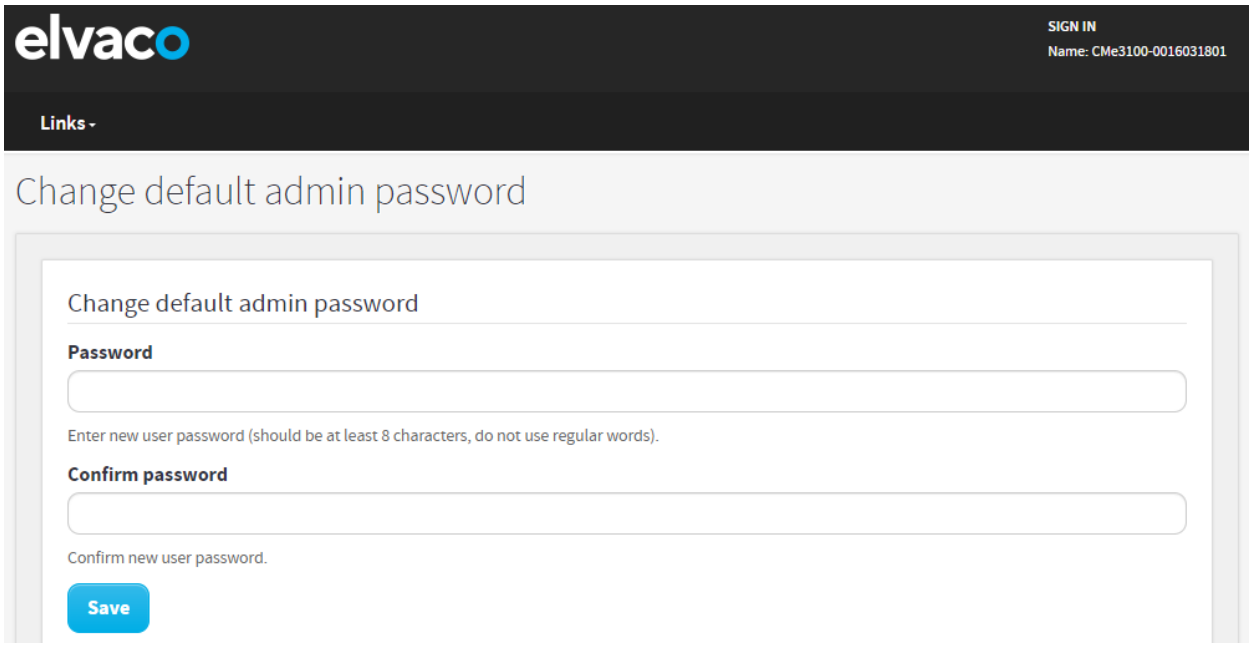


When the installation has completed, the web browser will open along with a login page. If the browser fails to do so, please enter the IP address for the device USB port manually. For software versions older than 1.6.0, the IP address 192.168.100.1 is used. For software version 1.6.0 or later, use the IP address 169.254.254.1.

Login using the following credentials:
Username: admin
Password: admin

After logging in for the first time, a new password will have to be registered.

⚠	If the SETUP.EXE utility has already been run once on the computer, it will not have to be run again. The utility has installed a driver that creates a virtual TCP/IP connection on the computer which accesses the CMe3100 using the local IP address.



5.6.2 Change the default administrator password

Use a strong password with at least 8 characters consisting of both letters and numbers. The password is case sensitive. Make sure to write your credentials down, since the only way of resetting the password is through a factory reset of the product.

6 Operations guide

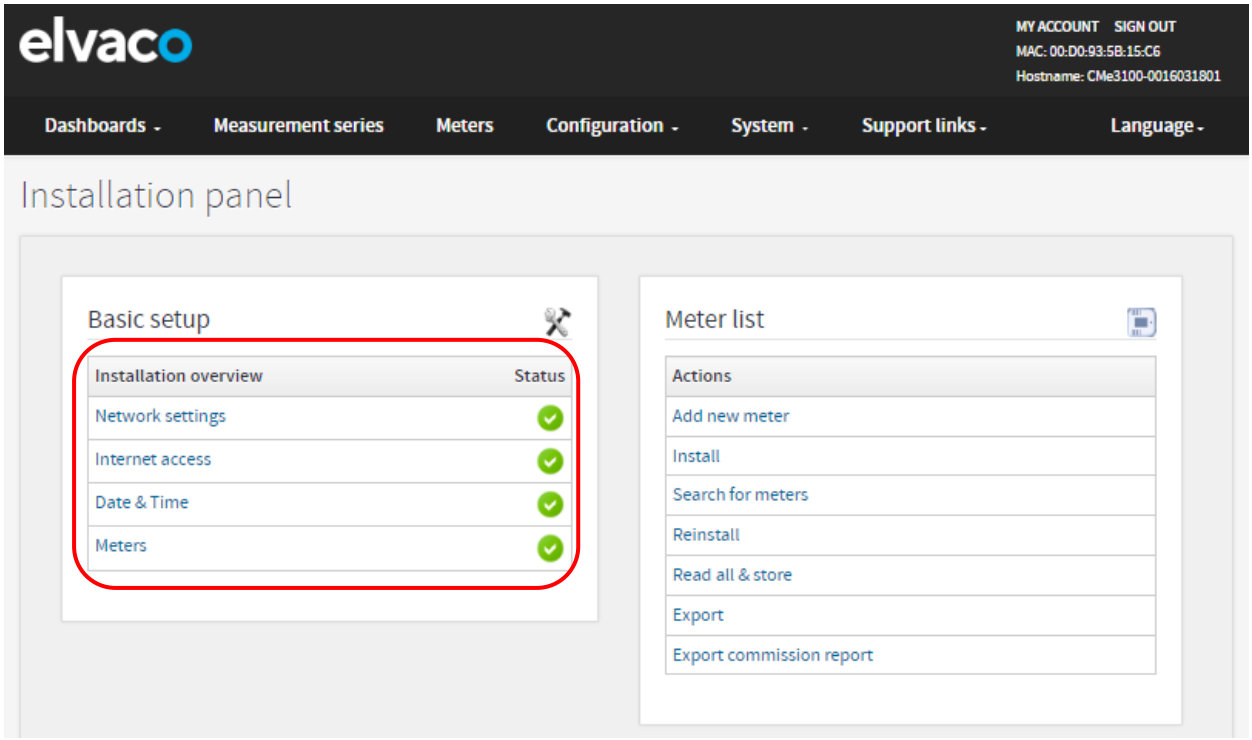
Basic operations

6.1 Purpose

This chapter provides instructions on how to use the web interface to configure the most basic settings of the CMe3100. After executing each step of this chapter, the Metering Gateway will perform scheduled readouts of its installed meters and deliver customized reports with meter values. Please read each step carefully.

6.2 Use the installation panel to perform basic setup

When logging in on the web interface, the Installation panel will be presented. From this page, all parts of the basic setup process are easily accessible. To ensure correct operation of the product, time and network settings should be configured first.



6.3 Set the time

Purpose

For the device to operate accurately, it is important to set the correct time and make sure that the clock stays synchronized. This is done by synchronizing it with a time server at a fixed time interval and selecting the maximum accepted time difference the device's clock is allowed to have.

6.3.1 Configure time settings

To configure time settings:

- Go to **Date & Time** from the Basic setup window of the Installation panel. Enter the time and select the time zone.
- Set the Time synchronizing schedule and the Maximum accepted time difference.
- Enter the address of the NTP (Network Time Protocol) time server and a server timeout

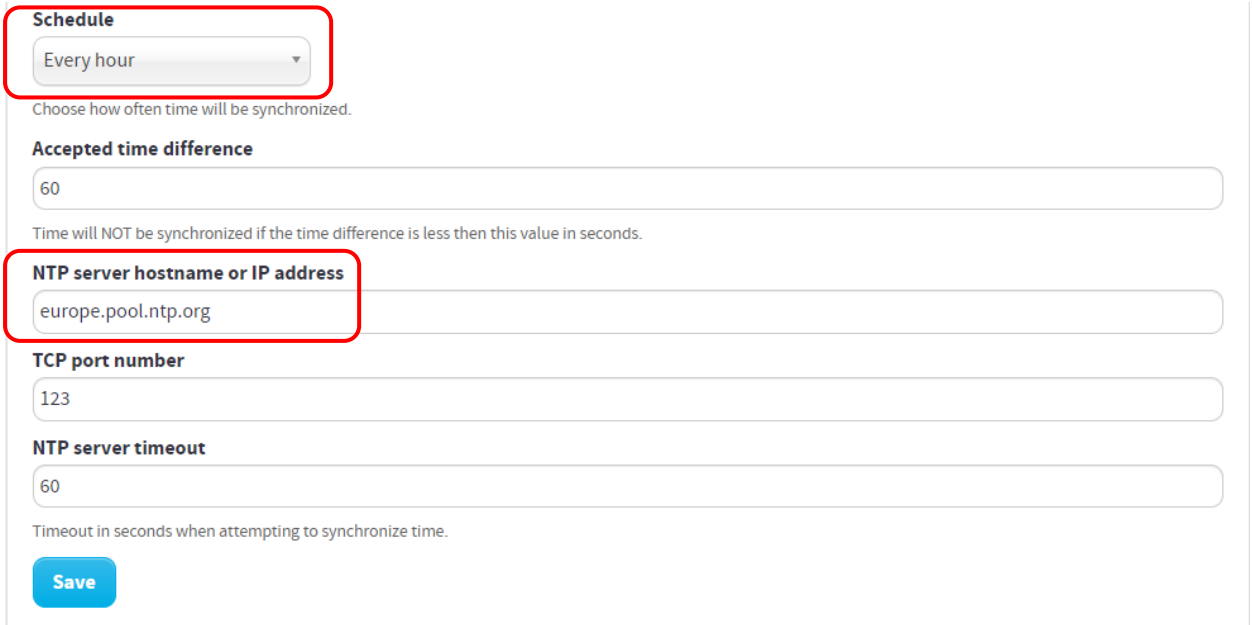
value. The timeout determines for how long the Metering Gateway will wait for the time server to respond during a time synchronization attempt before interrupting the action.

- Click **Save**.

The time synchronizing schedule that should be used depends on how tightly clocks need to be synchronized. Assuming that the maximum accepted time drift is in the order of one minute per month, utilizing a schedule of every 12th hour should assure that the product has less than one second's time difference (31 days * 24 hours = 744 hours, 60 seconds / 744 hours * 12 hours = 0,97 seconds). The default value will work well in most cases and allow for an ample timeout.
If the radio link between the product and the time server is of inadequate quality, the value might have to be increased until reliable operation is obtained. It is important to note that a radio link with inadequate quality will negatively affect the performance of the time synchronization as it relies on low latency communication.

You may disable the use of time synchronization and manually enter time and date in the product if the long-term accuracy is not a concern. However, be aware of:

- The product has a built-in super capacitor to maintain time and date during e.g., a power outage but it will only last around 24 hours. After that, the clock will no longer be running, and time will be offset accordingly.
- The built-in clock will drift over time, theoretical worst case is around the order of one minute per month but will be smaller in practice and will vary due to temperature, tolerances, and age of components.
- If you are using multiple products for collecting meter values, it is very strongly advised that you configure the products to use time synchronization to ensure that measurements from several sources are aligned with regards to time and date.



6.4 Configure network settings

Purpose

Configuring the basic network settings will enable the Metering Gateway to connect to the network. This is necessary to enable the Metering Gateway to connect to servers and deliver its collected meter data.

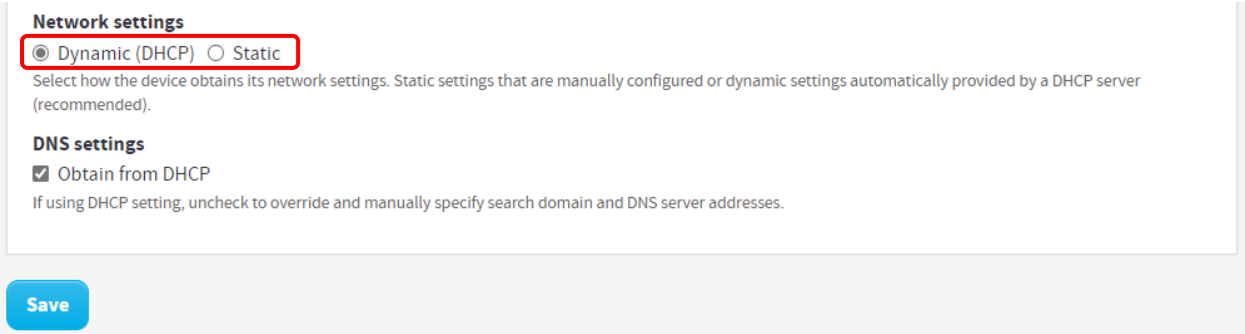
6.4.1 Configure IP address settings

There are two types of IP address assignment options available, the static and the dynamic option. Using a static IP address enables assignment of the IP address manually. It will thereafter stay constant over time. By instead using dynamic IP addressing, an available IP address is automatically assigned to the Metering Gateway through a DHCP server, which must be available on the local network.

To configure the IP address settings:

- Go to **Network settings** from the Basic setup window in the Installation panel or via **Configuration > Network**
- Select whether to use static or dynamic IP address assignment. If selecting the static option, enter IP-addresses and a netmask.
- Click **Save**.

It is highly recommended that you use dynamic IP-address assignment to avoid mistakenly duplicated IP-addresses and make IP-address administration as easy as possible. Please refer to your IT administrator for details and/or more information about what network settings to use.



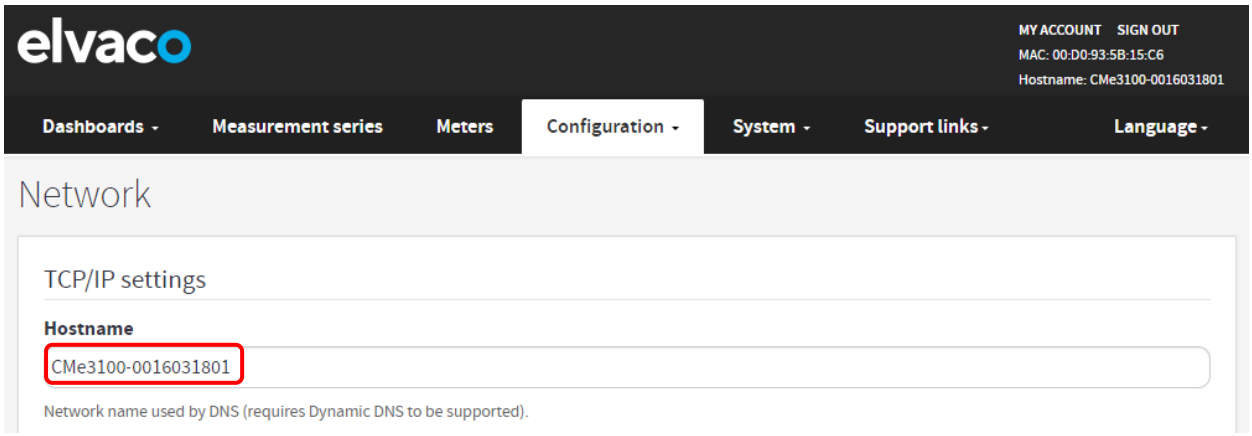
6.4.2 Change the hostname (optional)

The hostname setting determines which name the Metering Gateway will use to identify itself on the network. If not changed, a default name based on the product name and serial number will be used, e.g., “cme3100–0016002383”. The hostname is ONLY used for network addressing and should not be confused with the product’s name, the latter is used to identify the product in e.g., Push Reports. For more information about how to configure the device name used in Push Reports, see section 6.34 (Configure identity settings)

To change the hostname of the device:

- Go to **Network settings** from the Basic setup window in the Installation panel or via **Configuration > Network**
- Enter the name that will be assigned the Metering Gateway.
- Click **Save**.

Your DHCP server must have enabled support for dynamic DNS update to support resolution of the hostname to an IP-address. Please refer to your IT administrator for details and/or more information about what features that are supported.

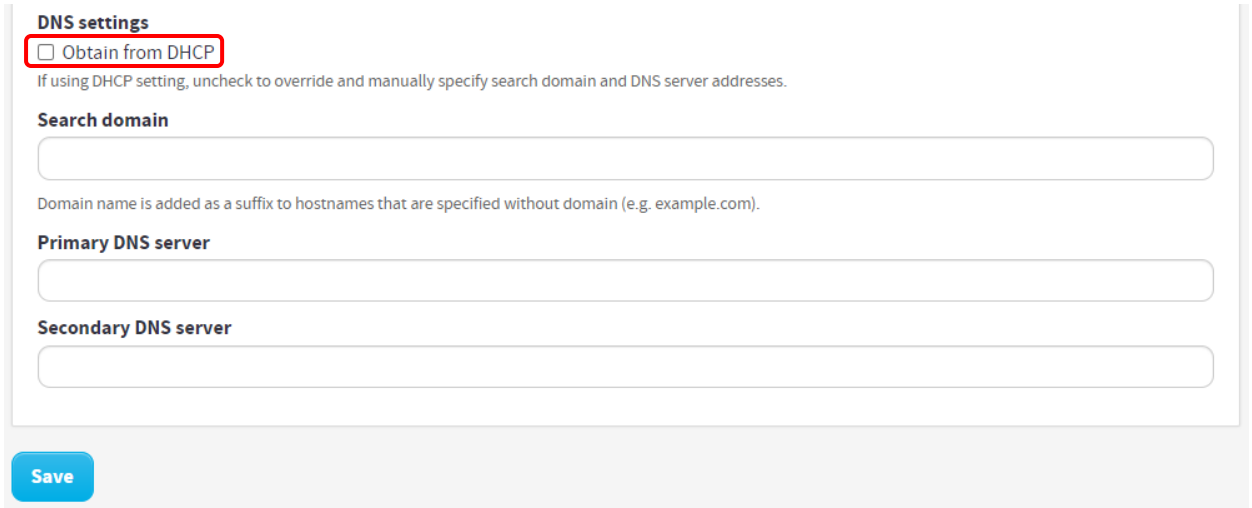


6.4.3 Set the Domain Name Server

The Domain Name Server (DNS) is used to find and retrieve information about the IP address corresponding to a certain domain name. DNS information can be configured manually or be obtained from a Dynamic Host Configuration Protocol (DHCP) server.

To set a Domain Name Server (DNS):

- Go to **Network settings** from the Basic setup window in the Installation panel or via **Configuration > Network**
- Choose to obtain DNS from DHCP server or add DNS information manually.
- Click **Save**.



6.5 Install meters

Purpose

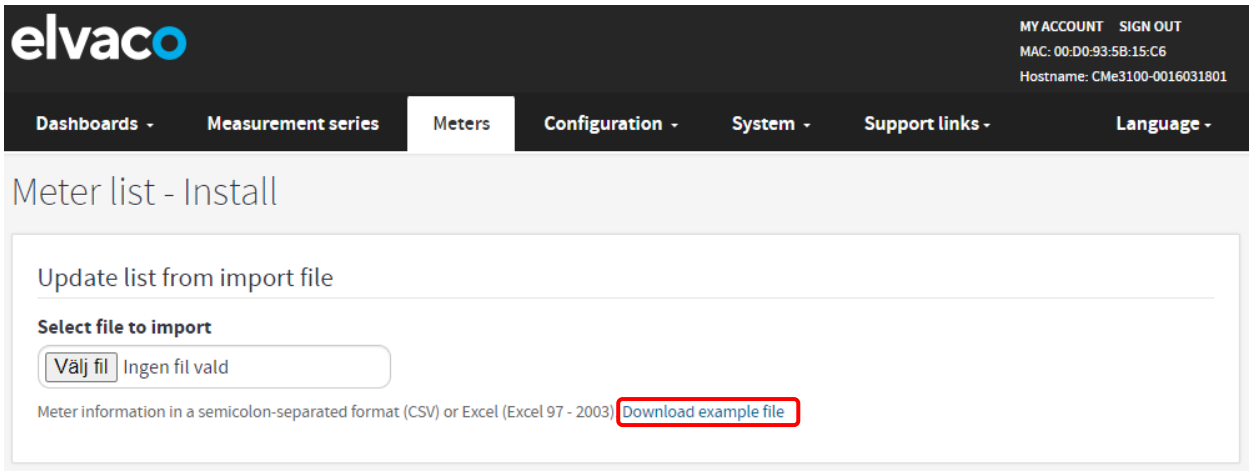
The Meter List contains information about all meters that the device will read and needs to be uploaded to the web interface before meters can be installed.

Figure 4 illustrates the template of such a Meter List and Table 4: Meter list fields explains what information should be added to each field. The Meter List template is available for download directly from the web interface under **Meters > Install**.

If not aware of the addresses of the meters, it is possible to perform an automatic search and installation of meters without uploading a Meter List. However, this also means that you will have to verify that the “right” meters have been installed after the installation has completed.

When the installation has completed, all installed meters will be displayed in the Meter List of the web interface, under **Meters > Meter List**. A Commission Report should always be downloaded after the installation to help ensure it was successful.

> ⚠ Make sure that your licence matches the number of meters included in the Meter List. If you try to install more meters than your licence supports, some will be marked as passive. By going to **Meters > Meter List** and check **Show passive meters**, passive meters will be displayed.



	A	B	C	D	E	F
1	Position	SecondaryAddress	BaudRate	AddressingMode	PrimaryAddress	EnhancedAddress
2						
3						
4						
5						
6						
7						
8						
9						
10						

Figure 4: Template of Meter List

Column	Explanation
Position	The position represents the name that will be used to identify the meter in the Meter List of the web interface. It may be arbitrarily chosen, but it is recommended to assign the field a name that relates to the meter’s function, e.g., its position in the metering system.
SecondaryAddress	The secondary address is set by the manufacturer and is printed on the meter. This address is unique for each device and expressed as an 8-digit number.
BaudRate	The Baud rate determines the speed of communication between the Metering Gateway and the meters. Set the field to “300” or “2400” (bit/s), but make sure that all meters support the baud rate selected.

AddressingMode	The addressing mode sets the way meters are addressed by the Metering Gateway. There are three options: the primary and the secondary addressing mode used for Wired M-Bus and the enhanced secondary addressing mode used for Wireless M-Bus. Set this field to one of: • primary • Secondary • esecondary
Primary Address (optional)	The primary address is assigned to the meter by the user as a number between 0 and 255. The column is optional to fill out. However, if using primary addressing mode, it will have to be included.
Enhanced Address (optional)	The enhanced address is only used when communication with the meters is held through a Wireless M-Bus Receiver. Nothing needs to be added to this column.

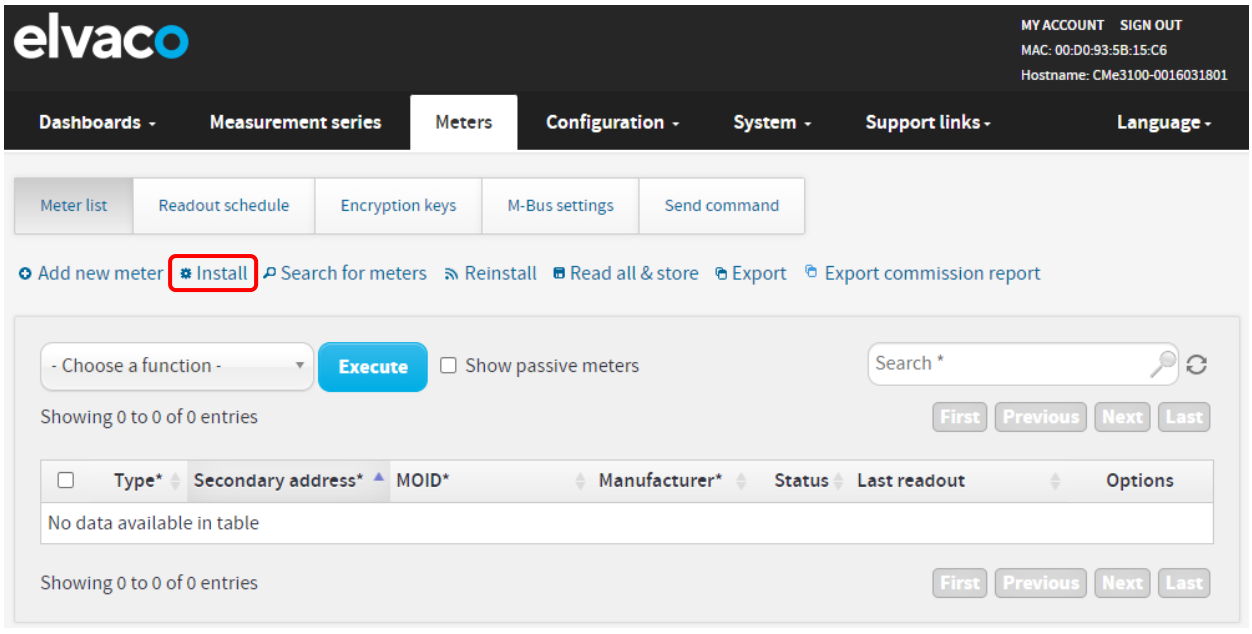
Table 4: Meter list fields

6.5.1 Create and install a list of Wired M-Bus meters

When using Wired M-Bus, each meter is addressed using either its primary or secondary address. It is recommended to use the secondary addressing mode, since this will ensure that each meter is addressed in a unique way.

To create and install a Meter List of Wired M-Bus meters:

- Go to **Meters > Install**.
- Select a Meter List, structured as comma-separated values (CSV format) to upload. The Meter List can be created in Excel and saved as a CSV file. Figure 5 illustrates what a Meter List might look like. The template can be downloaded from the web interface.
- Click **Install** to upload the Meter List to the web interface and install the included meters.



	A	B	C	D	E	F
1	Position	SecondaryAddress	BaudRate	AddressingMode	PrimaryAddress	EnhancedAddress
2	Cafeteria	13001651	2400	Secondary		
3	Sales office	14290591	2400	Primary	221	
4	Reception	67690871	2400	Secondary		

Figure 5: Example file of wired Meter List

6.5.2 Create and install a list of Wireless M-Bus meters

When using Wireless M-Bus, the Metering Gateway communicates with meters through one or several Wireless M-Bus Receivers. Each Elvaco Wireless M-Bus Receiver will assign itself an enhanced address and by combining it with the secondary address of the meter, the communication chain is specified. The Metering Gateway will automatically communicate with each meter through the Wireless M-Bus Receiver that has established the best connection.

To create and install a list of Wireless M-Bus meters:

- Go to **Meters > Install**.
- Select a Meter List, structured as comma-separated values (CSV format) to upload. The Meter List can be created in Excel and saved as a CSV file. Figure 6 illustrates how a Meter List for wireless meters might look. The template can be downloaded from the web interface.
- Click **Install** to upload the Meter List to the web interface and install the included meters.

	A	B	C	D	E	F
1	**Position**	**SecondaryAddress**	**BaudRate**	**AddressingMode**	**PrimaryAddress**	**EnhancedAddress**
2	Cafeteria	61007338	2400	esecondary		
3	Sales office	63000040	2400	esecondary		
4	Reception	74109179	2400	esecondary		

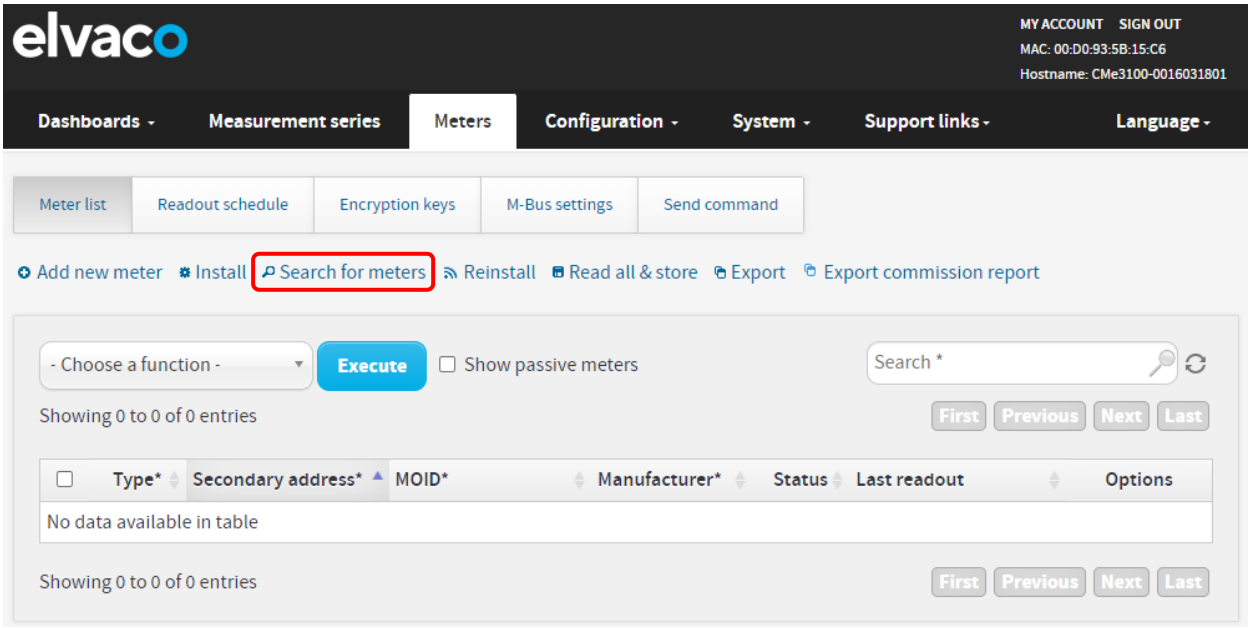
Figure 6: Example file of wireless Meter List

If conditions have changed since the last installation, for example if a meter has been moved, another Wireless M-Bus Receiver might be able to establish a better connection with that meter. By performing a reinstallation, communication will then be held through that Wireless M-Bus Receiver instead. To perform a reinstallation, go to **Meters > Reinstall > Reinstall**.

6.5.3 Install meters through a meter search

To perform an automatic meter search:

- Go to **Meters > Meter List > Search for meters.**
- Select what type of addressing mode will be used in the meter search and installation (wireless, secondary or primary).
- The installation process will start automatically when the search has been completed and might take up to 20 minutes to complete.



6.6 Download a Commission Report for installed meters

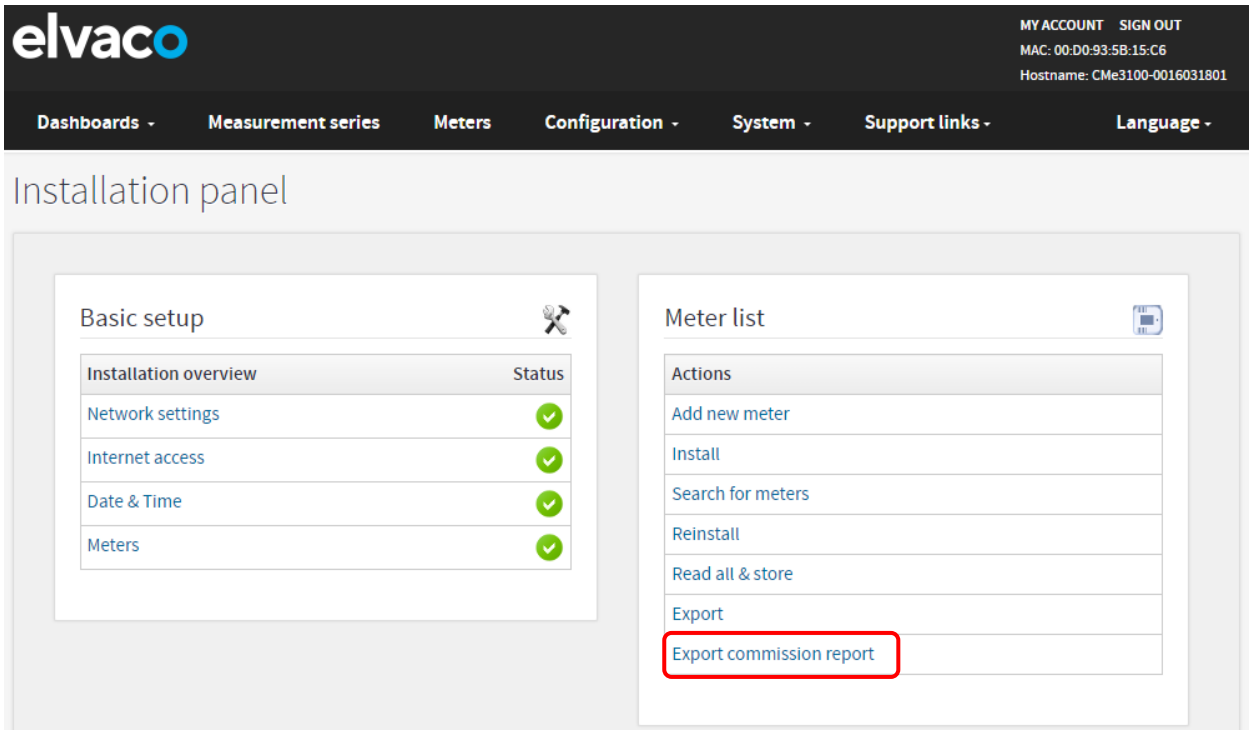
Purpose

After installing the meters, a Commission Report should always be downloaded. This report contains information about the settings of all installed meters and will help ensure that the installation was successful.

6.6.1 Download a Commission Report

To download a Commission Report:

- Click **Export commission report** in the Meter List window of the Installation panel. A download of the document will start.
- Open the downloaded document.
- There are four different tabs in the Commission Report. The first one provides an overview of the Metering Gateway settings, the second tab contains an overview of installed slave devices, the third tab displays the latest value for each measurement series, and the fourth tab provides an overview of what slave devices that have Modbus enabled.



6.7 Schedule meter readouts

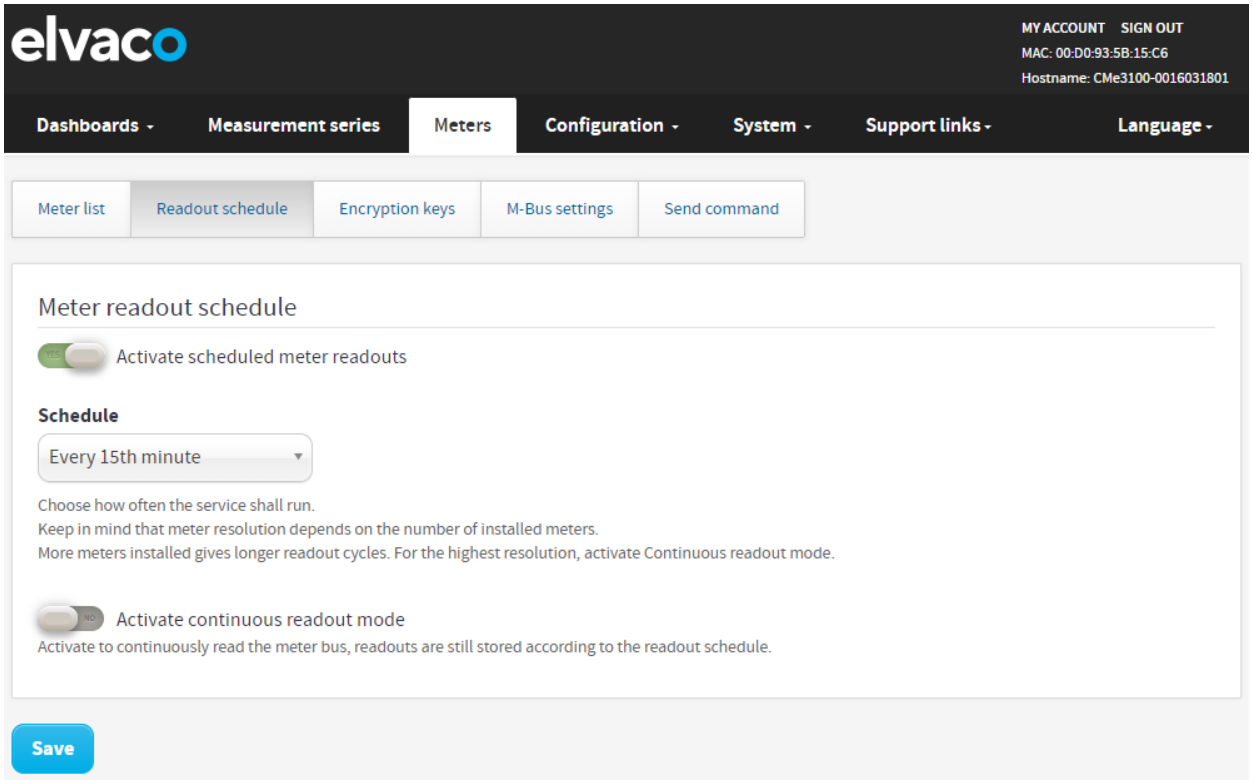
Purpose

When all meters have been installed, a readout schedule can be set. It will determine the time interval by which the Metering Gateway will perform readouts of the meters in its Meter List.

6.7.1 Activate and set the meter readout schedule

To activate and set the meter readout schedule:

- Go to **Meters > Readout schedule** and activate Scheduled meter readouts.
- Set a Meter readout schedule. By for example setting “Every 15th minute”, a readout of all meters in the Meter List will be performed every 15th minute.
- Click **Save**.



6.8 Configure Push Report Default settings

Purpose

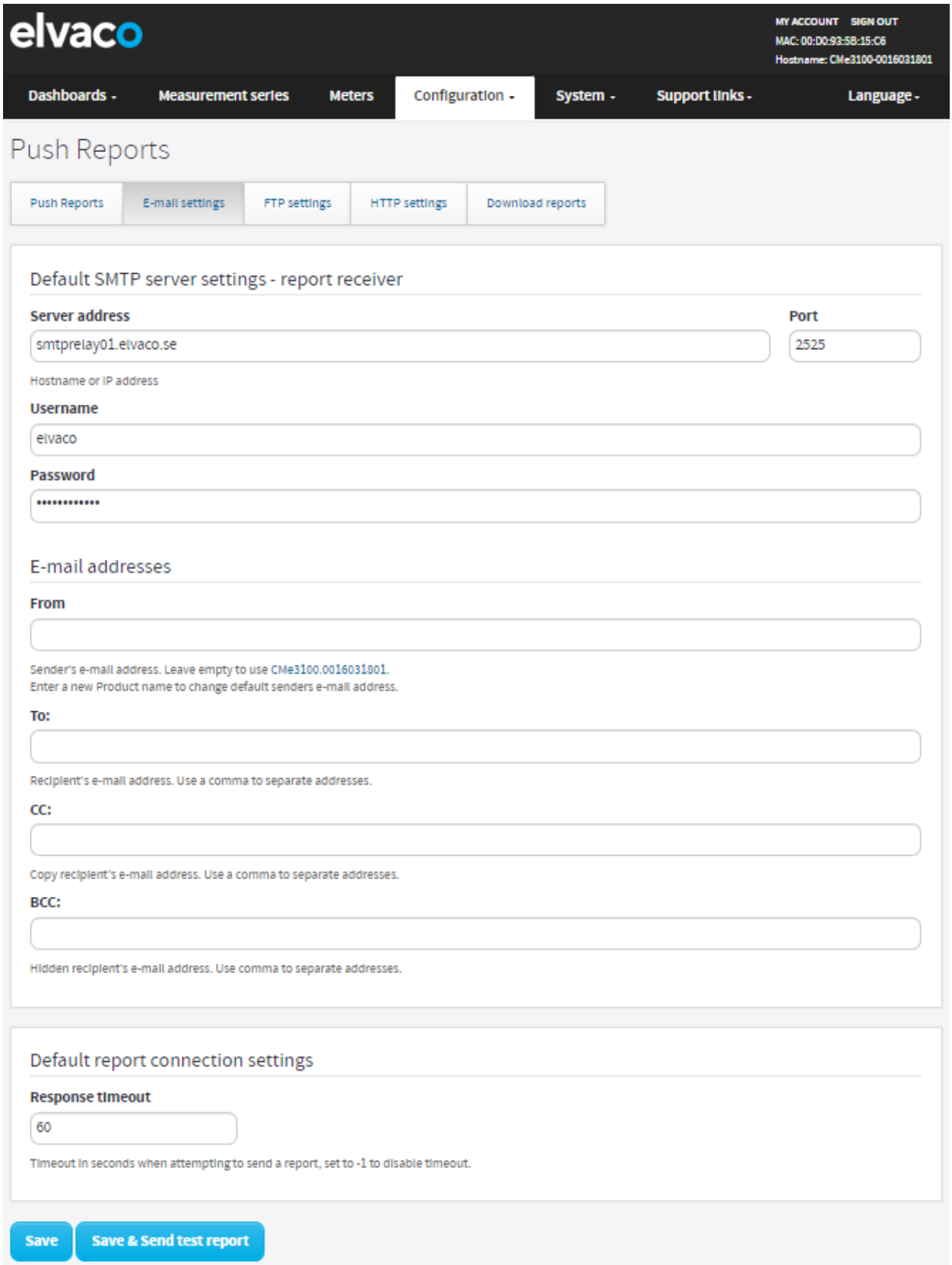
When all meters have been installed and the readout schedule has been set, Push Reports can be enabled. The Push Reports structure the data from the meter readouts by a chosen template and are delivered by a set schedule and protocol.

The Push Reports can be delivered by e-mail (SMTP), as a downloadable file (FTP) or uploaded to a server running a HTTP web service. The first step is to set the default recipient option for the alternatives that will be used. All activated Push Reports will be sent to the default recipient if not overridden in the settings of an individual Push Report.

6.8.1 Configure e-mail Push Report default settings

To configure the e-mail Push Report default settings:

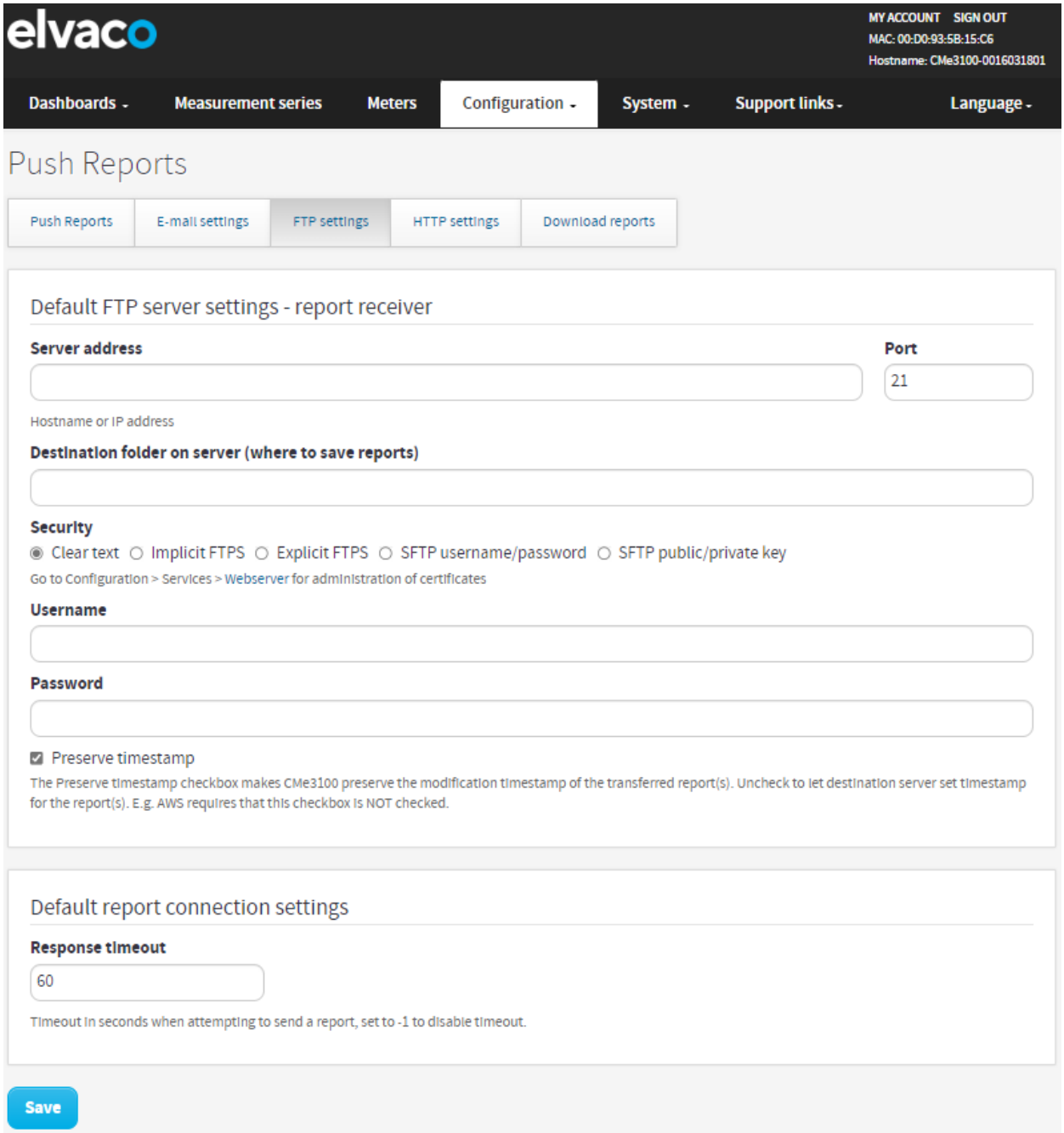
- Go to **Configuration > Push Reports > E-mail settings**.
- Set the address to a valid e-mail server.
- Add credentials used to access the e-mail server.
- Set the e-mail addresses of the default e-mail Push Report recipients.
- Click **Save**.


elvaco
MY ACCOUNT SIGN OUT
MAC: 00:D0:93:5B:15:C6
Hostname: CMe3100-0016031801
Dashboards
Measurement series
Meters
Configuration
System
Support links
Language
Push Reports
Push Reports
E-mail settings
FTP settings
HTTP settings
Download reports
Default SMTP server settings - report receiver
Server address
smtprelay01.elvaco.se
Port
2525
Hostname or IP address
Username
elvaco
Password
E-mail addresses
From
Sender's e-mail address. Leave empty to use CMe3100.0016031801.
Enter a new Product name to change default senders e-mail address.
To:
Recipient's e-mail address. Use a comma to separate addresses.
CC:
Copy recipient's e-mail address. Use a comma to separate addresses.
BCC:
Hidden recipient's e-mail address. Use comma to separate addresses.
Default report connection settings
Response timeout
60
Timeout in seconds when attempting to send a report, set to -1 to disable timeout.
Save
Save & Send test report

6.8.2 Configure FTP Push Report default settings

To configure the FTP Push Report default settings:

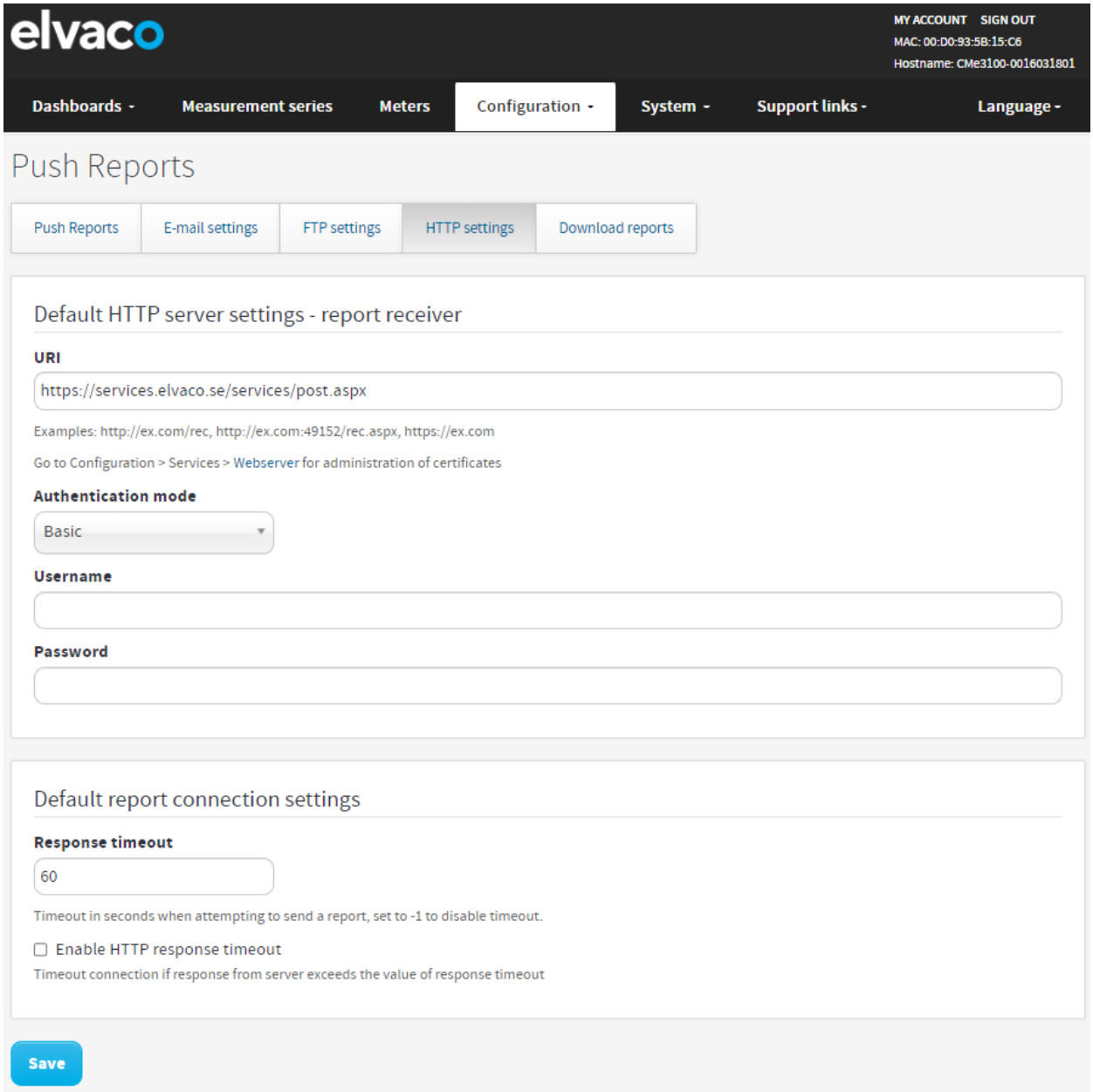
- Go to **Configuration > Push Reports > FTP settings**.
- Set the address to a valid FTP server.
- Add credentials for the CMe3100 to access the FTP server.
- Click **Save**.



6.8.3 Configure HTTP Push Report default settings

To configure the HTTP Push Report default settings:

- Go to **Configuration > Push Reports > HTTP settings**.
- Add a URL to a valid HTTP server where the Push Reports will be received.
- Set the Authentication mode (basic or none). If using the basic mode, add credentials for the CMe3100 to access the HTTP server.
- Click **Save**.



6.9 Schedule Push Reports and Event Reports

Purpose

After the Push Report default settings have been made, individual reports can be configured. By going to **Configuration > Push Report**, an overview of all available reports and their status is provided. There are two types of reports available, Push Reports and Event Reports. The difference between the two is explained in Table 5.

By default, the Metering Gateway supports three protocols for delivering reports:

- E-mail
- FTP
- HTTP

Each delivery protocol has several predefined report templates available. Report template names starts with a unique number depending on the protocol used for transporting the report:

1. E-mail reports
2. FTP reports
3. HTTP reports

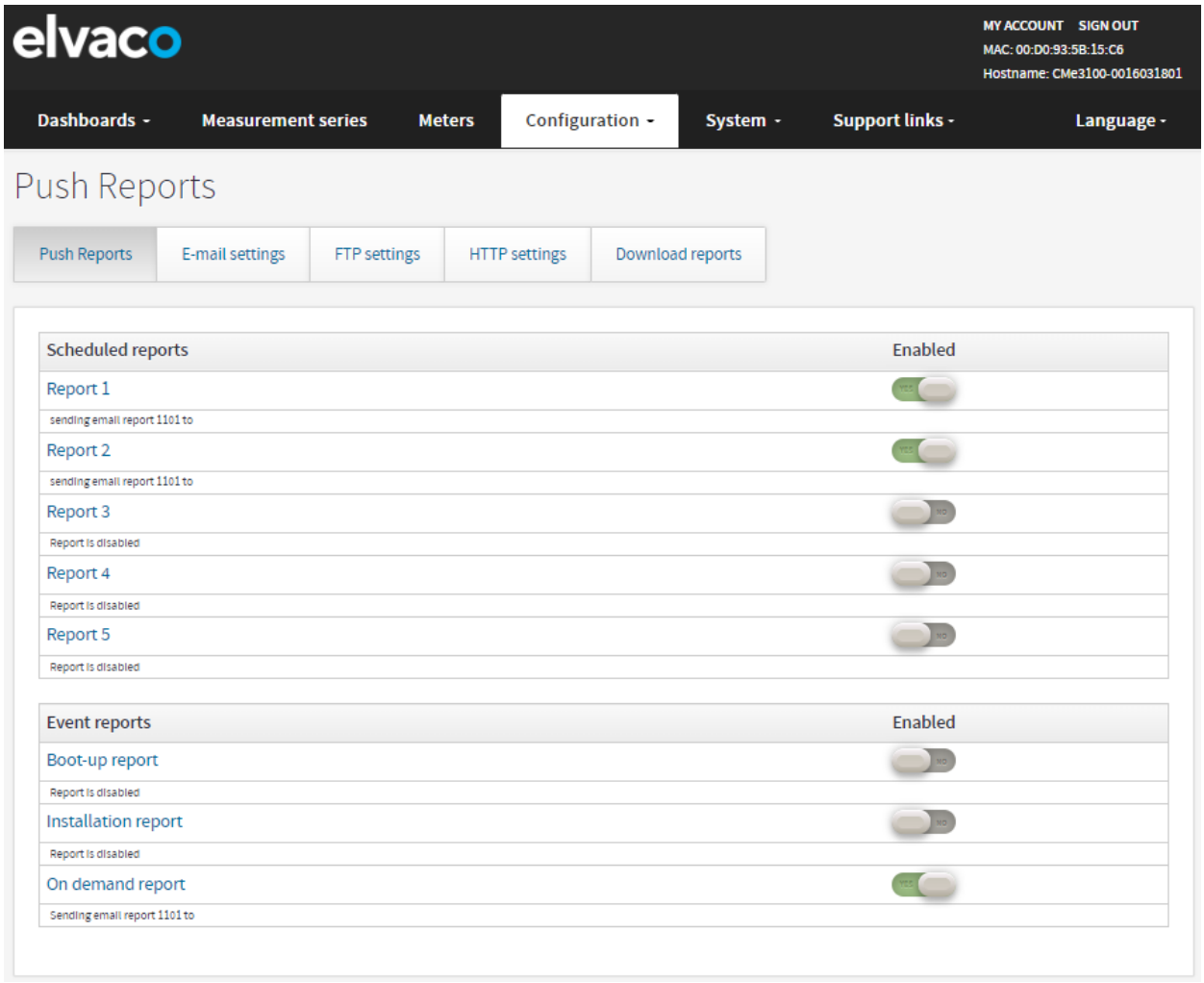
E.g., report *101, a report with all meter values collected in one single post, will be named:

- 1101 when sent as an E-mail report
- 2101 when sent to an FTP server
- 3101 when sent to an HTTP server

To learn more about the different templates available, please visit our support site, https://support.elvaco.com.

Type of report	Explanation
Push Report	Push Reports are used to deliver meter values by a set time interval, structured according to a selected template.
Event Report	The Event Report is triggered by a certain event taking place in the Metering Gateway. A schedule does therefore not have to be set for this type of report.

Table 5: Type of reports

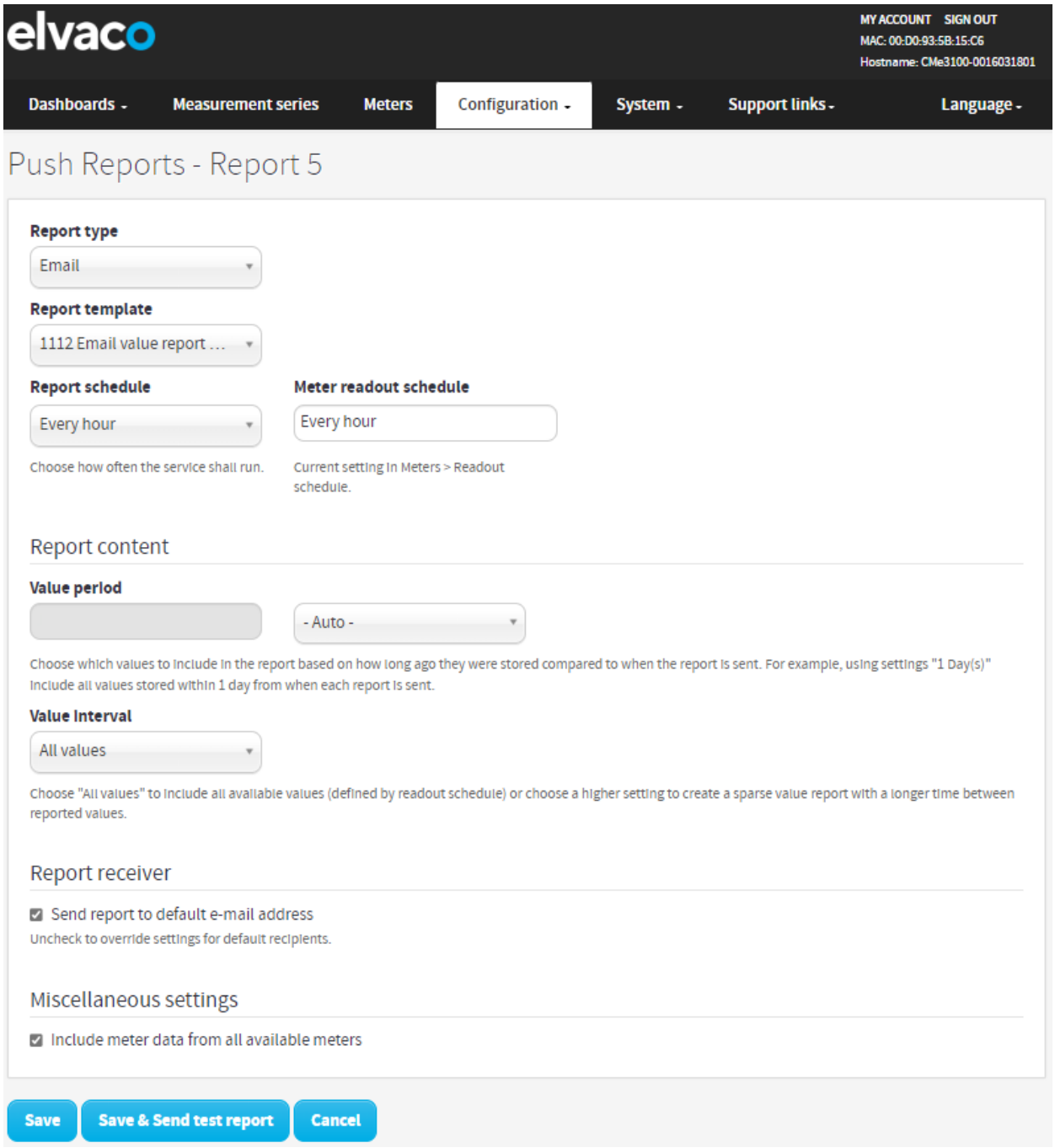


6.9.1 Enable and configure Push Reports

To configure Push Reports:

- Go to **Configuration > Push Report** and click on an arbitrary Push Report.
- Set what type of report to use (e-mail, FTP or HTTP) and the desired template.
- Set the Report schedule, preferably by using one of the preset options available. It will determine the time interval by which the Push Report will be sent
- Set the Value Period to “Auto” to ensure that all new meter values that have failed to be transmitted will be included in the next successful Push Report, thus also providing an automatic recovery mechanism.
- Set the Value Interval to “All Values” to include all available meter readouts in the Push Reports (as defined by the readout schedule).
- Add recipients of the report. If no recipient is added, the default option will be used.
- Click **Save**. By clicking **Save & Send test report** or **Save & Download test report** you will receive a copy of the Push Report, structured according to the template you have selected. In this way, you may test different templates to find the one you wish to use.

> For the advanced user it is possible to customize the Push Report schedule using cron patterns. However, this will also remove the automatic synchronization between readout cycles and report sending and might result in Push Reports being sent before a readout cycle has finished.

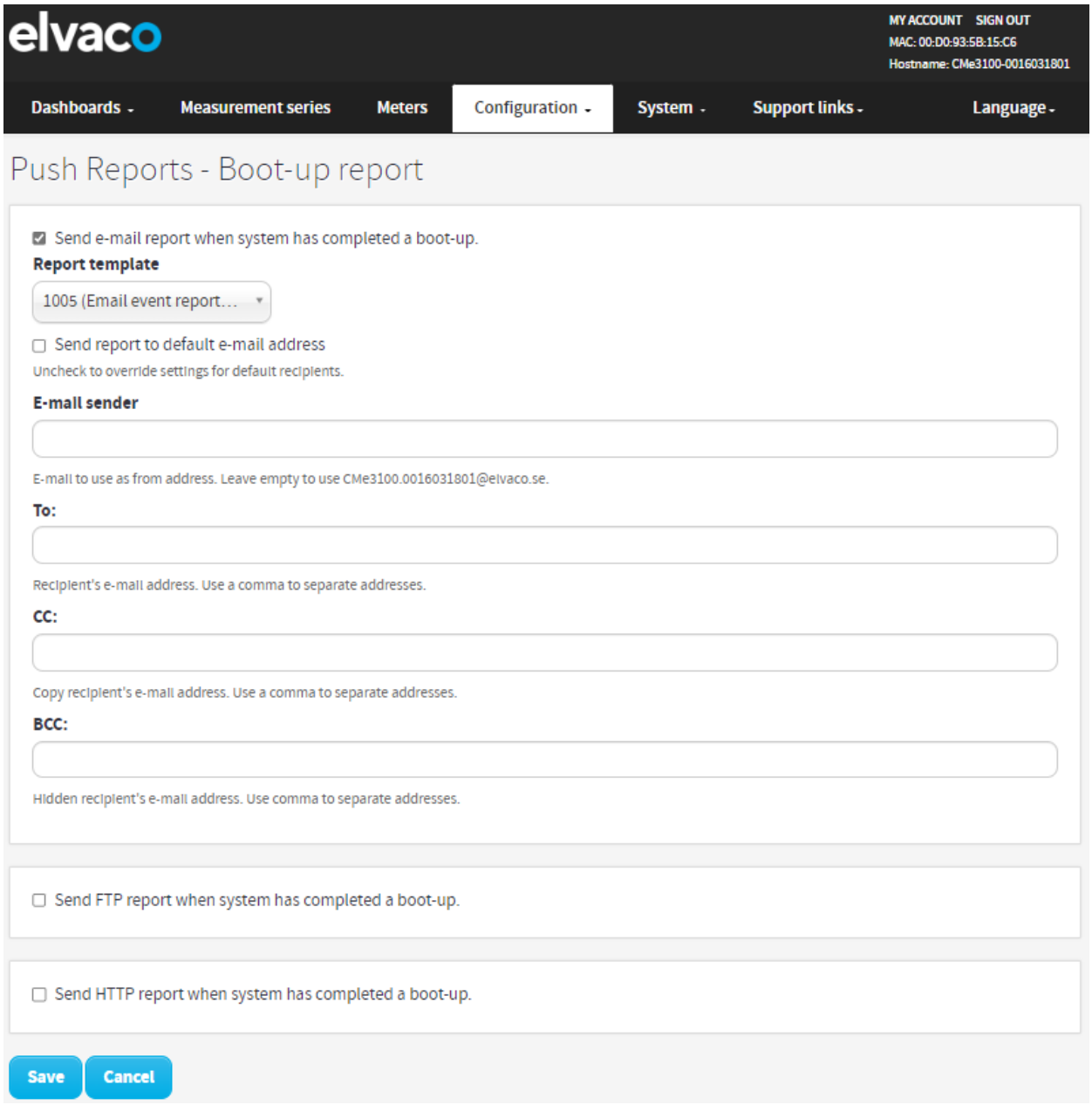


6.9.2 Enable and configure Event Reports

To enable and configure Event Reports:

- Go to **Configuration > Push Reports** and select one of the Event Reports by clicking on it.
- Set what type of report to use (e-mail, FTP or HTTP) and the desired template.

- Add receivers of the report. If no receiver is added, the default receiver option will be used.
- Click **Save**.



Common operations

6.10 Purpose

At this point you should have gotten started with your CMe3100 and are receiving recurrent Push Reports with meter values. This chapter will present some common features, which will help you enhance the operation of your Metering Gateway even further.

6.11 Create a configuration file

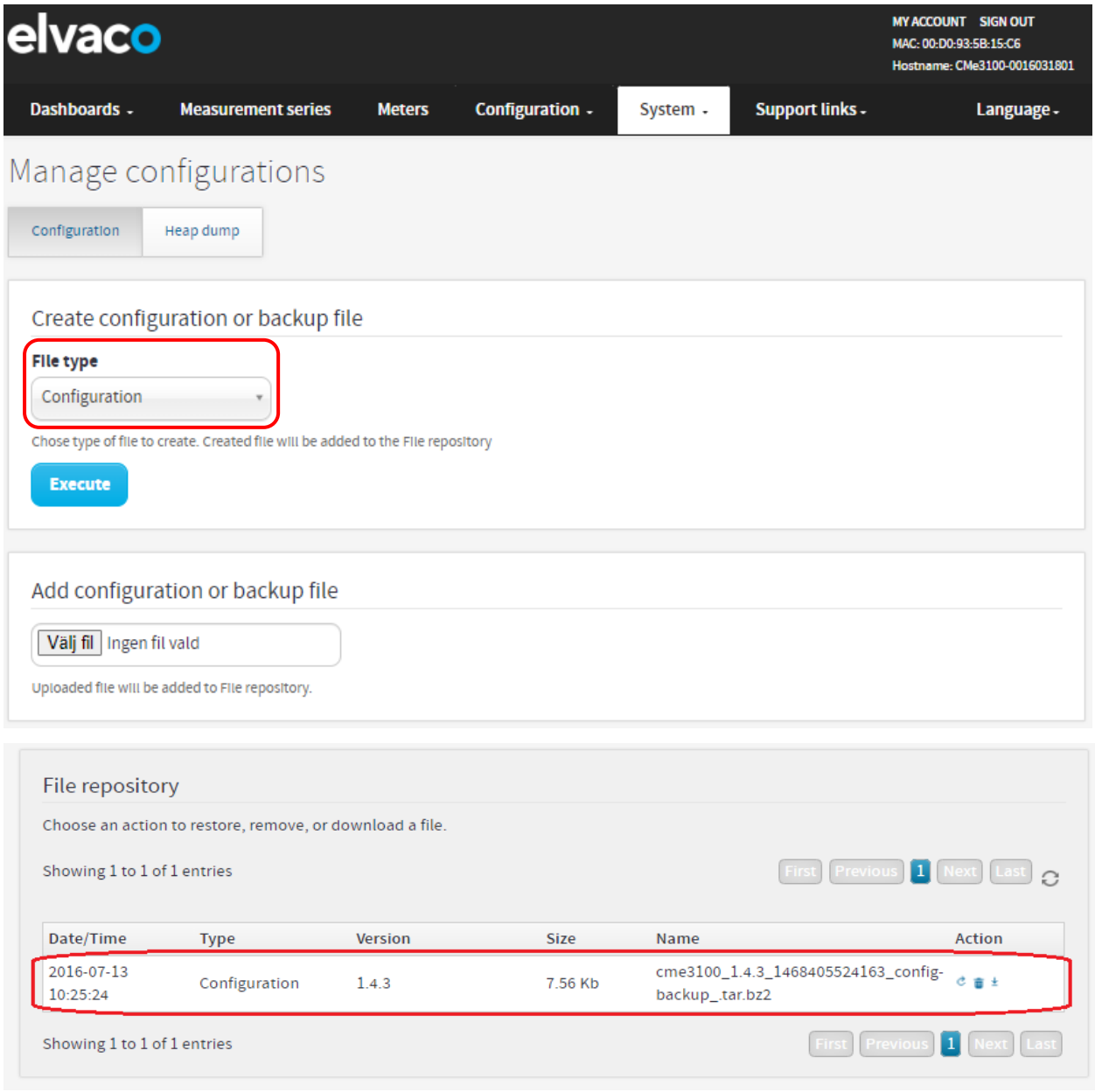
Purpose

A configuration file contains all *non-device specific* settings such as readout schedule and Push Report configurations (but excludes IP address, etc.). By using a configuration file, settings may be restored on an individual device or duplicated to a group of devices without having to go through all steps manually. Therefore, a configuration file should always be saved before performing an update to be able to restore the settings of the Metering Gateway if something should go wrong.

6.11.1 Save non-device specific settings in a configuration file

To save device specific settings in a configuration file:

- Go to **System > Manage configurations**.
- Select “Configuration” as File type and click **Execute**.
- When the configuration file has been created, it will be displayed in, and can be downloaded from, the File repository.



6.12 Create a backup file

Purpose

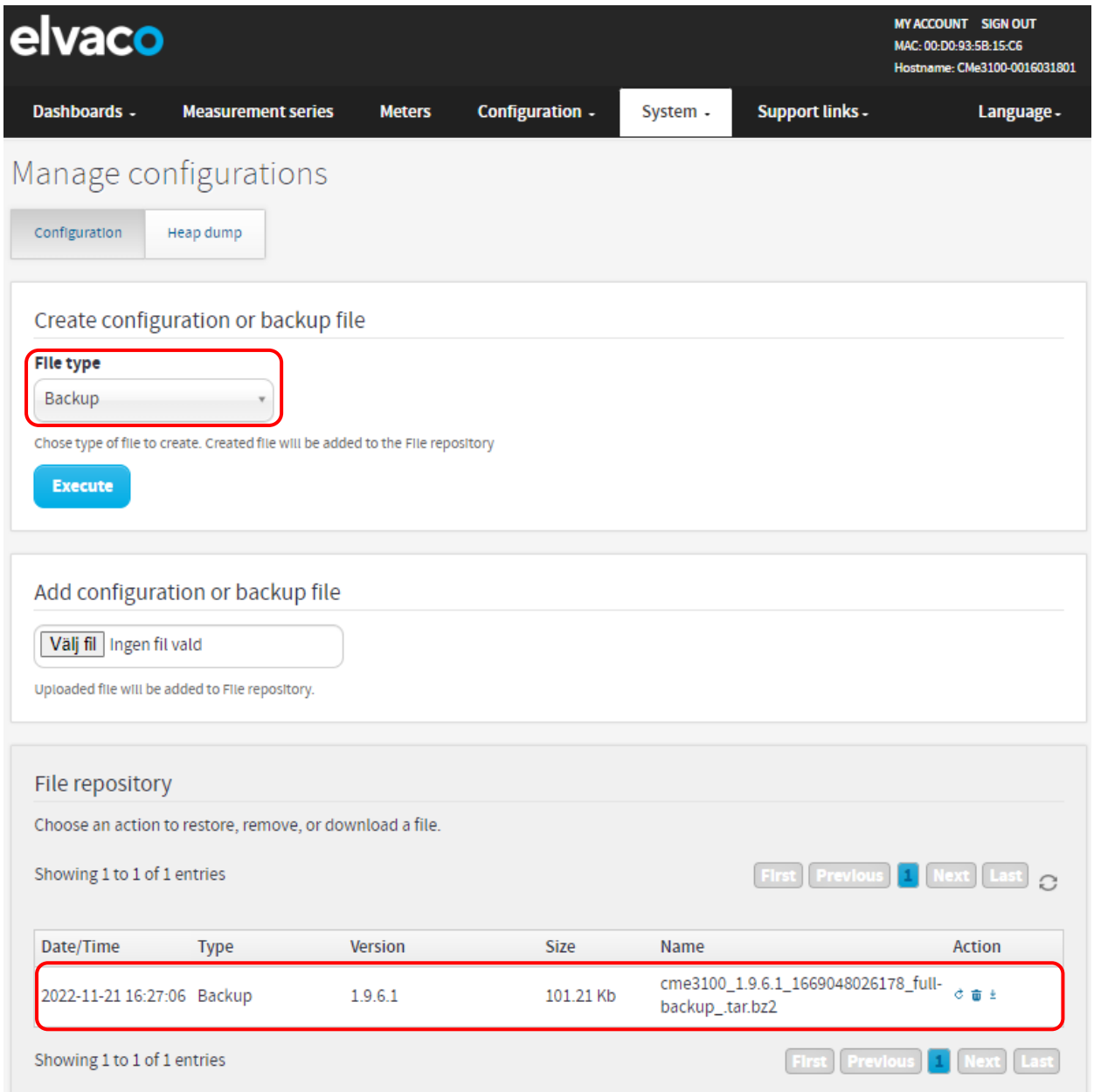
A backup file contains all meter values stored by the Metering Gateway and all settings including *device specific settings*. By using a backup file, the settings and stored data of a device may be completely restored and is suitable for restoring a device if the hardware is replaced. However, it should not be used to duplicate settings into different devices as it contains device specific settings such as IP address.

⚠	Back-up files can take a long time to create and restore settings and data from. They also consume a lot of storage space. It is therefore not recommended to keep more than one backup file in the device's repository at a given time. You may however of course choose to download backup files and keep them safe using another media.

6.12.1 Save meter values and device specific settings in a backup file

To save meter values and device specific settings in a backup file:

- Go to **System > Manage configurations**.
- Change File type to “Backup” and click **Execute**.
- When the backup file has been created, it will be displayed in, and can be downloaded from, the File repository.



6.13 Check device and meter settings

Purpose

There are several separate ways to use the web interface to check the current settings of the Metering Gateway and its installed meters. You may use:

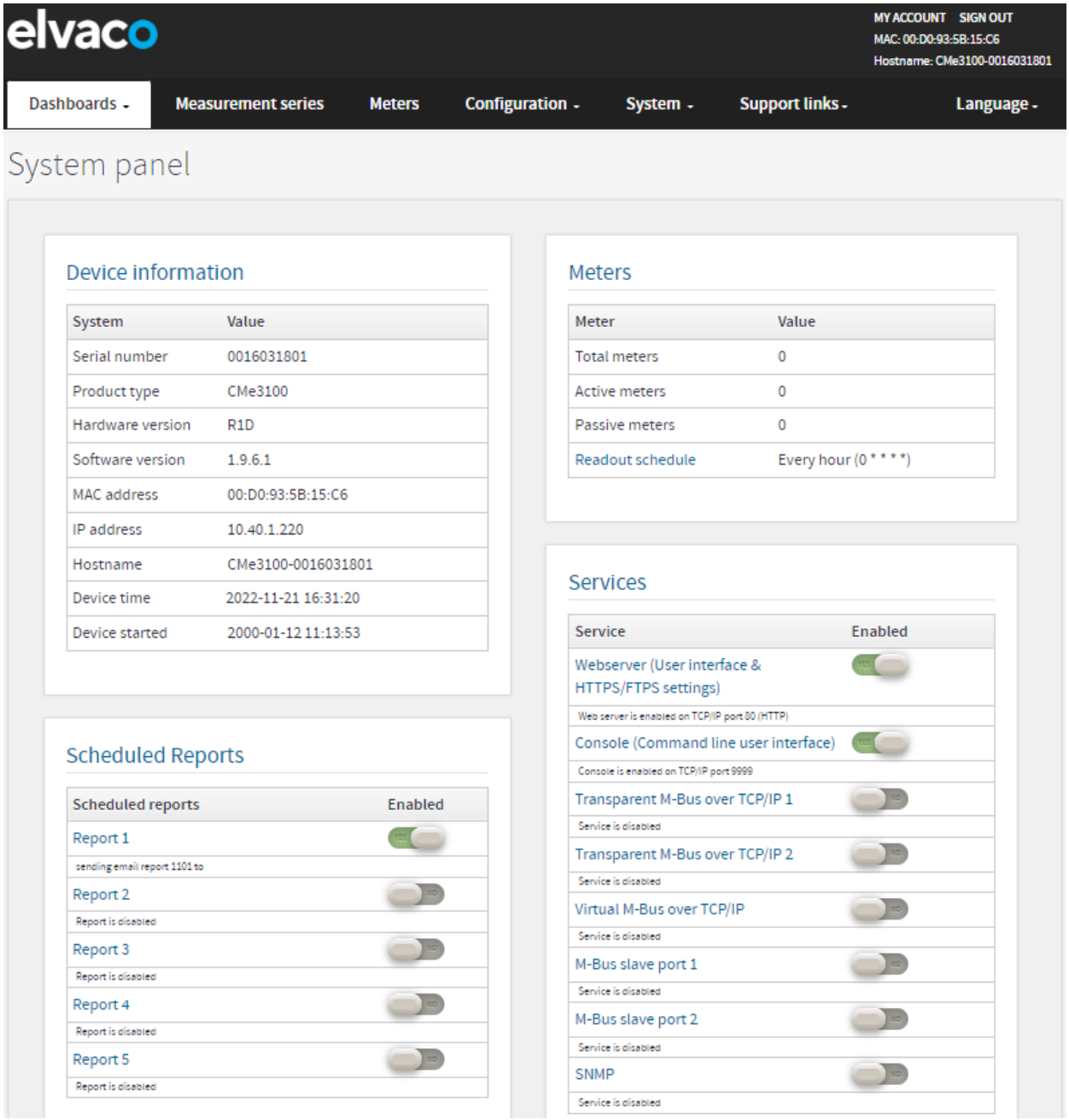
- The System Panel, which contain information about the Metering Gateway, active/passive meters and scheduled reports and services.
- The system overview, which displays system specific settings and scheduled tasks.

- The meter settings report, which contain addressing modes, baud rates and addresses.

6.13.1 Check status through the System Panel

To check status through the System Panel:

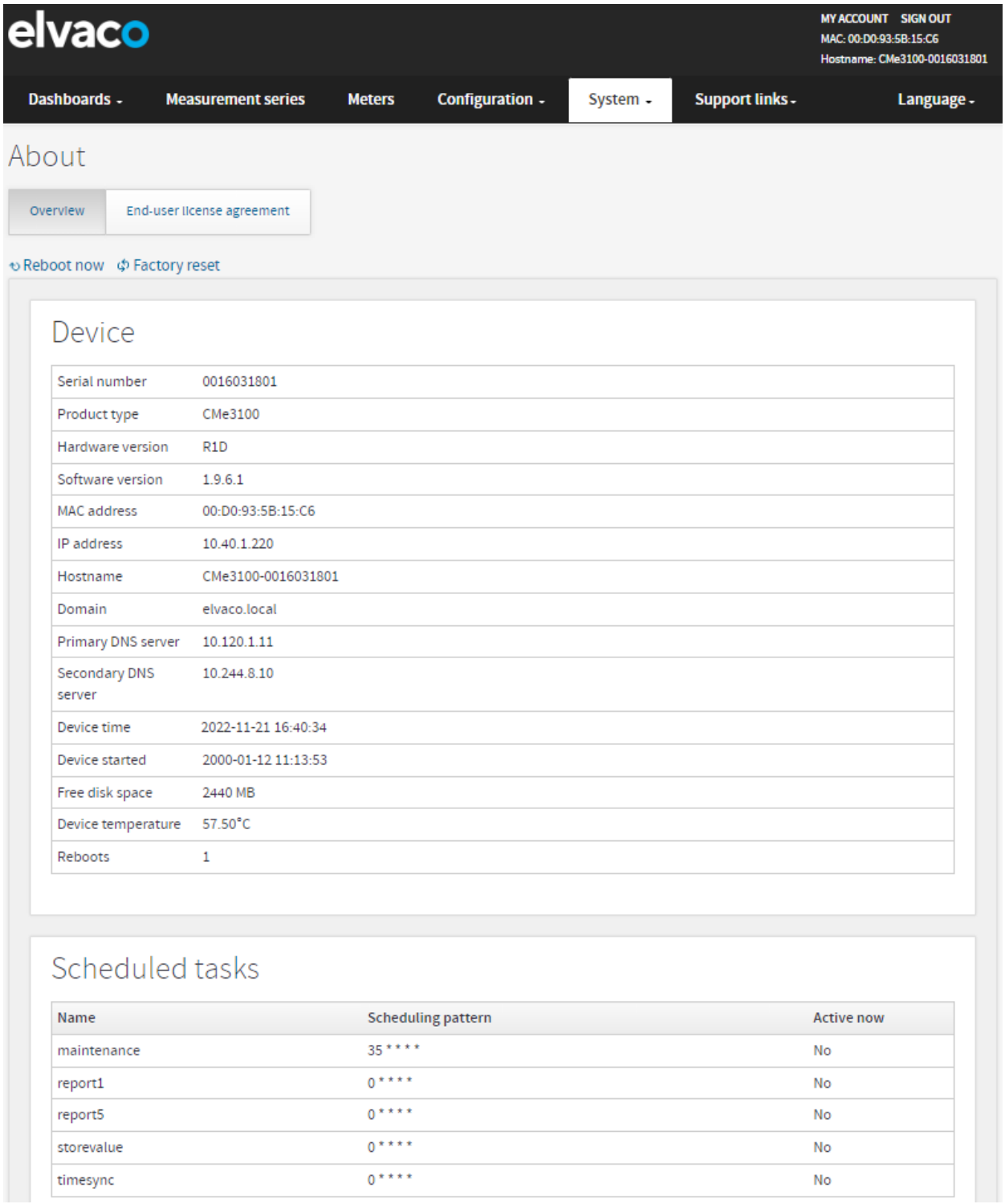
- Go to **Dashboards > System Panel**.
- The System Panel will display system information, scheduled reports, enabled services and information about installed meters.



6.13.2 Check the system overview

To check the system vice overview:

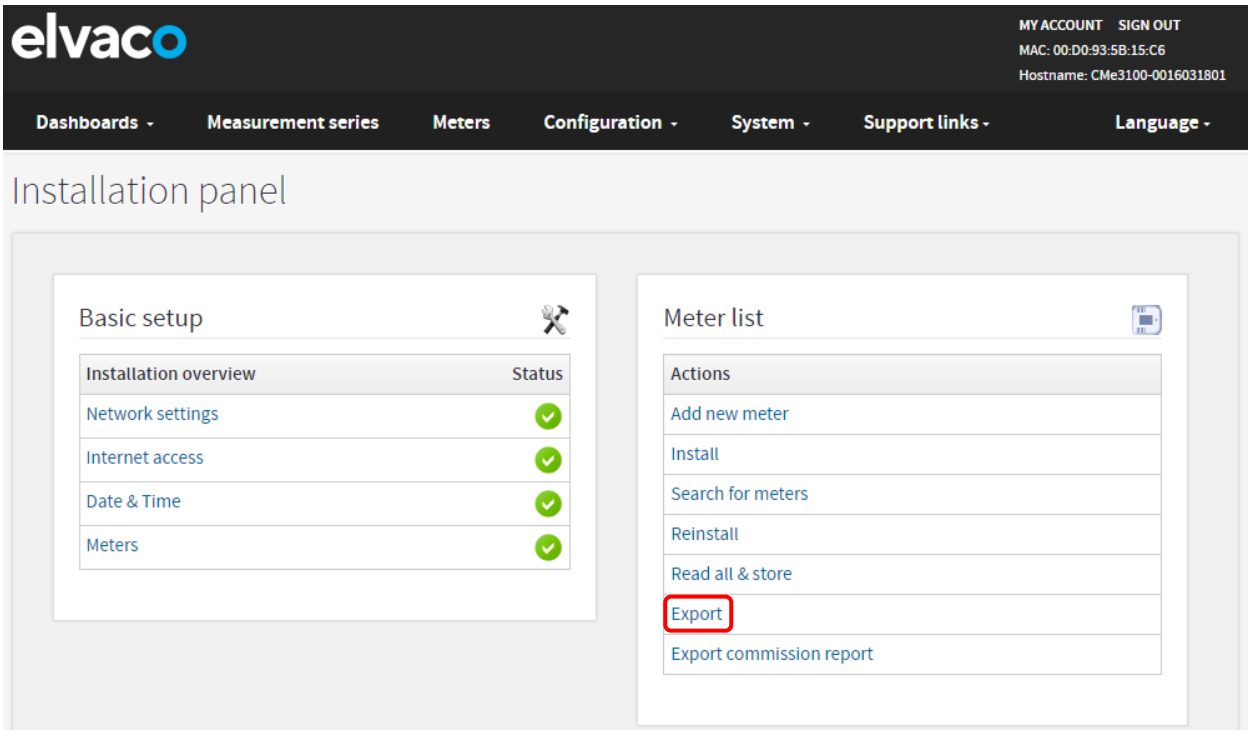
- Go to **System > About.**
- The system overview will display Metering Gateway information and scheduled tasks.



6.13.3 Download a meter settings report

To download a meter settings report:

- Go to the Meter List window in the Installation panel.
- Click **Export**.
- Open the document. It contains information about the addressing mode, baud rate and address of all installed meters.



6.14 Check operational status of the system

Purpose

All information about different system events is logged and stored in the System Log. For each log entry, a severity type icon (error, warning, or information), timestamp and plain text explanation is shown. This makes it a useful tool for investigating operational status of the system and pin-pointing errors in the metering process.

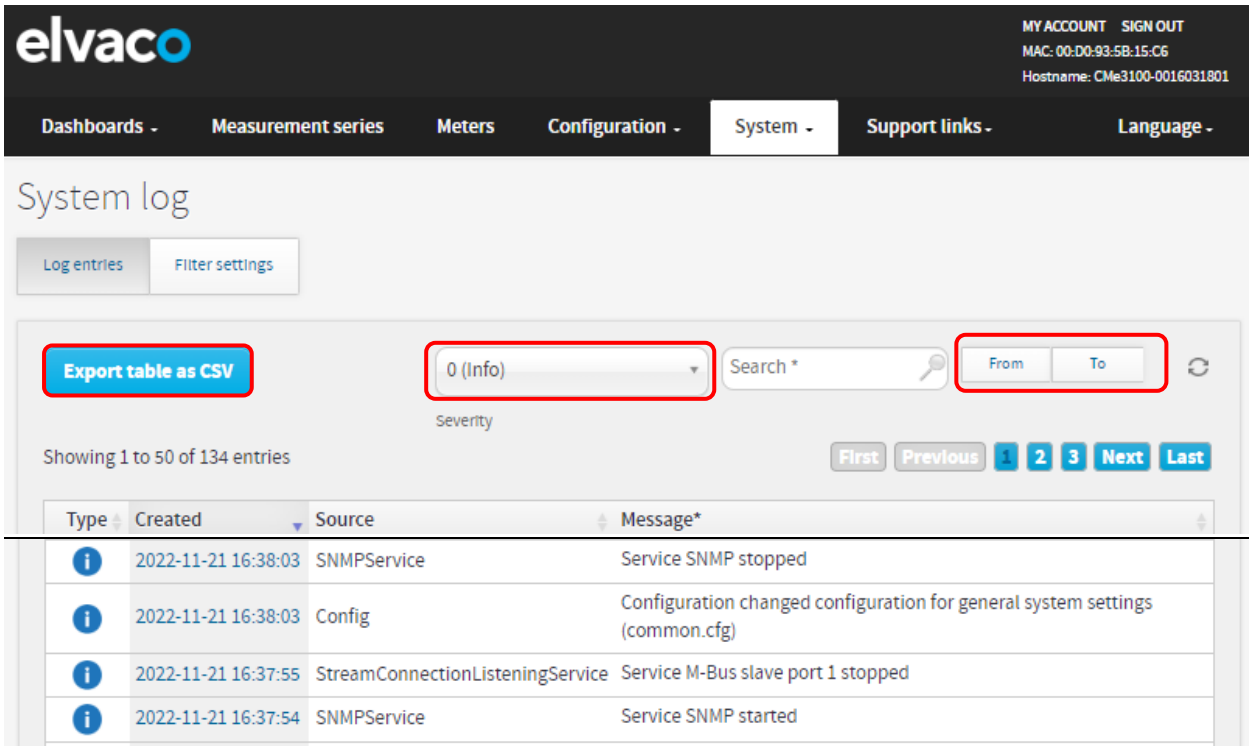
6.14.1 Filter the System Log

To facilitate inspection, the System Log can be filtered with respect to severity level and date interval of the logs.

To filter the System Log:

- Go to **System > System Log**. All saved log entries are displayed here.
- To filter the log entries by a specific severity level, click on the Severity tab and select a desired level. By using the **From** and **To** buttons, logs stored over a certain period can be displayed.
- To export the System Log table as a CSV file, click on “Export table as CSV”.

To learn more about the different log entries of the System Log and how they are interpreted, go to our support site, https://support.elvaco.com, and download the document named “CMe3100 Guide to System Log”.



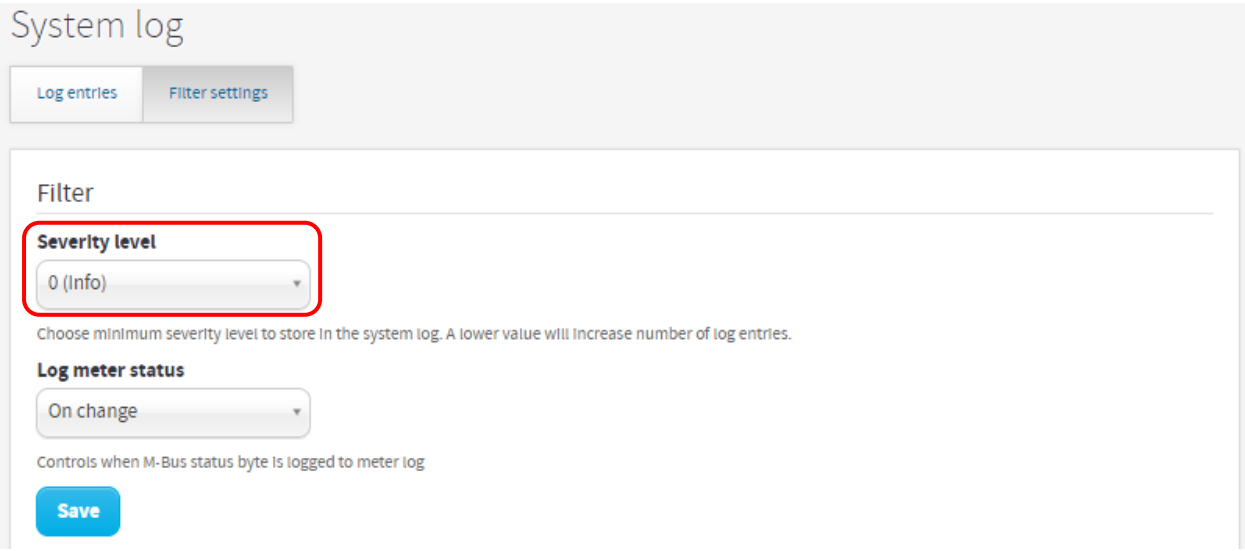
6.14.2 Set the minimum severity level of logged events

The minimum severity level for an event that gets stored in the System log is also configurable but should not be adjusted without good reasons as it may cause vital information to be lost or the log to become very extensive.

To set the minimum severity level of logged events:

- Go to **System > System Log > Filter settings**.
- Select a minimum severity level of the logs that should be saved. By choosing “0”, all events except the debug events are logged. By choosing “-1”, all events including the debug events are logged.
- Click **Save**.

⚠	It is highly recommended that the debug log entries are only logged in case of troubleshooting. If not, the System Log will fill up fast, and it might be hard to navigate. Activating debug log entries might also affect the performance of the Metering Gateway in a negative way.

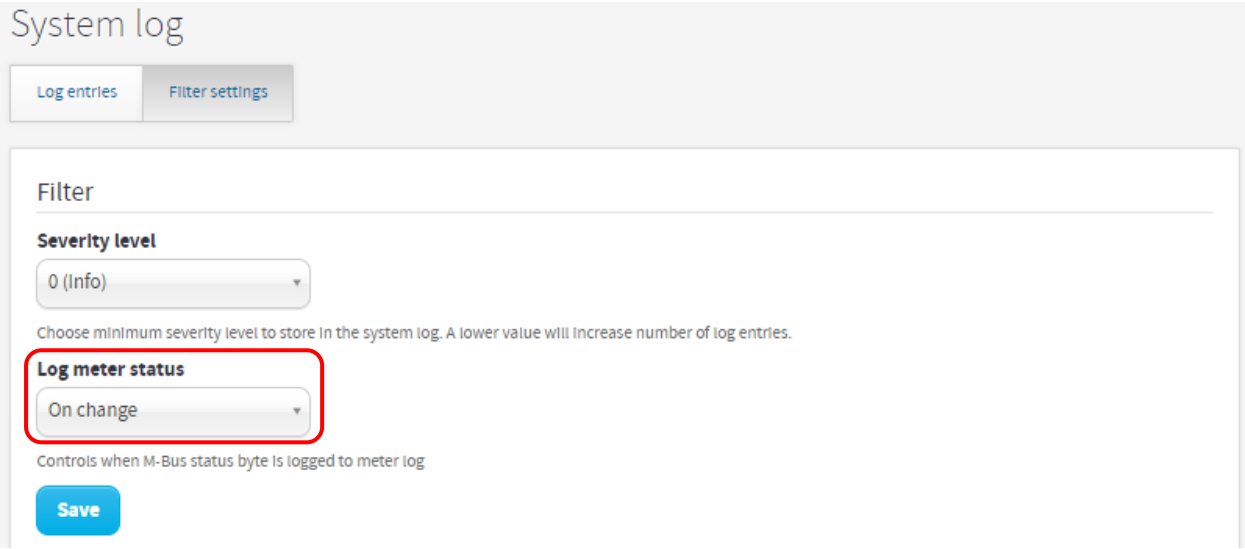


6.14.3 Set when M-Bus status byte is logged in meter log

It is possible to control when information about M-Bus status byte is logged to the meter log.

- Go to **System > System Log > Filter settings**.
- In the selecting box, choose when M-Bus status byte information is logged to meter log. Viable options are:
    - Always
    - Never
    - On change
    - On error

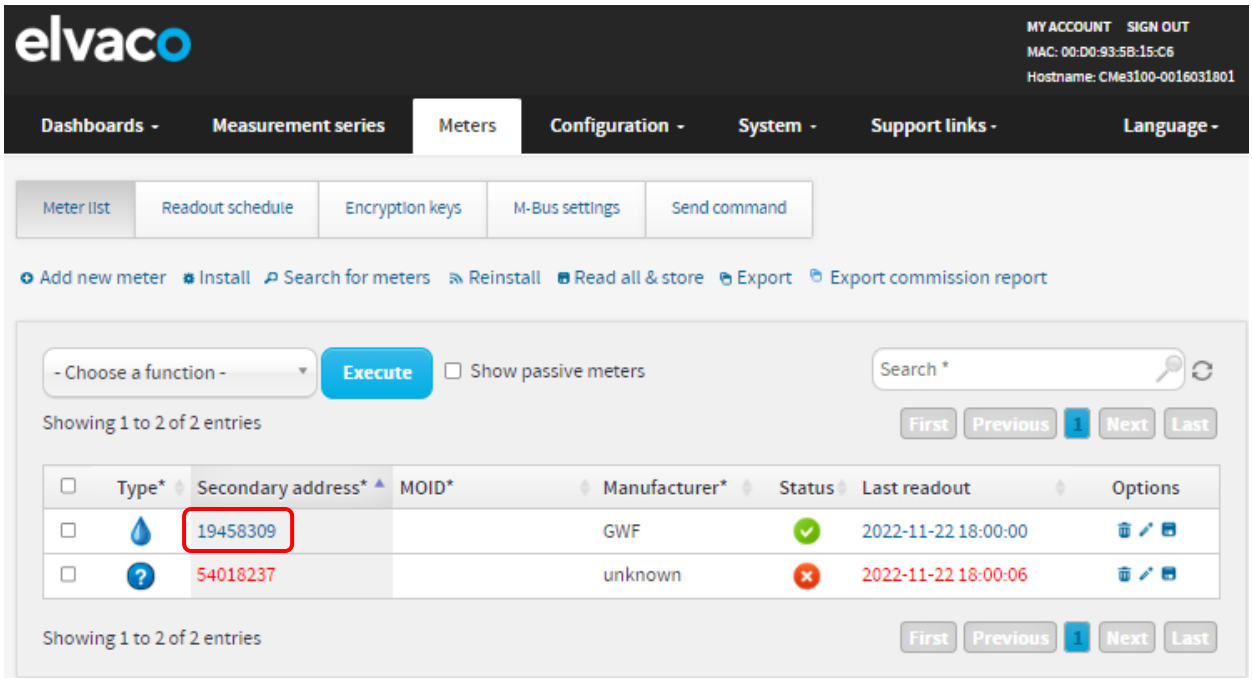
  By default, information is logged when status byte changes value.
- Click **Save**.

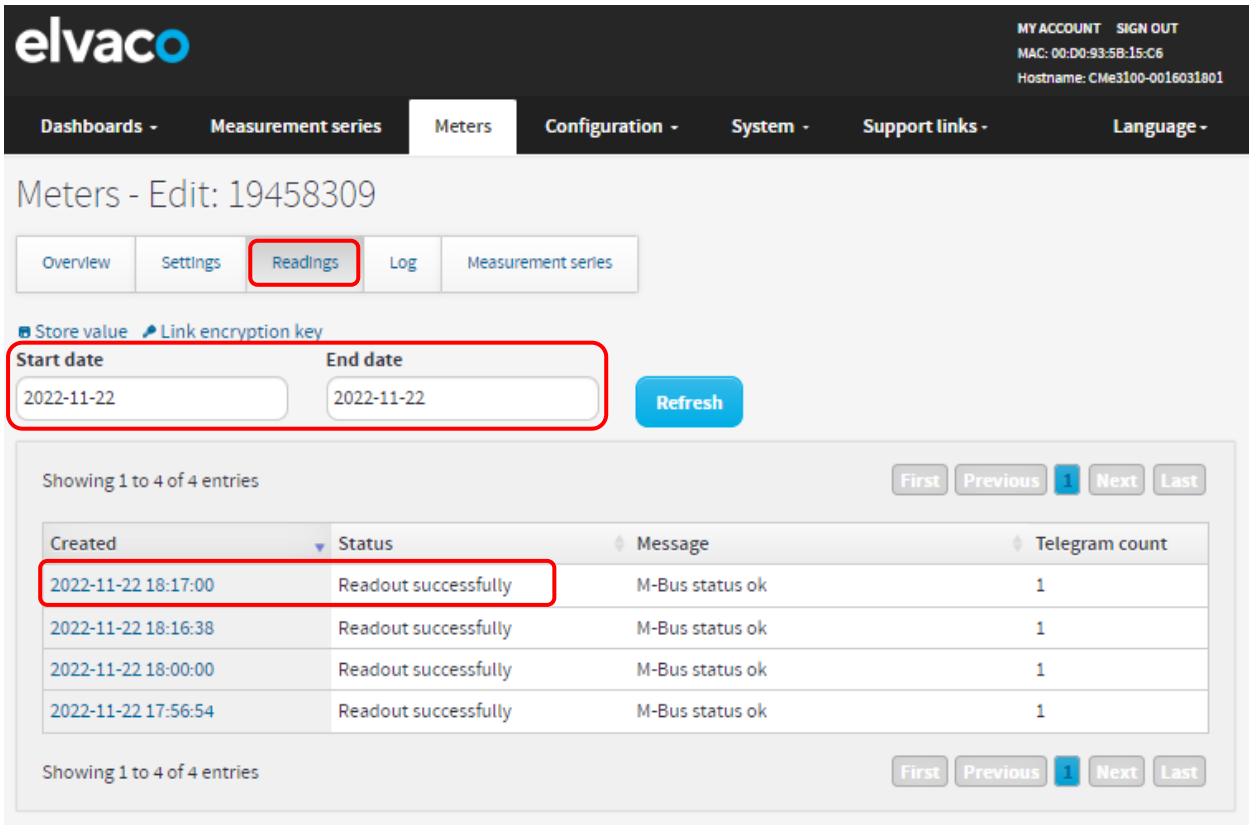


6.14.4 Check the readout status of an individual meter

To check the readout status of an individual meter:

- Go to **Meters** and click on the secondary address of a meter.
- Click **Readings.** Here, the status and time of recent readouts of that specific meter are displayed.
- By setting a start and an end date, readings conducted over that specific period will be displayed.





6.15 Install encryption keys for wireless meters

Purpose

The CMe3100 has a built-in management system for wireless encryption keys. The meter encryption key is registered in the web interface and will be used by the Metering Gateway to enable decryption of incoming messages.

Encryption keys are uploaded in an encryption key file (CSV or Excel 97-2003), structured by the template of Figure 7, or registered directly in the web interface. The encryption key file contains the matching criteria for each key which defines a filter for what meters the encryption key will be applied to.

See Table 6 for a full explanation of all fields in the key file, which together make up the matching criteria.

	A	B	C	D	E
1	**Address**	**Key**	**Manufacturer**	**DeviceType**	**Version**
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					

Figure 7: Template of encryption key file

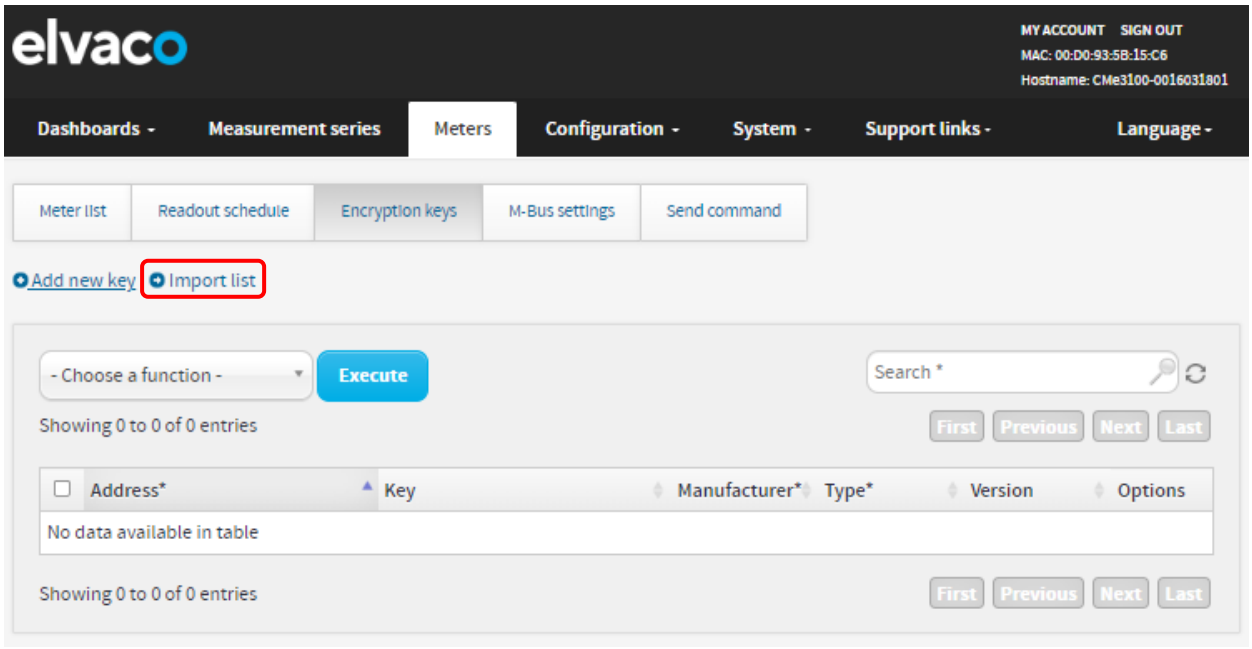
Encryption key field	Explanation
Address	This field contains the secondary address of the meter that the encryption key will be applied to. Set “-1” to exclude this field from the matching criteria.
Key	This field contains the actual encryption key that will be used, consisting of 32 characters in hex format.
Manufacturer	This field contains the manufacturer of the meter that the encryption key will be applied to. To find a list of the different manufacturers, and their initials, go to **Meters > Encryption keys > Add new key.** Uncheck the Manufacturer box and use the list. Use “*” character to exclude this field from the matching criteria.
DeviceType	This field contains the type of meters which the encryption key will be applied to. To find a list of the different device types, go to **Meters > Encryption keys > Add new key**. Uncheck the Type box and use the list. Use “-1” to exclude this field from the matching criteria.
Version	This field contains the version of the meter that the encryption key will be applied to. Use “-1” to exclude this field from the matching criteria.

Table 6: Encryption key file fields

6.15.1 Add an encryption key through a file upload

To add an encryption key through a file upload:

- Go to **Meters > Encryption keys.** Here, a list of all registered encryption keys is displayed.
- An encryption key is uploaded as an CSV or Excel (97-2003) file. Click **Import list** and select the file, structured according to Figure 7. An example file is provided in Figure 8. The template can be downloaded directly from the web interface by clicking **Download example file**.
- Click **Save**.



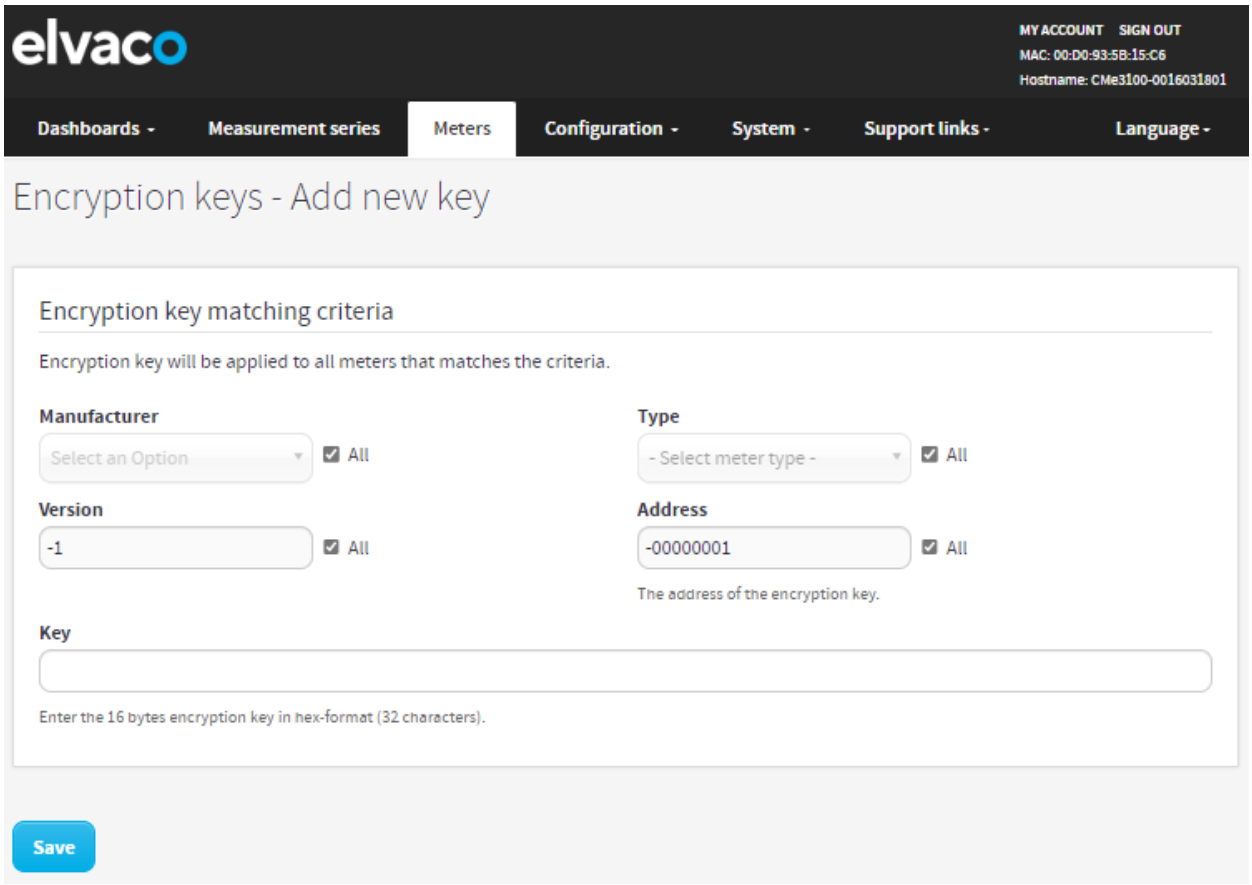
	A	B	C	D	E
1	**address**	**key**	**manufacturer**	**deviceType**	**version**
2	-1	AAAABBBBCCCCDDDDEEEEFFFF11112222	*	-1	-1
3	13360079	A1B2C3D4E5F6A1B2C3D4E5F678910111	ELV	-1	-1
4	-1	FFEEDDCCBBAA99887766554433221100	*	-1	-1
5	-1	AAAA1111BBBB2222CCCC3333DDDD4444	ACA	-1	-1
6	-1	9999AAAA8888BBBB7777CCCC6666DDDD	ELV	-1	2

Figure 8: Encryption key example file

6.15.2 Add an encryption key directly in the web interface

To enter an encryption key directly in the web interface:

- Go to **Meters > Encryption keys.**
- Click **Add new key**.
- Set the matching criteria to determine the meters the encryption key will be applied to. By checking the All box, the encryption key will be used for decryption of messages from all meters of that specific matching criteria field.
- Click **Save**.

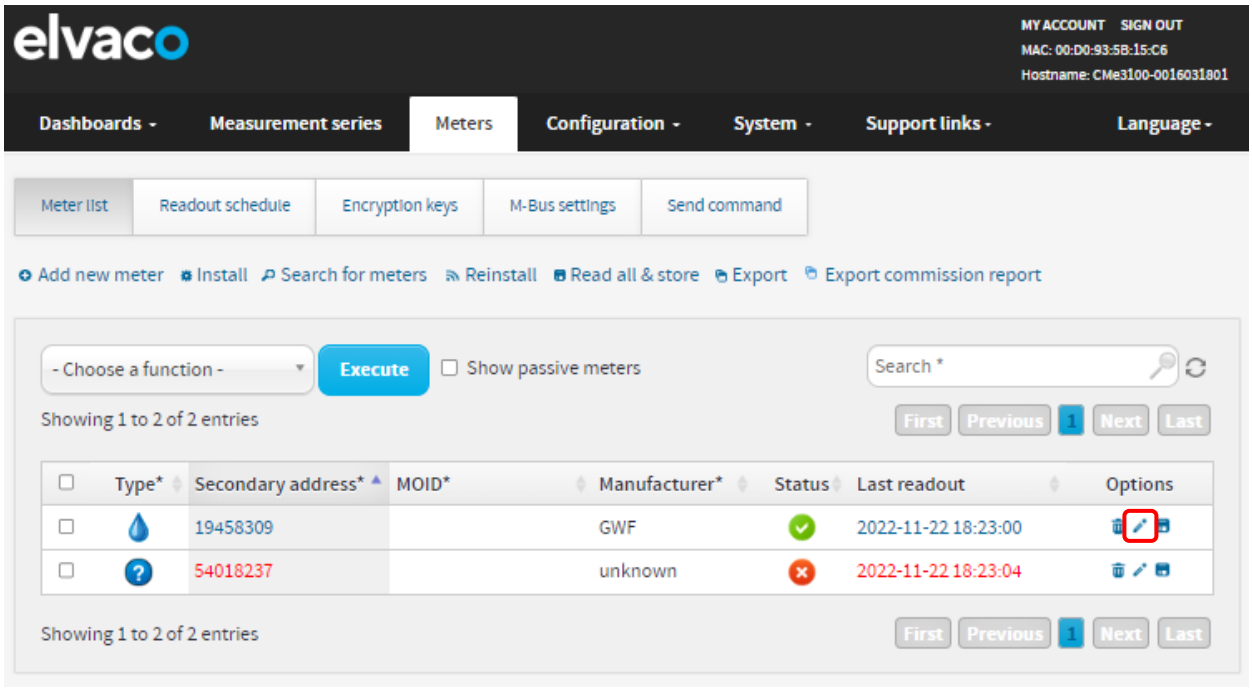


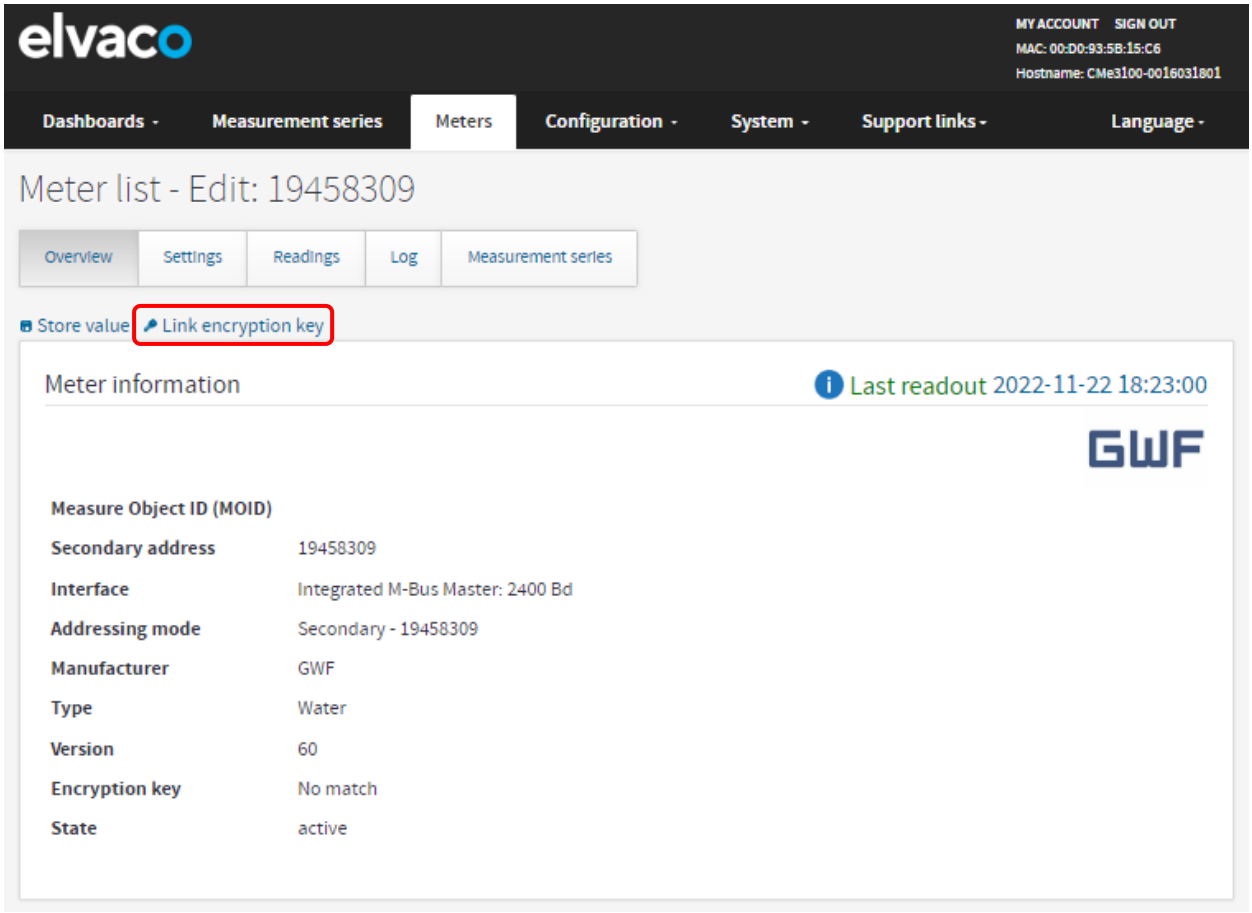
6.15.3 Link an encryption key to an individual meter

The Metering Gateway supports linking encryption keys to individual meters. Using this option will make the device apply the key to decrypt information from the linked meters only.

To link an encryption key to an individual meter:

- Go to **Meters** and select the desired meter from the list.
- Click the edit (pen) symbol in the **Options** column.
- Click **Link encryption key** on the top of the page.
- The meter information in the resulting menu should by default be correct. Now add the encryption key that will be used for decryption of meter values sent from that meter.
- Click **Save**.


elvaco
MY ACCOUNT SIGN OUT
MAC: 00:D0:93:5B:15:C6
Hostname: CMe3100-0016031801
Dashboards
Measurement series
Meters
Configuration
System
Support links
Language
Meter list
Readout schedule
Encryption keys
M-Bus settings
Send command
Add new meter
Install
Search for meters
Reinstall
Read all & store
Export
Export commission report
- Choose a function -
Execute
Show passive meters
Search *
Showing 1 to 2 of 2 entries
First
Previous
1
Next
Last
Type*
Secondary address*
MOID*
Manufacturer*
Status
Last readout
Options
19458309
GWF
2022-11-22 18:23:00
54018237
unknown
2022-11-22 18:23:04
Showing 1 to 2 of 2 entries


elvaco
MY ACCOUNT SIGN OUT
MAC: 00:D0:93:5B:15:C6
Hostname: CMe3100-0016031801
Dashboards
Measurement series
Meters
Configuration
System
Support links
Language
Meter list - Edit: 19458309
Overview
Settings
Readings
Log
Measurement series
Store value
Link encryption key
Meter information
Last readout 2022-11-22 18:23:00
GWF
Measure Object ID (MOID)
Secondary address 19458309
Interface Integrated M-Bus Master: 2400 Bd
Addressing mode Secondary - 19458309
Manufacturer GWF
Type Water
Version 60
Encryption key No match
State active

6.16 Configure settings for an individual meter

Purpose

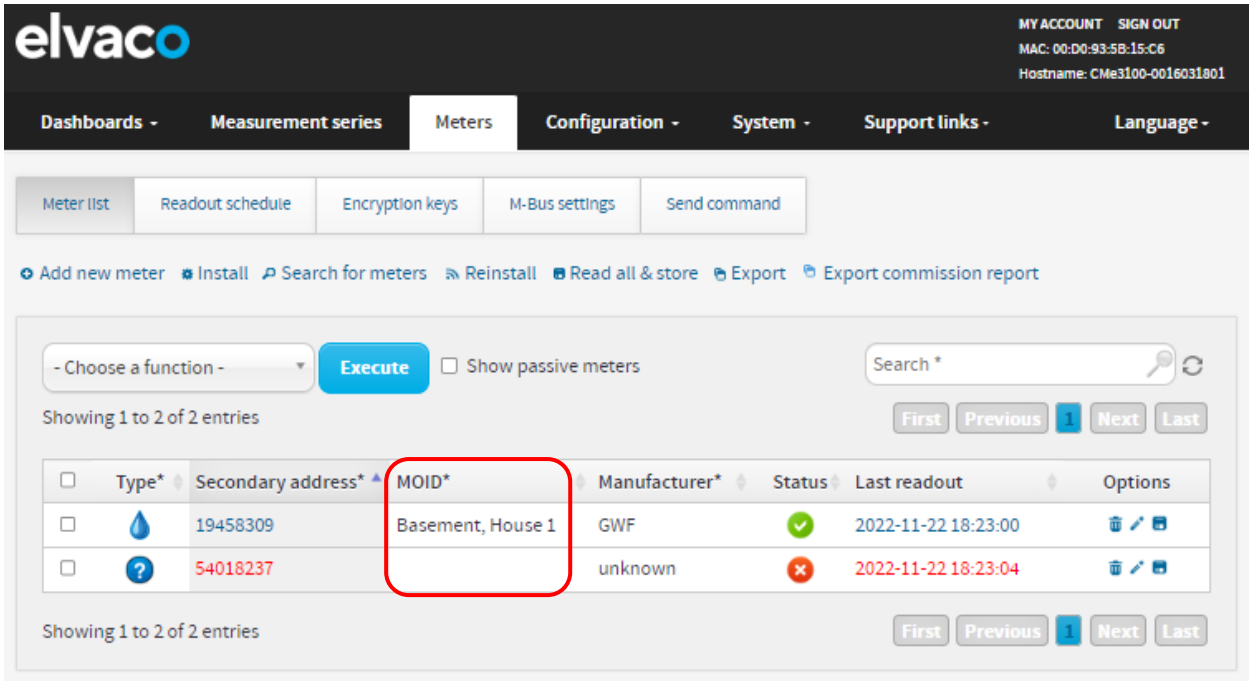
In some cases, it might be desired to configure individual settings of a specific meter. This might for example include changing the Measurement Object Identification (MOID), switching the state of the meter from active to passive (which will exclude it from the meter readout cycle) or changing the interface used by the Metering Gateway when communicating with the meter.

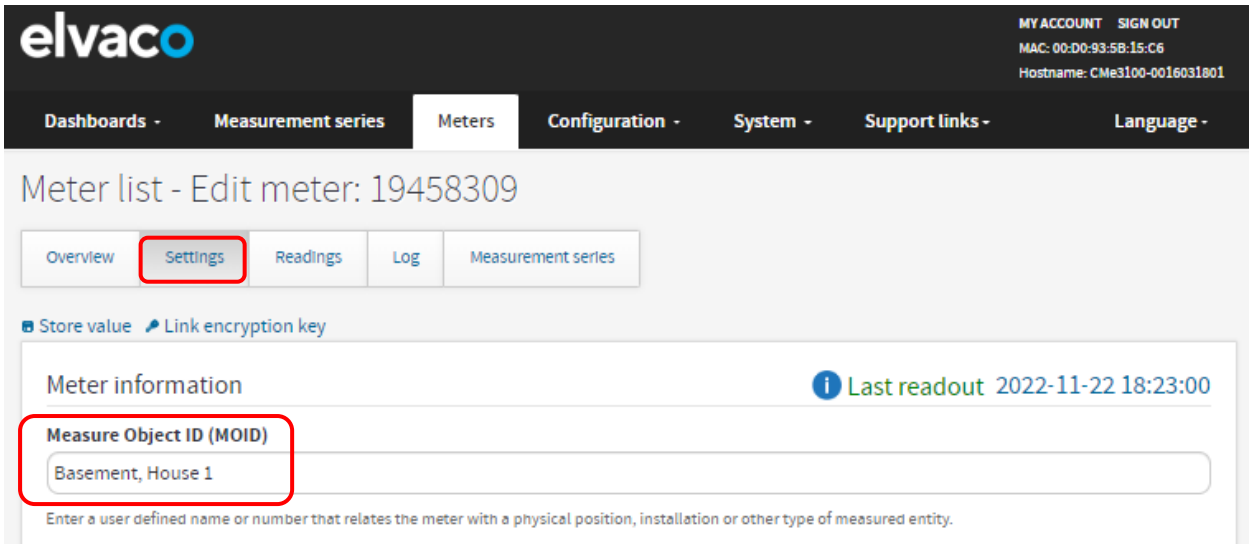
6.16.1 Edit Measurement Object Identification of a meter

The MOID is used to identify the meter in the Meter List and is preferably set to display the function or the location of the meter.

To edit the MOID:

- Go to **Meters** and click the secondary address of a desired meter.
- Click on **Settings**.
- Enter a MOID and click **Save**.
- The MOID will now be displayed for the meter in the Meter List.





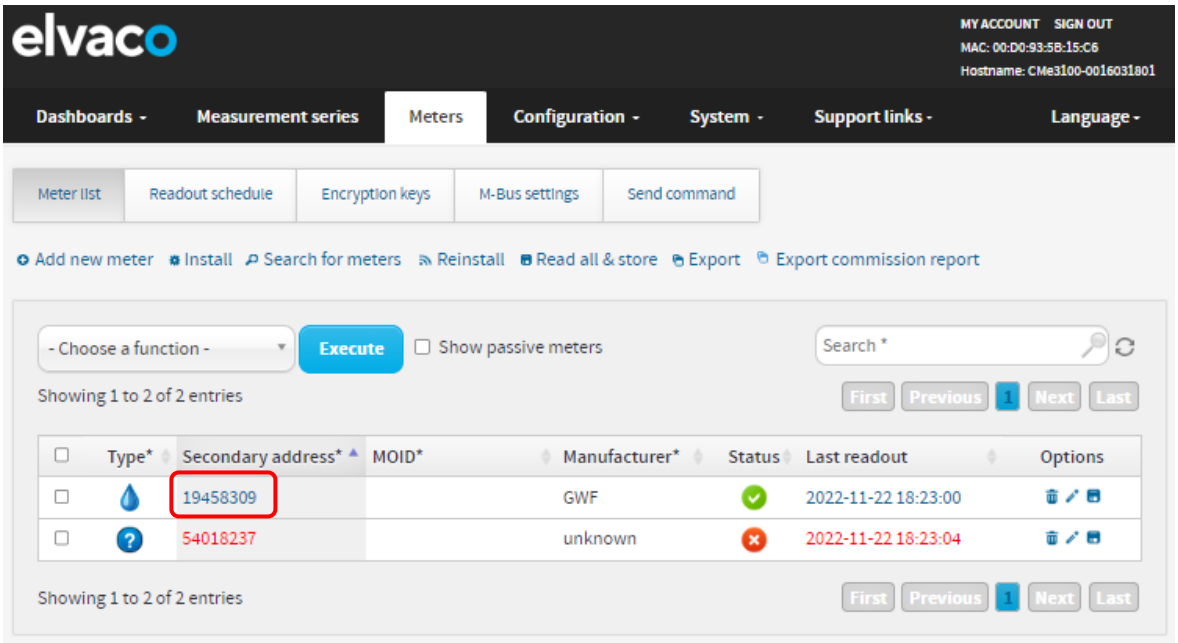
6.16.2 Configure communication settings of an individual meter

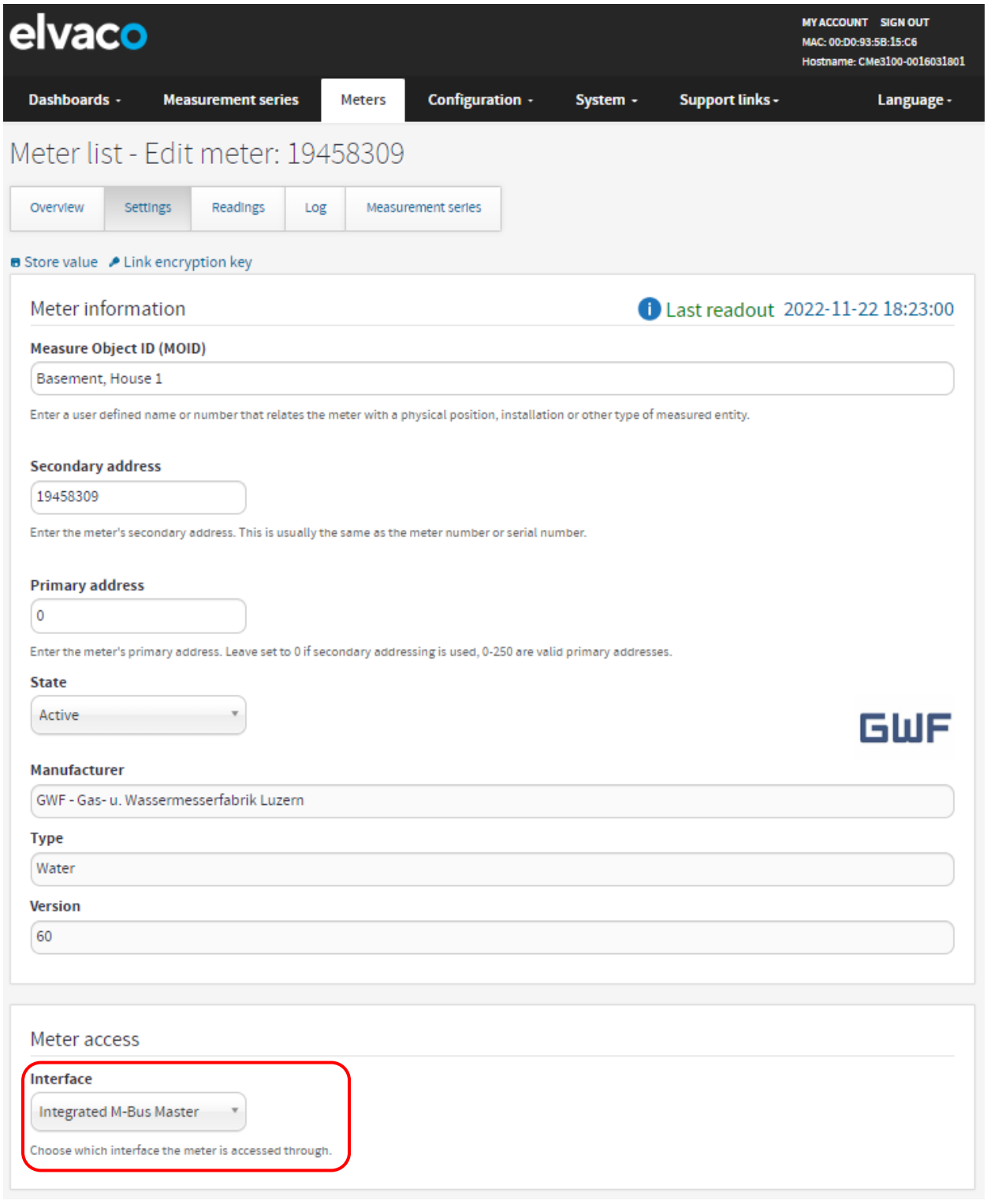
Switching a meter's status from active to passive means that it will no longer be included in the meter readout process. If more meters are installed than the software license supports, the latest installed meters will automatically be set to passive.

The meter access settings determine which interface will be used by the M-Bus Metering Gateway to access a specific meter. Normally, all meters are connected directly or indirectly to the integrated M-Bus master (by 2-wire M-Bus or the IR interface) but it is also possible to use the Ethernet network to connect a remote meter (M-Bus over TCP/IP).

To configure communication settings of an individual meter:

- Go to **Meters** and click the secondary address of a meter
- Click on **Settings**.
- Set the desired state of the meter and the interface that will be used by the Metering Gateway to access the meter.
- Click **Save**.




elvaco
MY ACCOUNT SIGN OUT
MAC: 00:D0:93:5B:15:C6
Hostname: CMe3100-0016031801
Dashboards
Measurement series
Meters
Configuration
System
Support links
Language
Meter list - Edit meter: 19458309
Overview
Settings
Readings
Log
Measurement series
Store value
Link encryption key
Meter information
Last readout 2022-11-22 18:23:00
Measure Object ID (MOID)
Basement, House 1
Enter a user defined name or number that relates the meter with a physical position, installation or other type of measured entity.
Secondary address
19458309
Enter the meter's secondary address. This is usually the same as the meter number or serial number.
Primary address
0
Enter the meter's primary address. Leave set to 0 if secondary addressing is used, 0-250 are valid primary addresses.
State
Active
GWF
Manufacturer
GWF - Gas- u. Wassermesserfabrik Luzern
Type
Water
Version
60
Meter access
Interface
Integrated M-Bus Master
Choose which interface the meter is accessed through.

Special operations

6.17 Purpose

This chapter is targeting advanced users and contains instructions on how to perform operations that are less frequently used. Typically, these operations are needed to configure more complex metering setups of the Metering Gateway and the M-Bus system.

6.18 Update software

Purpose

Elvaco regularly launches new software updates for products to enable continuous improvement and new functionality. New software can easily be installed using the web interface, simply by uploading the software file.

	Please visit our support site https://support.elvaco.com to find the latest software releases. Make sure to read the release notes carefully before installing new software.

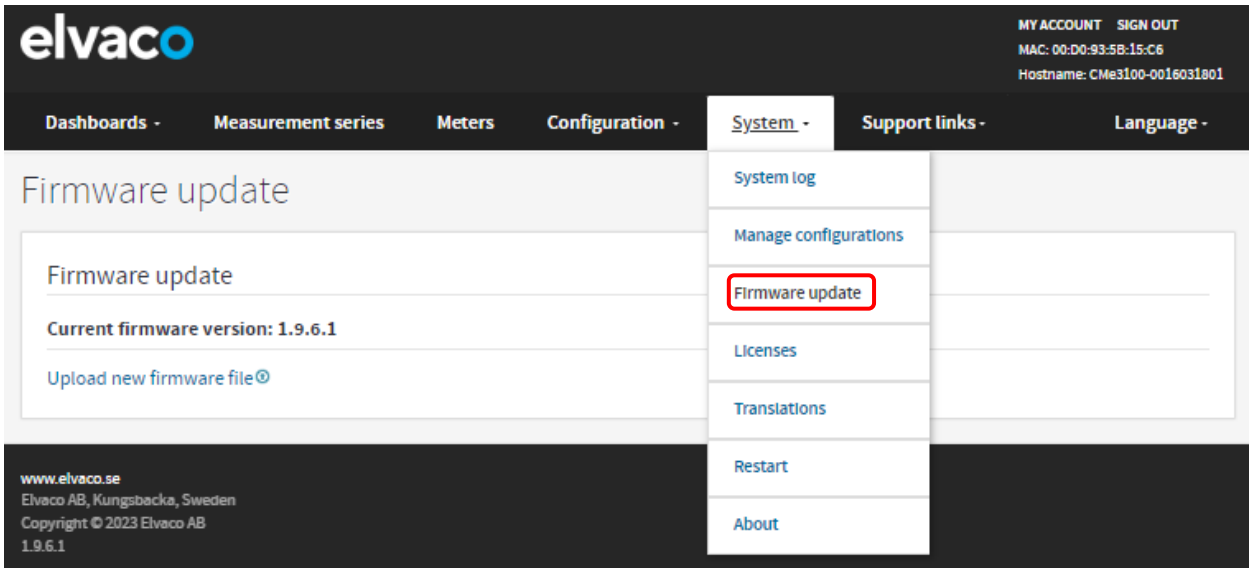
6.18.1 Perform a software update

To perform a software update:

- Go to **System > Firmware update**.
- Click **Upload new firmware file**, select a software file (.tar) and click **Upload**.
- Click **Continue**.
- Click **Reboot now.** The reboot might take up to an hour to complete.

	It is especially important that the power is not cut during the update. Do not attempt to update the browser, the page will automatically reload once the reboot has been completed.

	If the software version used is older than version 1.6.0 and is updated to 1.6.0 or later, the link-local address for the USB network interface will be changed from 192.168.100.1 to 169.254.254.1. The device will then be unable to automatically reload the page when the reboot has finished if performed over USB cable. The same applies if the IP address has been changed manually. To make sure that the reboot is completed, the LED lights will instead have to be used. When the green and the red LED light blink alternately, the reboot is ongoing. When the green LED blinks with a “80 percent on-20 percent off” frequency, the rebooting has been completed.



6.19 Administrate user accounts

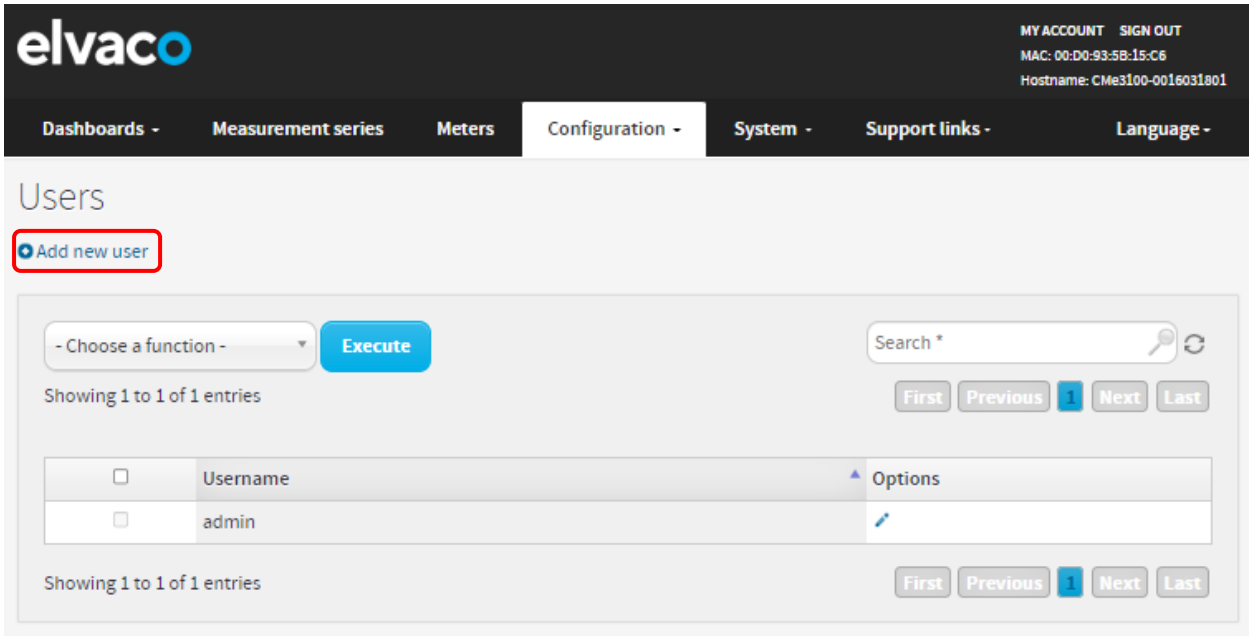
Purpose

Through the web interface, user accounts to log in on the web interface can be added, edited, or deleted.

6.19.1 Add a new user account

To add a new user account:

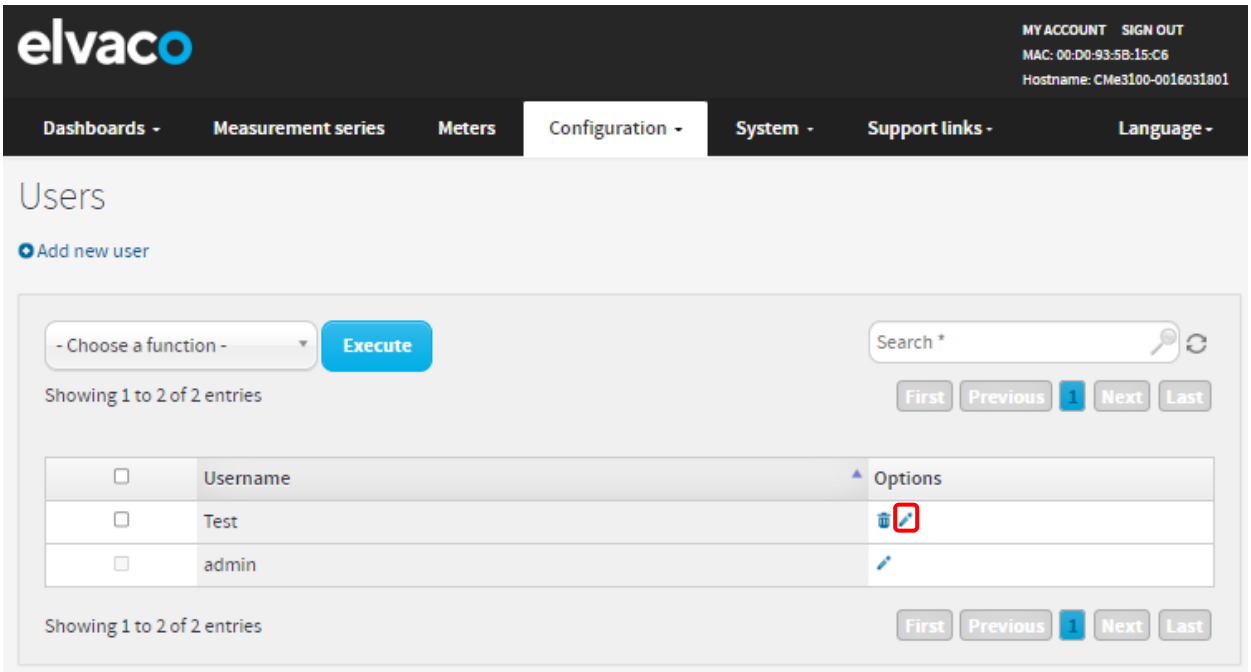
- Go to **Configuration > Users**.
- Click **Add new user**.
- Type a desired username and password. Use a strong password, consisting of at least 8 characters. Click **Save**.



6.19.2 Edit an existing user account

To edit an existing user account:

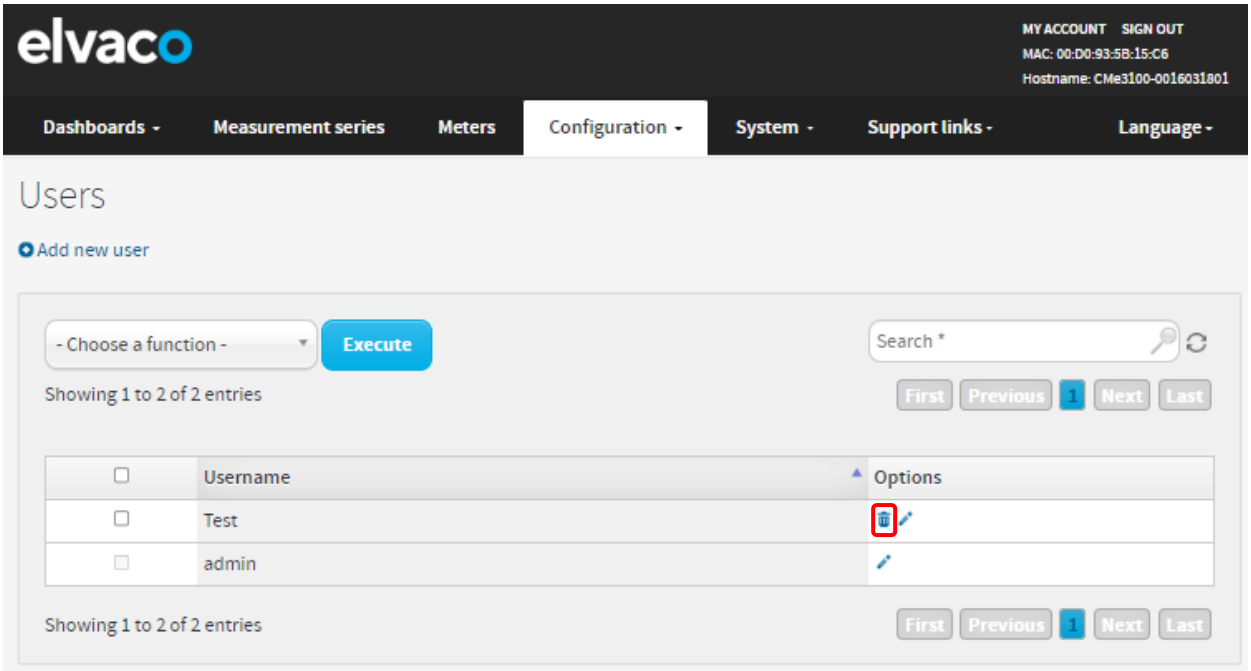
- Go to **Configuration > Users**.
- Click the edit (pen) symbol in the “Options” column of the account to be edited.
- Make desired changes to the username and password of the account.
- Click **Save**.



6.19.3 Delete an existing user account

To delete an existing user account:

- Go to **Configuration > Users**.
- Click the delete (trashcan) symbol in the “Options” column of the account to be deleted.
- Click **Yes**.



6.20 Add a new license

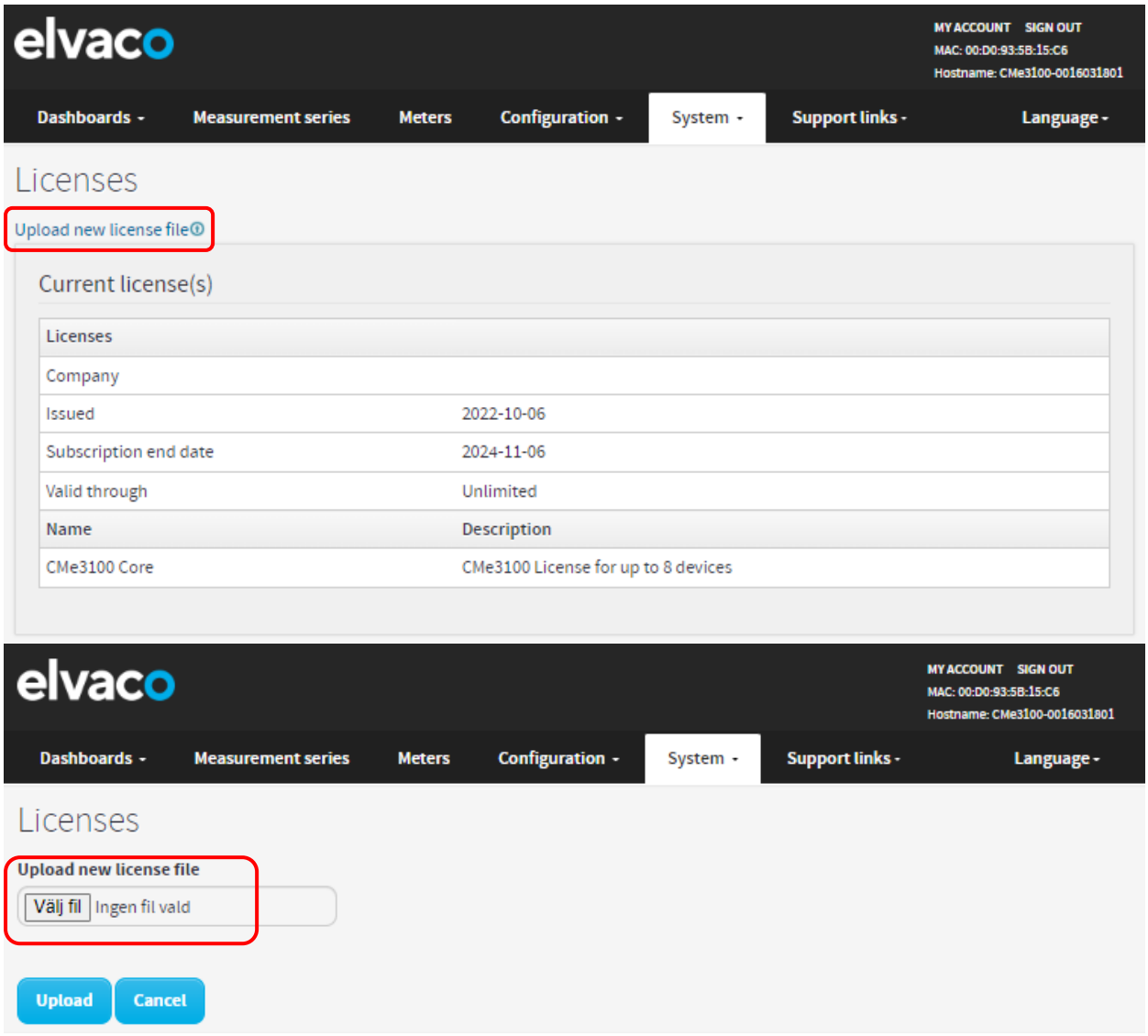
Purpose

The CMe3100 is equipped with a flexible licensing scheme that allows its capabilities and feature set to be altered through the addition of license files. See section 4.5.1 for more information about the licensing scheme. A license file needs to be uploaded to the web interface before the new capabilities are implemented on the Metering Gateway.

6.20.1 Upload and save license

To upload and install a license:

- Go to **System > Licences.**
- Click **Upload new licence file**, select the licence file, and click **Upload**.
- Click **Save**.



6.21 Perform an advanced meter search

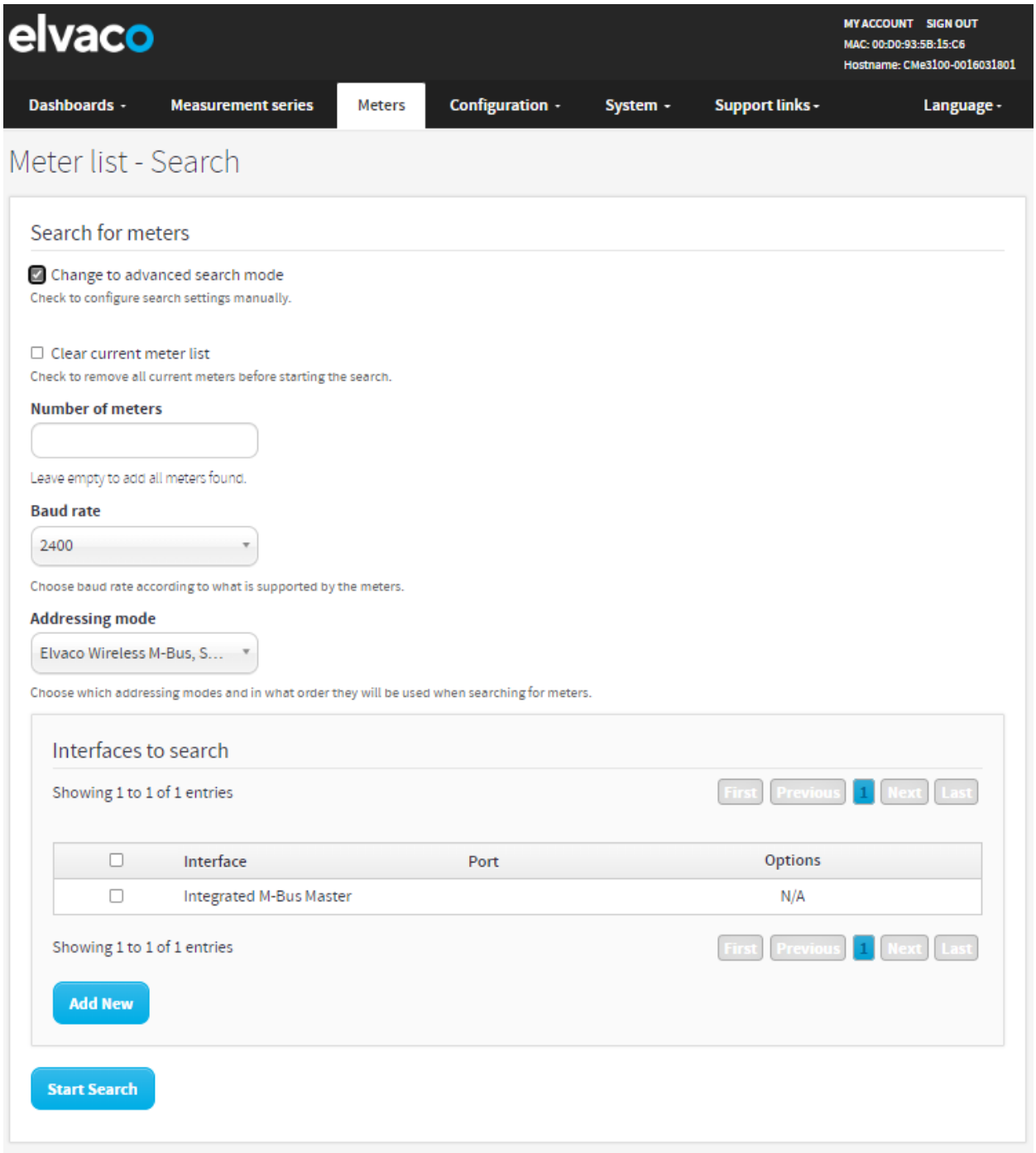
Purpose

The M-Bus Metering Gateway has the capability of performing advanced meter searches using certain predefined criteria defining what meters should be searched for.

6.21.1 Customize the meter search

To customize the meter search:

- Go to **Meters > Search for meters**. Check the Change to advanced search mode box.
- Select the number of meters that will be installed and the baud rate that will be used by the Metering Gateway to communicate with the meters.
- Set the addressing mode of the meters the Metering Gateway will search for. A priority order may also be set to determine what addressing mode will be used if the first choice should not work.
- Set the Interfaces to use to search for meters. Viable options include “integrated M-Bus master” (2-wire M-Bus), “TCP/IP” (Ethernet) or a combination of both. Click **Add new** to select an additional interface. Click **Save**.
- Click **Start Search**.



6.22 Perform manual meter readouts

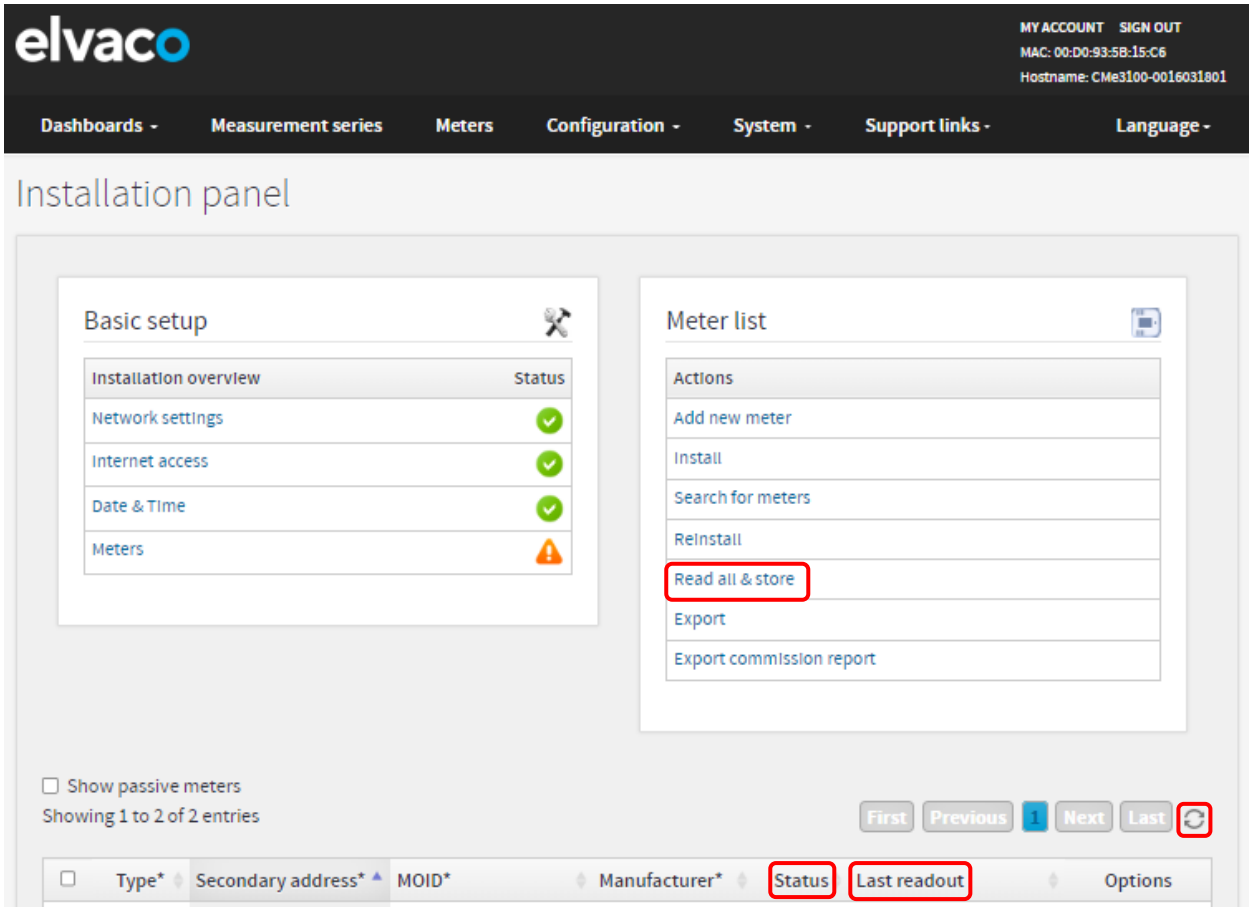
Purpose

The manual meter readout is most often used in troubleshooting purposes, to ensure that the readout process works the way it is supposed to. It will trigger a readout of one or all meters without having to wait for the scheduled readout cycle. When the settings of an individual meter have been edited, for example through a change of MOID, a manual readout of the meter must be performed before the change is fully implemented. Manual meter readouts can be performed for all installed meters or for one individual meter.

6.22.1 Perform a manual readout of all installed meters

To perform a manual readout of all installed meters:

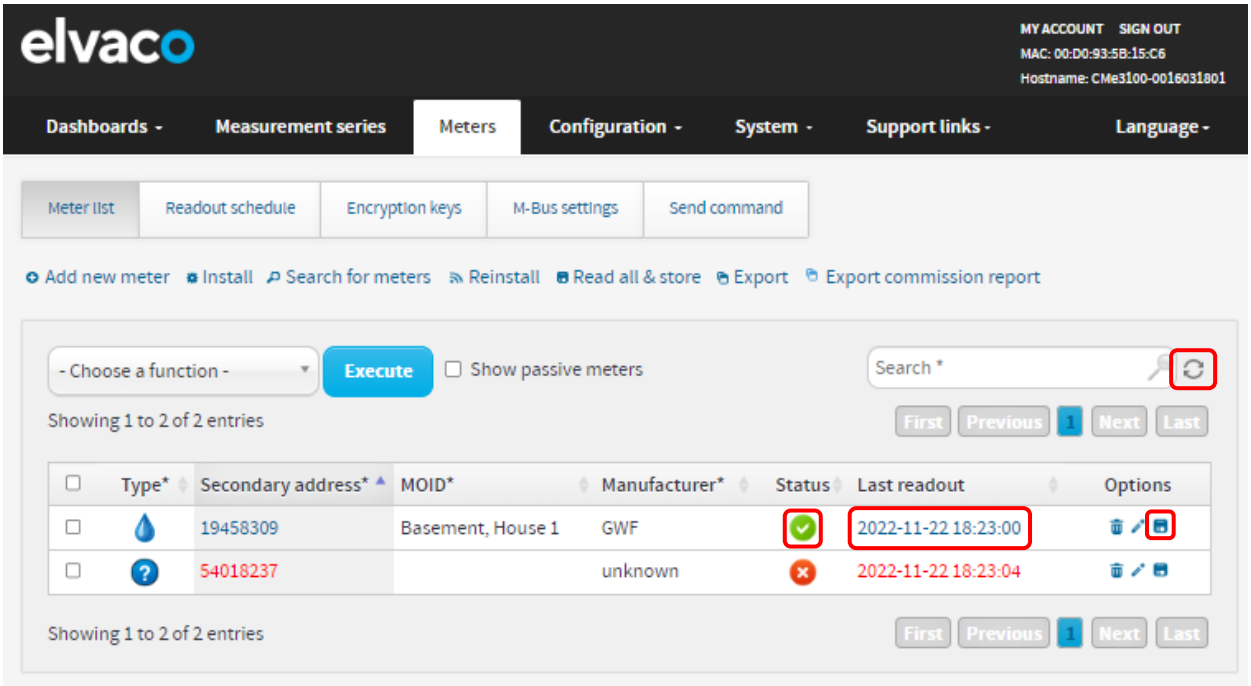
- Go to the Installation Panel
- Click **Read all & store**.
- Go to the Meter List, just below. Make sure that the readout succeeded by clicking the update symbol and check the last readout time along with the status of the readout.



6.22.2 Perform a manual readout of an individual meter

To perform a manual readout of an individual meter:

- Go to **Meters > Meter List**.
- Select the desired meter and click the readout (floppy) symbol.
- Click the update symbol and make sure that the latest readout was successful by checking the “Last readout” and the “Status” column.



6.23 Activate the Continuous Readout Mode

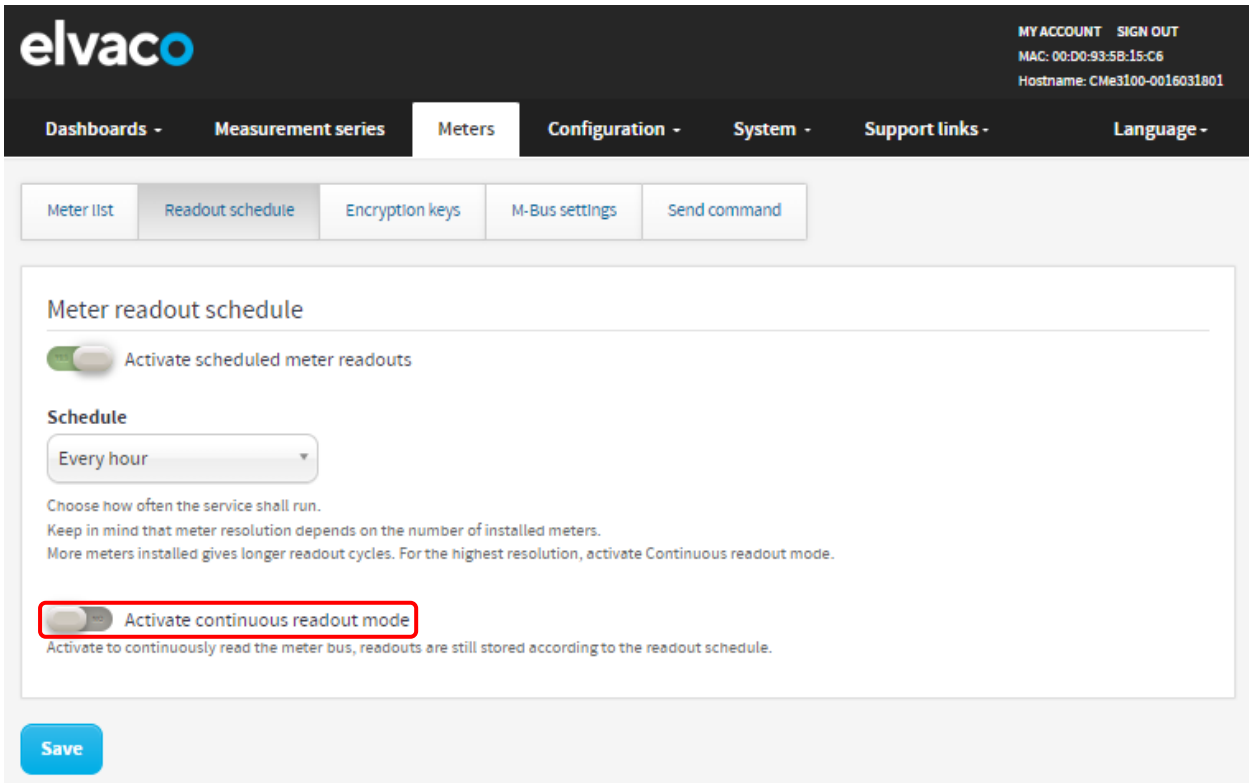
Purpose

The Metering Gateway offers the possibility of performing meter readouts continuously. The device will then constantly collect meter values, which can for example be used by a control system to regulate a heating system. Note that meter values collected through the Continuous Readout Mode will only be held in the internal memory of the M-Bus Metering Gateway (not stored in the database) and can *only* be accessed using integration protocols such as REST, Modbus, JSON or DLMS. They will therefore not be included in Push reports. To use Continuous Readout Mode in combination with Push Reports, the meter readout schedule still needs to be set.

6.23.1 Enable continuous meter readouts

To enable the Continuous Readout mode:

- Go to **Meters > Readout schedule**.
- Click on **Activate Continuous readout mode**.
- Click **Save**.



6.24 Enable security features

Purpose

The Metering Gateway supports HTTPS, FTPS and sFTP, where a Secure Socket Layer (SSL) is used to encrypt data between the device and the HTTP/FTP server. To enable HTTPS, FTPS, at least one SSL certificate must be uploaded to the web interface. To use sFTP, username and password, and username (password), key is supported.

Supported Key Exchange Methods for sFTP:

- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group14-sha256@ssh.com
- diffie-hellman-group16-sha384@ssh.com
- diffie-hellman-group16-sha512@ssh.com
- diffie-hellman-group18-sha512@ssh.com

It is important that your server certificate works with your web browser. Otherwise, you might not be able to log in on the device and must perform a factory reset.

6.24.1 Upload a certificate for device authentication

When enabling HTTPS/FTPS, an SSL certificate, either self-signed (default option) or executed by a certificate authority (CA), is uploaded in the device KeyStore. The KeyStore SSL certificate will be used by the Metering Gateway in two cases:

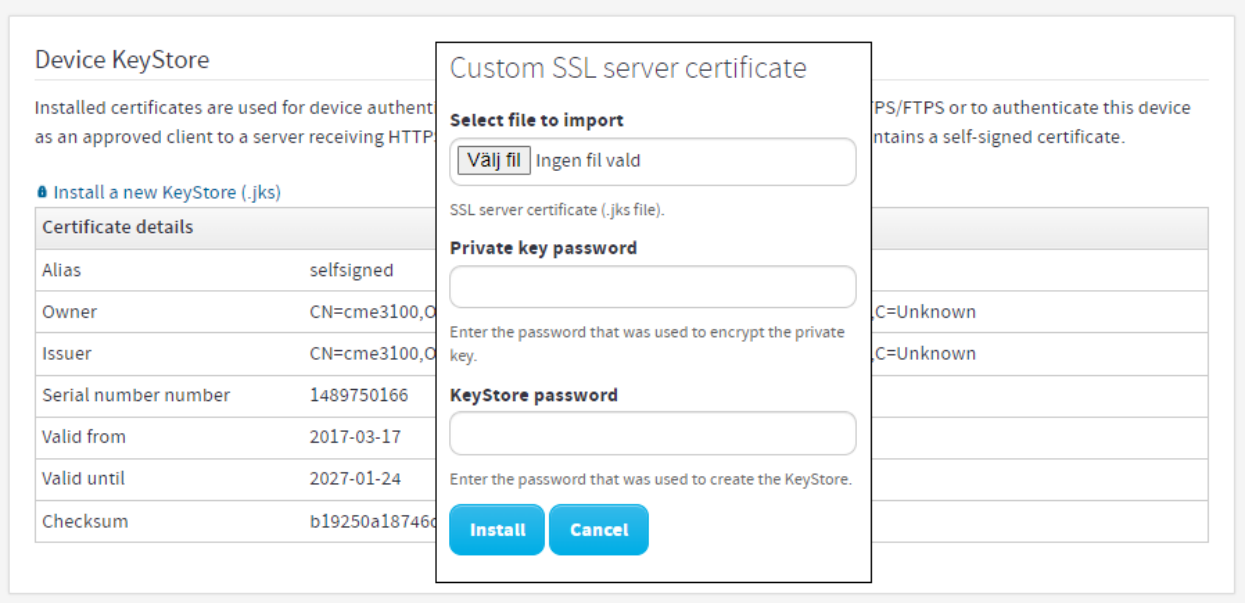
- To authenticate itself as a trusted server when a user accesses the web interface via HTTPS or FTPS.

- To authenticate itself as a trusted client to a server before delivering a HTTPS/FTPS Push Report.

If the SSL certificate has been executed by a CA, the Metering Gateway will automatically be trusted by the server/client. However, when a self-signed certificate is used, it always needs to be added to the server's/client's list of trusted certificates before a connection can be established.

To upload an SSL certificate in the KeyStore:

- Go to **Configuration > Services > Web server**.
- Click **Install a new KeyStore (.jks)**
- Attach the CA or the self-signed certificate (as a ".jks" file) as well as the private key password and the KeyStore password, which were both issued along with the certificate.
- Click **Install**.
- Click **Save**.

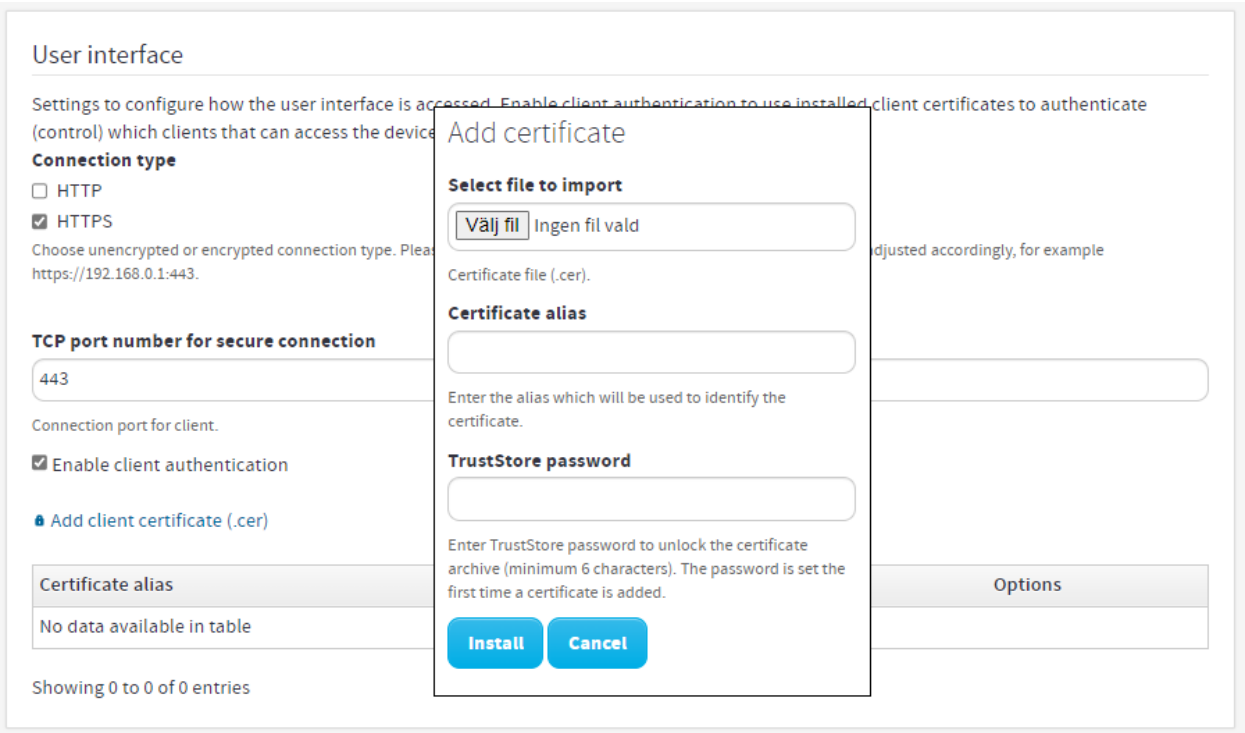


6.24.2 Enable HTTPS to access web interface

When enabling HTTPS for accessing the web interface, connecting clients will be authenticated by the Metering Gateway by using certificates uploaded in the device TrustStore.

To add a certificate of a trusted client:

- Go to **Configuration > Services > Web server**.
- Change the Connection type from HTTP to HTTPS.
- Check the "Enable client authentication" box.
- Click **Add client certificate**. Attach the client certificate (".cer" file) and a certificate alias as well as the TrustStore password, which were both issued along with the certificate.
- Click **Install**.
- Click **Save**.



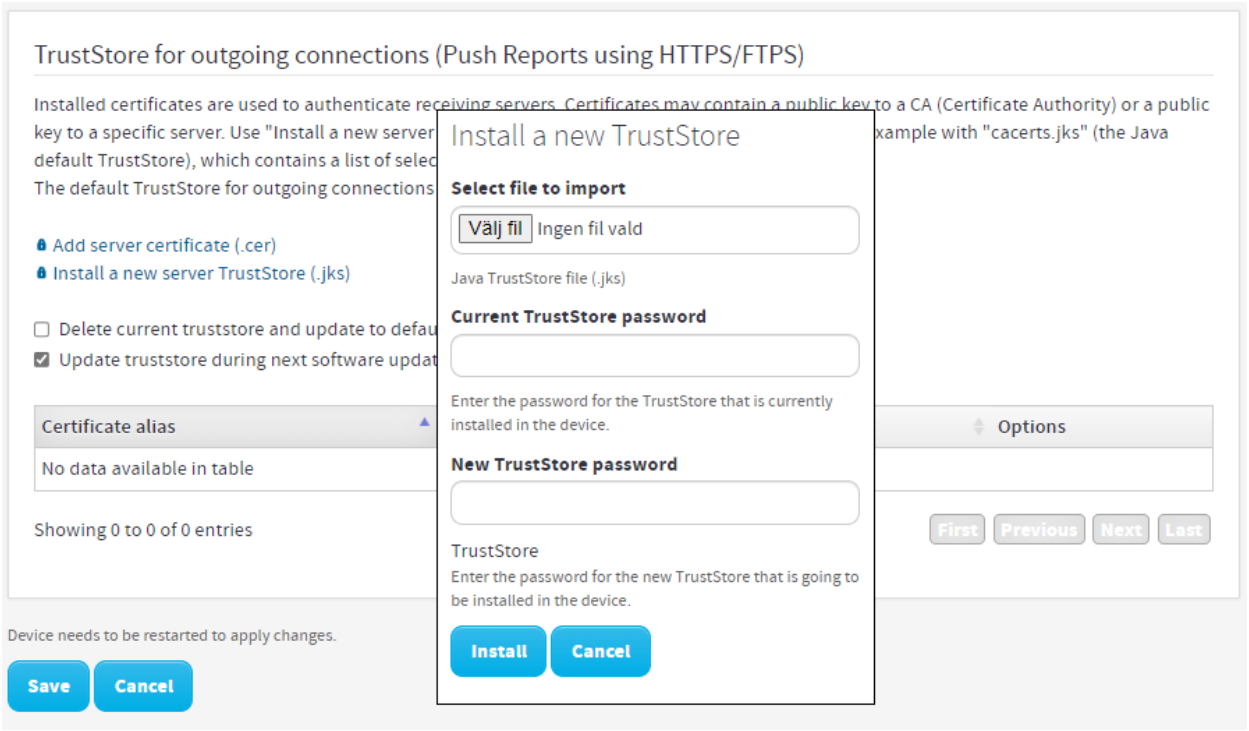
6.24.3 Authenticate receiving servers of HTTPS/FTPS/ Push Reports

CMe3100 supports transmission of Push Reports over HTTPS/FTPS. Server certificates uploaded in the TrustStore will then be used to authenticate a receiving server before sending a Push Report. By uploading a complete TrustStore, a list of trusted server certificates (for example Java standard TrustStore) can be uploaded and used by the device.

This section applies to the general Push Report settings. That means that settings configured for an individual Push Report will override changes made in this section.

To add a server certificate or a complete TrustStore:

- To Go to **Configuration > Services > Web server**.
- Click on **Add a new server TrustStore** to upload a list of trusted server certificates or click on **Add server certificate** to upload an individual certificate.
- Add current and new TrustStore password if uploading a new TrustStore. Add certificate alias and TrustStore password if uploading a separate certificate. Click **Install**.
- Click **Save**.



6.24.4 Enable HTTPS/FTPS for individual Push Reports

HTTPS/FTPS can be enabled for all Push Reports, without changing the default Push Report HTTP/FTP server of the device.

To enable HTTPS/FTPS for an individual Push Report:

- Go to **Configuration > Push Reports**. Select the Push Report you want to configure.
- Set **Report type (**“FTP” or “HTTP”).
    - For HTTP Push Reports: Uncheck “Send report to default HTTP server” and type in the URI of the HTTPS server. If applicable, set “Basic” as **Authentication mode**, and type the credentials to log onto the server.
    - For FTP Push Reports: Uncheck “Send report to default FTP server” and type the FTP server information you want to use. Select whether to use Implicit FTPS or Explicit FTPS. If applicable, type the credentials to log onto the server.

6.25 Configure M-Bus settings

Purpose

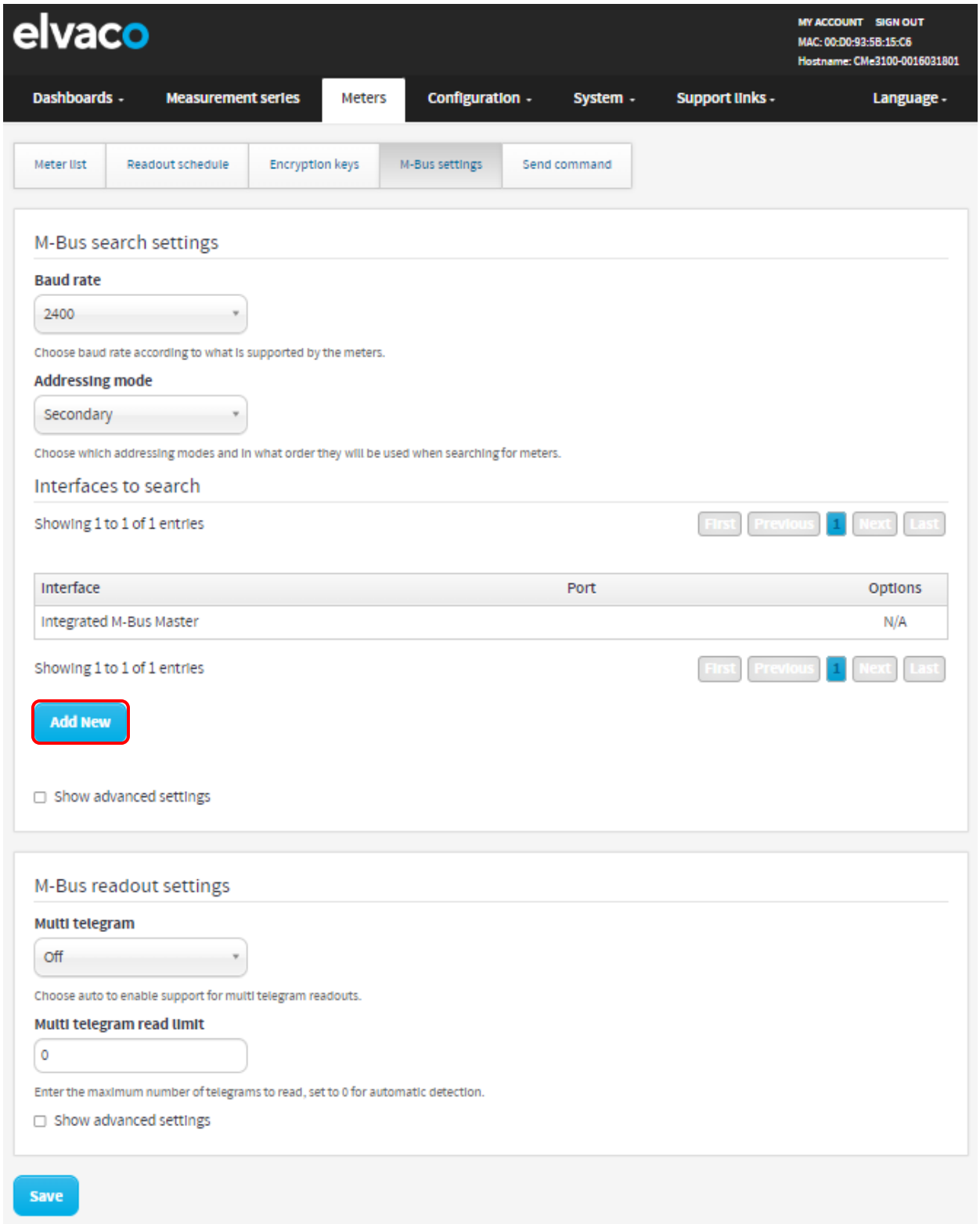
The web interface enables configuring of M-Bus settings which will be applied to all meters connected to the Metering Gateway over M-Bus. This includes baud rate, addressing mode and the interface used to search for meters.

The Metering Gateway also supports configuring of more advanced M-Bus settings, including timeout and retry settings for various M-Bus events as well as multi telegram settings.

6.25.1 Set the way meters are searched for

To set the way meters are searched for:

- Go to **Meters > M-Bus settings**.
- Set the Baud rate that will be used in the meter search. Make sure that the baud rate set for the M-Bus is supported by all the meters that the Metering Gateway is going to communicate with.
- Set the Addressing mode that will be used in the meter search. A priority order can also be set, determining what addressing mode to use if the first choice should not work.
- Set the Interfaces to search for meters. If using “Integrated M-Bus” meters will be accessed over the M-Bus interface. By selecting “TCP/IP” meters will be accessed over the Ethernet network. Click **Add New**, select TCP/IP or M-Bus and click **Save** to add an additional interface.
- Click **Save**.



6.25.2 Configure M-Bus time and retry settings

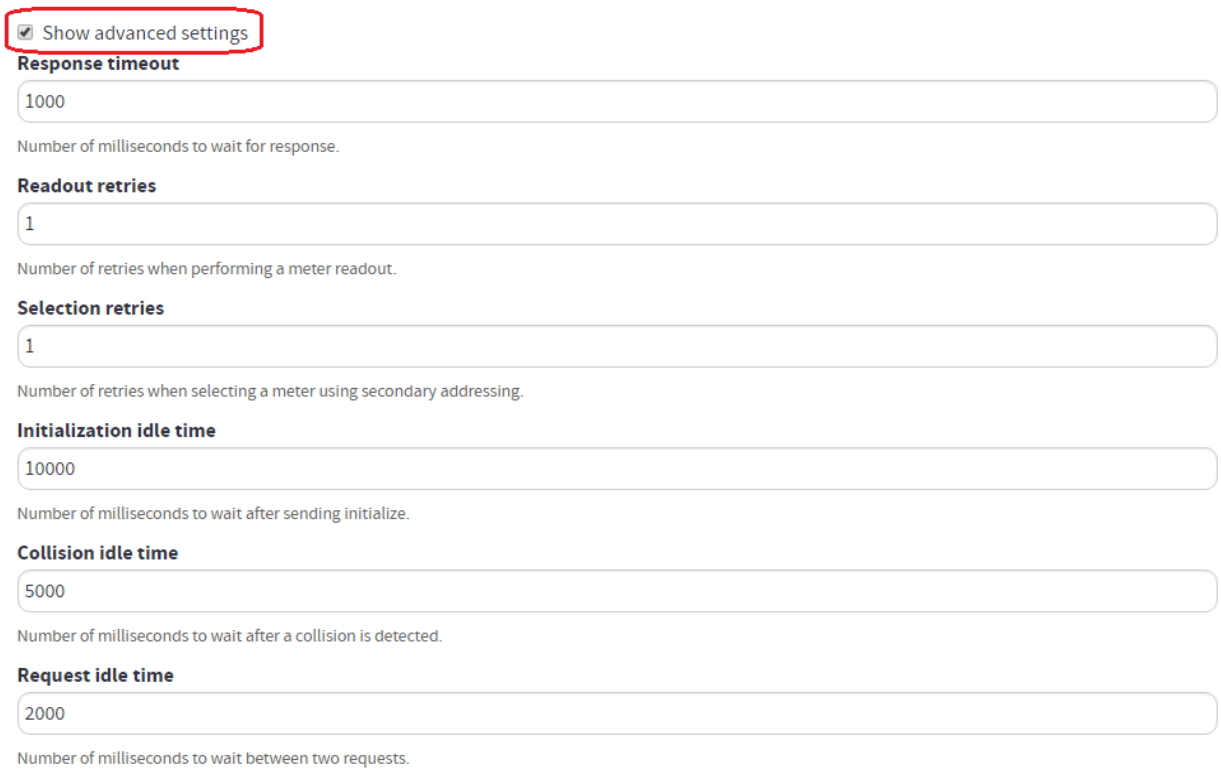
The timeout and retry settings for various M-Bus events are configurable through the web interface of the Metering Gateway. Table 7 provides a full description of customization options.

To configure the M-Bus time and retry settings:

- Go to **Meters > M-Bus settings** and check the Show advanced settings box.
- Set the Response timeout, Readout retries, Selection retries, Initialization idle time, Collision idle time and Request idle time.
- Click **Save**.

Field	Explanation
Response timeout	The Response timeout sets the number of milliseconds the Metering Gateway will wait for a response after making a request over the M-Bus.
Readout retries	The Readout retries set how many times a meter readout will be attempted before marked as a failed attempt.
Selection retries	The Selection retries set how many times the addressing of a meter will be attempted before marked as a failed attempt.
Initialization idle time	The Initialization time sets the number of milliseconds the Metering Gateway will wait after sending an initialization request over the M-Bus.
Collision idle time	The Collision idle time sets the number of milliseconds before a new request over the M-Bus is attempted after a collision has been detected.
Request idle time	The Request idle time sets the number of milliseconds of waiting time between making two requests over the M-Bus.

Table 7: M-Bus time and retry settings

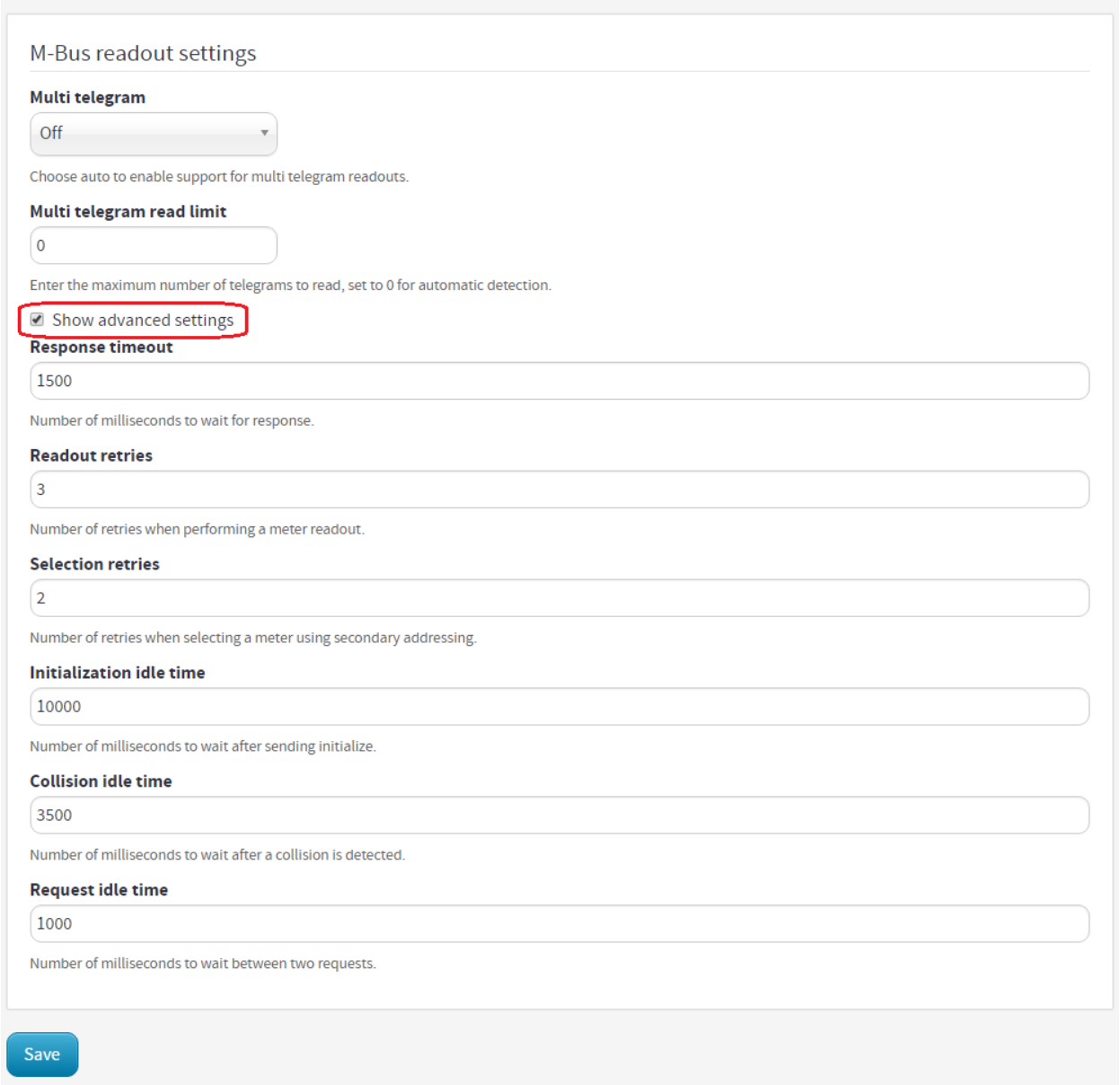


6.25.3 Configure M-Bus multi telegram settings

The M-Bus multi telegram settings determine the maximum amount of telegrams received by the Metering Gateway for each meter readout. Disabling Multi telegrams means that only the first telegram will be read for each meter readout, regardless of if the meter is trying to send additional ones. The maximum number of telegrams per readout is configured by setting the multi telegram read limit.

To configure M-Bus multi telegram settings:

- Go to **Meters > M-Bus settings**.
- To enable multi telegrams, select “Auto” in the Multi telegram tab.
- Set the Multi telegram read limit to configure the maximum number of telegrams sent per readout.
- Check the Show advanced settings box to configure time and retry settings for the multi telegrams. Explanation of each field is available in Table 7 of section 6.25.2 (Configure M-Bus time and retry settings).

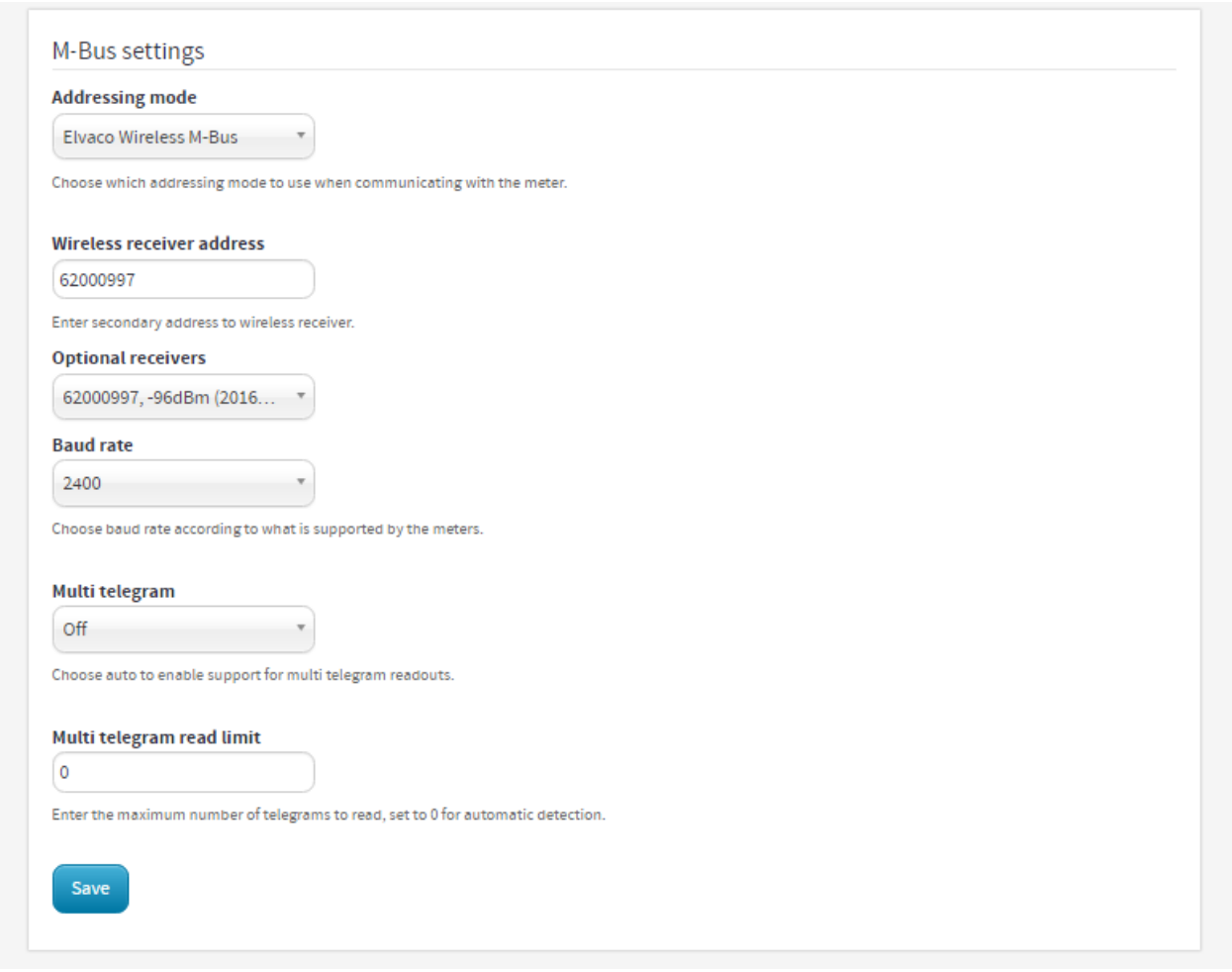


6.25.4 Configure M-Bus settings of an individual meter

. To configure M-Bus settings of an individual meter:

- Go to **Meters** and click the secondary address of a meter.

- Go to **Settings**.
- Set the Baud rate that will be used by the Metering Gateway to communicate with the meter.
- Set the Addressing mode that will be used by the Metering Gateway to access the meter. If using the wireless addressing mode, you may select through which Wireless M-Bus Receiver the meter should be accessed. However, the meter will by default automatically be assigned to the Wireless Receiver which has managed to establish the best connection.
- Set the state of the multi telegram. If enabled, set the Multi telegram read limit. It will determine the maximum number of telegrams read by the Metering Gateway per readout.
- Click **Save**.



6.26 Access the M-Bus from a master device

Purpose

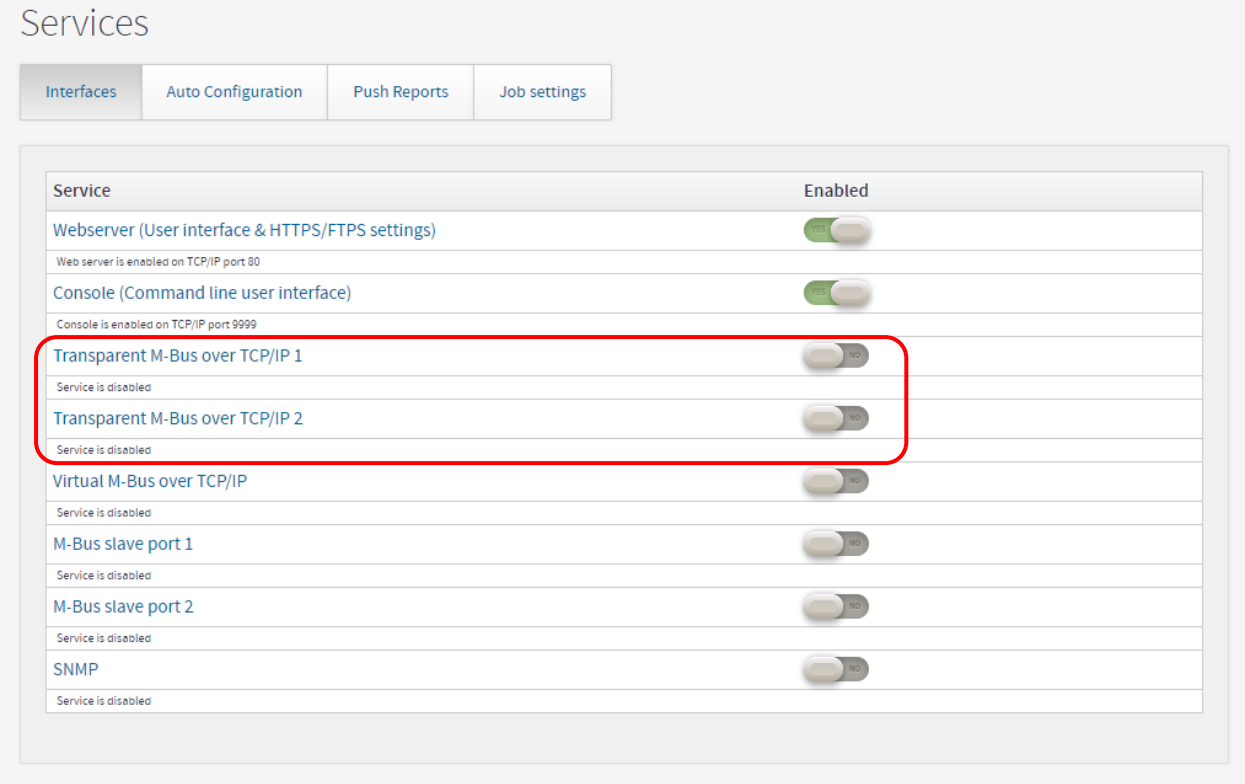
The Transparent M-Bus service enables a master device, other than the Metering Gateway, to communicate directly with the meters on the M-Bus. The Transparent M-Bus service might for example be used if direct communication with a meter is necessary for debug or meter software update purposes. In such cases, the service allows for example a Head-end system to communicate directly with the meter, completely bypassing the Metering Gateway. A maximum of two different Transparent M-Bus TCP/IP services with different baud rates can be enabled at the same time

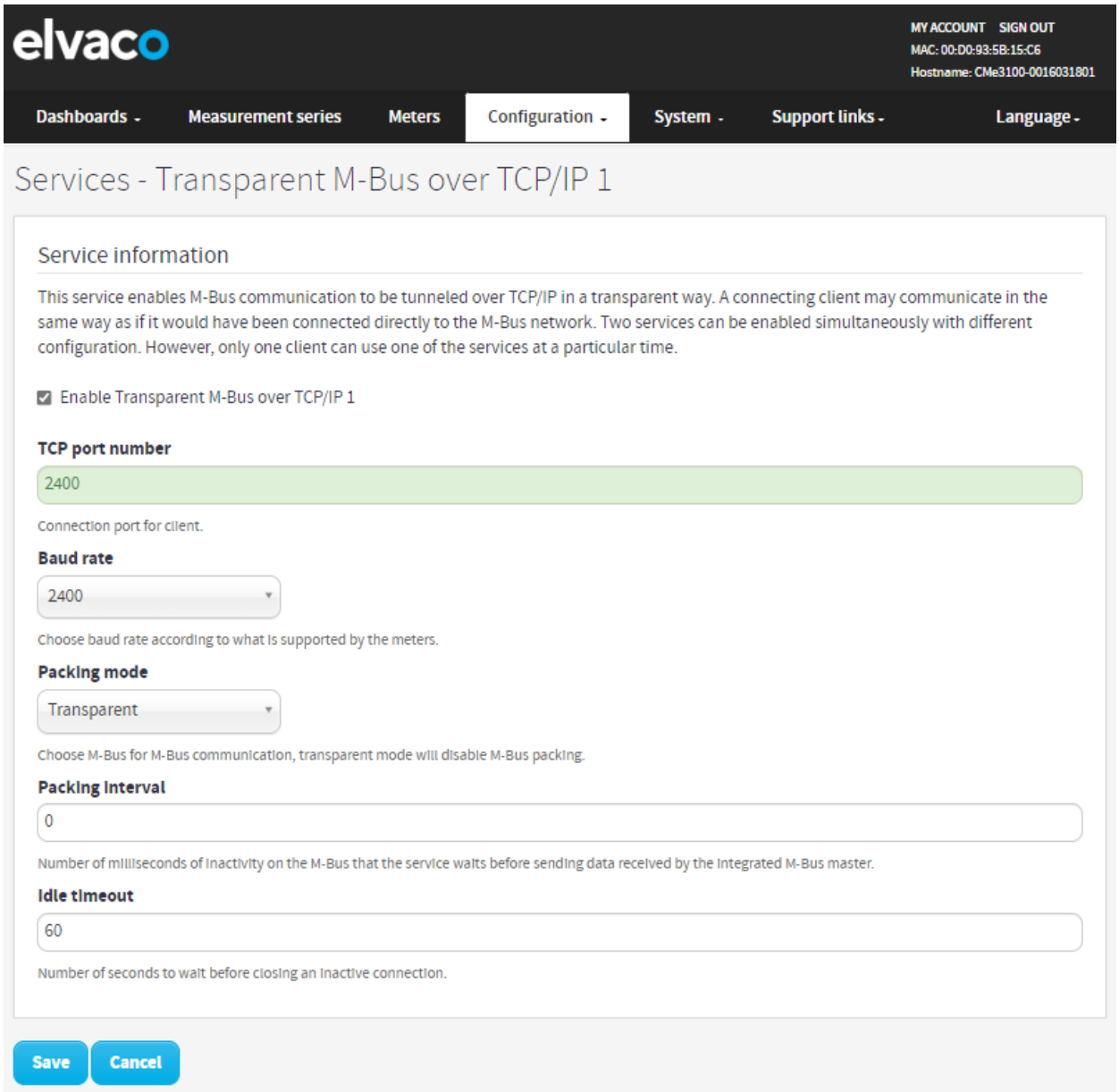
⚠	It is not recommended to enable the Transparent M-Bus service if other services that access the M-Bus, e.g., Push Reports, are active in the Metering Gateway. This might otherwise lead to that M-Bus activity due to one service interrupts the other service.

6.26.1 Enable a master device to communicate directly on the M-Bus

To enable a master device to communicate directly on the M-Bus:

- Go to **Configuration > Services**. In the list, the Transparent M-Bus services are easily enabled or disabled. Select one of the Transparent M-Bus services by clicking on it.
- Set the Baud rate and make sure it is supported by the M-Bus meters.
- Select a Packing mode. By using “M-Bus” all data transmitted over Transparent M-Bus is controlled by the Metering Gateway to assure it follows the M-Bus standard. By setting the packing interval to “Transparent” the data will be transmitted without performing any such control.
- Set the Packing interval to determine number of milliseconds that need to pass before data received from the master device is transmitted on the M-Bus.
- Set the Idle timeout to determine the number of seconds of inactivity that needs to pass before a connection with a master device is closed. Make sure that the time is set to reflect the connection scheme of the master device.
- Click **Save**.





6.27 Access meter readings from a master device

Purpose

The Metering Gateway supports Virtual M-Bus communication over TCP/IP, which means that another master device can retrieve data directly from the database of the CMe3100. When using the Virtual M-Bus mode, the master device will never communicate directly on the M-Bus, but only with the Metering Gateway and its meter value database.

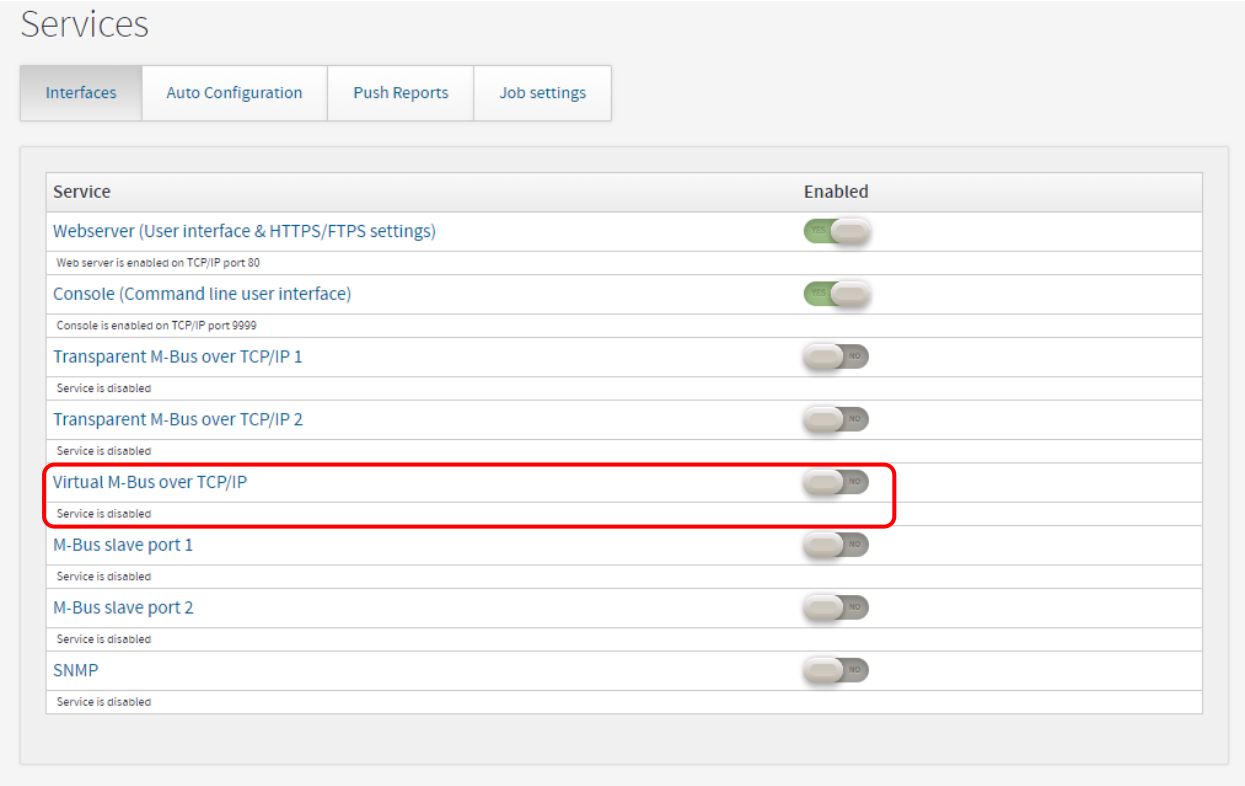
6.27.1 Allow a master device to collect meter values from the database

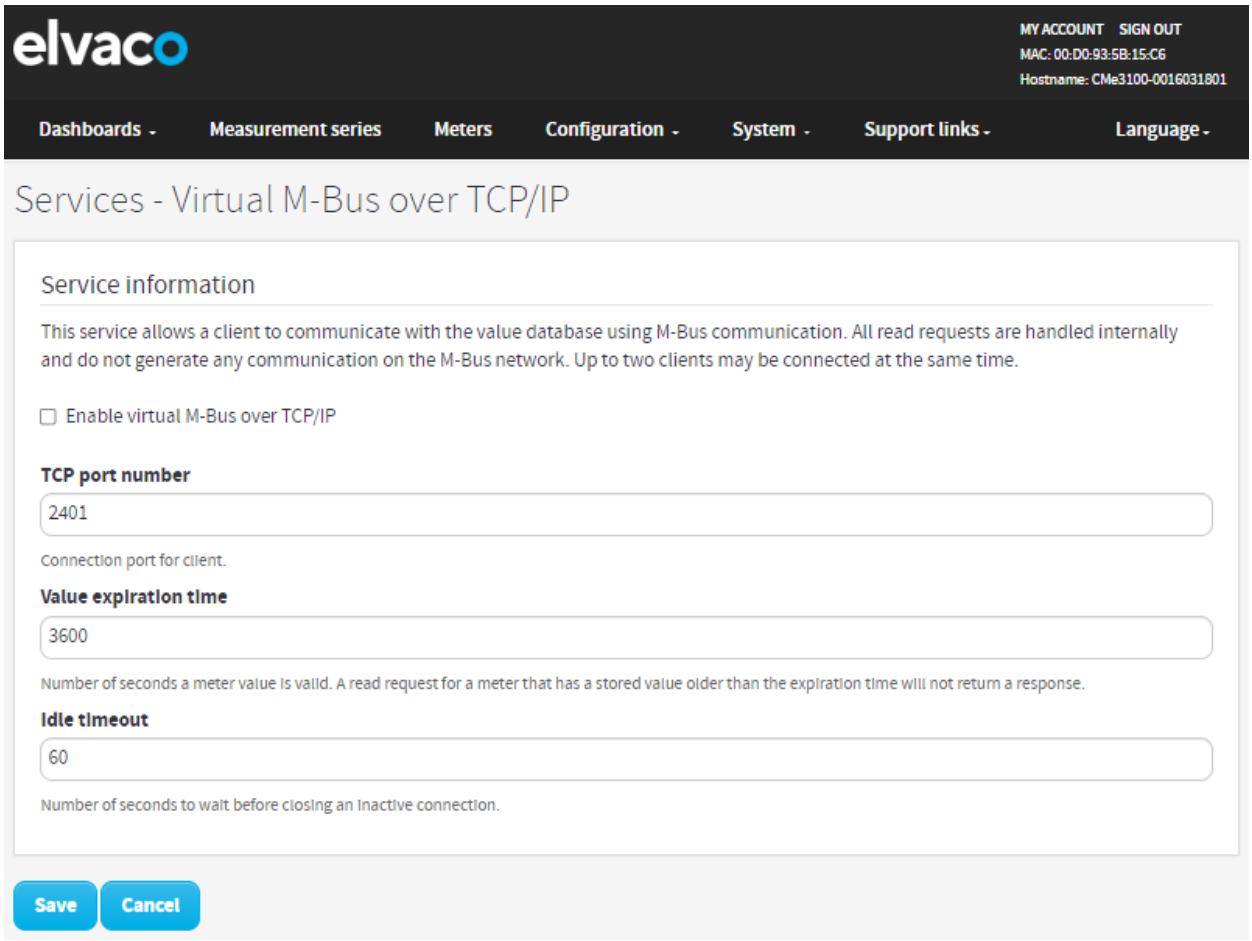
To allow a master device to collect meter values from the database of the Metering Gateway:

- Go to **Configuration > Services**.
- Enable the Virtual M-Bus service. Click on it to configure the Virtual M-Bus settings.
- Set the Value expiration date to determine how long a stored meter value will be valid if requested over Virtual M-Bus. If a meter value has been stored in the database for a longer time than the value expiration time, a requesting master device will receive a “not valid” notification if

the meter value should be requested.

- Set the Idle timeout to determine how many seconds a communication link with a master device may be inactive before it is closed. The default setting allows for ample time between operations without the need of reconnecting and assures that a connection that is lost, automatically closes after the timeout period. It will work well in most cases. However, the Idle timeout needs to be set to reflect the connection scheme of the master device.
- Click **Save**.





6.28 Use M-Bus slave ports for Virtual or Transparent M-Bus

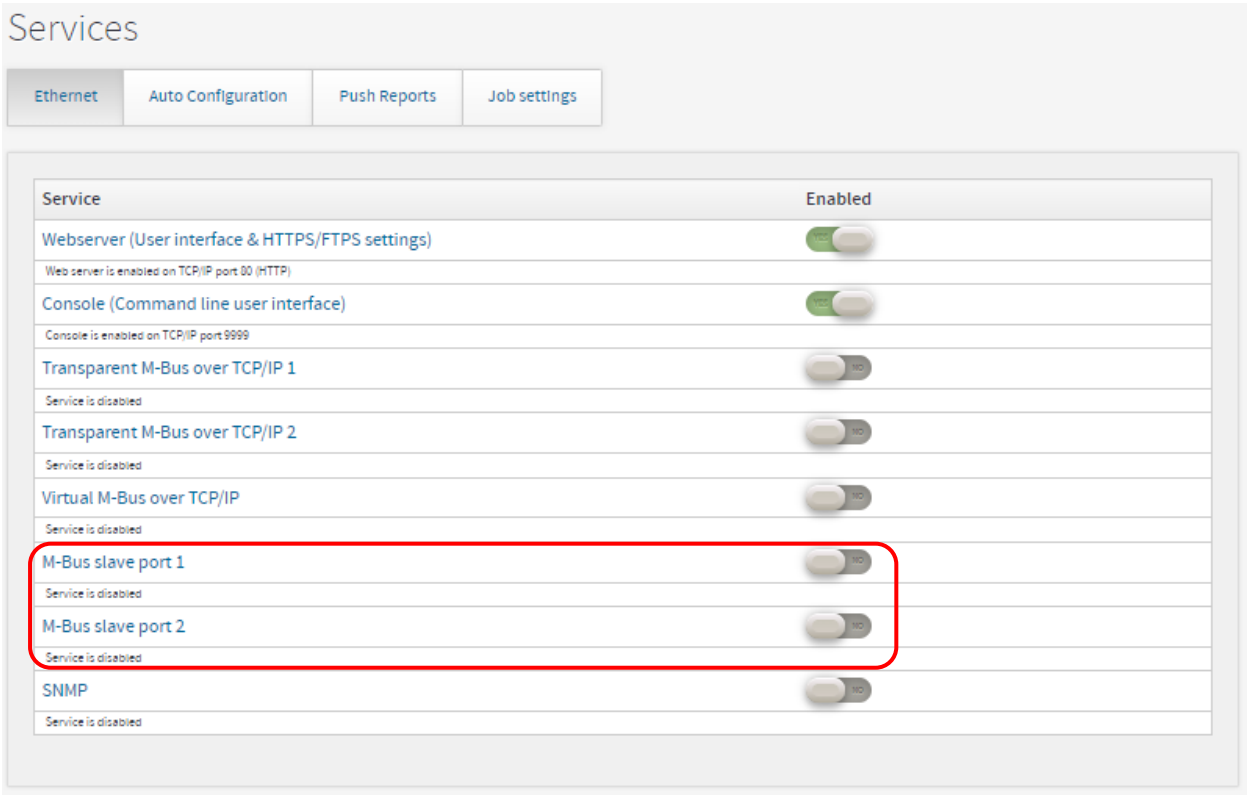
Purpose

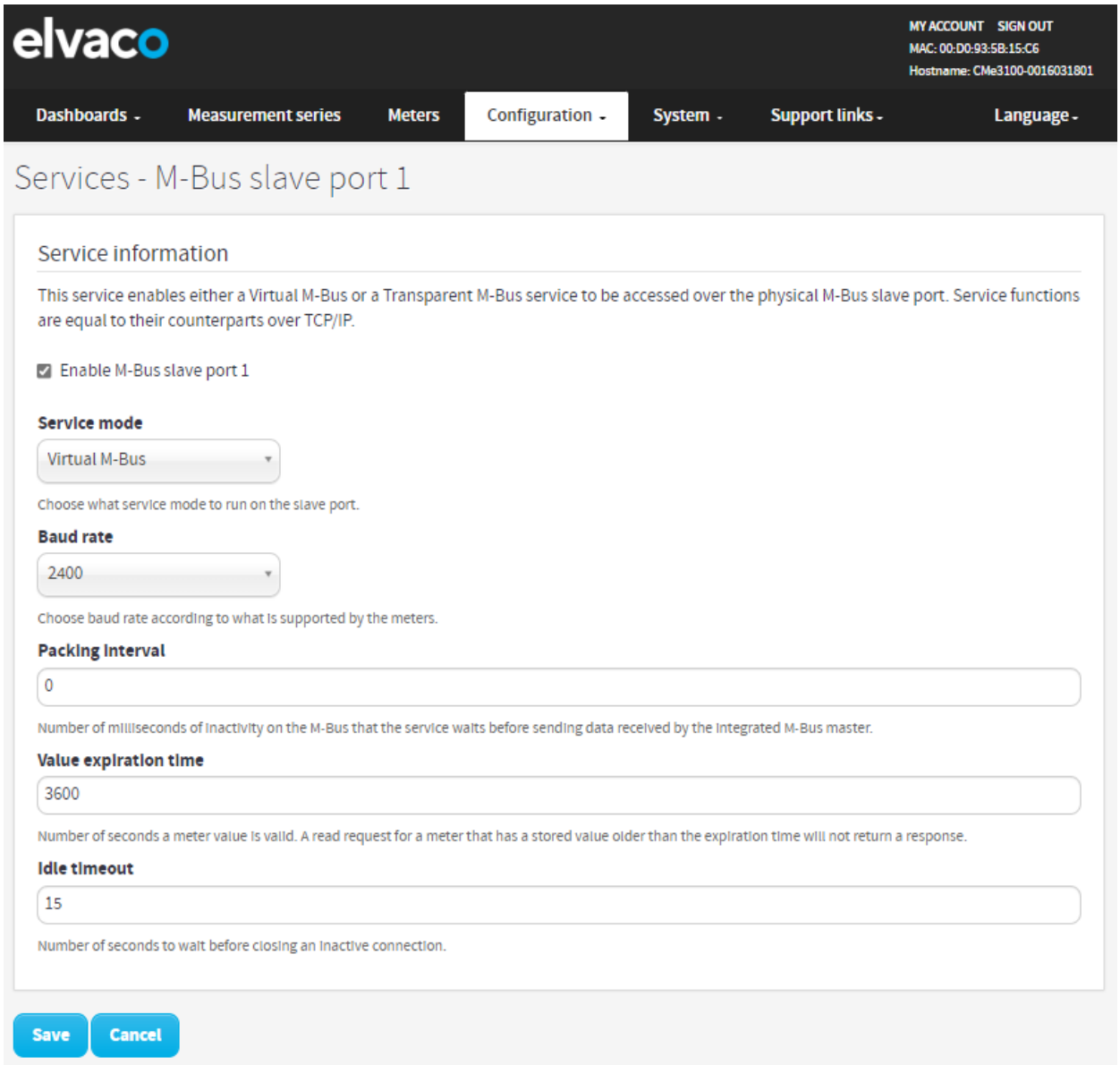
The Metering Gateway has two slave ports available, which can be used by a master device to access the Virtual or Transparent M-Bus services. Each port can be individually configured by setting the baud rate, packing interval and idle timeout settings.

6.28.1 Activate and configure the settings of the M-Bus slave ports

To activate and configure the settings of the M-Bus slave port:

- Go to **Configuration > Services**.
- Enable the desired slave port. Click on it to configure its settings. Select whether the master device should use the Transparent M-Bus or Virtual M-Bus service when connecting to the slave ports.
- Set the Baud rate to determine the rate of communication between the Metering Gateway and its master device.
- Set the Packing interval to determine how many milliseconds that will have to pass before data received by the Metering Gateway will be sent to the master device.
- Set the Idle timeout to determine the number of seconds of inactivity that needs to pass before a connection with the master device is closed. Make sure that the time is set to reflect the connection scheme of the master device.
- Click **Save**.


Services
Ethernet
Auto Configuration
Push Reports
Job settings
Service
Enabled
Webserver (User interface & HTTPS/FTPS settings)
Web server is enabled on TCP/IP port 80 (HTTP)
Console (Command line user interface)
Console is enabled on TCP/IP port 9999
Transparent M-Bus over TCP/IP 1
Service is disabled
Transparent M-Bus over TCP/IP 2
Service is disabled
Virtual M-Bus over TCP/IP
Service is disabled
M-Bus slave port 1
Service is disabled
M-Bus slave port 2
Service is disabled
SNMP
Service is disabled



6.29 Allow a master device to perform readouts over Modbus

Purpose

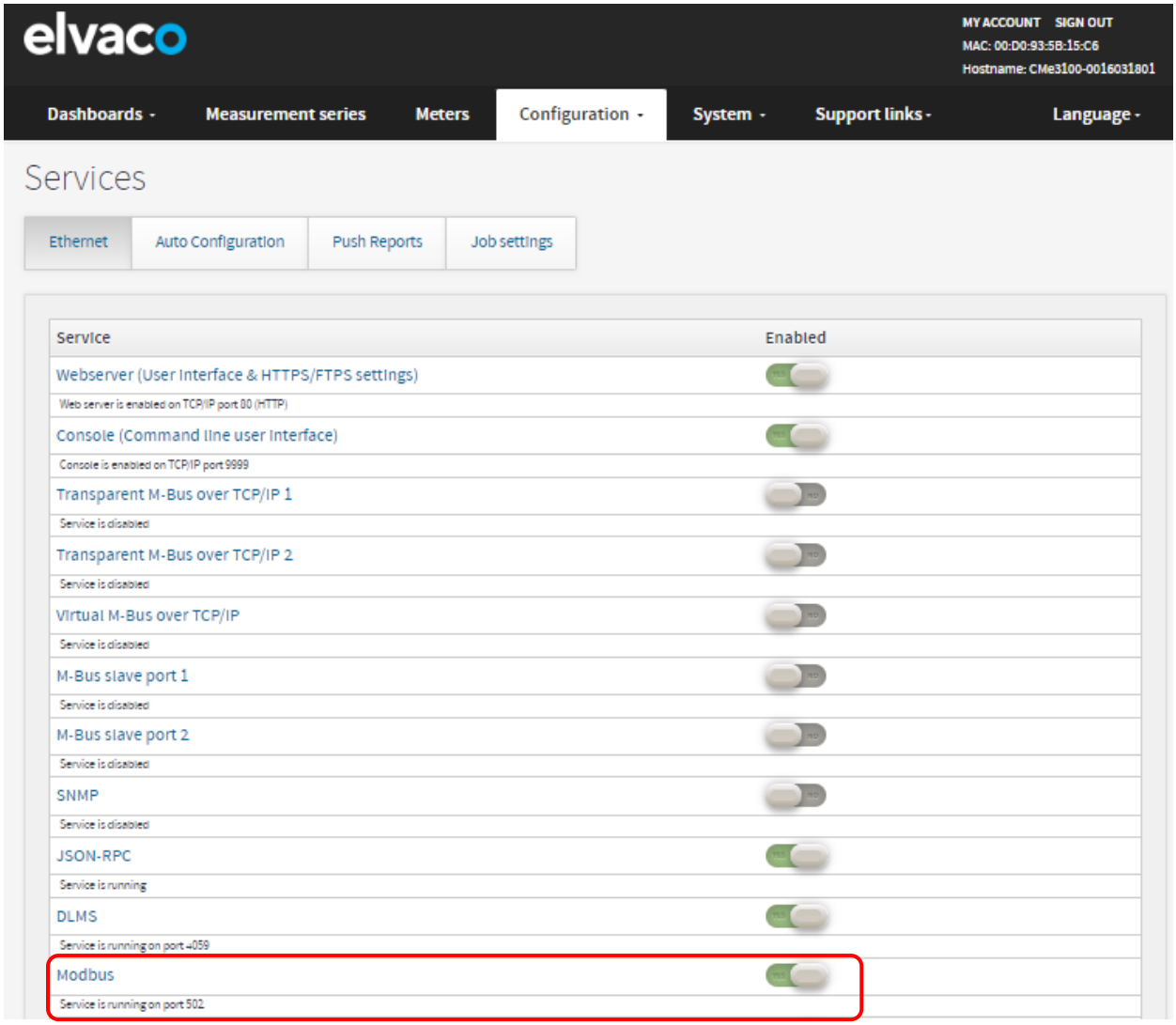
The Metering Gateway supports meter readouts by master devices over the Modbus protocol, which might for example be desired in a Digital Control System. The Modbus readout is performed by TCP/IP (Ethernet network).

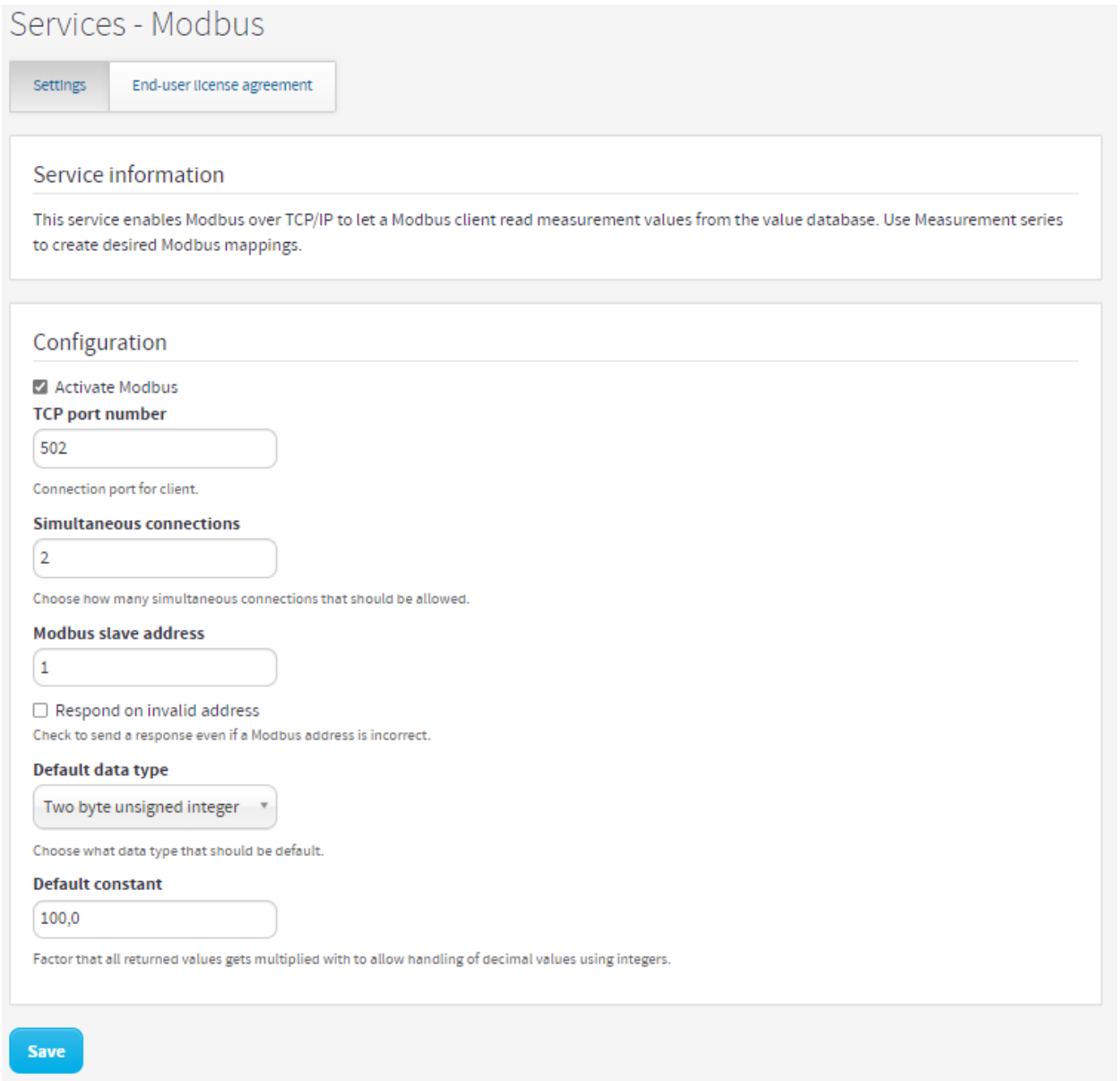
6.29.1 Enable meter readouts over Modbus

To enable meter readouts over Modbus:

- Go to **Configuration > Services**.
- Enable the Modbus service in the list. Click on it to enter the settings.
- Go to **Settings**. Set the Number of simultaneous connections that should be allowed (i.e., the number of requesting clients in the system).
- Set the Default data type and the Default constant to handle decimal values. Make sure they correspond with the ones used by the master device.

- Select if the Metering Gateway should respond to invalid Modbus addresses.
- Click **Save**.





6.30 Monitor metering status using SNMP

CMe3100 supports SNMP v2c, a standardized protocol used for monitoring of devices on a TCP/IP network. By activating the SNMP service, the Metering Gateway will aggregate the result of the last meter readout and the last round of Push Reports and make it available for an SNMP manager to poll. There are three available status codes used to describe the status of meter readouts and Push Reports. Table 8 describes each one.

Status	Mode	Description
1	OK	The last meter readout and the last round of Push Reports were both successful.
2	WARNING	The last meter readout completed with errors for one or several (but not all) meters or the last round of Push Reports completed with errors for one or several (but not all) reports.
3	ERROR	The last meter readout was unsuccessful for all meters, or the last round of Push Reports was unsuccessful for all reports.

Table 8: Aggregated status of meter readouts and Push Reports

CMe3100 uses a MIB-file, which can be downloaded from the web interface to structure lists that will present the SNMP manager with the status of the last meter readout and the last round of Push Reports. The following lists are available for the SNMP manager software to access:

- A Status Report, which presents the aggregated status of the last meter readout and the last round of Push Reports. Table 8 describes the meaning of each status code.
- A Meter Status List, which presents the last readout status for each individual meter. If the last meter readout succeeded, the status code will be “1”. If it failed, the status code will be “3”. Status code “2” indicates that CMe3100 was unable to decrypt the last message from that specific meter or that the meter has never been read.
- A Report Status List, which presents the last status of each individual Push Report. If the last Push Report succeeded, the status code will be “1”. If it failed, the status code will be “3”.

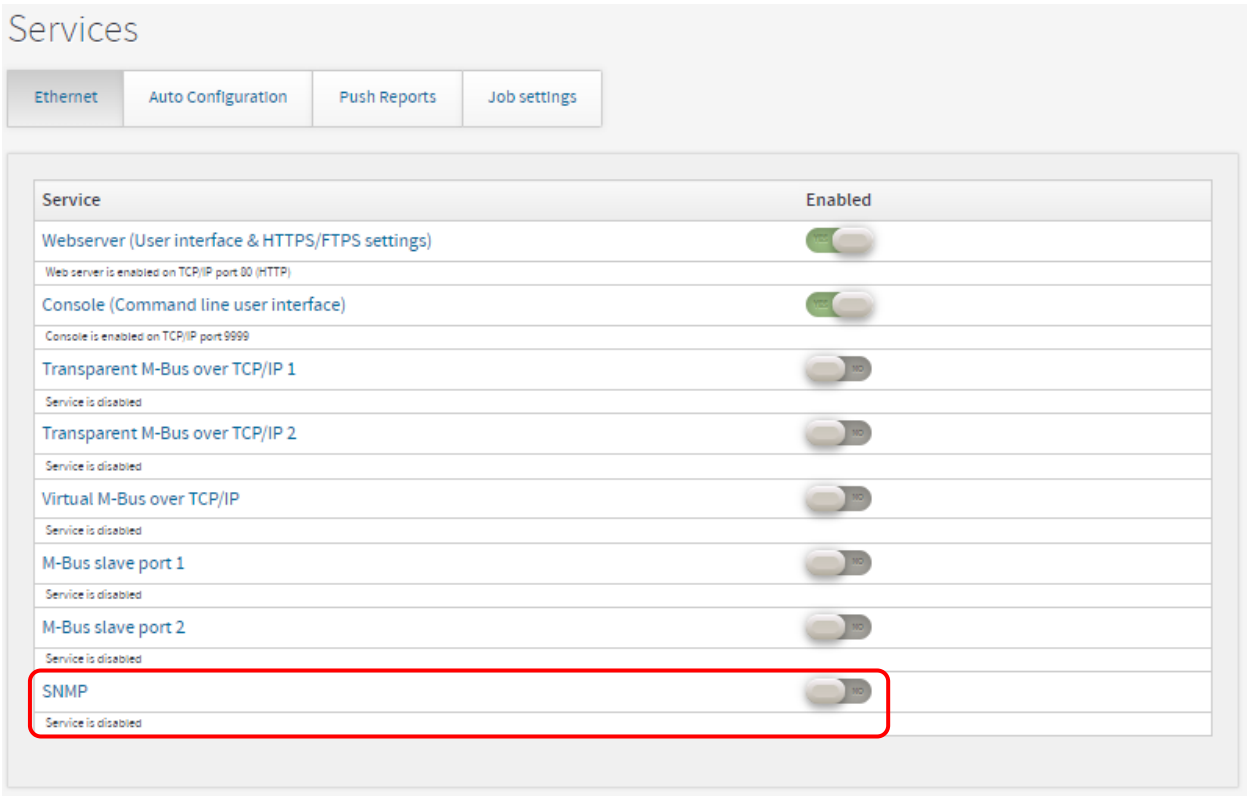
CMe3100 also supports SNMP traps, which are asynchronous notifications sent to all configured recipients each time the aggregated status of the meter readout or the Push Reports changes. For example, if one of the activated Push Report suddenly fails (and the aggregated status changes from “1” to “2”), an SNMP trap will be triggered, and all recipients will be notified.

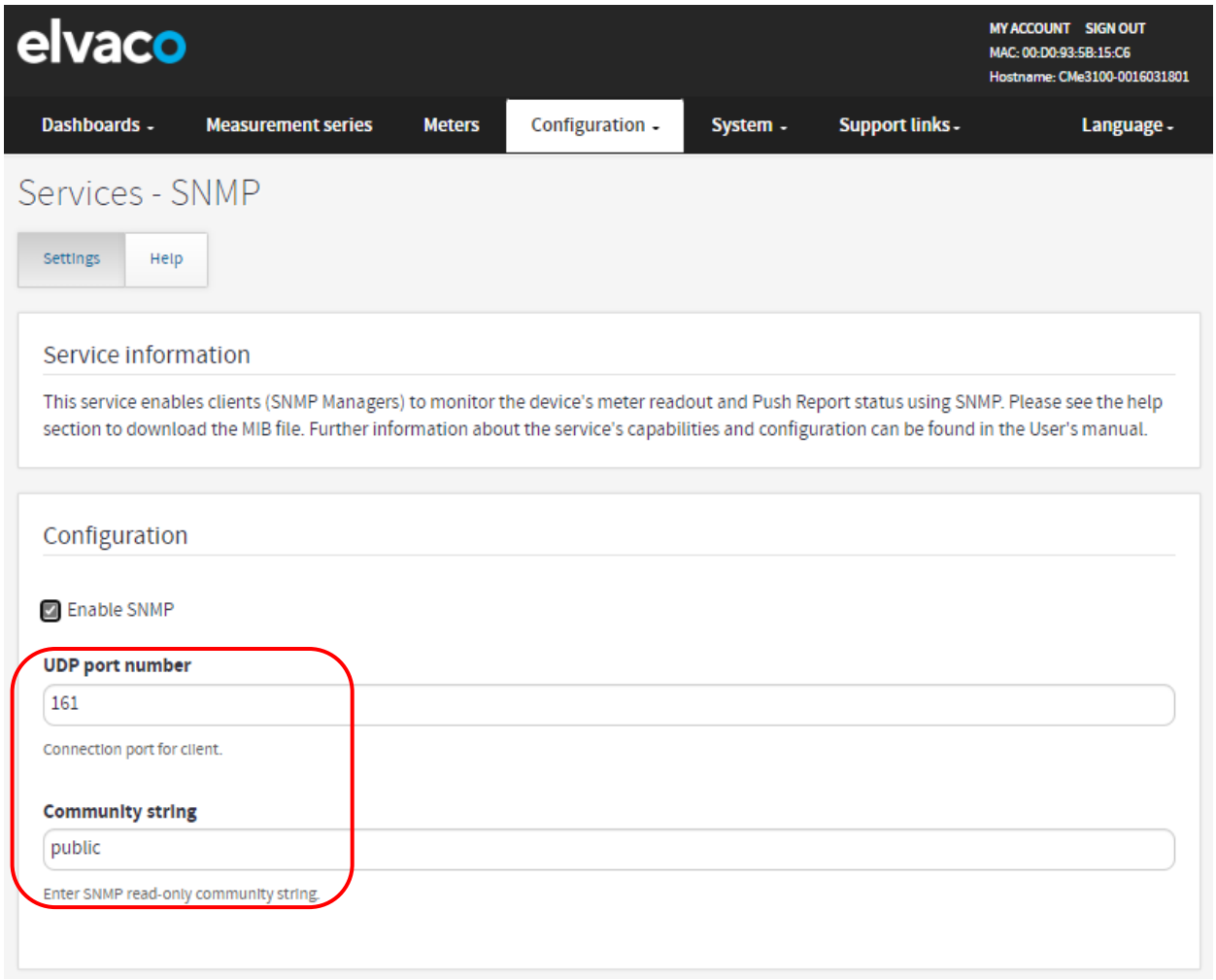
The SNMP trap message only informs that the aggregated status has changed. Information about the meters or Push Reports that have caused the change of status can be accessed by using the Meter Status List and the Report Status List.

6.30.1 Enable and configure the SNMP service

To enable and configure the SNMP service:

- Go to **Configuration > Services**.
- Activate SNMP in the list.
- Click on the service to enter its settings.
- Set the TCP port number for the SNMP manager to connect to.
- Set the Community string. The SNMP manager and the device need to use the same community string to communicate with each other.
- Click **Save**.

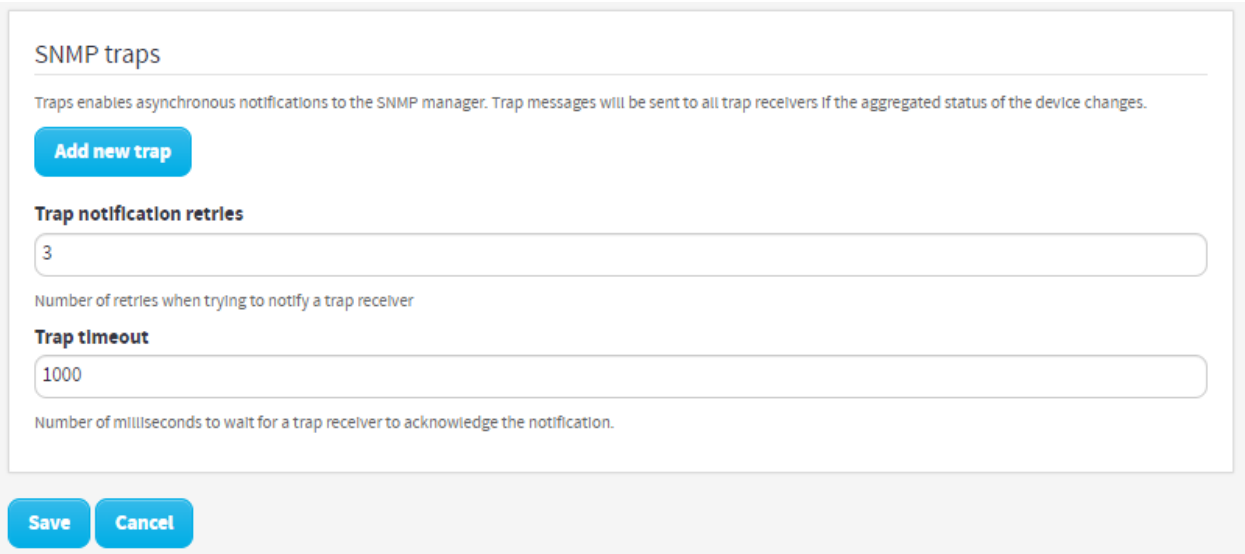

Services
Ethernet
Auto Configuration
Push Reports
Job settings
Service
Enabled
Webserver (User interface & HTTPS/FTPS settings)
Web server is enabled on TCP/IP port 80 (HTTP)
Console (Command line user interface)
Console is enabled on TCP/IP port 9999
Transparent M-Bus over TCP/IP 1
Service is disabled
Transparent M-Bus over TCP/IP 2
Service is disabled
Virtual M-Bus over TCP/IP
Service is disabled
M-Bus slave port 1
Service is disabled
M-Bus slave port 2
Service is disabled
SNMP
Service is disabled



6.30.2 Set recipients of SNMP traps (optional)

To set recipient of SNMP traps:

- Go to **Configuration > Services** and activate the SNMP service. Click on the service and go to **Settings**.
- Click **Add new trap** and type in the hostname and the port of the desired recipient.
- Set Trap notification retries to determine the maximum number of retries the CMe3100 will perform when trying to notify a trap receiver.
- Set “Trap timeout” to determine the maximum number of seconds the CMe3100 will wait for a response from the SNMP manager when sending a trap notification.
- Click **Save**.



6.31 Enable automatic updates of configuration settings

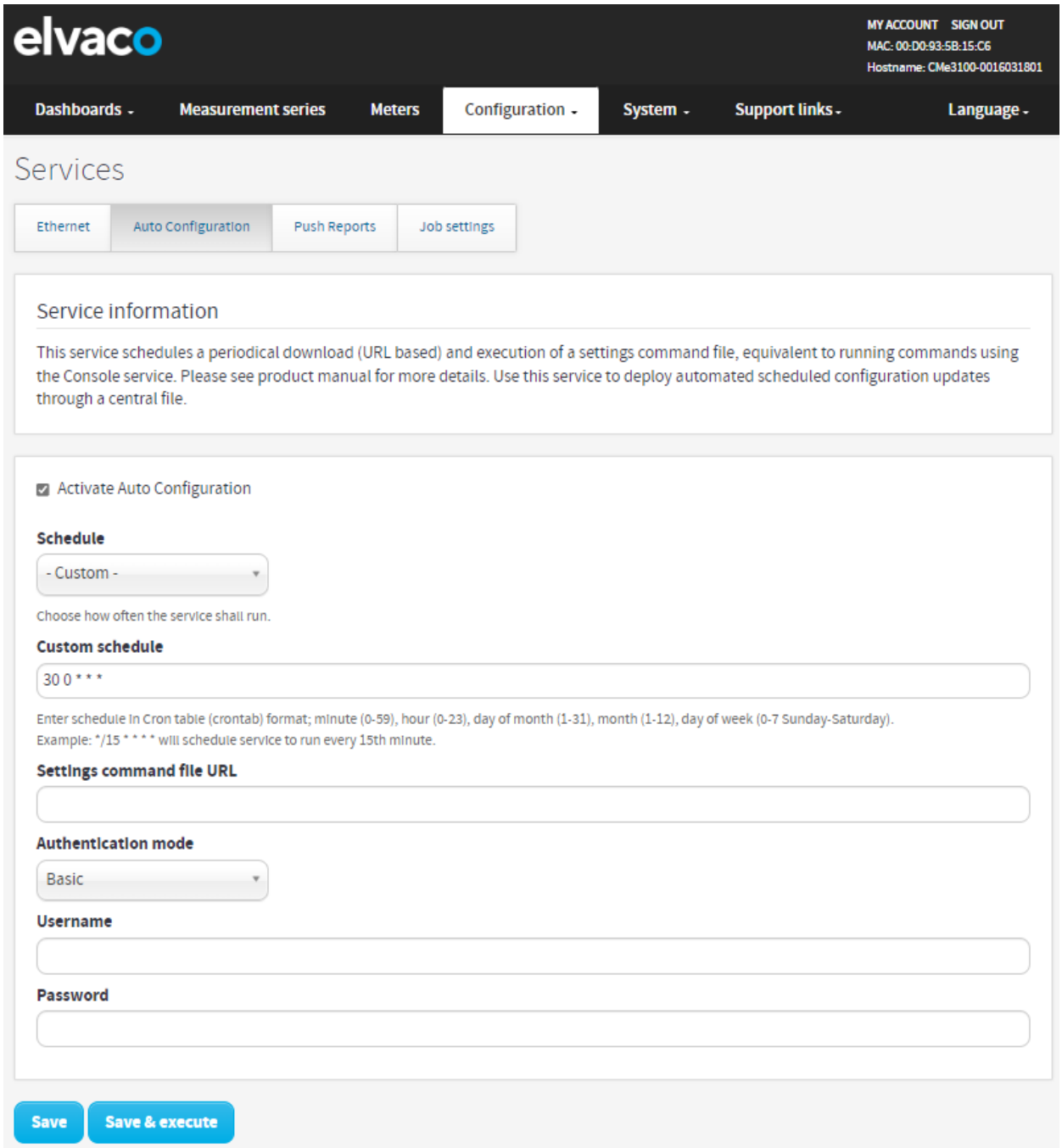
Purpose

By activating the Auto Configuration service, the Metering Gateway will periodically check a URL for a settings command file (.cad file) which will be downloaded and parsed. The settings command file can include settings updates like what is possible using the command line interface.

6.31.1 Enable and configure the Auto Configuration service

To enable and configure the Auto Configuration service:

- Go to **Configuration > Services > Auto Configuration**.
- Check the Activate Auto Configuration box.
- Select the schedule of the Auto Configuration service out of the preset alternatives or by using cron patterns. To learn more about cron patterns, see section 6.39.1 (Set schedules with cron patterns).
- Type in the URL of the command file.
- Select whether to enable Basic authentication mode, which will then be used every time an Auto Configuration is run.
- Click **Save**.



6.32 Configure advanced Push Report settings

Purpose

There is a group of more advanced Push Reports settings, configurable through the web interface of the Metering Gateway. These include:

- Adaptive Retries functionality, which adjust retry attempts for failed Push Reports to the schedule in use.
- Value Period, which determines how far back in time the Metering Gateway will include values for when compiling a Push Report.
- Value Interval, which determines the time between the readouts included in the Push Reports.

- Timeout value, which for each protocol determines how long a Push Report transmit attempt may linger before timing out

6.32.1 Disable Adaptive Retries

The Adaptive Retries ensure that all Push Report retry attempts are performed before the next scheduled Push Report is going to be sent. For example, if the Push Report schedule is set to every 16th-60th minute, up to two retries will be attempted with 300 seconds between each one. If all retry attempts fail, the meter values will instead be included in the next Push Report. Table 9 provides a description of the concept.

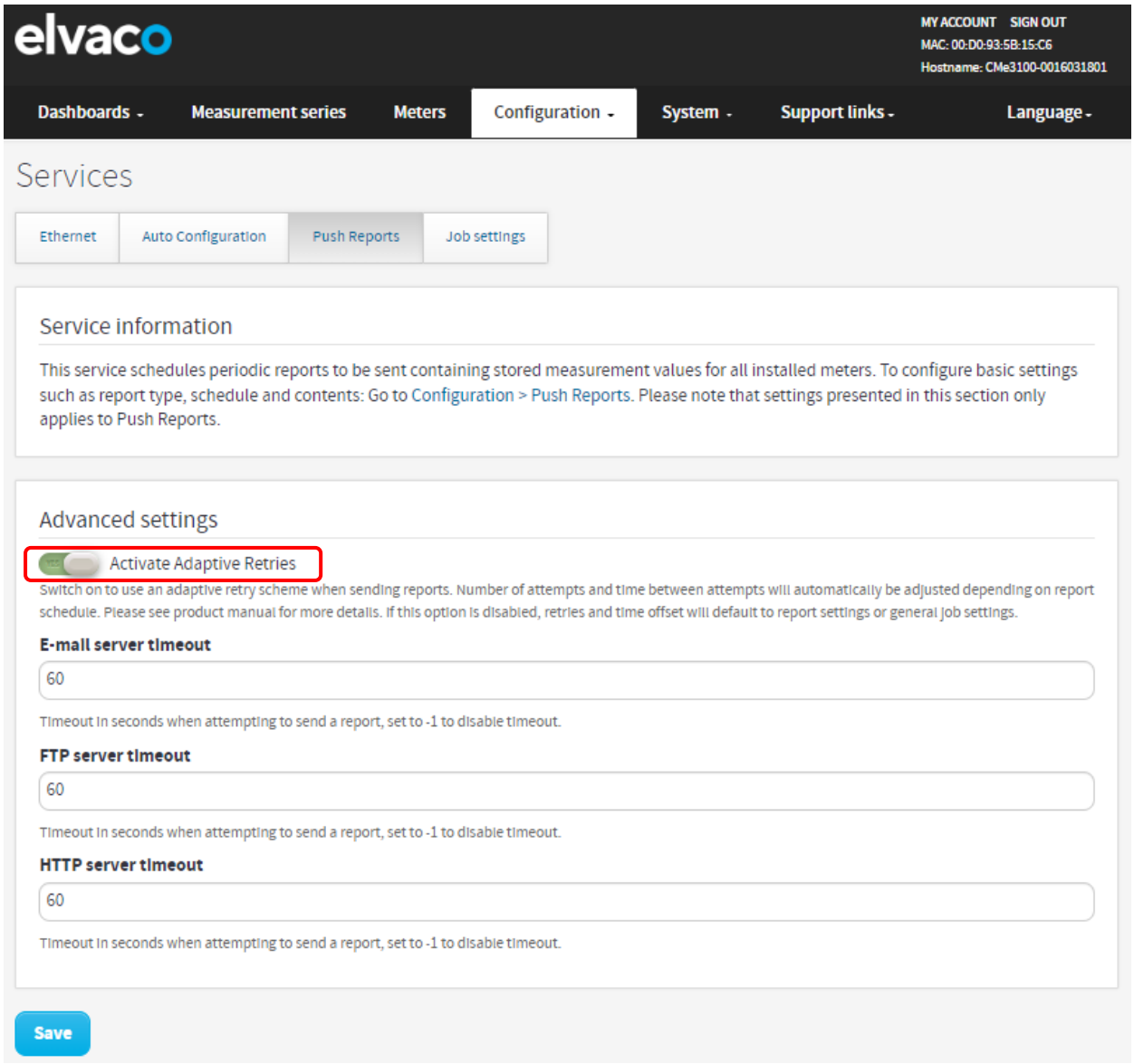
Push Report schedule	Max amount of retry attempts	Seconds between each attempt
1-15 min	1	0
16-60 min	2	300
61 min-23 h	3	500
>23 h	6	3600

Table 9: Adaptive retry schedule

If choosing to disable the Adaptive Retries, the Metering Gateway will use its individual report settings to determine how to handle failed Push Report attempts. These settings are not displayed in the web interface but can be accessed through the console interface. If no such report settings have been configured for the Metering Gateway, general job settings will determine how the device handles failed Push Report retry attempts.

To disable Adaptive Retries:

- Go to **Configuration > Services > Push Reports.**
- Disable Adaptive Retries.
- Click **Save**.

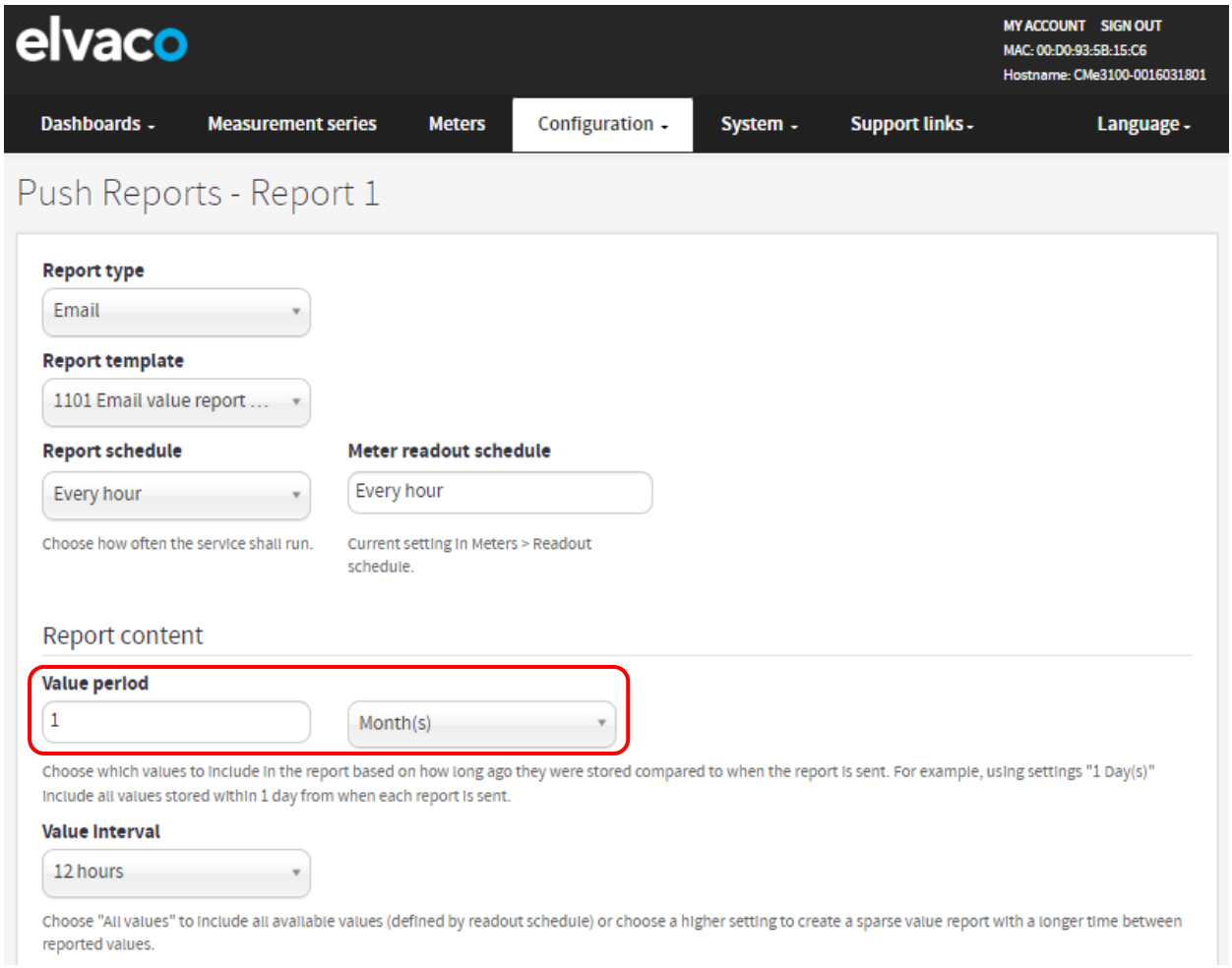


6.32.2 Configure the Value Period

The Value Period of the Metering Gateway can be set to “Auto” or to a fixed number. Using the “Auto” settings will deliver all previously unsent meter values up to a max limit of 180 meter readouts. For example, if the Metering Gateway has been unable to send Push Reports, scheduled every 15th minute for a certain amount of time, it will be able to go back and deliver a maximum of 45 hours of undelivered meter values with the next successful Push Report (180 * 15 minutes = 2700 minutes = 45 hours). When setting the Value Period to a fixed number, the Metering Gateway will look exactly that far back in time for undelivered meter values.

To configure the Value Period of the Metering Gateway:

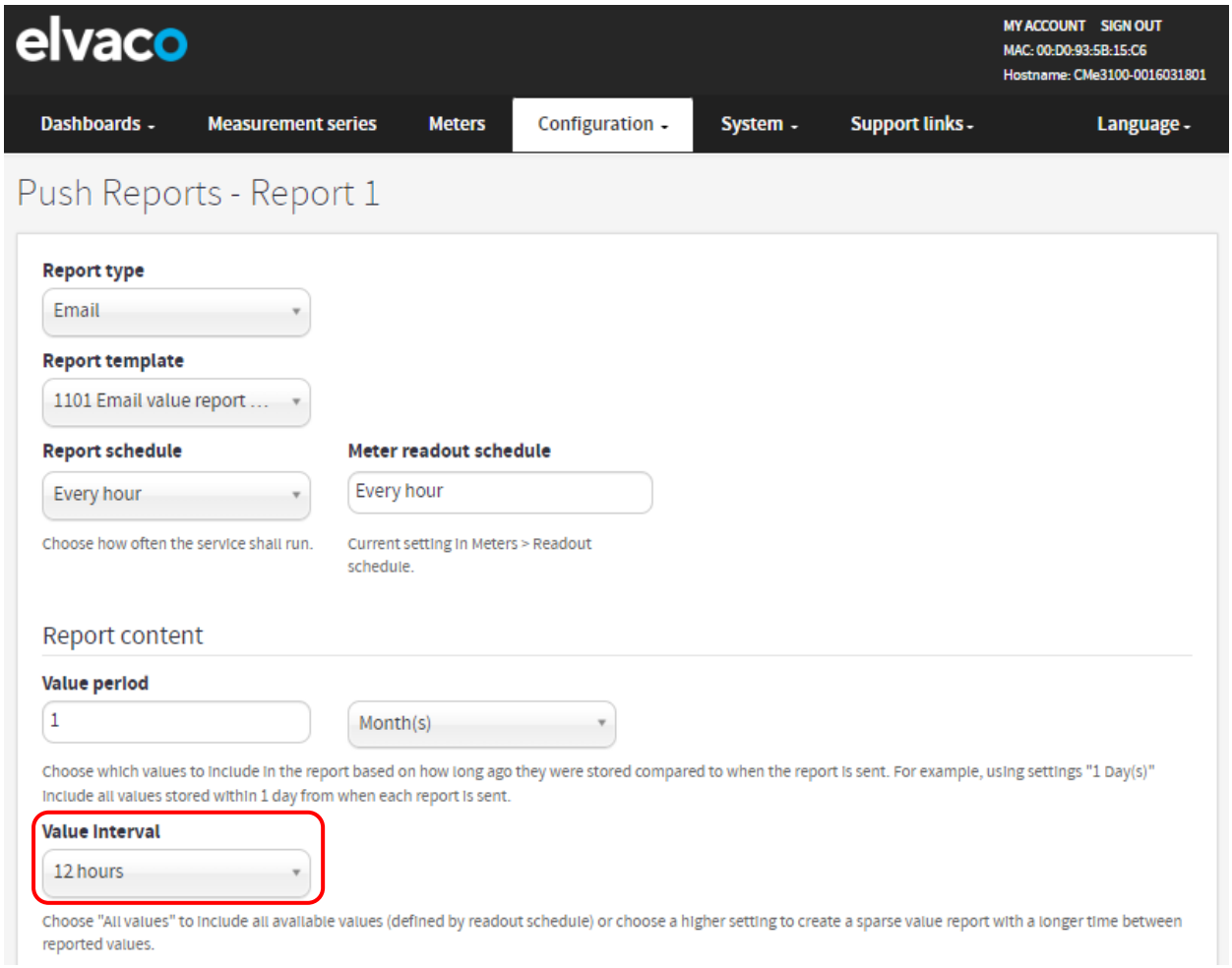
- Go to **Configuration > Push Reports**. Select a Push Report by clicking on it.
- By setting the Value Period to “Auto” the Metering Gateway will calculate the Value Period based on how far back in time it is able to find unsent meter values. By setting the Value Period to a specific value, meter values exactly that long back in time will be included in the Push Report, regardless of if there are older unsent meter values.
- Click **Save**.



6.32.3 Configure the Value Interval

To configure the Value Interval:

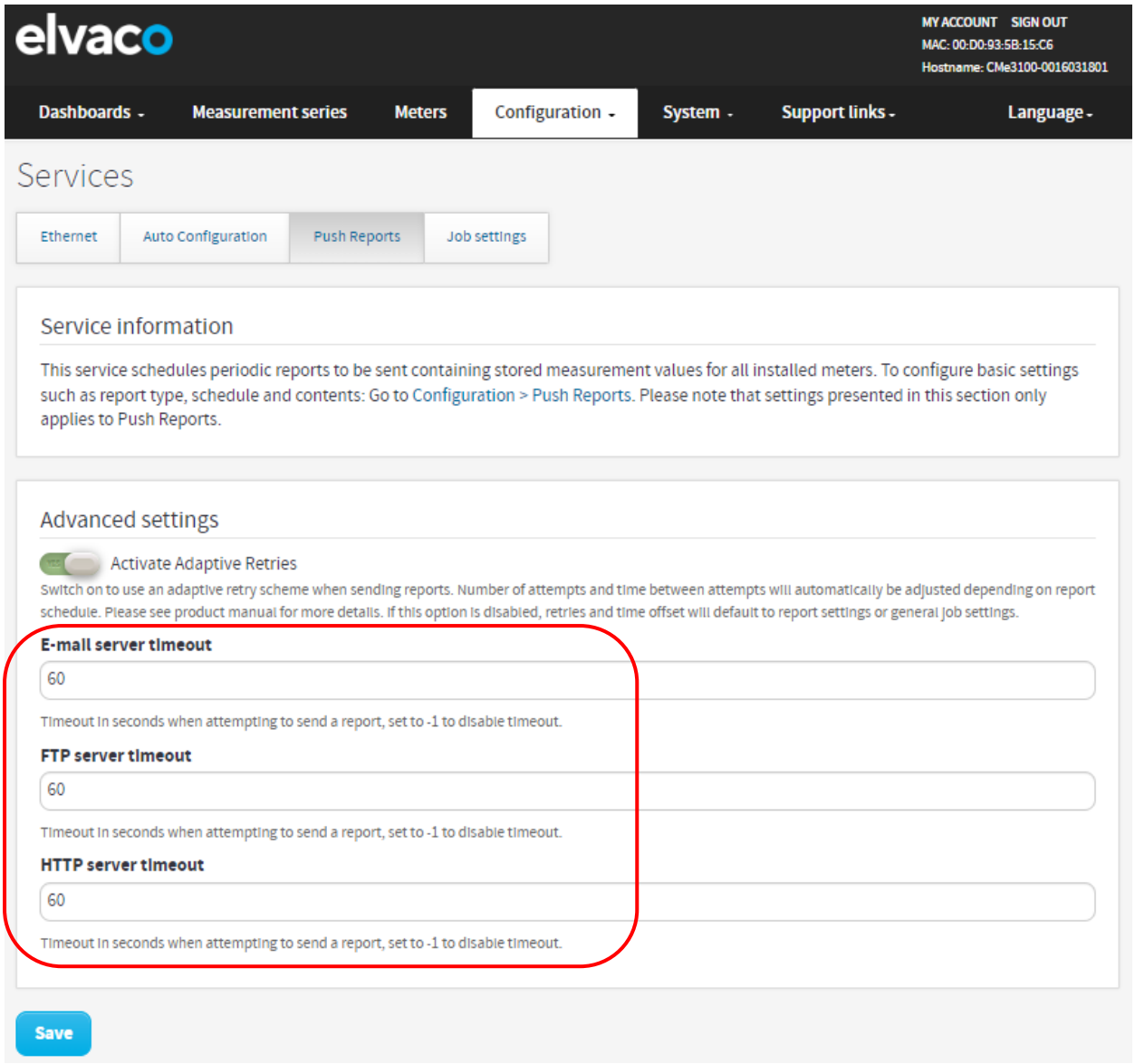
- Go to **Configuration > Push Reports**. Select a Push Report by clicking on it.
- Set the Value Interval to determine the time between each meter readout included in the Push Report. Setting the Value Interval to “All values” will automatically ensure that all meter values read by the Metering Gateway are included in the Push Reports.
- Click **Save**.



6.32.4 Configure the Push Report timeout settings

To configure the Push Report timeout settings:

- Go to **Configuration > Services > Push Reports.**
- Set the desired Timeout for each protocol. Setting it to “-1” will disable the timeout functionality of the Metering Gateway, and instead let the server determine when a connection should be closed. The default settings will work well in most cases. However, if the connection between the Metering Gateway and the server is slow, the timeout value might have to be increased accordingly.
- Click **Save**.



6.33 Configure Job retries

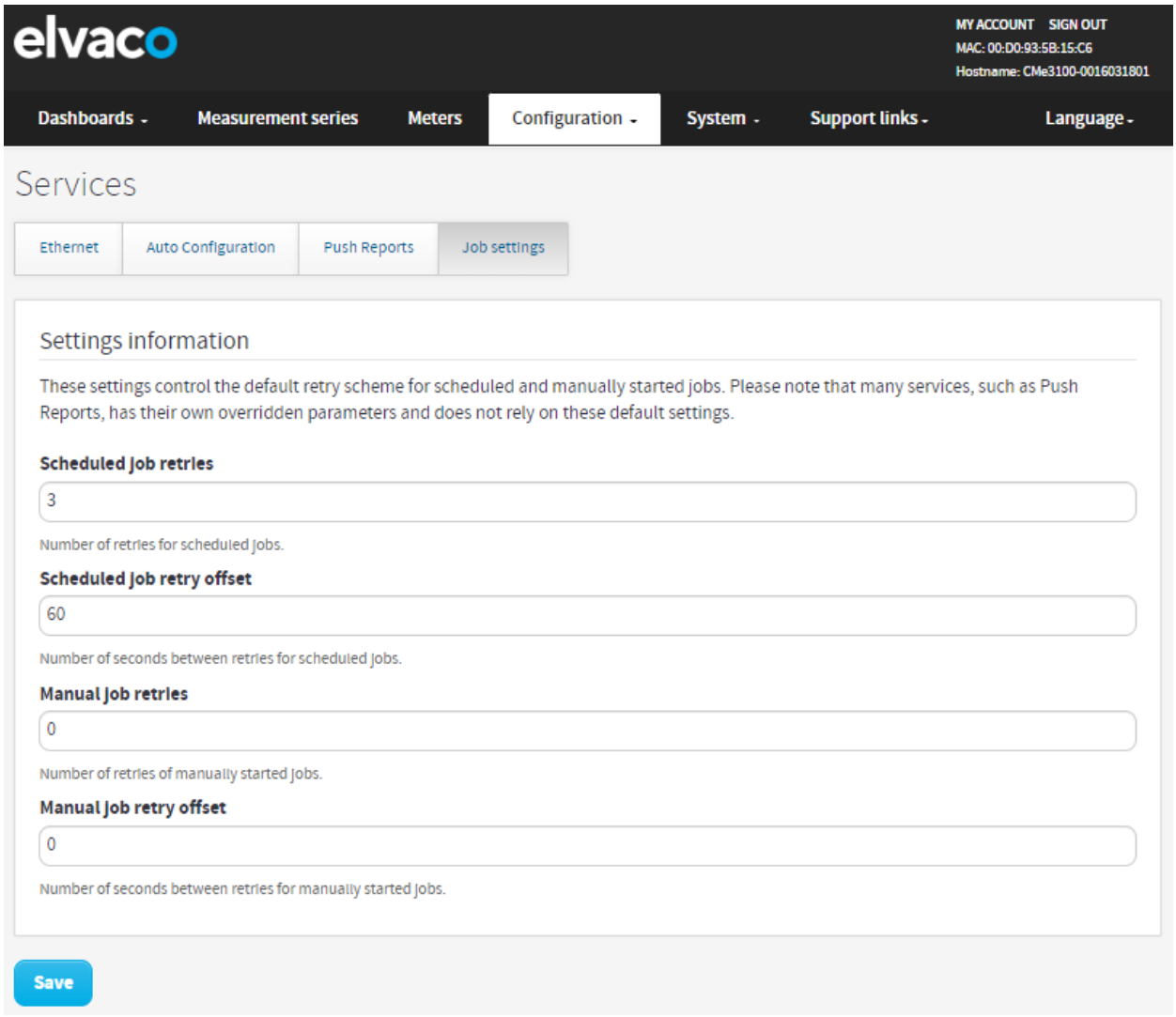
Purpose

The job retries settings determine how the Metering Gateway will perform retry attempts for scheduled and manual jobs, for example meter readouts, if failing the first time. If Adaptive Retries have been disabled for Push Reports, and no other retry settings have been configured for the Metering Gateway, these retry settings will also affect the Push Report retry settings.

6.33.1 Configure retry settings for scheduled and manual jobs

To configure retry settings for scheduled and manual jobs:

- Go to **Configuration > Services > Job settings**.
- Set the desired number of retries to determine the maximum number of times the Metering Gateway will attempt to perform a job.
- Set the Retry offset to determine the time between the Metering Gateway will wait between each attempt for these jobs.
- Click **Save**.



6.34 Access the device through a console application

Purpose

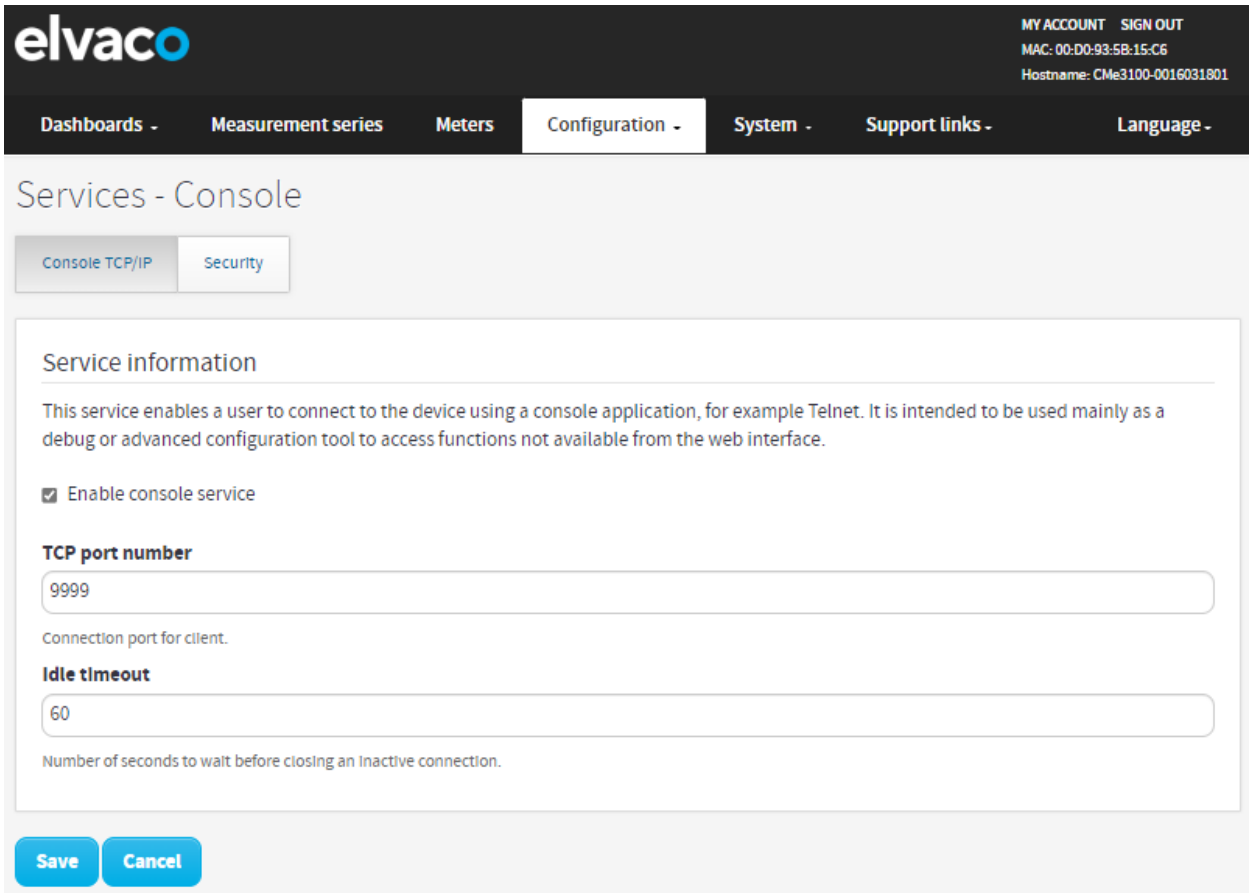
The Metering Gateway can be accessed through a console application, i.e., by using a command-line interface. This is most often used for troubleshooting and advanced operations. To increase the security of the console application, the Metering Gateway supports the usage of passwords to access various levels of device functions. It is also possible to create a list of specific IP addresses which are allowed to access the Metering Gateway through the console application.

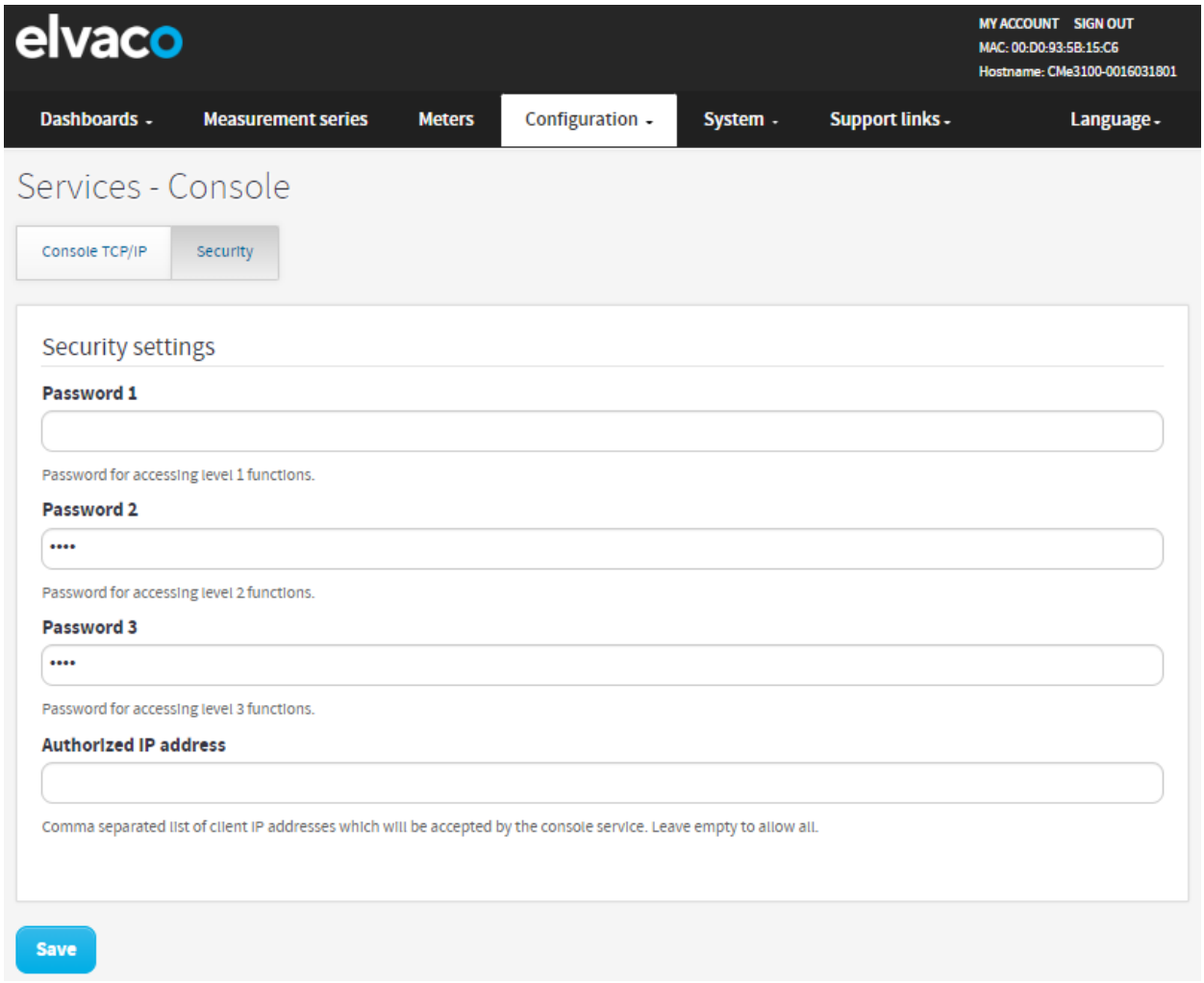
6.34.1 Enable and configure the console application

To enable and configure the console application:

- Go to **Configuration > Services**.
- The console application is easily enabled or disabled in this menu. Click on it to enter the settings.
- Set the TCP port where the console application will connect
- Set the Idle timeout to determine the number of seconds of inactivity that needs to pass before a connection with a console application is closed.

- Go to **Security**. Add a password for accessing various levels of device functions and a list of authorized IP addresses which will be able to use the console application.
- Click **Save**.





6.35 Use On Demand Reports

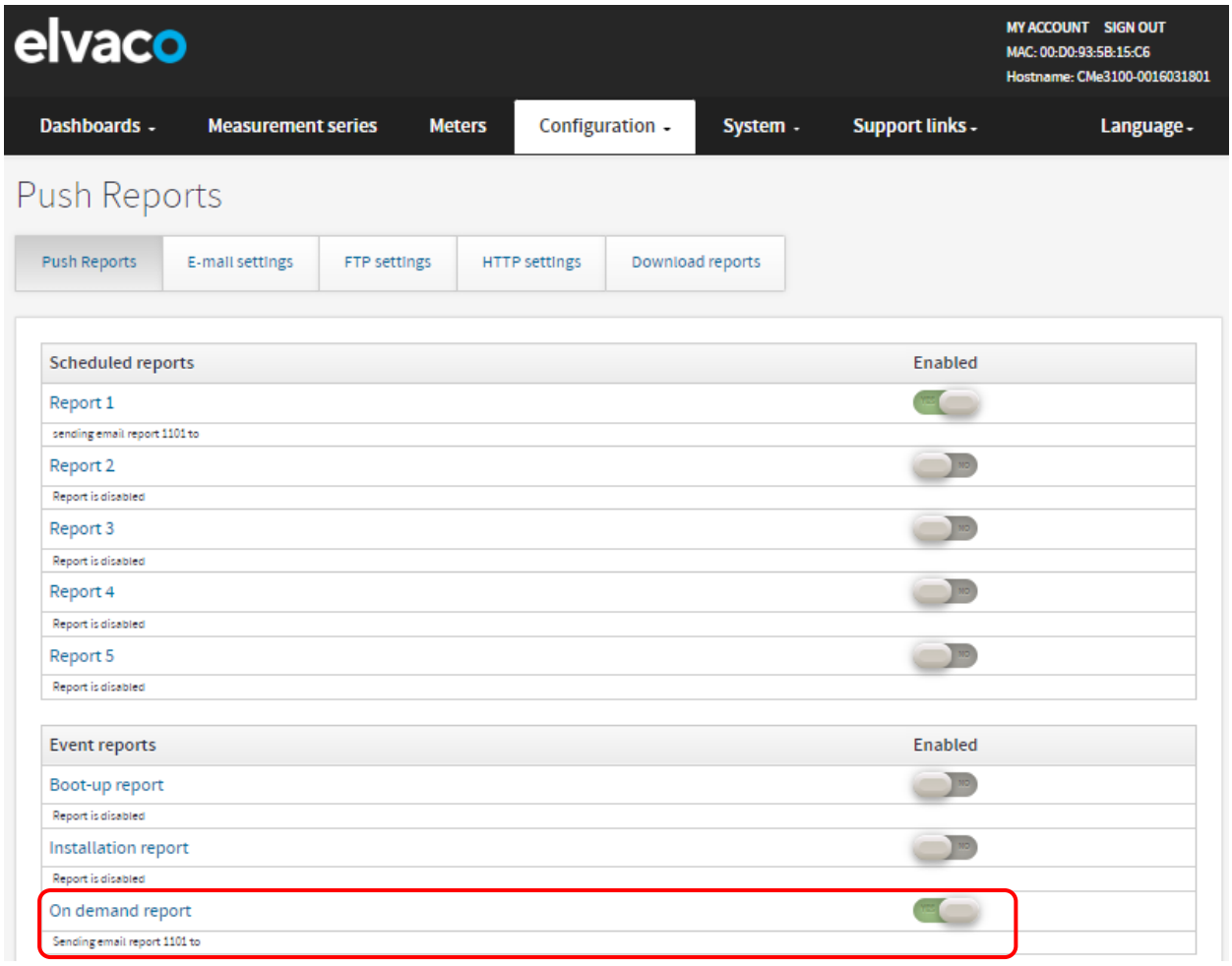
Purpose

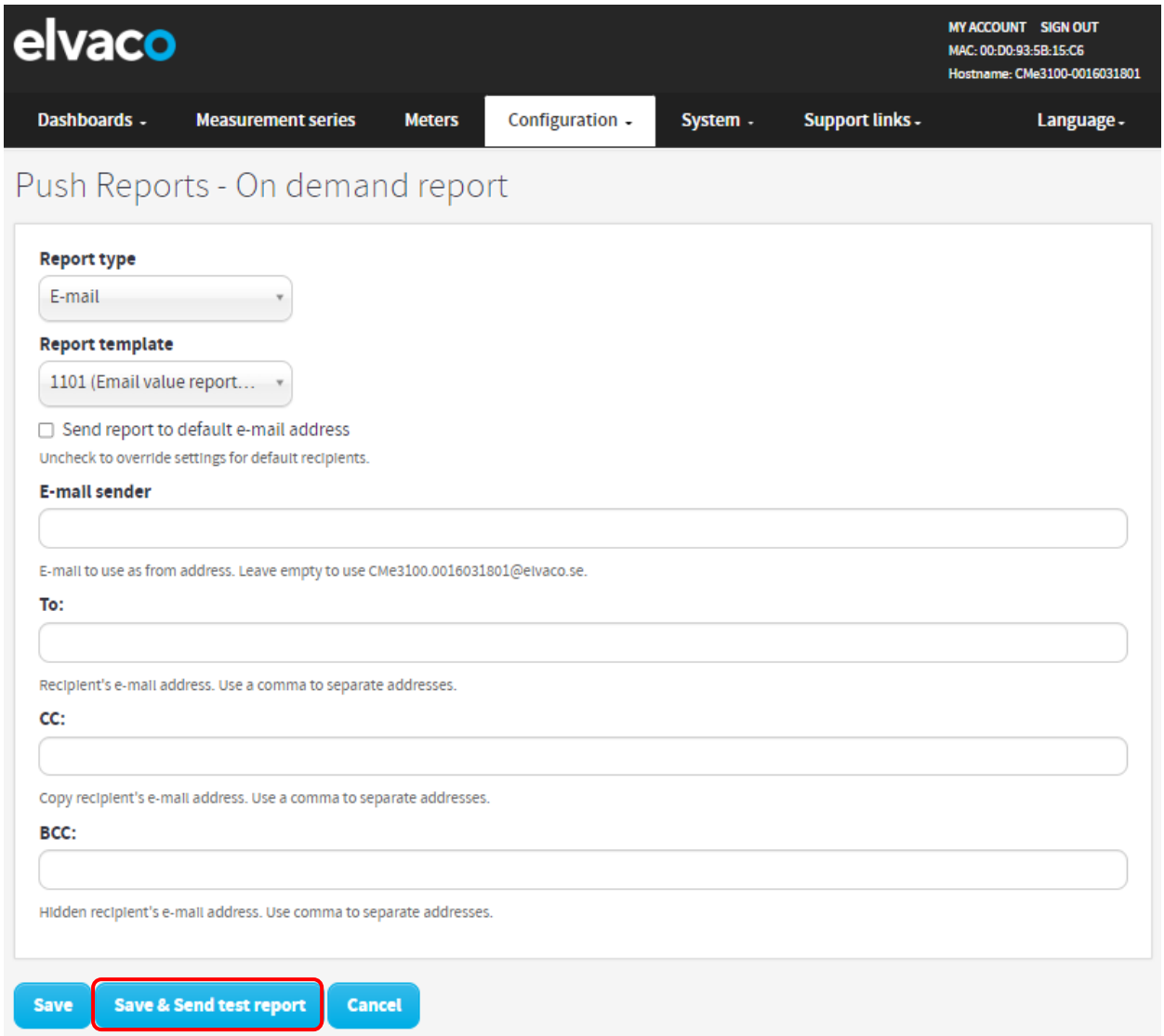
The On Demand Report is a way of triggering a report manually, without having to set a schedule. It differs from other types of reports in the sense that an actual meter readout is performed each time the On Demand Report is requested. In contrast, all other types of Push Reports include meter values that has already been stored in the database of the Metering Gateway.

6.35.1 Enable and configure the On Demand Report

To enable and configure the On Demand Report:

- Go to **Configuration > Push Reports > On demand report**. Enable the On Demand Report and click on it to enter the settings.
- Set the protocol to receive the report by and a report template. To learn more about the report templates available, please visit our support site https://support.elvaco.com.
- Add recipients of the On Demand Report.
- Click **Save** (or **Save & Send test report** to test the settings).


elvaco
MY ACCOUNT SIGN OUT
MAC: 00:D0:93:5B:15:C6
Hostname: CMe3100-0016031801
Dashboards
Measurement series
Meters
Configuration
System
Support links
Language
Push Reports
Push Reports
E-mail settings
FTP settings
HTTP settings
Download reports
Scheduled reports
Enabled
Report 1
sending email report 1101 to
Report 2
Report is disabled
Report 3
Report is disabled
Report 4
Report is disabled
Report 5
Report is disabled
Event reports
Enabled
Boot-up report
Report is disabled
Installation report
Report is disabled
On demand report
Sending email report 1101 to



6.36 Configure identity settings

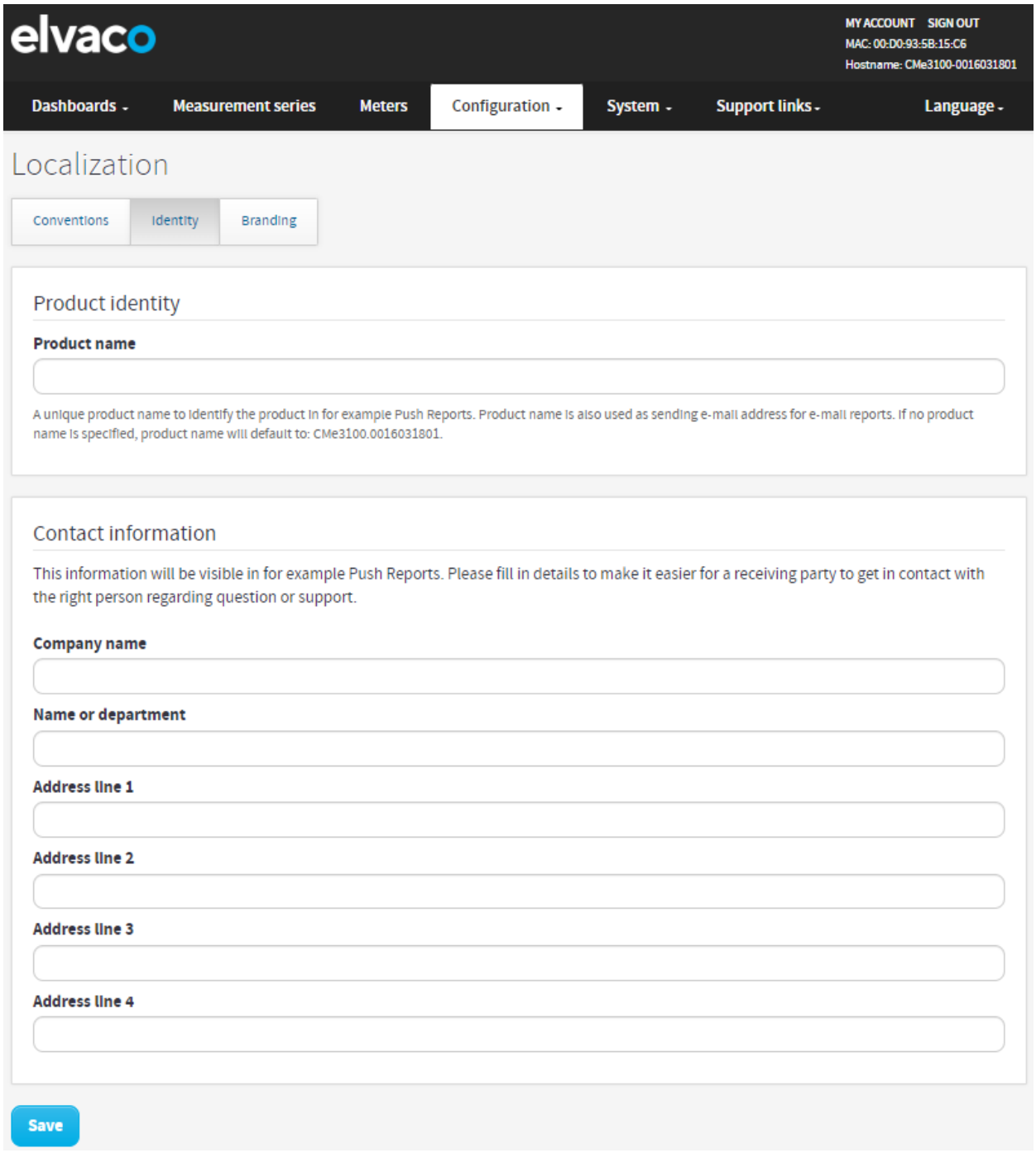
Purpose

Configuring device identity settings includes assigning an identity for the Metering Gateway, which will be displayed as the sender of Push Reports, as well as contact information to be included in the Push Reports.

6.36.1 Customize the Push Report identity settings

To customize the Push Report identity settings:

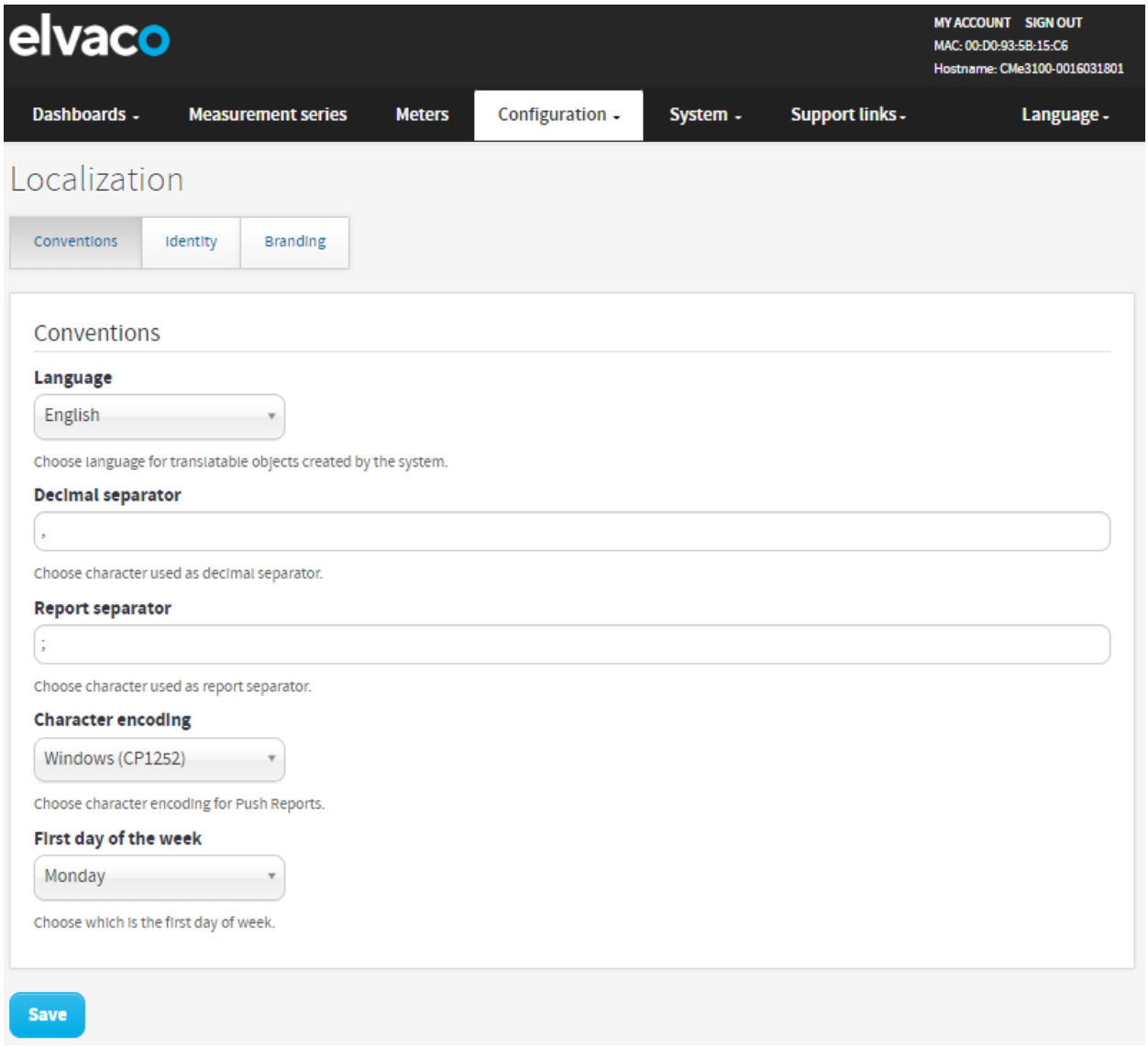
- Go to **Configuration > Localization > Identity**.
- Assign a product identity for the Metering Gateway by assigning it a name. Also add contact information to be included in the Push Reports, if desired.
- Click **Save.**



6.36.2 Configure localization settings for Push Reports

To configure localization settings for Push Reports:

- Go to **Configuration > Localization > Conventions**.
- Set Desired language, Decimal separator, Report separator, and First day of the week. The Character encoding should be set with respect to the operational system used to make sure that all characters of the Push Reports will be encoded correctly.
- Click **Save**.



6.37 Perform a reboot of the device

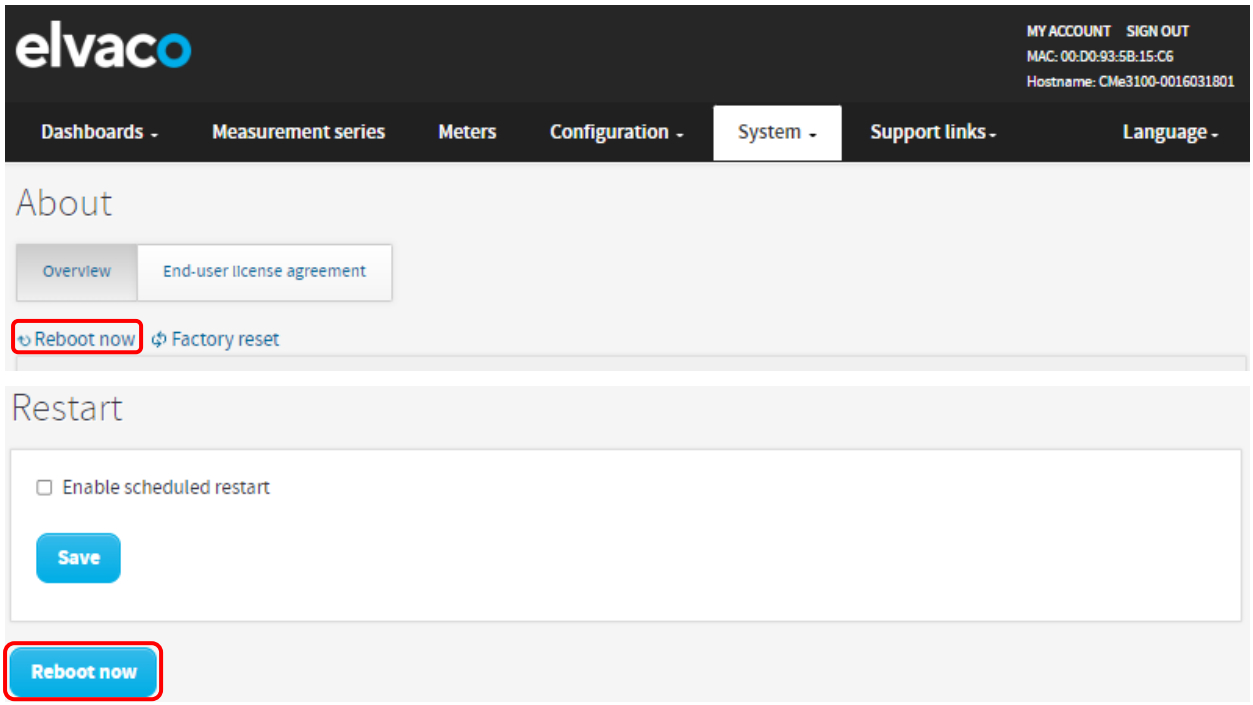
Purpose

In rare cases, e.g., in case of troubleshooting, it might be desired to perform a reboot of the Metering Gateway. This can be done directly through the web interface.

6.37.1 Reboot the device

To perform a reboot of the device:

- Go to **System > About** or **System > Restart**
- Click **Reboot now**



6.38 Reset the device to factory default settings

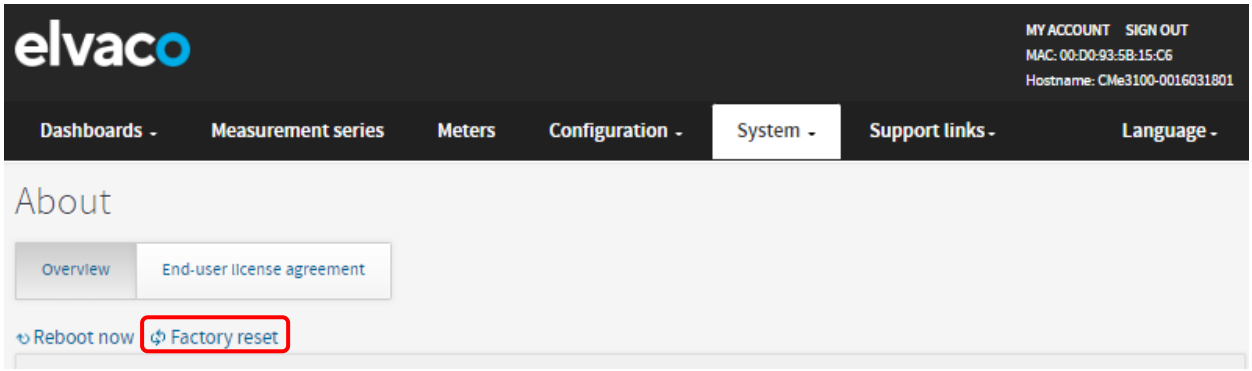
Purpose

By performing a factory reset of the Metering Gateway, all settings will be reset to default and the meter value database and logs will be cleared.

6.38.1 Perform a factory reset

To perform a factory reset:

- Go to **System > About**.
- Click **Factory reset**.



6.39 Customize service and job schedules

6.39.1 Specify schedules using cron patterns

For scheduled jobs, e.g., meter readouts and Push Reports, cron patterns can be used to customize the time interval by which the jobs will be performed. It is done by setting up to five different time variables, each one represented by a star. Replace each star with a number to set a specific job execution schedule.

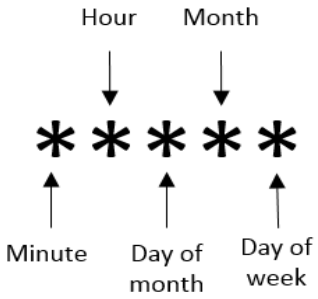


Figure 9: Illustration of cron pattern

The “/” character is used to set periodic values, i.e., schedule a job with a recurrent time interval. The “?” character is used to generate a random value. Lastly, using the “|” character allows to combine several cron patterns. An example table including a list of chosen cron patterns is presented in Table 10.

Cron pattern	Description
15 * * * *	Schedule a job 15 minutes past every hour, i.e., 00:15, 01:15, 02:15 etc.
*/15 * * * *	Schedule a job every 15th minute, i.e., 00:00, 00:15, 00:30, etc.
* * * * *	Schedule a job every minute, i.e., 00:01, 00:02, 00:03, etc.
* 12 * * mon	Schedule a job every minute during the 12th hour of every Monday.
* 12 16 * mon	Schedule a job every minute during the 12th hour of every Monday if the day is the 16th of the month.
59 11 * * 1,2,3,4,5	Schedule a job 11:59 on Monday, Tuesday, Wednesday, Thursday, and Friday.
59 11 * * 1-5	Schedule a job 11:59 on Monday, Tuesday, Wednesday, Thursday, and Friday.
*/15 9-17 * * *	Schedule a job every 15th minute between the 9th and the 17th hour of the day, i.e., 09:00, 09:15, 09:30, etc.
* 12 10-16/2 * *	Schedule a job every minute during the 12th hour of the day, if the day is the 10th, the 12th, the 14th, or the 16th of the month.
* 12 1-15,17,20-25 * *	Schedule a job every minute during the 12th hour of the day, if the day is between the 1st and the 15th, the 17th or between the 20th and 25th day of the month.

0 5 * * *|8 10 * * *|22 17 * * *	Schedule a job every day at 05:00, 10:08 and 17:22.
?1-30 0 * * *	Schedule a job at a random chosen minute during the first 30 minutes of every hour.

Table 10: Examples of different cron patterns

7 Technical specifications

7.1 Characteristics

Type	Value	Unit	Comments
Mechanics			
Casing material	Polyamide	-	
Protection class	IP20	-	
Dimensions (w x h x d)	70 x 90 x 64	mm	4 DIN modules
Weight	190	g	
Mounting	DIN rail	-	Mounted on DIN rail (DIN 50022) 35 mm
Electrical connections			
Supply voltage	Screw terminal	-	Cable 0.25-1.5 mm^2, 0.5Nm tightening torque
M-Bus master port	Pin terminal	-	Solid Wire 0.6-0.8 Ø mm
M-Bus slave port 1	Screw terminal	-	Cable 0.25-1.5 mm^2
M-bus slave port 2	Screw terminal	-	Cable 0.25-1.5 mm^2
USB master port	Type A	-	
USB slave port	Type mini B	-	
Network	RJ45	-	Ethernet
Electrical characteristics			
Nominal voltage	100-240	VAC	+/- 10%
Frequency	50/60	Hz	
Power consumption (Max)	<15	W	
Power consumption (Nom)	<5	W	
Installation/overvoltage	CAT 3	-	
Environmental specifications			
Operating temperature	-25 to +55	ºC	
Operating humidity max.	5 to 90	%	Non-condensing
Operating altitude	0-2000	m	
Pollution degree	Degree 2	-	
Usage environment	Indoors	-	Can be extended with IP67 enclosure for outdoor use
Storage temperature	-40 to +85	ºC	

User interface			
Green LED	Power	-	
Red LED	Error	-	
Yellow LED	Status Ethernet	-	
Blue LED	USB active	-	
Push button	Factory reset	-	
Configuration	Web interface (HTTP), Auto configuration (URL), Telnet, REST/JSON	-	
M-Bus			
Interfaces	IR, integrated M-Bus Master, M-Bus slave	-	
Maximum number of M-Bus devices (software limit)	Software licences for 8, 32, 64, 128, 256 or 512 devices	-	
Transparent M-Bus	TCP/IP and M-Bus 2-wire slave interface	-	Software limit does not apply to Transparent M-Bus mode
Virtual M-Bus	TCP/IP and M-Bus 2-wire slave interface	-	
Decryption	Yes	-	
Integrated M-Bus Master			
M-Bus standard	EN 13757	-	Full M-Bus decoder implemented
M-Bus baud rate	300 and 2400	bit/s	
Nominal voltage	28	VDC	
Maximum unit loads	32/48	T/mA	Can be extended with CMeX10-13S Series
M-Bus search modes	Primary, secondary, enhanced secondary	-	
Maximum cable length	1000	m	100 nF/km, maximum 90 Ω
M-Bus slave interface			
M-Bus standard	EN 13757	-	
M-Bus baud rate	300 and 2400	bit/s	
Nominal voltage	21-42	VDC	
Addressing mode	Primary, secondary	-	
General			
Real time clock backup	24	h	
Real time clock accuracy	<2	s/day	

Script engine	Intelligent engine for active content generation	-	
Software/firmware update	Web interface	-	
Measurement reports	HTTP, FTP, SMTP (e-mail)	-	
Additions	Modbus, REST, JSON-RPC, DLMS	-	
Continuous Readout Mode	Modbus, REST	-	
Data storage (examples)			
15-minute values	Meters / Years 1 / 15 32 / 4 128 / 1 256 / 0.5 512 / 0.25	-	
Hourly values	Meters / Years 1 / >15 32 / >15 128 / 4 256 / 2 512 / 0.5	-	
Fixed network (Ethernet)			
Speed and duplex	10/100	MBit	Half/Full duplex

Table 11: Technical specification

8 Type approvals

CMe3100 is designed to comply with the directives and standards listed below.

Approval	Description
EMC	EN 61000-6-2, EN 61000-6-3, FCC 47 CFR
Safety	EN 62368-1 2018, UL 62368-1:2014 Ed.2], CSA C22.2#62368-1:2014 Ed.2]

Table 12: Type approvals

9 Document History

9.1 Versions

Version	Date	Description	Author
1.0	2016-11	Initial version	Anton Larsson
1.1	2017-03	Added information about new feature “SNMP”	Anton Larsson
1.2	2017-12	Added information about new security feature “FTPS”	Anton Larsson
1.3	2018-02	Added links to new website	Anton Larsson
1.4	2023-01	General updates of text and image to match current gui	Peter Janson & Niclas Andersson
1.5	2023-05	Added information about built in database 4.2	Niclas Andersson

Table 13: Document version

9.2 Document software and hardware appliance

Type	Version	Date	Comments
Hardware	Rev-1D	2022-06	CMe3100 G2
Software	1.9.10	2023-05	

Table 14: Document software and hardware appliance

10 References

10.1 Terms and abbreviations

Abbreviation	Description
CA	Certificate Authority
CSV	Comma-Separated Values
DCS	Digital Control System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
MAC	Media Access Control
MOID	Measurement Object Identification
NTP	Network Time Protocol
PLC	Programmable Logic Controller
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
URI	Uniform Resource Identifier

Table 15: Terms and abbreviations