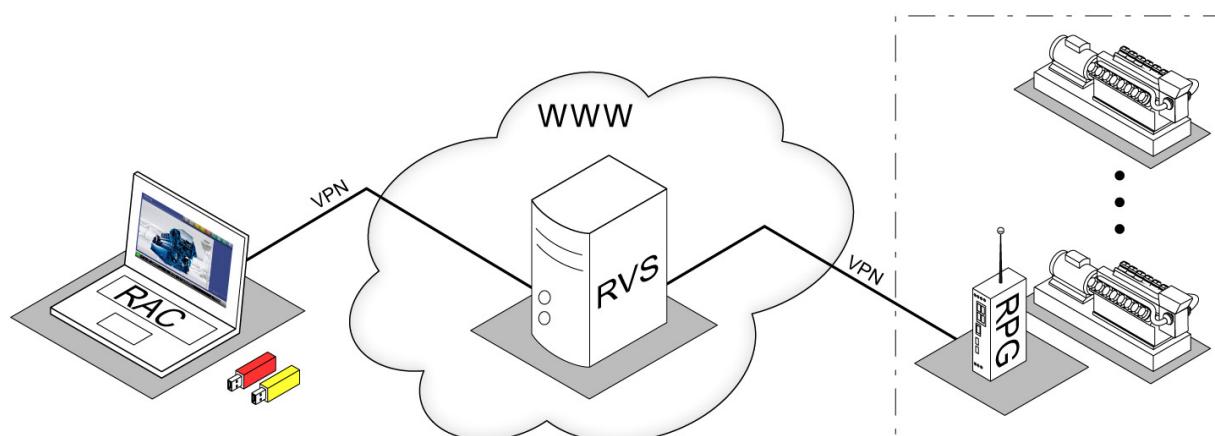




Remote Engine Management

**Remote Engine Management
Part number 12511700, 12511702
Operating manual
2024-09, Language EN
Service Level (SL)**



The original language of this document is German.
All translations are based on the German original.



Technical modifications required to improve our products are reserved with regard to specification data and other technical information contained in the document. No parts of this document may be reproduced in any form or by any means without the written approval of the manufacturer.

The document contains information that is necessary for maintenance and repair work on the product. When performing the work listed in the maintenance schedule, only original parts or parts and operating media approved by the manufacturer may be used.

Masthead
Caterpillar Energy Solutions GmbH
Carl-Benz-Str. 1
68167 Mannheim
Germany

+49 621 384 0
+49 621 384 8800
www.caterpillar-energy-solutions.de
All rights reserved



Contents

1	Safety information	5
1.1	General safety notes.....	5
1.2	Information on operating media.....	5
2	Technical data	7
2.1	Dimensions	7
2.2	Technical data	7
2.3	Rating plate.....	8
3	Structure and function	11
3.1	Description.....	11
3.2	Router	12
3.3	Scope of delivery	16
3.4	List of abbreviations.....	17
4	Assembly	19
4.1	Safety notes.....	19
4.2	Assembly overview	19
4.3	Installing the router in the switch cabinet.....	21
4.4	Installing the mobile antenna (optional).....	22
4.5	Connecting the power supply	23
4.6	Connecting the router to the interface converter ModemKon (single engine plant)	24
4.7	Connecting the router to the Intelligent Selection Unit IAE (multiple engine plant)	26
4.8	Connecting router to the TEM MFR.....	26
4.9	Checking the settings on the Function Selection Unit [FAE]	27
4.10	Checking the settings on the Intelligent Selection Unit (IAE) (multiple engine plant)	27
5	Commissioning	29
5.1	Registering the router and users	29
5.2	Inserting the SIM card (optional).....	32



Contents

5.3	Checking the network settings.....	32
5.4	Connecting a computer to the router	34
5.5	Installing the configuration program.....	37
5.6	Starting the configuration program	39
5.7	Configuring the WAN connection.....	42
5.8	Configuring the mobile connection	44
5.9	Configuring the VPN connection.....	47
5.10	Updating the configuration.....	50
5.11	Changing settings	52
5.12	Final inspection.....	54
5.13	Exporting log data.....	54
6	Operation	57
6.1	Installing a Remote Access Client	57
6.2	Connecting to a plant.....	66
6.3	Closing the connection	80
6.4	Closing the Remote Access Client	82
7	Decommissioning	85
7.1	Decommissioning Remote Engine Management.....	85
8	Troubleshooting	87
8.1	Faults with the router	87
8.2	Faults with the Remote Access Client RAC.....	89
9	Feedback on documentation	91

1 Safety information

1.1 General safety notes

For general safety notes, see Service Library, [Safety and Product Information Specification](#).

- Please take note of all instructions in that document.

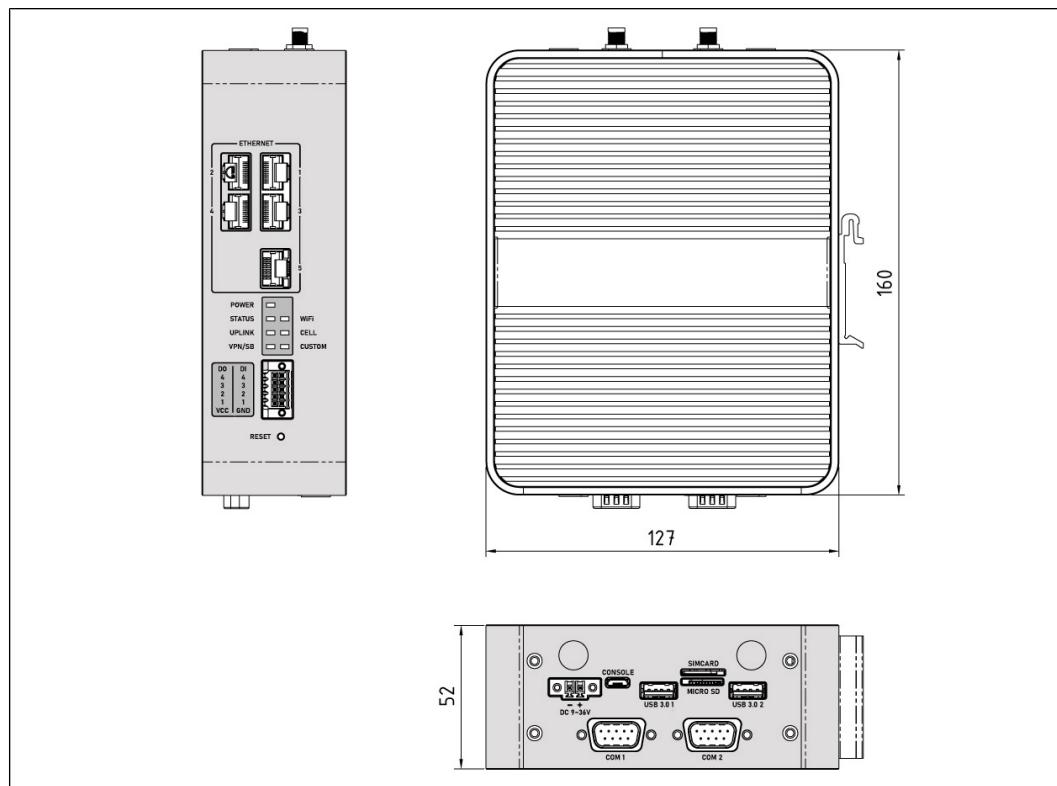
1.2 Information on operating media

All information on operating media can be accessed in the Service Library. When using operating media, observe the respective specification:

- [Specification for fuel gas](#)
- [Specification for auxiliary media](#)
- [Specification for coolant](#)
- [Specification for lube oil](#)
- [Specification for combustion air](#)

2 Technical data

2.1 Dimensions



9007199545339019: Dimensions in millimeters (mm)

2.2 Technical data

Router	
Part number	12524313
Type designation	TEM-RPG-04A
Weight	0.9 kg
Supply voltage	9 V ... 36 V DC
Current consumption	max. 1 A

Router	
Permissible ambient temperature during operation	-20 °C ... +70 °C
Permissible ambient temperature during storage	-40 °C ... +80 °C
Permissible relative humidity of the ambient air	10 % ... 95 % (non-condensing)

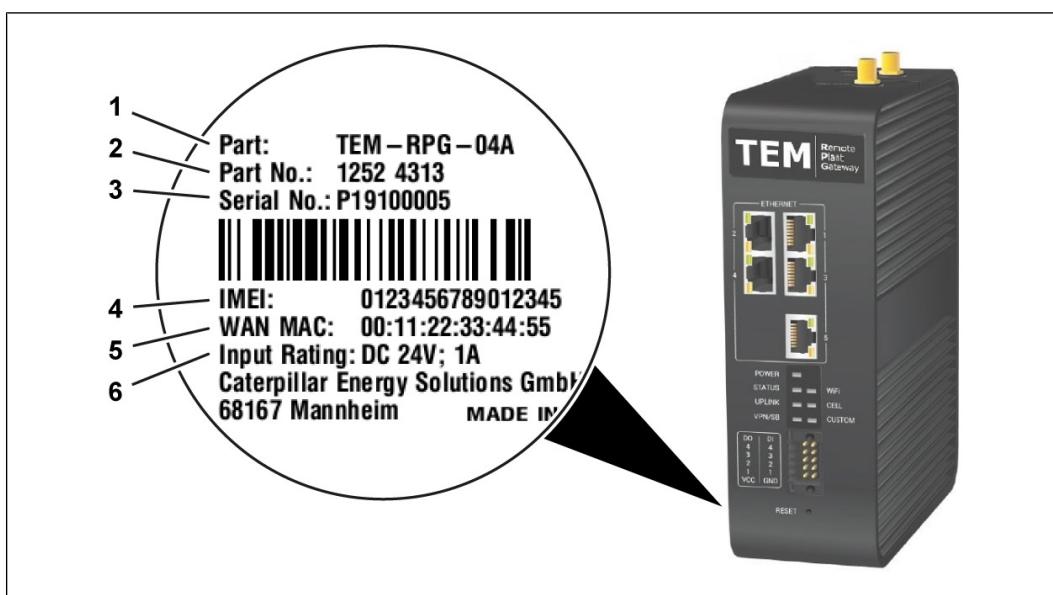
Table 1: Technical data

The serial interface through which the router communicates with the ModemKon interface converter has the following properties:

- Flow control: none
- Serial mode: RS232
- Speed: 9600 bits per second
- Parity: N
- Stop bits: 1
- Server port: 3112
- FIFO size: 64 bytes

2.3 Rating plate

The rating plate is affixed to the left side of the router.



18014398799315083

- 1 Type designation
- 2 Part number
- 3 Serial number
- 4 IMEI of the mobile radio interface
- 5 MAC address of the WAN interface
- 6 Input voltage; current consumption

On the back of the router is a sticker showing the approval logos.

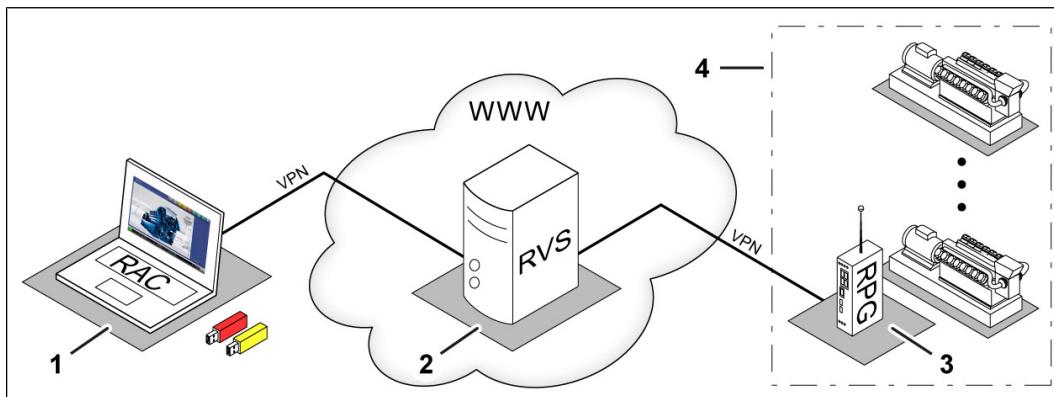


18014398799320075

3 Structure and function

3.1 Description

Remote Engine Management means accessing a genset's control system on a computer via the internet. This way, the genset can be monitored and operated remotely in just the same way as on the operating computer on site.



9007199544542347: Remote access to a plant (schematic representation)

- 1 Computer with a Remote Access Client (RAC) and JView
- 2 Rendezvous Server (RVS)
- 3 Router (Remote Plant Gateway, RPG)
- 4 Plant with one or more gensets

The key component of the Remote Engine Management system is the router. After commissioning, the router (3) automatically establishes a VPN connection to the Rendezvous Server (2) and maintains this connection.

To contact the Rendezvous Server, the router uses an internet connection available at the plant location.

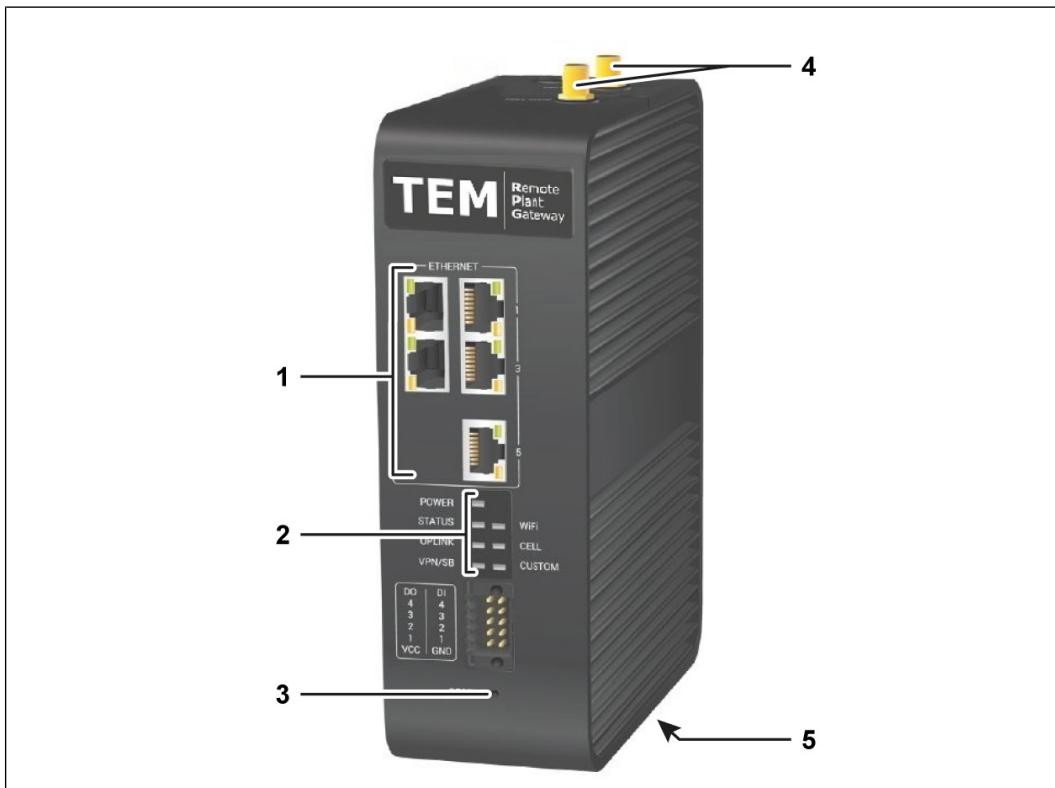
Using the Remote Access Client program RAC, the user establishes a connection to the Rendezvous Server from their computer (1). The Rendezvous Server (2) checks the user's login credentials to see which plants they may access. In the Remote Access Client program, the user can select the plant they wish to connect to.

With the JView program, which has to be installed on the computer (1), the user can access the TEM Evo control system via the established connection. With the Woodward ToolKit program, which has to be installed on the computer (1), the user can access the TEM MFR (if available).

As long as a user is connected to the TEM Evo control system via the router, the operating computer on site is locked.

3.2 Router

Overview



9007199544551307: Router overview

- 1 Ethernet connections 1 to 5
- 2 Status LEDs
- 3 Reset button
- 4 Connections for mobile antennae
- 5 Other connections

The router needs access to the internet to communicate with the Rendezvous Server RVS and get security updates. To access the internet, the router uses either the WAN interface (ethernet connection 5) or the built-in mobile modem.

The prerequisite for using the WAN interface is that there is already an internet connection at the router location. The internet connection should provide a bandwidth of at least 10 MBit/s in uplink and downlink. The packet loss rate must not exceed 18 % and the latency must be under 200 ms.

Mobile modem

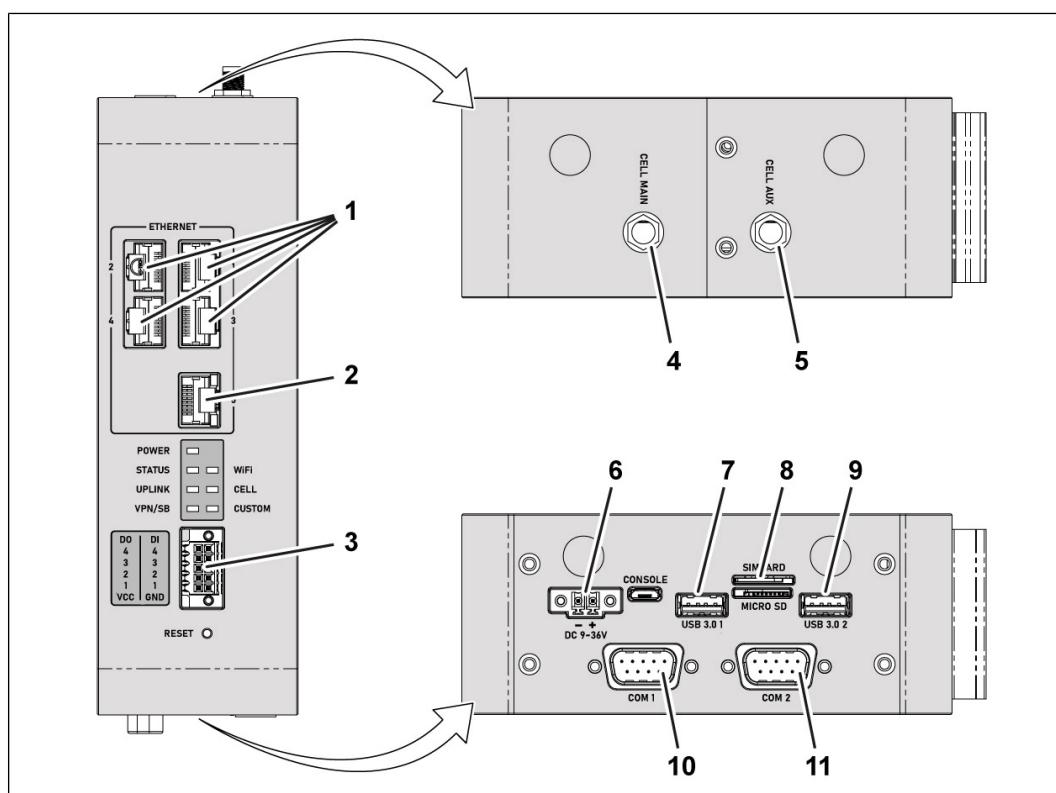
The mobile modem built into the router is functional, but is not supported by us. This means: Even if a mobile network is available on site, we cannot guarantee that the router will connect to the mobile network and transfer data.

If you wish to use the mobile modem, contact your service partner. Note however, that we also do not provide support if there are faults following a successful mobile connection.

The prerequisite for using the mobile modem is that there is a 4G mobile network at the router location. If no 4G mobile network is available, or if the signal is too weak, the router will automatically switch to one of the older mobile networks (3G or 2G). If no 3G or 2G mobile network is available either, then no data transfer via mobile networks is possible. Information for 2G mobile networks: Due to the lower bandwidth and higher latency in the 2G network the Remote Engine Management functions will be limited in this case.

Connections

The router has many connections for other devices and for the supply voltage.



2651026699: Connections to the router

No.	Name	Description
1	ETHERNET 1/2/3/4	LAN connections 1 to 4 (Ethernet, RJ45)
2	ETHERNET 5	WAN connection (Ethernet, RJ45)
3	DO / DI	Digital outputs and inputs
4	CELL MAIN	Sockets for mobile antennae (SMA, not RP-SMA)
5	CELL AUX	Sockets for additional mobile antennae (SMA, not RP-SMA)

No.	Name	Description
6	DC 9~36V	Voltage input (DC 24 V)
7	USB 3.0 1	USB connection 1 (USB 3.0)
8	SIMCARD	SIM card slot (Micro SIM)
9	USB 3.0 2	USB connection 2 (USB 3.0)
10	COM 1	COM connection 1 (RS-232)
11	COM 2	COM connection 2

The mobile antenna must be connected to the socket (4) to use the mobile modem. An additional mobile antenna can be connected to the socket (5). The additional mobile antenna is not required, but can improve reception quality under certain conditions.

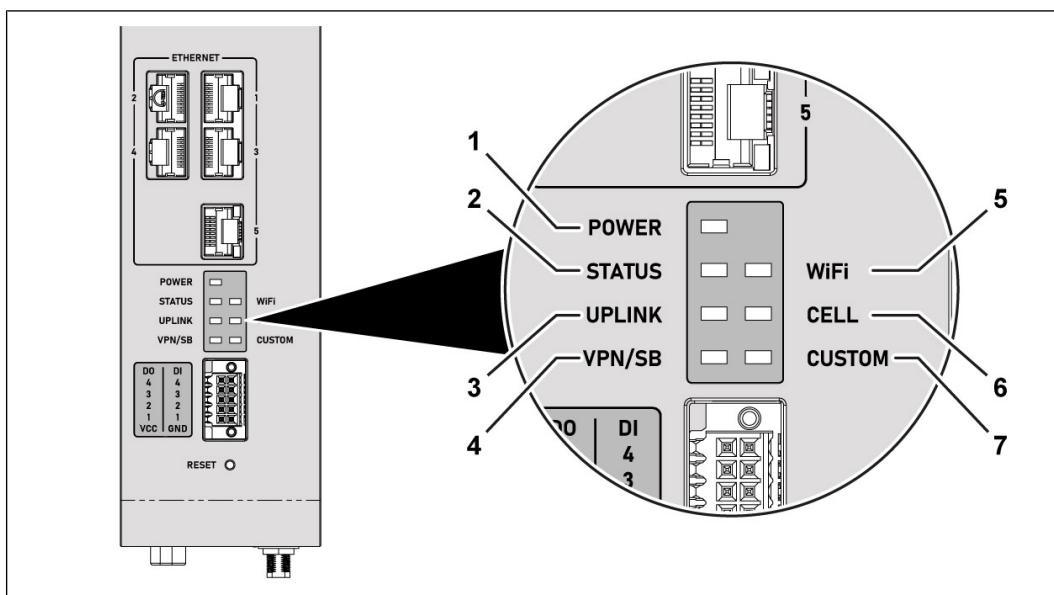
The digital inputs and outputs (3) have no function.

Light-emitting diodes

The router has several light-emitting diodes (LED), which provide information on the operating state of the router via their light signals and colors.

The following light signals are possible: solid color, slow flashing, rapid flashing, very slow flashing.

The following light colors are possible: green, blue, red.



9007199546180363: LEDs on the router

No.	Name	Status	Meaning
1	POWER	LED is off	No supply voltage
		LED lights up green	Supply voltage is present
2	STATUS	LED lights up green	Router is running
		LED flashes blue slowly or rapidly	Router is starting up
		LED flashes red very rapidly	System error
3	UPLINK	LED is off	No internet connection set up
		LED lights up green	Main internet connection is running
		LED lights up blue	Reserve internet connection is running
		LED lights up red	Internet connection is not possible or is currently being established
4	VPN/SB	LED is off	VPN connection is not set up or is not activated or is currently being established
		LED lights up green	VPN connection is running

No.	Name	Status	Meaning
		LED lights up red	VPN connection error
5	WiFi	(not used)	
6	CELL	(not used)	
7	CUSTOM	(not used)	

3.3 Scope of delivery

The parts set 12511700 (Remote Engine Management system for a single engine plant) includes:

Part number	Designation	Quantity
12524313	Router (Remote Plant Gateway)	1
12511790	FAE cable	1
12511751	easYgen cable	1

The parts set 12511702 (Remote Engine Management system for a multiple engine plant) includes:

Part number	Designation	Quantity
12524313	Router (Remote Plant Gateway)	1
12511791	IAE cable	1
12511751	easYgen cable	1

A mobile antenna and a valid SIM card are required for internet access via the mobile network. These parts are not included in the scope of delivery of the Remote Engine Management System. The SIM card must have the following properties:

- The SIM card must be in micro SIM format (12 mm x 15 mm).
- The SIM card must not be protected with a PIN.

If the router is subsequently installed in a plant, further components, which have to be ordered separately, are required depending on the plant:

- ModemKon (only for single engine plant)
- Connecting cable from FAE to ModemKon (single engine plant only)
- Miniature circuit breaker type B with 2 Ampere automatic fuse
- Ethernet cable

3.4 List of abbreviations

The following are some of the abbreviations that can be found on the router and in this document:

Abbreviation	Explanation
3G	Third Generation – Collective name for several mobile standards, among others UMTS and HSPA
AC	Alternating Current
AGS	Genset control cabinet
APN	Access Point Name
COM	Communication Port – General designation for a serial interface
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DI	Digital Input
DNS	Domain Name Service
DO	Digital Output
FAE	Function Selection Unit
HAS	Auxiliary cabinet
HSPA	High Speed Packet Access – Third generation mobile standard (3G)
IAE	Intelligent Selection Unit
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
JView	Computer program that enables a TEM-Evo control system to be operated and monitored from a normal computer
LAN	Local Area Network
LED	Light-emitting diode
ModemKon	Device that converts RS-232 signals into TTY signals and vice versa

Abbreviation	Explanation
PIN	Personal Identification Number
PLC	Programmable Logic Controller
RAC	Remote Access Client
REM	Remote Engine Management
RPG	Remote Plant Gateway
RVS	Rendezvous Server
SELV	Safety Extra Low Voltage
SIM	Subscriber Identification Module
SMA	SubMiniature version A - plug-in connector for coaxial cable
TEM Evo	Total Electronic Management Evolution – Name of the control system of the gensets
TEM MFR	TEM Multi Function Relay
UMTS	Universal Mobile Telecommunications Service – Third generation mobile standard (3G)
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
ZAS	Master Control Cabinet

4 Assembly

4.1 Safety notes



DANGER

Danger of death from electric shock when coming into contact with live parts

- Do not touch live parts.
- Switch off the switch cabinet's power supply and secure it against accidentally switching back on.



Risk of destruction of components

Electrostatic discharge can damage electrostatically sensitive components

- Before working on the switch cabinet, touch a grounded object.

4.2 Assembly overview

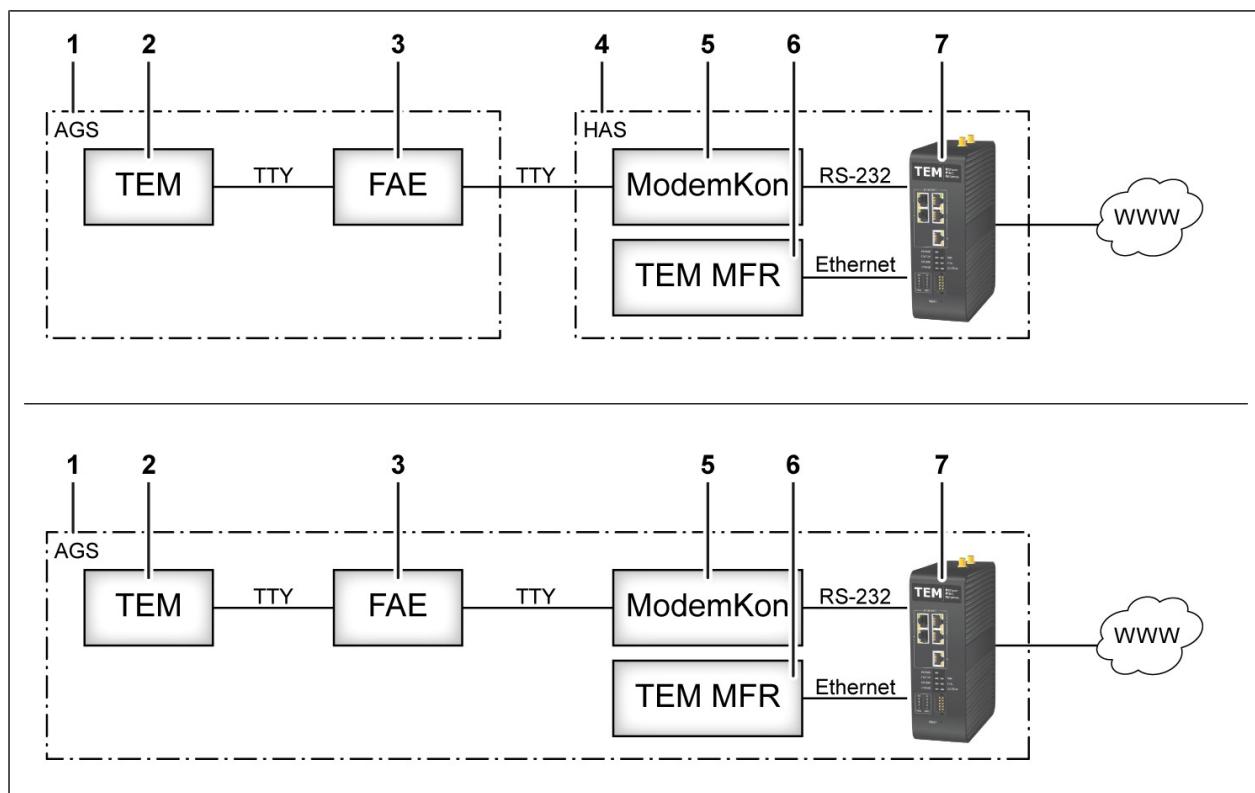
The activities described in this chapter are only necessary if the router is going to be installed in a plant at a later date.

For information on installing and connecting the router, see the circuit diagram.

Single engine plant

If a ModemKon is already installed, then it is either in the genset control cabinet or in the auxiliary cabinet. The router must be installed in the same switchgear cabinet as the ModemKon.

If there is still no ModemKon installed, the ModemKon and router are always installed in the genset control cabinet.

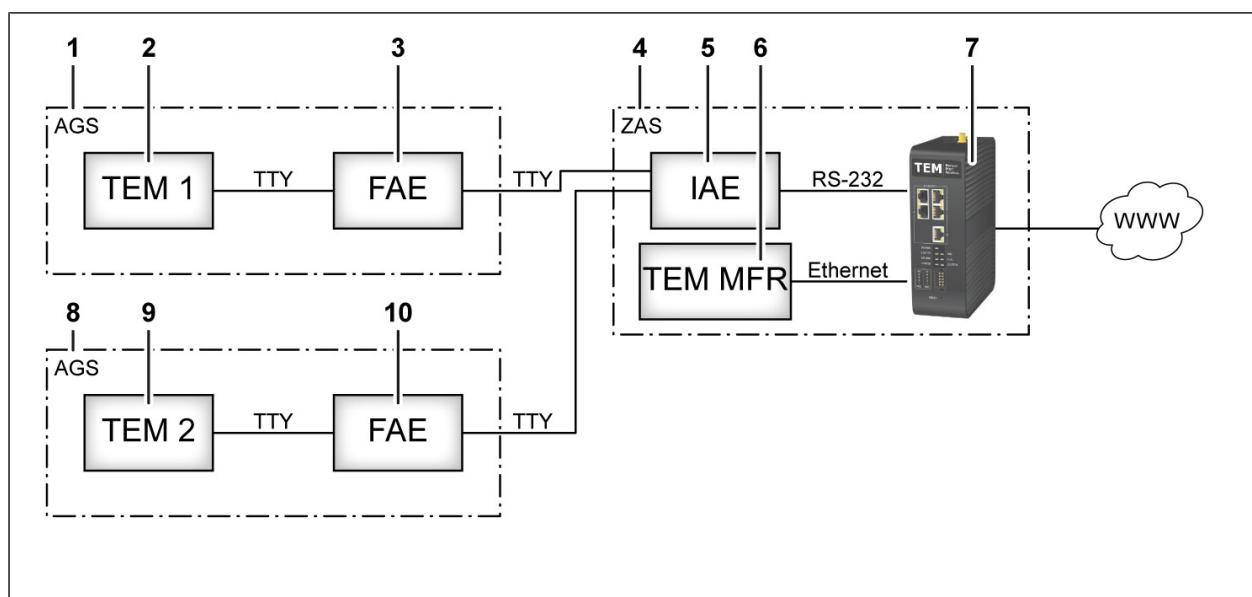


18014398799345419: Single engine plant: The router is either in the auxiliary cabinet (above) or in the genset control cabinet (below)

- 1 Genset control cabinet
- 2 TEM Evo control system
- 3 Function Selection Unit
- 4 Auxiliary cabinet
- 5 Interface converter ModemKon
- 6 TEM MFR
- 7 Router

Multiple engine plant

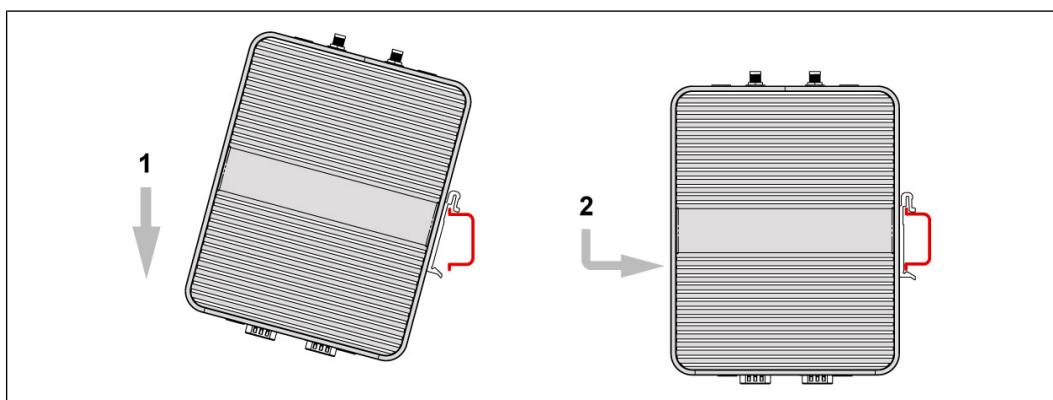
In the case of a multiple engine plant, the router is installed in the master control cabinet. If the plant does not have a master control cabinet, the router is installed as for a single engine plant.



18014398799365259: Multiple engine plant: The router is in the master control cabinet

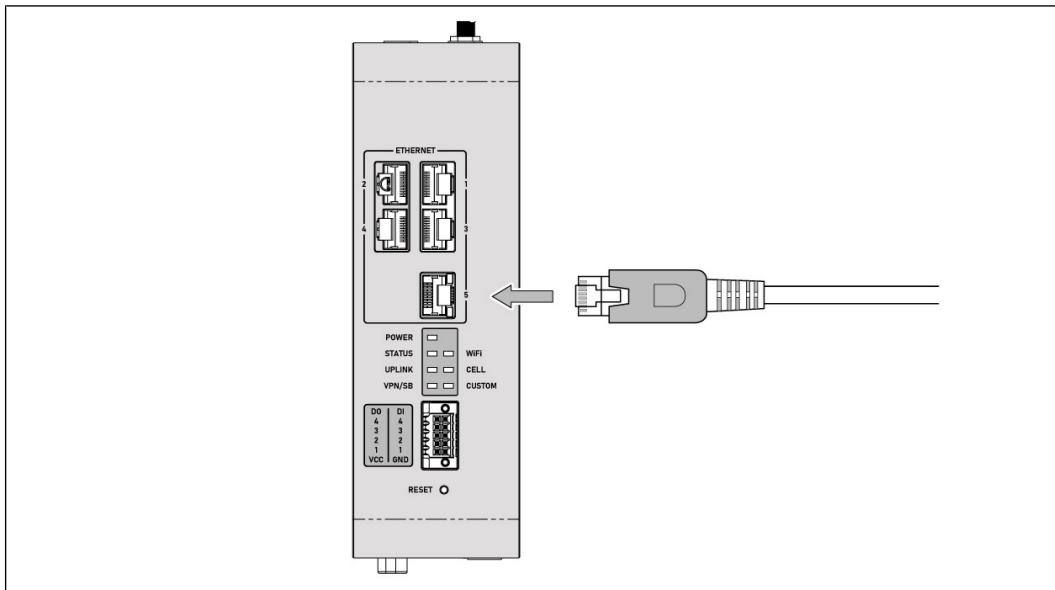
- 1 Genset control cabinet of genset 1
- 2 TEM Evo control system of genset 1
- 3 Function Selection Unit of genset 1
- 4 Master Control Cabinet
- 5 Intelligent Selection Unit
- 6 TEM MFR
- 7 Router
- 8 Genset control cabinet of genset 2
- 9 TEM Evo control system of genset 2
- 10 Function Selection Unit of genset 2

4.3 Installing the router in the switch cabinet



18014398799375115

1. Hook the router into the mounting rail from the front and press down.
 - The antenna connector must point upward.



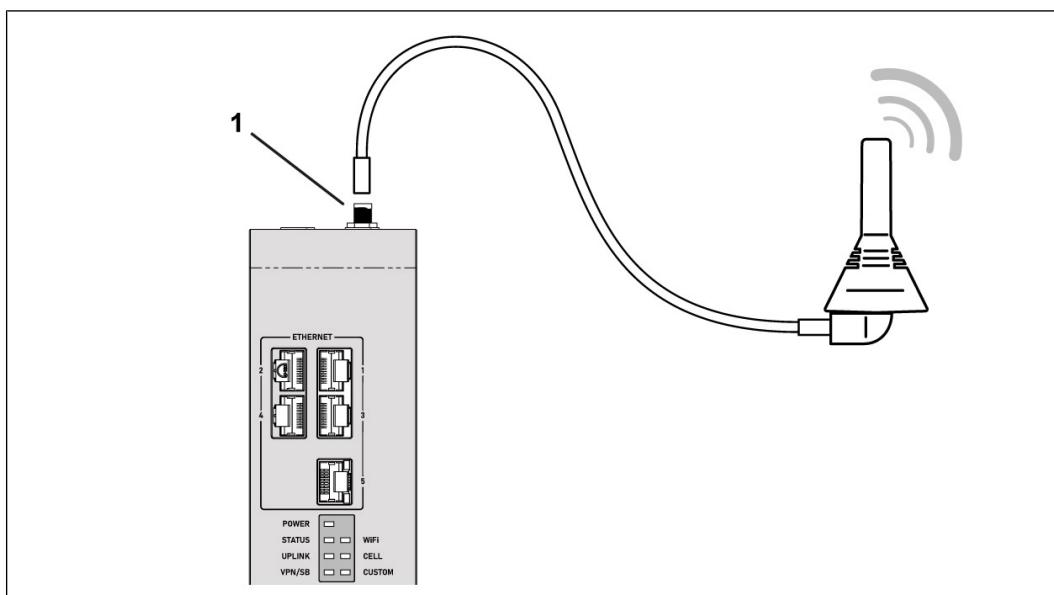
18014398799474059

2. Connect the router to the internet.
 - Insert the ethernet cable (1) into the ETHERNET5 connection (2).
 - The connector of the cable (1) must audibly snap into place.

4.4 Installing the mobile antenna (optional)

For the router to establish an internet connection via the mobile network, the antenna must be connected to the router.

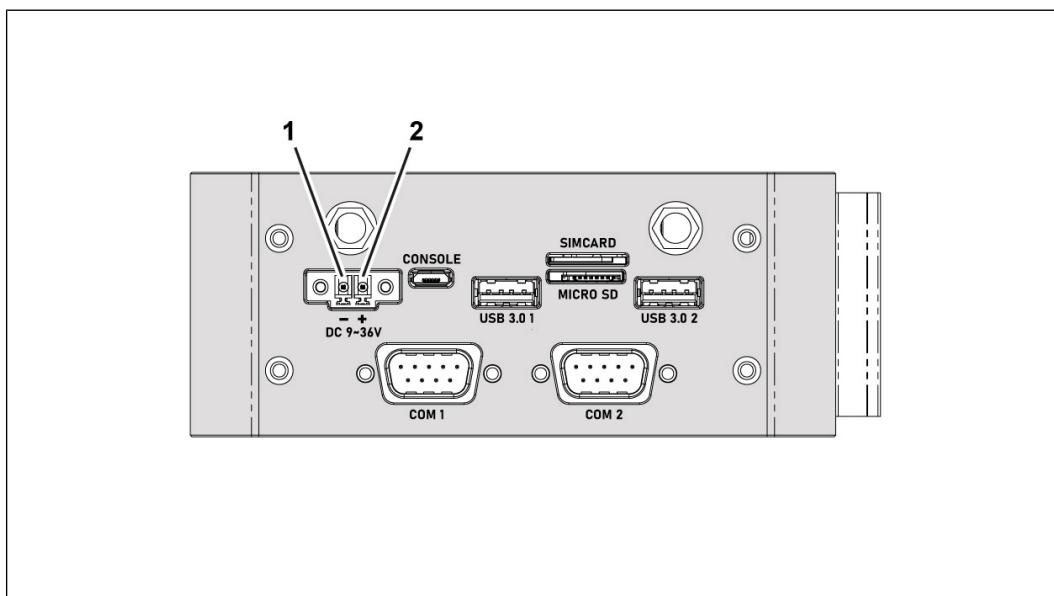
1. Install an antenna on a vibration-free area outside the switch cabinet, for example on the switch cabinet roof.
 - If necessary, use an antenna holder (available from the antenna manufacturer).
 - The antenna cable should be as short as possible. The longer the antenna cable, the more it dampens the received signal. Above a cable length of 5 m to 10 m, an antenna amplifier is usually required.
 - The antenna cable must have an SMA connector (male). Cables with RPSMA connectors are not compatible.
2. Guide the antenna cable into the switchgear cabinet.



18014398799384715

3. Screw the antenna cable onto the antenna connector CELL MAIN (1) and tighten hand-tight.
 - The antenna connector CELL MAIN is for the main antenna. The antenna connector CELL AUX is intended for an optional second antenna.

4.5 Connecting the power supply



18014398799402507

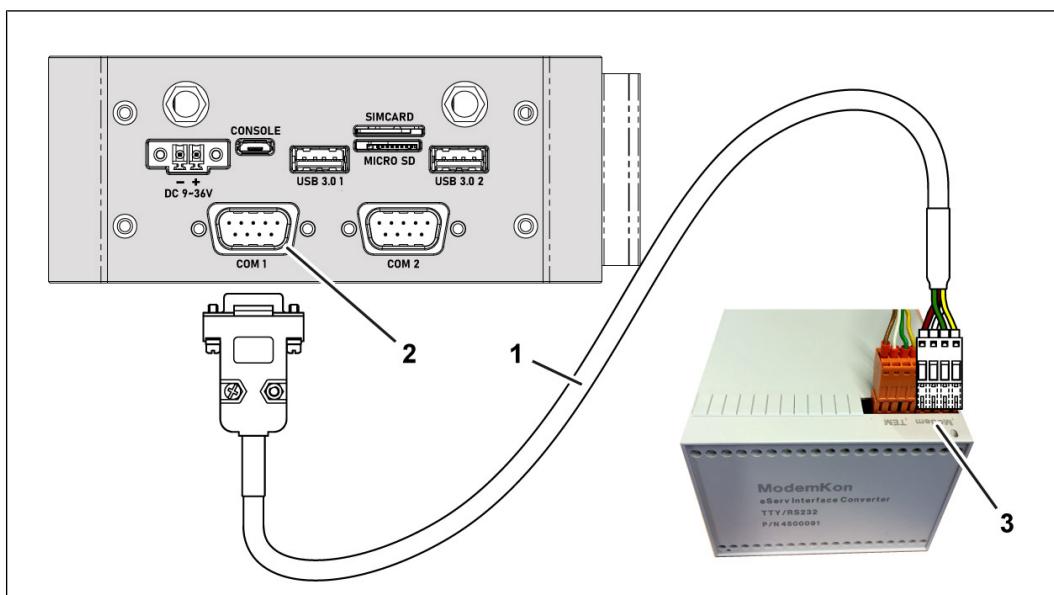
1. Connect the DC voltage supply (DC 24 V) to the terminals (1, 2).
 - Observe the polarity: Connect the negative pole to terminal (1), connect the positive pole to terminal (2).
2. Install a miniature circuit breaker in the power supply line to the router. The miniature circuit breaker must have the following properties:
 - Rated current: 2 A
 - Trigger characteristics: B
 - Number of poles: 1
 - Rated voltage: AC 230 V
 - Operating voltage: DC 24 V

4.6 Connecting the router to the interface converter ModemKon (single engine plant)

NOTE

If a ModemKon has not yet been installed in the genset control cabinet AGS or in the auxiliary cabinet HAS:

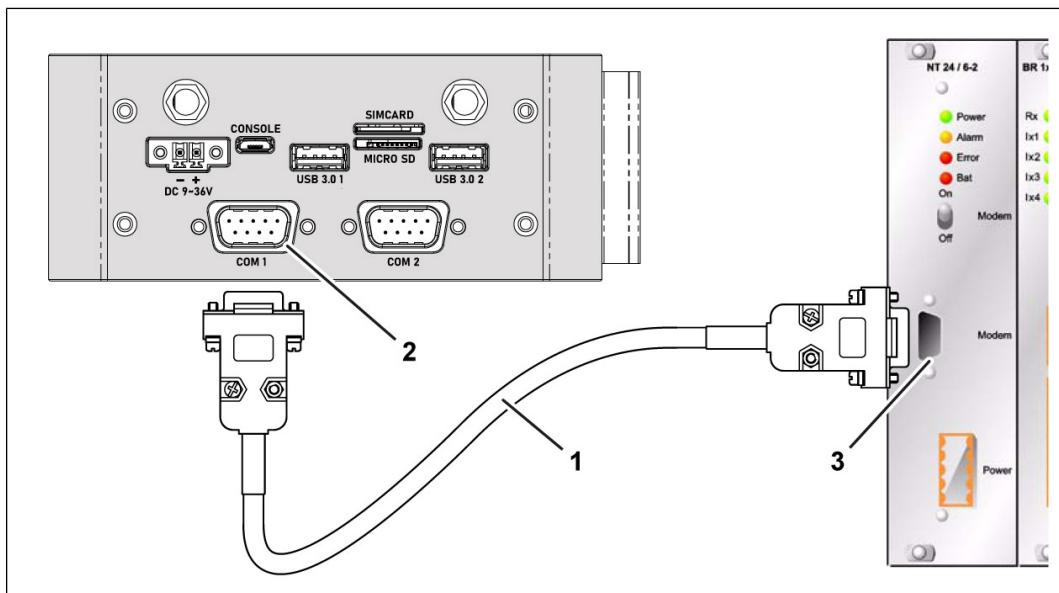
- Install the ModemKon next to the router in the switchgear cabinet.
 - Using the corresponding cable, connect the **TEM** connection of the ModemKon to the **modem** connection of the FAE.
-



18014398799407499

1. Insert the connector of the FAE cable (1) into the COM1 connection (2) of the router and tighten the screws hand-tight.
 - Do not use the COM2 connection.
2. Insert the connector of the FAE cable (1) into the modem connection (3) of the ModemKon.

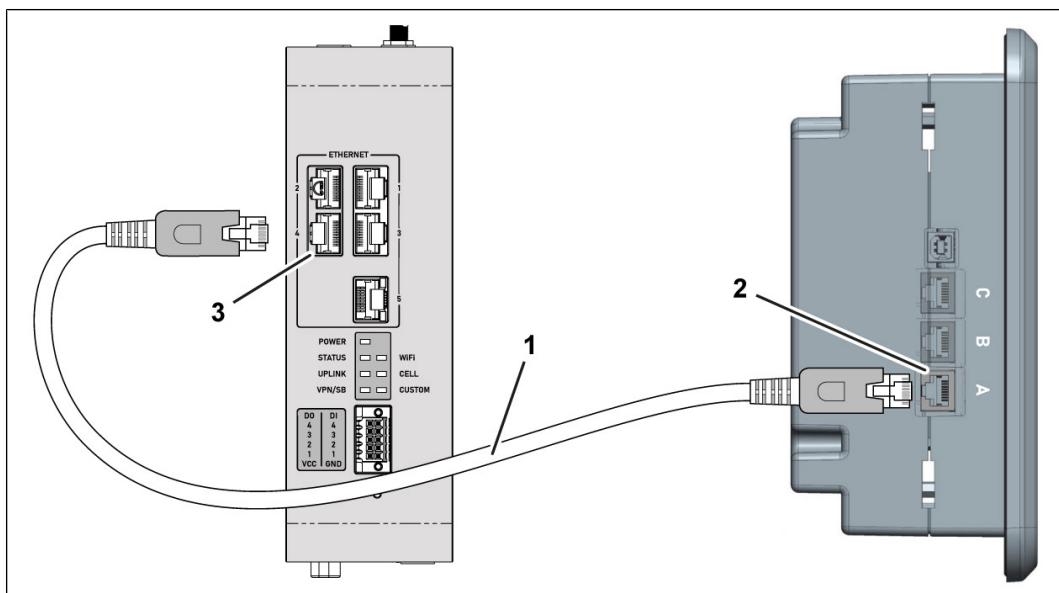
4.7 Connecting the router to the Intelligent Selection Unit IAE (multiple engine plant)



18014398799412491

1. Insert the connector of the IAE cable (1) into the COM1 connection (2) of the router and tighten the screws hand-tight.
 - Do not use the COM2 connection.
2. Insert the connector of the IAE cable (1) into the modem connection (3) of the IAE and tighten the screws hand-tight.

4.8 Connecting router to the TEM MFR



18014398799417483

1. Insert the connector of the ethernet cable (1) into the LAN A connection (2) on the TEM MFR.
2. Insert connector of the ethernet cable (1) into the ETHERNET4 connection (3) on the router.
 - The ETHERNET4 connection is preconfigured at delivery for the connection of the TEM MFR. Connect the TEM MFR to ETHERNET4 only and not to one of the other ethernet connections.

NOTE

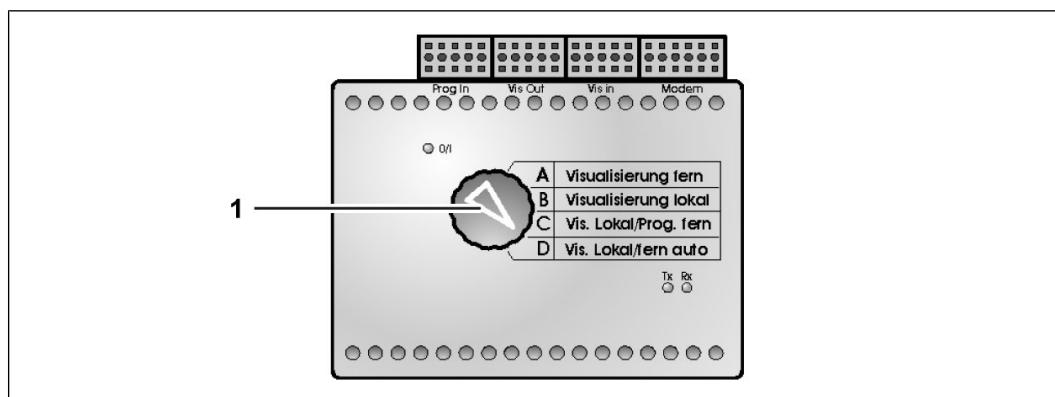
The LAN interfaces on the TEM MFR are configured as follows:

- LAN A: IP address 10.0.0.82/28, subnet mask 255.255.255.240, default gateway 10.0.0.81
- LAN C: IP address 192.168.0.1/24
- LAN C: IP address 172.22.20.21/24

4.9

Checking the settings on the Function Selection Unit [FAE]

There is a rotary switch on the Function Selection Unit [FAE] that can set four different operation modes. Whether it is possible to remotely access the control system TEM Evo, which is connected to the FAE, depends on the operation mode of the FAE.



9007199544698507

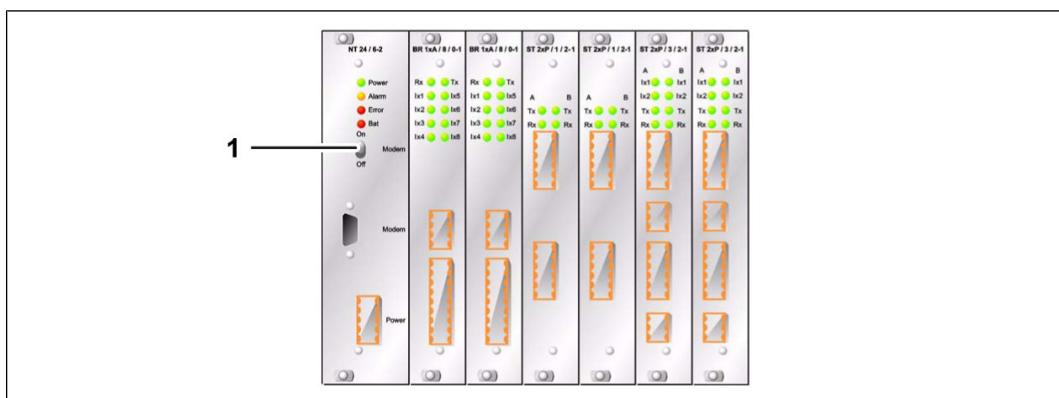
1. Set the rotary switch (1) to operation mode **D** to enable remote access to the control system.

4.10

Checking the settings on the Intelligent Selection Unit (IAE) (multiple engine plant)

Only for a multiple engine plant with Intelligent Selection Unit (IAE):

On the IAE-NT module of the Intelligent Selection Unit (IAE), there is a switch that can set whether it is possible to remotely access the TEM Evo control systems that are connected to the IAE.



9007199544703243

1. Set switch (1) to the On position to enable remote access to the control systems.

5 Commissioning

5.1 Registering the router and users

Remote access to a plant is only possible once the router and every user that will access the plant via the router are registered with Caterpillar Energy Solutions.

Normally, the commissioner or the responsible service partner will perform the registration.

There are two ways to register a router and a user:

- TCG Portal
- Email

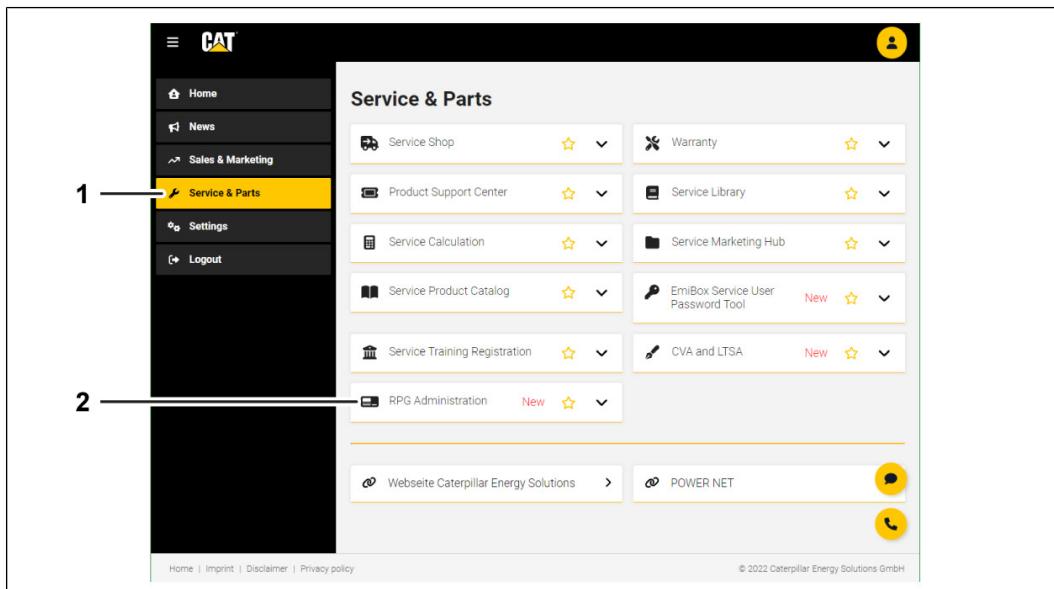
Registration via TCG Portal is available exclusively to service partners with CWS ID.

Registering router and users via TCG Portal

We recommend registering the router and users via the TCG Portal because this method is faster and more secure.

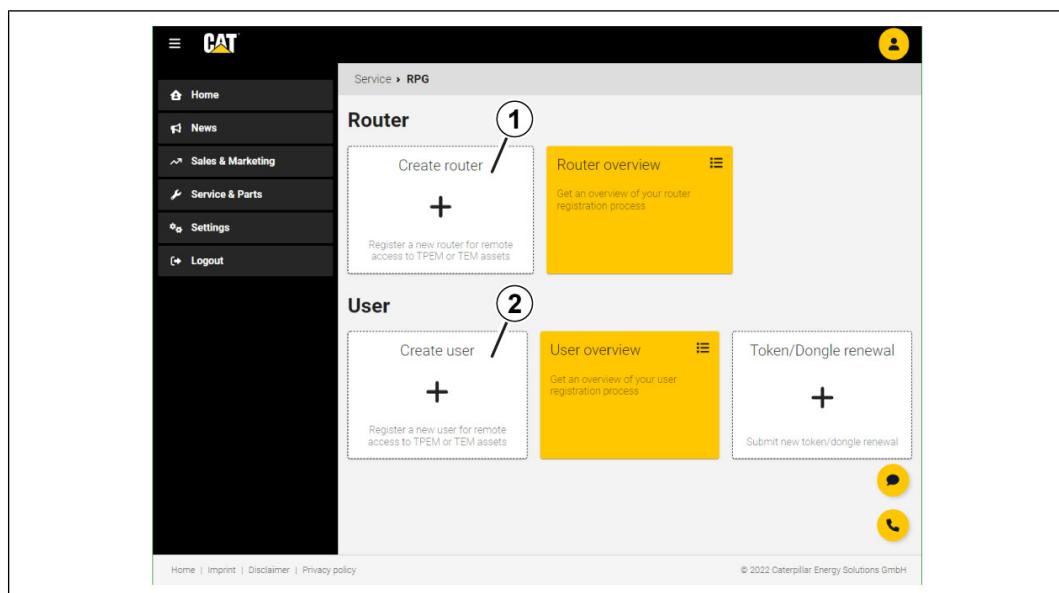
To register a router or a user via the TCG Portal, your CWS ID must be approved for the "RPG Administration" application.

1. Visit the [TCG Portal](#) and log on with your access credentials.



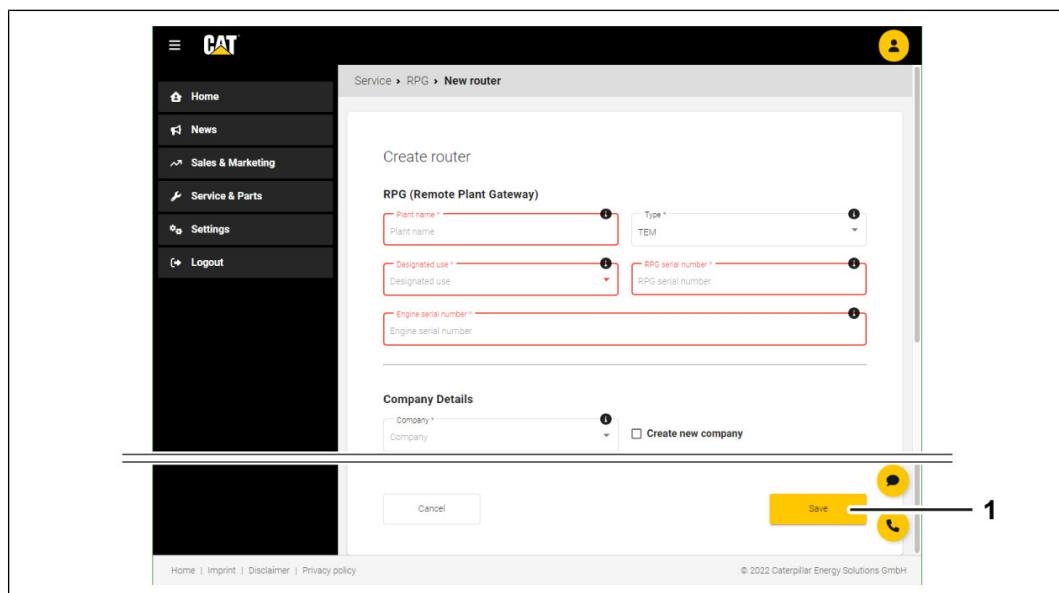
870819723

2. Select the "Service & Parts" menu (1) and then click there on the link "RPG Administration" (2).
 - If you do not see the "RPG Administration" link, your CWS ID has not yet been approved for this application. To get approved, send your CWS ID to rpg@mwm.net.



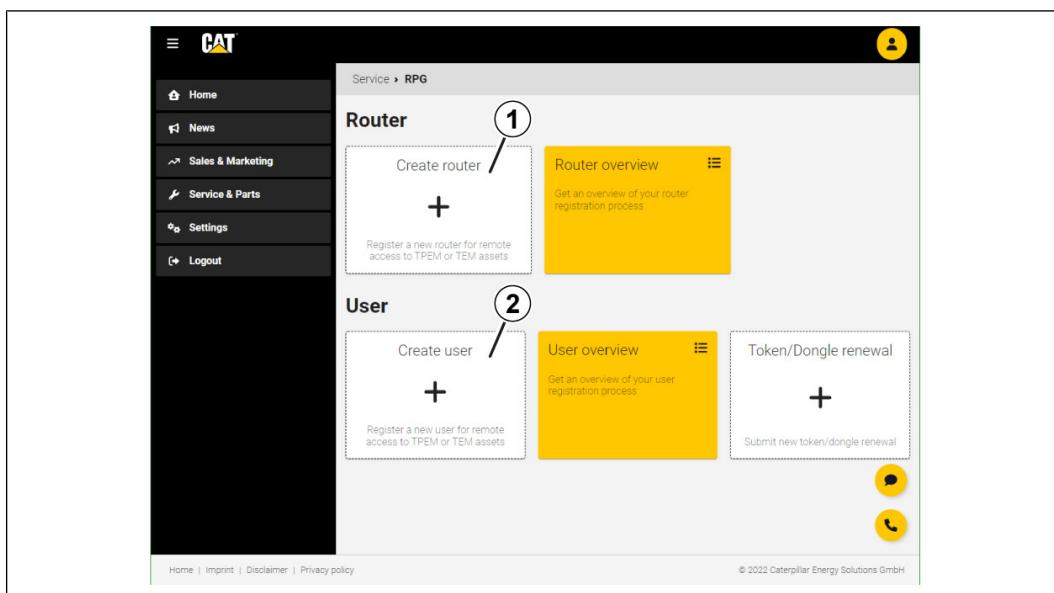
872804363

- Click on "Create router" (1) to register a new router.



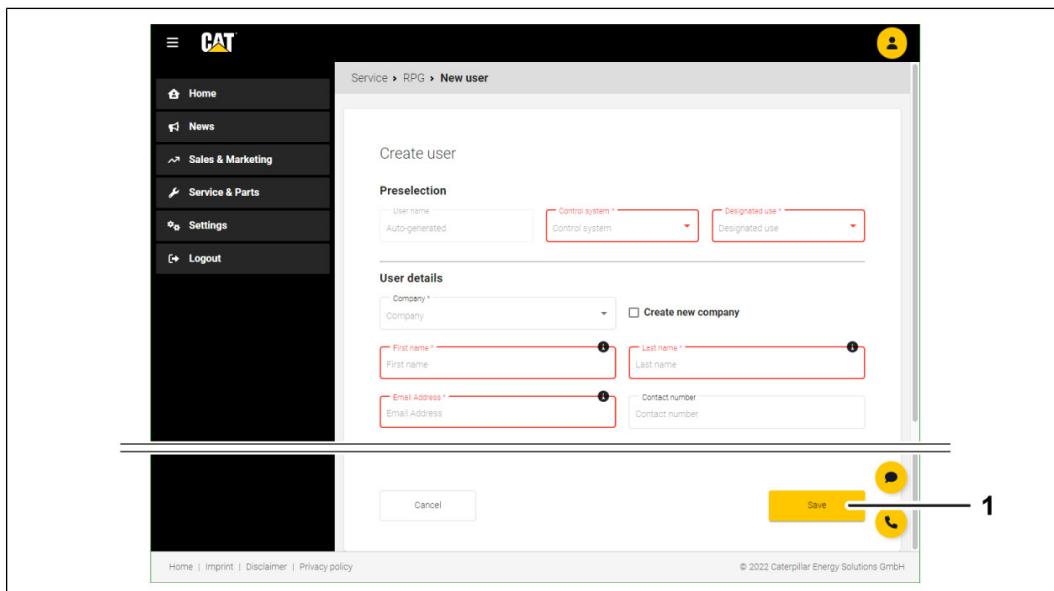
872812427

- Fill out all the required form fields and then click "Save" (1).



872804363

- To register a user, click on "Create user" (2).



878447499

- Fill out all the required form fields and then click "Save" (1).

We will automatically check your request and send the end customer an email with an activation link. After the activation link is clicked, we will immediately approve the router or the user account. The end customer will also receive an email with more information for remote access. Notify the end customer of the emails.

Once we have approved a user account, the user will receive the following information from us by email:

- The link for downloading the Remote Access Client
- The login credentials (username, password)

Remote access is only possible once we have sent the login credentials.

Registering router and user via email

There is a form for registering the router and user. Since it can take several days to process the request, we recommend sending the registration form to us in good time before commissioning the router.

1. Fill out and sign the registration form.
2. Send registration form via email to rpg@mwm.net.
 - In the subject line write: **REM - router activation**

You will receive an automatic confirmation of receipt from us by email.

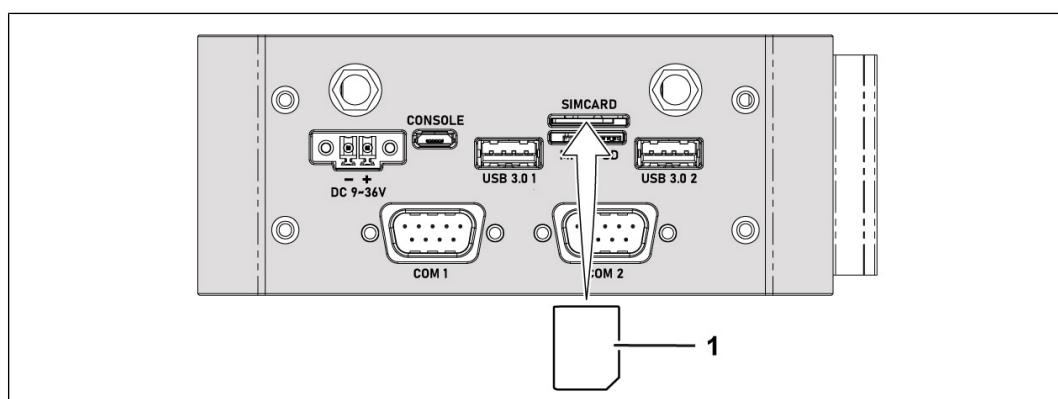
Once we have processed your inquiry, you will receive the following information from us by email:

- The link for downloading the Remote Access Client
- The login credentials (username, password)

Remote access is only possible once we have sent the login credentials.

5.2 Inserting the SIM card (optional)

For the router to establish an internet connection via the mobile network, a valid SIM card must be inserted.



18014398799520523

1. Push the SIM card (1) into the SIM card slot.
 - The SIM card must be in micro SIM format (12 mm x 15 mm).

5.3 Checking the network settings

Rendezvous Server (RVS)

In order for remote access to be possible, the router must communicate with the Rendezvous Server.

Domain name	IP address	Port	Protocol
rem-portal.caterpillar-energy-solutions.de	153.95.148.211	1194	UDP
rem-portal.caterpillar-energy-solutions.de	153.95.148.211	443	TCP
rvs-01.caterpillar-energy-solutions.de		1194	UDP
rvs-01.caterpillar-energy-solutions.de		443	TCP

If the router's data traffic runs via a proxy server, the router can only use the TCP protocol and port 443. The proxy server must allow data traffic to the specified addresses; the same applies to a firewall.

NOTE

For authentication via the Rendezvous Server some older routers contain a certificate which is only valid for the domain **endian.mwm.net**. This domain has been switched off since July 2023. So that the effected routers still work, an update must be run on the router. For further information see section [Updating the configuration \[▶ 50\]](#).

Security updates

The router regularly contacts the following servers to get any security updates:

Domain name	IP address	Port	Protocol
repository.endian.com	176.34.133.58	80	TCP
service.endian.com	54.229.13.53	443	TCP
register.endian.com			
sms.endian.com			
bouncer.endian.com	54.72.165.247	22, 12000 – 15000	TCP
liveclient.endian.com	54.72.218.11	8991	TCP
network.endian.com	176.34.145.208	80, 443	TCP

If the data traffic of the router runs via a proxy server, the proxy server must allow data traffic to the specified addresses; the same applies for a firewall.

The router must be able to contact the specified addresses on a regular basis. If the router receives security updates too late or not at all, there may be security risks.

Name resolution (DNS)

If there is no internal DNS server in the network, the router requires access to an external DNS server. As an example, the following table contains the addresses of Google DNS servers.

Name	IP address	Port	Protocol
Google Public DNS	8.8.8.8, 8.8.4.4	53, 853	TCP, UDP

Data filtering

If the data traffic of the router is filtered on OSI layer 2, the MAC address of the router must be allowed.

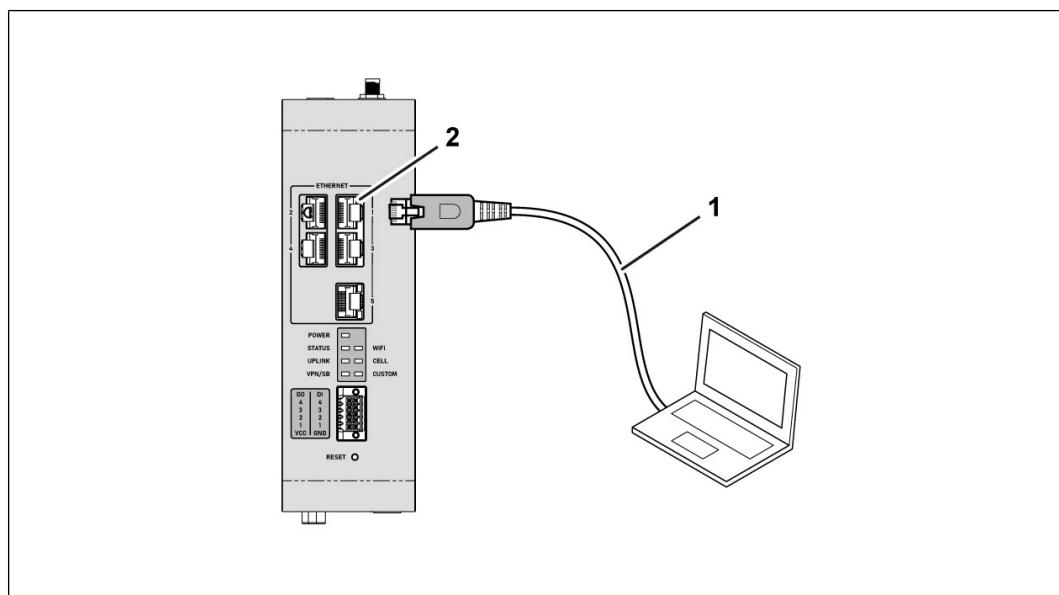
If the data traffic of the router is filtered on OSI layer 7, https and openvpn must be approved.

Protocols

The router uses the IPv4 protocol. Data traffic via the IPv6 protocol is not possible.

5.4 Connecting a computer to the router

To configure the router, it is necessary to temporarily connect a computer (e.g. a laptop) to the router.



18014398799525515

1. Connect the computer to the router's ETHERNET1 connection (2) using an ethernet cable (1).
 - Alternatively, ETHERNET2 and ETHERNET4 are also possible.

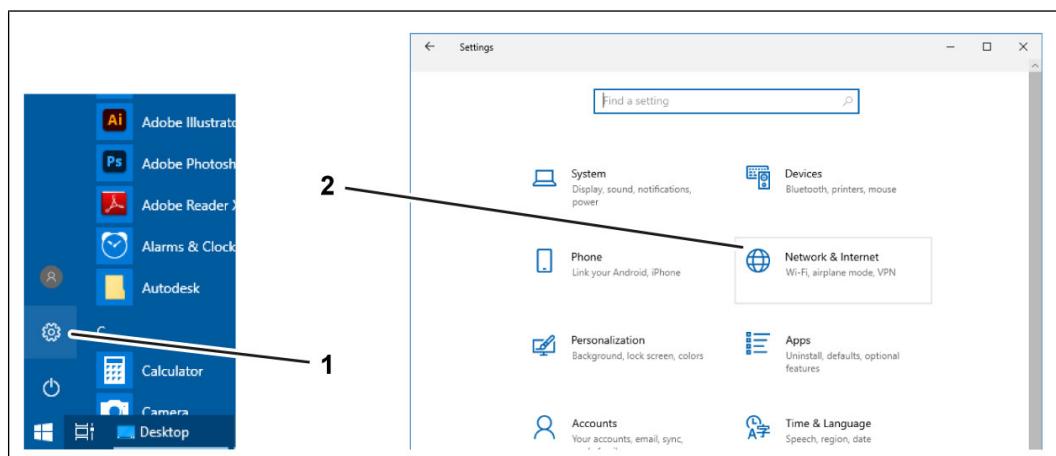
The router's LAN interface has the default IP address **10.0.0.53**. In order for the computer to be able to communicate with the router, the computer's IP address must be in the same address range as the router. This means that the IP address of the computer must start with **10.0.0**.

If necessary, change the computer's IP address as follows:

NOTE

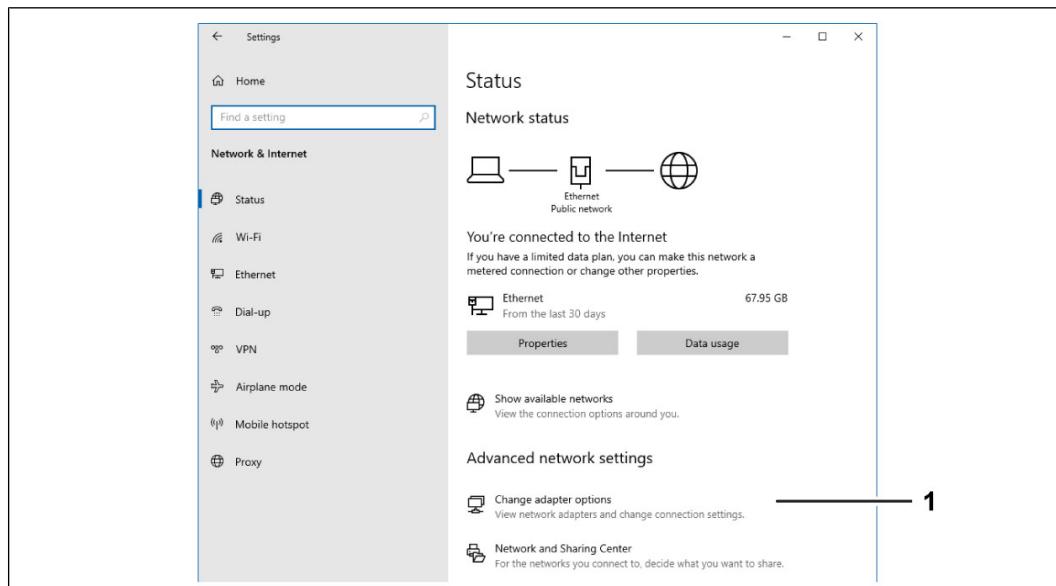
The following description applies to the operating system Windows 10.

On the Microsoft internet site, there is a description that also applies for Windows 11, Windows 8.1 and Windows 7. It is available in multiple languages: <https://support.microsoft.com/en-us/help/15089/windows-change-tcp-ip-settings>



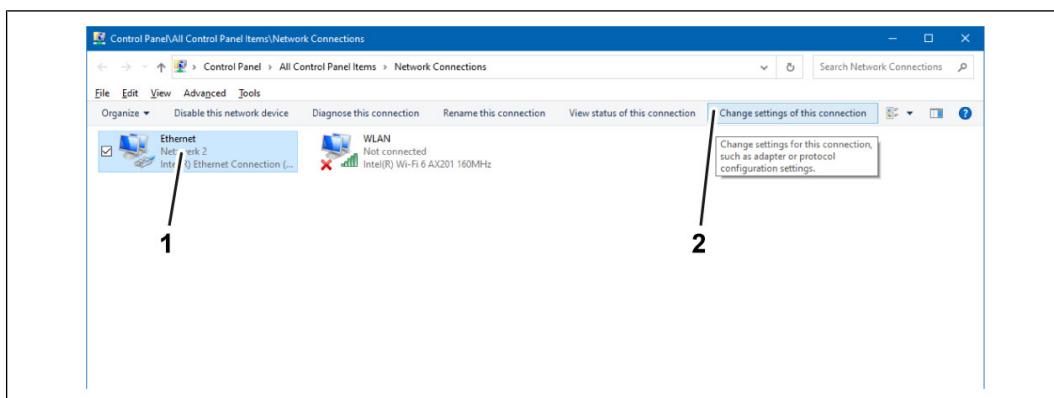
18014398799530507

1. Open the Windows settings (**Start > Settings** (1)), then go to **Network & Internet** (2).



18014398799535499

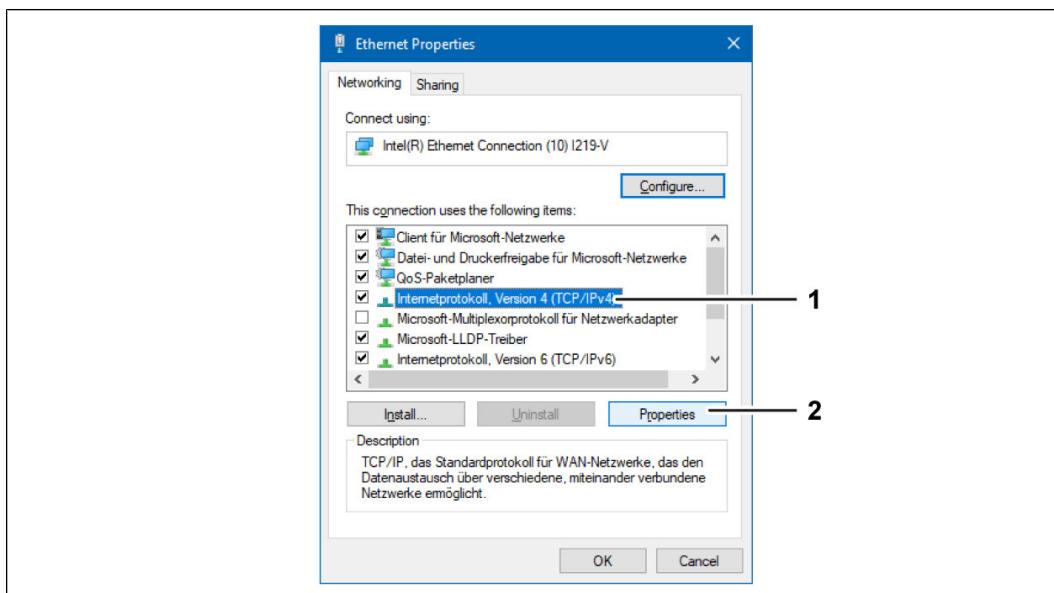
2. Click on **Change adapter options** (1).



18014398799540491

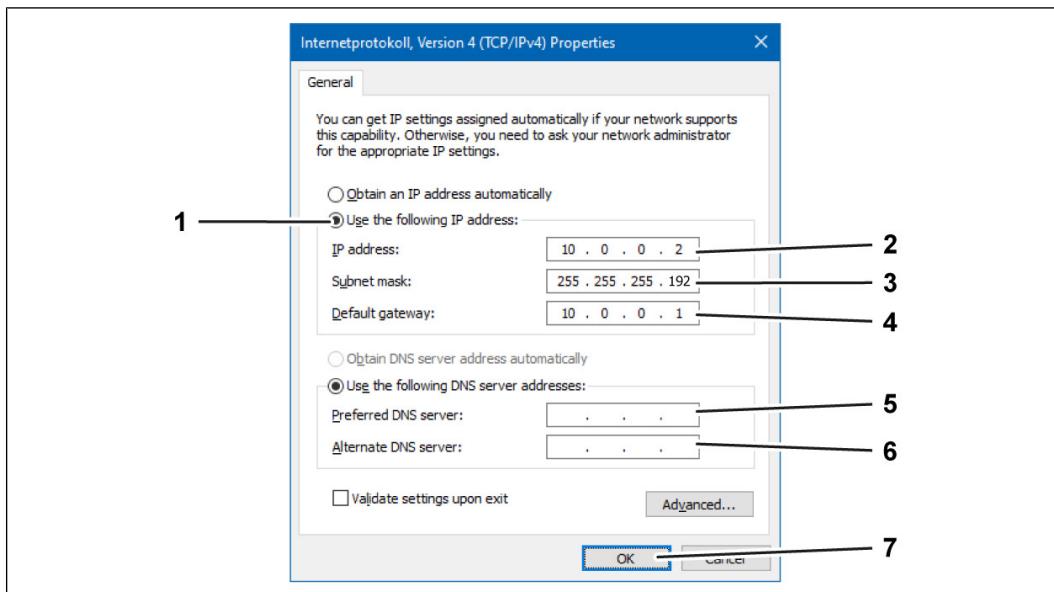
3. Select the Ethernet interface to be changed (1), and then click on **Change settings of this connection** (2).

 - Administrator rights are typically required to change the settings.
 - If the computer has multiple Ethernet interfaces, make sure to select the correct interface here.



18014398799558283

4. Select the line for **Internet Protocol, Version 4 (TCP/IPv4)** (1).
5. Click on **Properties** (2).



27021598054304267

6. Select the **Use following IP address** (1) option field.
7. In the **IP address** field (2), enter the IP address that the computer should use, e.g. **10.0.0.2**.
 - The first three figures of the IP address must be 10.0.0. The fourth figure of the IP address must not be 53, since the router already has this IP address.
8. In the **Subnet mask** field (3), enter the subnet mask **255.255.255.192**.
9. In the **Default gateway** field (4), enter the IP address **10.0.0.1**.
 - The fields **Preferred DNS server** (5) and **Alternate DNS server** (6) can remain empty, since no DNS server is required for communication between the computer and the router.
10. Click on **OK** (7).

5.5 Installing the configuration program

Before the router can commence operation, you need to configure it. This means you have to adjust router-internal settings using a program, the **RPG Configurator**.

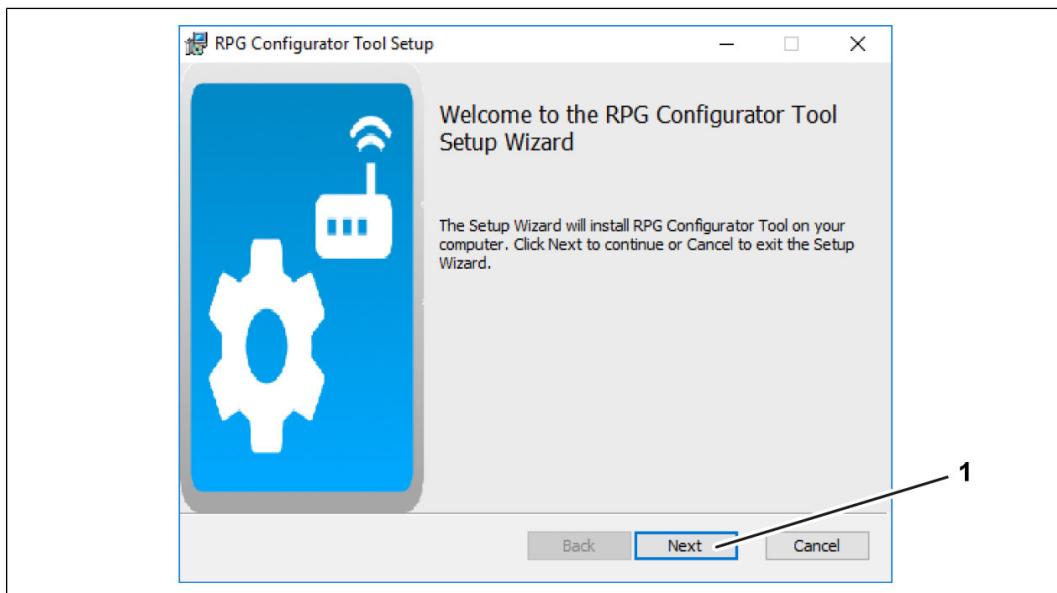
You can also find the current version of the RPG Configurator in the [Service Library](#).

The computer on which you are installing the configuration program must satisfy the following requirements:

- Operating system Microsoft Windows 7 or newer
Microsoft and Windows are registered trademarks of Microsoft Corporation, USA.
- At least 40 megabytes of free hard disk space

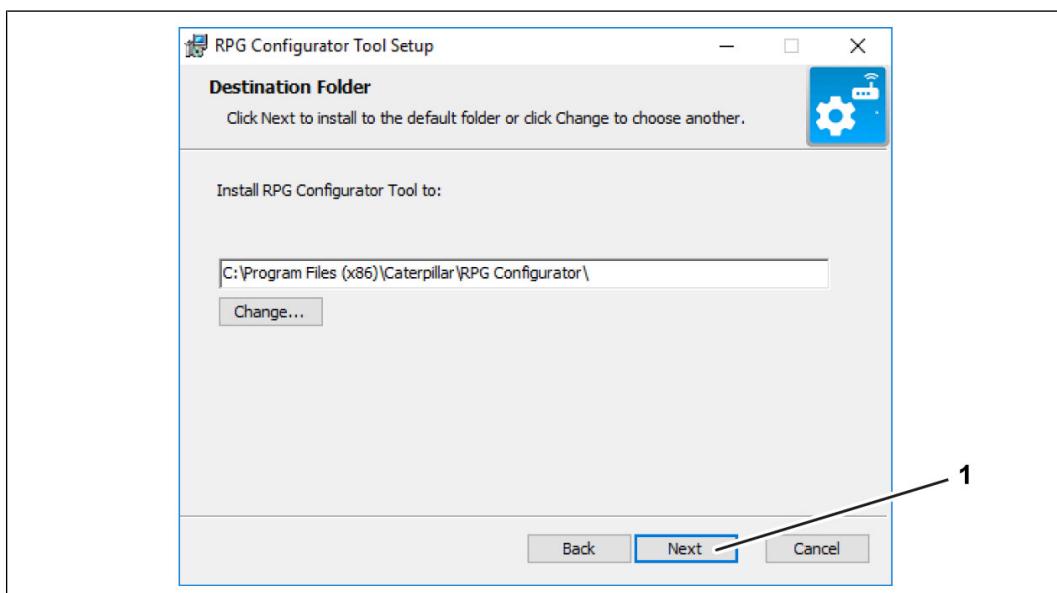
To install the configuration program, proceed as follows:

1. Start the installation program **RPG_Configurator_vX.X.X.X.msi**. Administrator rights are required to install the configuration program.



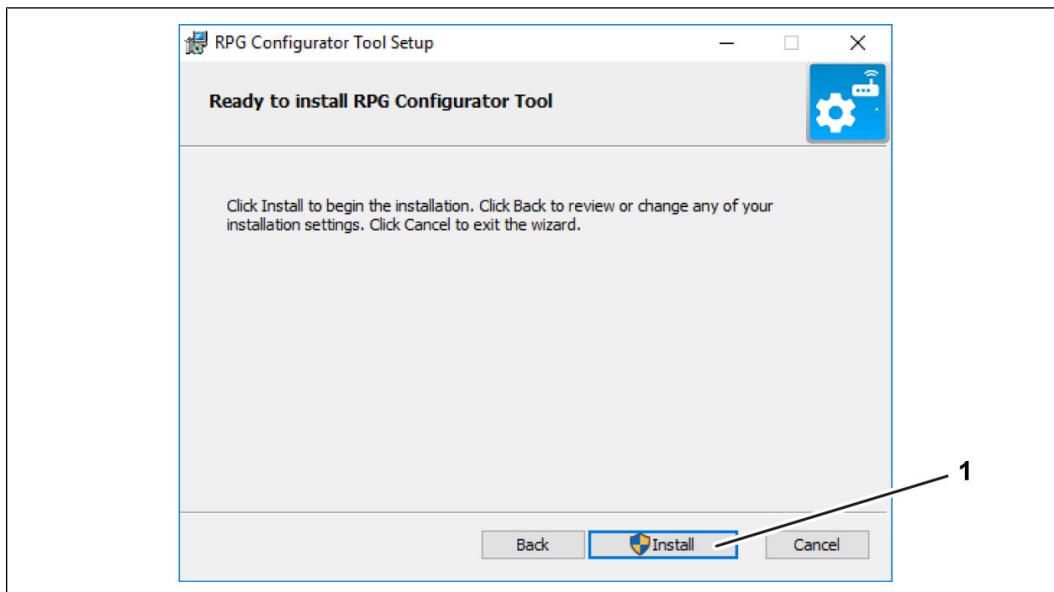
18014398799581067

2. Click on **Next** (1).



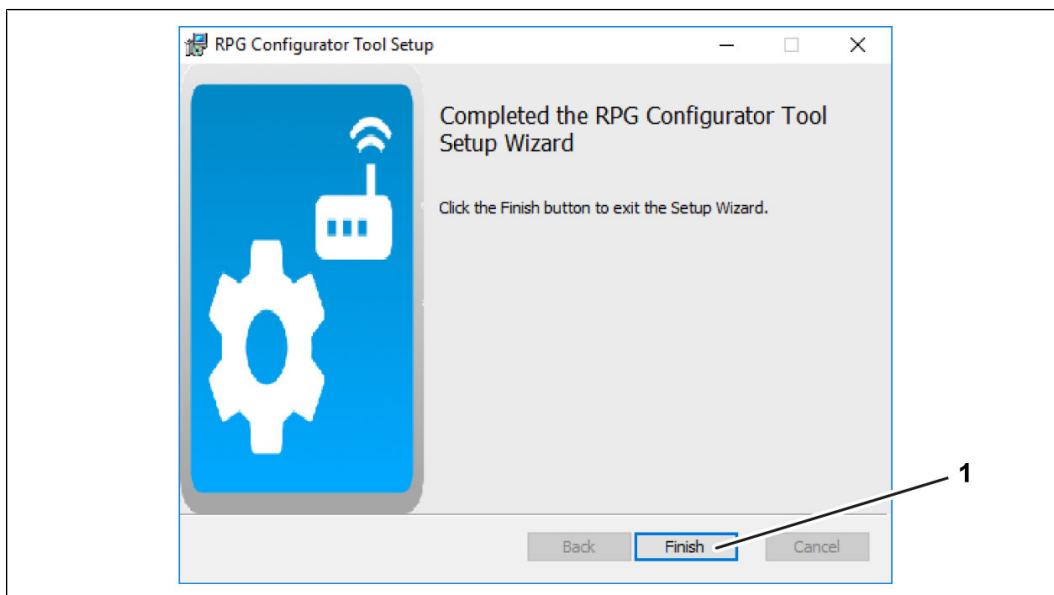
18014398799585803

3. Click on **Next** (1).



18014398799590539

4. Click on **Install** (1) to begin the installation process.



18014398799595275

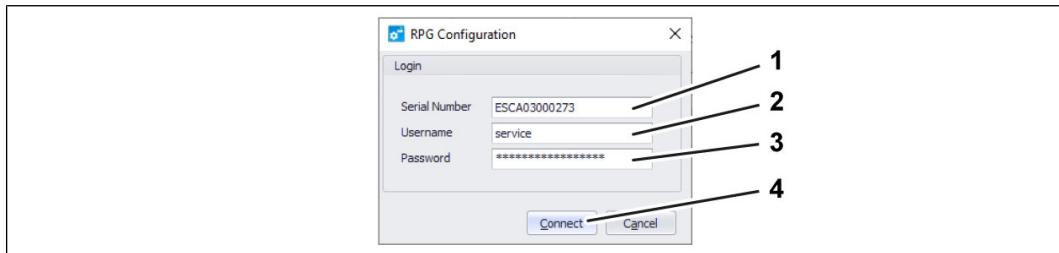
5. When the installation process is completed, click on **Finish** (1) to close the window.
 - ⇒ The configuration program is now installed.
 - ⇒ To start the configuration program, click the entry in the Start menu or double-click the shortcut icon on the desktop.

5.6 Starting the configuration program

Prerequisite: The computer must be connected to the router (► [Connecting a computer to the router \[▶ 34\]](#)).

1. Start the configuration program (RPG Configurator).

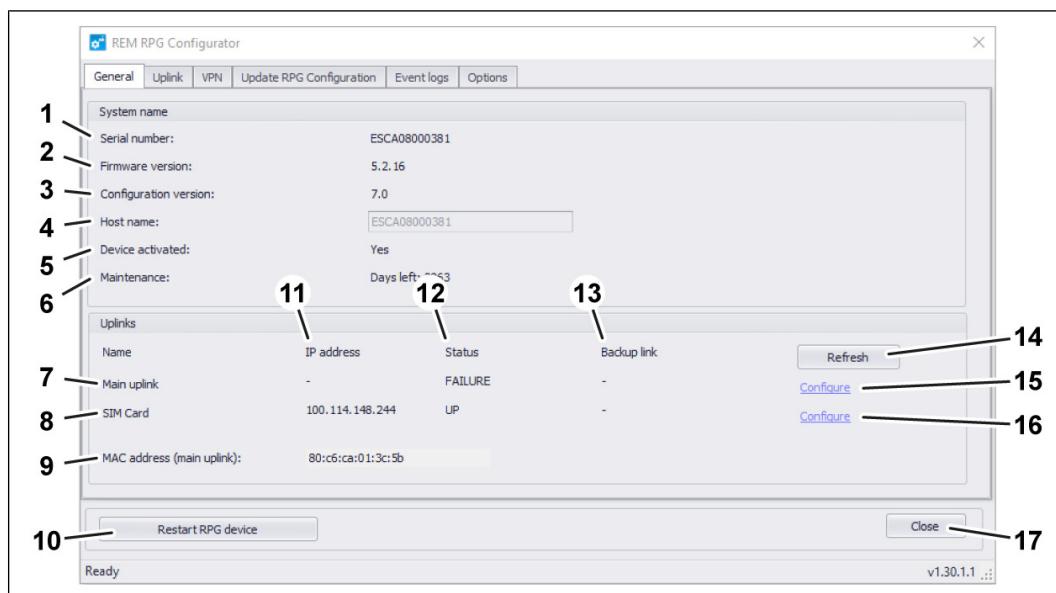
– The following window appears:



27021598055739531

2. In the **Serial Number** field (1), enter the router's serial number.
 - The serial number is on the rating plate.
3. In the **Username** field (2), enter the username **service**.
4. Enter the password **#Tem_Rpg-Service!** in the **Password** field (3).
5. Click on **Connect** (4).

⇒ The following window appears:



27021598055744267

- 1 Serial number of the router
- 2 Version number of the router's firmware
- 3 Version number of the router's configuration
- 4 Name of the router
- 5 Activation status of the router
- 6 Number of days until the end of the support period
- 7 Name of the WAN connection
- 8 Name of the mobile connection
- 9 MAC address of the WAN interface
- 10 Restart router
- 11 IP address of the active connection
- 12 Connection status
- 13 Backup connection
- 14 Refresh
- 15 Configuring the WAN connection
- 16 Configuring the mobile connection
- 17 Close configuration program

The serial number (1) of the router is also the name (4) of the router. The router is displayed in the Remote Access Client under this name. The name cannot be changed.

The router is always activated upon delivery (5).

Once the end of the support period (6) has been reached, the router no longer receives security updates. This does not reduce the functioning of the router, but there may be security risks. It is possible to extend the support period.

The router needs access to the internet to communicate with the Rendezvous Server (RVS) and get security updates. To access the internet, the router uses either the WAN interface or the mobile modem.

Normally, one of the connections (WAN, mobile) has the status (12) **UP**. UP means that the connection is active; INACTIVE means that the connection is disabled. The router never uses both connections at the same time. Under **IP Address** (11), the router displays the IP address of the active connection.

If one connection is defined as a backup connection for the other one, the name of the backup connection is listed under **Backup link** (13).

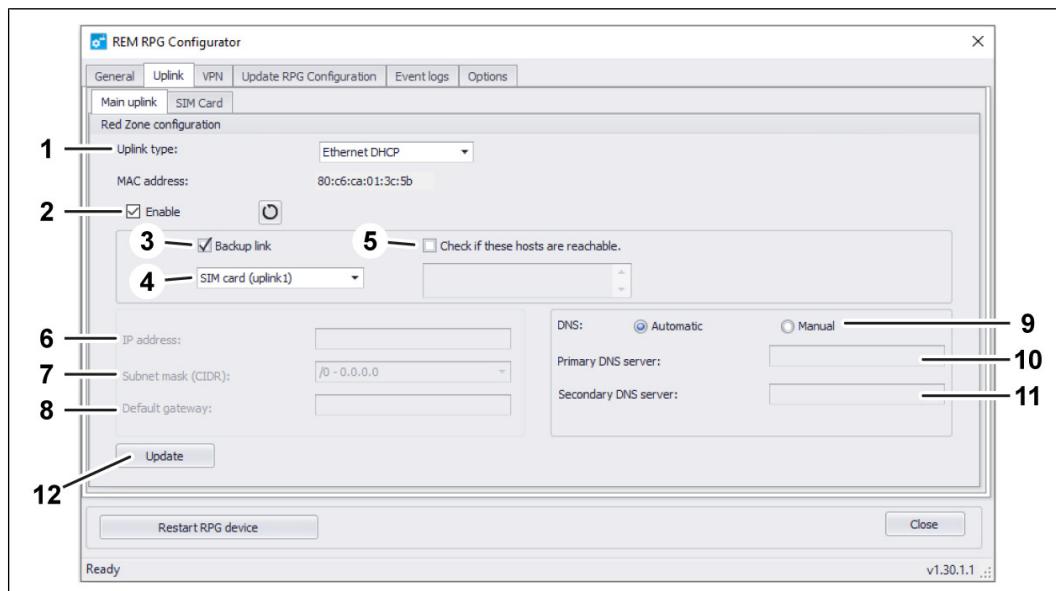
After clicking **Restart RPG device** (10) the router restarts. Restarting the router is normally only necessary if an error has occurred or if the router has not correctly adopted configuration changes. Note: It takes up to 10 minutes until the router is fully ready to function again.

5.7 Configuring the WAN connection

If there is a DHCP server in the network where the router's WAN interface is connected, the router can get its IP address automatically from the DHCP server. Alternatively, you can assign the router a static IP address.

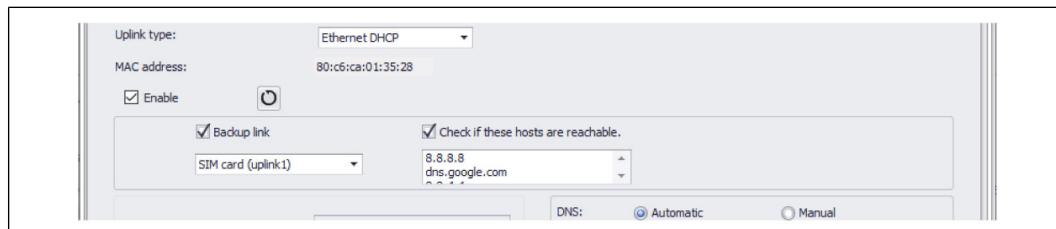
If available, you can set the mobile network connection as a backup connection for the WAN connection. This means that the router will transfer data over the mobile network if the WAN connection is interrupted. Once the WAN connection is available again, the router ceases data transfer over the mobile network.

- Click on the **Uplink** tab, then click on the **Main uplink** tab.



27021598055749003

- In the **Uplink type** list (1), select how the router will get its IP address:
 - Select **Ethernet DHCP** if the router should get its IP address from a DHCP server. This assumes that there is a DHCP server in the same network in which the router has its WAN interface.
 - Select **Ethernet static** if the router should receive a static IP address.
- Tick the **Enable** checkbox (2) to turn on the WAN interface.
 - If this checkbox is not ticked, the WAN interface will be turned off. This is necessary, for example, if the router will exclusively use the mobile network connection.
- If the mobile network connection should serve as a backup for the WAN connection, tick the **Backup link** checkbox (3) and select **SIM Card (uplink1)** from the list (4).
 - The mobile connection can only be selected if it has been configured beforehand. Only service personnel may configure the mobile connection.
- If you ticked the **Backup link** checkbox (3), also tick the checkbox for **Check if these hosts are reachable** (5). Enter one or more IP addresses in the text field below.
 - If the checkbox (5) is ticked, the router will continuously check whether it can reach the addresses in the text field while in operation. If not, the router will switch to the backup connection.



9007199971855371

- You can specify the Google DNS server as the IP address, for example: 8.8.8.8 and 8.8.4.4
 - You can also enter domain names in place of IP addresses (for example, dns.google.com). However, in the event of a fault, the advantage of IP addresses is that they require no name resolution via DNS.
6. If you set the **Uplink type** setting (1) to **Ethernet static**, specify the required information:
 - In the **IP address** field (6), enter the IP address that the router should have.
 - In the **Subnet mask (CIDR)** field (7), enter the subnet mask.
 - In the **Default Gateway** field (8), enter the IP address of the default gateway.
 7. If the router should use a DNS server automatically: Set the **DNS** option field (9) to **Automatic**.
 8. If the router should use a particular DNS server: Set the **DNS** option field (9) to **Manual**.
 - In the **Primary DNS server** field (10), enter the IP address of the preferred DNS server.
 - In the **Secondary DNS server** field (11), enter the IP address of the alternative DNS server.
 9. Click **Update** (12) to save the settings you have changed.

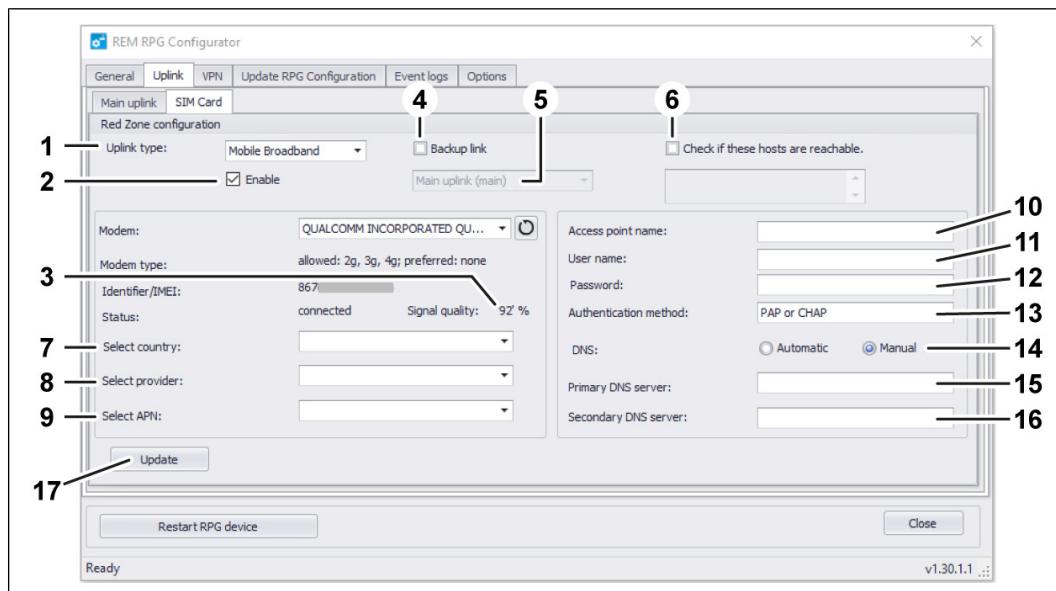
5.8 Configuring the mobile connection

If available, you can set the WAN connection as a backup connection for the mobile connection. This means that the router will transfer the data via the WAN interface if the mobile connection is interrupted. Once the mobile connection is available again, the router will cease data transfer over the WAN connection.

NOTE

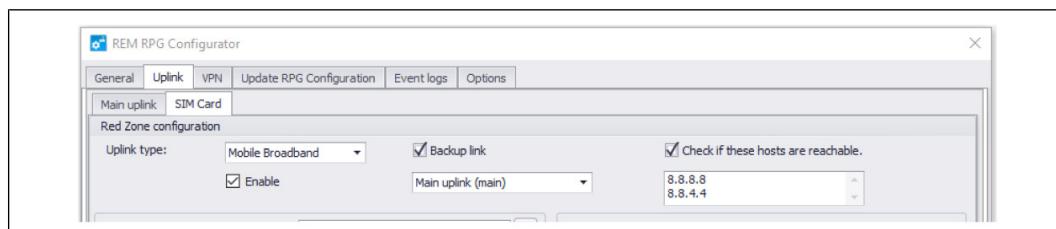
The mobile modem built into the router is functional, but is not supported by us. This means: Even if a mobile network is available on site, we cannot guarantee that the router will connect to the mobile network and transfer data.

- Click on the **Uplink** tab, then click on the **SIM Card** tab.



27021598055771275

- In the **Uplink type** list (1), select the entry **Mobile Broadband**.
- Tick the **Enable** checkbox (2).
 - If this checkbox is unticked, the mobile connection will be turned off. This is necessary, for example, if the router will exclusively use the WAN connection.
- Check the signal quality (3).
 - The number in the **Signal quality** field (3) indicates how good the mobile reception quality is. At "100%", the reception quality is the highest. If the reception quality is too low, it may help to readjust the mobile antenna.
- If the WAN connection should serve as a backup for the mobile network connection, tick the **Backup link** checkbox (4) and select **Main uplink (main)** from the list (5).
- If you ticked the **Backup link** checkbox (4), also tick the checkbox for **Check if these hosts are reachable** (6). Enter one or more IP addresses in the text field below.
 - If the checkbox (6) is ticked, the router will continuously check whether it can reach the addresses in the text field while in operation. If not, the router will switch to the backup connection.



9007199972809739

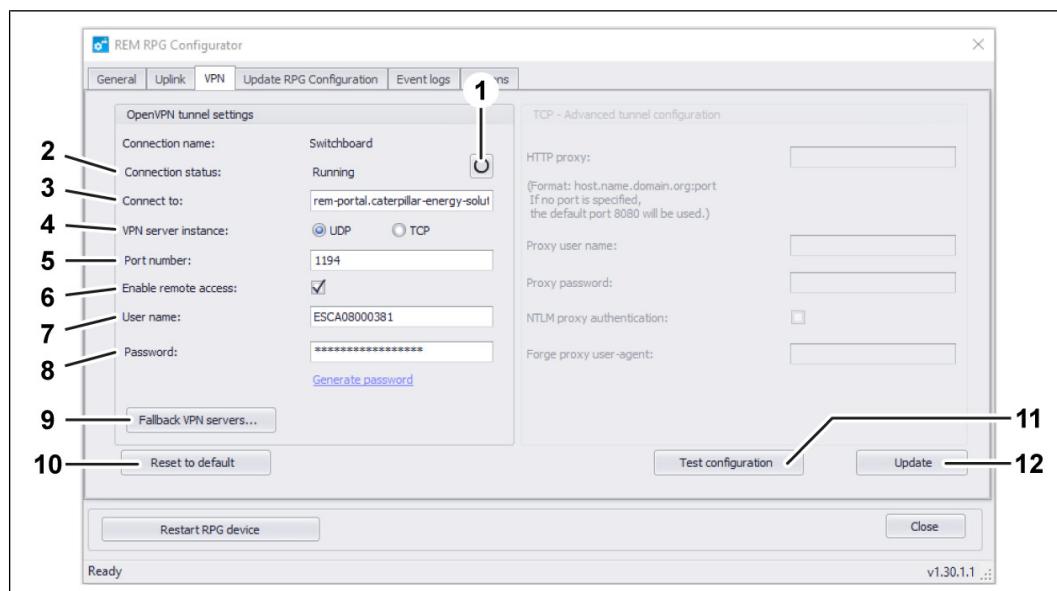
- You can specify the Google DNS server as the IP address, for example: 8.8.8.8 and 8.8.4.4

- You can also enter domain names in place of IP addresses (for example, dns.google.com). However, in the event of a fault, the advantage of IP addresses is that they require no name resolution via DNS.
7. In the **Select country** list (7), select the country whose mobile communications network the router is supposed to use.
 - Normally this is the country in which the router is located.
 8. In the **Select provider** list (8), select the operator of the mobile communications network supposed to be used by the router.
 9. The configuration program automatically enters the APN of the mobile communications network operator in the **Select APN** (9) and **Access point name** (10) fields. The APN is the name of the transition point from the mobile communications network to IP-based data networks.
 10. If the mobile communications provider requires authentication:
 - In the **Username** field (11), enter the username provided to you by the mobile communications provider.
 - In the **Password** field (12), enter the password provided to you by the mobile communications provider.
 - In the **Authentication method** list (13), select the protocol to be used by the router to authenticate itself to the APN.
 11. If the mobile communications provider does not require authentication:
 - Leave the **Username** (11) and **Password** (11) fields empty.
 - In the **Authentication method** list (13), leave the value as **PAP or CHAP**.
 12. If the router should use the DNS servers of the mobile communications provider: Set the **DNS** option field (14) to **Automatic**.
 13. If the router is supposed to use other DNS servers: Set the **DNS** option field (14) to **Manual**.
 - In the **Primary DNS server** field (15), enter the IP address of the preferred DNS server.
 - In the **Secondary DNS server** field (16), enter the IP address of the alternative DNS server.
 14. Click on **Update** (17).

5.9 Configuring the VPN connection

The router is preconfigured so that it normally establishes a connection to the Rendezvous Server automatically once the prerequisites are fulfilled. Therefore, only change the settings on the **VPN** tab if necessary.

1. Click on the **VPN** tab.



27021598055785483

If you click on the **Refresh** button (1), the configuration program updates the displayed data.

In the **Connection status** text field (2), the configuration program shows whether the router can contact the Rendezvous Server:

- The status **Running** means that the router can contact the Rendezvous Server.
- The status **Connection refused** means that the router cannot contact the Rendezvous Server. The IP address (3), username (7) or password (8) may be wrong.
- The status **Closed** means that the router has closed the connection to the Rendezvous Server. Checkbox (6) might be unticked.

The text field **Connect to** (3) shows the IP address of the Rendezvous Server. The **VPN server instance** option field (4) sets which protocol the router uses for communication with the Rendezvous Server. The text field **Port number** (5) shows the port number used by the router for communication with the Rendezvous Server.

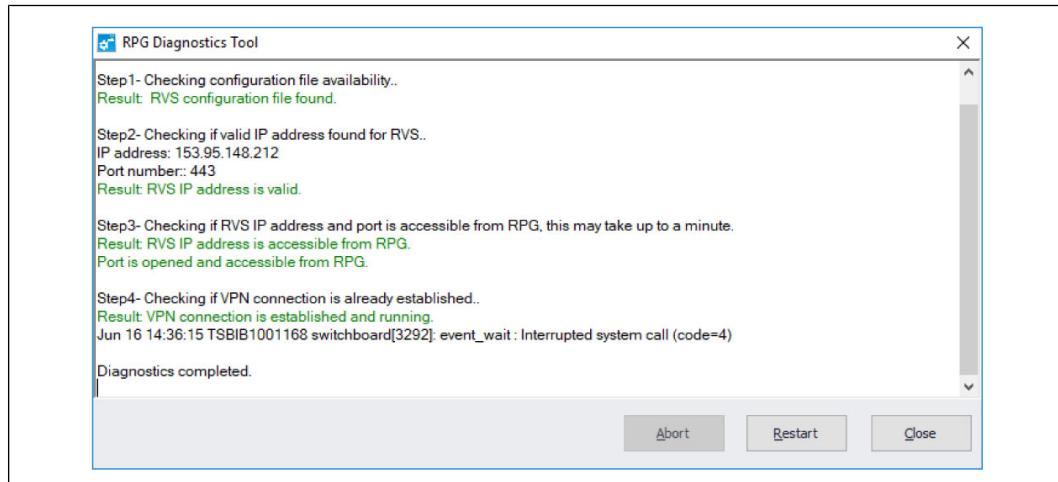
If you untick the **Enable remote access** checkbox (6), the router no longer communicates with the Rendezvous Server. It is then no longer possible to access the plant remotely.

The **Username** (7) and **Password** (8) text fields contain the username and password that the router uses to log on to the Rendezvous Server.

After clicking on the **Fallback VPN servers...** button (9), a new window with the addresses of the Rendezvous Server will appear. You only need to change something in this window if the VPN connection will be made via a proxy server.

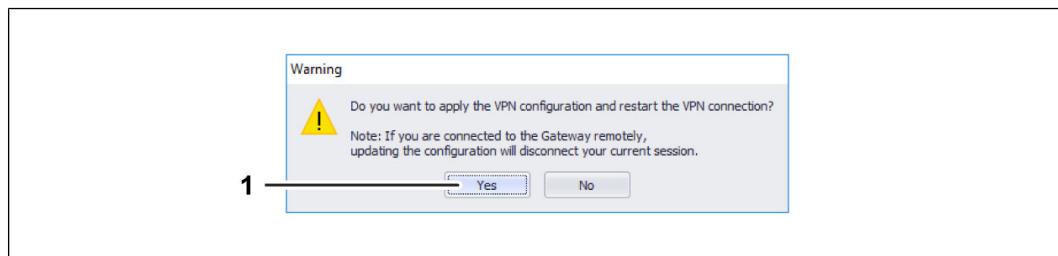
Clicking the **Reset to default** button (10) will cause the router to reset all VPN settings to their factory defaults.

When you click the **Test configuration** button (11), the router tests the connection to the Rendezvous Server. The router displays the test results in a separate window. The test results help to find the cause of connection problems.



18014398799934219

To save changed settings, click the **Update** button (12). The router then asks if you want to apply the configuration and restart the VPN connection.



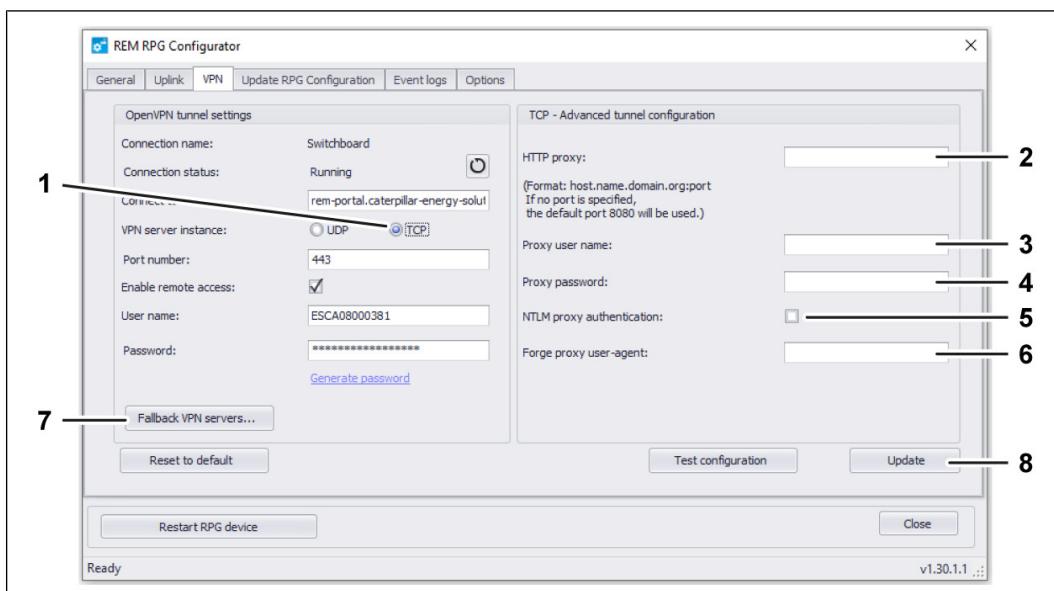
18014398799938955

1. Click on **Yes** (1).

⇒ You then have to wait 60 seconds until the configuration program can be used again.

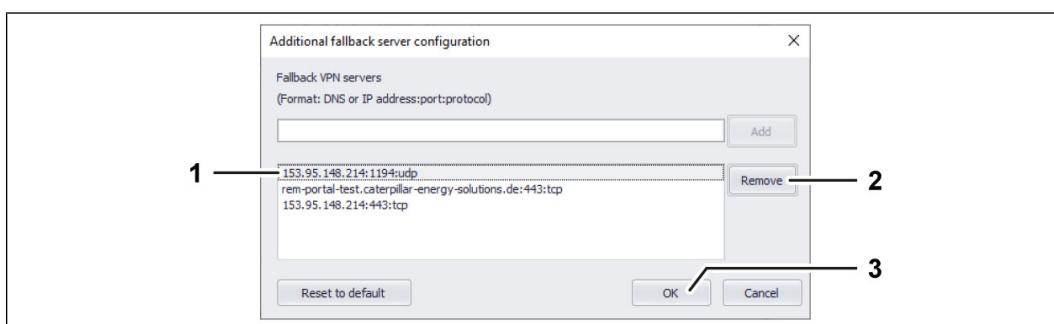
VPN connection via a proxy server

If the router's data traffic is supposed to run via a **proxy server**, proceed as follows:



27021598055790219

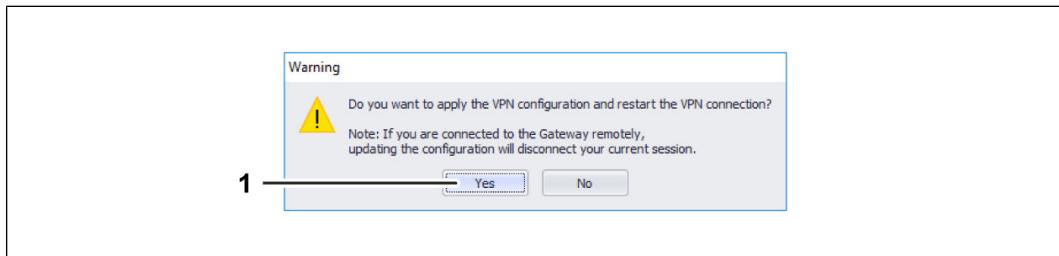
1. Set the **VPN Server Instance** option field (1) to **TCP**.
 - The configuration program automatically sets the port number to 443.
2. Enter the IP address of the proxy server in the **HTTP proxy** (2) field.
3. In the **Proxy username** field (3), enter the username that the router should use to log on to the proxy server.
4. In the **Proxy password** field (4), enter the password that the router should use to log on to the proxy server.
5. If necessary, tick the **NTLM proxy authentication** checkbox (5).
6. If necessary, fill in the **Forge proxy user-agent** field (6).
7. Click on **Fallback VPN servers...** (7). The following window appears:



18014399130556043

8. Remove all addresses that end in "udp" by selecting the entry (1) and then clicking **Remove** (2).
 - Explanation: HTTP proxy servers can only process TCP, therefore you must remove all entries that use UDP.
 - Click on **OK** (3) to close the window.

9. Click on **Update** (8, located on the **VPN** tab).
 - The router asks if you want to apply the configuration and restart the VPN connection.



18014398799938955

10. Click on **Yes** (1).
 - ⇒ You then have to wait 60 seconds until the configuration program can be used again.

5.10 Updating the configuration

The router is preconfigured at delivery so that it normally establishes a connection to the Rendezvous Server automatically once the prerequisites are fulfilled.

For a number of reasons, it can however be necessary, for example, to update the firmware, to change the network settings or to replace the expired certificates during the initial commissioning of a router.

In such cases Caterpillar Energy Solutions will provide an update for the router configuration. An update consists of a file, the so-called configuration container, which includes all settings that are to be updated on a router.

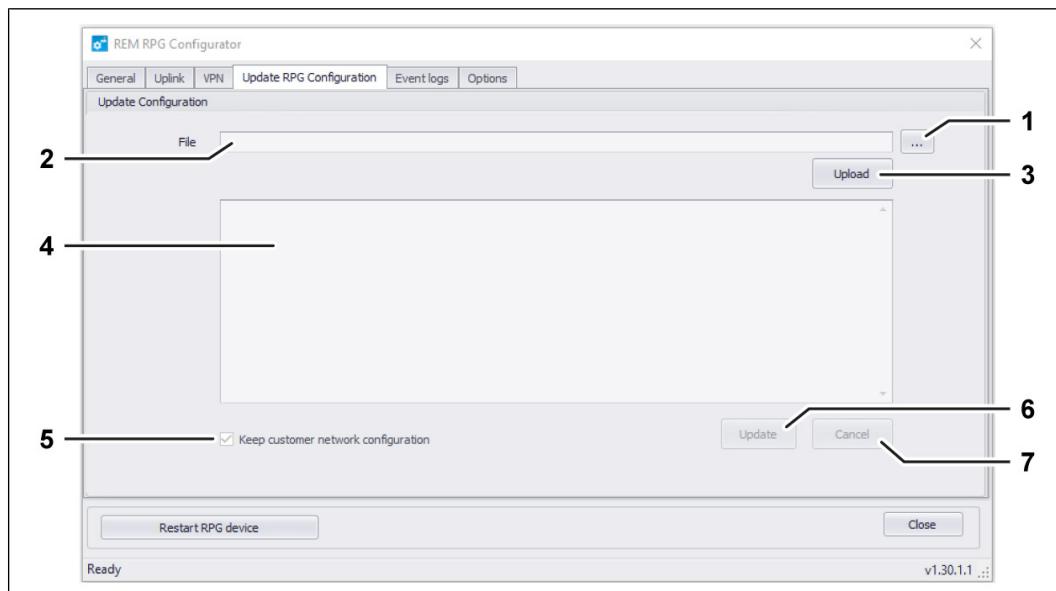
To run the update on a router, load the configuration container using the RPG configurator on the router and then start the update process.

Once the update process is complete, the configuration container is no longer required and is automatically deleted from the router's memory. If the update process is disrupted due to an error, the configuration container is automatically deleted as above. The configuration container never permanently remains on the router.

The automatic deletion only affects the configuration container, which is found in the internal memory of the router. Configuration containers that are found on the laptop connected to the router, for example, are *not* deleted.

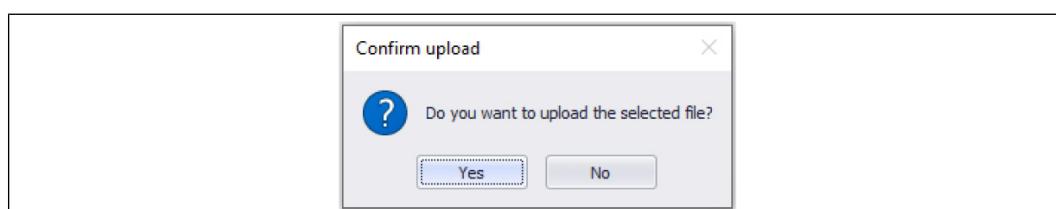
- ✓ Requirements for the following steps: The configuration container must be available locally, for example on the laptop's hard disk.

1. Click on the tab **Update RPG Configuration**.



18014398881789963

2. Click on the button with the three dots (1) and then select the configuration container.
 - The configuration container is an encrypted tar file with the file ending .tar.enc.
 - The file name of the selected configuration container will appear in the text field **File** (2).
3. Click on the button **Upload** (3).
 - The program will ask if you want to upload the selected file.
 - Note: Uploading simply means that the program will transfer the configuration container into the router's memory. Uploading will not yet change the configuration of the router.



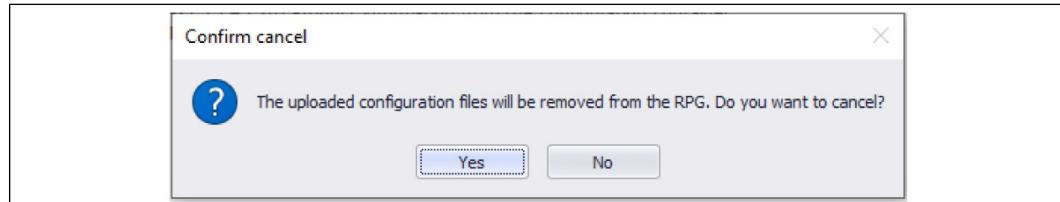
2802966923

4. Click on the **Yes** button to upload the configuration container.
 - When the program has uploaded the configuration container, the message "Upload completed..." will appear in the notification list (4).

```
[2023-07-27 13:45:20] Uploading Config_RPG-02-03_7.0.tar.enc into the device ESCA08000381...
[2023-07-27 13:45:20] Upload completed...
[2023-07-27 13:45:20] Product information from the configuration container:
product: RPG-02-03 version:7.0
```

2803097355

- Additionally, following a successful upload the buttons **Update** (6) and **Cancel** (7) are active.
5. If you wish to override the available network configuration, deactivate the option **Keep customer network configuration** (5). If not, leave this option activated.
 - The network configuration is all of the settings in the **Uplink** tab. If the option **Keep customer network configuration** is deactivated, the available network configuration is overridden during the update process by the default settings from the configuration container.
 6. Decide now if you wish to run the update on the router: If yes, click on the button **Update** (6). If not, click on the button **Cancel** (7).
 - If you have clicked **Cancel**, a message will appear, stating that the program will delete the uploaded configuration container. To begin the process, click **Yes**.



2803195787

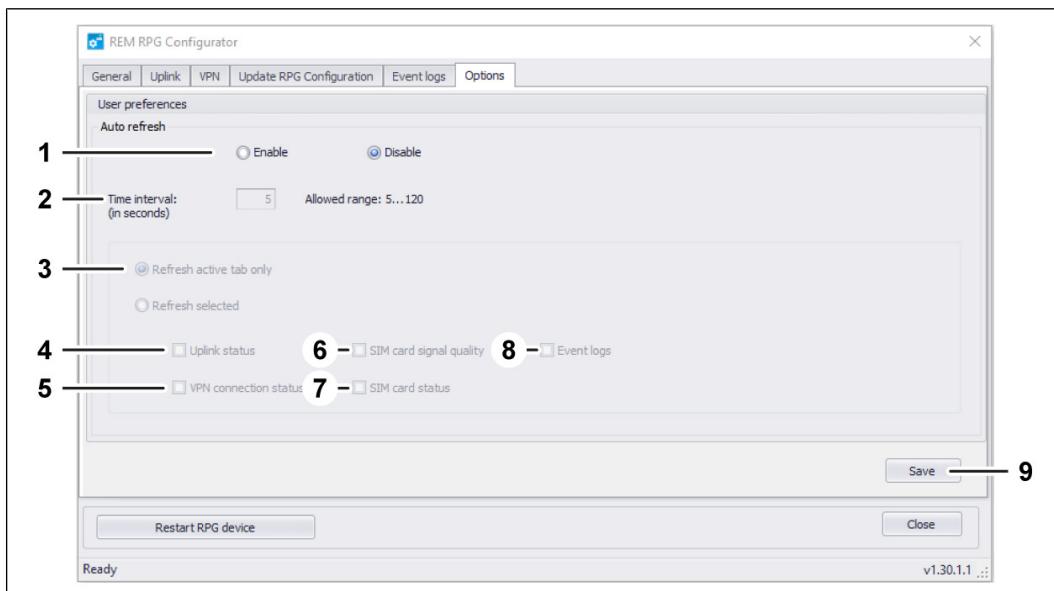
- If you have clicked **Update**, the program will run the update. In the notification list (4) you will see which changes have been implemented and whether the update process has been successful.
- Once the update process has been successfully completed, restart the router, so that the changes come into effect. When restarting, the router automatically deletes the uploaded configuration container.
- If the update process is disrupted due to an error, the uploaded configuration container is automatically deleted. To restart the update process, you must first once again upload the configuration container.

5.11 Changing settings

Refresh buttons can be found on some tabs of the configuration program tabs. If you click on a Refresh button, the configuration program will update the displayed values.

The **Options** lets you tell the configuration program to automatically refresh given values after a certain time. In this way, you can save yourself repeated clicks on the Refresh button.

1. Click on the **Options** tab.

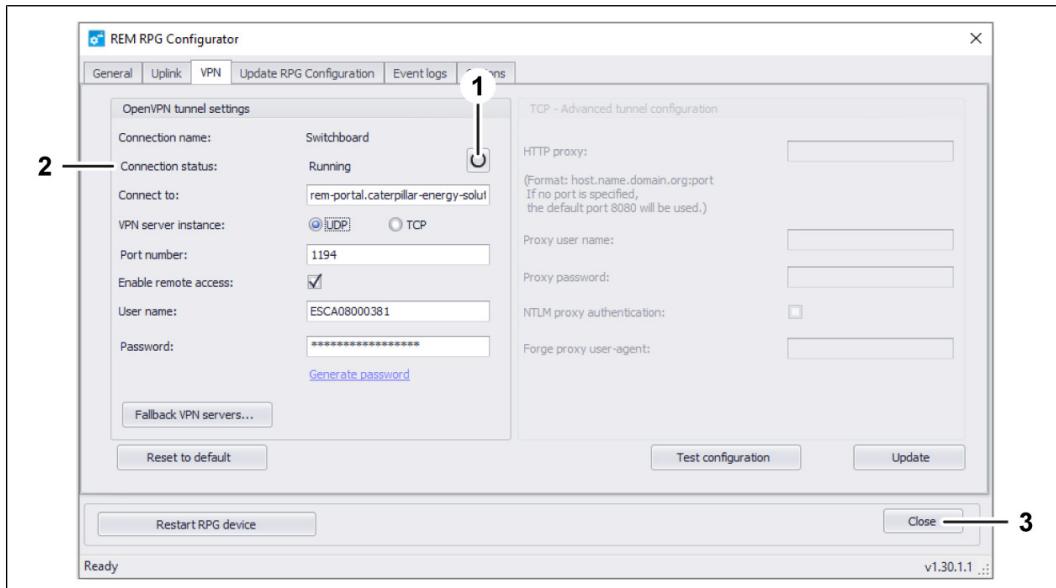


9007199943628555

2. Set option field (1) to **Enable** to turn on automatic refresh.
3. Enter the refresh interval in field (2).
 - Valid values: 5 seconds up to a maximum of 120 seconds.
4. Use option field (3) to select which values the configuration program should refresh automatically:
 - The **Refresh active tab only** option causes only the values on the active tab to be refreshed.
 - The **Refresh selected** option causes the selected values (4 to 8) to be refreshed.
 - Ticking the **Uplink status** checkbox causes the "Status" field on the "General" tab to be refreshed automatically.
 - Ticking the **VPN connection status** checkbox causes the "Connection status" on the "VPN" tab to be refreshed automatically.
 - Ticking the **SIM card signal quality** checkbox causes the "Signal quality" field on the "SIM Card" tab to be refreshed automatically.
 - Ticking the **SIM card status** checkbox causes the "Status" field on the "SIM Card" tab to be refreshed automatically.
 - Ticking the **Event logs** checkbox causes the list on the "Event logs" tab to be refreshed automatically.
5. Click **Save** (9) to save the settings you have changed.

5.12 Final inspection

- Click on the **VPN** tab.



27021598055807755

- Click on the **Refresh** button (1).
- Check whether the connection from the router to the Rendezvous Server has the status (2) **Running**.
 - If the connection does not have the status **Running**, a fault has occurred ([► Faults with the router \[▶ 87\]](#)).

If everything is correct and there are no faults:

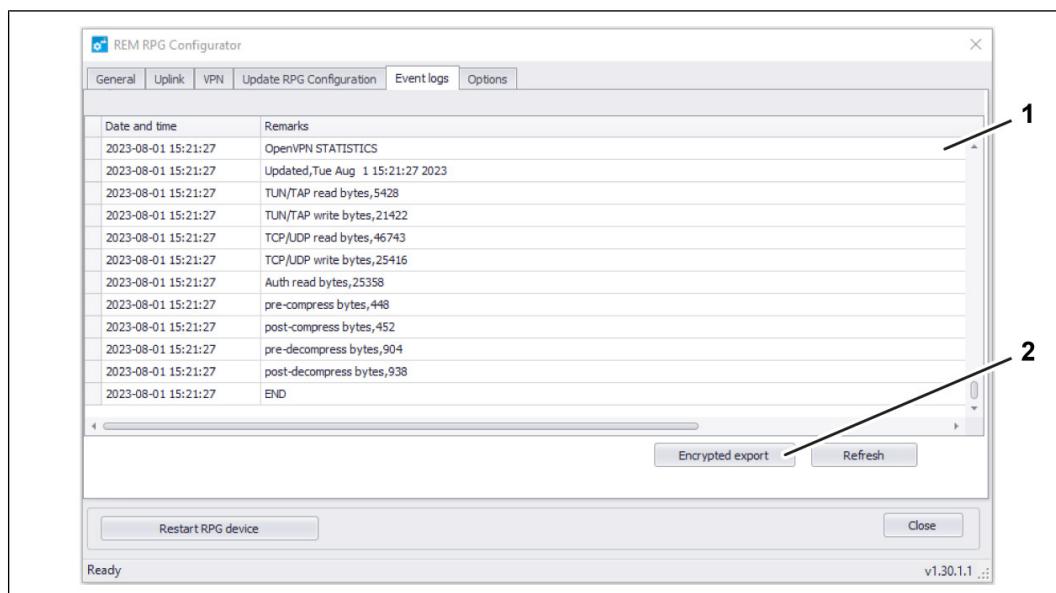
- Click on **Close** (3) to close the configuration program.
- Disconnect the computer from the router.

This completes commissioning.

5.13 Exporting log data

While the router is in operation, it writes system events as well as events concerning the connection to the Rendezvous Server to its internal memory. In the case of a fault, the log data help identify the cause of the fault more quickly.

- Click on the **Event Logs** tab.
 - The list (1) shows the recorded log data.



18014398881798155

- It is possible to export the log data. For security reasons, the configuration program encrypts the log data when exporting. Only Caterpillar Energy Solutions can decrypt the exported data.

2. Click on the **Encrypted Export** button (2).

6 Operation

6.1 Installing a Remote Access Client

Prerequisites for installation

The computer on which you are installing the Remote Access Client must satisfy the following requirements:

- Operating system Microsoft Windows 10 or Windows 11
Microsoft and Windows are registered trademarks of Microsoft Corporation, USA.
- An installation with Microsoft Windows 7 or Windows 8 is possible under certain conditions, but is not supported by us. That means: If problems occur during installation or use, our service cannot provide further assistance.

For Windows 7, the update KB3033929 must be installed or a newer update that replaces it.

For Windows 7, the Microsoft .NET Framework 4.5 (or newer) must be installed.

- Screen resolution of at least 1024 x 768
- At least 100 megabytes of free hard disk space
- If the "Virtual Serial Ports Emulator" program from Eterlogic.com is running on the computer, exit or uninstall it. The Remote Access Client does not work if Virtual Serial Ports Emulator is running simultaneously.
- If an older version of the Remote Access Client is installed on the computer, it must be uninstalled before the new version can be installed.
- The COM ports 394, 395, 500 and 600 must be free. If one of these COM ports is busy, the Remote Access Client will not work. (It is possible to assign other COM ports to the Remote Access Client after installation.)

You also require the installation file. You will receive the link to the download address of the installation file from us via email after you have received your login credentials.

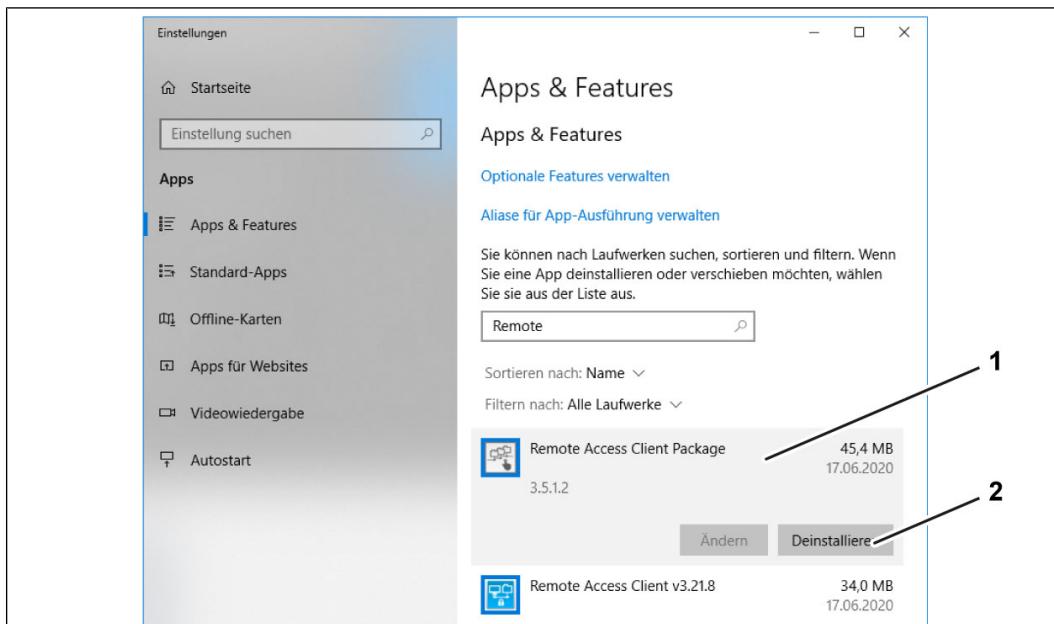
For more information on login credentials, see chapter [Registering the router and users \[▶ 29\]](#).

If you have any queries, please contact rpg@mwm.net.

Uninstalling the old program version

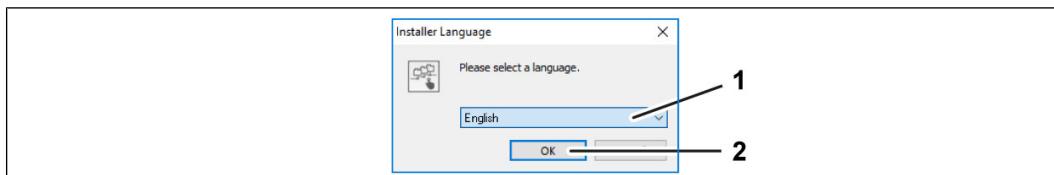
If an older version of the Remote Access Client is installed on the computer, it must be uninstalled before the new version can be installed. To do so, proceed as follows:

1. Close Remote Access Client. Close all open application programs.
2. In **Windows Settings**, go to the page **Apps > Apps & Features** and search for "Remote Access Client Package".



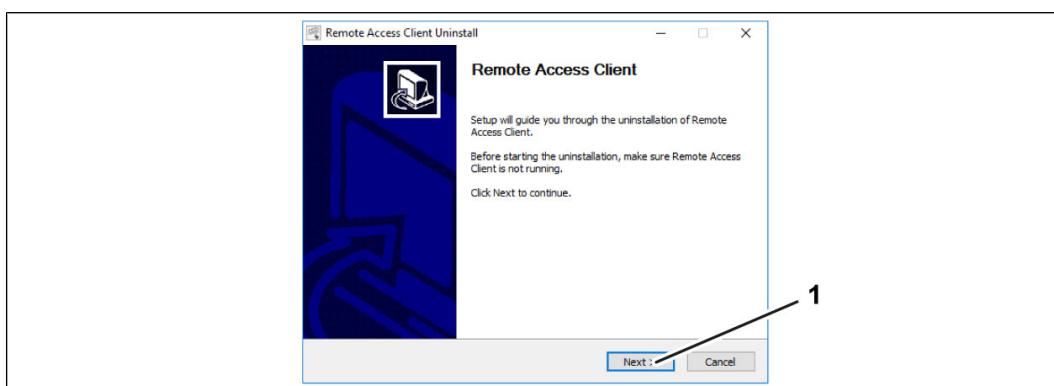
18014398800132619

3. Select the entry "Remote Access Client Package" (1) and click on **Uninstall** (2).
 - Administrator rights are required for the deinstallation.
 - The programs "Remote Access Client vX.X.X" and "Virtual Com Port Service" are automatically uninstalled along with it.



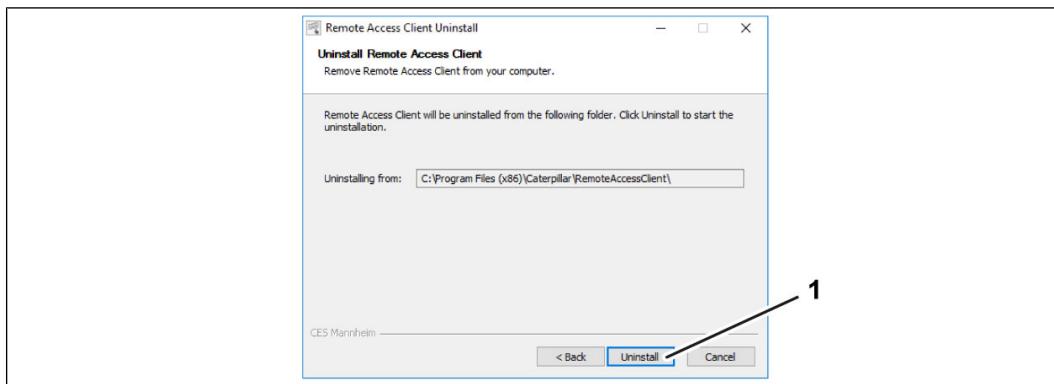
18014398800137355

4. Select the language of the uninstaller from the list (1) and then click on **OK** (2).
 - Note: the following illustrations show the English version of the deinstallation program.

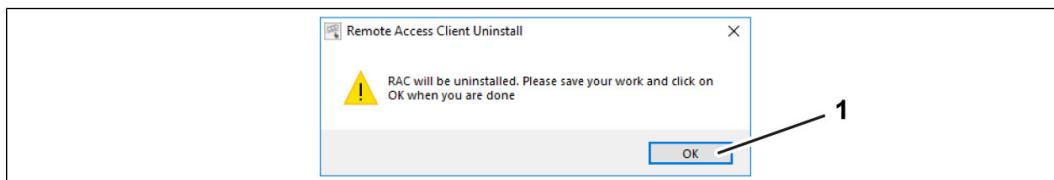


18014398800142091

5. Click on **Next** (1).

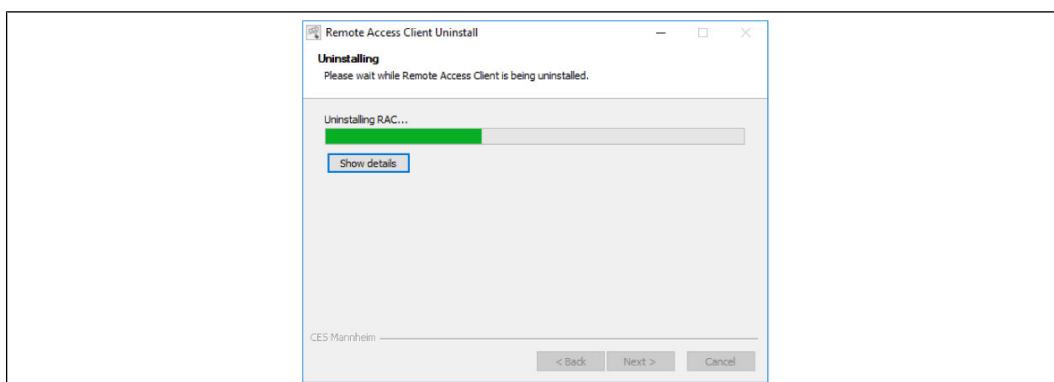


18014398800153995

6. Click on **Uninstall** (1).

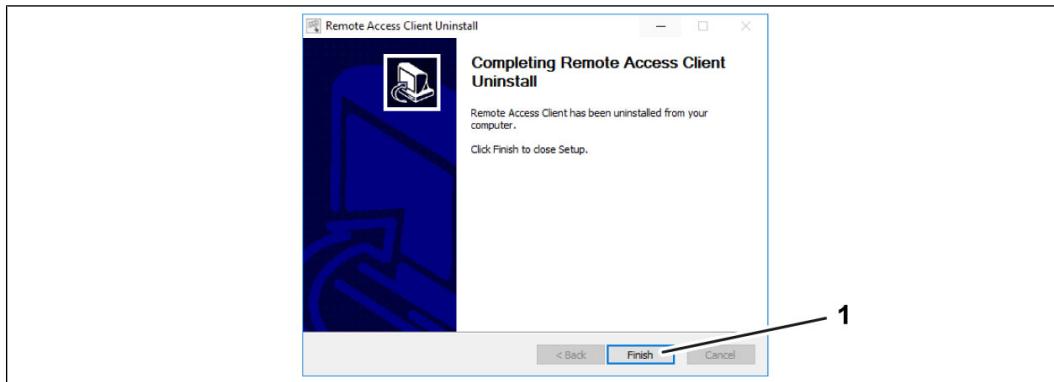
18014398800171531

- The uninstaller shows the message “RAC will be uninstalled. Please save your work and click on OK when you are done” (The Remote Access Client will be uninstalled. Please save all opened files and then click OK).

7. Click on **OK** (1).

18014398800176267

8. Wait until the deinstallation is finished.



18014398800181003

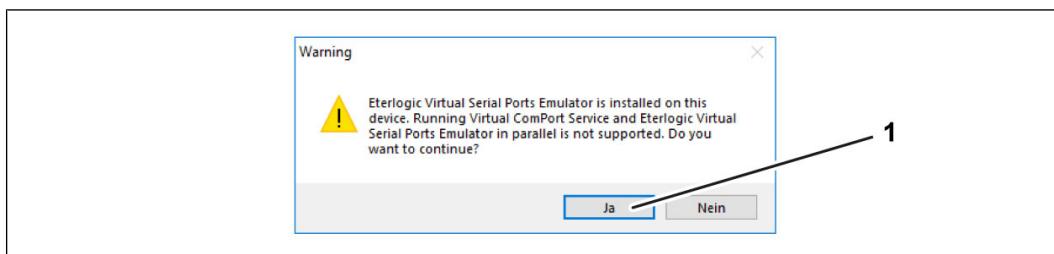
9. Click on **Finish** (1).

⇒ The Remote Access Client is now uninstalled.

Installing the new program version

To install the Remote Access Client, proceed as follows:

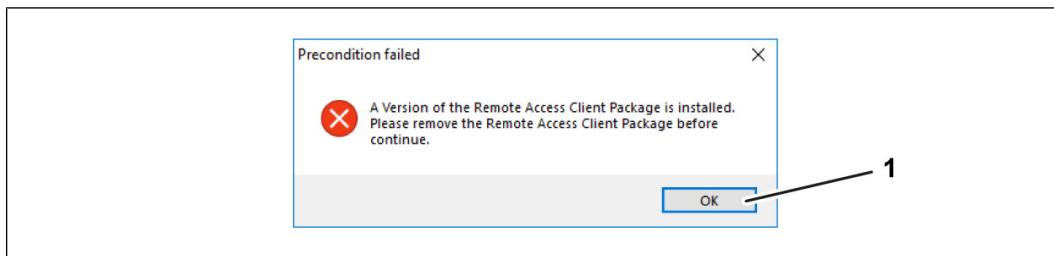
1. Close all open application programs.
2. Start the installation program **RemoteAccessClientPackageInstaller-X.X.X.X.exe**.
 - Administrator rights are required for the installation.
 - If the Virtual Serial Ports Emulator program is installed on the computer, a warning message appears.



18014398800198539

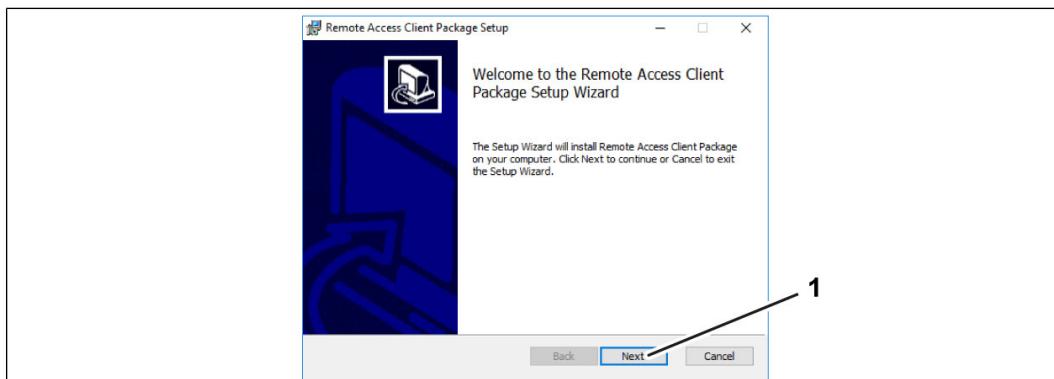
3. Click on **Yes** (1) to begin the installation.

- Note: it is possible to install both the Virtual Serial Ports Emulator and the Remote Access Client on one computer. However, it is not possible to use both programs at the same time. If you do not uninstall Virtual Serial Ports Emulator, you must quit it before each launch of the Remote Access Client.
- If an older version of the Remote Access Client is installed on the computer, the installation process will be aborted.



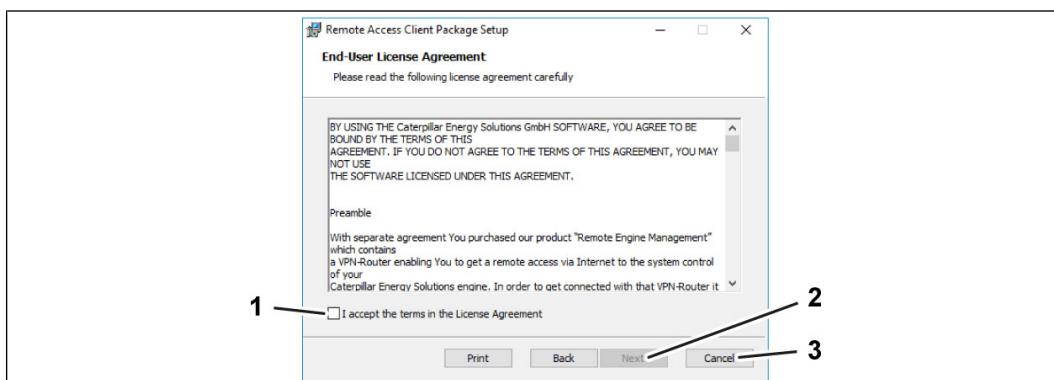
18014398800203531

4. Click on **OK** (1). Uninstall older versions of the Remote Access Client, then start the installation program again.



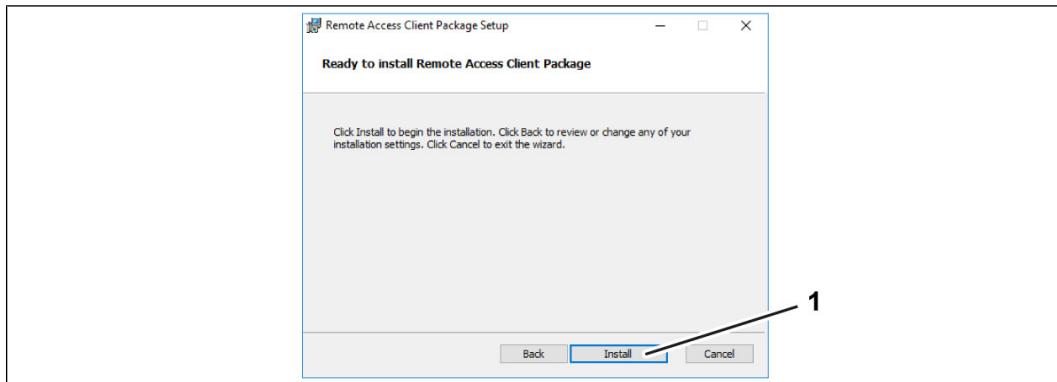
18014398800208523

5. Click on **Next** (1).



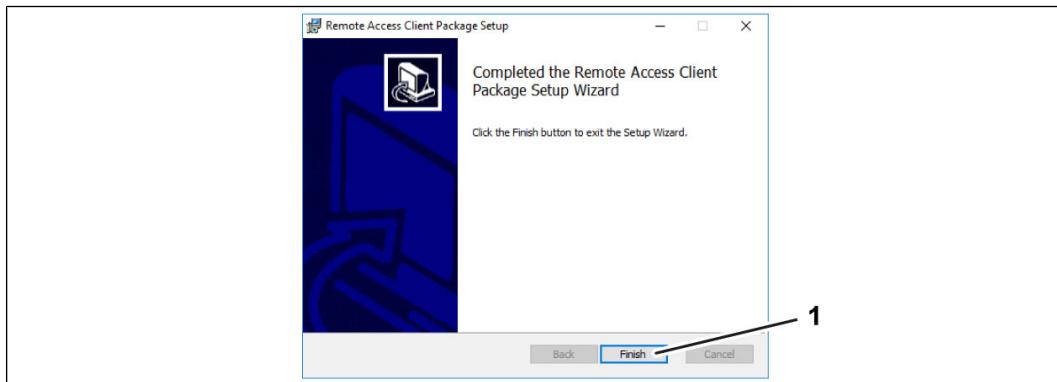
18014398800213515

6. If you accept the license terms, activate the checkbox (1) and click **Accept** (2).
 - If you do not accept the license terms, click on **Cancel** (3).



18014398800218507

7. Click on **Install** (1).



18014398800236299

8. Click on **Finish** (1) to complete the installation.

⇒ The Remote Access Client is now installed.

Checking the network settings

In order for remote access to be possible, the Remote Access Client must communicate with the Rendezvous Server.

Domain name	IP address	Port	Protocol
rem-portal.caterpillar-energy-solutions.de	153.95.148.211	443	TCP, https
rem-portal.caterpillar-energy-solutions.de	153.95.148.211	1194	UDP

If the data traffic of the Remote Access Client runs via a proxy server, the proxy server must allow the data traffic to the specified addresses; the same applies for a firewall.

OpenVPN and the local router network use the IP address areas listed in the following Table. Other customer-side devices cannot be in the same network segment, i.e. they must use a different IP address range.

The Remote Access Client must be able to create routes on the client system that lead to the networks listed below.

Remote address	IP address range	Port	Protocol
—	10.0.0.0/24	443	TCP
		1194	UDP
153.95.148.212	10.10.0.0/16	1194	UDP
153.95.148.211	10.20.0.0/16	443	TCP
153.95.148.211	10.30.0.0/16	1194	UDP
153.95.148.212	10.40.0.0/16	443	TCP
—	100.64.0.0/100	443	TCP
		1194	UDP

Checking the internet connection

The internet connection used to transfer data from the TEM Evo control system to the JVView program must have a certain minimum quality. The measure of the quality of the internet connection here is the bandwidth, the latency and the packet loss rate. If the internet connection does not meet the minimum requirements, JVView can only be used to a limited extent or not at all.

Bandwidth

The bandwidth is the maximum data throughput of the internet connection.

The transmission of the operating cycle history with the full number of signals (20/20) requires a bandwidth of up to 18 kbit/s with an average of 12 kbit/s.

Latency

Latency (also: packet runtime) is the amount of time it takes for a data packet to get from the control system to JVView.

If the latency is too high, JVView cannot seamlessly capture and display the operating cycle history.

How high the latency may be depends on the speed of the motor. The higher the speed, the shorter the operating cycle and the lower the maximum permissible latency.

The following table shows how high the average latency may be for JVView to still display a seamless operating cycle history.

Engine series	Rated speed / mains frequency	Maximum permissible average latency
CG132	1500 rpm / 50 Hz	80 ms
	1800 rpm / 60 Hz	66.6 ms
CG170	1500 rpm / 50 Hz	80 ms
	1500 rpm / 60 Hz	80 ms
CG260	1000 rpm / 50 Hz	120 ms
	900 rpm / 60 Hz	133.3 ms

The permissible latency specified in the table applies to the full number of signals (20/20).

Packet loss rate

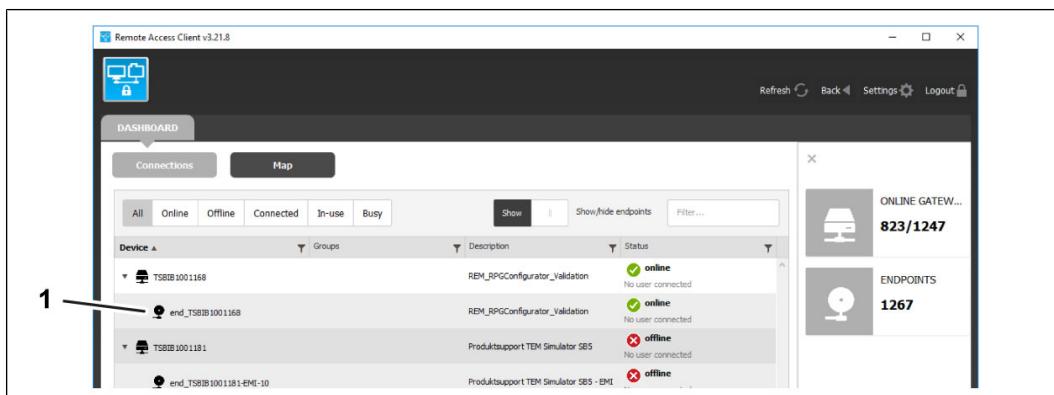
The packet loss rate indicates how many data packets were lost on the way from the control system to the JView.

When using JView, the packet loss rate must not exceed 18 %. If the packet loss rate is higher, connection interruptions occur.

Measuring latency and packet loss rate

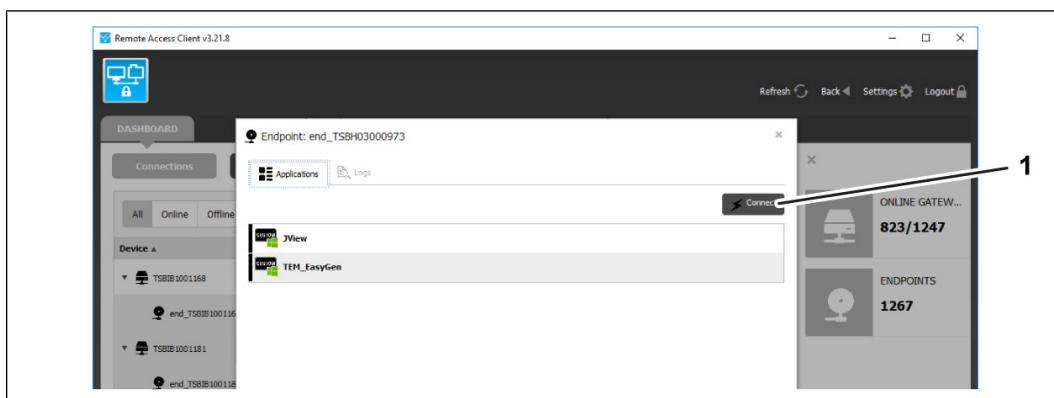
You can measure the latency and packet loss rate using the "Ping.exe" program.

1. Connect to the Rendezvous Server.



18014398800258059

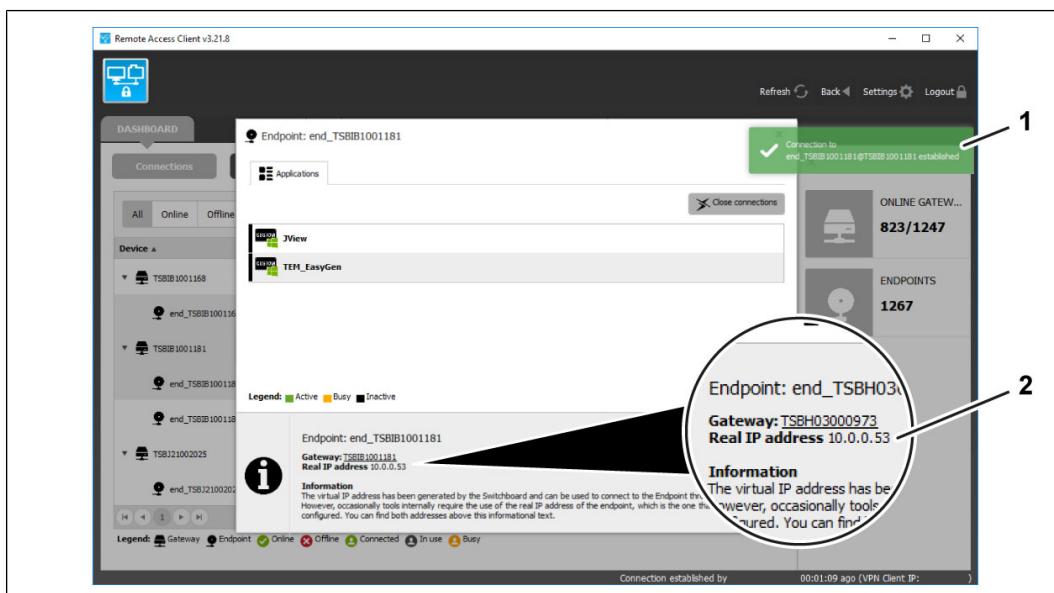
2. Click on the **Endpoint** (1) you would like to connect to.



18014398800262795

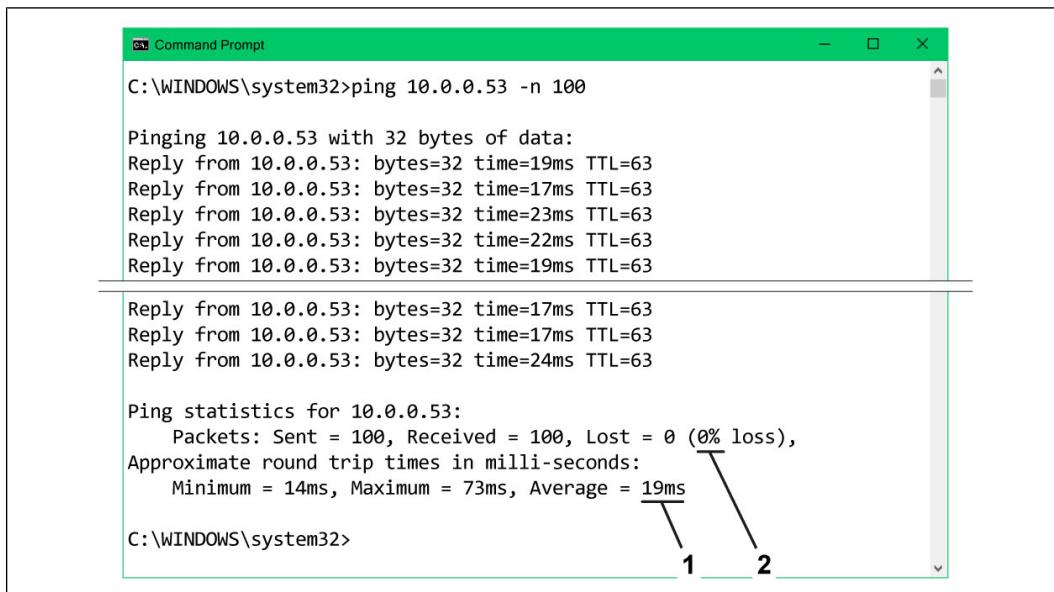
3. Click on **Connect** (1).

- Do not click on any of the applications (JView, TEM_EasyGen).
- Once the connection is established, a brief message appears (1, see the next illustration).



18014398800267531

4. Start command prompt (Start > Windows System > Command Prompt).
5. Enter ping <IP address> -n 100, typing the IP address (2) displayed in the Remote Access Client instead of <IP address>. Then press Enter.
 - Example: If the IP address (2) is 10.0.0.53, enter: ping 10.0.0.53 –n 100.



```
C:\WINDOWS\system32>ping 10.0.0.53 -n 100

Pinging 10.0.0.53 with 32 bytes of data:
Reply from 10.0.0.53: bytes=32 time=19ms TTL=63
Reply from 10.0.0.53: bytes=32 time=17ms TTL=63
Reply from 10.0.0.53: bytes=32 time=23ms TTL=63
Reply from 10.0.0.53: bytes=32 time=22ms TTL=63
Reply from 10.0.0.53: bytes=32 time=19ms TTL=63

Reply from 10.0.0.53: bytes=32 time=17ms TTL=63
Reply from 10.0.0.53: bytes=32 time=17ms TTL=63
Reply from 10.0.0.53: bytes=32 time=24ms TTL=63

Ping statistics for 10.0.0.53:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 73ms, Average = 19ms

C:\WINDOWS\system32>
```

18014398800272267

- 1 Average latency
- 2 Packet loss rate

If the measured average latency (1) is greater than the permissible latency, reduce the number of signals. With a reduced number of signals (for example 9/20 instead of 20/20), the permissible latency increases. However, with a reduced number of signals, the time intervals between the measured values are greater. The operating cycle history is then somewhat less accurate.

If the measured packet loss rate (2) is greater than 18 %, you will experience connection interruptions while using JView. In this case, it is not possible to use JView via the Remote Access Client RAC.

6.2 Connecting to a plant

To connect to a plant using the Remote Access Client, you require:

- An internet connection
The internet connection must allow data traffic to and from the Rendezvous Server. For example, if data traffic passes through a proxy server or firewall, the proxy server and firewall must be set so as to allow this data traffic.
- Login credentials (username and password)
- JView and/or Woodward ToolKit

Connecting to the Rendezvous Server

1. Start the Remote Access Client (Start menu > Caterpillar > Remote Access Client).



18014398800283019

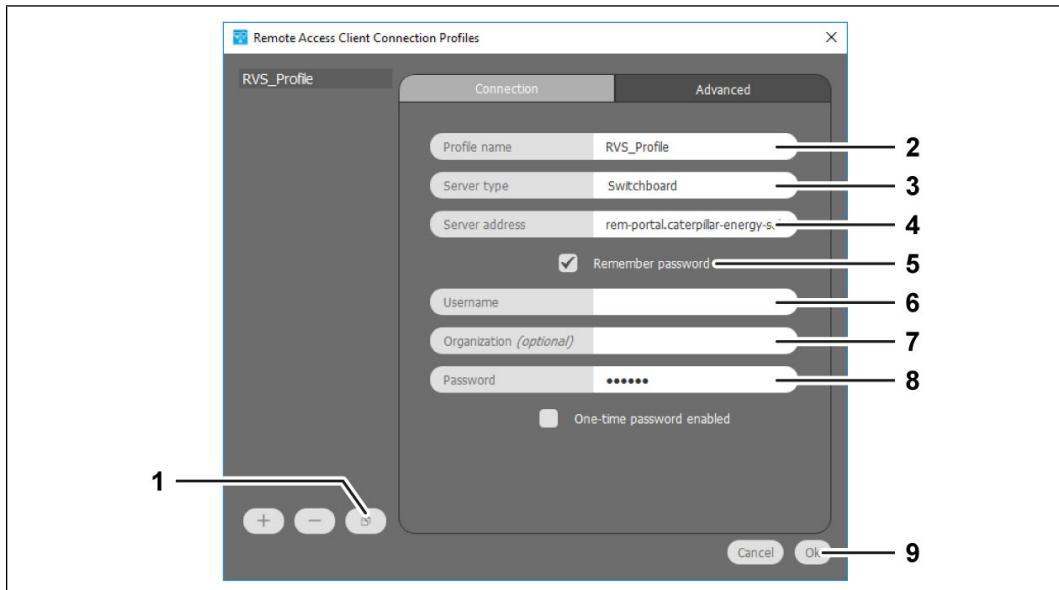
You can select a connection profile in the **Profile** field (1). When you start the client for the first time, the default profile "RVS_Profile" is selected here.

1. Click on the gear icon (2) to change the connection profile.

Note: The default profile "RVS_Profile" will be overwritten with each new installation of the Remote Access Client. Therefore, save your connection settings in your own, new profile.

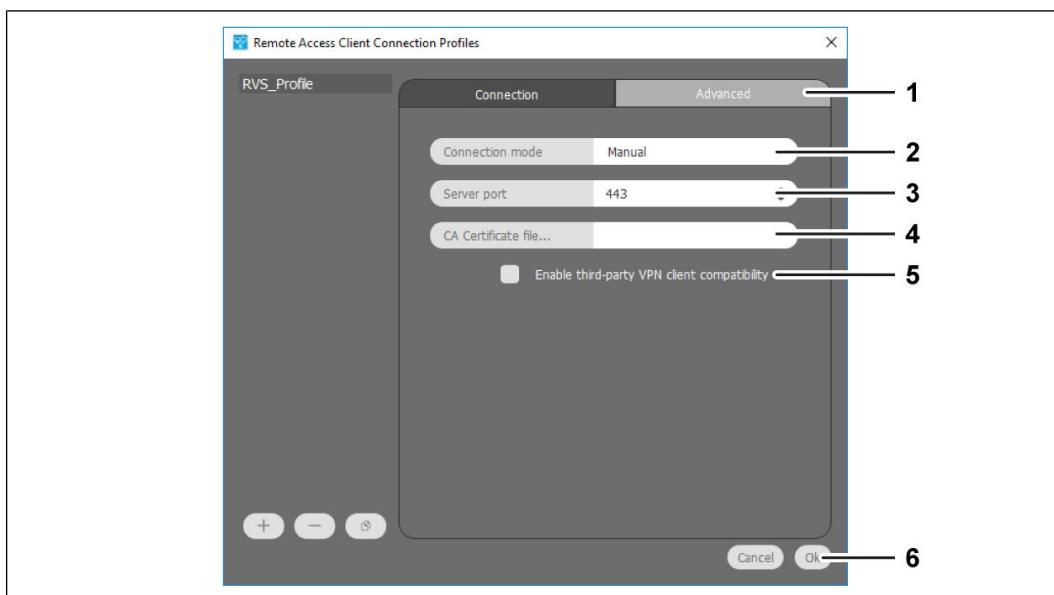
If a previously created profile no longer appears in the selection list (1) after updating the Remote Access Client, then the profile is not compatible with the new program version. In this case, create the profile again.

Creating a new profile



18014398800313355

1. Click the button (1) to create a new profile based on the default profile.
2. To rename the profile, you can enter a different name in the **Profile name** field (2).
3. The setting **Server type** (3) must be set to "Switchboard".
4. The field **Server address** (4) must contain the address of the Rendezvous Server (RVS). This is "rem-portal.caterpillar-energy-solutions.de". If the DNS name resolution does not function, the IP address can also be entered here.
5. If the **Remember password** option (5) is activated, the password (8) is saved in the connection profile. If you deactivate the option, you must re-enter the password each time you establish a connection.
6. Enter your username in the **Username** field (6).
7. Leave the **Organization** field (7) empty, otherwise no connection will be established.
8. Enter your password in the **Password** field (8).



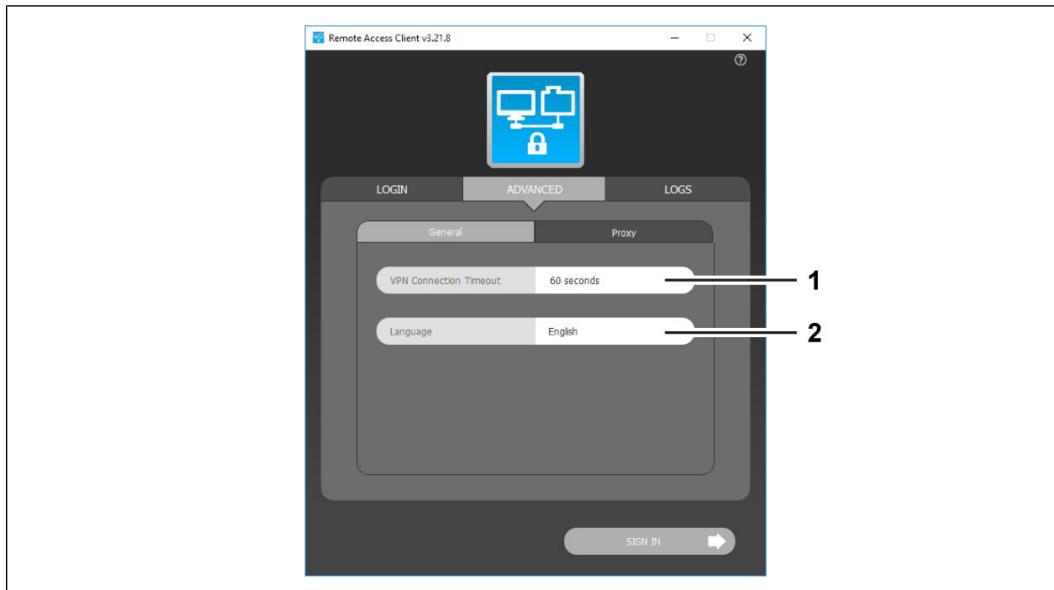
18014398800318091

In the **Advanced** tab (1), you can alter certain special settings.

1. In the **Connection mode** field (2), one of two options can be selected:
 - The "Manual" option allows Remote Engine Management to establish a connection with the Rendezvous Server only when prompted.
 - The "Upon computer start" option allows Remote Engine Management to automatically establish a connection with the Rendezvous Server when the computer boots up.
2. In the **Server port** field (3) "443" is entered by default. This setting cannot be changed.
3. The field **CA Certificate file** (4) can remain empty.
4. The option **Enable third-party VPN client compatibility** (5) must remain deactivated.
5. Click on **Ok** (6) to save the settings.

Advanced settings

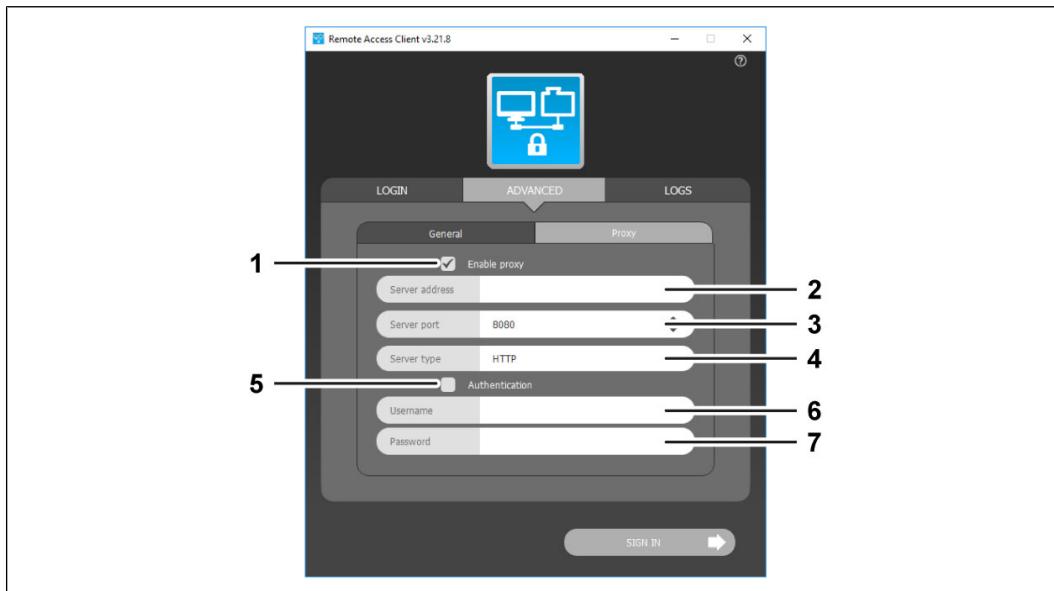
In the **ADVANCED > General** tab, you can enable additional settings:



18014398800335627

1. The **VPN Connection Timeout** field (1) contains the amount of time after which the Remote Access Client will disconnect if no data has been transferred. The default setting is 60 seconds.
2. In the **Language** field (2), the user interface language can be changed. (Currently English and German are the only options.)

In the tab **ADVANCED > Proxy** you can enter the data for a proxy server, if the connection should be made via a proxy server.

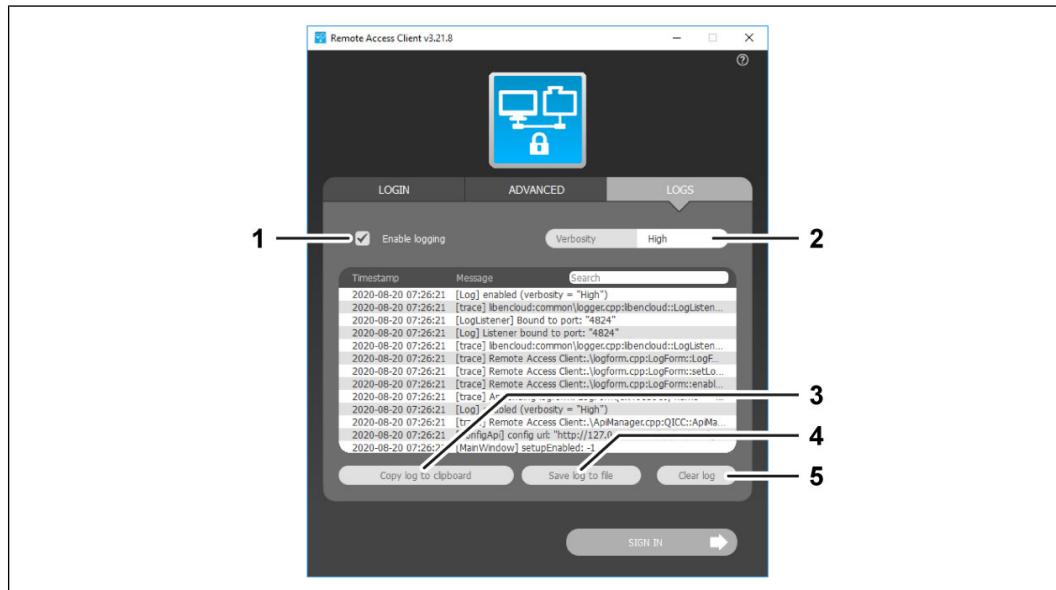


18014398800340363

1. Tick the checkbox **Enable proxy** (1) and fill out the fields **Server address** (2), **Server port** (3) and **Server type** (4).
2. If the proxy server requires authentication: Tick checkbox **Authentication** (5) and fill out the fields **Username** (6) and **Password** (7).

Log data

The Remote Access Client can log its own activity in detail. The log data collected in this way helps the service personnel to find the cause of any faults.

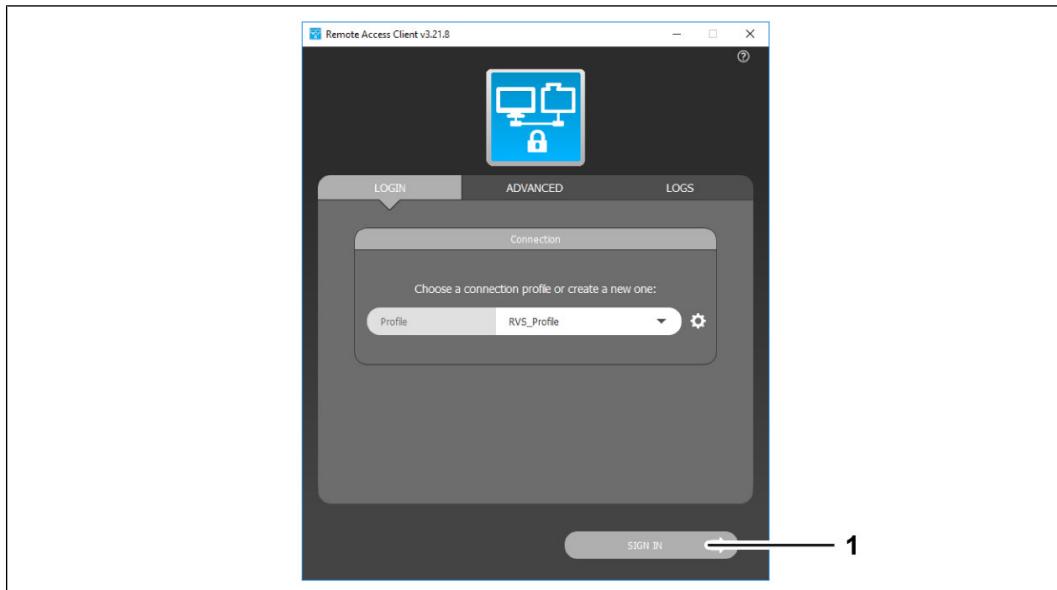


18014398800345099

1. The option **Enable logging** (1) is activated by default.

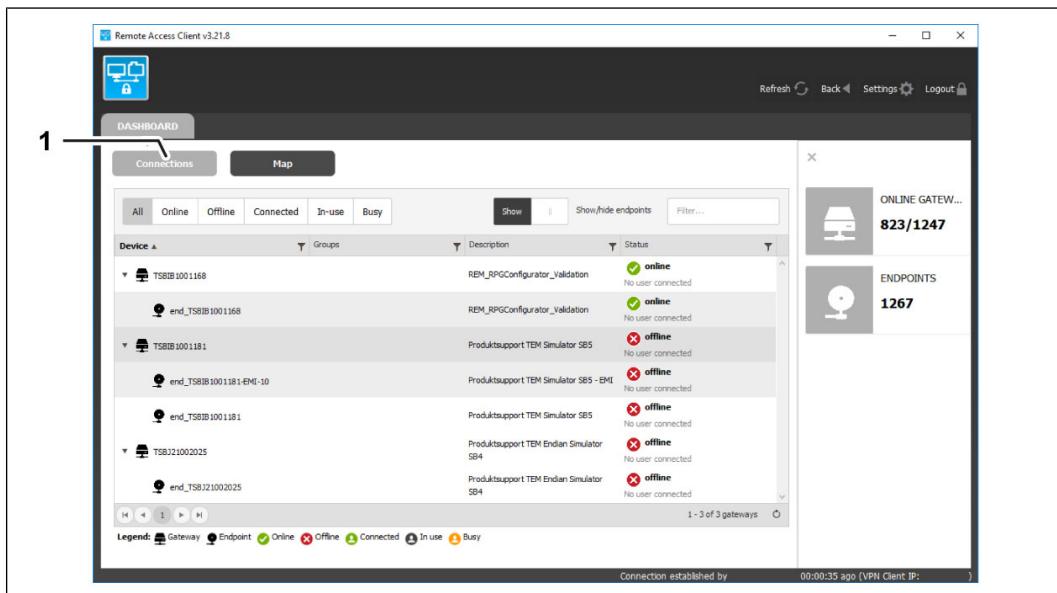
- The option **Verbosity** (2) determines how detailed the log data is. The setting "High" creates the most detailed log data.
- **Copy log to clipboard** (3) copies the log data to the clipboard.
- **Save log to file** (4) saves the log data to a file.
- **Clear log** (5) deletes the log data.

Establishing connection



18014398800362635

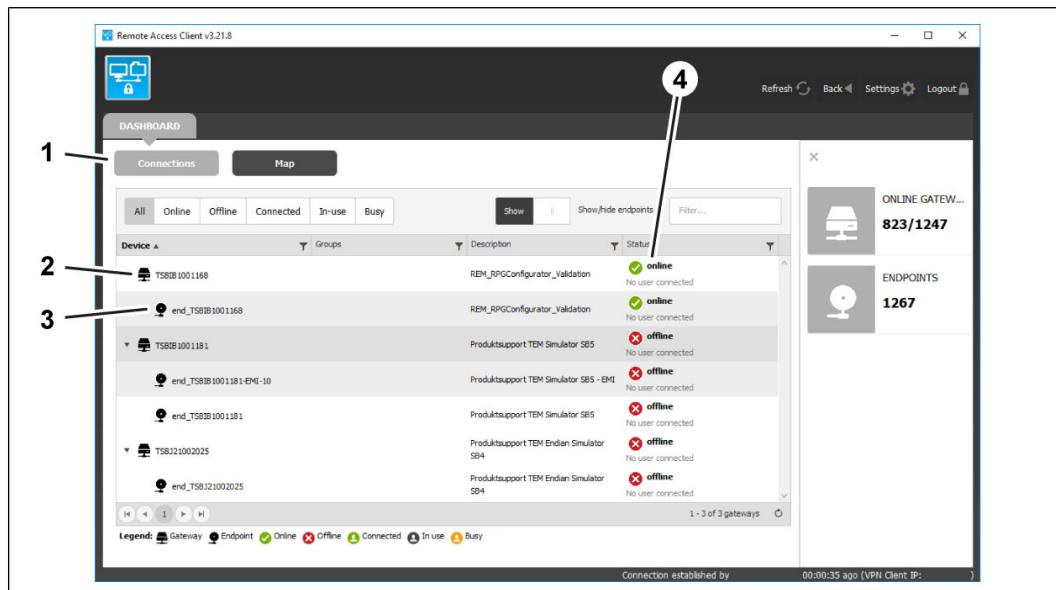
1. Click on **SIGN IN** (1).
 - It may take a moment to connect to the server.
- ⇒ When the connection to the server is established, the following window appears.



18014398800367371

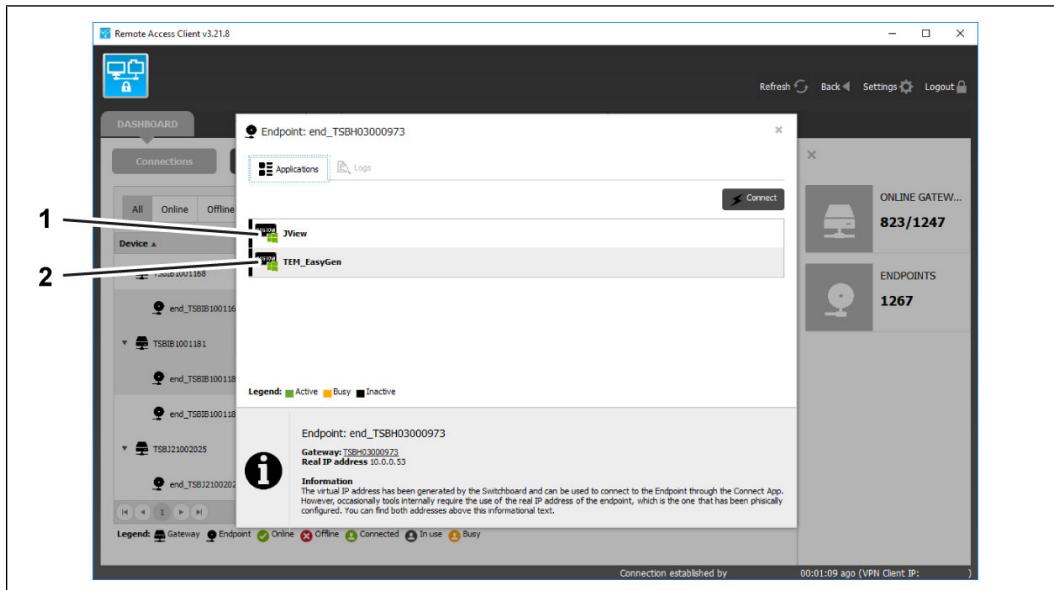
The Remote Access Client shows the plants that you can access in list form by default.

Selecting a plant



18014398800386059

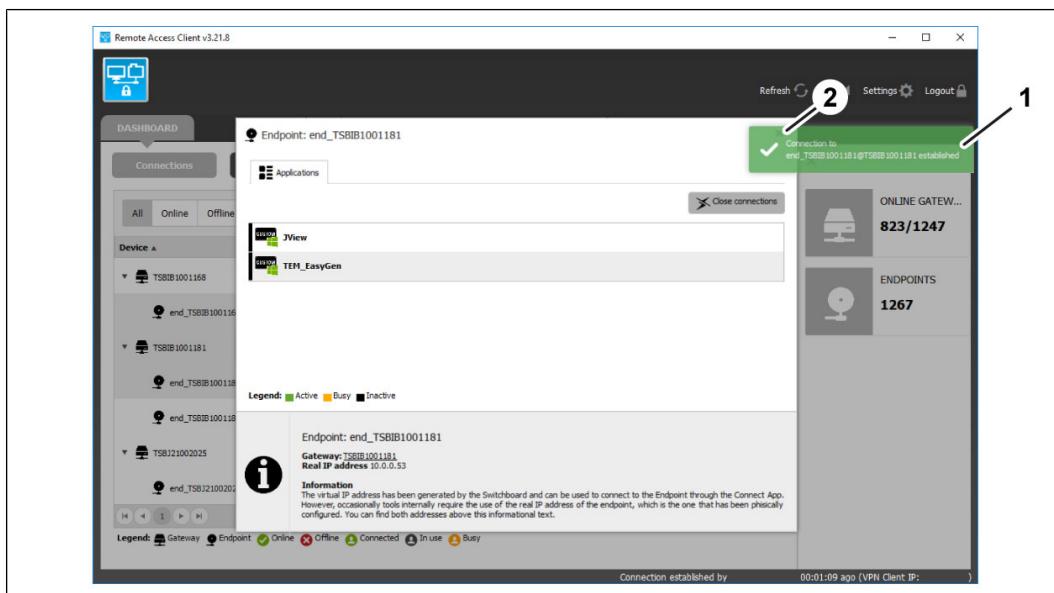
1. Click on the **Connections** button (1) to see a list of available plants.
 - The list contains "Gateways" (2) and "Endpoints" (3). A "gateway" is a router; it provides access to one or more "endpoints". An "endpoint" is usually a genset (more accurately: the control system of a genset).
 - One or more gensets can be connected to a router. The router and its associated gensets combined form a plant.
 - If the plant is a multi-engine plant with an Intelligent Selection Unit IAE, only **one** of the gensets will appear in the list.
 - If "online" and "**No user connected**" appear in the **Status** column (4), you can establish a connection to the plant.
2. Click on the **Endpoint** (3) you would like to connect to.



18014398800390795

3. Click on the **application** you want to use.

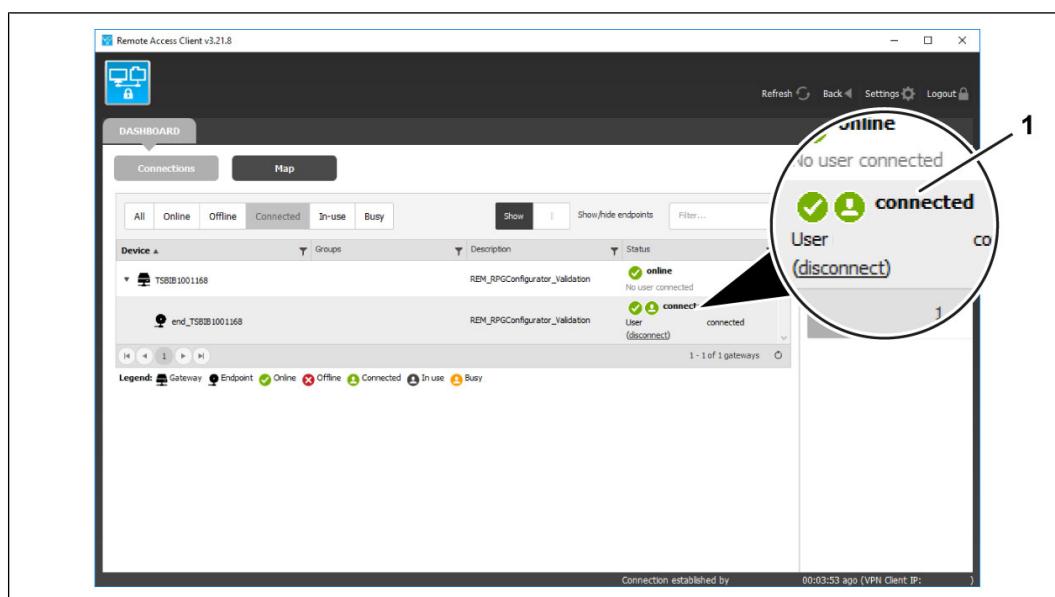
- Click on **TEM_JVIEW** (1) to access the control system TEM Evo with the program **JView**.
- Click on **TEM_EasyGen** (2) to access the TEM MFR (easYgen control device) with the program **Woodward ToolKit**.



18014398800413067

- Once the connection has been created, a brief message (1) appears.

4. Click on **X** (2) to close the window.



18014398800417803

⇒ Once a user is logged in to a plant, the status (1) switches from **online** to **connected**.

Additional steps:

- [Connecting to a plant \[▶ 75\]](#)
- [Connecting to a plant \[▶ 77\]](#)

Using JView

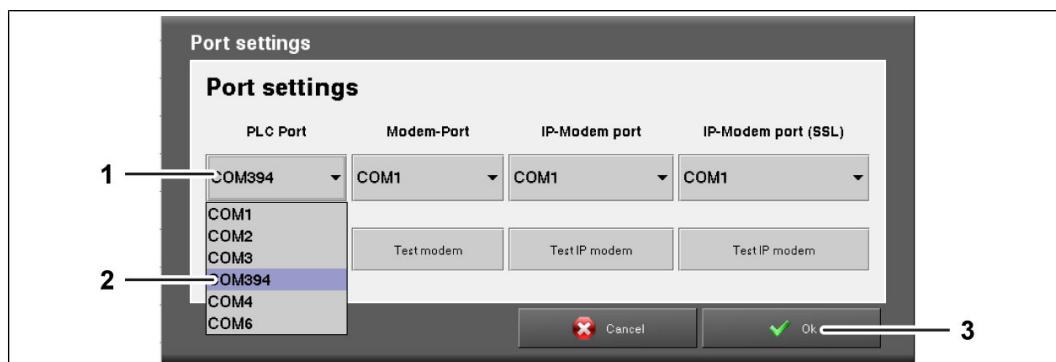
1. Connect the red USB dongle and, if available, the yellow USB dongle to the computer.
2. Start the **JView** program.



290941707

3. Press the button (1) to call up the **System** input screen.

4. Click on the arrow symbol (2) and select the **Visualization** list entry.
5. Click on the **Settings** button (3).
6. Click on the **Port settings** button (4).



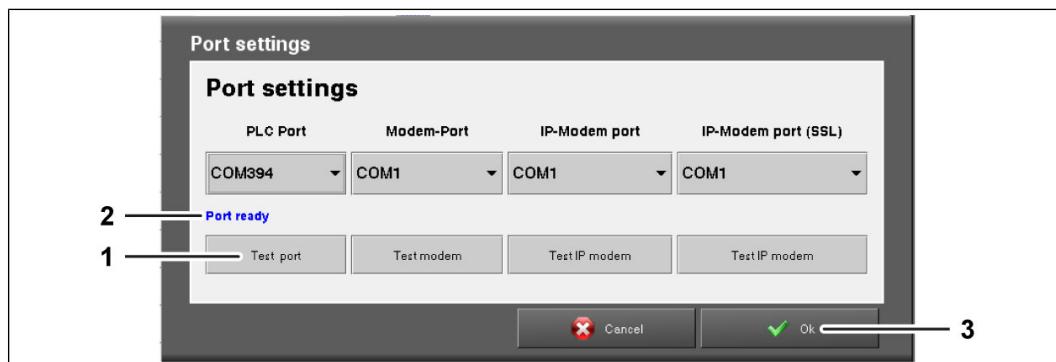
290964491

7. Expand the **PLC Port** combination field (1) and select the **COM394** entry (2).

NOTE

If the **PLC Port** (1) **COM394** (2) is assigned, an error message will appear. Contact Service to have another **PLC Port** enabled.

8. Click on the **OK** button (3).



290982283

9. Click on **Test Port** button (1).
 - If the test was successful, the message **Port ready** (2) will appear above the button (1).
10. Click on the **OK** button (3).

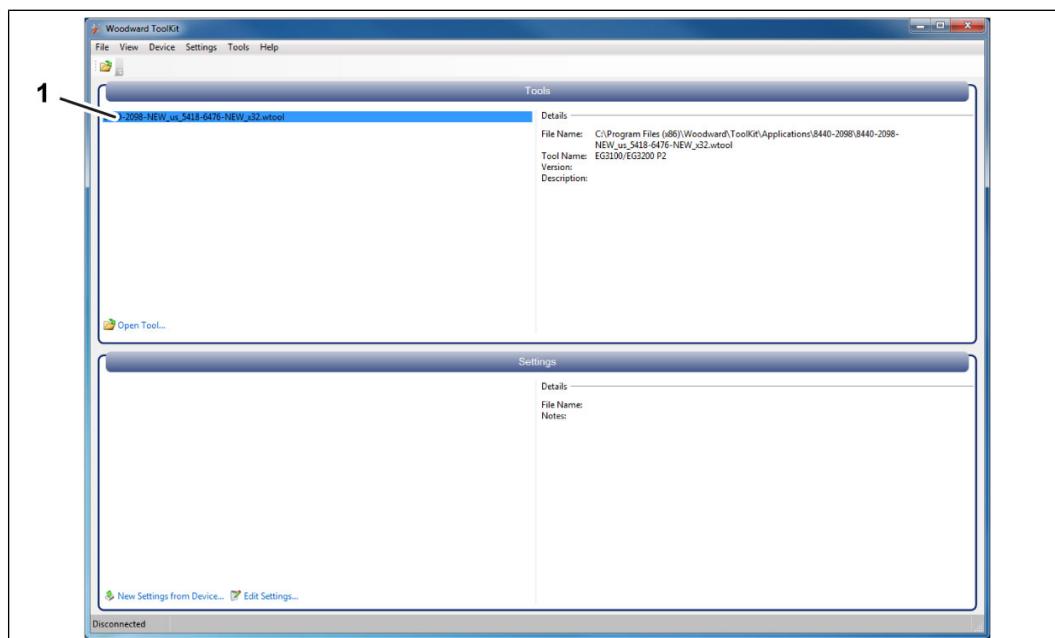


290987275

A green symbol (1) in the status line shows that the connection to the control system is active.

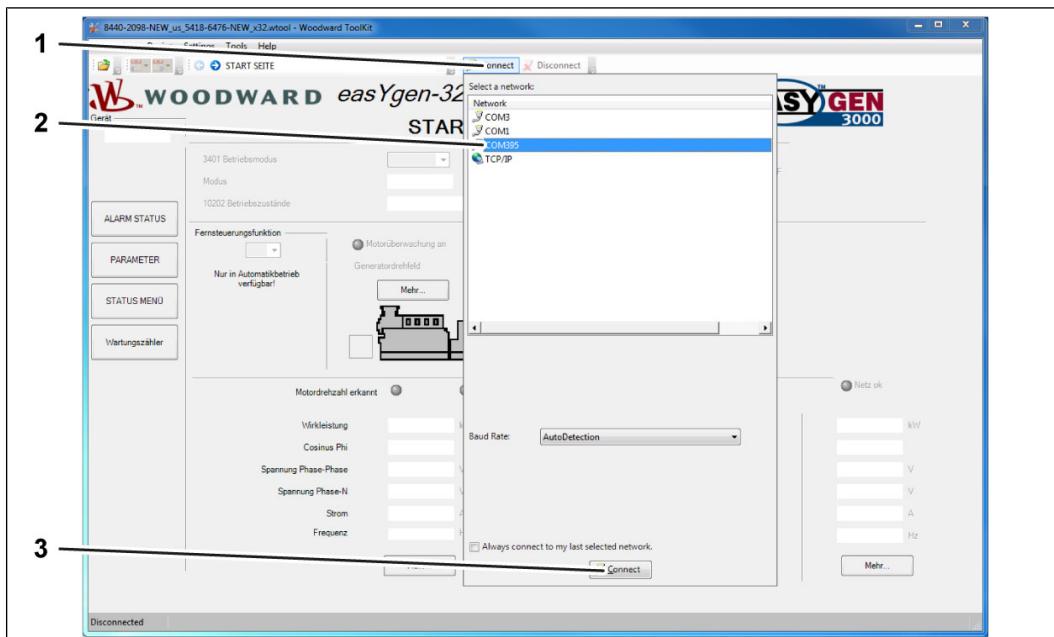
Using Woodward ToolKit

1. Start the program **Woodward ToolKit**.



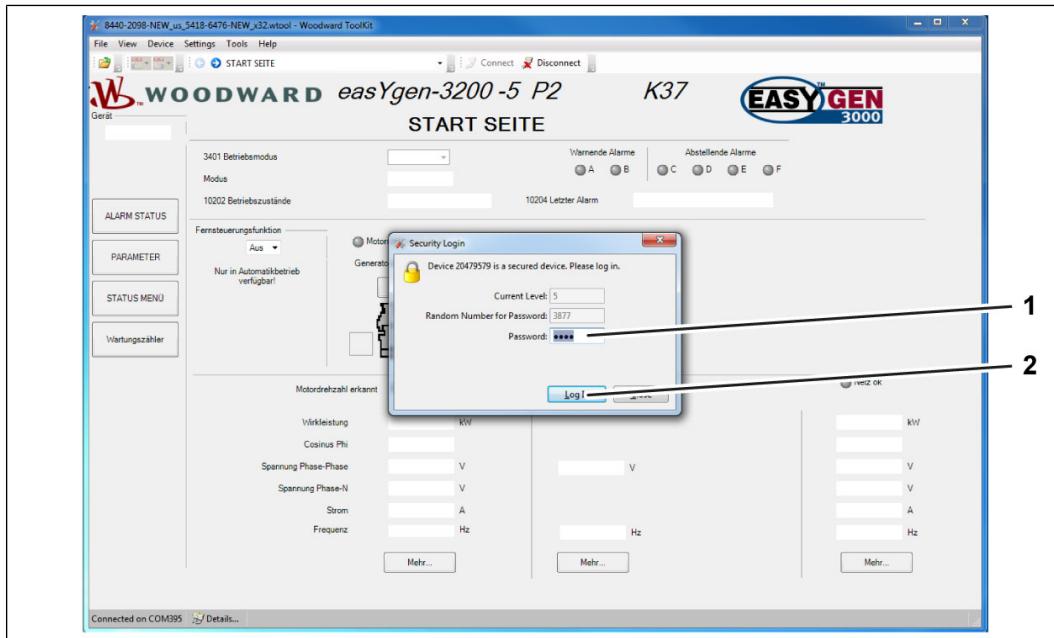
291005195

2. Select the tool (1).



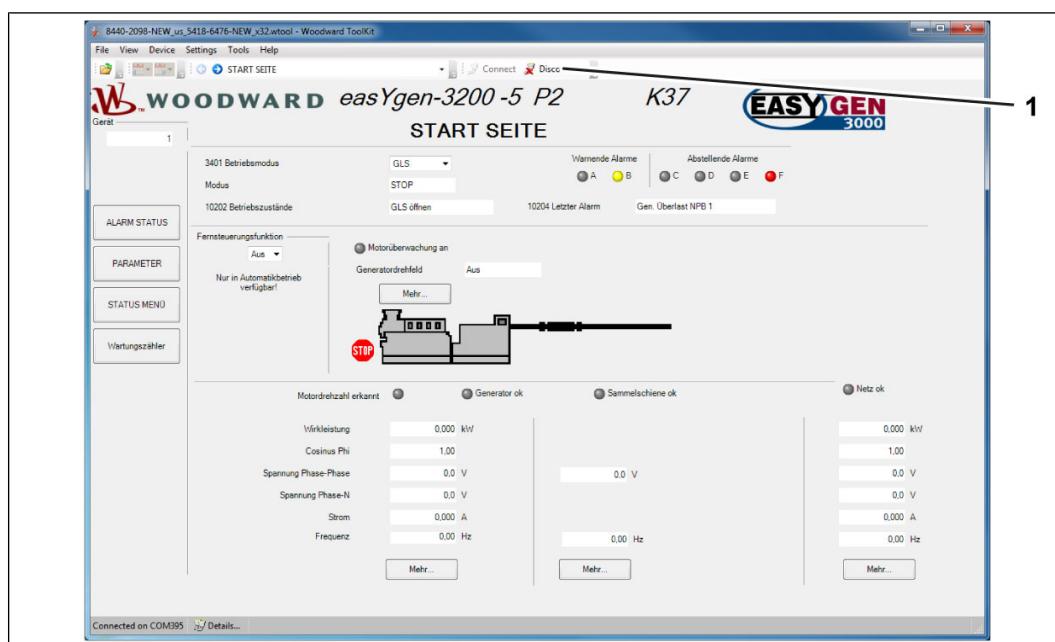
291022987

3. Click on the **Connect** button (1).
4. Click on the list entry **COM395** (2).
5. Click on the **Connect** button (3).



291027979

6. Enter the password in the **Password** field (1).
 - You can find information on the password in the documentation for the easYgen control device (TEM MFR).
7. Click on **Log In** (2).



291032971

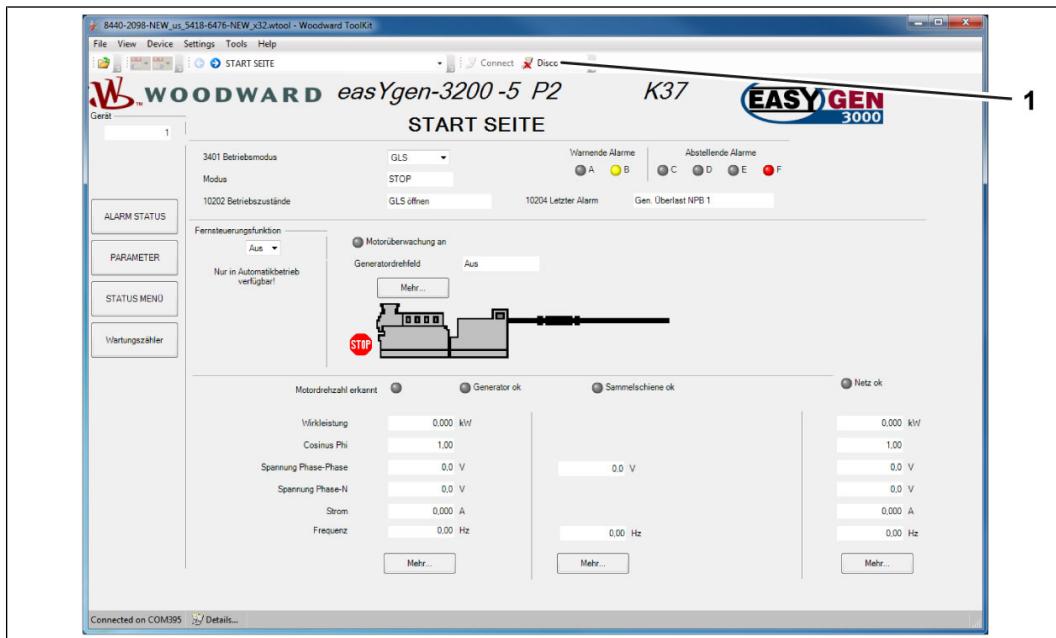
- ⇒ The connection to the easYgen control device (TEM MFR) has been established.

6.3 Closing the connection



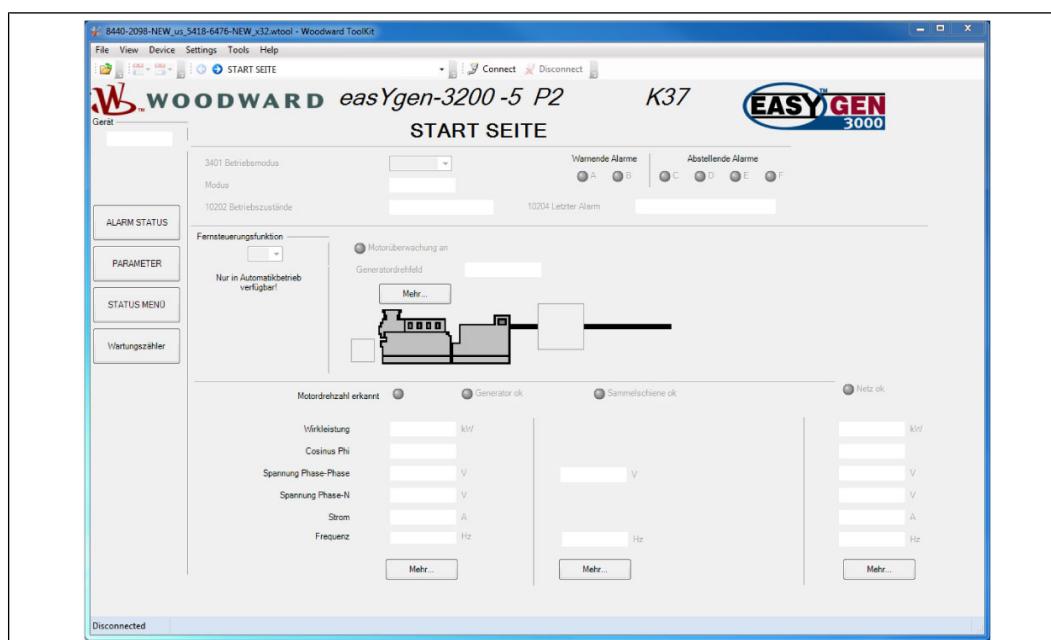
291123083

1. If JVview has been started: Click on the X (1) to close the connection to the control system.



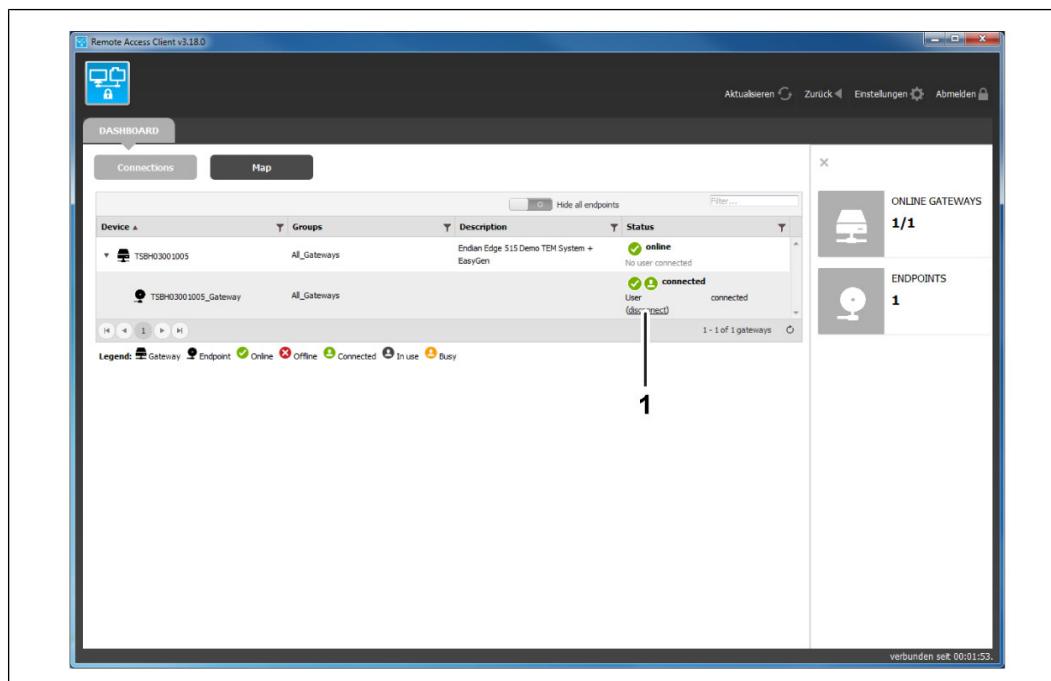
291032971

2. If Woodward ToolKit has been started: Click on **Disconnect** (1) to close the connection to the control device.



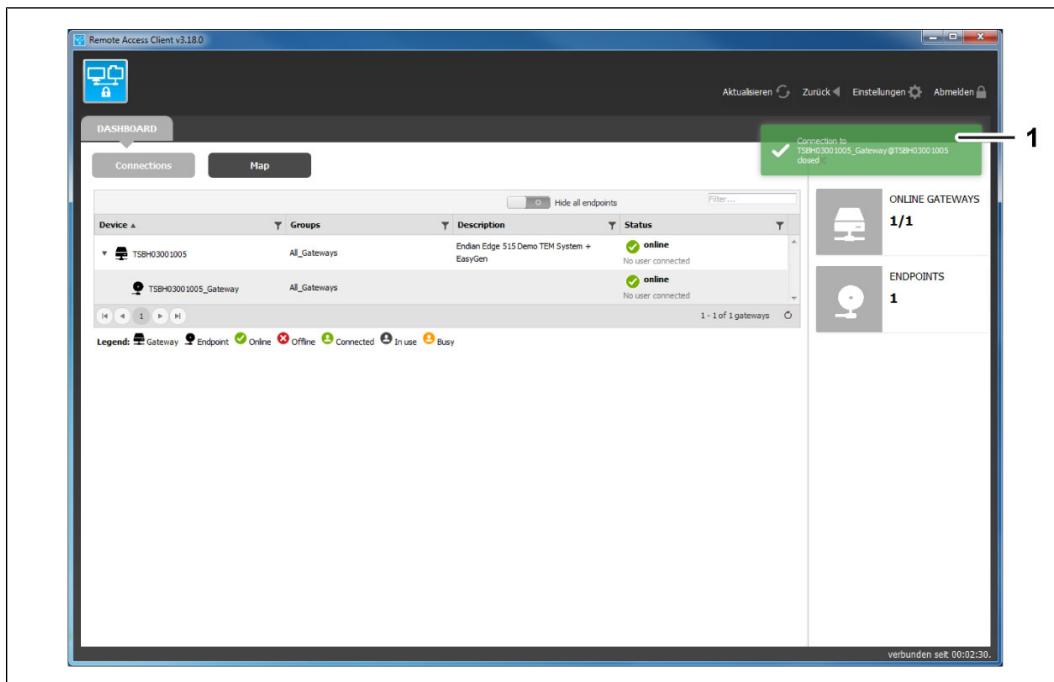
291128075

- The connection to the control device has been closed.



18014398800615051

3. Click on **Disconnect** (1) to close the connection to the plant.



18014398800645387

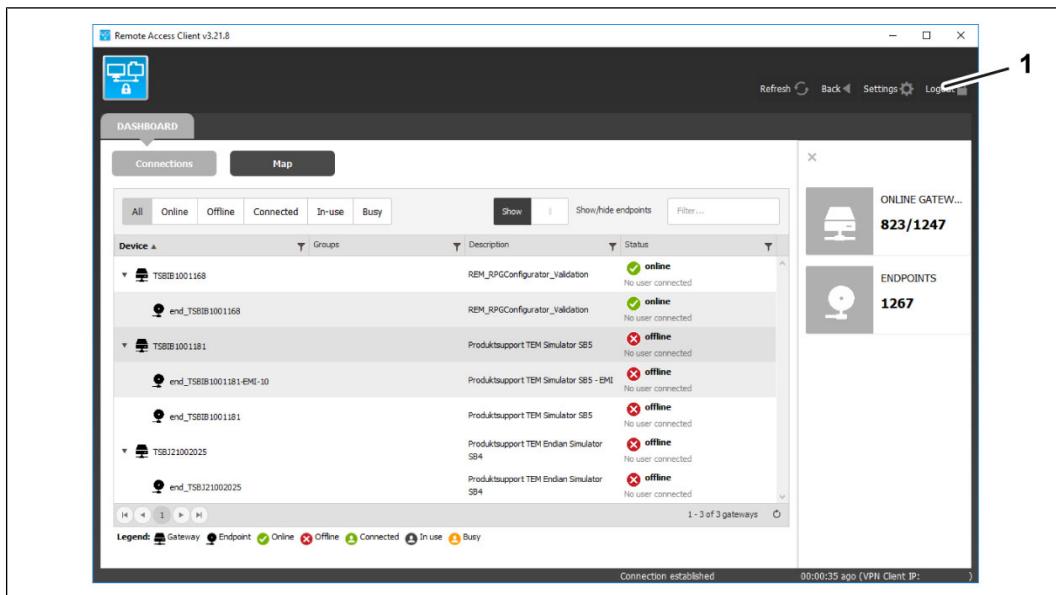
⇒ Once the connection has closed, a brief message (1) appears.

You can now establish a new connection to a plant (► [Connecting to a plant \[▶ 73\]](#)) or close the program (► [Closing Remote Access Client \[▶ 82\]](#)).

6.4

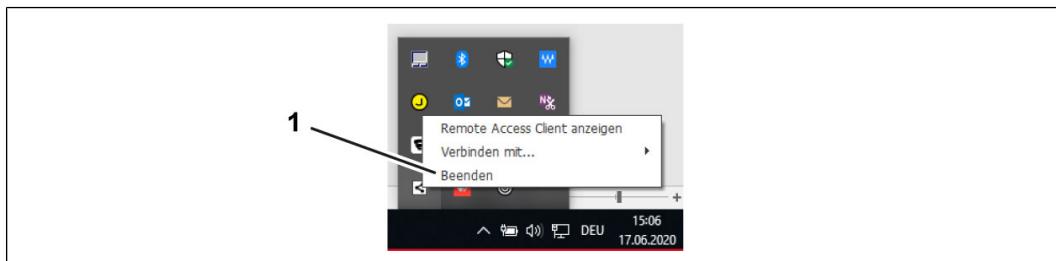
Closing the Remote Access Client

1. If one or more gensets are still connected: Terminate all connections (► [Closing the connection \[▶ 80\]](#)).
 - When someone is connected to the genset's control system via the router, the operating computer on site is locked. The operating computer is only unlocked again once you have closed the connection.
 - It is not possible to launch multiple instances of the Remote Access Client on a computer and establish multiple connections in parallel. If, for example, multiple persons with different user accounts are using the computer that runs the Remote Access Client, each user must fully exit the Remote Access Client before logging off. Otherwise, other users will not be able to establish a connection.



18014398800670091

2. Click on **Logout** (1).
3. In the Windows taskbar notification area, right-click the icon for the Remote Access Client then select "Exit".



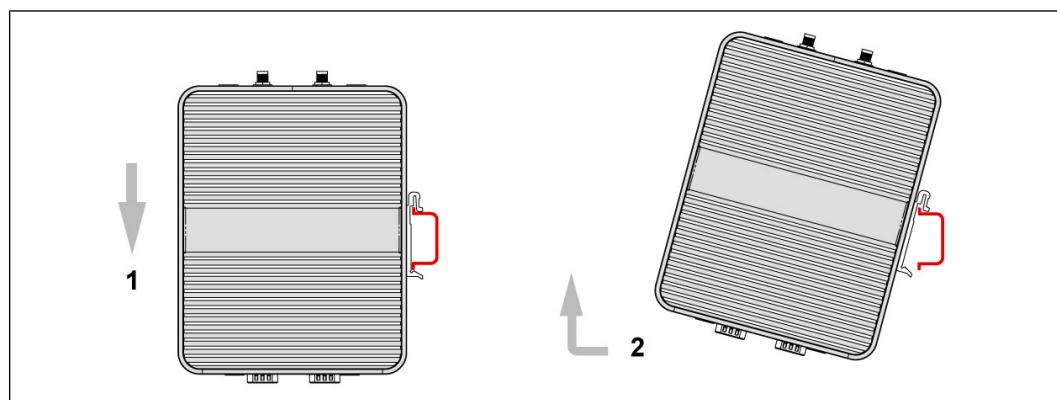
18014398800674827

7 Decommissioning

7.1 Decommissioning Remote Engine Management

If you no longer wish to use the Remote Access Client, proceed as follows, in order to deactivate the router and to dismantle the switchgear cabinet.

1. Disconnect the router from the power supply.
2. Remove all cables that are connected to the router.
3. Remove the router from the mounting rail.



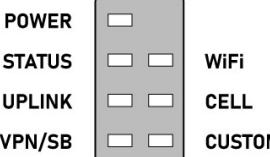
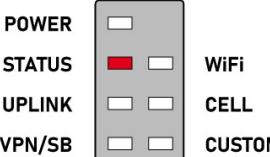
9007199545317387

4. Remove mobile antennae (if applicable).

8 Troubleshooting

8.1 Faults with the router

Fault	Possible cause	Troubleshooting
The router cannot establish a connection to the Rendezvous Server.	The router has no power.	1. Check the power supply.
	The router is defective.	1. Replace the router.
	The VPN connection is incorrectly configured.	1. Configure the VPN connection as described in section Configuring the VPN connection [▶ 47].
	The certificate is invalid.	1. Uninstall the configuration program and then reinstall. 2. Start the configuration program and open the "VPN" tab. 3. Click on the "Update" button.
	Other cause.	1. Start the configuration program and open the "Event Logs" tab. 2. Check the recorded log data for error messages.
The router cannot establish a connection to the Rendezvous Server via the WAN interface.	The cable is not plugged in at the WAN connection on the router or the cable is defective.	1. Check whether the cable is plugged in and in good condition. See section Installing the router in the switch cabinet [▶ 21].
	A proxy server or firewall is blocking the data traffic of the router.	1. Configure the proxy server and/or firewall to allow data traffic to the Rendezvous Server. See section Checking the network settings [▶ 32].
	The router has no static IP address, even though this is required.	1. Assign the router a static IP address. See section Configuring the WAN connection [▶ 42].
	The fixed IP address of the router is already assigned in the network.	1. To change the IP address of the router, see section Configuring the WAN connection [▶ 42].
	For further potential causes, see the fault "The router cannot establish a connection to the Rendezvous Server."	

Fault	Possible cause	Troubleshooting
The router cannot establish a connection to the Rendezvous Server via the mobile network.	The receive signal is too weak. The SIM card is invalid or the prepaid credit has been used up. The SIM card is protected with a PIN. The mobile connection is incorrectly configured. No mobile network (4G, 3G, 2G) is available at the router's location.	<ol style="list-style-type: none"> Move the mobile antenna to a different place. Contact the mobile network operator. <ol style="list-style-type: none"> Check the SIM card. <ol style="list-style-type: none"> Remove PIN protection. The router cannot use SIM cards that are protected with a PIN. <ol style="list-style-type: none"> Configure the mobile connection as described in section Configuring the mobile connection [▶ 44]. <ol style="list-style-type: none"> Use a WAN interface.
The "POWER" LED does not light up.	<p>The power supply is interrupted.</p> 	<ol style="list-style-type: none"> Reconnect the power supply.
	The router is defective.	<ol style="list-style-type: none"> Replace the router.
The "STATUS" LED is flashing red very rapidly.	The operating system of the router is faulty.	<ol style="list-style-type: none"> Contact Cat dealer.
		

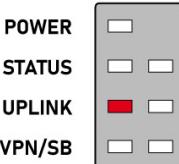
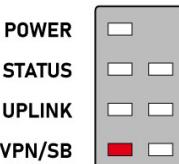
Fault	Possible cause	Troubleshooting
The "UPLINK" LED lights up red. 	The router cannot connect to the internet.	<ol style="list-style-type: none"> Check if the internet connection is correctly configured, see section Configuring the WAN connection [▶ 42]. Check if a firewall is blocking data traffic.
The "VPN/SB" LED lights up red. 	The router cannot establish a VPN connection.	<ol style="list-style-type: none"> Check if the internet connection is correctly configured, see section Configuring the WAN connection [▶ 42]. Check if a firewall is blocking data traffic.

Table 2: Faults with the router

8.2 Faults with the Remote Access Client RAC

Fault	Possible cause	Troubleshooting
The Remote Access Client RAC displays the message Request timed out.	No Internet connection.	<ol style="list-style-type: none"> Check whether the computer that is running the Remote Access Client has access to the Internet.
The message means that the Remote Access Client RAC was unable to establish a connection to the Rendezvous Server RVS.	A proxy server or a firewall is blocking data traffic to the Rendezvous Server.	<ol style="list-style-type: none"> Set the proxy server and/or firewall in such a way as to allow data traffic to the Rendezvous Server.
The Remote Access Client RAC displays the message Server Authentication Failure - please check credentials.	<p>No username and/or password was specified.</p> <p>The specified username and/or password are incorrect.</p>	<ol style="list-style-type: none"> Enter username and password. Check username and password, and correct if necessary.
The Remote Access Client displays a router as offline.	The router cannot establish a connection to the Rendezvous Server.	Troubleshooting information in this table.

Fault	Possible cause	Troubleshooting
Remote Access Client cannot establish a connection to the Rendezvous Server.	The "Virtual Serial Ports Emulator" program from Eter-logic.com is running on the computer.	1. Exit or uninstall Virtual Serial Ports Emulator.
The Remote Access Client cannot establish a connection to the control system TEM Evo.	The operation mode B or C is set on the function selection unit FAE.	1. Set D operation mode.
	Only in case of a multi-engine plant: The modem switch on the IAENT module of the intelligent selection unit (IAE) is in the Off position.	1. Set switch to On position.
	The IP addresses in the local network overlap with the addresses of the VPN and router.	1. Change the IP addresses of the devices in the local network.

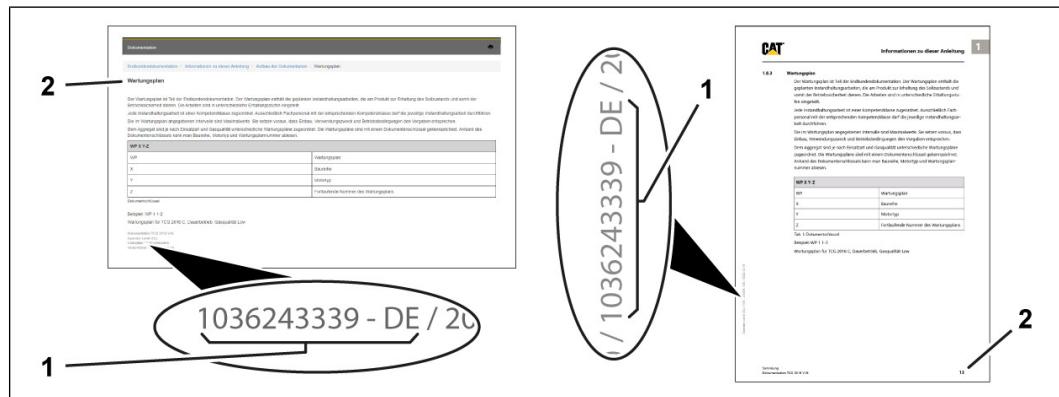
Table 3: Faults when using the Remote Access Client RAC

9 Feedback on documentation

Do you have any praise, criticism or suggestions for improvement for this document?

Send an e-mail to techred@mwm.net.

Describe your request as precisely as possible. So that we can categorize your feedback, please also provide the following information:



9007199541383307: Example document (HTML page in the Service Library on the left, and a PDF page on the right side)

- Document number and language (1)
- Page title or page number (2)
- Contact data (name, email) for potential further enquiries

Thank you for your support. We read all feedback carefully.

We look forward to hearing from you!

