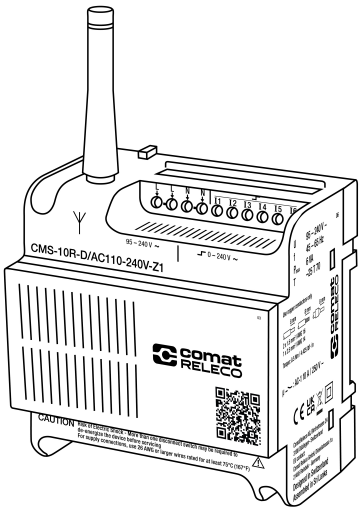
User Manual

CMS-10R



This user manual provides the information required to install, operate, and maintain the product safely and correctly. It includes general instructions, safety information, operating procedures, maintenance guidelines, and technical references.

Important Information

ComatReleco reserves the right to modify, correct, and improve the technical documentation and the products described therein at its own discretion and without prior notice, insofar as this is reasonable for the user. The same applies to technical changes made in the interest of technical progress.

The receipt of technical documentation, in particular user documentation, does not create any further obligation on the part of ComatReleco to provide information about possible changes to products and/or technical documentation. You are responsible for verifying the suitability of the products for their intended use in your specific application, particularly with regard to compliance with the applicable standards and regulations. All information provided in the **Technical data** is supplied without any express, implied, or tacit warranty.

Exclusively the provisions of the current Terms and Conditions of ComatReleco apply, in particular with regard to warranty and the privacy policy.

This user manual contains important information for the commissioning, operation, maintenance, and disposal of the device. It also provides safety-related information and practical guidance for resolving issues. The user manual must be made available with the equipment, either in physical or electronic form, and must be included whenever the equipment is transferred. It is also available on the ComatReleco web portal.

Copyright

This manual, including all illustrations contained herein, is protected by copyright. Any modification of the content or publication of excerpts from this document is prohibited. ComatReleco reserves the right to register its own intellectual property rights for the product identifications of ComatReleco products used in this document. Registration of such intellectual property rights by third parties is prohibited. Other product identifications may also be legally protected, even if they are not specifically indicated as such.

Disclaimer

The information in this document is provided for guidance only. The manufacturer reserves the right to modify the product, documentation, or specifications without prior notice. The manufacturer shall not be liable for damages resulting from incorrect installation, misuse, or failure to follow the instructions in this manual.

Contents

1 About this manual **7**

1.1 Device types covered . . . 7
1.2 Find the information you need . . . 7
1.3 Product conformity . . . 8
1.4 Documents and support . . . 8
1.5 Contact details . . . 8

2 Safety instructions **9**

2.1 Safety symbols and notices . . . 9
2.2 General safety instructions . . . 9
2.3 Who may install and use the device . . . 10
2.4 Intended use . . . 11
2.5 Applications the device is not intended for . . . 11
2.6 Prevent configuration errors . . . 11
2.7 Information security . . . 11

3 Understand your CMS-10R **13**

3.1 Overview . . . 13
3.2 Identify your device variant . . . 13
3.3 Main operating functions . . . 14
3.4 Locate terminals, controls, and status indicators . . . 14
3.5 Check the delivery . . . 18
3.6 Transport, storage, and returns . . . 18
3.7 Check mobile network compatibility and coverage . . . 18
3.7.1 Network coverage . . . 18
3.7.2 Country versions . . . 18
3.7.3 Frequency bands by modem variant . . . 18
3.8 What happens during interruptions, resets, and updates . . . 19

4 Install and connect the device **22**

4.1 Before installation . . . 22
4.2 Mounting . . . 22
4.2.1 Mounting the device . . . 22
4.2.2 Dismantling the device . . . 23
4.3 Connect the power supply, inputs, and outputs . . . 23

4.3.1 Power supply . . . 23
4.3.2 Wiring of the CMS-10R-D inputs . . . 23
4.3.3 Wiring the CMS-10R-DA inputs . . . 24
4.3.4 Wiring the CMS-10R-DAC inputs . . . 24
4.3.5 Wiring the CMS-10R-D / -DA / -DAC relay outputs . . . 25
4.4 Antennas and antenna cables . . . 25
4.4.1 Antenna . . . 25
4.4.2 Antenna extension cables . . . 26

5 Commission the device in the IoT Portal 27
5.1 Access the IoT Portal and plan commissioning . . . 27
5.1.1 Commissioning sequence . . . 27
5.1.2 Log in, create an account or reset your password . . . 28
5.2 Add a device to your account . . . 29
5.2.1 Add a device as the installer . . . 29
5.2.2 Add a device as the owner . . . 31
5.2.3 Add a device using an invitation code . . . 33
5.3 Pair your device . . . 34
5.3.1 Pair directly after adding the device . . . 34
5.4 Select a service profile and SMS packages . . . 35

6 Configure and monitor your device 36
6.1 Find devices and check their status . . . 36
6.2 Configure and operate a device . . . 37
6.2.1 Check device status: Overview . . . 37
6.2.2 Manage device settings and ownership: Manage . . . 39
6.2.3 Give users and machines access: Users / machines . . . 41
6.2.4 Configure input monitoring: Inputs . . . 45
6.2.5 Configure and control relay outputs: Outputs . . . 52
6.2.6 Configure notifications and acknowledgement: Events . . . 54
6.2.7 Review and export activity: Event Log . . . 60
6.2.8 Manage the service profile: Service profile . . . 63
6.2.9 Allow a support session: Support . . . 65
6.3 Update the device firmware . . . 65

7 Manage your account and payments 67
7.1 Notification usage and allowances . . . 67
7.1.1 Usage by notification method . . . 67
7.1.2 Included SMS credit and additional packages . . . 67

7.1.3 SMS length and character encoding . . . 68
7.1.4 When SMS credit runs out . . . 68
7.1.5 When the event allowance runs out . . . 68
7.2 Manage your account and SMS credit . . . 69
7.2.1 Menu: Profile . . . 69
7.2.2 Menu: Password . . . 70
7.2.3 Menu: SMS package . . . 70
7.2.4 Set up two-factor authentication (2FA) . . . 71
7.2.5 Log out . . . 72
7.3 Manage payments, billing groups and account inactivity . . . 72
7.3.1 Set your payment preferences . . . 73
7.3.2 Create invoice groups . . . 73
7.3.3 Assign an invoice group to a service profile renewal . . . 74
7.3.4 Review the shopping cart and pay . . . 74
7.3.5 Set automatic log out for the browser . . . 75

8 Mobile operation and SMS status **76**
8.1 Choose how to access the device . . . 76
8.2 Use the app . . . 76
8.2.1 Install the app and sign in . . . 77
8.2.2 Find your device and check its status . . . 77
8.2.3 Change account settings or add a device . . . 78
8.2.4 Open the detailed view and switch outputs . . . 78
8.3 Request input and output status by SMS . . . 79

9 Monitor data and connect external systems **81**
9.1 Monitor device data in the Dashboard . . . 81
9.1.1 Refresh the view or export data . . . 82
9.1.2 Read input and output information . . . 82
9.1.3 Display the device location on the map . . . 82
9.1.4 Locate a device by triangulation . . . 82
9.2 Configure event actions to trigger outputs . . . 83
9.2.1 Add or change an event action . . . 83
9.2.2 Switch a local output when an event occurs . . . 84
9.2.3 Switch a remote output when an event occurs . . . 85
9.2.4 Review event action history . . . 86
9.3 Configure webhook integration . . . 87
9.3.1 Register a webhook integration in the Integration center . . . 87
9.3.2 Assign the integration to a device . . . 88

9.3.3 Configure the webhook request . . . 90
9.4 Access the device through the Public REST API . . . 91
9.4.1 Obtain the Account SID and API Key . . . 91
9.4.2 Create an API Key and select its permissions . . . 92
9.4.3 Copy the Device SID . . . 92
9.4.4 Send a Set output ON request . . . 93
9.4.5 Send a Set output OFF request . . . 93
9.4.6 Send a Get device status request . . . 93
9.4.7 Review API-triggered output changes . . . 93

10 Troubleshooting, maintenance and replacement 95
10.1 Troubleshooting . . . 95
10.1.1 RUN LED does not flash . . . 95
10.1.2 Device is offline in the IoT Portal . . . 96
10.1.3 Mobile network connection is poor . . . 96
10.1.4 Links in e-mails do not work . . . 96
10.1.5 Input or output states in the IoT Portal are incorrect . . . 96
10.1.6 No notifications are received . . . 97
10.1.7 The event allowance is exhausted . . . 97
10.1.8 No e-mails are received . . . 98
10.1.9 Cannot log in . . . 98
10.1.10 Cannot log in with two-factor authentication (2FA) . . . 98
10.1.11 No SMS messages or voice calls are received . . . 99
10.1.12 No push notifications are received on the smartphone . . . 99
10.1.13 Call-in does not work . . . 99
10.1.14 No push notifications are received on the PC . . . 100
10.2 Maintenance . . . 100
10.3 Replace or return a defective device . . . 100
10.4 Replace a CMS-10x predecessor with a CMS-10R . . . 100

11 Disposal 102
11.1 For private households . . . 102
11.2 For professional users in the European Union . . . 102
11.3 For disposal in countries outside the European Union . . . 102
11.4 Packaging material . . . 102

12 Technical data 103
12.1 Data sheets for your device type . . . 103

A Glossary 104

Chapter 1

About this manual

1.1 Device types covered

This user manual applies to the CMS-10R device types listed below. Use the type designation on your device to identify the relevant instructions and specifications.

Type designation	Characteristics
CMS-10R-D/AC110-240V	• ComatReleco 4G/3G/2G IoT Messaging System • 6 × digital inputs, 95–240 V ~
CMS-10R-DA/DC12-48V	• ComatReleco 4G/3G/2G IoT Messaging System • 6 × switchable inputs: digital 10–48 V ⎓ / analogue 0–10 V ⎓
CMS-10R-DAC/DC12-48V	• ComatReleco 4G/3G/2G IoT Messaging System • 4 × switchable inputs: digital 10–48 V ⎓ / analogue 0–10 V ⎓ • 2 × analogue inputs: 4–20 mA ⎓

Service profiles and subscription

The CMS-10R operates on a subscription basis, with annual charges depending on the selected service profile. The profile determines the available features and usage limits. For current service profile and SMS package prices, included allowances and regional conditions, consult the applicable page:

- CMS-10R service profiles – Switzerland.
- CMS-10R service profiles – Worldwide.

1.2 Find the information you need

Use the following task guide to find instructions for your stage of use. Read the safety instructions before installing or operating the device.

- **Understand the product and identify its controls:** Chapter 3, Understand your CMS-10R.
- **Check safety requirements and user qualifications:** Chapter 2, Safety instructions.
- **Mount, wire, and connect an antenna:** Chapter 4, Install and connect the device.
- **Set up an account and commission the device:** Chapter 5, Commission the device in the IoT Portal.
- **Configure inputs, outputs and notifications; review events:** Chapter 6, Configure and monitor your device.
- **Manage your account, SMS credit and payments:** Chapter 7, Manage your account and payments.
- **Use the mobile app or query status by SMS:** Chapter 8.
- **Use dashboards, webhooks or the REST API:** Chapter 9.
- **Understand what happens during an interruption, reset, or update:** Section 3.8, What happens during interruptions, resets, and updates.
- **Resolve a problem or replace a device:** Chapter 10, Troubleshooting, maintenance and replacement.
- **Check specifications:** Chapter 12, Technical data.
- **Look up a term or abbreviation:** Glossary, page 104.

1.3 Product conformity

Find the **EC Declaration of Conformity** on the ComatReleco web portal under **User manuals**, in the document CMS-10R Safety instructions.

1.4 Documents and support

Use the ComatReleco web portal to obtain **CMS-10R documents**, including short instructions, drawings, **Technical data**, and general terms and conditions.

The **CMS-10R Support Centre** provides **video tutorials** and an **FAQ** (Frequently Asked Questions).

For further information, contact ComatReleco support. See Section 1.5, Contact details.

1.5 Contact details

Switzerland

ComatReleco AG
Birchstrasse 24
3186 Düdingen
Switzerland

Phone +41 31 838 55 77
E-mail support@comatreleco.com
Web www.comatreleco.com

Chapter 2

Safety instructions

2.1 Safety symbols and notices

Symbol	Meaning
	**Danger:** Indicates a hazard with high risk potential. Failure to observe the safety measures may result in serious injury or death.
	**Warning:** Indicates a hazard with medium risk potential. Failure to observe the safety measures may result in serious injury or property damage.
	**Information:** Provides additional information and helpful notes.
	**Disposal:** Observe the specific disposal regulations for electronic devices.
	The **Class 2 protective insulation** symbol is printed on the device. The device is protected against accidental contact with live electrical parts by Class 2 protective insulation. With this electrical protection class, no protective conductor (earthing) must be connected.

2.2 General safety instructions



DANGER

- Only mount or dismantle the device when it is disconnected from the power supply. This applies to the power supply and to all inputs and outputs.
- During operation, the electrical connection points of the device carry hazardous voltages. Do not touch these connection points.
- The device must be installed only by qualified electricians.
- Install and operate the device in accordance with the applicable national regulations and specifications.
- This device is not suitable for use in wet areas, explosive atmospheres — for example, areas where the air contains high concentrations of flammable chemicals, vapours, or particles such as grain, dust, or metal powder — or near medical devices.
- **Risk of electric shock:** More than one disconnect switch may be required to de-energise the device before servicing.

WARNING

- Do not apply a voltage greater than **240 V**~ to the **CMS-10R-D**, or greater than **48 V**⎓ to the **CMS-10R-DA** and **CMS-10R-DAC**.
- The device must be disconnectable from the **Power supply** by means of a suitable installation-side disconnecting device, such as a fuse or circuit breaker. The disconnecting device must be located as close to the device as possible.
- When connecting the device to the **240 V**~ mains, ensure that the **Power supply** and the input supply are connected to the same outer conductor.
- Before commissioning, check that all cables are connected correctly.
- The device is intended for installation in an enclosure, such as a control cabinet, distribution box, or terminal box. The enclosure must also provide protection against electric shock (touch protection). The device must not be operated before installation is complete.
- During operation, keep a minimum safety distance of **20 cm** between the antenna and any person.

Important operating restrictions

- Read the user manual carefully before using the device.
- Ensure that the product documentation applicable to this device remains available throughout the device's entire life cycle. See also Section 1.1, Device types covered.
- This device is not suitable for monitoring sensitive systems or time-critical processes. Failures in the mobile phone network, poor reception, or interruptions in the power supply may impair its functions.
- Operate the device only with the specified antenna types. See also Chapter 4, Install and connect the device.
- This equipment is not suitable for use in locations where children are likely to be present.

Restrictions on use

Frequency band	Maximum power
GSM 900	Power Class 4
GSM 1800	Power Class 1
3G, all bands	Power Class 3
LTE Bands 1, 3, 7, 8, 20, 28, 38, and 40	Power Class 3

The EU and UK Declarations of Conformity are available on the ComatReleco Downloads page for Declarations of Conformity.

2.3 Who may install and use the device

Device installation

All installation, assembly, and wiring work must be carried out exclusively by qualified electricians familiar with the applicable standards, regulations, and safety provisions for installation and automation technology.

Using the device

Users of the IoT Portal and the app must possess basic PC skills, be able to use a web browser, and understand the relevant terminology.

Users may be electricians or end users authorized by the owner, or by the owner's authorized representatives, to manage, configure, or modify the devices.

The owner of the equipment is responsible for ensuring that all users have understood the user manual, the functions of the equipment, and the effects of functions performed with the equipment, including remote operation, so that no person is put at risk of injury.

2.4 Intended use

Devices in the CMS-10R series are intended for remote monitoring and remote control in industrial and building technology. They transmit changes in the values of the digital and/or analogue inputs via the mobile phone network to message recipients by push notification, SMS, pager, e-mail, and/or voice call. The potential-free changeover contacts of the relay outputs can be switched via the IoT Portal, an Internet browser, the app, SMS, or telephone control.



For questions regarding availability in your region, see Section 3.7.2, Country versions, or contact ComatReleco Technical Support.

2.5 Applications the device is not intended for

- Applications with high requirements for availability or redundancy.
- Use of the devices in cases where the availability of the Internet connection or the IoT Portal cannot be fully guaranteed.

2.6 Prevent configuration errors

- If an incorrect device configuration is loaded onto the device, or if settings that do not correspond to the application are made, this may lead to undesired behaviour of the inputs and outputs.
- After an update or import of the device configuration, the configuration must be checked on the device to prevent undesired behaviour of the inputs and outputs.

2.7 Information security

The system implements the following security measures in response to the increasing number of cyberattacks. These measures support the confidentiality, integrity, and availability of the system, data, and information, and the traceability of data and information handling.

Account access and authentication

- **Password:** at least 8 characters, including one number, one special character, and uppercase and lowercase letters. See also Section 5.1.2, Log in, create an account or reset your password
- **Two-factor authentication (2FA):** supported apps include Google Authenticator, Microsoft Authenticator, and similar apps. See also Section 7.2.4, Set up two-factor authentication (2FA).
- **Login attempts:** after 5 failed login attempts, access is blocked for 5 minutes. See also Section 5.1.2, Log in, create an account or reset your password

Encrypted data transmission

- **TLS 1.2 encryption:** from the modem of the CMS-10R to the IoT Portal.

Network security

- **128-bit VPN connection:** between the CMS-10R and the IoT Portal.

Roles and access rights

- **Roles and rights:** owner, installer, or user.

Data storage

- **Data** is stored on servers in Switzerland.

To minimise risk, users must also take the following measures:
- Restrict access.
- Create a backup copy of the device configuration. See also Section 6.2.2.3, Manage your device
- Use anti-virus software and firewalls.
- Raise awareness among other users, and train and empower them.

Chapter 3

Understand your CMS-10R

3.1 Overview

Use the CMS-10R to monitor and control equipment remotely in industrial and building technology applications.

When a digital and/or analogue input value changes, the device can notify message recipients through the mobile phone network by push notification, SMS, pager, e-mail, and/or voice call. Use the IoT Portal, the app, a web browser, SMS, or telephone control to switch the potential-free changeover contacts of the relay outputs.

All operations are temporarily stored on a server hosted in Switzerland and forwarded to the corresponding end device. If the server connection is unavailable, fallback mode provides temporary communication via SMS.

To configure the device, use a web browser on an Internet-connected computer or tablet. You need a user account on the ComatReleco IoT Portal for configuration and/or administration.

3.2 Identify your device variant

Characteristic	CMS-10R-D/AC110-240V (Z2/Z1)	CMS-10R-DA/DC12-48V (Z2/Z1)	CMS-10R-DAC/DC12-48V (Z2/Z1)
Nominal voltage and frequency	95–240 V ~, 45–65 Hz	10–48 V ⎓	10–48 V ⎓
Inputs	6 digital	6 digital / analogue 0–10 V ⎓	4 digital / analogue 0–10 V ⎓ 2 analogue 4–20 mA ⎓ (I5, I6)
Outputs	**4 x relay with changeover contacts, 10 A / 250 V** ~	**4 x relay with changeover contacts, 10 A / 250 V** ~	**4 x relay with changeover contacts, 10 A / 250 V** ~
Countries	**Z2:** Device type for Europe, Middle East, Africa and Asia **Z1:** Device type worldwide	**Z2:** Device type for Europe, Middle East, Africa and Asia **Z1:** Device type worldwide	**Z2:** Device type for Europe, Middle East, Africa and Asia **Z1:** Device type worldwide
Mobile networks	**4G, 3G, 2G** supported frequency bands.	**4G, 3G, 2G** supported frequency bands.	**4G, 3G, 2G** supported frequency bands.
Accessories included	Device antenna stubby CMS-ANT-STUB/INT-50MM	Device antenna stubby CMS-ANT-STUB/INT-50MM	Device antenna stubby CMS-ANT-STUB/INT-50MM
* Terminal type	Screw	Screw	Screw

Standard signals

Standard signal type	Range
Voltage standard signal	0–10 V
Current standard signal	4–20 mA

Compared with the voltage standard signal, the 4–20 mA current standard signal is less susceptible to electromagnetic interference. It is also largely unaffected by the disadvantages of long cable runs between the signal sources and the CMS-10R.

3.3 Main operating functions

The device operates cyclically according to the selected sequence.

- Switch outputs on and off through the IoT Portal, the app, a web browser, an SMS message, or the call-in function.
- Request input and output status through the app, a web browser, or SMS to obtain an overview of the system status. Input and output status can also be included in each message.
- Configure a switch-off delay for an individual relay output if you want a command to switch its contact on and return it automatically to its initial position after an adjustable time.
- If required, configure the device to send a status message automatically at regular intervals.
- If enabled under **Manage** / **Events** / **Power on/off**, the device detects a power supply interruption and sends a message as its last event. It sends another message when power is restored.
- When the IoT Portal is inaccessible, **Fallback mode** sends pending alarms directly to the preset message receivers by SMS only. Status messages also work only via SMS in this mode.

3.4 Locate terminals, controls, and status indicators

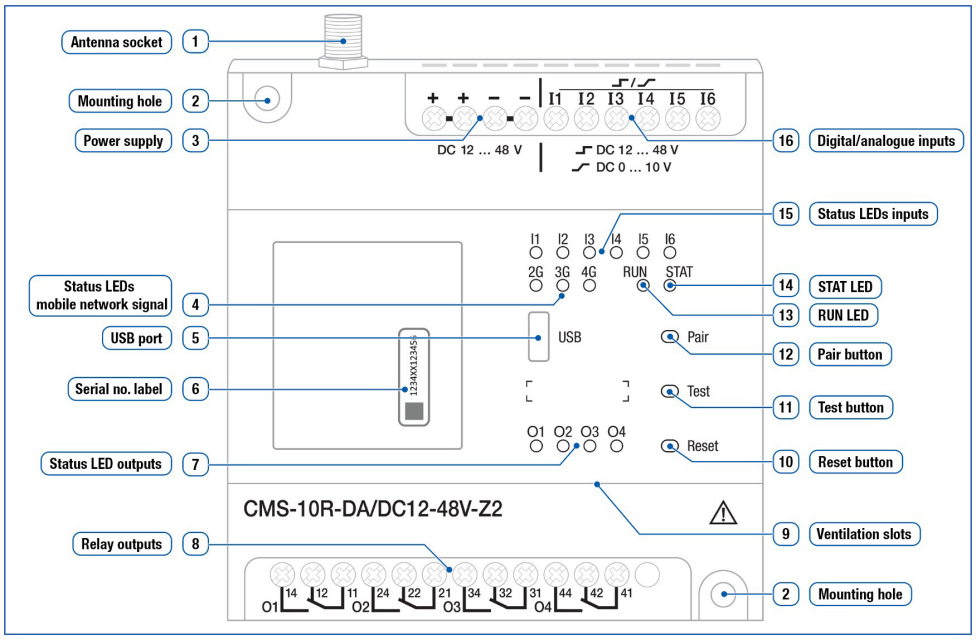


Figure 3.1: CMS-10R front view: numbered terminals, controls, and status indicators.



Figure 3.2: CMS-10R rear views: mounting holes and DIN rail mounting bracket.

1 - Antenna socket

- Connect the antenna to the **antenna socket**.
- Choose **antennas** and **antenna extensions** to suit your application. See Section 4.4.1, Antenna.

Important: Do not exceed the tightening torque of **1.0 Nm**.

2 - Mounting holes

- Use mounting screws with a maximum thread diameter of **3.9 mm**.
- **Important:** Do not exceed the tightening torque of **1.0 Nm**.
- If the housing has pre-installed screws, remove them before mounting the device on the wall.

3 - Power supply

- Connect stranded conductors or wires with a maximum cross-section of **2.5 mm²** to the screw terminals.
- Terminals with the same designation are connected electrically inside the device. Use them as feed-through terminals to avoid multiple assignments.
- Terminal designation for the AC version:
  L: outer conductor
  N: neutral conductor
- Terminal designation for the DC version:
  +: plus
  -: minus
- The terminals designated **N** / **-** form the common reference potential for the inputs.
- For the **Power supply** details of each device type, see Section 3.2, Identify your device variant.

4 - Status LEDs, Mobile network signal

Use these LEDs to identify the active mobile network standard (**2G, 3G, or 4G**). Their colour indicates signal strength.

LED status	Operating mode	Mobile network	IoT Portal
LED off	Fallback: event storage on the device	None	Not connected
LED flashing orange	Fallback: SMS directly to recipient	Poor reception	Not connected
LED lit orange	Normal operation	Poor reception	Connected
LED flashing green	Fallback: SMS directly to recipient	Good reception	Not connected
LED lit green	Normal operation	Good reception	Connected

5 - USB port

- The USB connection is for internal purposes only.

6 - Serial no. label

- Enter this serial number when pairing the device.

7 - Status LEDs, Outputs

LED status	Status	Flashing frequency
LED off	Relay switched off. Relay contact is open.	—
LED lit	Relay switched on. Relay contact is closed.	—

8 - Relay outputs

- Every device type provides **4 changeover contacts**.

9 - Ventilation slots

- Keep the ventilation slots clear to maintain adequate cooling. Do not tape over them or cover them with components.

10 - Reset button

- For a normal restart, press the **Reset button** briefly and release it before **4 seconds**.
- To perform a forced hardware reset, hold the **Reset button** for more than **4 seconds**. Use this only if the system is unresponsive; a forced hardware reset may result in data loss.

11 - Test button

- Use the **Test button** to test the connection to the IoT Portal.
- Pressing the button sends a message by push notification, SMS, pager, e-mail, and/or voice call according to the configuration.
- Check the test status in the IoT Portal under **Overview**/**Test**. See Section 6.2.1, Check device status: Overview.

12 - Pair button

- Use the **Pair button** to pair the device with the IoT Portal.

13 - RUN LED

LED status	Status	Flashing frequency
LED off	The device is switched off or is not functioning. See also Section 10.1, Troubleshooting.	—
LED flashing	The device and the firmware are ready for use and are in operation.	Slow

14 - STAT LED

- The **STAT LED** indicates the operating status.

LED status	Status	Flashing frequency
LED off	Normal operation	—
LED flashing	Firmware update	Fast, flashing
LED flashing	Firmware update / restart	Slow
LED lit	Device shuts down / exits all running tasks	—
LED flashing	Device shuts down / terminates the connection to the IoT Portal and the mobile network	Fast, even

15 - Status LEDs, Inputs

Digital inputs

LED status	Status	Flashing frequency
LED off	Input value = logic level 0, low	—
LED lit	Input value = logic level 1, high	—

Analogue inputs

LED status	Status	Flashing frequency
LED off	Input level $\leq$ lower threshold value	—
LED flashing	Lower threshold value $<$ input level $<$ upper threshold value	Slow
LED lit	Input level $\geq$ upper threshold value	—

16 - Inputs, Digital / Analogue

Digital

A digital input is interpreted as logic level **1** (high) when its applied voltage exceeds the switch-on threshold.

Always use the same reference potential for the input voltages and the device **Power supply**.

Logic 1	Switch-on threshold
`CMS-10R-D/AC110-240V-Zx`	$>$ 24 V AC
`CMS-10R-DA/DC12-48V-Zx`	$>$ 6.0 V DC
`CMS-10R-DAC/DC12-48V-Zx`	$>$ 6.0 V DC

Analogue, voltage

- When an input is configured as **analogue**, it converts **0–10 V DC** into a value that you can scale, such as temperature or flow rate.
- If the voltage exceeds **10 V DC** but does not exceed the operating voltage, the input applies the configured maximum value.
- The voltage input complies with **IEC 60381-2**.

Analogue, current

- The **4–20 mA DC** input is designed as a current loop interface.
- The current input burden is **150** Ω. The full **4–20 mA DC** range is converted into a scalable value.
- You can enable the current input. It complies with **IEC 60381-1**.

17 - DIN rail mounting bracket

- Use this slot to mount the device on a **35 mm DIN rail** in accordance with **IEC 60715**.

3.5 Check the delivery

- When the device arrives, check the delivery against the delivery note.
- Contact your seller immediately if you find any defects or missing parts on receipt.
- For delivery conditions and information about returning goods, see the ComatReleco web portal.
- For the next steps, see also Section 10.3, Replace or return a defective device.

3.6 Transport, storage, and returns

The device is supplied in its original cardboard packaging, which provides the best possible protection during transport.

Store the device at room temperature in a dry place if you will not use it for an extended period.

For a return, repack the device in its original packaging as it was received. This ensures safe transport.

3.7 Check mobile network compatibility and coverage

3.7.1 Network coverage

The device can communicate through 750 mobile network providers worldwide. Coverage at your installation site depends on the extent of the local provider's network.

At the installation site, the device automatically selects the available network generation with the highest field strength.

Allow up to 5 minutes for roaming when the device switches between mobile networks or connects to the IoT Portal from abroad.
Contracts with local providers are updated annually, so short-term coverage changes may occur at the installation site.

3.7.2 Country versions

Check the ordering-code suffix to identify the modem variant: **Z1** or **Z2**. These two variants support different public mobile networks.

Network operation depends on both the frequency bands and cellular technologies supported by the selected modem variant and the corresponding services offered by the local operator in the country of installation. These conditions vary between operators and may change over time. This manual therefore does not give a fixed list of supported countries or operators.

Before commissioning, verify that your product variant is suitable for the intended country and mobile network operator. If you need assistance, contact **ComatReleco Technical Support**. See Section 1.5, Contact details.

3.7.3 Frequency bands by modem variant

The following table lists the bands for modem variants **Z1** and **Z2**. You are responsible for ensuring that the selected variant is suitable for your application and operating region.

Standard	Zone/region	Frequency type	Frequency bands
4G LTE	Z1	LTE-FDD	B1 (2100 MHz), B2 (1900 MHz), B3 (1800 MHz), B4 (1700 MHz), B5 (850 MHz), B7 (2600 MHz), B8 (900 MHz), B12 (700 MHz), B13 (700 MHz), B18 (850 MHz), B19 (850 MHz), B20 (800 MHz), B25 (1900 MHz), B26 (850 MHz), B28 (700 MHz)
4G LTE	Z1	LTE-TDD	B38 (2600 MHz), B39 (1900 MHz), B40 (2300 MHz), B41 (2500 MHz)

Standard	Zone/region	Frequency type	Frequency bands
4G LTE	Z2	LTE-FDD	B1 (2100 MHz), B3 (1800 MHz), B7 (2600 MHz), B8 (900 MHz), B20 (800 MHz), B28A (700 MHz)
3G UMTS	Z1	UMTS	B1 (2100 MHz), B2 (1900 MHz), B4 (1700 MHz), B5 (850 MHz), B6 (800 MHz), B8 (900 MHz), B19 (800 MHz)
3G UMTS	Z2	UMTS	B1 (2100 MHz), B8 (900 MHz)
2G GSM	Z1	GSM	B2 (1900 MHz), B3 (1800 MHz), B5 (850 MHz), B8 (900 MHz)
2G GSM	Z2	GSM	B3 (1800 MHz), B8 (900 MHz)

Important: A band listed in the device specification does not guarantee network access in a particular country or on a particular operator network. Access also depends on that operator's services and band configuration.

3.8 What happens during interruptions, resets, and updates

Power failure and recovery

If the device detects a failure of the **Power supply**, it uses its remaining stored energy to initiate message transmission through the IoT Portal. It then shuts down automatically.

Messages are distributed either by simultaneous alarm activation or by an escalation chain. Settings remain permanently stored in internal memory. The outputs switch off and the device disconnects from the IoT Portal.

When the **Power supply** is restored, the device restores the most recent electrical output settings and applies the most recent input configuration, regardless of the duration of the failure. It also re-establishes the mobile connection and reconnects to the IoT Portal.

The IoT Portal then transfers any pending configurations to the device. If acknowledgement is enabled, the waiting time continues. Events are sent to message receivers according to the configured maximum number of acknowledgement runs.



After the **Power supply** is restored, you must check that all outputs are in the correct and intended state.

Notification when power is restored

If this message is enabled, the device notifies the recipient when operating voltage is restored and the device returns to normal operation.

Mobile network interruption and recovery

While the mobile network connection is interrupted, the device temporarily stores any events that occur.

When the mobile network connection is restored, the device sends its cached events to the IoT Portal. The IoT Portal then transfers any pending configurations to the device.

If acknowledgement is enabled, the waiting time continues. Events are sent to message recipients according to the configured maximum number of acknowledgement runs.

IoT Portal interruption: fallback mode

If the IoT Portal is inaccessible, the device activates **Fallback mode** and sends pending alarms directly to the predefined message receivers by SMS only.

Output control by **Call-in** and **SMS control messages** works as in normal operation. See Section 6.2.5, Configure and control relay outputs: Outputs, and Section 6.2.2.2, SMS output control. Message receivers are notified by SMS only.

When the IoT Portal connection is restored, events are sent to message receivers through the channels configured under **Notifications**: push, SMS, pager, e-mail, and/or voice call.

To query the status of all inputs and outputs in fallback mode, send the SMS command **status** to the device.
Before controlling the device in fallback mode, enable **SMS control** for the relevant **outputs** and enable **SMS output control** under **Manage**.

Use the acknowledgement code **code** in fallback mode.

The acknowledgement message is sent to all message receivers in this format: **OK: Mobile phone number**.

After the cloud connection is lost, switching to fallback mode may take up to 10 minutes. Status messages may therefore be delayed. The device nevertheless continuously registers events and sends them directly to message receivers. This ensures reliable operation at all times.

Reset button: restart and forced hardware reset

- **Short press** ($<$ 4 s): release the button before 4 seconds to restart the device. The restart takes approximately 30 seconds to 1 minute.
- **Long press** ($>$ 4 s): hold the button for more than 4 seconds to perform a forced hardware reset.

Both actions switch off the outputs and terminate the connection between the device and the IoT Portal.

After a successful restart, the device restores the last state of each output and applies the last received configuration. It also re-establishes the mobile connection and reconnects to the IoT Portal.

Once connected, the device receives any pending configurations from the IoT Portal.

Use the forced hardware reset only if the system is unresponsive. A forced hardware reset may result in data loss.

Firmware update

Do not use the device during the firmware update.

When you start a firmware update, the device downloads the latest firmware. It restarts after the download completes successfully.

The relay outputs switch off during the restart. They are not restored immediately after the firmware update. The device then restores the last output states and applies the last received input configuration. It re-establishes the mobile connection and reconnects to the IoT Portal, which then transfers any pending configurations to the device.

If the update fails, the device starts with the previous firmware version and existing configuration.

Check the installed firmware version in **Overview**; see Section 6.2.1, Check device status: Overview. The **Cogwheel icon** under **Manage** continues to indicate that a firmware update is available; see Section 6.2.2, Manage device settings and ownership: Manage.

Internal firmware error: watchdog restart

If an internal firmware error occurs, the watchdog automatically restarts the device within 2 minutes at the latest to correct the fault. The behaviour is the same as after a manual reset.

Chapter 4

Install and connect the device



DANGER
Risk of death due to electric shock!
Only mount or dismantle the device when it is disconnected from the power supply. See Section 2.2, General safety instructions.



WARNING
Only qualified electricians may carry out the work in this chapter. See Section 2.3, Who may install and use the device.

4.1 Before installation

- Follow these installation instructions. Observe the regulations and safety requirements for installation and operation, including national safety regulations and generally recognised engineering practices. Refer to the package insert and the certificate of conformity for safety-related data.
- Do not open, modify, or repair the device. Only the manufacturer may carry out repairs. Replace a damaged device with an equivalent one.
- Install the device only as a permanently fixed installation. Do not use it as a mobile unit.
- The device has protection class IP40 according to IEC 60529 / EN 60529. Use it only in clean, dry environments. Do not expose it to mechanical and/or thermal stress beyond the limits in the technical data.



Before installation, check that the device zone or region (**Z1** or **Z2**) is suitable for the installation site. See Section 3.7.2, Country versions

4.2 Mounting

4.2.1 Mounting the device

Install the device inside an additional protective housing. Mount it on a **35 mm DIN rail** compliant with **IEC 60715**, or use the mounting holes to attach it directly to the housing wall. See Section 2.2, General safety instructions.

The following minimum requirements apply to the protective housing:

- Ingress Protection **IP40**
- Pollution Degree **II**
- Overvoltage Degree **II**
- Mechanical dimension standard **DIN 43880**

DIN rail mounting

1. Place the device on the DIN rail from above.
2. Press the device evenly from the front onto the rail until it audibly clicks into place.

Mounting on a wall of the protective housing

1. Choose a mounting position on the rear wall of the enclosure. The device can be mounted directly, for example using press-in nuts.
2. Check that the mounting position complies with the data sheet specification and allows adequate air circulation through the ventilation slots.
3. Screw the device to the enclosure wall. Use screws with a maximum head diameter of **6 mm** and a maximum thread and shank diameter of **3.9 mm**. Do not exceed the tightening torque of **1.0 Nm**.

4.2.2 Dismantling the device

DIN rail mounting

1. Remove all electrical connection wires.
2. Insert a screwdriver into the tab at the bottom of the device and release the lock by moving it downward.
3. Lift the device off the DIN rail.

Removal from the enclosure wall

1. Remove all electrical connection wires.
2. Loosen the screws.
3. Remove the device.

4.3 Connect the power supply, inputs, and outputs

4.3.1 Power supply

- When connecting to the **230 V AC mains**, ensure that the **Power supply** and the supply to the inputs are connected to the same outer conductor.
- No voltage exceeding **240 V AC** may be present on the device.
- The device is insulated and does not require a protective conductor (earthing) connection.
- Connect the device according to one of the following connection variants.

4.3.2 Wiring of the CMS-10R-D inputs

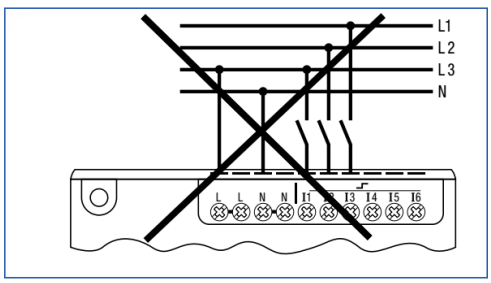


Figure 4.1: CMS-10R-D input wiring: invalid connection to different outer conductors.

- The digital inputs must not be connected to different outer conductors, L1, L2, L3.

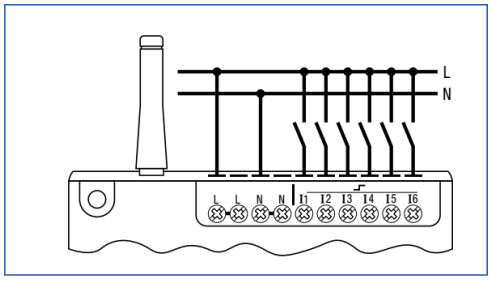


Figure 4.2: CMS-10R-D input wiring: digital inputs connected to one outer conductor.

- Connect the digital inputs to an outer conductor, L.

4.3.3 Wiring the CMS-10R-DA inputs

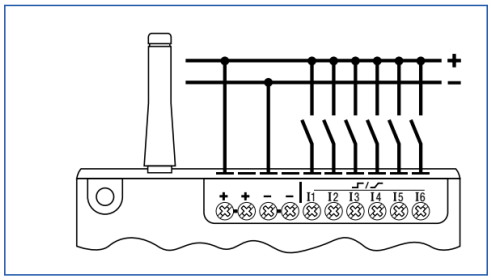


Figure 4.3: CMS-10R-DA digital input wiring.

- Connect the digital input contacts between **+** and inputs **I1–I6**.
- **I1–I6**: Digital inputs.

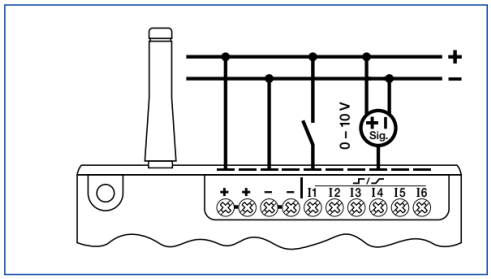


Figure 4.4: CMS-10R-DA analogue input wiring.

- Connect the positive lead of the **0–10 V** analogue source to the input configured as analogue (**I4** in this example). Connect its negative lead to the device **-** terminal.
- **I1–I6**: Configurable analogue inputs, 0–10 V ⎓.

4.3.4 Wiring the CMS-10R-DAC inputs

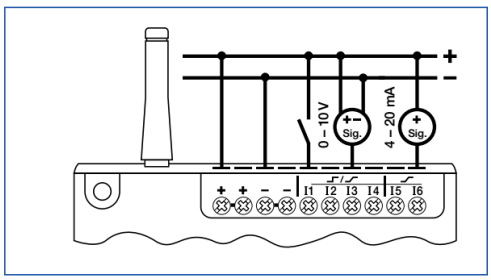


Figure 4.5: CMS-10R-DAC digital, voltage, and current input wiring.

- Connect the contacts of the digital inputs to **+**.
- Connect the analogue sources between **+** and **-**.
- Connect the power sources to **+**.
- **I1–I4**: Digital inputs or analogue inputs, 0–10 V ⎓.
- **I5–I6**: Current inputs, 4–20 mA ⎓.

4.3.5 Wiring the CMS-10R-D / -DA / -DAC relay outputs

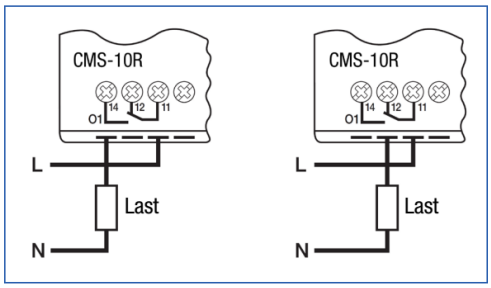


Figure 4.6: CMS-10R relay output connection example.

- Connect the input signal of the relay contact to terminal 11. Connect the load to terminal 12 or 14.
- Connect a load that meets the minimum contact load of 10 mA, 12 V ⎓.

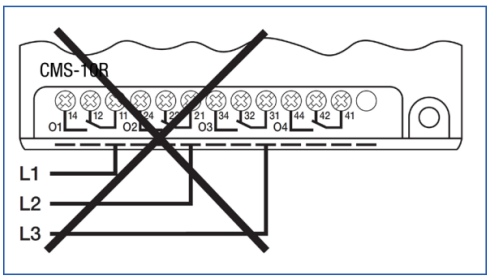


Figure 4.7: CMS-10R relay output wiring.

Do not apply three-phase voltage (400 V / 3-phase) to the outputs.

4.4 Antennas and antenna cables

The CMS-10R is supplied with the `CMS-ANT-STUB/INT-50MM` GSM device antenna. Use a remote antenna where required by the installation conditions.

The antenna and cable types described below are available.

4.4.1 Antenna

The **Stubby** GSM device antenna (`CMS-ANT-STUB/INT-50MM`) is a fixed antenna. Connect it to the **antenna socket**.

Use this antenna where signal strength is good and electromagnetic shielding is negligible. It is suitable for indoor installation in a non-metallic control cabinet or distribution box, such as a plastic enclosure, or in a timber-frame building.

4.4.2 Antenna extension cables

All listed antenna types can be used with any of these extension cables:

- CMS-ANT-KAB/2.5M
- CMS-ANT-KAB/5M
- CMS-ANT-KAB/10M
- CMS-ANT-KAB/20M

Keep antenna cables as short as possible to avoid unnecessary losses.

An extension cable is recommended for magnetic-base and outdoor antennas.

- The CMS-10R may only be operated with antennas and antenna cables from the ComatReleco accessories range. Refer to this range for *Order details and accessories*.
- The supplied device antenna CMS-ANT-STUB/INT-50MM is not suitable for installation in a metallic control cabinet because of the shielding effect.
- When using antenna cables, ensure that the total length does not exceed **25 m**. Wherever possible, use a single antenna cable rather than several shorter cables. Select the shortest possible antenna cable.
- During operation, persons must maintain a minimum distance of **20 cm** from the antenna.
- Take care when installing external antennas. Twisting the antenna cable may cause damage and impair correct operation.
- Observe the maximum bending radius of the antenna cable.
- For pre-assembled antenna cables and other antenna types, contact ComatReleco Technical Support, see also Section 1.5, Contact details.

Chapter 5

Commission the device in the IoT Portal

Use this chapter to create or access your account, add and pair the device, then choose a service profile. Pair the device before configuring it. Pairing starts the fee-based service profile. Continue with device configuration in Chapter 6; account and payment settings are in Chapter 7.

5.1 Access the IoT Portal and plan commissioning

Use the ComatReleco IoT Portal to commission and operate your device. You do not need programming skills. You need basic PC and web browser skills and an understanding of the relevant terms.



Figure 5.1: ComatReleco IoT Portal login page.

5.1.1 Commissioning sequence

Commissioning requires a user account in the IoT Portal. Create an account first if you do not already have one.

To commission a new device, follow this sequence:

1. Create an account or log in; see Section 5.1.2, Log in, create an account or reset your password.
2. Add the device using the procedure for your role; see Section 5.2, Add a device to your account.
3. Pair the device using its serial number and the device's **Pair** button; see Section 5.3, Pair your device.
4. As the owner, select a service profile; see Section 5.4, Select a service profile and SMS packages.
5. Configure the device; see Section 6.2, Configure and operate a device.

Pair the device before configuring it. Using **Pair** activates the fee-based service profile for a **one-year term**.

5.1.2 Log in, create an account or reset your password

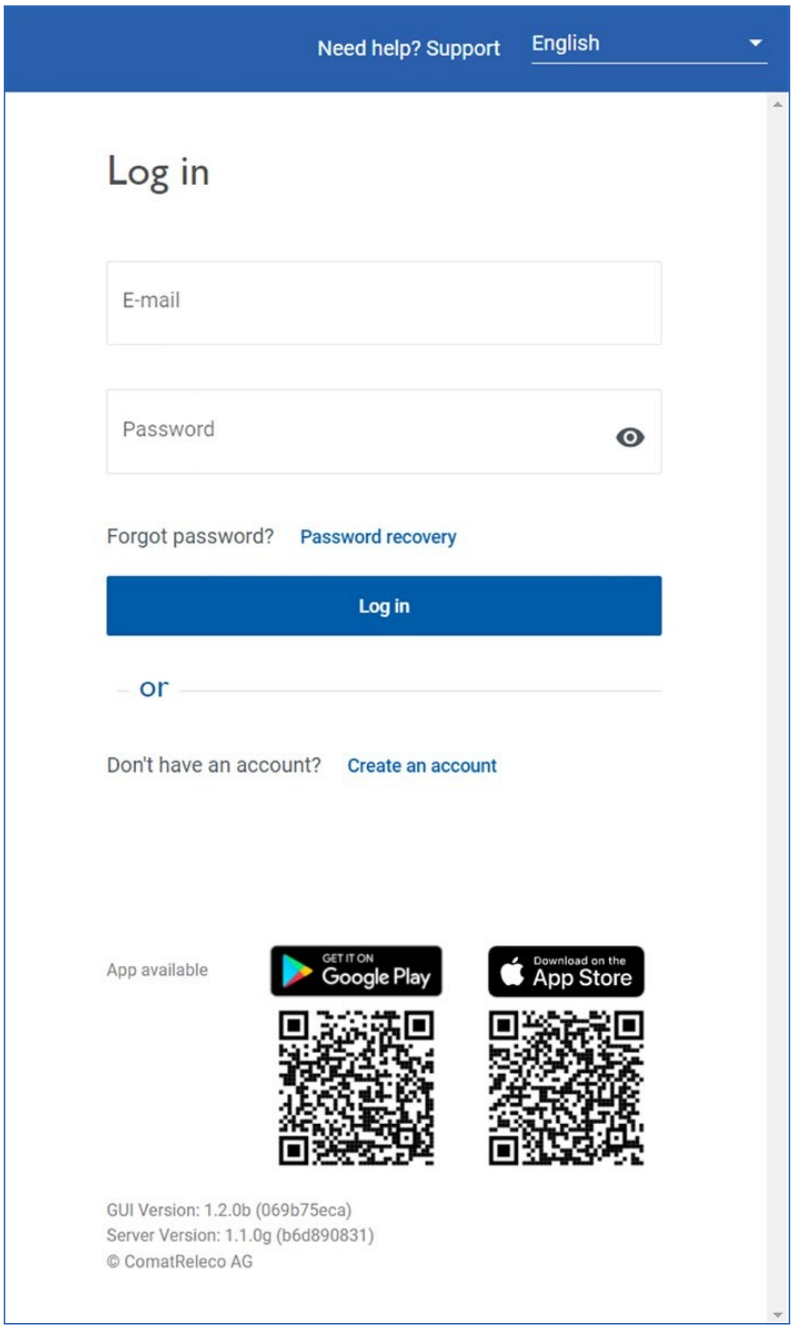


Figure 5.2: Login, account creation and password recovery options.

Log in to an existing account

Enter your **e-mail** address and **password**, then select **Login**.

Create a new account

1. Select **Create account**.
2. Complete all mandatory fields marked with an asterisk, *.
3. Read and accept the privacy policy.
4. Confirm your e-mail address using the confirmation e-mail sent to you.

If you do not receive the confirmation e-mail, check your spam folder or ask your IT Manager to adjust the firewall settings.

Reset a forgotten password

1. On the home page, select **Reset password**.
2. Enter your account e-mail address and select **Send recovery e-mail**.
3. Open the link to the IoT Portal in the recovery e-mail.
4. Enter a new password using this link.
5. Log in with your new password.

Select a language

You can select the language on the login page or change it later in your profile. See Section 7.2.1, Menu: Profile.

Your password must contain at least 8 characters, including a number, a special character, an uppercase letter and a lowercase letter. After five consecutive incorrect password entries, login is blocked for 5 minutes.
Use the eye symbol to display the password text.

5.2 Add a device to your account

Before you start: Create a user account and log in. The devices overview appears after login. If the system asks whether notifications are allowed, select **Allow**.

Choose the procedure that matches your role: installer, owner or invited user with an invitation code.

5.2.1 Add a device as the installer

Use this procedure when you install a device for another owner.

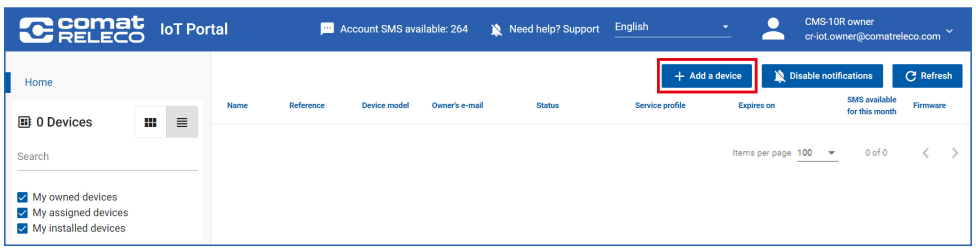


Figure 5.3: Devices overview: adding a device as installer.

1. From the devices overview, select **+ Add a device** to add a new device.
2. Select **Set up a new device**.

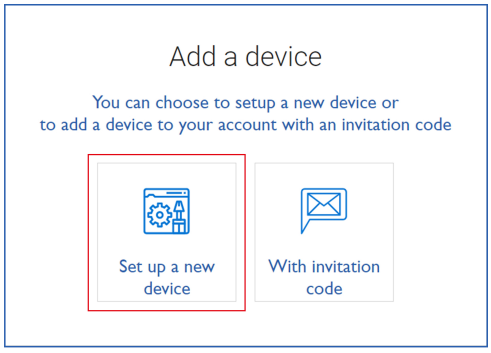


Figure 5.4: Start setting up a new device.

Select **Set up a new device** to begin the installer setup.

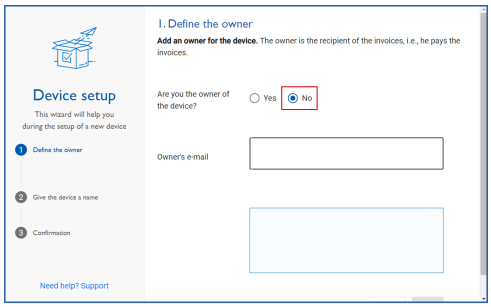


Figure 5.5: Specify that you are the installer and identify the owner.

3. Select **No** because you are the device installer.
4. Enter the device owner's e-mail address.

The database checks whether this user already has an account.

If the owner already has an account

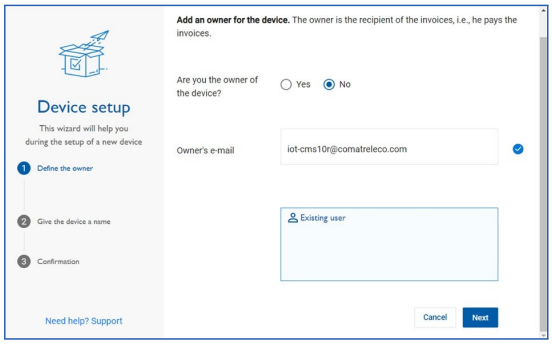


Figure 5.6: Owner invitation for an existing IoT Portal user.

Case A: The future owner receives an e-mail with a link to log in to the IoT Portal and accept or decline the invitation.

If the user accepts, that user becomes the owner. If the user rejects the invitation, the installer remains the owner.

The invitation is valid for 30 days. After this period, resend it under **Manage, Change owner**; see Section 6.2.2, Manage device settings and ownership: Manage.

After the invitation is accepted, complete only the owner setup steps still outstanding in Section 5.2.2, Add a device as the owner. Follow the guidance at the start of that section if owner setup is already complete.

If the owner does not yet have an account

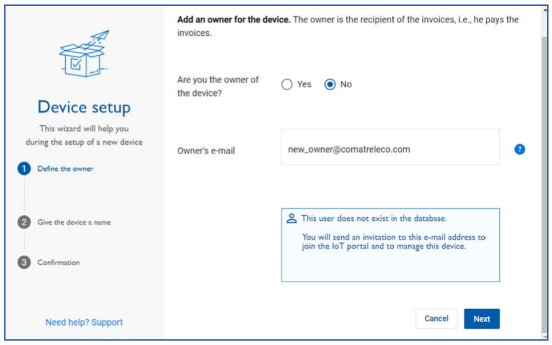


Figure 5.7: Owner invitation for a new IoT Portal user.

Case B: The user receives an e-mail with a link to create an account and log in to the IoT Portal.

The user must create an account and add a standard payment method before accepting or rejecting the invitation.

The invitation is valid for 30 days. After this period, resend it under **Manage, Change owner**; see Section 6.2.2, Manage device settings and ownership: Manage.

After the invitation is accepted, complete only the owner setup steps still outstanding in Section 5.2.2, Add a device as the owner. Follow the guidance at the start of that section if owner setup is already complete.

5.2.2 Add a device as the owner

Check what is already complete: If the device has already been added, do not add it again. Complete only the owner setup steps that are still outstanding. If owner setup is complete, skip this procedure and continue with the next outstanding task:

- If the device is not yet paired, continue with Section 5.3, Pair your device.
- If it is already paired, complete any outstanding service-profile selection and device configuration; see Sections 5.4 and 6.2.

Before you start: Create a user account and log in. If the system asks whether notifications are allowed, select **Allow**.

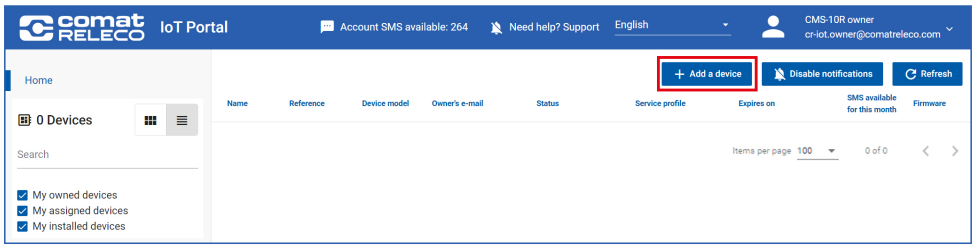
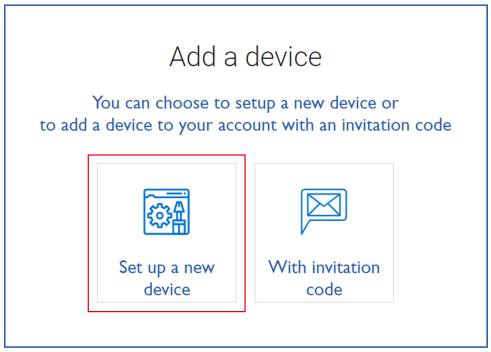


Figure 5.8: Devices overview: adding a device as owner.

1. From the devices overview, select **+ Add a device** to add a new device.
2. Select **Set up a new device**.



Select **Set up a new device**.

Figure 5.9: Start setting up a new device as owner.

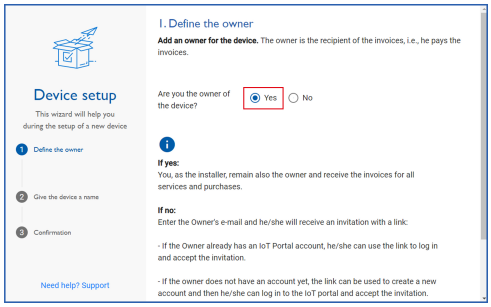


Figure 5.10: Confirm that you are the device owner.

3. Select **Yes** because you are the device owner.

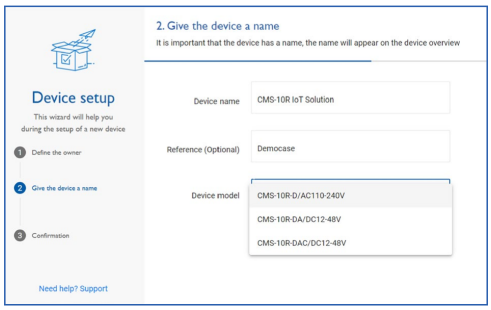


Figure 5.11: Enter the device name, model and optional reference.

4. Enter a device name of no more than 30 characters and select the device model.
5. Optionally, enter a reference, such as the name of the building, plant or machine to which the device belongs.

The reference appears in the devices overview and is printed on the order confirmation and invoice for the service profile purchase.

If you use SMS notifications, keep the device name and reference short and avoid special characters. Long names, long references and special characters may increase the SMS length. A notification may then be split into multiple SMS messages and charged accordingly.

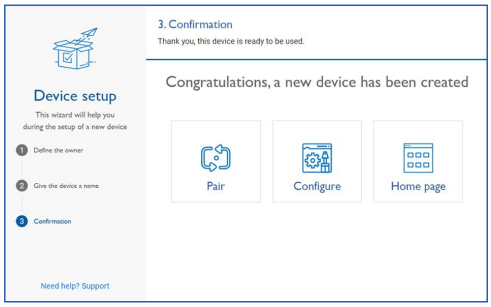


Figure 5.12: Continue commissioning after adding the device.

6. Select **Pair** to continue commissioning; see Section 5.3, Pair your device.

To return to the devices overview, select **Home page**; see Section 6.1, Find devices and check their status.

Pair the device before configuring it. Using **Pair** starts the one-year, fee-based service profile. See Section 5.1.1, Commissioning sequence.

5.2.3 Add a device using an invitation code

Use this procedure if another user has sent you an invitation code by e-mail or SMS.

Before you start: Create a user account and log in. If the system asks whether notifications are allowed, select **Allow**.

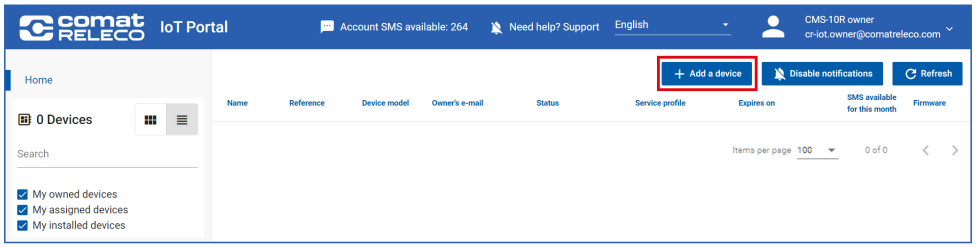


Figure 5.13: Devices overview: adding a device with an invitation code.

1. From the devices overview, select **+ Add a device** to add a new device.
2. Select **With invitation code**.

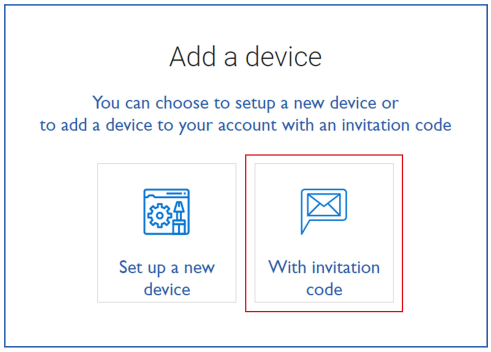


Figure 5.14: Choose the invitation-code option.

Select **With invitation code** for the code received from another user by e-mail or SMS.

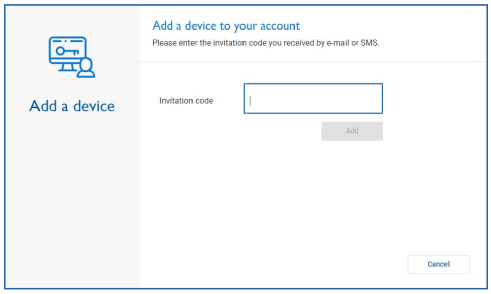


Figure 5.15: Enter the invitation code.

3. Enter the invitation code received by e-mail or SMS.

You can then use the device.

5.3 Pair your device

Pair the device after adding it and before configuring it. Pairing starts the **one-year, fee-based service profile**. See Section 5.1.1, Commissioning sequence.

5.3.1 Pair directly after adding the device

Before you start: Complete the **Device setup** procedure in Section 5.2, Add a device to your account. Have the device serial number available; it is printed on the label on the front of the device.

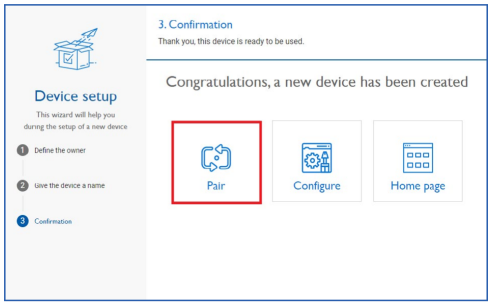


Figure 5.16: Pairing at the end of Device setup.

1. In the last step of **Device setup**, select **Pair**.

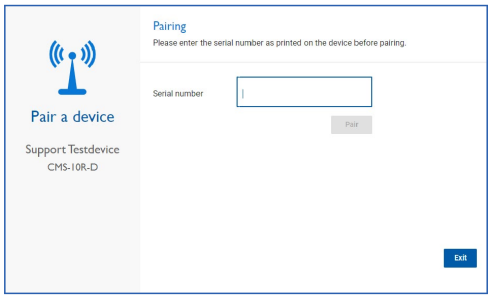


Figure 5.17: Enter the serial number printed on the device.

2. Enter the device serial number from the front label.

Example: `1939VS000096`.

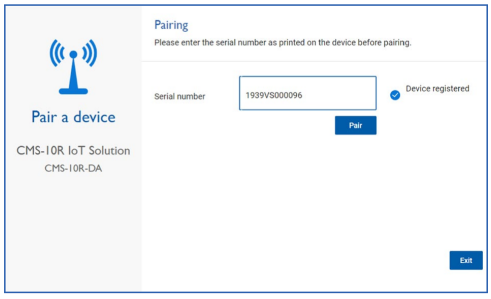


Figure 5.18: The portal confirms a valid serial number.

3. Check that **Device registered** appears on the right. This information appears when the serial number is valid.
4. Select **Pair**.

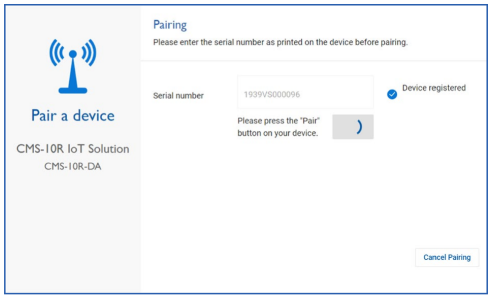


Figure 5.19: Acknowledge pairing on the device.

5. Press the **Pair** button on the device to acknowledge pairing. See Figure 3.1, item **12**.

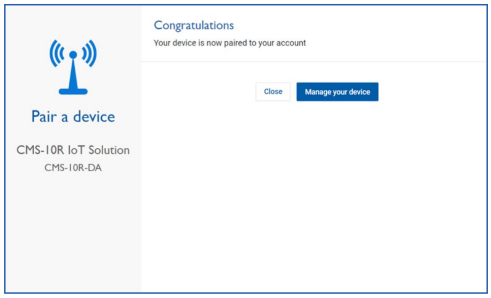


Figure 5.20: Successful pairing and next actions.

After successful pairing, choose your next action:

- **Close**: return to the devices overview; see Section 6.1, Find devices and check their status.
- **Manage your device**: configure the device; see Section 6.2, Configure and operate a device.

It can take up to 10 minutes for the status to appear in the IoT Portal.

Using **Pair** starts the one-year, fee-based service profile.

5.4 Select a service profile and SMS packages

Before you start: Pair the device. Only the device **owner** can select and manage its service profile.

A **service profile** must be selected after pairing. For details of the available functions and service profile settings, see Section 6.2.8, Manage the service profile: Service profile.

Select the service profile

Select a service profile that provides the functions you require.

- During the **one-year term**, you can switch to the next higher service profile at any time.
- You can switch to a lower service profile only after the current term has expired.

Select optional SMS packages

Select the required number of **SMS packages** and add them to your shopping cart.

You can skip this step and purchase SMS packages later at any time. See Section 7.2.3, Menu: SMS package.

Review the selected items and complete payment in the shopping cart; see Section 7.3.4, Review the shopping cart and pay. For payment preferences, invoice groups and renewals, see Section 7.3, Manage payments, billing groups and account inactivity.

Chapter 6

Configure and monitor your device

Use the device view to configure inputs and outputs, select recipients and notification behaviour, and review recorded events. The following sections retain the menu names used in the IoT Portal so that you can match each instruction to the screen.

6.1 Find devices and check their status

After you have configured a new device successfully, the IoT Portal shows an overview of all your devices. Choose **device view** or **list view**. The information shown depends on the selected view.

Device view

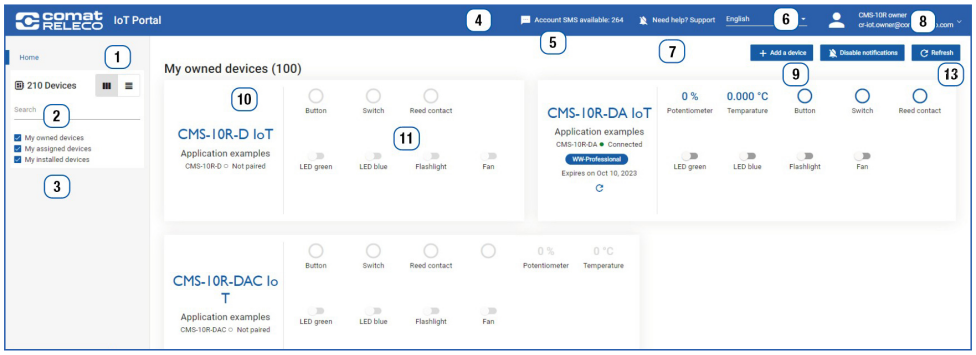


Figure 6.1: Devices overview in device view.

List view

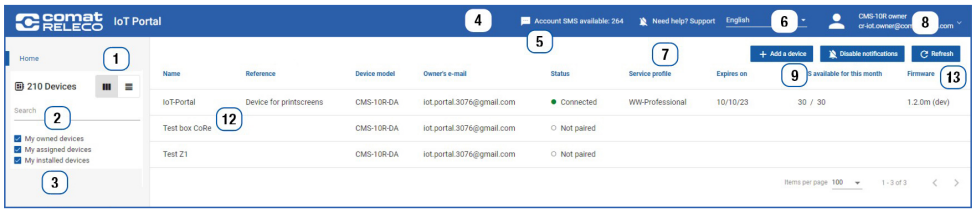


Figure 6.2: Devices overview in list view.

Find a device

Enter a keyword in **Search**, item **2**. To limit the overview to a particular group, choose a filter at item **3**:

- **My owned devices**: devices for which you are the owner.
- **My assigned devices**: devices assigned to you.
- **My installed devices**: devices for which you are the installer.

Read and use the overview

The numbered elements in the figures provide the following functions and information:

1. Switch between **device view** and **list view**.
2. Enter a keyword to search for a device.
3. Select the filter criteria for the devices shown.
4. Check the number of SMS remaining in the purchased SMS package. All devices belonging to the same owner can use these SMS.
5. Open the **SMS Package** menu; see Section 7.2.3, Menu: SMS package.
6. Select the IoT Portal language.
7. Activate or deactivate push notifications.
8. Open the user account settings; see Section 7.2, Manage your account and SMS credit.
9. Add a new device.
10. In device view, read the device's **Name** and **Reference**, **Device model**, **Status**, **Service profile** and **Expires on**. Status information includes *Connected, excellent and good reception / Connected, bad reception / Device not paired / Last connection*. Click the device to open its **Overview** menu; see Section 6.2.1, Check device status: Overview.
11. Check input and output statuses and switch outputs on or off directly.
12. In list view, read the device's **Name** and **Reference**, **Device model**, **Owner's e-mail**, **Status**, **Service profile**, **Expires on**, **SMS available for this month** and **Firmware version**. Status information includes *Connected, excellent and good reception / Connected, bad reception / Device not paired / Last connection*. Click the device to open its **Overview** menu; see Section 6.2, Configure and operate a device.
13. Select **Refresh** to retrieve all device statuses again.

6.2 Configure and operate a device

Use this section after adding and commissioning the device. Follow the menu descriptions in the order that suits your task: check status, manage access and settings, configure inputs and outputs, set notifications, and review activity. Keep actual device and IoT Portal menu labels when following the procedures.

6.2.1 Check device status: Overview

Open the device's **Overview** menu to check its connection, available SMS and event quotas, firmware versions, and input/output states. The numbered items below correspond to Figure 6.3.

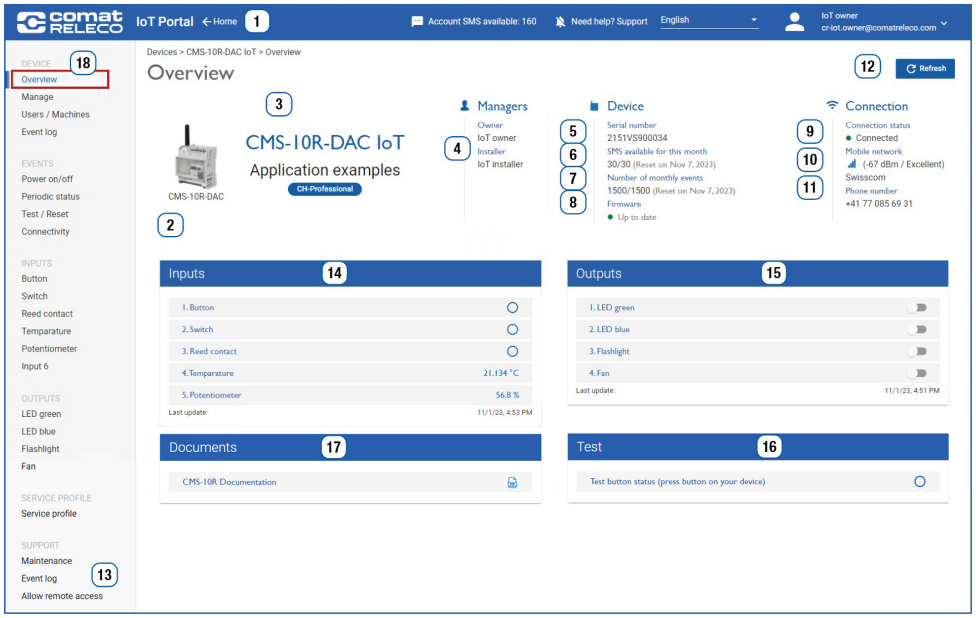


Figure 6.3: Menu Overview.

1. Select **Home** to return to **Devices overview**; see Section 6.1, Find devices and check their status.
2. Device type
3. Device name and service profile, including device reference if entered
4. Names of the device owner and the device installer
5. Device serial number
6. SMS available for the current month under the selected service profile
7. Events available for the current month under the selected service profile
8. Firmware, MCU and modem versions, with an indication of whether they are up to date or an update is available
9. Connection status: connected with excellent or good reception; connected with bad reception; device not paired; last connection in the format DD/MM/YY, HH:MM AM/PM; or maintenance mode
10. Mobile network provider and signal strength display, 1–4 bars

Signal strength	2G [dBm]	3G [dBm]	4G [dBm]
Not connected	$<$ -102	$<$ -103.7	$<$ -93.3
Poor	$\leq$ -89	$\leq$ -90	$\leq$ -80
Good	$>$ -89	$>$ -90	$>$ -80
Excellent	$>$ -74	$>$ -75	$>$ -70

11. Device telephone number
12. Select **Refresh** to retrieve the current device statuses.
13. If you need support, select **Allow remote access** to authorise the ComatReleco AG support team to access the device for one hour.
14. Status of inputs
15. Output states. You can switch outputs on or off directly if you have the required authorisation.
16. State of the device's **Test** button; see also Section 1.4, Documents and support.
17. Documentation

6.2.2 Manage device settings and ownership: Manage

Use **Manage** to identify the device, set its local time, change ownership or installer access, and open the event and device-management functions.

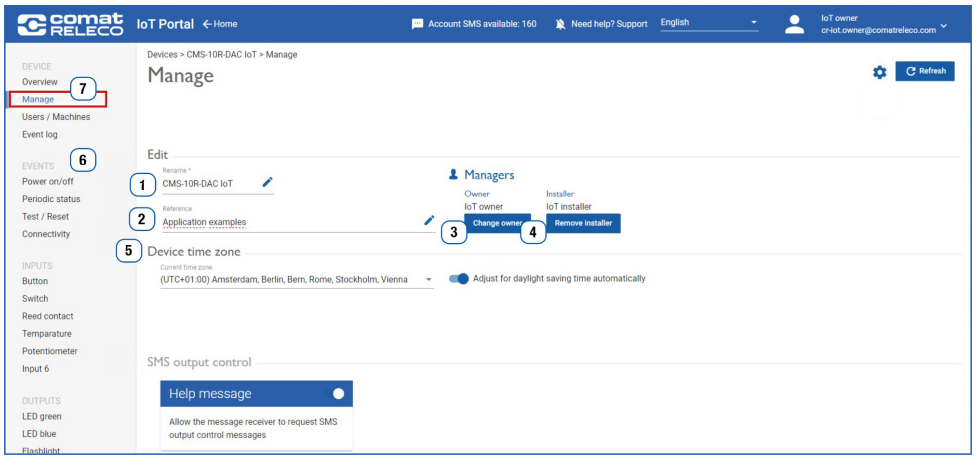


Figure 6.4: Menu Manage.

1. Change the device name.
2. Change the device reference.
3. Change the owner. Only the current owner can do this; see Section 6.2.2.1, Change owner / Remove installer.
4. Remove the installer. Only the owner or installer can do this. Once the installer is removed, **Add installer** appears; see Section 6.2.2.1, Change owner / Remove installer.
5. Set the **current time zone** for the device location. Choose whether to **adjust for daylight saving time automatically** (DST).

Set the time zone before scheduling reports

- A new device defaults to Coordinated Universal Time (UTC). Change this setting to suit the device location. Selecting a time zone other than UTC activates DST automatically; you can then disable DST if required.
- The time-zone setting ensures that the times entered for **Periodic status report** in **Manage** and **Inputs** correspond to the local time at the device.

6. Configure events; see Section 6.2.6, Configure notifications and acknowledgement: Events.
7. Manage the device; see Section 6.2.2.3, Manage your device.

6.2.2.1 Change owner / Remove installer

Only the current owner can transfer ownership.

1. Select **Change owner** (Figure 6.4, item **3**).
2. The proposed new owner receives an owner invitation by e-mail.
3. If the new owner already has an IoT Portal account (**Case A**), they use the link to accept or reject the invitation. If they do not have an account (**Case B**), they must create one before accepting or rejecting the invitation via the link.

- The invitation is valid for **30 days**. After this period, it is set to **Ignored** and is no longer valid.
- The current owner remains active until the new owner accepts the invitation.
- To remove installer access, select **Remove Installer** (Figure 6.4, item **4**).
- Use this function when installation and configuration are complete and the installer no longer needs device access.

6.2.2.2 SMS output control

Request available SMS switching commands

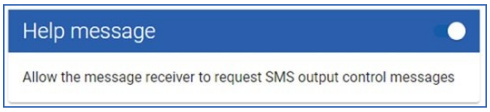


Figure 6.5: SMS output control help message.

You can allow message receivers to request the available output control messages by **SMS**.

1. Send **Help** by SMS to the device telephone number (Figure 6.3, item **11**).
2. The requester receives the current **SMS control messages** for every output whose message is activated (Figure 6.20, item **5**).

Any user can request an output control message, even if they are not entered in the **Message receiver** window.

Activate the **Help** message if you need to query these messages in fallback mode; this is the recommended setting.

Select **Apply** to save the settings. Selecting **Close** does not apply them.

6.2.2.3 Manage your device

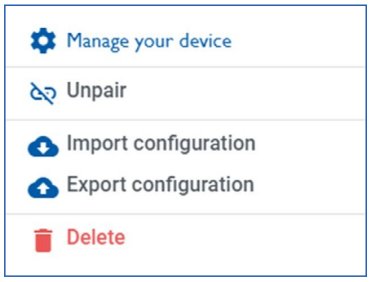


Figure 6.6: Device management functions.

Use these functions to back up, transfer, unpair or delete a device:

- **Unpair**: Disconnect the device from the owner account. The device can no longer be used after unpairing. Allow up to **10 minutes** for the status to appear in the IoT Portal.
- **Import configuration**: Transfer a configuration from an old CMS-10 or another CMS-10R. Check every value after importing.
- **Export configuration**: Save the current configuration as a backup or for transfer to another device.
- **Delete**: Delete the device entry. Unpair the device first.

6.2.2.4 Importing the configuration from an old device

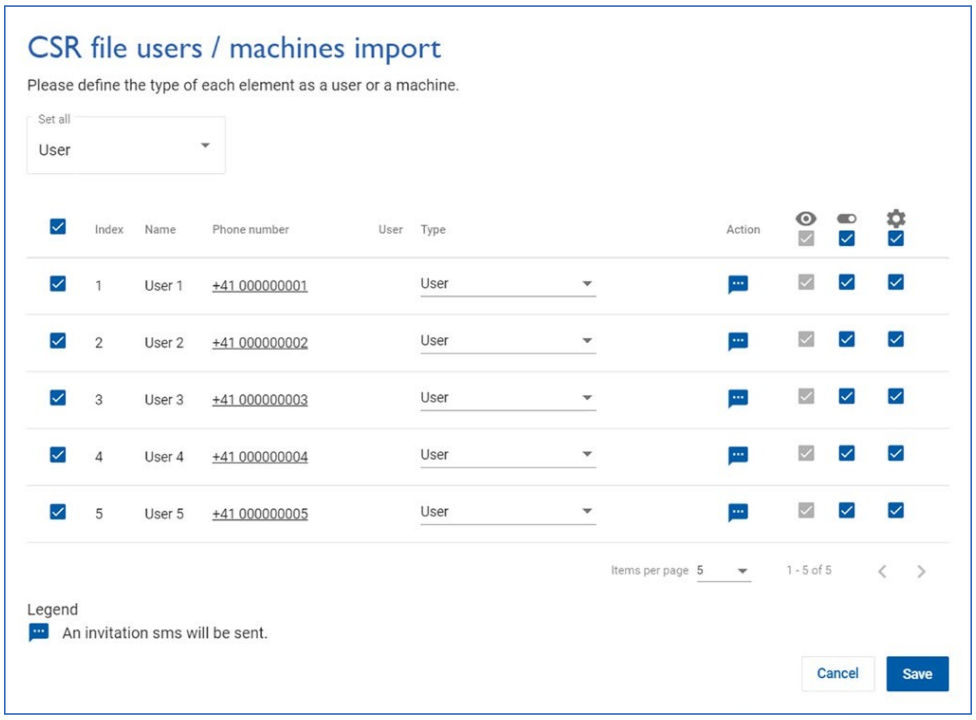


Figure 6.7: Importing the configuration from an old device.

- When importing an old **CMS-10** configuration, select the type (**user** or **machine**) and rights (**View status**, **Control device**, **Manage device**). Set them individually or apply them to all entries.
- Check **Action** for the note indicating that an invitation SMS has been sent to the corresponding number.

6.2.3 Give users and machines access: Users / machines

- To configure the device, you must be an **Installer**, an **Owner**, or a user with **"Manage Access"** privileges.
- Use this menu to view the registered **users** and **machines**.

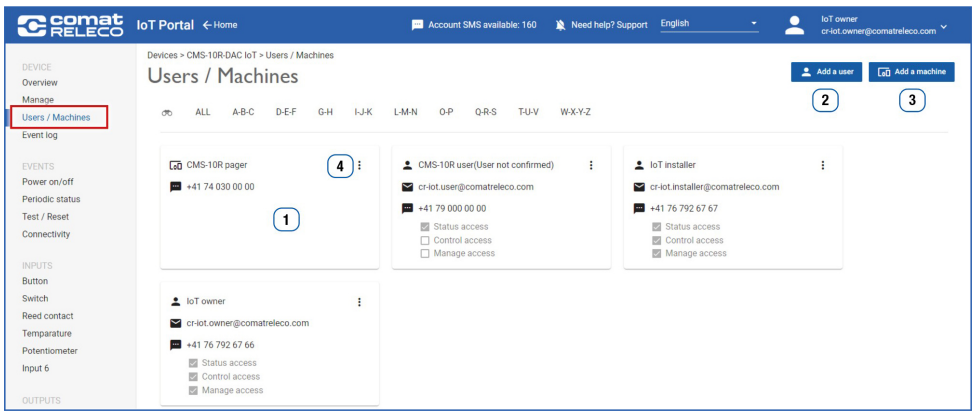


Figure 6.8: Menu Users / machines.

1. Business card for each **user** / **machine**
2. Add a **user**

3. Add a **machine**
4. Menu item: **Edit user** / **Delete user**

6.2.3.1 Add / edit users

- Before adding users, check the user limit of the selected **service profile**; see Section 6.2.8, Manage the service profile: Service profile.
- Select the rights for each user according to the access they need:

Rights	Possible functions
Status access	• View all input and output states in **Overview**; see Section 6.2.1, Check device status: Overview. • Receive and acknowledge messages
Control access	• View all input and output states in **Overview**; see Section 6.2.1, Check device status: Overview. • Receive and acknowledge messages • Control the relay outputs
Manage access	• View all input and output states in **Overview**; see Section 6.2.1, Check device status: Overview. • Receive and acknowledge messages • Access all management options

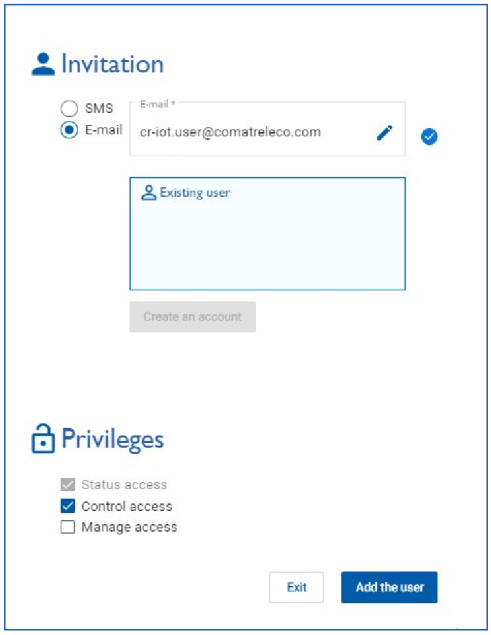


Figure 6.9: Add or edit users - Case A.

1. Select **Add a user** (Figure 6.8, item **2**).
2. Choose **SMS** or **e-mail** and enter the mobile phone number or e-mail address.
3. Select the user's rights from the options described in the preceding table.
4. **Case A:** If the user already has an IoT Portal account, select **Add user**. The user is added immediately.

Language selection for invitations

- Select the **invitation language** when inviting a new user.
- This option is available only if the invited user does not already have an account.
- You can also select the invitation language when inviting a new device owner.

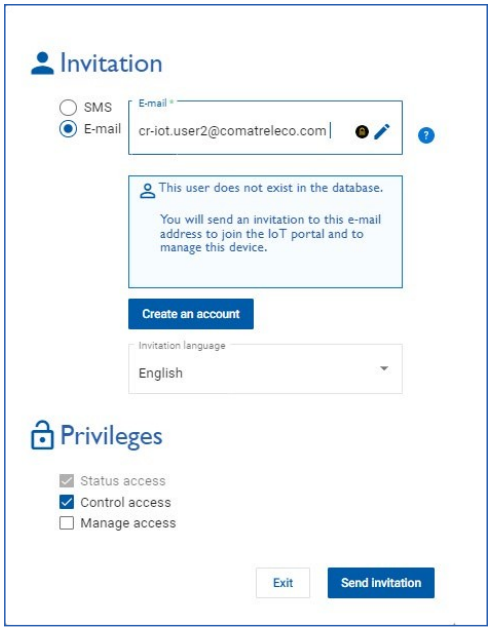


Figure 6.10: Add or edit users - Case B.

Case B: If the user does not yet have an IoT Portal account, choose one of the two options below.

- Select the required user rights; see Section 6.2.3.1, Add / edit users.

Case B1: Select **Send invitation**.

- The user receives an invitation code by SMS or e-mail. They log in to the IoT Portal and use the code to add the device.
- The invitation expires after **30 days**. If it expires, send it again under **User**.

Case B2: Select **Create account**.

- Enter the required information to create the new user account directly.
- The user receives the login credentials and an account-confirmation link by e-mail.

Unconfirmed user

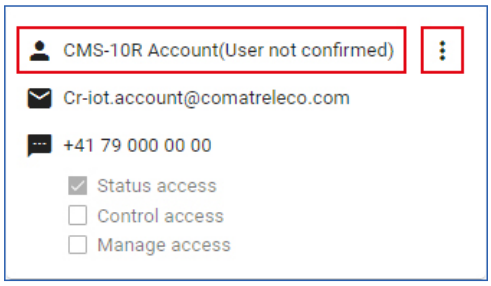


Figure 6.11: Unconfirmed user.

- Until the invited user confirms the account, their business card shows **User not confirmed**.
- To resend the invitation code by e-mail or SMS, select **Edit**.

Change user rights

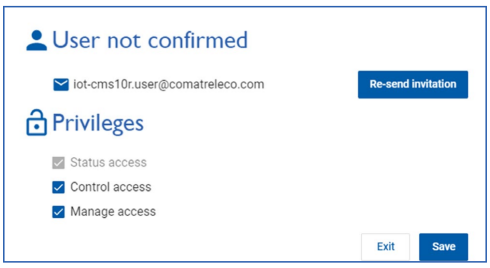


Figure 6.12: Change user rights.

1. Open **Edit** on the user's business card (Figure 6.8, item **4**).
2. Select the required rights; the options are described in Section 6.2.3.1, Add / edit users.

Change a user's e-mail address or telephone number in that user's account, rather than in this rights window; see Section 7.2.1, Menu: Profile.

6.2.3.2 Delete user

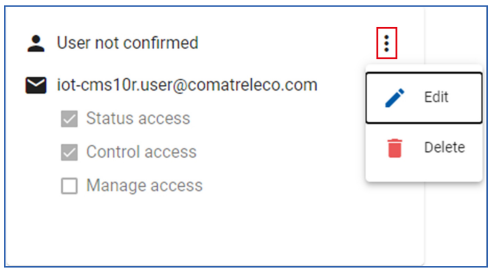


Figure 6.13: Delete user.

- Select **Delete** and confirm the security prompt to remove the user's business card and their access to this device.

6.2.3.3 Add / Edit / Delete machine

- Use a machine entry for a telephone server, alarm server or pager system, such as a paging receiver or radio paging receiver.
- The device sends messages to the machine. The machine can forward them automatically to message receivers such as on-call services or emergency organisations.
- An SMS sent to a machine contains only the message text. It excludes the device name, input/output names, and analogue input values and units.
- E-mails to a machine contain the same information as e-mails to a user.

Machine-to-machine SMS sender numbers

For security reasons, the SMS sender numbers used for machine-to-machine communication are provided on request. Please contact **ComatReleco Technical Support** to obtain the numbers required to configure your receiving system.

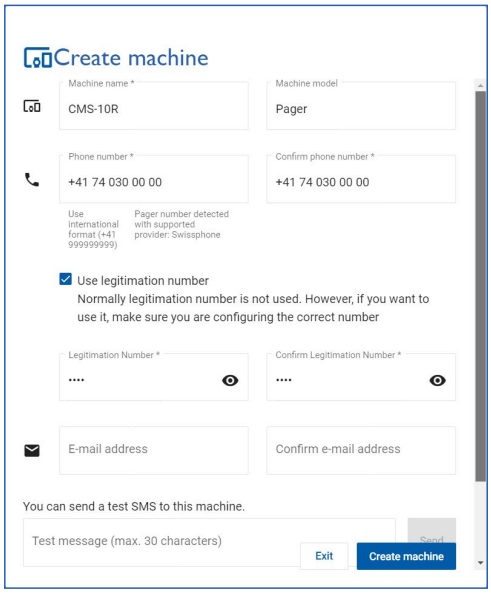


Figure 6.14: Add machine.

Add machine

1. Select **Add a machine** (Figure 6.8, item **3**).
2. Enter the machine's telephone number or e-mail address.
3. Enter it again in the second field to confirm it. A machine cannot respond to an account-confirmation e-mail as a user can.
4. Use the lower part of the window to send a message or test SMS and check reception.

Legitimisation number for pagers: If your pager provider, for example **Swissphone**, stores a unique identification number for the pager system, enter it as the **legitimisation number**.

Each pager notification deducts **1 SMS** from the SMS account.
Messages to machines use **UCS2** by default. A message containing only **GSM7** characters uses **GSM7**.
The legitimisation number must contain at least **4 numbers**.
You can configure any telephone number for a machine, including a landline/fixed telephone number.

If pager notifications are enabled without a pager number associated with the account, an alarm message is still sent and one SMS is deducted. The message is not received and no notification is delivered.

For machine messaging, use the following English-language opt-out, opt-in and help keywords:

- **STOP** prevents notification and adds the recipient to the blacklist.
- **START** starts notification.
- **HELP** provides help.

Message and data charges may apply.

6.2.4 Configure input monitoring: Inputs

Before configuring an input, check the device type selected when the device was created. It determines which input functions are available:

Type and scope of functions

Type	Scope of functions
CMS-10R-D	6 digital voltage inputs Input voltage range: **95–240 V** ~
CMS-10R-DA	6 digital or analogue voltage inputs, switchable Input voltage range, digital: **10–48 V** ⎓ Input voltage range, analogue: **0–10 V** ⎓
CMS-10R-DAC	4 digital or analogue voltage inputs, switchable Input voltage range, digital: **10–48 V** ⎓ Input voltage range, analogue: **0–10 V** ⎓ 2 current inputs, **I5** and **I6**: **4–20 mA** ⎓

Each input channel is sampled at **10 Hz**.
Signals lasting less than **100 milliseconds** at an input are not detected.

6.2.4.1 Configure digital inputs

Use the numbered controls in Figure 6.15 to set up a digital input and its high/low messages.

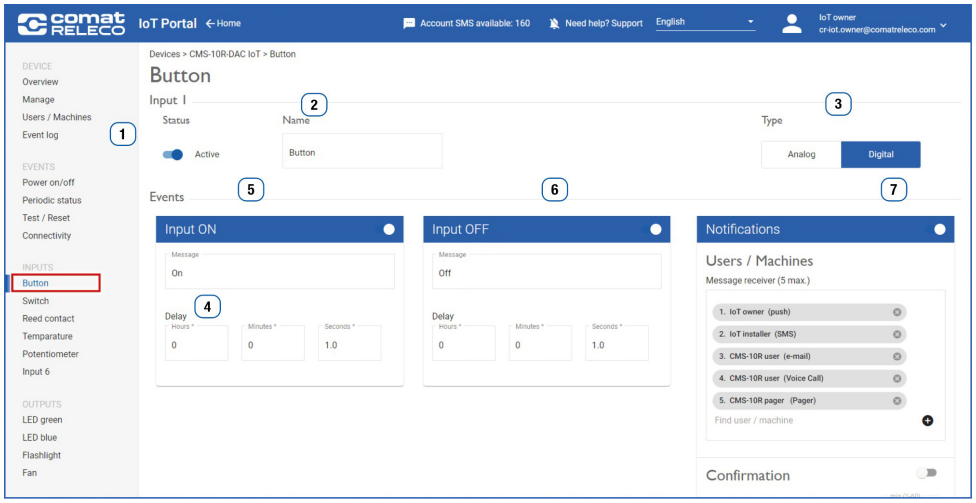


Figure 6.15: Configure digital inputs.

1. Activate or deactivate the input.
2. Enter the input name.
3. Select **digital** or **analogue**, according to the device type. Digital is selected by default.
4. Set the digital input event message delay.
5. Enter the message for a controlled input (input high).
6. Enter the message for an input that is not controlled (input low).
7. Select message receivers and channels with **(+)**. Configure acknowledgement as described in Section 6.2.6, Configure notifications and acknowledgement: Events.

Event message delay for digital inputs Set a message delay for each digital input event. The message is sent to the user only after the delay has elapsed.

Enter the delay in **hours**, **minutes** and **seconds**.

The message delay limits are:
- **0–99 hours**
- **0–59 minutes**
- **0–59.9 seconds**
- maximum **99:59:59.9**

The minimum value is **0.5 seconds**.
The default value is **1.0 second**.

- Select **Apply** to apply the settings.
- Selecting **Close** does not apply the settings.
- If several inputs change state at the same time, separate messages are sent for each input and each activated event.
- Input state changes that generate messages are processed in their order of occurrence. Several messages can be triggered at the same time.
- Example: Separate inputs report **Pump failure** and **Excess temperature** simultaneously. The resulting messages are processed and sent one after the other.

6.2.4.2 Configure analogue inputs

Select **Analogue** for each input that you want to use for analogue measurements.

Analogue inputs accept standardised voltage signals of **0–10 V** ⎓ or current signals of **4–20 mA** ⎓, compliant with **IEC 60381-1/-2**.

The resolution is:

- **12.5 mV** ⎓ for voltage input
- **20 µA** ⎓ for current input

To display a voltage input in another unit, such as temperature, enter the minimum and maximum display values for that unit in **Value**.

The IoT Portal converts the voltage automatically into the selected unit.

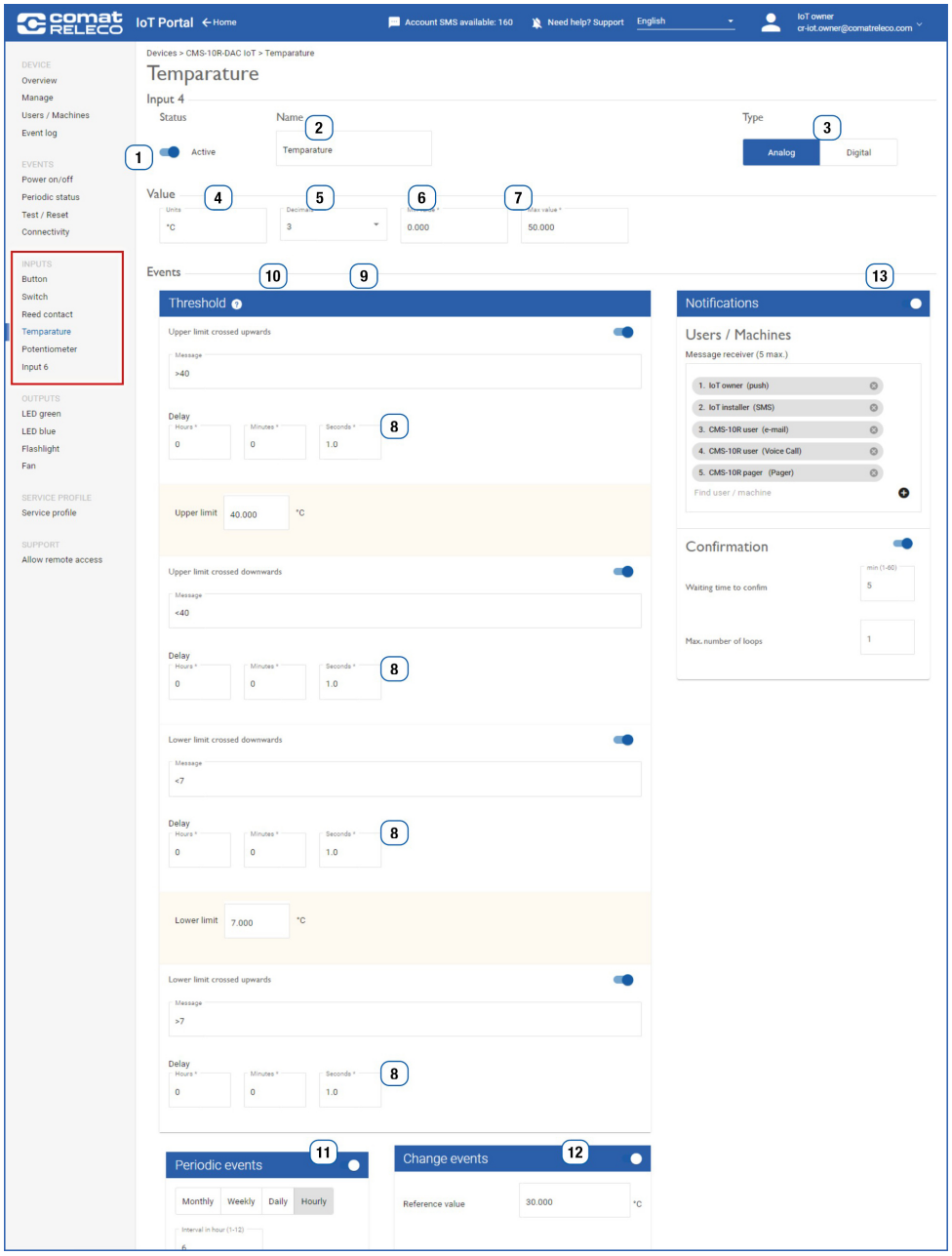


Figure 6.16: Configure analogue inputs.

1. Activate or deactivate the input.
2. Enter the input name.
3. Select **digital** or **analogue**, according to the device type.
4. Enter the unit, for example **m**, **V**, **°C** or **%**.
5. Select **0–3** displayed decimal places.
6. Enter the minimum display value for **0 V** ⎓ or **4 mA** ⎓.
7. Enter the maximum display value for **10 V** ⎓ or **20 mA** ⎓.
8. Set the analogue input event message delay.
9. Enter the upper and lower limits and their messages.
10. Select the question mark to open the graphical explanation of the limits.
11. Configure periodic sending of activated messages.
12. Configure change events.

13. Select message receivers and channels with **(+)** and set acknowledgement; see Section 6.2.6, Configure notifications and acknowledgement: Events.

Event message delay for analogue inputs Set a message delay for each analogue input threshold, for example to avoid switch bouncing.

The message is sent to the user only after the delay has elapsed.

Enter the delay in **hours**, **minutes** and **seconds**.

The message delay limits are:
- **0–99 hours**
- **0–59 minutes**
- **0–59.9 seconds**
- maximum **99:59:59.9**

The minimum value is **0.5 seconds**.
The default value is **1.0 second**.

Limit values and messages Activate or deactivate each of the four limit values individually.

- The message includes the analogue input value and unit.
- Select the question mark to view the graphical explanation of the limits.
- Select the graphic again to close the window (Figure 6.19).

Periodic messages

- Send activated messages periodically if required.
- Enter the message and choose a reporting interval, from hourly to monthly.

Each periodic message also transmits the input value and unit.

See also Section 6.2.6.2, Figure 6.27.

Change events

- Define an additional limit value to trigger a change-event message.
- The additional limit can lie within or outside the upper and lower limits.
- Enter the additional limit in **Reference value**.
- Enter the value at which a message is to be sent in **Step**.
- Example: If the **limit value** is **7 V** and the **step** is **2 V**, the message is sent when the voltage falls below **5 V** or exceeds **9 V**.
- Enter the required message in **Message**.

Analogue value processing: measured value is greater than limit value

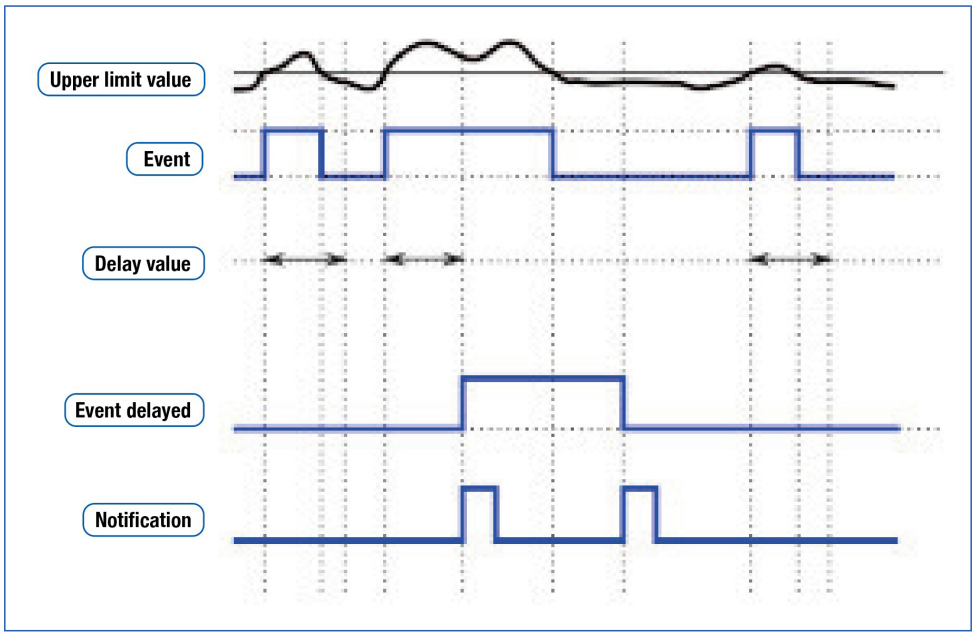


Figure 6.17: Analogue value processing: measured value is greater than limit value.

- The current measured value is above the upper limit value.
- The event is only detected if the measured value has fallen below the lower limit value for longer than the delay value.
- The event is delayed by the delay time.
- The display of the LED at the input is also delayed.
- Notification is given when the upper limit value has been undercut and exceeded again.

Analogue value processing: measured value is smaller than limit value

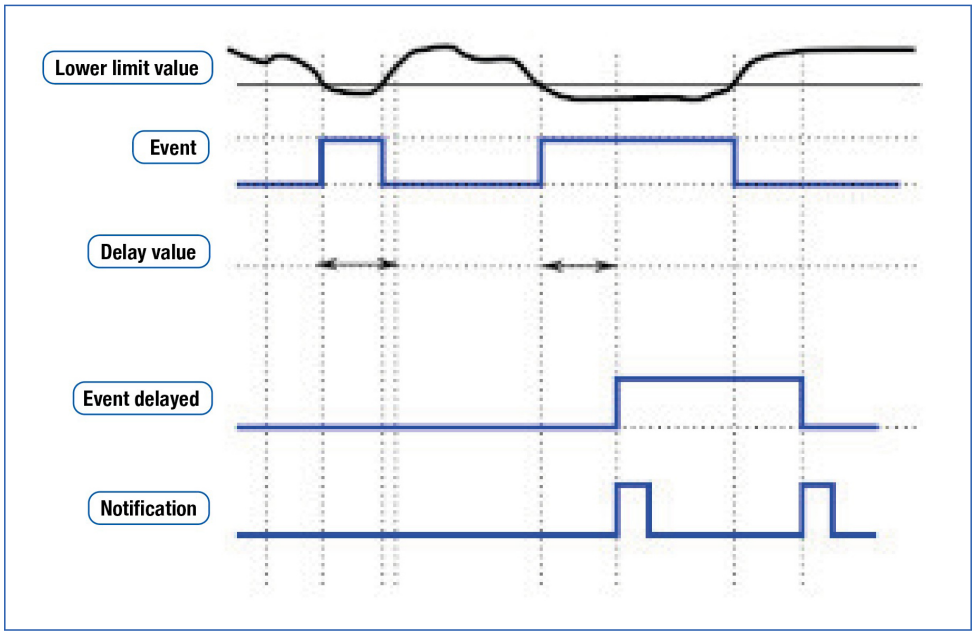


Figure 6.18: Analogue value processing: measured value is smaller than limit value.

- The current measured value is below the upper limit value.
- The event is detected only if the measured value remains below the lower limit value for longer than the configured delay time.
- Event detection is delayed by the configured delay time.
- The LED indication at the input is also delayed.

A notification is triggered when the upper limit value is undershot and then exceeded again.

Graphical view of the interpretation of the limit values Select the question mark (Figure 6.16, item **10**) to open this graphic. Select the graphic to close it.

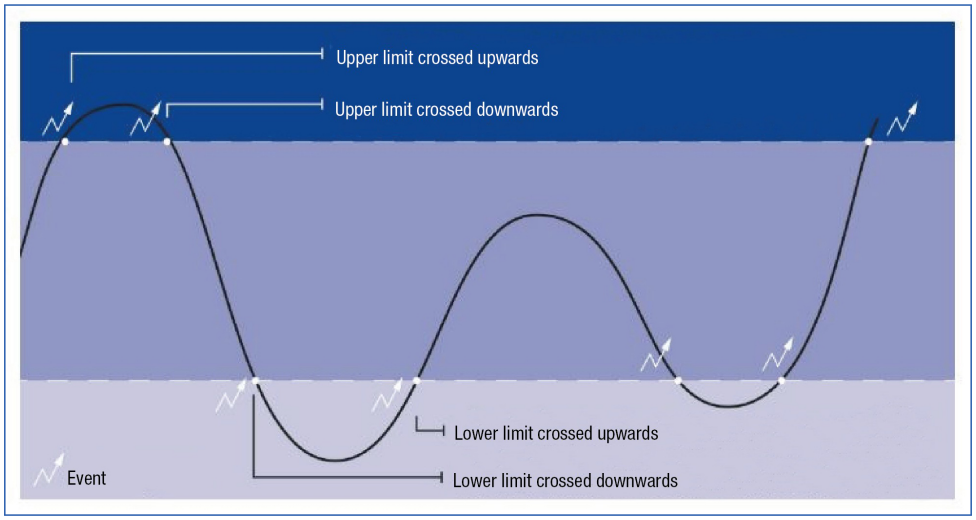


Figure 6.19: Graphical view of the interpretation of the limit values.

6.2.5 Configure and control relay outputs: Outputs

This device is not suitable for monitoring sensitive systems or time-critical processes. Mobile network failures or interruptions in the power supply can impair safe operation.

You can switch the four relay outputs on or off from the IoT Portal, the app, an SMS or a call-in telephone call.

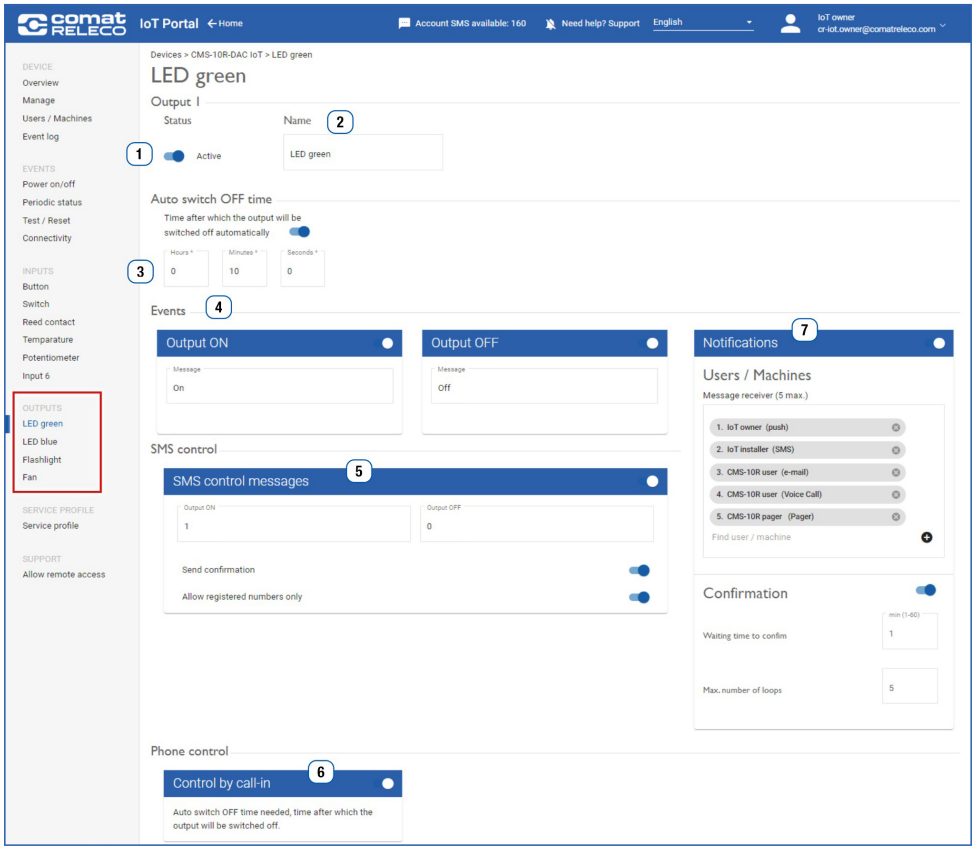


Figure 6.20: Menu Outputs.

1. Activate or deactivate the output.
2. Enter the output name.
3. Auto turn off
4. Events
5. SMS control messages

Auto turn off Use automatic switch-off to turn an output off after a set time, without sending a switch-off command from the IoT Portal, app, SMS or call-in.

- Set a switching time from **0.5 seconds** to **99:59:59.9** in the format **hh:mm:ss.s**.
- When the output switches off after the set time, a message confirms the action.
- A switch-off command sent before the timer expires is still taken into account.
- The **time** function is disabled by default.
- Enable **Events** and **notifications**.

Events Activate or deactivate each output individually.

- Enter the message to send when the output is switched.

SMS control messages To switch an output on or off by SMS, configure its switching command text.

- The device responds only to the configured wording.
- The SMS message (switching command) must match **Output on** or **Output off** exactly.
- Letter case is ignored.
- Enter spaces and all other characters exactly as configured.

Switch multiple outputs with the same SMS control message Configure simultaneous switching in the digital output settings under **SMS Control** > **SMS Control Messages**.

- Use the same SMS control message to switch several outputs at the same time.
- Enter the same message in **Output on** or **Output off** for each output, then select **Apply**.
- A warning indicates that the same control message is used for more than one output (Figure 6.21).
- If **Auto turn off** is set, the output switches off after that time (Figure 6.20, item **3**).

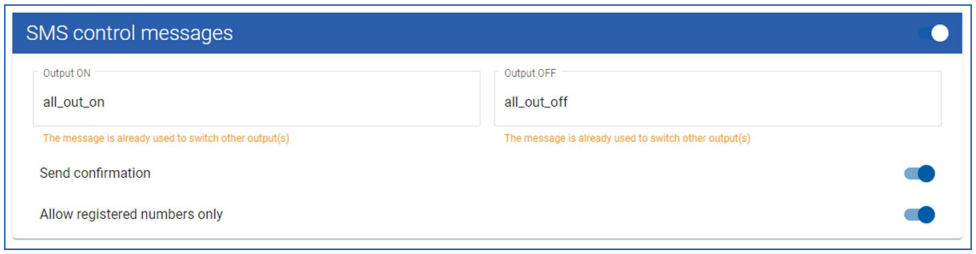


Figure 6.21: Switching multiple outputs with the same SMS control message.

SMS messages do not support all special characters. The programming software identifies unsupported characters with an error message. Remove them.

Choose any control message that meets these restrictions:
- The character set is **Latin 1**
- Maximum length: **30 characters**
- The semicolon **;** is not allowed

Enable **Send confirmation** to return an SMS containing **Output ON** or **Output OFF** to the sender of the switching command.

Enable **Allow only registered numbers** to accept switching commands only from telephone numbers registered in **Users** / **Machines**.

If this setting is disabled, anyone who knows the device telephone number can control the outputs from any telephone number.

For security reasons, only registered telephone numbers should be allowed whenever possible.

Examples:

- Switch on all outputs simultaneously: message in each **Output on** field: **all_out_on**
- Switch off all outputs simultaneously: message in each **Output off** field: **all_out_off**

Call-in function Use the **Call-in function** to switch each activated output on by caller identification for the period entered in **Auto turn off**.

Before you start: The calling mobile telephone number must be registered in **Users** / **Machines**.

Configure call-in

1. Enable **Auto turn off** for the output and set the required time.
2. Activate **Control by call-in**. If **Auto turn off** is disabled, selecting **Apply** displays a message.
3. Select message receivers and channels with **(+)** and configure acknowledgement (Figure 6.23).
4. Select **Apply** to apply the settings. Selecting **Close** does not apply them.

Use call-in

Find the device telephone number in **Overview** (Figure 6.3, item **11**) and call it from a registered mobile telephone number.

- The device detects the incoming call and switches the outputs on without answering. This allows an action without incurring costs.
- The device rejects the call. You may hear a busy signal, depending on the telephone provider; call-in still executes correctly.
- The outputs switch off automatically after the preset time.

6.2.6 Configure notifications and acknowledgement: Events

For notification charges, SMS credit consumption and event allowances, see Section 7.1.

Use **Events** (Figure 6.22) to configure notifications for device events. Five notification methods are available:

- E-mail
- Push
- SMS
- Voice call
- Pager

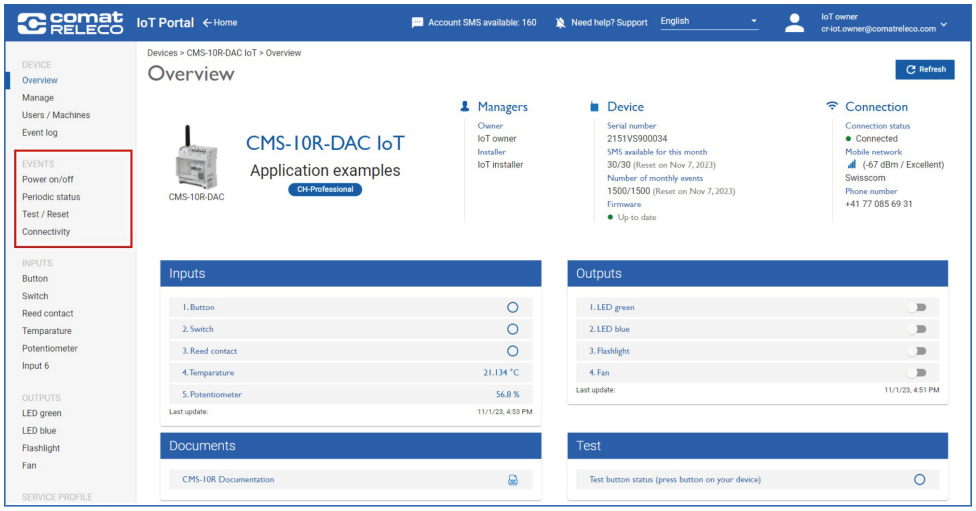


Figure 6.22: Menu Events.

SMS and pager messages do not support all special characters. Remove any character identified by an error message.

Activate or deactivate each event using the slide button on the right of its bar.

An SMS using the GSM standard coding alphabet can contain up to **160 characters**. If the message contains characters outside that alphabet, such as special characters, Greek letters or Cyrillic characters, the system switches automatically to **UCS-2** coding.

With UCS-2, the maximum SMS length is **70 characters**. Longer messages are sent as concatenated SMS messages, and one SMS is deducted for each segment.

Message recipient

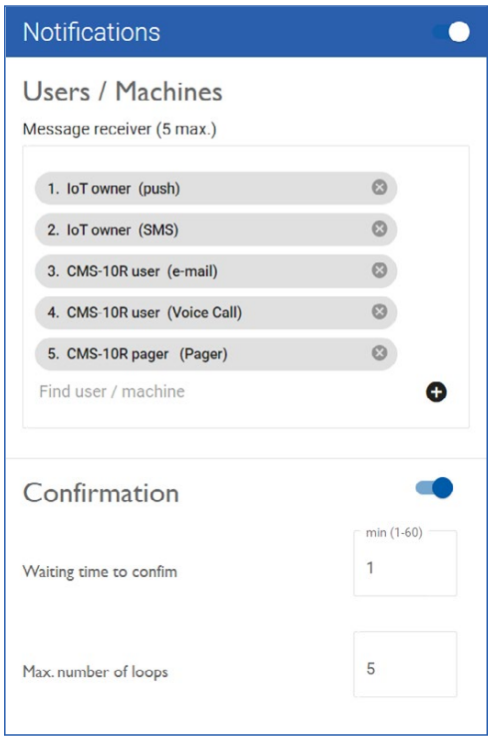


Figure 6.23: Message recipient configuration.

- Select **(+)** to choose the recipients of activated messages and the notification channel for each recipient.
- With **acknowledgement** enabled, the list of message recipients forms an **escalation chain**.
- Notifications can be sent via:
  - Push
  - SMS
  - Pager
  - E-mail
  - Voice call

Arrange the users / machines in the required order using drag & drop. The recipient limit depends on the service profile:

Service profile	Maximum message recipients
Eco	2
Standard	5
Professional	5
Expert	5

Acknowledgement Enable **acknowledgement** when a recipient must confirm receipt of an event message.

1. The IoT Portal sends the event message to the assigned recipient.
2. If the recipient does not acknowledge via push, SMS, e-mail or voice call within the configured waiting time, the message is sent to the next recipient.
3. The IoT Portal works through the recipient numbers cyclically and starts again at the first number, subject to the service profile's maximum number of passes.
4. The process stops as soon as the device receives an acknowledgement.

Use the acknowledgement method for the notification channel:

Notification method	Acknowledgement method
Push	Click on the message
SMS	Sent code
E-mail	Sent link
Voice call	**1#**

The service profile limits the number of passes through the recipients while a message remains unacknowledged:

Service profile	Maximum passes
Eco	1
Standard	3
Professional	5
Expert	5

With acknowledgement **not activated**, all listed recipients receive the message at the same time. The message is not repeated.

Set the acknowledgement waiting time between **1 and 60 minutes**.

The same recipient and acknowledgement window is available for inputs and outputs.

Acknowledging a message opens a new browser window if the IoT Portal is already open.

In fallback mode, the acknowledgement code is: **code**.

All message recipients receive the acknowledgement message **OK: Mobile phone number**.

6.2.6.1 Menu: Power on / off

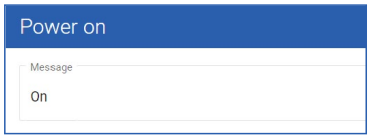


Figure 6.24: Menu Power on / off: power on message.

Power on

- Enter the message to send after device startup.

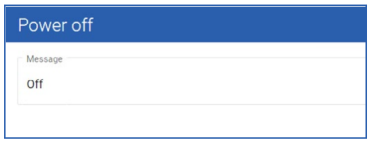


Figure 6.25: Menu Power on / off: power off message.

Power off

- Enter the message to send after a power failure or restart.
- The message is sent before the device switches off.
- The device switches off in the following cases:
  - a prolonged power failure occurs
  - the watchdog detects a malfunction
  - the device is restarted manually by pressing **Reset** for less than **4 seconds**
  - a firmware update is performed
- Power failures lasting **1 second or less** are not recognised by the power supply and do not change the device status.
- Power failures lasting **more than 1 second** are recognised. Depending on the settings, a notification is sent via push, SMS, pager, e-mail and voice call. The device then switches itself off.
- After a power failure, the device restarts automatically and logs on to the mobile network. The initial status is then restored.

The relay outputs remain de-energised throughout the power interruption.
Example: contact **11-14 = open**, contact **11-12 = closed**.

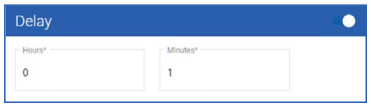


Figure 6.26: Minimum interval for generating the notification.

Minimum interval for generating the notification

- Use this setting to delay power on/off event messages.
- The message is sent to the user only after the delay has elapsed.
- Enter the required delay. The values below use the **hh:mm:ss** format (hours:minutes:seconds).

The limit values for the signalling delay are:
- **0–99 hours**
- **0–59 minutes**
- maximum **99:59:00** (99 hours, 59 minutes, 0 seconds)

The minimum value is **00:01:00** (**1 minute**).
The default value is **00:01:00** (**1 minute**).

6.2.6.2 Menu: Regular status

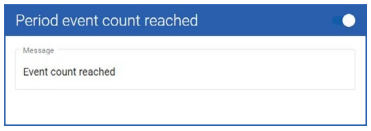


Figure 6.27: Menu Regular status.

Periodic number of events reached

- When the maximum number of events for the selected service profile is reached, this is the only message sent even without an event quota. See Section 6.2.8, Manage the service profile: Service profile.

This message is sent once, unless the device is restarted.

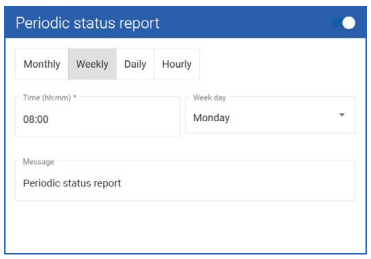


Figure 6.28: Menu Regular status: periodic status report.

Periodic status report

- Use this function to monitor device operation.
- Enter the report message and configure when the device should report.

Every hour:

- Select a reference interval of **1–12 hours**.
- Example: An interval of **5 hours** sends messages at **00:00, 05:00, 10:00, 15:00, 20:00**, then again at **00:00**.

Daily, weekly, monthly:

- Enter a time (**hh:mm**), weekday (**Monday–Sunday**) or day of the month (**1–31**). These refer to the local time at the device.
- The UTC time entered in **Manage** is converted automatically according to the device location and daylight saving time; see Section 6.2.2, Manage device settings and ownership: Manage.

Check the available monthly events in Figure 6.3, item **7**, before choosing a report interval. Short intervals can trigger many events. Make sure the monthly quota is not exceeded.

6.2.6.3 Menu: Test / Reset

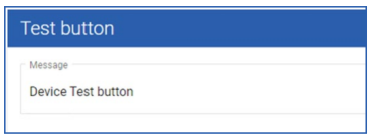


Figure 6.29: Menu Test / Reset. A

Test button

- Enter the message to send when the device's **Test** button is pressed; see Section 3.4, Locate terminals, controls, and status indicators, item **11**.

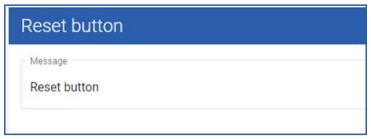


Figure 6.30: Menu Test / Reset. B

Reset button

- Enter the message to send after the device's **Reset** button is pressed.

Case A: Short press (< 4 seconds): restart

- To restart the device, press **Reset** for less than **4 seconds**.
- The device shuts down safely and then reboots. Allow up to **one minute**.
- The following events may be generated: **Reset button**, **Shutdown**, **Disconnected**, **Connected** and **Startup**.
- Enable these **Events** under **Manage**.

Case B: Long press (> 4 seconds): forced hardware reset

- To perform a forced hardware reset, press **Reset** for more than **4 seconds**. The device restarts immediately.
- The following events may be generated: **Reset button**, **Shutdown**, **Disconnected**, **Connected** and **Startup**.
- Enable these **Events** under **Manage**.

6.2.6.4 Menu: Connection

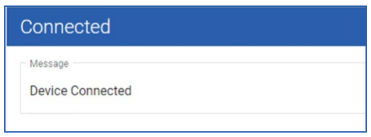


Figure 6.31: Menu Connection.

Connected to the IoT Portal

- Enter the message to send when the device connects to the IoT Portal.

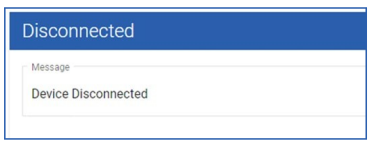


Figure 6.32: Menu Connection.

Disconnected from the IoT Portal

- The device operates in fallback mode; see Section 3.8, What happens during interruptions, resets, and updates.
- Enter the message to send when the device disconnects from the IoT Portal.

6.2.7 Review and export activity: Event Log

Use **Event Log** to review and export historical **Events**, **Notifications** and **System operation** data. Each category is displayed in a table.

You need **Manage access** rights to use this function for **My owned devices**, **My assigned devices** or **My installed devices**.

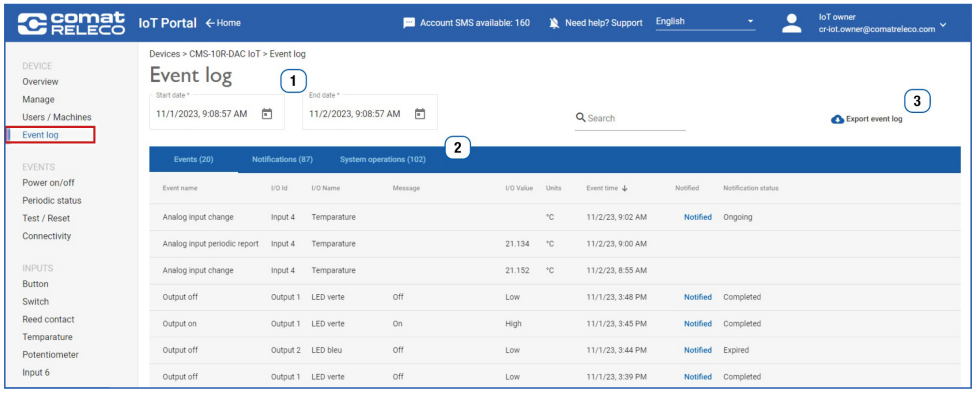


Figure 6.33: Menu Event Log.

Check the retention period for the selected **Service profile** before searching for older data:

Service profile	Retention time
Eco	14 days
Standard	45 days
Professional	90 days
Expert	90 days

1. Set **Start date** and **End date** to define the search period.
2. Use **Search** with a keyword or filter to find the relevant event.
3. Check the counts displayed as **Events (xx)**, **Notifications (xx)** and **System operation (xx)**.
4. To export the selected data as a **.csv** file, select **Export Event Log**.

Events: The **Events** tab uses the event names and descriptions below.

Event name and description

Event name	Description
Startup	System started
Shutdown	System shutdown
Test button	Test button pressed
Reset button	Reset button pressed
Periodic event count reached	Event count reached
Periodic status report	System periodic event
Connected	Connected to the IoT Portal
Disconnected	Disconnected from the IoT Portal
Input high	Digital input high
Input low	Digital input low
Upper limit crossed upwards	Analog input crosses the upper limit upwards

Event name	Description
Upper limit crossed downwards	Analog input crosses the upper limit downwards
Lower limit crossed downwards	Analog input crosses the lower limit downwards
Lower limit crossed upwards	Analog input crosses the lower limit upwards
Analog input change	Analog input level changed
Analog input periodic report	Analog input periodic reporting
Output on	Digital output high
Output off	Digital output low

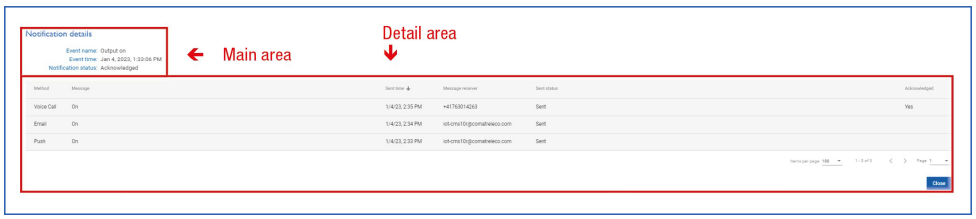


Figure 6.34: Notification details pop-up window.

Use the **Notification details** pop-up window to review the notifications associated with an event (Figure 6.34).

The upper part shows the **event name**, **event time** and **notification status**.

The lower **details area** lists the associated notifications in a table with the fields **Method**, **Message**, **Sent time**, **Message receiver**, **Sent status** and **Acknowledged**.

The following table explains the notification fields.

Notifications: Field name and description

Field name	Description
Method	Shows the method used to send the notification, see also Section 3.8, What happens during interruptions, resets, and updates. • SMS • E-mail • Push • Voice call • Pager
Serial number	Serial number of the device.
Device name	User-defined device name.
Related event	Shows the event name label of the event that generated the notification message. When the related event is linked to an input or output, this field also includes the input/output information in the following format: `<event-name-label>, <user-defined-input/output-name>, <input/output-id>`
Message	Shows the message content of the notification.
Event time	Shows the date and time when the event occurred. The format is: `yyyy-MM-dd hh:mm:ss`
Sent time	Shows the date and time when the notification was sent from the IoT Portal. The format is: `yyyy-MM-dd hh:mm:ss`

Field name	Description
Destinator	Shows the user or machine to which the notification was sent. • For e-mail notifications, the destinator e-mail address is displayed. • For push notifications, the e-mail address of the destinator user is displayed. • For SMS notifications, the destinator phone number is displayed. • For voice call notifications, the destinator phone number is displayed.
Sent status	Shows the sent status of the notification. For pager notifications, the recipient's telephone number is displayed.
Acknowledged	If the notification message has been acknowledged, this field displays **Yes**. Otherwise, the field remains empty.

System operation:

Use the following definitions to interpret entries in the system operations tab.

Operation name and description

Operation name	Description
Set output high state	Occurs when the user switches on an output in the **Devices > device-name > Overview** screen of the IoT Portal.
Set output low state	Occurs when the user switches off an output in the **Devices > device-name > Overview** screen of the IoT Portal.
Input configuration update	Occurs when the user updates the input configuration in the **Devices > device-name > input-name** screen.
Output configuration update	Occurs when the user updates the output configuration in the **Devices > device-name > output-name** screen.
Manage configuration update	Occurs when the user updates the device system configuration in the **Devices > device-name > Manage** screen.
Users / Machines update	Occurs when the user updates the **Users** / **Machines** configuration in the **Devices > device-name > Users** / **Machines** screen.
Import configuration	Occurs when the user uploads an existing device configuration in the **Import configuration** pop-up window.
Export configuration	Occurs when the user exports the device configuration.
Firmware update	Occurs when the user updates the firmware version of the device.
Pair device	Occurs when the user pairs a virtual device with a physical device.
Unpair device	Occurs when the user unpairs a virtual device from a physical device.
Incoming call	Occurs when the user makes a phone call to the device.
Incoming SMS	Occurs when the user sends an SMS message to the device or when the user tests an SMS message when creating a machine.



Messages sent in fallback mode are not logged.

6.2.8 Manage the service profile: Service profile

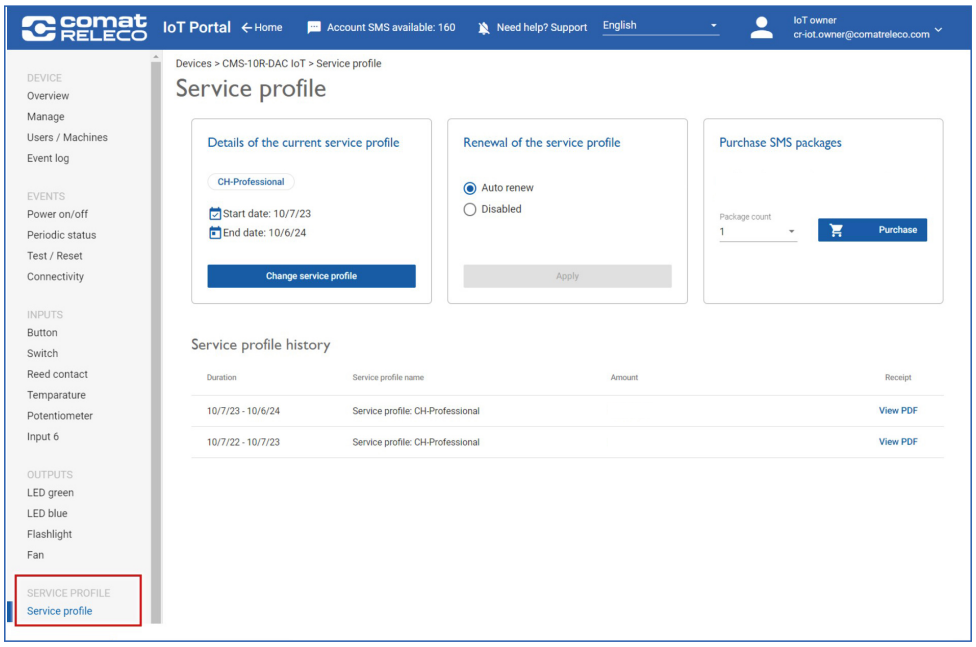


Figure 6.35: Menu Service profile (prices and package sizes omitted).

To see **Service profile**, log in as the device owner and select a service profile; see Section 5.4, Select a service profile and SMS packages.

6.2.8.1 Details of the current service profile

- Select a service profile from the available variants.
- The service profile and its included quotas, such as events and SMS, are tied to that device.
- The service profile starts at the first device pairing. Unpairing and pairing the device again later does not change that start point.
- You cannot stop or interrupt the service profile during its term.

You can select a higher service profile at any time after selecting a service profile.
You can downgrade only after the one-year contract period expires.
Disable automatic renewal before downgrading. Otherwise, the same service profile renews automatically.

- The service profile runs until contract expiry and cannot be cancelled during the term.
- You receive a request to renew before the contract expires.
- If you do not renew the contract, the device becomes inactive. Select a service profile to reactivate it.

6.2.8.2 Service profile extension

- Choose whether to renew the service profile automatically.
- Automatic renewal is enabled by default.
- Leave **Auto renew** enabled for uninterrupted operation; this is the recommended setting.

- You cannot downgrade during the one-year term. The service profile can only be changed within **30 days** after expiry.
- The device becomes inactive thirty days after expiry.
- To reactivate an inactive device, select a service profile.

The owner receives these reminder e-mails:

Reminder e-mail	Description
30 days before renewal / expiry of the service profile	Reminder that the service profile will be renewed or will expire. It can be renewed or modified within 30 days after expiry of the one-year period.
After renewal / expiry of the service profile	Reminder that the service profile was renewed or has expired. If it has expired, it can be renewed or modified within 30 days.
7 days before device being set to inactive	Reminder that the device will become inactive after 7 days if the service profile is not renewed or modified.
1 day before device being set to inactive	Reminder that the device will become inactive after 1 day if the service profile is not renewed or modified.

6.2.8.3 Cancellation of the service profile

- Only the owner can cancel the service profile, and only after the one-year term expires.
- You cannot cancel during the term.
- ComatReleco reserves the right to block the device for provable misuse or non-payment of the purchased service profile.
- The device is unblocked only after the outstanding amount is paid. Charges may apply.

If you do not want to renew, disable **automatic renewal** before the service profile expires.

If you no longer need the device, unpair it as described in Section 6.2.2.3, Manage your device. It can no longer be used after unpairing.

6.2.8.4 SMS packages purchase

- Purchased SMS belong to the owner and can be used across all devices.
- Check the owner's available SMS in the devices overview (Figures 6.1 and 6.2, item **4**).
- Find SMS package invoices under **Account settings > SMS package > SMS package history**; see Section 7.2.3.

6.2.8.5 Service profile history

Use **Service profile history** to view the service profile's **order confirmations**.

Important: The invoice is sent to the customer by e-mail and is not available in the IoT Portal.

To request an invoice copy, e-mail info@comatreleco.com.

6.2.9 Allow a support session: Support

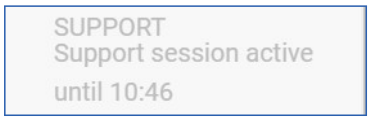


Figure 6.36: Menu Support.

Support session

- Select **Allow remote access** to authorise the ComatReleco support team to access the device for **one hour**; see Section 1.5, Contact details.

6.3 Update the device firmware

Firmware updates are transferred over the mobile network, *over the air*. You can choose when to perform an available update, but you should install it as soon as possible. The update may take a few minutes.

During the installation of a firmware update, the device is out of operation.
Make sure that the device is not used during installation.

Start from the automatic update notification

A pop-up window appears automatically as soon as a firmware update is available.

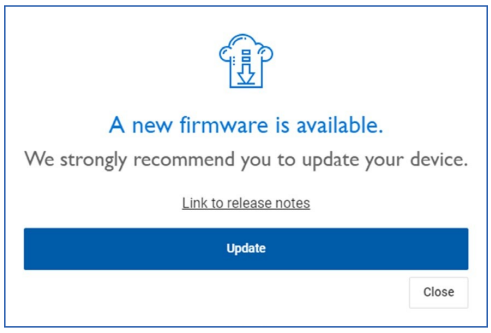


Figure 6.37: Automatic notification of an available firmware update.

1. Select **Update** to start the update process.
2. Follow the instructions that guide you through the process.

Allow a few minutes for the update.

Start from the Manage menu

If the update does not start automatically, open the settings window from **Manage**.

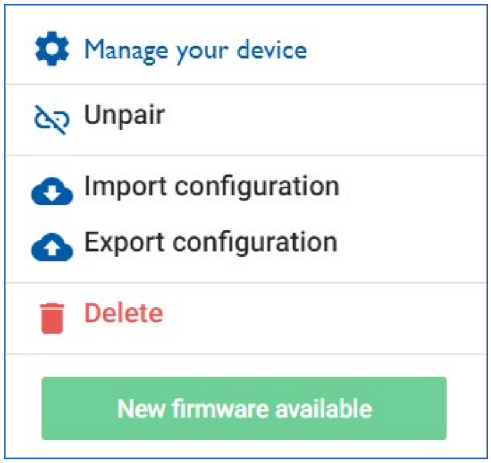


Figure 6.38: Start a firmware update from Manage.

1. Select the cogwheel symbol in **Manage**; see Figure 6.4, item **6**.
2. Check the available firmware update displayed in the settings window.
3. Select **New firmware available** to start the update.
4. Follow the instructions that guide you through the process.

The update may take a few minutes.

Chapter 7

Manage your account and payments

This chapter covers notification usage and allowances, personal account details, account SMS packages, security, billing preferences and payment. Device-specific service profile information remains in Section 6.2.8.

7.1 Notification usage and allowances

The CMS-10R uses two separate resources: **SMS credit** and the **event allowance** of the selected service profile. Depending on the notification method, sending an alarm or message consumes one or both resources.

7.1.1 Usage by notification method

Method	SMS credit used	Events used
SMS	At least one SMS credit per recipient. Each message segment consumes one credit. Included monthly credit is used first, followed by purchased account credit.	One event per alarm.
Voice call	Four SMS credits per call, taken exclusively from purchased SMS packages. Included monthly SMS credit cannot be used.	One event per call.
E-mail	None.	One event per e-mail sent.
Push notification	None.	One event per push notification sent.

E-mail and push notifications consume events but do not use SMS credit. To receive push notifications, install the **ComatReleco IoT Portal app** and enable notifications on the receiving device.

7.1.2 Included SMS credit and additional packages

Depending on the service profile, each device includes **0, 10 or 30 SMS credits per month**. These credits are included in the selected service profile and can be used only by that device.

For SMS notifications, the device uses its included monthly SMS credit first. Once that credit is exhausted, further SMS are deducted from the owner's purchased account credit. Purchased account credit can be used by all devices belonging to that owner.

Additional SMS packages are available for purchase. Purchased SMS credits have **no expiry date** and remain available until used.

For current SMS package prices, package sizes and regional conditions, consult the applicable service profile page:

- CMS-10R service profiles – Switzerland.
- CMS-10R service profiles – Worldwide.

For manual purchases and account settings, see Section 7.2.3.

Voice calls always require purchased account credit: each call consumes four SMS credits from an additional SMS package, even if the device still has included monthly SMS credit available.

7.1.3 SMS length and character encoding

Each recipient of an SMS alarm requires at least one SMS. The actual credit consumption depends on the message length, the characters used and the number of recipients.

A single-part SMS can contain up to **160 characters using GSM standard encoding**, or up to **70 characters using UCS-2 encoding**. Characters outside the GSM standard alphabet, such as certain special characters and Greek or Cyrillic letters, can cause the message to be encoded in UCS-2.

Messages exceeding the applicable limit are split into concatenated SMS segments. **Each segment sent to each recipient consumes one SMS credit.** Keep messages short and use GSM standard characters where possible to reduce consumption.

7.1.4 When SMS credit runs out

If both the device's included monthly SMS credit and the owner's purchased account credit are exhausted, SMS notifications cannot be sent. Voice calls require at least **four purchased SMS credits** per call; included monthly credit cannot cover them.

E-mail and push notifications do not require SMS credit. They still require an available event allowance and the corresponding connection and notification configuration.

The owner can purchase additional packages under **Account settings > SMS package**. To help prevent interruptions caused by depleted credit, enable **Automatic purchase** and configure:

- the remaining SMS credit threshold that triggers a purchase;
- the number of packages to purchase when the threshold is reached;
- the payment method.

When the configured threshold is reached, the system automatically purchases the selected number of SMS packages. See Section 7.2.3.

7.1.5 When the event allowance runs out

The event allowance belongs to the individual device's service profile. Once it is exhausted, further regular event notifications cannot be sent. The quota-reached notification described below is an exception. **Purchasing SMS packages does not increase the event allowance.**

To receive a warning when the allowance is exhausted, enable **Periodic number of events reached** under **Events > Regular status** before the limit is reached. When enabled, this notification is sent when the event allowance has been fully used, including when no event allowance remains. See Section 6.2.6.2.

The owner can select a higher service profile under **Service profile > Change service profile**. The available event allowance then depends on the newly selected profile. The **Service profile** menu is visible only to the owner. See Section 6.2.8.

Enable the quota-reached notification in advance so that the owner can respond when the limit is reached.

7.2 Manage your account and SMS credit

7.2.1 Menu: Profile

Open your account settings from item **8** in Figure 6.1 or Figure 6.2. Use **Profile** to enter or change the account holder's details; see Figure 7.1.

Complete the mandatory fields marked with an asterisk, *. Check your **e-mail** and **mobile phone number** carefully: these are used to communicate with the account holder.

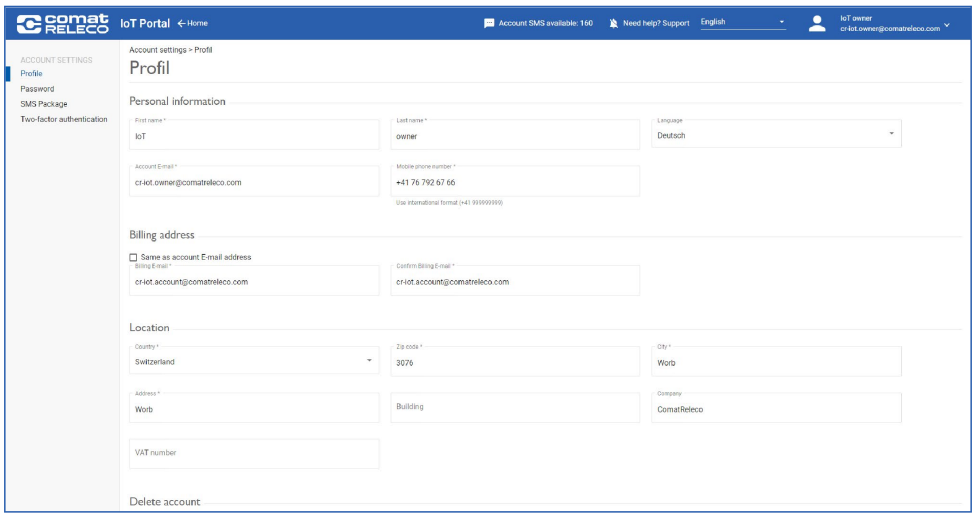


Figure 7.1: Account settings: Profile.

Set the billing e-mail address

1. Enter a dedicated **billing e-mail address** if required. Invoices for purchased services are sent to this address when it is provided.
2. If invoices should go to your account e-mail address, select **Same as account e-mail address**.

You can set a dedicated billing e-mail address when creating an account or later in the settings of an existing account.
Same as account e-mail address is activated by default.

Delete your account

Once your account has been deleted, it cannot be restored.

Before deleting your account, make sure that all **automatic purchases** and **automatic service profile renewals** have been cancelled. Account deletion does not automatically terminate these services or related payment obligations.

1. Cancel all automatic purchases and automatic service profile renewals before deleting the account.

2. Make sure that you no longer own any device. Otherwise, account deletion may fail.
3. Select **Delete my account**.

Contact support if you have any questions.

7.2.2 Menu: Password

The account password screen contains fields for your old password, new password and password confirmation. For the password requirements, see Section 5.1.2, Log in, create an account or reset your password.

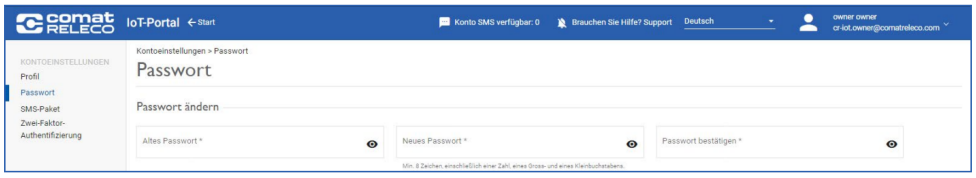


Figure 7.2: Account settings: password screen (German interface).

7.2.3 Menu: SMS package

There are two types of SMS credit: the monthly credit in each device's service profile and the owner's account SMS packages. The scope and use of each type are different.

For notification usage and the distinction between SMS credit and event allowances, see Section 7.1.

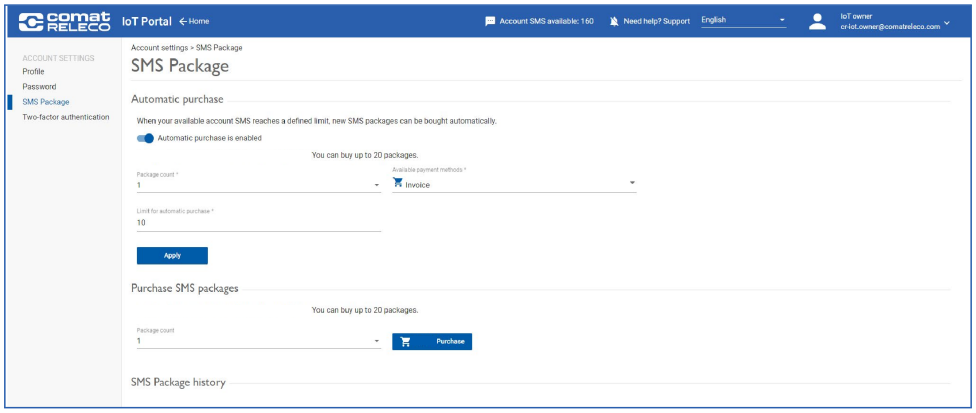


Figure 7.3: Account settings: SMS package (prices and package sizes omitted).

Device credit: SMS in the Service profile / SMS available for this month

The selected **Service profile** determines the monthly number of SMS:

Service profile	SMS per month
Eco	0
Standard	10
Professional	30
Expert	30

This service profile credit can be used only by the associated device.

Owner credit: SMS packages in the Account settings / Account SMS available

- Purchased SMS packages belong to the **Owner**. All devices owned by that owner can use them. The remaining credit is shown at item **4** in Figures 6.1 and 6.2.
- Once a device has used all its service profile SMS, further SMS are debited from the owner's SMS account.
- If both the service profile credit and the account SMS credit are 0, no more SMS can be transmitted.

The SMS packages are not transferable.

To help prevent interruptions caused by depleted SMS credit, we recommend enabling **Automatic purchase** of SMS packages; see Figure 7.3.

Set up Automatic purchase

You can activate or deactivate automatic purchase of chargeable SMS packages. Enter:

- the required number of SMS packages;
- the payment methods;
- the SMS credit threshold that triggers an automatic package purchase.

Automatic purchase helps maintain sufficient purchased SMS credit for SMS notifications and voice calls.

Purchase SMS packages manually

1. Select one or more SMS packages.
2. Select **Purchase** to add the amount to the shopping cart.
3. In the shopping cart, choose the payment method.
4. Select **Purchase** to initiate payment.

View the SMS package history

The SMS package history lists previous purchases. Download the invoices as PDF from the **Receipt** column.

7.2.4 Set up two-factor authentication (2FA)

Two-factor authentication verifies your identity using two independent components: your password and a PIN code.

Before you start: Have your current password and an authenticator app available, for example Google Authenticator, Microsoft Authenticator or a similar app.

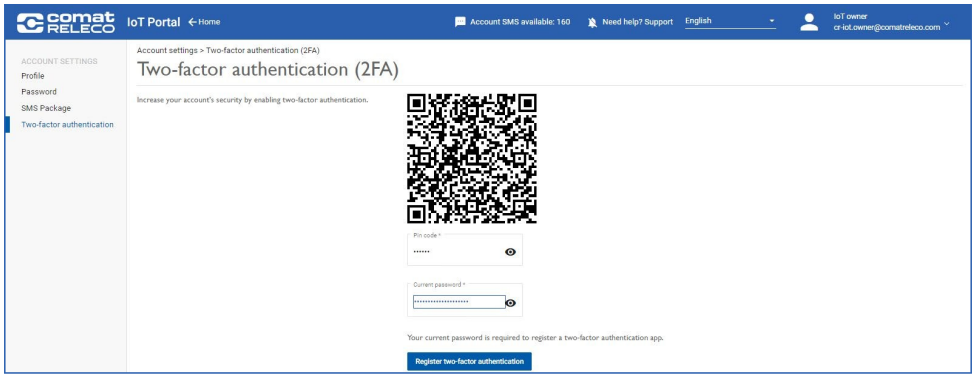


Figure 7.4: Two-factor authentication setup.

1. Scan the QR code with your authenticator app.
2. Enter the 6-digit PIN code and your current password.
3. Select **Register two-factor authentication**.

If you lose your phone or access to your secret time password, use a recovery code to restore account access. Each recovery code can be used only once. Keep the codes in a safe place so that you do not lose access to your account.

7.2.5 Log out



Figure 7.5: Log out of the IoT Portal.

Select **Logout** to end your IoT Portal session.

To log in again, see Section 5.1.2, Log in, create an account or reset your password.

7.3 Manage payments, billing groups and account inactivity

Payment preferences define the standard payment method for service profile purchases and renewals. **Credit card** is the standard payment method. Payment by invoice is available on request for **B2B customers** only.

7.3.1 Set your payment preferences

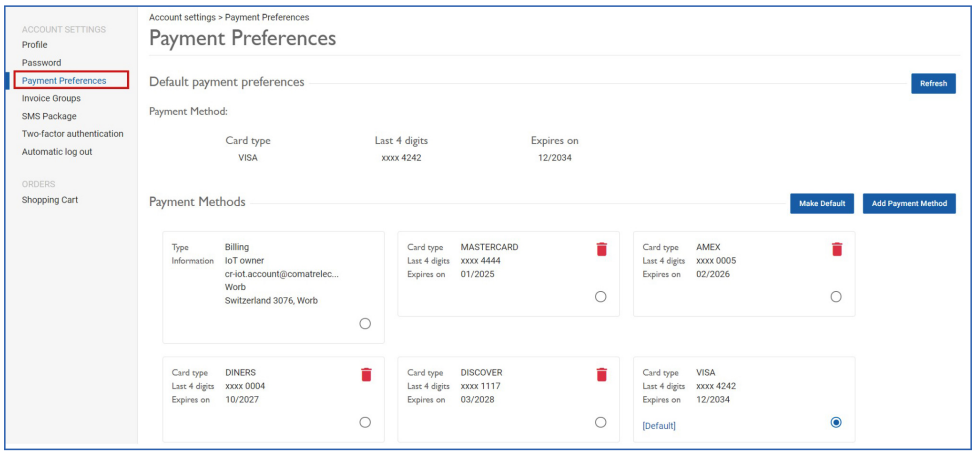


Figure 7.6: Account settings: Payment Preferences.

1. Open **Account settings**.
2. Select **Payment Preferences**.
3. Add or edit the available payment methods.
4. Choose the default payment method.

7.3.2 Create invoice groups

Use invoice groups to combine several devices under one billing configuration. All devices that use the default payment method appear in the default group. You can create additional groups to define a specific payment method and billing interval for several devices.

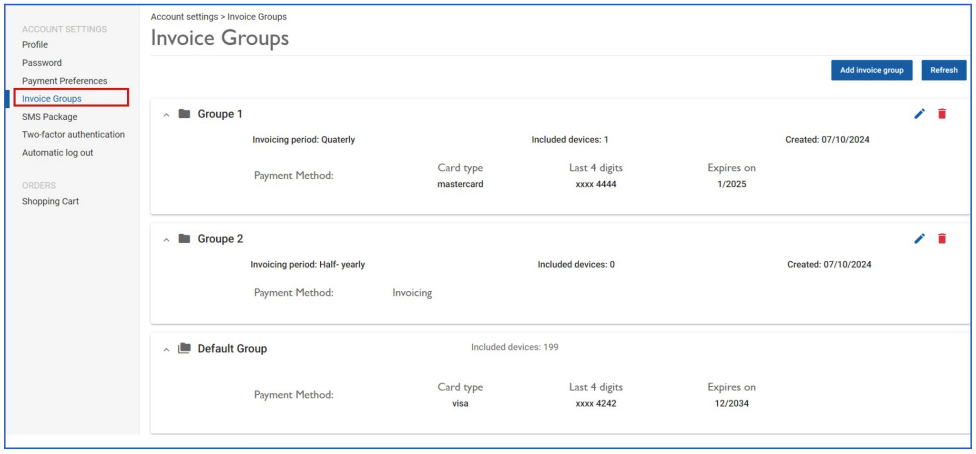


Figure 7.7: Account settings: Invoice Groups.

1. Open **Account settings** and select **Invoice Groups**.
2. Review the devices in the default group. These devices use the default payment method.
3. Create an individual invoice group for devices that should be billed together.
4. Define the payment method for that group.
5. Select the billing interval: **annual**, **half-yearly** or **quarterly**.

A collective invoice is issued for all service profiles due within the selected billing period.

7.3.3 Assign an invoice group to a service profile renewal

The owner can assign the corresponding devices to a defined invoice group during service profile renewal. Use **Service profile > Renewal of the service profile**; the billing group is selected under **Auto renew**.

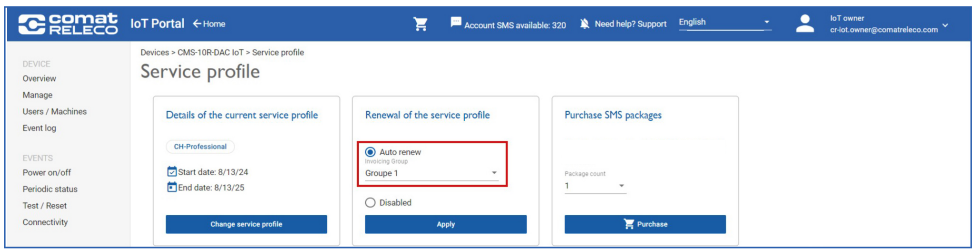


Figure 7.8: Select a billing group for service profile renewal (prices and package sizes omitted).

1. Open the device's **Service profile** menu.
2. Go to **Renewal of the service profile**.
3. Under **Auto renew**, select the billing group.
4. Apply the settings to assign that invoice group to the renewal.

Renewal and expiry notifications

The owner receives the following e-mails:

- **30 days before renewal or expiry**: a reminder that the service profile will be renewed or will expire.
- **After renewal or expiry**: confirmation of renewal or notification that the service profile has expired.

An expired service profile can be renewed or modified within **30 days** after expiry.



Important: Devices with outstanding invoices may be disconnected. Reconnection may be subject to an additional fee.

7.3.4 Review the shopping cart and pay

The **Shopping Cart** contains your selected service profiles and SMS packages.

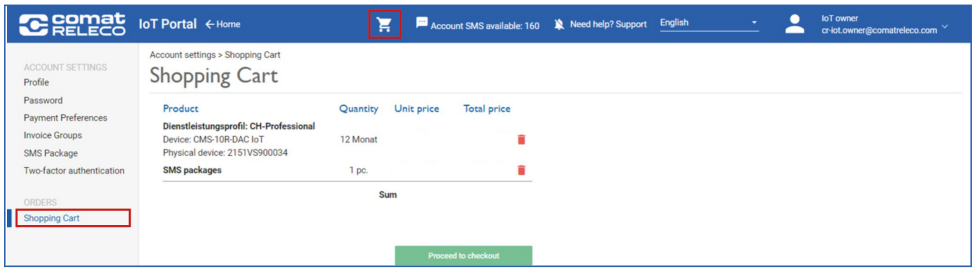


Figure 7.9: Review purchases in the Shopping Cart (prices omitted).

1. Review the selected items before payment.
2. Select the payment method.

3. Confirm the purchase to complete payment.

You can also make credit card purchases using the mobile app.

For information about how the payment partner Stripe handles security, see the Stripe security documentation.

Obtain an invoice copy

Important: The **invoice** is sent to the customer by e-mail and is **not available in the IoT Portal**.

To obtain a copy, request it by e-mail from info@comatreleco.com.

7.3.5 Set automatic log out for the browser

When **Automatic log out** is activated, your browser account session ends automatically after the configured inactivity time. This setting applies to the browser session only; it does not apply to the mobile app.

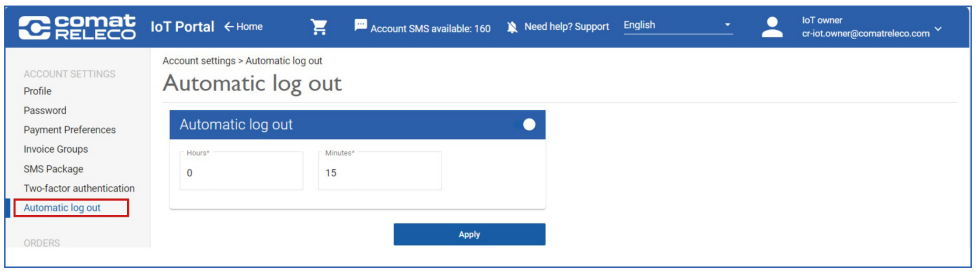


Figure 7.10: Account settings: Automatic log out.

1. Open **Account settings**.
2. Select **Automatic log out**.
3. Activate **Automatic log out**.
4. Enter the inactivity time after which you should be logged out.
5. Apply the setting to save the configuration.

The existing configuration from versions later than **1.0.0** is adopted.

Chapter 8

Mobile operation and SMS status

Use the **ComatReleco IoT Portal** app on a smartphone or tablet to check input status and switch outputs. You can also request the status of the device by SMS, as described in Section 8.3.

8.1 Choose how to access the device

- **Tablet:** install the app (Section 8.2, Use the app), or open the IoT Portal in a web browser (Chapter 5, Commission the device in the IoT Portal).
- **Smartphone:** install the app. See Section 8.2, Use the app, for its functions and operation.



We recommend using the latest version of **Android** or **Apple iOS** and enabling automatic updates for the **ComatReleco IoT Portal** app.
To use the IoT Portal in a web browser, the app must be uninstalled.

8.2 Use the app

The app lets you view input status and switch outputs on or off directly. You can also change:

- profile data, including personal information and location;
- your password;
- SMS package settings, including purchasing SMS packages and configuring automatic SMS purchase.

Firmware updates: when a new firmware version is available, selecting the device prompts you to update it. This option is available only to users with the **Manage** access right.

Device owners only: if no service profile has been selected, or if the service profile has expired, you are prompted to select a service profile. The upgrade must still be carried out on a computer. You can accept an invitation to become the owner of a device on a smartphone or tablet.



The device cannot be configured via the app.

8.2.1 Install the app and sign in

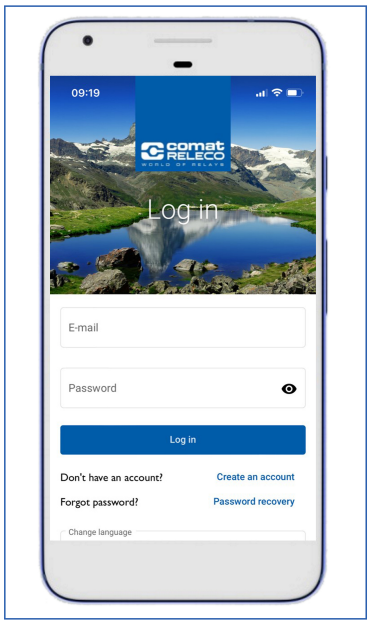


Figure 8.1: ComatReleco IoT Portal app.

The **ComatReleco IoT Portal** app is available free of charge for **iOS** and **Android** smartphones and tablets.

1. Download and install the app from the appropriate store:
   - Apple App Store
   - Google Play
2. Sign in with your existing account, or create a new account when setting up the app.

You can also reset your password or request a new password.

8.2.2 Find your device and check its status

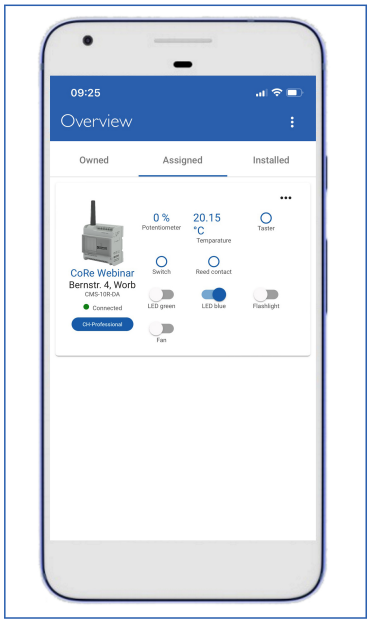


Figure 8.2: App overview.

1. Use the tabs below the menu bar to display devices in **My owned**, **My assigned**, or **My installed**.
2. Check the device name, device type, and connection status on the left, below the device image.
3. Read the input values and status on the right. The output controls are below them; use these controls to switch outputs on or off directly.

Tap the three-dot menu in the menu bar to open the menu options shown in Figure 8.3.

8.2.3 Change account settings or add a device

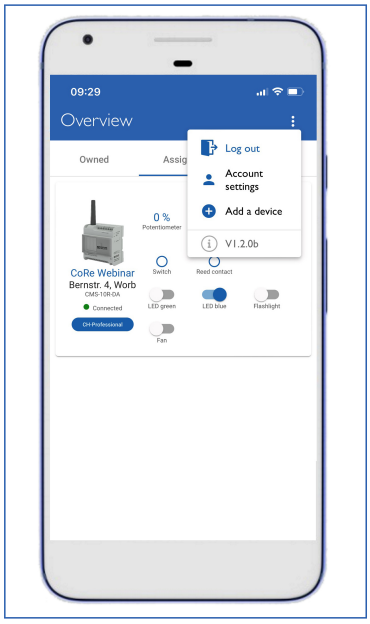


Figure 8.3: App menu options.

Open the three-dot menu to access:

- **Log out**: sign out of your user account in the app.
- **Account settings > Profile**: update **personal information** and **location**. See Section 7.2.1, Menu: Profile.
- **Account settings > Password**: change your existing password.
- **Account settings > SMS package**: purchase a new **SMS package** and configure automatic **SMS purchase**. See Section 7.2.3, Menu: SMS package.

Add a device: use the invitation code received by e-mail or SMS. After the device is added, it is also visible in the IoT Portal.

The app version is displayed at the bottom.

8.2.4 Open the detailed view and switch outputs

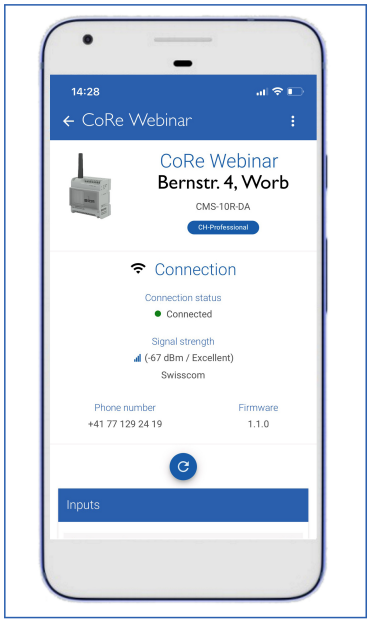


Figure 8.4: Detailed view in the app.

1. In the overview (Figure 8.2), tap the device display on the left to open its detailed view.
2. Check the device connection status, signal quality, and phone number.
3. Use the refresh control below this information to refresh the display, including input and output status.
4. Read the input status below the refresh control. The status display shows the date and time of the last change to an input or output.
5. Swipe upward to view more information.

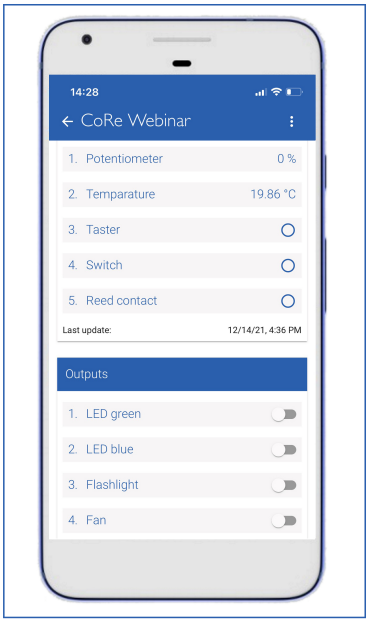


Figure 8.5: Output controls and documents in the app.

- Use the sliders to switch outputs on or off directly.
- Open **CMS-10R Documents** to access the ComatReleco download area. All documents related to the CMS-10R device are available there.

8.3 Request input and output status by SMS

During operation, you can request the status of all inputs and outputs by SMS.

Prerequisite: the sender must be a registered user or machine assigned to the device. The device does not return status information to other senders.

1. Send an SMS containing the command **Status** to the device phone number.
2. Read the returned status information in the format for users or machines described below.

The command is not case-sensitive: **Status**, **STATUS**, and **status** are all accepted.

SMS format for users

The reply contains:

- device name;
- input *n*: configured name, followed by **0** or **1** for a digital input, or the actual value and configured unit for an analogue input;
- output *n*: configured name, followed by **0** or **1**.

Disabled or unused inputs and outputs are not shown in the SMS sent to a user.

SMS format for machines

```
<serial-number>;<timestamp>;<i1>;<i2>;<i3>;<i4>;<i5>;<i6>;<o1>;<o2>;<o3>;<o4>
```

Example:

```
1939VS000096;2021-08-12 13:15:21.000Z;0;1;x;54.1 %;28.97 °C;x;0;x;x;1
```

- **Serial number:** 12-digit unique device serial number.

- **Timestamp:** ISO 8601 format, `YYYY-MM-DD HH:mm:SS.sssZ`; time is displayed in **UTC**.
- **Digital inputs and outputs:** `0` or `1`.
- **Analogue inputs:** actual value followed by the configured unit.
- **Disabled or unused input/output:** `x`.



SMS messages sent by the device are deducted from the number of SMS messages available for that device per month. If none remain, they are deducted from the owner's account.
Depending on the configured input and output names and parameters, a message may exceed the maximum SMS length of **160 characters**. It is then sent as more than one SMS.
If a message contains characters outside the GSM standard coding alphabet, **3GPP 23.038**, such as special characters, Greek letters, or Cyrillic characters, the system automatically switches to **UCS-2** encoding. The maximum SMS length is then **70 characters**.

Chapter 9

Monitor data and connect external systems

This chapter explains how to view CMS-10R data graphically, trigger outputs automatically when events occur, and exchange data with external systems.

For normal operation, the CMS-10R can be configured and operated directly through the **IoT Portal** or the **ComatReleco IoT Portal app**. In many applications, this is sufficient. For the functions and limitations of the app, see Section 8.2, Use the app.

Read this chapter when you need a graphical view of device data, another system needs to exchange data with the CMS-10R, or an external platform must respond automatically to device events.

Function	When to use it
Dashboard	View and evaluate device data graphically in the IoT Portal, including input and output values, device status, and location. No external programming is required. See Section 9.1.
Event actions	Automatically switch an output on the same CMS-10R device or on another CMS-10R device when a configured input or output event occurs. See Section 9.2.
Webhook API	Notify a monitoring system, automation platform, or customer-specific application automatically when a configured input or output event occurs. See Section 9.3.
Public REST API	Let an external application query device status or switch outputs on or off by sending requests to the IoT Portal. See Section 9.4.

The **Webhook API** is event-driven: the IoT Portal sends information when a configured event occurs, so the external system does not need to continuously ask the CMS-10R for updates. The **Public REST API** is request-driven: the external system sends a request when it needs information or wants to switch an output.



If you use the CMS-10R only for standard alarm notifications, manual output control, and basic monitoring through the IoT Portal or app, you may not need this chapter.



Configure API functions only if you understand the external system to be connected and the possible effects of remote output control.

9.1 Monitor device data in the Dashboard

The **Dashboard** provides a graphical overview of device status, input and output values, historical trends, and device location directly in the IoT Portal.

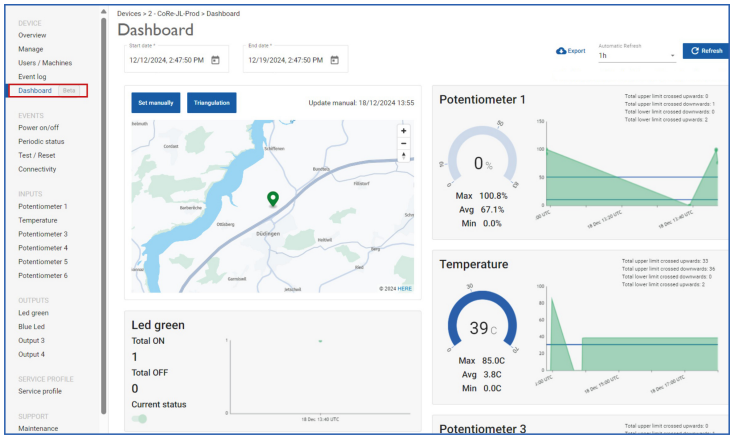


Figure 9.1: Dashboard.

1. Open the **Dashboard** menu in the IoT Portal.
2. View the device position and the input and output values in graphical form.
3. Use **Refresh** or an automatic refresh interval to update the view.
4. Use **Export** to download the displayed data as a **.csv** file.

9.1.1 Refresh the view or export data

- **Manual refresh:** press **Refresh**.
- **Automatic refresh:** select a time interval: **10 s**, **30 s**, **1 min**, **5 min**, **15 min**, **30 min**, **1 h**, or **2 h**.
- **Export:** press **Export** to download the displayed data as a **.csv** file in tabular form.

9.1.2 Read input and output information

The Dashboard shows:

- the current status of inputs and outputs;
- the total number of **ON** and **OFF** states for outputs;
- the **minimum**, **maximum**, and **average** values for analogue values;
- limit value information in graphical form, where applicable.

9.1.3 Display the device location on the map

The Dashboard includes a map showing the device location. Enable location service authorisation to display the map on the screen.

You can enter the position manually using latitude and longitude, or determine it by triangulation.

9.1.4 Locate a device by triangulation

Triangulation calculates the approximate device position from surrounding mobile phone masts. It uses the geometry between the device and nearby masts, with time or angle measurements to calculate the position in the mobile network.

Prerequisite: device firmware version **1.3.1** or higher.



Always operate the device with the latest firmware version. If the firmware is not up to date, perform a firmware update on the device.

9.2 Configure event actions to trigger outputs

Use **Event actions** to switch an output automatically when an enabled input or output event occurs. The available output actions are:

- **Trigger ON/OFF Local Output**: switch an output of the same CMS-10R device on or off.
- **Trigger ON/OFF Remote Output**: switch an output of another CMS-10R device on or off.

Event actions can also send event data to an external system through a Webhook API integration. For this workflow, see Section 9.3.

Event actions are available only with the **Standard** service profile **or higher**. The device owner can upgrade the service profile under **Service Profile > Change service profile**.

Event actions are executed on a best-effort basis. The IoT Portal aims for timely and reliable delivery, but timing and synchronisation may vary with network conditions and system load.

9.2.1 Add or change an event action

Prerequisite: the input or output event must be enabled. Event actions cannot be configured for disabled events.

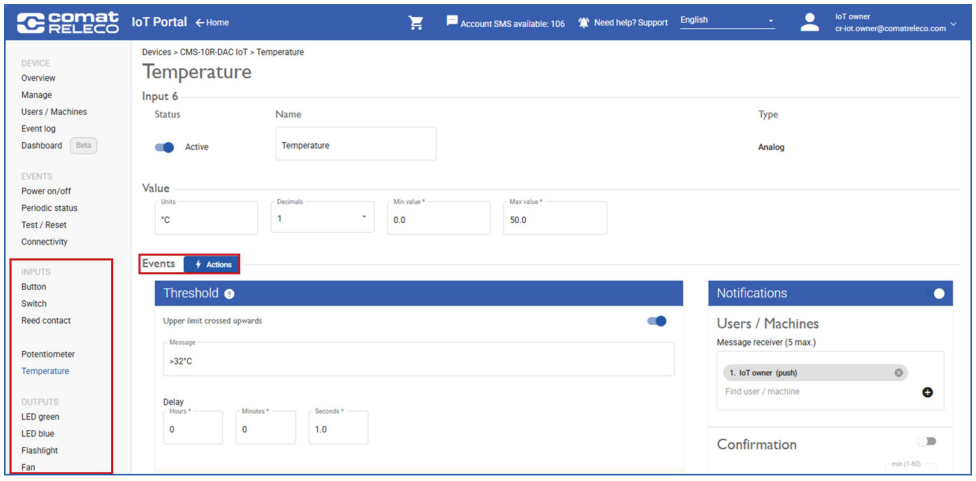


Figure 9.2: Actions button.

Open the input or output configuration screen and use the **Actions** button for the enabled event.

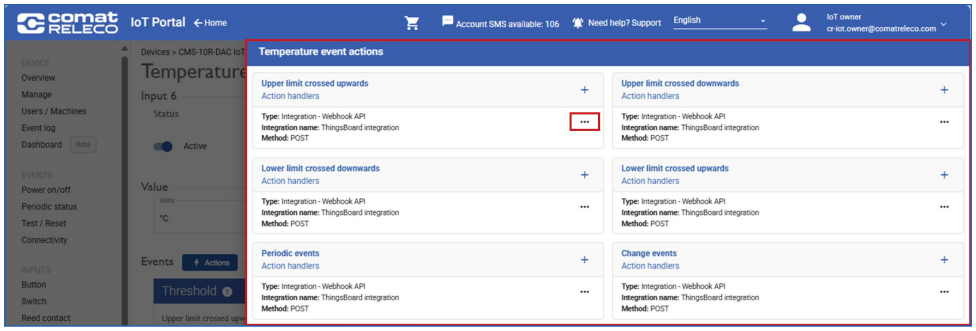


Figure 9.3: Event action configuration.

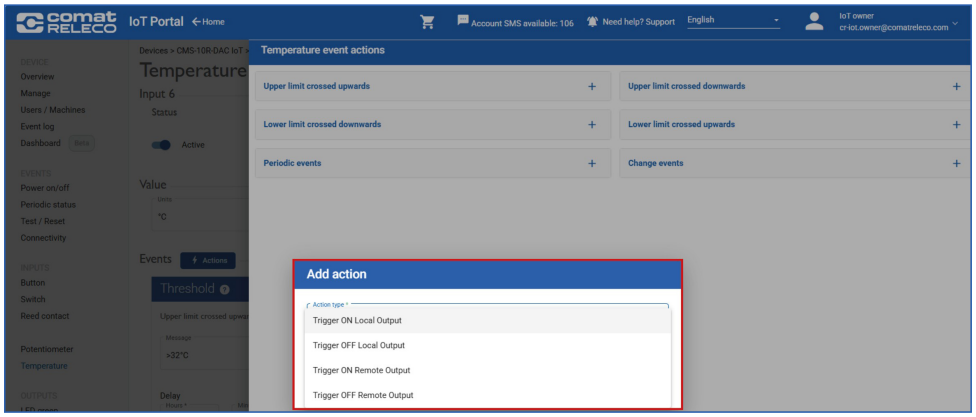


Figure 9.4: Add event action screen.

1. Click **Add** (**+**) to add an action to the event.
2. Select the required action type:
   - **Integration**: use a configured Webhook API integration (Section 9.3.3).
   - **Trigger ON/OFF Local Output**: switch a local output (Section 9.2.2).
   - **Trigger ON/OFF Remote Output**: switch an output on another CMS-10R device (Section 9.2.3).

9.2.2 Switch a local output when an event occurs

The **Trigger ON/OFF Local Output** action switches an active output of the same CMS-10R device.

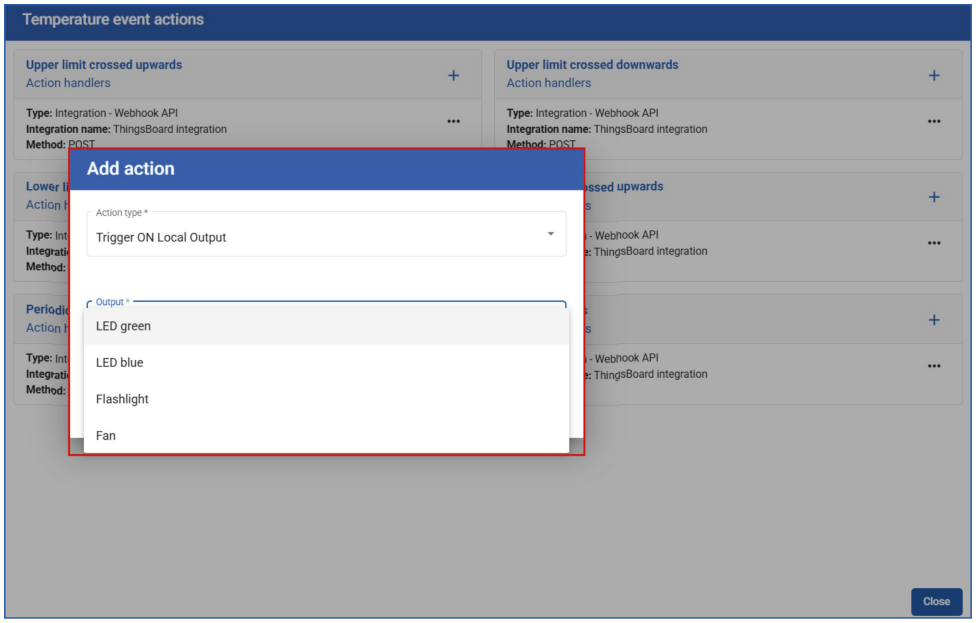


Figure 9.5: Add Local Output.

1. Select **Trigger ON/OFF Local Output** as the action type.
2. Select the local output to switch.
3. Set the required state: **ON** or **OFF**.
4. Apply the configuration to save the event action.

9.2.3 Switch a remote output when an event occurs

The **Trigger ON/OFF Remote Output** action switches an active output of another CMS-10R device.

Prerequisite: add the remote CMS-10R device as a CMS-10R node before controlling its output.

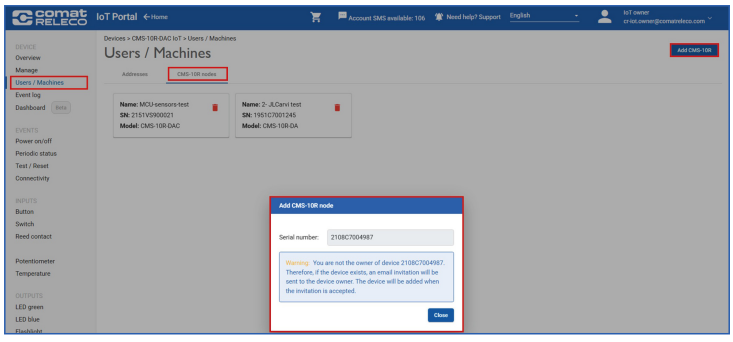


Figure 9.6: CMS-10R nodes.

1. Open **Users** / **Machines** > **CMS-10R nodes**.
2. Add the serial number of the remote device.

If the remote device exists and you are not its owner, an e-mail invitation is sent to its owner. The remote device is added after the invitation is accepted.

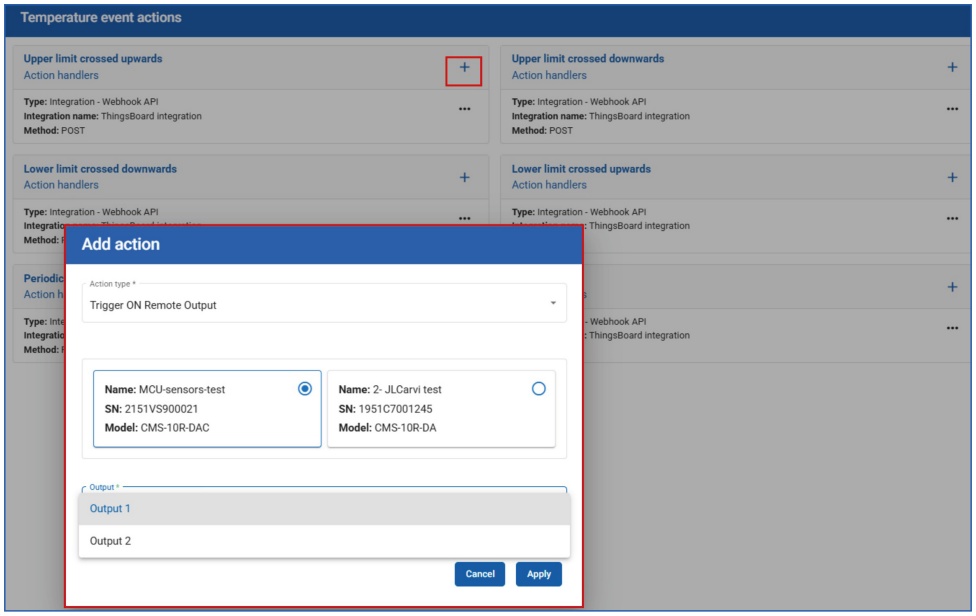


Figure 9.7: Add Remote Output.

1. Select **Trigger ON/OFF Remote Output** as the action type.
2. Select the remote CMS-10R node.
3. Select the output of the remote device.
4. Set the required state: **ON** or **OFF**.
5. Apply the configuration to save the event action.

9.2.4 Review event action history

All event action functions are recorded under **Event Log > Event actions** and in the **Dashboard**.

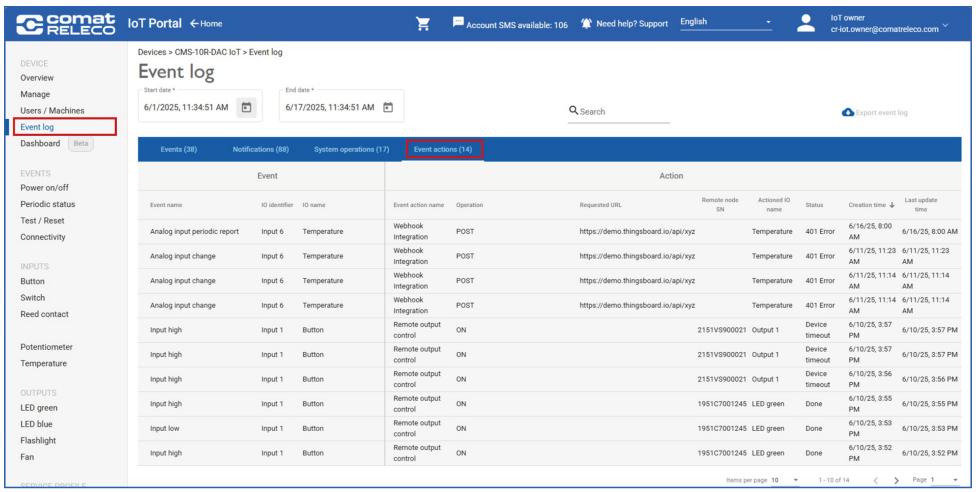


Figure 9.8: Event log for event actions.

Open **Event Log > Event actions** to see the history in table form, including each executed action and its status.

The log shows the timestamp, event name, and input or output name, together with:

- event action name;
- operation;
- requested URL, for a Webhook API integration;
- remote node serial number, for a remote output;
- name of the affected input or output;
- status.

Event actions cannot be exported using **Export event log**.

Always operate the device with the latest firmware version.

9.3 Configure webhook integration

Use the **Webhook API** to send telemetry data or input and output event information from the IoT Portal to an external system. Examples include **ThingsBoard**, **Zapier**, **N8N**, and customer-specific platforms.

Webhook integration uses the **Integration** event action type. First register the integration in the Integration center, then assign it to a device and configure the webhook request for the required event.

9.3.1 Register a webhook integration in the Integration center

Register the external Webhook API before assigning it to a device.

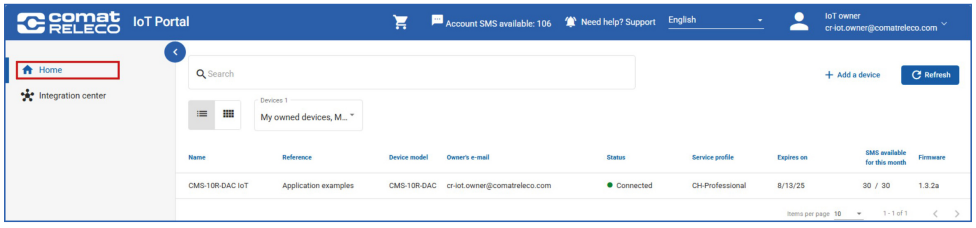


Figure 9.9: Home screen.

1. Open the IoT Portal home screen. Existing filters are arranged under **Home**.
2. Open the **Integration center**.

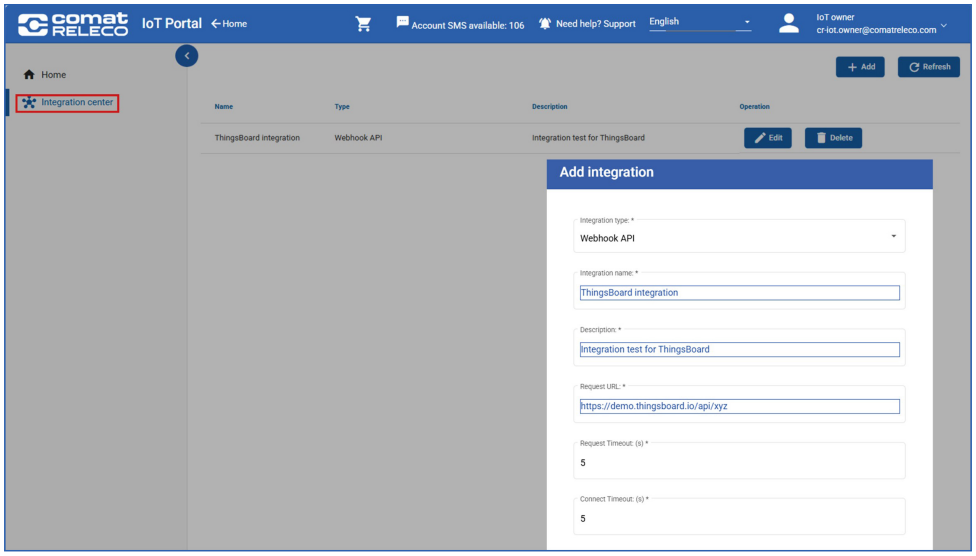


Figure 9.10: Integration center.

3. Select **+ Add** to create a Webhook API integration, or **Edit** to modify an existing integration.
4. Complete the mandatory fields below.

Mandatory field	Entry or default
Integration type	Select **Webhook API**.
Integration name	Enter a unique name for the external Webhook API integration.
Description	Enter a reference or description for the integration.
Request URL	Enter the URL of the external Webhook API.
Request Timeout (s)	Default: **5 seconds**.
Connect Timeout (s)	Default: **5 seconds**.

A registered integration can send telemetry data and notify external systems about CMS-10R events.

9.3.2 Assign the integration to a device

Prerequisite: you must have **Manage access** to the device. You can select one Webhook API integration for each device under **Manage > Integrations**.

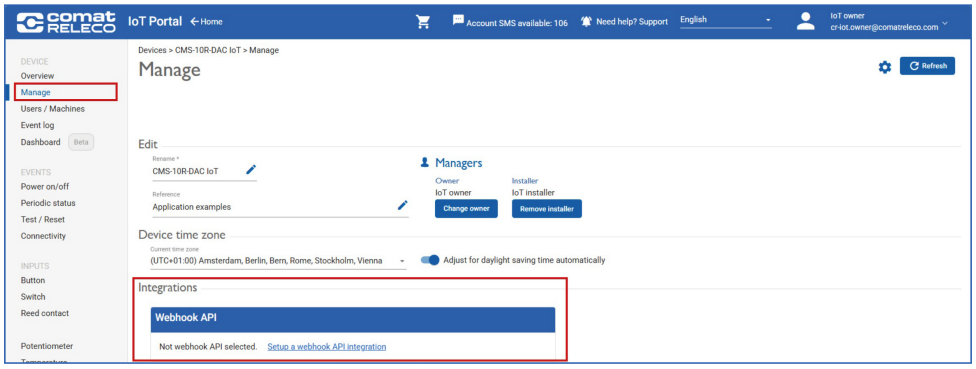


Figure 9.11: Webhook API integration in the Manage screen.

1. Open the device configuration.
2. Go to **Manage > Integrations**.
3. Select the Webhook API integration to use for this device.



If the device owner is changed to a user without management access to the device, the Webhook API integration will be lost.

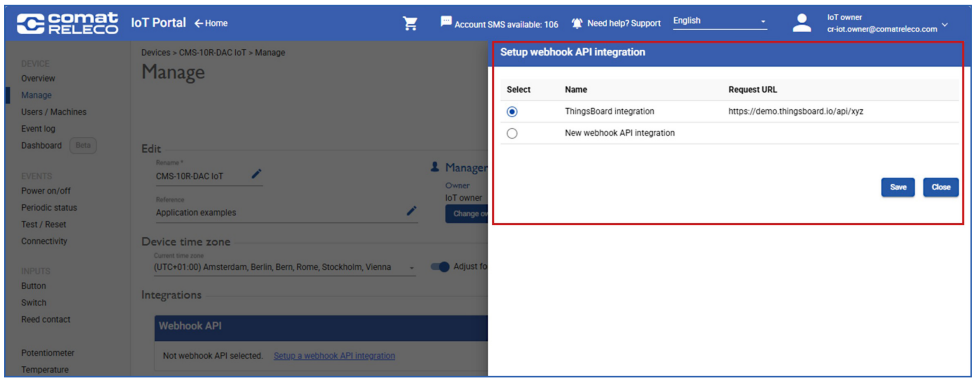


Figure 9.12: List of Webhook API integrations.

The list contains integrations created in the **Integration center**. Select an existing integration, or create a new integration from this view.

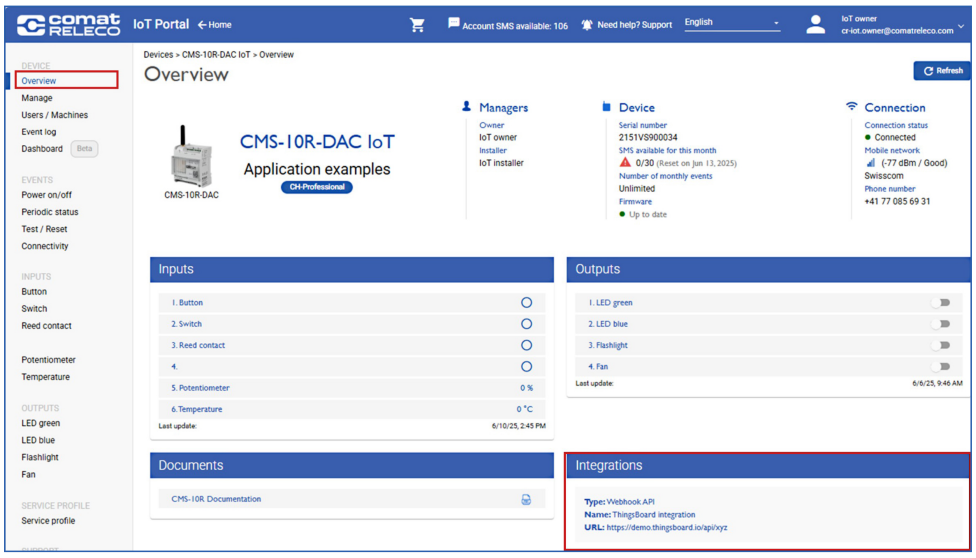


Figure 9.13: Overview screen: selected Webhook API integration.

Check the result: open **Overview > Integrations** to verify which integration is assigned to the device.

9.3.3 Configure the webhook request

Open the event action configuration as described in Section 9.2.1.

Select **Integration** as the event action type to use the Webhook API integration assigned in the **Manage** menu.

If a Webhook API integration is already selected under **Manage > Integrations**, a default configuration appears. You can update it, or delete it using the **...** button.

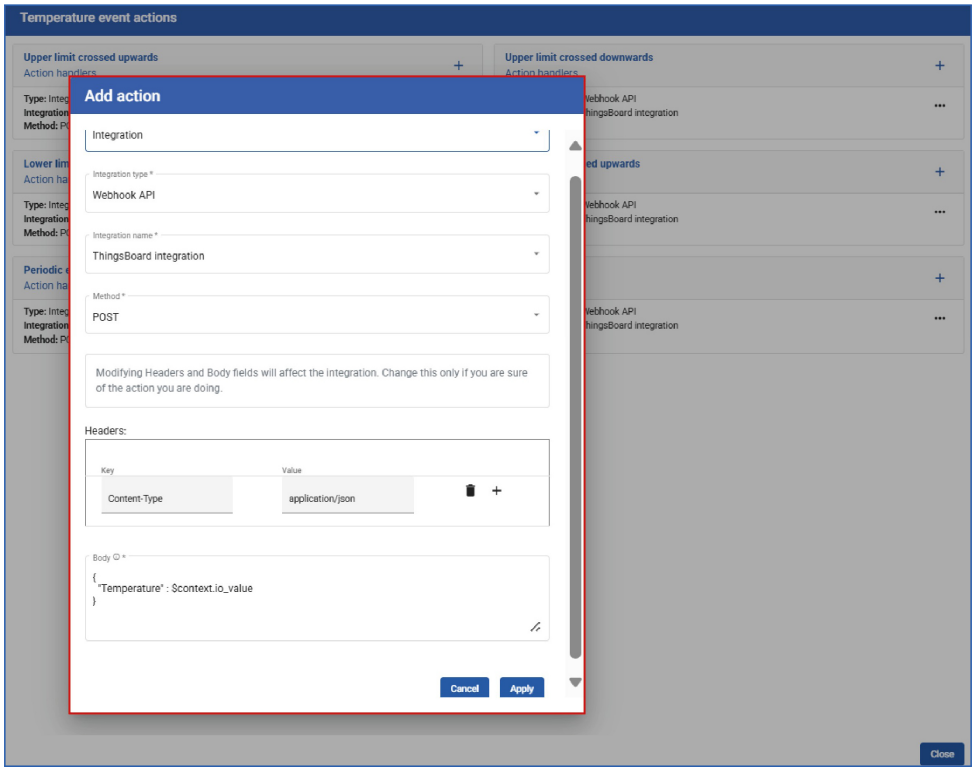


Figure 9.14: Webhook API integration setup.

1. Select the Webhook API integration.
2. Select the HTTP method: **POST**, **PUT**, or **GET**.
3. Complete all mandatory fields marked with an asterisk (*).

Telemetry data is sent in **JSON** format by default.



Change the **Headers** and **Body** fields only if you are sure of the action you are performing.

9.4 Access the device through the Public REST API

Use the **Public REST API** when an external system needs to access selected CMS-10R functions through the IoT Portal:

- **Set output ON**: switch activated device outputs on.
- **Set output OFF**: switch activated device outputs off.
- **Get device status**: retrieve current device information and status.

Public REST API functions are available only with the **Professional** service profile. The device owner can upgrade the service profile under **Service Profile > Change service profile**.

Public REST API services are provided on a best-effort basis. The IoT Portal aims for timely and reliable delivery, but timing and synchronisation may vary with network conditions and system load.

9.4.1 Obtain the Account SID and API Key

Prerequisites: an **Account SID** and an **API Key** are required for an external system to access the IoT Portal. The Account SID identifies the account. An API Key provides API access to devices owned by that account.

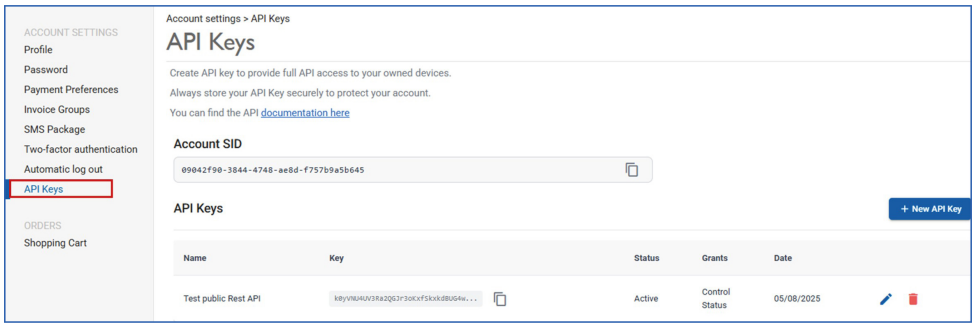


Figure 9.15: API Keys.

1. Open **Account settings > API keys**.
2. Copy the existing **Account SID** as required.
3. Copy an existing **API Key**, or create a new one as described in Section 9.4.2.
4. Open **Documentation** for detailed Public REST API configuration information.

Always store your **Account SID** and **API Key** in a safe place to protect your account and devices from unauthorised access.

Detailed configuration information is also available in the Public REST API documentation.

9.4.2 Create an API Key and select its permissions

A new API Key requires a **Name** and the required **Permissions**.

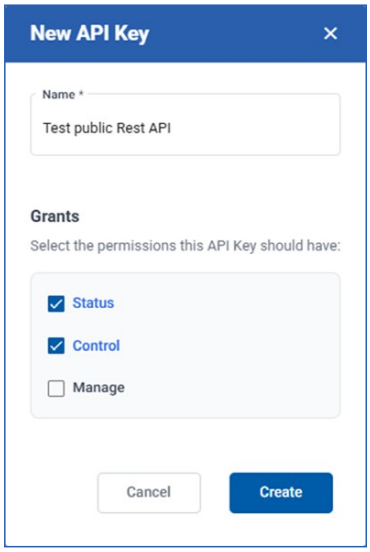


Figure 9.16: New API Key.

1. Select **New API Key**.
2. Enter a name.
3. Select the required permissions from the table below.
4. Create the API Key.
5. Store the generated API Key securely.

Right	Available functions
Status	Get device status.
Control	Get device status; Set output ON and OFF.
Manage	Get device status; Set output ON and OFF; Future use.

9.4.3 Copy the Device SID

The unique **Device SID** identifies a specific CMS-10R in Public REST API requests. It has **36 characters** and can be copied from the corresponding device in the IoT Portal.

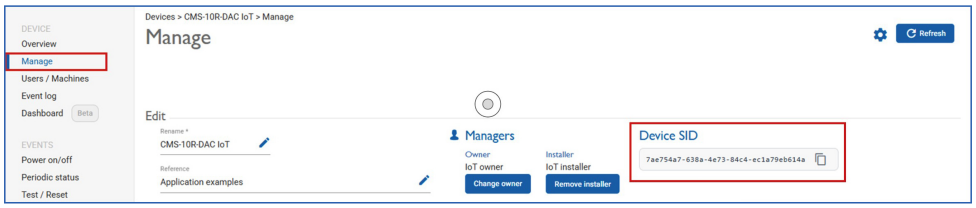


Figure 9.17: Device SID.

1. Open the CMS-10R device to be addressed.
2. Go to **Manage > Device SID**.
3. Copy its unique **Device SID**.
4. Use this Device SID in the Public REST API request.



Always keep your **Device SID** in a safe place to protect your account and device from unauthorised access.

9.4.4 Send a Set output ON request

Use **Set output ON** to switch on selected activated outputs of a specified CMS-10R. The function uses the **POST** method and the target device's unique **Device SID**.



Figure 9.18: Set output ON.

1. Use the **POST** method.
2. Specify the unique **Device SID** of the target device.
3. Select the output to switch on.
4. Send the request from the external system.

9.4.5 Send a Set output OFF request

Use **Set output OFF** to switch off selected activated outputs of a specified CMS-10R. The function uses the **POST** method and the target device's unique **Device SID**.



Figure 9.19: Set output OFF.

1. Use the **POST** method.
2. Specify the unique **Device SID** of the target device.
3. Select the output to switch off.
4. Send the request from the external system.

9.4.6 Send a Get device status request

Use **Get device status** to retrieve current device information and status. The function uses the **GET** method and the target device's unique **Device SID**.



Figure 9.20: Get device status.

1. Use the **GET** method.
2. Specify the unique **Device SID** of the target device.
3. Send the request from the external system.
4. Read the returned current device information and status.

9.4.7 Review API-triggered output changes

The IoT Portal records Public REST API **Set output ON** and **Set output OFF** events.

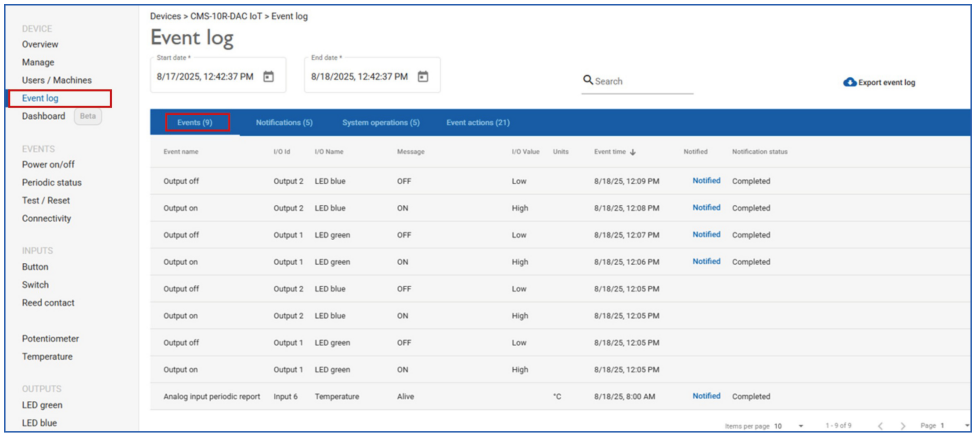


Figure 9.21: Event log for Public REST API events.

Open **Event Log** > **Events** to review API-triggered output changes. These switching events are also displayed in the **Dashboard**.

Always operate the device with the latest firmware version.

Chapter 10

Troubleshooting, maintenance and replacement

Use the symptom list below to find the relevant checks. Replacement and return instructions follow the troubleshooting sections.

10.1 Troubleshooting

Symptom	Section
RUN LED does not flash	10.1.1
Device is offline in the IoT Portal	10.1.2
Mobile network connection is poor	10.1.3
Links in e-mails do not work	10.1.4
Input or output states in the IoT Portal are incorrect	10.1.5
No notifications are received	10.1.6
The event allowance is exhausted	10.1.7
No e-mails are received	10.1.8
Cannot log in	10.1.9
Cannot log in with two-factor authentication (2FA)	10.1.10
No SMS messages or voice calls are received	10.1.11
No push notifications are received on the smartphone	10.1.12
Call-in does not work	10.1.13
No push notifications are received on the PC	10.1.14

10.1.1 RUN LED does not flash

Possible cause

No power supply

Checks and remedies

- Check the power supply.
- Restart the device with a short press of the **Reset** button: release it before 4 seconds.
- If the system remains unresponsive, hold the **Reset** button for more than 4 seconds to perform a forced hardware reset. This may result in data loss. See Section 3.4, Locate terminals, controls, and status indicators, item **10**.

10.1.2 Device is offline in the IoT Portal

Possible causes

- No power supply.
- No mobile network connection or insufficient signal strength.
- The connection to the IoT Portal is interrupted.

Checks and remedies

- Check the power supply and its connections, including fuses, circuit breakers and disconnecting switches.
- Check whether the **RUN LED** is flashing. See Section 3.4.
- Check whether a **2G**, **3G**, or **4G** LED is lit on the device. See Section 3.4.
- Check the antenna connection and mobile network reception. For poor reception, see Section 10.1.3.
- Refresh the **Overview** screen in the IoT Portal and check the connection status again.
- If power and mobile network reception are available but the device remains offline, restart the device as described in Section 3.8.

10.1.3 Mobile network connection is poor

Possible cause

Weak signal strength

Checks and remedies

- Check the signal strength in the IoT Portal, see Section 6.2.1, Check device status: Overview, item **10**.
- Check the colour of the **mobile network signal LEDs** on the device, see Section 3.4, Locate terminals, controls, and status indicators.
- Use a remote antenna if necessary, see Section 4.4, Antennas and antenna cables.

10.1.4 Links in e-mails do not work

Possible cause

Outdated web browser.

A security function is preventing the link from working correctly.

Checks and remedies

- Use **Google Chrome**, **Mozilla Firefox**, or **Microsoft Edge**, and update the browser to the latest version.
- Copy the link from the e-mail and paste it into the browser address bar.
- Reset the password, see Section 5.1.2, Log in, create an account or reset your password.

10.1.5 Input or output states in the IoT Portal are incorrect

Possible cause

The IoT Portal has not been refreshed

Checks and remedies

- Refresh the IoT Portal in the **Overview** menu, see Section 6.2.1, Check device status: Overview, or press **F5**.

10.1.6 No notifications are received

Possible causes

- The device has no power or no connection.
- The expected notification channel is unavailable in fallback mode.
- The monthly event allowance has been exhausted.
- The event, recipients or notification channels are not configured correctly.
- Insufficient SMS credit for SMS notifications.

Checks and remedies

- Check the device power supply and connection status. See Section 10.1.2.
- Check that the relevant event is enabled and that the intended recipients and notification channels are configured. See Section 6.2.6.
- Review the **Event Log** for the relevant event and its notification status. See Section 6.2.7.
- Check the remaining monthly event allowance in **Overview**. If the allowance has been exhausted, review the selected service profile. See Section 6.2.8.
- If the device is operating in **fallback mode**, alarms are sent directly by **SMS only**. Check for SMS messages, verify the recipients' mobile telephone numbers and confirm that mobile SMS communication is available. See Section 3.8.
- For missing SMS messages, also check the available SMS credit. The event allowance and SMS credit are separate. See Section 10.1.11.

If the problem affects a specific notification channel, continue with the corresponding e-mail, SMS or push notification checks below.

10.1.7 The event allowance is exhausted

Possible cause

The device has used the event allowance of its selected service profile.

Checks and remedies

- Check the remaining event allowance in the device's **Overview** screen.
- Ask the owner to select a higher profile under **Service profile > Change service profile**. This menu is visible only to the owner. See Section 6.2.8.
- Enable **Periodic number of events reached** under **Events > Regular status** in advance to notify the owner when the allowance is fully used. See Section 6.2.6.2.
- Check the configured recipients and notification channels for this quota-reached notification.

SMS credit and the event allowance are separate. Purchasing an SMS package does not replenish the event allowance. See Section 7.1.

10.1.8 No e-mails are received

Possible cause

Incorrect configuration.

Firewall settings

Checks and remedies

- Check the device configuration, see Section 6.2.6, Configure notifications and acknowledgement: Events.
- Check the firewall settings.
- Check the spam folder.

10.1.9 Cannot log in

Possible cause

Incorrect e-mail address or password.

Firewall settings

Checks and remedies

- Check the e-mail address.
- Check the password.
- Reset the password, see Section 5.1.2, Log in, create an account or reset your password.
- Try logging in from another PC or smartphone.
- Allow the following domains in the firewall:
  - `prod.api.core-iiot.com`
  - `comatreleco-iot-api.com`
  - `core-iiot.com`

10.1.10 Cannot log in with two-factor authentication (2FA)

Possible cause

Incorrect PIN code or current password

Checks and remedies

- Check the password.
- Reset the password, see Section 5.1.2, Log in, create an account or reset your password.
- Check the 6-digit PIN code.
- Use the one-time recovery code, see Section 7.2.4, Set up two-factor authentication (2FA).

10.1.11 No SMS messages or voice calls are received

Possible causes

- The device's included SMS credit and the owner's purchased account credit are both exhausted.
- Fewer than four purchased SMS credits remain for a voice call.
- The device's event allowance is exhausted.

Checks and remedies

- Check the device's remaining monthly SMS credit and the owner's purchased account credit. SMS notifications use included credit first, then purchased credit.
- For voice calls, check that at least **four purchased SMS credits** are available per call. Included monthly SMS credit cannot be used for voice calls.
- Purchase SMS packages or enable **Automatic purchase** under **Account settings > SMS package**. See Section 7.2.3.
- Check the remaining event allowance. If it is exhausted, follow Section 10.1.7.

For notification charges and message segmentation, see Section 7.1.

10.1.12 No push notifications are received on the smartphone

Possible cause

The smartphone operating system or the app is not up to date.

Battery management on the smartphone is blocking push messages.

Checks and remedies

- Update the operating system, **iOS** minimum version 6 / **Android** minimum version 9.
- Update the app in the **Apple App Store** or **Google Play Store**.
- On the smartphone, under **Settings > Apps**, allow notifications for the **ComatReleco IoT Portal** app.
- On the smartphone, under **Settings > Battery management**, set battery management to manual, **Android only**.
- Use the IoT Portal in the web browser, **Google Chrome**, instead of the app, and create a shortcut if required.

10.1.13 Call-in does not work

Possible cause

Telephone control is not activated

Checks and remedies

- Check whether the telephone number is stored under **Users** / **Machines**.
- Activate telephone control **Call-in** for the required output, see Section 6.2.5, Configure and control relay outputs: Outputs.
- Check the signal strength on the device, see Section 3.4, Locate terminals, controls, and status indicators, item **4**, or in the IoT Portal.

10.1.14 No push notifications are received on the PC

Possible cause

Incorrect configuration.

An ad blocker extension may be installed or enabled in the web browser.

Checks and remedies

- Check the configuration, **Users** / **Machines**, with controls and notifications enabled as required.
- Check the signal strength on the device, see Section 3.4, Locate terminals, controls, and status indicators, item **4**, or in the IoT Portal.
- Disable or uninstall the ad blocker extension in the web browser.

Further information and assistance are available in the IoT Portal under **Overview** / **Documents**, see Figure 6.3, item **17**, or in the CMS-10R Support Centre on the ComatReleco Internet portal under **FAQ**: Frequently Asked Questions.

10.2 Maintenance

The device is maintenance-free.

10.3 Replace or return a defective device

Only ComatReleco may repair the device. Send a defective device to ComatReleco or your dealer. Before returning goods to ComatReleco, request a return material authorisation (**RMA**) number.

For return shipment, pack the device in a similar manner to the original packaging to ensure safe transport.

For delivery conditions and information on returning goods, refer to the ComatReleco legal information page.



Risk of death due to electric shock
Mount or dismantle the device only when it is disconnected from the **Power supply**. More than one disconnecting switch may be required to de-energise the device.



The work described in this chapter must only be carried out by qualified electricians, see also Section 2.3, Who may install and use the device.

10.4 Replace a CMS-10x predecessor with a CMS-10R

When replacing a predecessor device, follow this sequence:

1. Switch off the voltage.
2. Remove all cables and connections.
3. Dismantle the device as described in Section 4.2.2.
4. Replace it with an identical device, using the current and previous versions listed below.

CMS-10R devices have the same electrical pin assignment as CMS-10 predecessor units.

Current device version and previous version

Current device	Version	Previous version
CMS-10R-D/AC	110–240 V	CMS-10F/AC110–240V
CMS-10R-DA/DC	12–48 V	CMS-10F/DC12–48V or CMS-10ADF/DC12–48V
CMS-10R-DAC/DC	12–48 V	CMS-10ACDF/DC12–48V

The configuration of the previous CMS-10 device can be imported into the new CMS-10R device, see also Section 6.2.2.3, Manage your device.

Chapter 11

Disposal

Follow the disposal information below for waste electrical and electronic equipment in accordance with the **WEEE Directive** (**Waste Electrical and Electronic Equipment**).



Electrical and electronic equipment must not be disposed of with general household waste.

11.1 For private households

The symbol shown above indicates that electrical and electronic equipment must not be disposed of with general household waste.

Take this product to a designated collection point for proper treatment, recovery, and recycling. The product will be accepted free of charge.

Correct disposal of this product helps conserve valuable resources and prevents potential negative effects on human health and the environment that could result from improper waste handling.

Contact your local authority for information about the nearest designated collection point.

Penalties may be imposed for improper disposal of this waste, depending on national legislation.

11.2 For professional users in the European Union

Before disposing of electrical and electronic equipment, contact your dealer or supplier for further information. Observe the country-specific regulations.

11.3 For disposal in countries outside the European Union

The symbol shown above is valid only in the European Union, **EU**. Before disposing of this product outside the EU, ask your local authorities or your dealer for the correct disposal method.

11.4 Packaging material

Dispose of the packaging material in accordance with the applicable national regulations.

Chapter 12

Technical data

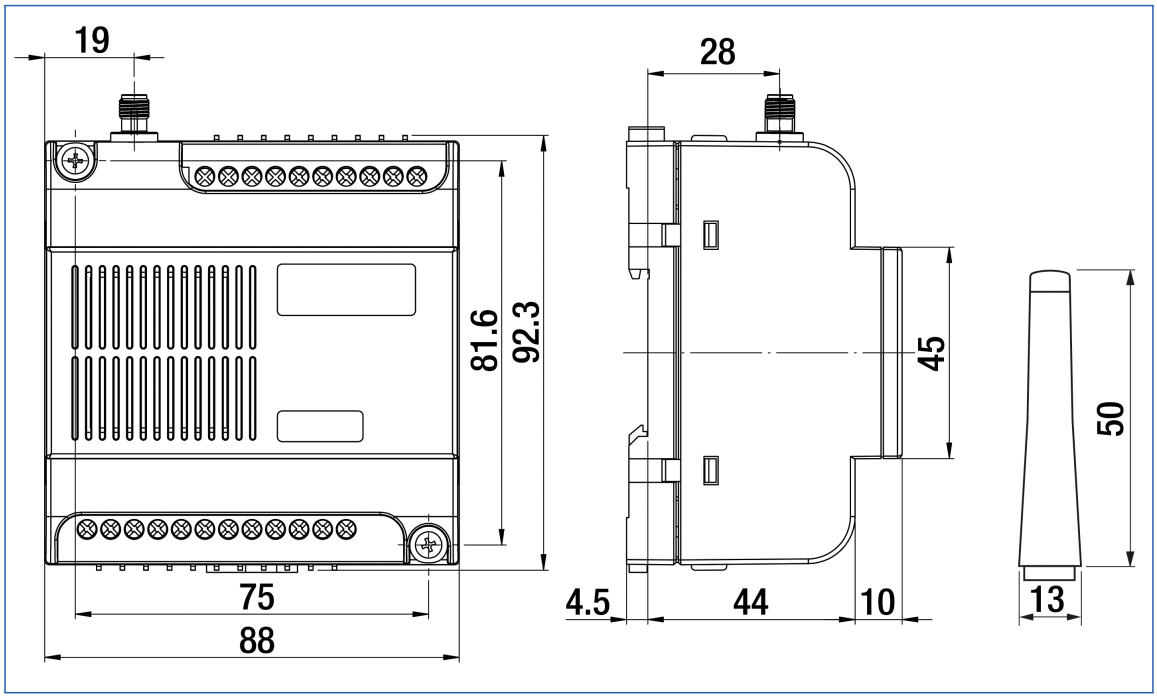


Figure 12.1: CMS-10R technical data overview.

12.1 Data sheets for your device type

For the technical data of your device type, open the **CMS-10R data sheets** section on the ComatReleco web portal. Data sheets are available for all device types.

Use the ComatReleco download area.

Chapter A

Glossary

Term	Explanation
2FA	Two-factor authentication verifies a user's identity using two different, independent factors: a password and an app. See also Section 7.2.4, Set up two-factor authentication (2FA).
2G GSM	Second-generation (2G) digital cellular networks used by mobile terminals.
3G UMTS	Third-generation (3G) digital cellular networks used by mobile terminals.
4G LTE	Fourth-generation (4G) digital cellular networks used by mobile terminals.
Call-in	Control of a digital output by telephone call. See also Section 6.2.5, Configure and control relay outputs: Outputs
CMS-10R	**C**omatReleco **M**essaging **S**ystem.
Confirmation loops	An escalation chain that contacts several subscribers in succession, depending on the service profile, by push message, SMS, pager message, e-mail, or voice call. The chain stops as soon as one participant acknowledges the notification by push message, SMS, e-mail, or voice call. See also Section 6.2.6, Configure notifications and acknowledgement: Events
dBm	Unit used to express a power ratio in decibels **(dB)** relative to one milliwatt **(mW)**. See also Section 6.2.1, Check device status: Overview
Delay time	The value entered in the delay window. It postpones sending a message by the specified time. See also Section 6.2.6.1, Menu: Power on / off
E-mail messages	Messages sent from the CMS-10R device via the Internet.
Event	A notification sent by push message, SMS, pager message, e-mail, or voice call. Depending on the service profile, a defined number of events per month is available.
Fallback mode	If the IoT Portal fails, pending events are sent directly from the device via SMS to defined message recipients. See also Section 3.8, What happens during interruptions, resets, and updates
Firmware	Operating software used to load and run the user software. See also Section 6.2.1, Check device status: Overview
Firmware Over the Air (FOTA)	Updating the system software (firmware) via the mobile network. See also Section 6.3, Update the device firmware
GSM	**G**lobal **S**ystem for **M**obile Communications, a mobile communications standard for fully digital mobile radio networks. It is mainly used for telephony, packet-switched data transmission, and short messages. See also Section 3.7.1, Network coverage
GUI	**G**raphical **U**ser **I**nterface.
IoT	**I**nternet **o**f **T**hings. See also Chapter 5, Commission the device in the IoT Portal
IoT Portal	Virtual data storage in the cloud. See also Section 5.1, Access the IoT Portal and plan commissioning
LED	**L**ight **E**mitting **D**iode, used as an indicator lamp. See also Section 3.4, Locate terminals, controls, and status indicators
Limit value (upper, lower)	A threshold that triggers an action when an input value exceeds it or falls below it. See also Section 6.2.4.2, Configure analogue inputs
MCU	**M**icro **C**ontroller **U**nit. See also Section 6.2.1, Check device status: Overview
Neutral conductor	Returning conductor or cable that transmits electrical energy. See also Section 3.4, Locate terminals, controls, and status indicators
Outer conductor	Voltage-carrying conductor or cable, commonly referred to as a "pole conductor" or "phase", that transmits electrical energy. See also Section 3.4, Locate terminals, controls, and status indicators
Pager message	A notification that sends text to the recipient's pager display.
Provider	Mobile network operator. See also Section 6.2.1, Check device status: Overview
Push message	Notification that appears on a phone without opening the relevant app.
Spam (folder)	Also referred to as the "junk mail folder". Folder for unsolicited mass e-mail messages.
SMS message	**S**hort **M**essage **S**ervice. A mobile phone service that sends short text messages to the recipient's display.
Threshold	Equivalent to limit value. See also Section 6.2.4.2, Configure analogue inputs
TLS	**T**ransport **L**ayer **S**ecurity, an encryption protocol for secure data transmission over the Internet. See also Section 2.7, Information security

Term	Explanation
UTC time zone	Coordinated Universal Time. Enter the time zone of the device location in the **Manage** menu. The time zone can usually be found in the clock app on a mobile phone or on the Internet, for example at timeanddate.com. Examples: London = UTC, Bern = UTC + 1, New York = UTC - 5. See also Section 6.2.2, Manage device settings and ownership: Manage
Voice call	Voice call transmitted from the CMS-10R device via the telephone network.
VPN	**V**irtual **P**rivate **N**etwork, providing encrypted remote access. See also Section 2.7, Information security
Watchdog	The watchdog monitors the operating software. See also Section 3.8, What happens during interruptions, resets, and updates, and Section 2.3, Who may install and use the device