KM2

en

Manual

KM2 Communication module

beginning with firmware version 3.00

Approvals:

Meets Class B: ICES & FCC Part 15

Contains IC: 25416-OMEGA2S

Contains FFC ID: 2AJVP-O2S

Thank you for buying this product.

Please read this manual carefully to get the best performance from this unit. Please keep this manual safe.

Safety advice

Please pay attention to the following safety advice in order to avoid danger and damage to people and property.

- Danger of electric shock: Do not use the device if it is visibly damaged!
- If the mains adapter or its cable is damaged, it has to be replaced by an identical mains adapter, which is available from the manufacturer or its customer service.

The device must not be used by children or persons with reduced physical, sensory or mental abilities or without any experience and knowledge. Make sure that children do not play with the device!

Only connect accessories authorised by the manufacturer to the device.

Make sure that the housing is properly closed before commissioning the device.

Target group

These instructions are exclusively addressed to authorised skilled personnel.

Only qualified electricians are allowed to carry out electrical works.

Initial commissioning must be effected by authorised skilled personnel.

Authorised skilled personnel are persons who have theoretical knowledge and experience with the installation, commissioning, operation, maintenance, etc. of electric/electronic devices.

Instructions

Attention must be paid to the valid local standards, regulations and directives!

Subject to technical change. Errors excepted.

Information about the product

Proper usage

The KM2 Communication module is designed for the connection to a controller via VBus® and is used for forwarding the system data to VBus.net as well as for parameterising the controller connected in compliance with the technical data specified in this manual.

Any use beyond this is considered improper.

Proper usage also includes compliance with the specifications given in this manual.

Improper use excludes all liability claims.

Note

Strong electromagnetic fields can impair the function of the device.

➔ Make sure the device as well as the system are not exposed to strong electromagnetic fields.

EU Declaration of conformity

The product complies with the relevant directives and is therefore labelled with the CE mark. Hereby, RESOL – Elektronische Regelungen GmbH declares that the radio equipment type KM2 Communication module is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following Internet address: www.resol.com

Included

The scope of delivery of this product is indicated on the packaging label.

Storage and transport

Store the product at an ambient temperature of 0 … 40 °C and in dry interior rooms only.

Transport the product in its original packaging only.

Cleaning

Clean the product with a dry cloth. Do not use aggressive cleaning fluids.

Data security

Change and note down the remote access password and keep it in a suitable place.

In order to delete personal data, reset the device to its factory settings before disposal / decommissioning / transfer to a third party.

Decommissioning

1. Disconnect the device from the power supply.
2. Dismount the device.

Disposal

- Dispose of the packaging in an environmentally sound manner.
- At the end of its working life, the product must not be disposed of as urban waste. Old appliances must be disposed of by an authorised body in an environmentally sound manner. Upon request we will take back your old appliances bought from us and guarantee an environmentally sound disposal of the devices.

Description of symbols

Warnings are indicated with a warning symbol!

Signal words describe the danger that may occur, when it is not avoided.

ATTENTION **means that damage to the appliance can occur.**

➔ It is indicated how to avoid the danger described.

Note
Notes are indicated with an information symbol.

➔ Texts marked with an arrow indicate one single instruction step to be carried out.

1. Texts marked with numbers indicate several successive instruction steps to be carried out.

KM2 Communication module

The KM2 Communication module is the ideal interface between a solar or heating controller and the Internet. In only a few steps, the controller can be connected to the VBus.net visualisation portal.

The communication module is suitable for all controllers with VBus® and enables the easy and secure access to system data via VBus.net. Remote access to your controller via the RPT Parameterisation Tool is also possible.

Navigator

Installation page 24

Application examples page 27

Web interface page 29

Troubleshooting page 35

Contents

1 Overview ... 23
2 Scope of delivery ... 23
3 Installation ... 24
3.1 Mounting ... 24
3.2 Electrical connection ... 24
3.3 (W)LAN connection ... 25
4 Indication and operating elements ... 26
4.1 Operating control LED ... 26
4.2 Button ... 26
5 Application examples ... 27
5.1 Direct service access via WLAN access point ... 27
5.2 Connection to the router ... 27
5.3 Connection to VBus.net ... 28
5.4 Configuration for RPT ... 28
6 Finding the communication module in the network ... 29
6.1 DeviceDiscoveryTool ... 29
7 Web interface ... 29
7.1 Menu ... 29
7.2 Setup assistant ... 30
7.3 Menu overview ... 30
7.4 Displaying general device information ... 30
7.5 Displaying the connection status ... 31
7.6 Displaying remote access over Internet ... 31
7.7 Displaying network configuration information ... 31
7.8 Displaying WLAN connection information ... 31
7.9 Displaying access point information ... 31
7.10 Changing the Web interface language ... 31
7.11 Changing the device name ... 31
7.12 Configuring the user mode ... 31
7.13 Configuring date and time settings ... 32
7.14 Carrying out updates ... 32
7.15 Network configuration ... 33
7.16 Changing general WLAN settings ... 33
7.17 Changing WLAN STA settings ... 33
7.18 Changing access point settings ... 34
7.19 Configuring the remote access ... 34
7.20 Changing the user password ... 34
8 Troubleshooting ... 35
9 Ordering software ... 35
10 Spare parts ... 35

1 Overview

- Internet access to the system data via VBus.net
- Comfortable system parameterisation via the RPT Parameterisation Tool possible
- Suitable for all controllers with VBus®
- WLAN functionality
- Automatic firmware updates

Technical data

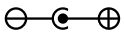
Housing: plastic
Ingress protection: IP 20 / EN 60529
Protection class: III
Ambient temperature: 0 … 40 °C
Maximum altitude: 2000 m above MSL
Relative humidity: 10 … 90 %
Dimensions: 95 × 70 × 25 mm
Mounting: wall mounting (optional)
Display: operating control LED

Approvals:
Meets Class B: ICES & FCC Part 15
Contains IC: 25416-OMEGA2S
Contains FFC ID: 2AJVP-O2S

Interfaces: VBus® for the connection to the controller, 10/100 Base TX Ethernet, Auto MDIX, WLAN 2.4~2.4835 GHz
WLAN encryption: WPA / PSK, WPA2 / PSK
Transmit power limit (e.i.r.p.): < 100 mW
Power consumption: < 1.75 W
Power supply:
Mains adapter: 100 – 240 V~, 1 A / 12 V ⎓, 1 A (Level 6)
Communication module: 12 V ⎓, 120 mA
Electrical energy source: ES1 (EN 62368-1)
Electrical power source: PS1 (EN 62368-1)
Thermal energy source: TS1 (EN 62368-1)
Mechanical energy source: MS1 (EN 62368-1)

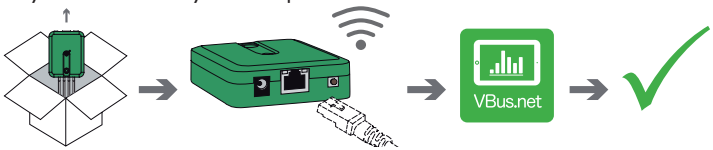
Use mains adapter in dry interior rooms only.

Mains adapter protection class: II



Coaxial connector polarity:
internal: plus
external: minus (GND)

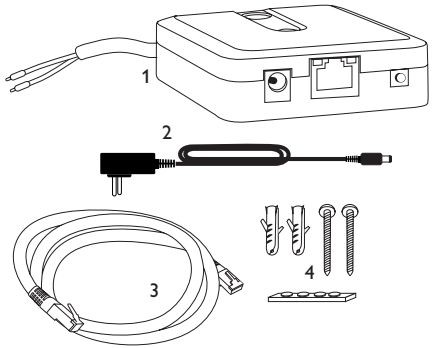
Easy installation in only three steps



Note
After commissioning, check whether the latest firmware version is installed on the device. The current firmware can be downloaded from www.resol.com/firmware.

➔ If a newer firmware version is available, update the device!

2 Scope of delivery



If one of the items mentioned below is missing or defective, please contact your distributor:

1	Communication module incl. mains adapter, VBus® cable pre-connected
2	Interchangeable mains adapter plugs (EURO, UK, USA, AUS)
3	Network cable (CAT5e, RJ45), 2 m
4	Wall plugs, screws and rubber pads
	Manual (not illustrated)

3 Installation

ATTENTION! ESD damage!

Electrostatic discharge can lead to damage to electronic components!

➔ **Take care to discharge properly before touching the inside of the device! To do so, touch a grounded surface such as a radiator or tap!**

The device comes with a VBus® cable already connected to the device.

The housing does not have to be opened in order to mount the device.

Initial commissioning must be effected by authorised skilled personnel.

3.1 Mounting

Note

Strong electromagnetic fields can impair the function of the device.

➔ Make sure the device as well as the system are not exposed to strong electromagnetic fields.

The device must only be located in dry interior rooms.

In order to prevent disturbances caused by electromagnetic fields, pay attention to separate routing of mains cables and bus cables.

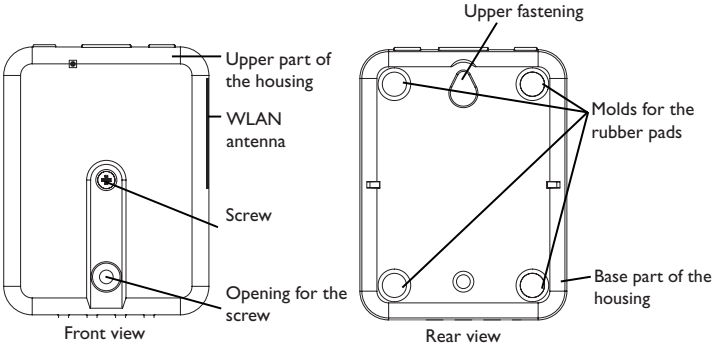
4 self-adhesive, skid-proof rubber pads are included with the device. If necessary, these can be affixed to the corresponding molds on the base part of the housing to ensure a secure placement of the device without wall mounting.

If desired, the device can be mounted to a wall. To do so, proceed as follows:

1. Mark the desired position on the wall.
2. Drill and prepare the hole with a wall plug and screw.
3. Hang the housing from the upper fastening point and mark the lower fastening point (centres 70 mm).
4. Insert lower wall plug.
5. Fasten the housing to the wall with the lower fastening screw and tighten.

Note

Wall materials reduce the WLAN range.



3.2 Electrical connection

ATTENTION! ESD damage!

Electrostatic discharge can lead to damage to electronic components!

➔ Take care to discharge properly before touching the inside of the device! To do so, touch a grounded surface such as a radiator or tap!

ATTENTION! Short circuit!

A short circuit can lead to damage to electronic components!

➔ Establish the power supply only after you have connected all cables required to the terminals and closed the housing.

If the mains adapter or its cable is damaged, it has to be replaced by an identical mains adapter, which is available from the manufacturer or its customer service.

Do not use the device if it is visibly damaged!

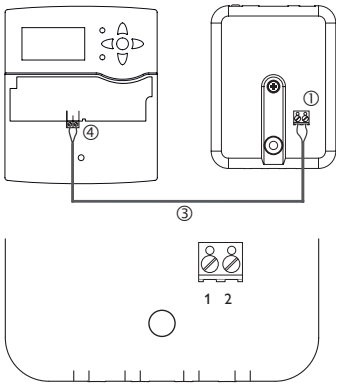
The device is to be connected to the controller via the pre-connected VBus® cable (terminals 1 and 2). The corresponding terminal allocation is described in the controller manual.

The VBus® cable can be extended using a 2-wire cable (bell wire).

With the VBus®-Repeater distances of up to 150 m between the controller and the communication module are possible.

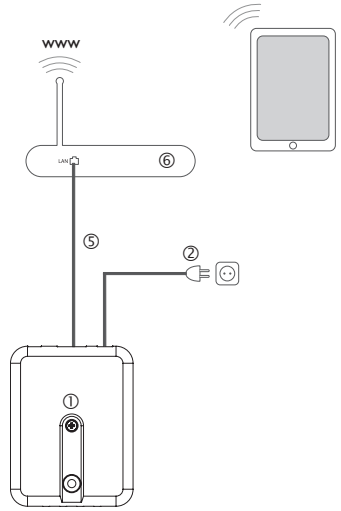
Carry out the connection of the device ① to the controller / other modules in the order described below:

1. Connect the data cable (VBus®, ③) to the controller ④. If necessary, extend the cable using a 2-wire cable (bell wire).



Connection terminals of the communication module

2. Connect the device to the mains by means of the mains adapter ②.
3. For a direct connection to a router, connect the device to a router ⑥ using the network cable (included with the device, ⑤). Alternatively use the WLAN connection.

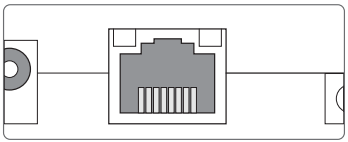


3.3 (W)LAN connection

The device can be connected to a router by using a network cable (CAT5e, RJ45 or similar) or via WLAN (see chap. 4.2 on page 26).

➔ Connect the network cable included to the LAN connector of the router and to the LAN connector of the device.

For the next step of commissioning, see chap. 5.3 on page 28.

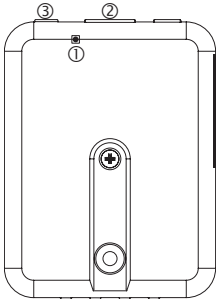


The LAN connector is located on the front side of the device and supports transfer rates of up to 100 MBit per second.

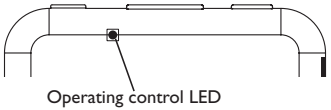
4 Indication and operating elements

The following elements are featured on / in the housing of the device:

① Operating control LED
② LAN connector
③ Button



4.1 Operating control LED

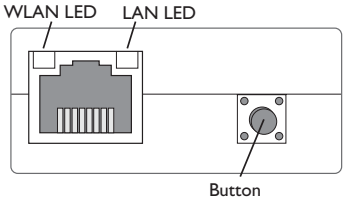


The operating control LED indicates the operating status of the device:

LED flashing codes

Colour	Permanent	Flashing
Red	VBus® signal available, no connection to VBus.net	No VBus® signal
Green	VBus® signal and connection to VBus.net (if the VBus.net option is enabled) available	VBus® signal and IP address available, no connection to VBus.net although the VBus.net option is enabled
Red / green		The device is booting
LED off	No mains voltage	

4.2 Button



With the button, the following functions can be carried out:

- **WLAN:**

The button can be used for activating or deactivating the WLAN connection, respectively. If the WLAN is activated, the WLAN LED glows orange.

➔ In order to activate or deactivate the WLAN, respectively, press the button for approx. 1 s.

- **Reset:**

The button can be used for carrying out a reset in order to set back the configuration of the device to the factory settings.

➔ In order to reset the device, press the button for approx. 20 s.

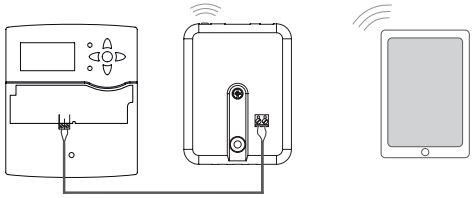
The device will restart, the settings and passwords set back to factory settings. This process may take several minutes.

Note
After a reset, the device has to be added to VBus.net again.

5 Application examples

5.1 Direct service access via WLAN access point

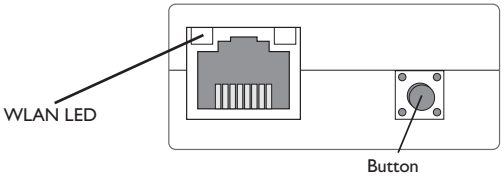
The access point allows the installer to directly connect with the device without having to access the network of the customer. All access data required can be found on the underside of the housing.



Controller | KM2 – Internal WLAN access point | KM2 Web interface

In order to connect a mobile to the device via the WLAN access point, proceed as follows:

1. If the WLAN LED is not illuminated, briefly press the button.



The WLAN access point is activated.

2. Select the WLAN network of the device on your mobile and enter the Network name (SSID).

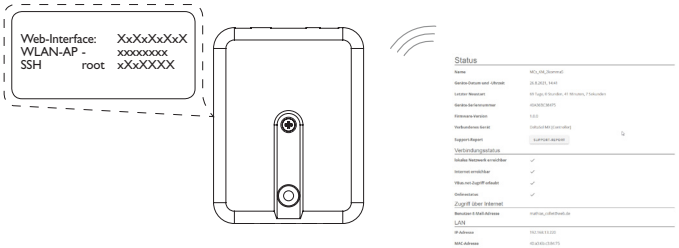
The default SSID name is KM2-{12-digit serial number}.

3. Click **Connect**.
4. Enter the WLAN code of the device.

This code can be read from the label on the underside of the housing (WLAN-AP).

5. Establish the connection.

After the WLAN connection to the device has been established, the Web interface can be reached with an Internet browser under the IP address http://192.168.240.1 or the controller can be parameterised over RPT. If you access the website in its encrypted version (https), a security enquiry may appear. You can either ignore this warning or access the unencrypted version (http).



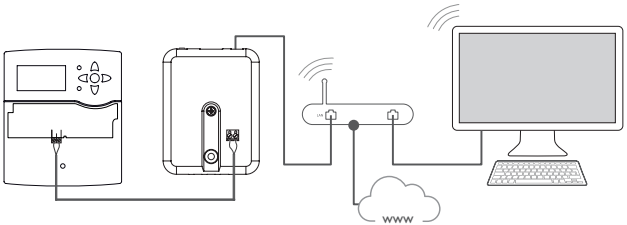
Note
if **Refresh** is clicked in the **WLAN-STA** menu, the WLAN access point connection is automatically disconnected.
➔ Re-establish the connection.

Note
If a WLAN has been selected in the **Available wireless networks** menu item and if **Join** is clicked, the WLAN access point connection is automatically disconnected.
➔ Re-establish the connection.

5.2 Connection to the router

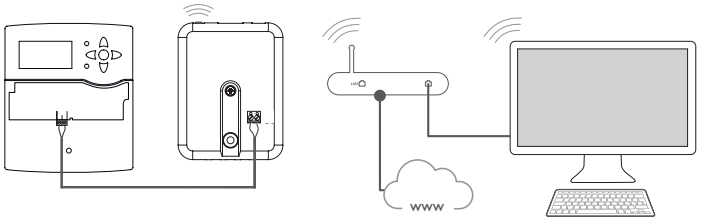
The device can be connected to a router via LAN or WLAN, in order to have access to the home network and additionally to the Internet.

5.2.1 Connection via LAN



Controller | KM2 | Router | Internet device

5.2.2 Connection via WLAN



Controller KM2 Router Internet device

For further information, see:

chap. 3.3 (W)LAN connection on page 25

chap. 1 Overview on page 23

chap. 7.15 Network configuration on page 33

chap. 7.19 Configuring the remote access on page 34

5.3 Connection to VBus.net

For the connection to VBus.net, the communication module requires an Internet connection (via LAN or WLAN) as well as a VBus.net account.

Note
In order to enable VBus.net access, the device must have unrestricted access to the ports 80 and 1194 - 1197.

In order to access the communication module over the VBus.net server, proceed as follows:

1. Note down the alphanumeric 8-10-digit code (Token) indicated on the underside of the housing.
2. Enter VBus.net into the address bar of the browser and click **Sign up**.
3. Wait for the confirmation e-mail (check spam folder if necessary).
4. Click **Add new device**.
5. Enter the alphanumeric 8-10-digit code (Token).

For further information, see:

chap. 3.3 (W)LAN connection on page 25

chap. 1 Overview on page 23

chap. 7.19 Configuring the remote access on page 34

5.4 Configuration for RPT

In order to use RPT, **VBus.net access over the local network** has to be enabled, see chap. 7.19 on page 34.

5.4.1 Using RPT without VBus.net

In order to use RPT without VBus.net, proceed as follows:

1. Download and install the software.
2. Select the **Communication** menu.
3. Click **Connect**.
4. Select the **DL2/KM1/KM2** interface.
5. Enter the URL/IP address.
6. Enter the password into the **Password** field.
7. Click **Connect**.

5.4.2 Using RPT via VBus.net

In order to use RPT via VBus.net, **Remote access over Internet** has to be enabled, see chap. 7.19 on page 34.

With a VBus.net account you can easily use RPT in order to parameterise the controller over the Internet:

1. In the VBus.net menu **My Devices**, click on **Edit**.
2. On the **General settings** page, tick the option **Allow parameterization using the via address and the RESOL Parameterization Tool (RPT)**.
3. Download and install the software.
4. Select the **Communication** menu.
5. Click **Connect**.
6. Select the **DL2/KM1/KM2** interface.
7. Enter the via tag from the VBus.net menu item **General settings** into the RPT field **URL/IP**.
8. Enter the password into the **Password** field.
9. Click **Connect**.

6 Finding the communication module in the network

6.1 DeviceDiscoveryTool

The DeviceDiscoveryTool is a software that displays RESOL products connected via the local network.

There are different possibilities to start the DeviceDiscoveryTool:

- Starting the tool from the hard disk after having downloaded it from https://www.resol.de/de/software
- Starting the tool from VBus.net (under **Tools**)

Starting the DeviceDiscoveryTool

In order to start the DeviceDiscoveryTool, proceed as follows:

1. Open the folder **discovery-tool-xxx**.
2. Start **discovery-tool Setup xxx**.
3. Confirm all following dialogues with **OK**.
4. Click **Start/Programs/discovery-tool**.
5. Click **Find devices**.

All LAN-enabled RESOL products available in the network will be displayed.

6. Click the **Open Web interface** button of the corresponding device.

A new window with the Web interface will open.

7. Enter the password, see chap. 7.1 on page 29.

Note
The password can be found on the underside of the housing (**Web-Interface**).

Note
After commissioning, check whether the latest firmware version is installed on the device. The current firmware can be downloaded from www.resol.com/firmware.

➔ If a newer firmware version is available, update the device!

7 Web interface

The Web interface is integrated in the device and runs on an Internet browser.

The Web interface has the following functions:

- Display device status
- Configure device

Note
If display problems occur, update the Internet browser or use a different browser.

7.1 Menu

All main menus and the **Login** menu item are displayed in the bar at the top of the Web interface.

Note
The menu structure may change in later firmware versions.

Note
The indicated information and setting possibilities depend on the user mode selected, see chap. 7.3 on page 30.

In order to use the Web interface to its full extent, a login is required. In order to log in, proceed as follows:

1. Click **Login** on the menu bar.

The **Login** window appears. The password can be found on the underside of the housing (**Web-Interface**) or on the last page of this manual.

Web-Interface:		XxXxXxXxX
WLAN-AP -		xxxxxxxx
SSH	root	xXxXXXX

2. Enter the password into the **Password** field.
3. Click the **Login** button.

7.2 Setup assistant

When the Web interface of the device is accessed for the first time, a setup assistant appears. The setup assistant allows you to change passwords.

ATTENTION! Third-party access!

When the default password is not changed, third parties may gain unauthorised access to the controller connected.

➔ **Change and note down the password and keep it in a suitable place.**

For security reasons, it is strongly recommended that you change the Web interface password in the menu item **Change admin password**.

In order to do so, proceed as follows:

1. Enter the default password into the **Password** field.
2. Enter the new password into the **New password** field.
3. Enter the new password into the **Confirm new password** field.
4. Click **Change password**.
5. Click **Next step**.

For security reasons, it is strongly recommended that you change the access point password in the menu item **Change access point password**.

In order to do so, proceed as follows:

1. Enter the new password into the **New password** field.
2. Enter the new password into the **Confirm new password** field.
3. Click **Change password**.
4. Click **Next step**.

After making the changes, click **Complete setup** in the **Done** menu item.

7.3 Menu overview

Main menu	Submenu	Function
Home	-	-
Status	Status	Displaying general device information Displaying the connection status Displaying remote access over Internet Display LAN / WLAN information Displaying access point information
Configuration	General	Change general configuration Run VBus specifications update Run firmware update
	Date and time	Change date and time configuration
	Network	Change LAN configuration Change WLAN settings Change WLAN STA settings Change access point settings
	Remote access	VBus.net access over local network Configure remote access over Internet
	Users	Change password
About	General	Order KM2 Communication module open source software
	Powered by	Display the open source applications and libraries used
	History	Display firmware updates
Login/Logout	-	Log in and log out

7.4 Displaying general device information

In order to display general device information, proceed as follows:

➔ Click the **Status** main menu.

The following information is displayed in **Status**:

- Name
- Date and time
- Device uptime
- Serial number
- Firmware version
- Device connected
- Support report

7.5 Displaying the connection status

In order to display the connection status, proceed as follows:

➔ Click the **Status** main menu.

The following information is displayed in **Connection status**:

- Local network accessible
- Internet accessible
- VBus.net access enabled
- Online status

7.6 Displaying remote access over Internet

In order to display the status of the remote access over Internet, proceed as follows:

➔ Click the **Status** main menu.

The following information is displayed in **Remote access over Internet**:

- User e-mail address or Token

7.7 Displaying network configuration information

In order to display the network configuration, proceed as follows:

➔ Click the **Status** main menu.

The following information is displayed in **LAN**:

- IP address
- MAC address

7.8 Displaying WLAN connection information

In order to display the WLAN connection information, proceed as follows:

➔ Click the **Status** main menu.

The following information is displayed in **WLAN**:

- Network name (SSID)
- Signal strength (for more information on signal strength, see chap. 7.17 on page 33).
- Encryption
- Channel
- IP address
- MAC address

7.9 Displaying access point information

In order to display access point information, proceed as follows:

➔ Click the **Status** main menu.

The following information is displayed in **Access point**:

- Network name (SSID)
- Encryption
- MAC address
- Channel
- IP address

7.10 Changing the Web interface language

The Web interface can be displayed in different languages.

➔ Click the flag to select the language.

- German
- English
- French
- Spanish
- Italian

The language is then changed for this session.

7.11 Changing the device name

Note
Choose a descriptive device name to facilitate identifying the device in the network.

In order to change the device name, proceed as follows:

1. In the **Configuration** main menu, select the **General** submenu.
2. In the **General Configuration** menu, enter the device name in the **Device name** field.

Permitted characters are: letters, numbers, underscores, hyphens.

Special characters are not allowed.

3. Click **Save configuration**.

7.12 Configuring the user mode

The user mode of the Web interface can be changed from standard user to expert and vice versa. In the expert mode, additional information and settings are available, such as: LAN configuration, LAN information, firmware updates, etc.

In order to adjust the user mode, proceed as follows:

1. In the **Configuration** main menu, select the **General** submenu.
2. Activate the expert mode in the **Expert mode** menu item.
3. Click **Save configuration**.

7.13 Configuring date and time settings

The date and time configuration determines where the device obtains its date and time information.

The device receives the date and time configuration automatically via the adjustable time zone (factory setting UTC). Settings can also be carried out manually.

In order to adjust date and time manually, proceed as follows:

1. In the **Configuration** main menu, select the **Date and time** submenu.
2. Tick the **Set date / time** field.
3. Adjust the date in the date field.
4. Adjust the time in the time field.
5. Click **Save configuration**.

7.14 Carrying out updates

If the device is connected to the Internet, it automatically checks for available updates once a week. Updates available are indicated during login.

➔ In order to start the update query manually, click on the **Query updates** button in the **Configuration** main menu, **General** submenu.

7.14.1 Carrying out a VBus® specifications update

In order to make sure that the controller connected can be recognised and read out to its full functional extent, VBus® specification updates are provided on the Internet.

The update can be carried out over the Internet or via a computer connected to the device.

If the device is connected to the Internet, it will find and upload the update file automatically.

➔ In order to carry out the update, click **Install**.

After the update has been carried out, the device will restart. A new login is required.

An update can also be installed via a computer connected to the device.

In order to carry out the update, proceed as follows:

1. Download the **vbus_specification.cbor** update file onto the computer.
2. In order to upload the update file, click **Select**.
3. Select the update file and confirm the selection.

After the upload has been completed, the update file appears in the Web interface.

4. In order to carry out the update, click **Install**.

After the update has been carried out, the device will restart. A new login is required.

If no update is to be carried out, click **Discard**.

7.14.2 Carrying out a firmware update

The firmware is the internal software of the device.

Note
Previous configurations will not be affected by a firmware update.

In order to configure and carry out firmware updates, proceed as follows:

➔ In the **Configuration** main menu, select the **General** submenu.

The **Download firmware updates automatically** menu item in the **Firmware update** menu, is activated by default.

The device checks for updates weekly. If an update is available, it will be downloaded.

In the **Perform downloaded updates** menu item you can select how to proceed with downloaded updates:

- **automatically**: downloaded updated are installed automatically.
- **after manual confirmation**: downloaded updates are installed after manual confirmation only.

If you change the default setting, click **Save configuration**. The message **Successful** appears.

If an update has been downloaded but not carried out automatically, proceed as follows:

➔ Under **Version available**, click the **Install** button.

Note
The automatic download of firmware updates requires an Internet connection.

If the automatic download has been deactivated, it is possible to query updates manually.

1. In the **Configuration** main menu, select the **General** submenu.
2. In the **General configuration** menu, click the **Query updates** button.

Updates available are indicated in the **Firmware update** menu.

In order to install the update click the **Install** button under **Version available**.

Besides the firmware, source codes and compiler scripts of the open source applications and libraries are downloaded.

The **Upload** menu item can be used to install an older firmware version, e.g. to downgrade the device.

7.15 Network configuration

The network configuration determines where the device obtains its IP information from for the LAN connection.

There are 2 different settings possible for the network configuration:

- **Dynamic (DHCP)**: The IP information is automatically assigned to the device by the DHCP server.
- **Static**: The user manually assigns IP information to the device.

Note
Consult the system administrator before changing the factory settings!

In order to configure the network, proceed as follows:

1. In the **Configuration** main menu, select the **Network** submenu.
2. In the **Address type** dropdown menu, select the desired value.

If the **Static Address type** is selected, further input fields appear.

3. Click **Save configuration**.
4. Restart the device.

The menu item **IP recovery** can be used for automatically retrieving a new IP address for the device in case that the previous one is lost. In order to adjust the automatic IP address configuration, proceed as follows:

1. Activate **IP recovery**.
2. Click **Save configuration**.

As soon as the remote access over Internet has been enabled, the device will check every 15 min if a connection to the VBus.net server exists. If VBus.net does not answer, the device will restart. After the restart, the time starts running from 0 on in **Device uptime**. A restart can take up to 90 s.

7.16 Changing general WLAN settings

In order to activate or deactivate the WLAN, respectively, proceed as follows:

1. In the **Configuration** main menu, select the **Network** submenu.
2. Activate the WLAN in the **Off/On** menu item.
3. After the WLAN has been activated, select the country the device is to be used in.
4. Click **Save configuration**.

The WLAN can also be activated or deactivated by means of the button, see chap. 4.2 on page 26.

7.17 Changing WLAN STA settings

In order to adjust WLAN STA settings, proceed as follows:

1. In the **Configuration** main menu, select the **Network** submenu.

In the **Available wireless networks** menu item, all networks available are indicated with their signal strength.

2. In order to refresh the display of available wireless networks, click the **Refresh** button.
3. In order to connect to a WLAN, click on the desired network.

If the WLAN connection has already been established, it has to be disconnected first, for all WLAN networks available to be indicated.

4. Enter the WLAN password.
5. Click the **Join** button.

The connection will be established and indicated in the **Network name (SSID)** menu item. To re-establish the WLAN connection, disconnect it first for all WLAN networks available to be indicated.

In order to disconnect a connection, proceed as follows:

1. Select the connection from the **Available wireless networks** menu item.
2. Click the **Disconnect** button.

Note
The WLAN connection uses the DHCP address type.

The **Available wireless networks** menu item also shows the signal strength.

If a connection to a wireless network has been established, but cannot be accessed anymore, no reception will be indicated.

If a WLAN is not displayed but to be used, proceed as follows:

1. Enter the WLAN name into the **Network name (SSID)** field.
2. Select the WLAN encryption type.
3. Enter the WLAN password.
4. Click the **Join** button.

7.18 Changing access point settings

If WLAN is activated, the access point will be automatically active.

In order to make access point adjustments, proceed as follows:

➔ In the **Configuration** main menu, select the **Network** submenu.

In the **Network name (SSID)** menu, the network name can be changed.

In the **Password** menu item, the access point password can be changed.

In the **IP address** menu item, a selection between the IP addresses of the access point can be made.

7.19 Configuring the remote access

The remote access password is required whenever a controller connected to the device is to be accessed via the Parameterisation Tool.

The **Bus access over local network** is deactivated by default. In order to use the bus access, proceed as follows:

1. In the **Configuration** main menu, select the **Remote access** submenu.
2. Activate the access.

Important security information is displayed.

3. Select the security level in the **Bus access over local network** field:

- **Activated (secure)**: encrypted transmission (factory setting after activating the access)
- **Activated (insecure)**: unencrypted transmission

4. Enter the new password into the **New password** field.
5. Enter the new password into the **Confirm new password** field.
6. Click **Save configuration**.

The **Remote access over Internet** is activated by default.

1. In order to deactivate the **Remote access over Internet**, click the corresponding toggle button.
2. Click **Save configuration**.

7.20 Changing the user password

In order to change the user password of the Web interface, proceed as follows:

1. In the **Configuration** main menu, select the **Users** submenu.
2. Under **Change password** click the toggle button.
3. Enter the current password into the **Password** field.

The default password can be found on the underside of the housing (**Web-Interface**).

4. Enter the new password into the **New password** field.
5. Enter the new password into the **Confirm new password** field.
6. Click **Save configuration**.

8 Troubleshooting

Problem	Solution
The user password is not available.	When the user password is not available, the device has to be reset to its factory settings in order to regain access to the Web interface. The password can be found on the underside of the housing (**Web-Interface**).
Signal strength of the WLAN too low.	➔ Use the device in another location. The VBus® cable can be extended to up to 50 m.
The status LED is green although no connection is available.	If all network settings are changed, it might occur that the status LED is not able to signal this change. ➔ Restart the device.
No connection to VBus.net possible.	➔ If the device is connected via WLAN and LAN and if one of the connections is then disconnected, restart the device. ➔ Use one connection type only.
The device is not found by the DeviceDiscoveryTool.	Check the following points in order to find and eliminate the error. ➔ Check if the power supply to the device is established. ➔ Check if the network cable is properly connected at both ends! ➔ Alternatively check the WLAN connection. ➔ Check if the firewall software of the computer inhibits the connection to the device. ➔ Switch off the firewall software and use the DeviceDiscoveryTool to find the device. ➔ When the device has been found, the firewall software has to be reconfigured. ➔ Activate the firewall software! ➔ Check if an IP address is assigned to the device. An IP address has to be assigned to the device by a router.

9 Ordering software

For an expense allowance of EUR 50,-, a DVD containing the source code and the compiler scripts of the open source applications and libraries can be ordered.

Please send your order to:

RESOL – Elektronische Regelungen GmbH

Heiskampstraße 10

45527 Hattingen

GERMANY

Please name the version number of the firmware in your order. It can be found in the Web interface, main menu **About**, submenu General, bottom area (e.g.: „1.0 (200805241128")). Per order, only one version number can be named.

The source code and the compiler scripts of the open source applications and libraries can also be downloaded free of charge.

In order to download the source codes and compiler scripts from the Web interface of the device, proceed as follows:

1. In the **Configuration** main menu, select the **General** submenu.
2. Under **Firmware update**, click **Download firmware**.

Besides the firmware, source codes and compiler scripts of the open source applications and libraries are downloaded.

The firmware can also be downloaded from the RESOL website. Besides the firmware, source codes and compiler scripts of the open source applications and libraries are downloaded.

10 Spare parts

VBus® cable

Article no.: 112091 98

12V DC/1A ZDD mains adapter

Article no.: 11209199

Optionales Zubehör | Optional accessories | Accessoires optionnels | Accesorios opcionales | Accessori opzionali:
www.resol.de/4you

Distributed by:

RESOL – Elektronische Regelungen GmbH

Heiskampstraße 10
45527 Hattingen / Germany

Tel.: +49 (0) 23 24 / 96 48 - 0
Fax: +49 (0) 23 24 / 96 48 - 755

www.resol.com
info@resol.com

Important note

The texts and drawings in this manual are correct to the best of our knowledge. As faults can never be excluded, please note:

Your own calculations and plans, under consideration of the current standards and directions should only be basis for your projects. We do not offer a guarantee for the completeness of the drawings and texts of this manual - they only represent some examples. They can only be used at your own risk. No liability is assumed for incorrect, incomplete or false information and / or the resulting damages.

Note

The design and the specifications can be changed without notice.

The illustrations may differ from the original product.

Imprint

This mounting- and operation manual including all parts is copyrighted. Another use outside the copyright requires the approval of **RESOL – Elektronische Regelungen GmbH**. This especially applies for copies, translations, micro films and the storage into electronic systems.

© RESOL – Elektronische Regelungen GmbH

Ihre kundenspezifischen Einstellungen

de

Gerätename _____

Passwörter

Web-Interface: _____

WLAN-AP: _____

SSH: _____

Fernzugriff: _____

www.vbus.net

Benutzer-E-Mail-Adresse:

_____ @ _____

WLAN

Land: _____

SSID: _____

LAN

Adresstyp:

☐ DHCP

☐ Static IP

Statische IP-Adresse: _____

Subnetzmaske: _____

Standardgateway: _____

Nameserver 1: _____

Ihr Fachhändler

Your customised settings

en

Device name _____

Passwords

Web interface: _____

WLAN AP: _____

SSH: _____

Remote access: _____

www.vbus.net

User e-mail address:

_____ @ _____

WLAN

Country: _____

SSID: _____

LAN

Address type:

☐ DHCP

☐ Static IP

Static IP address: _____

Subnet mask: _____

Default gateway: _____

Nameserver 1: _____

Your distributor

Visualisierungsportal VBus.net (de)

Das KM2 kann ohne Konfiguration mit VBus.net verbunden werden.
Registrieren Sie sich auf www.vbus.net
Die Basic-Version steht kostenlos zur Verfügung.
Aktion für Neukunden: die PRO-Version mit erweitertem Funktionsumfang jetzt 30 Tage kostenlos testen.

VBus.net visualisation portal (en)

The KM2 can be connected to VBus.net without any configuration.
Sign up on www.vbus.net
The basic version is free of charge.
For new customers: test the PRO version with extended functionality for 30 days free of charge.

Portail de visualisation VBus.net (fr)

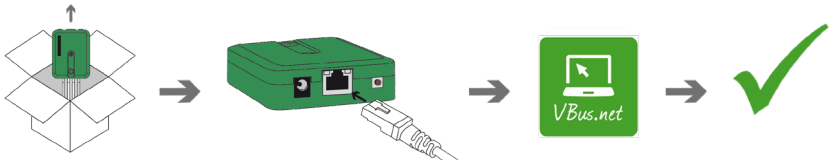
Le KM2 peut être connecté à VBus.net sans configuration.
Créez un compte VBus.net gratuitement.
La version de base est gratuite.
Pour les nouveaux clients : veuillez tester la version PRO avec une gamme de fonctions élargie gratuitement pendant 30 jours.

Portal de visualización VBus.net (es)

El módulo KM2 se puede conectar a VBus.net sin configuración alguna. Regístrese en www.vbus.net
La versión básica está disponible de forma gratuita.
Oferta especial para nuevos clientes: pruebe la versión PRO con funciones ampliadas ahora 30 días de forma gratuita.

Portale di visualizzazione VBus.net (it)

Il KM2 può essere collegato senza dover configurare VBus.net. Registratevi su www.vbus.net
La versione Basic è gratuita.
Promozione per i nuovi clienti: la versione PRO con gamma ampliata di funzioni ora è in prova gratuita per 30 giorni.



Werkseinstellungen / Factory settings / Réglages d'usine / Ajustes de fábrica / Impostazioni di fabbrica

Aufkleber Passwörter hier aufkleben!
Put password labels here!
Appliquez l'autocollant mots de passe ici !
¡Ponga aquí las pegatinas con las contraseñas!
Applicare qui l'adesivo delle password!