TC CLOUD CLIENT 1002-4G...

COMPLETE line

Cloud client for North American mobile networks (Verizon or AT&T)

Data sheet
107731_en_04

1 Description

The **TC CLOUD CLIENT...** devices are industrial VPN gateways which connect your machines to the mGuard Secure Cloud securely via the Internet. The devices enable access to the cloud via the 4G mobile network.

The devices are optimized for use with the mGuard Secure Cloud. All TC CLOUD CLIENT devices therefore support Virtual Private Networks (VPNs) as standard.

You can configure the devices via the mGuard Secure Cloud. The devices are immediately ready for use in the machine. This enables quick startup in the field and error-free, autonomous operation.

mGuard Secure Cloud

mGuard Secure Cloud constitutes a high-performance and scalable VPN infrastructure in the cloud, which connects service staff with machines and systems via the Internet.

mGuard VPN technology uses the IPsec security protocol with strong encryption. This ensures the confidentiality, authenticity, and integrity of all data transmitted between the service technicians and the machines.

Features

- Secure communication via IPsec
- Configuration via web-based management or microSD card
- Two local Ethernet connections
- Switching input and switching output
- Cloud-based VPN infrastructure from Phoenix Contact
- Turnkey VPN infrastructure for operators, machine builders, and systems manufacturers
- Secure and reliable, thanks to industry-proven mGuard security technology
- Support for mobile, iOS-based devices, such as Apple iPads and iPhones

The devices are intended for use in the USA.
Please also refer to “6 Countries of use”.

Make sure you always use the latest documentation.

2 Table of contents

3 Ordering data

Description	Type	Order No.	Pcs./Pkt.
Industrial VPN gateway for mGuard Secure Cloud, 2 Ethernet interfaces, cloud communication via 4G LTE, Verizon wireless (US), IPsec support, NAT, 1 digital input, 1 digital output	TC CLOUD CLIENT 1002-4G VZW	2702887	1
Industrial VPN gateway for mGuard Secure Cloud, 2 Ethernet interfaces, cloud communication via 4G LTE, AT&T (US), IPsec support, NAT, 1 digital input, 1 digital output	TC CLOUD CLIENT 1002-4G ATT	2702888	1

Accessories	Type	Order No.	Pcs./Pkt.
Primary-switched TRIO POWER power supply with push-in connection for DIN rail mounting, input: 1-phase, output: 24 V DC/3 A C2LPS	TRIO-PS-2G/1AC/24DC/3/C2LPS	2903147	1
PCB connector, nominal current: 8 A, number of positions: 5, pitch: 3.81 mm, connection method: Push-in spring connection, color: light gray, contact surface: tin	FK-MCP 1,5/ 5-ST-3,81GY35BD-D0	1105116	50
Attachment plug with Lambda/4 technology as surge protection for coaxial signal interfaces Connection: Male/female SMA connectors	CSMA-LAMBDA/4-2.0-BS-SET	2800491	1
Mobile network antenna cable, 5 m in length, SMA (male) -> SMA (female), 50 ohm impedance	PSI-CAB-GSM/UMTS- 5M	2900980	1
Mobile network antenna cable, 10 m in length, SMA (male) -> SMA (female), 50 ohm impedance	PSI-CAB-GSM/UMTS-10M	2900981	1
Multiband mobile communication antenna for wall mounting, 0.5 m antenna cable, with SMA circular connector, suitable for LTE/4G	TC ANT MOBILE WALL 0,5M	2702274	1

Operation of the wireless system is only permitted when using accessories available from Phoenix Contact. The use of any other components can lead to the withdrawal of the operating license.

4 Technical data

Supply	
Supply voltage range	10 V DC ... 30 V DC (SELV)
Typical current consumption	< 200 mA (24 V DC) 65 mA (with activated energy-saving mode)
Electrical isolation	VCC // LTE // Ethernet // PE
Conductor cross section	0.14 mm² ... 1.50 mm² (26 AWG ... 16 AWG)

Use copper wires rated 85 °C.

Functions	
Management	Web-based management, SNMP
Number of VPN tunnels	1
1:1 Network Address Translation (NAT) in the VPN	Supported
Encryption methods	3DES, AES-128, -192, -256
Internet Protocol Security (IPsec) mode	ESP tunnel
Authentication	X.509v3, PSK
Data integrity	MD5, SHA-1
Dead peer detection (DPD)	RFC 3706

Ethernet interface, 10/100Base-T(X) in acc. with IEEE 802.3u	
Number of ports	2 (SELV)
Connection method	RJ45 socket, shielded
Serial transmission speed	10/100 Mbps, auto negotiation
Transmission length	100 m (shielded twisted pair)
Protocols supported	TCP/IP, UDP/IP, FTP, HTTP
Auxiliary protocols	ARP, DHCP, PING (ICMP), SNMP V1, SMTP

Wireless interface	TC CLOUD CLIENT 1002-4G VZW	TC CLOUD CLIENT 1002-4G ATT
Interface description	LTE (FDD)	LTE (FDD) / UMTS
Frequency	700 MHz (LTE B13) 1700 MHz (LTE B4)	850 MHz (UMTS/HSPA B5) 1900 MHz (UMTS/HSPA B2) 700 MHz (LTE B13 / B17) 850 MHz (LTE B5) 1700 MHz (LTE B4) 1900 MHz (LTE B2)
Data rate	≤ 150 Mbps (LTE (DL)) ≤ 50 Mbps (LTE (UL))	≤ 150 Mbps (LTE (DL)) ≤ 50 Mbps (LTE (UL))
Antenna	50 Ω impedance SMA antenna socket	50 Ω impedance SMA antenna socket
SIM Interface	1.8 volt, 3 volt	1.8 volt, 3 volt
UMTS		HSPA 3GPP R9
LTE	CAT4	CAT4

Digital input	
Number of inputs	1
Input signal, Voltage	10 V DC ... 30 V DC
Switching level "1" signal	10 V DC ... 30 V DC
Digital output	
Number of outputs	1 (resistive load)
Output signal, Voltage	10 V DC ... 30 V DC (depending on the operating voltage)
Output signal, Current	≤ 50 mA (not short-circuit proof)
General data	
Degree of protection	IP20 (manufacturer's declaration)
Degree of pollution	2 (indoor use only)
Dimensions (W/H/D)	45 mm x 130 mm x 126 mm
Housing material	Plastic gray
Vibration resistance in acc. with EN 60068-2-6/ IEC 60068-2-6	5g, 10...150 Hz, 2.5 h, in XYZ direction
Shock in acc. with EN 60068-2-27/IEC 60068-2-27	15g
MTTF (mean time to failure) SN 29500 standard, temperature 25 °C, operating cycle 21 % (5 days a week, 8 hours a day)	383 Years
MTTF (mean time to failure) SN 29500 standard, temperature 40 °C, operating cycle 34.25 % (5 days a week, 12 hours a day)	184 Years
MTTF (mean time to failure) SN 29500 standard, temperature 40 °C, operating cycle 100 % (7 days a week, 24 hours a day)	78 Years
Noise immunity according to	EN 61000-6-2
Electromagnetic compatibility	Conformance with EMC Directive 2014/30/EU
Ambient conditions	
Ambient temperature (operation)	0 °C ... 60 °C
Ambient temperature (storage/transport)	0 °C ... 60 °C
Permissible humidity (operation)	10 % ... 95 % (non-condensing)
Permissible humidity (storage/transport)	10 % ... 95 % (non-condensing)
Approvals / Certificates	
UL, USA/Canada	Class I, Zone 2, AEx nA IIC T4 / Ex nA IIC T4 Gc Class I, Div. 2, Groups A, B, C, D T4
Noxious gas test	ISA-S71.04-1985 G3 Harsh Group A

Conformance with EMC Directive 2014/30/EU		
Noise immunity according to EN 61000-6-2		
Electrostatic discharge	EN 61000-4-2	
	Contact discharge	± 6 kV (Test Level 3)
	Discharge in air	± 8 kV (Test Level 3)
	Comments	Criterion B
Electromagnetic HF field	EN 61000-4-3	
	Frequency range	80 MHz ... 3 GHz (Test Level 3)
	Field intensity	10 V/m
	Comments	Criterion A
Fast transients (burst)	EN 61000-4-4	
	Input	± 2 kV (Test Level 3)
	Signal	± 2 kV (Ethernet)
	Comments	Criterion B
Surge current loads (surge)	EN 61000-4-5	
	Input	± 0.5 kV (symmetrical) ± 1 kV (asymmetrical)
	Signal	± 1 kV (Data line, asymmetrical)
	Comments	Criterion B
Conducted interference	EN 61000-4-6	
	Frequency range	0.15 MHz ... 80 MHz
	Voltage	10 V
	Comments	Criterion A

Emitted interference in acc. with EN 61000-6-4	
Radio interference voltage in acc. with EN 55011	Class B, area of application: Industry and residential
Emitted radio interference in acc. with EN 55011	Class B, area of application: Industry and residential

Criterion A	Normal operating behavior within the specified limits
Criterion B	Temporary impairment of operating behavior that is corrected by the device itself

Conformance with RED Directive 2014/53/EU	
EMC - immunity to interference (electromagnetic compatibility of wireless systems)	EN 61000-6-2 Generic standard for the industrial sector
Safety - protection of personnel with regard to electrical safety	EN 60950
Health - limitation of exposure of the population to electromagnetic fields	EC Gazette 1999/519/EC EC Council recommendation of July 12, 1999
Radio - effective use of the frequency spectrum and prevention of radio interference	DIN EN 301511

5 Safety notes

5.1 Intended use

Installation is only permitted in countries that allow the operation of wireless devices in this frequency band and supply range.

The devices are only for export outside of the European Economic Area.

5.2 Safety notes

CAUTION:

Observe the following safety notes when using the device.

- Installation, operation, and maintenance may only be carried out by qualified electricians. Follow the installation instructions as described.
- When installing and operating the device, the applicable regulations and safety directives (including national safety directives), as well as general technical regulations, must be observed. The technical data is provided in the package slip and on the certificates (conformity assessment, additional approvals where applicable).
- The device must not be opened or modified. Do not repair the device yourself, replace it with an equivalent device. Repairs may only be carried out by the manufacturer. The manufacturer is not liable for damage resulting from violation.
- The IP20 protection (IEC 60529/EN 60529) of the device is intended for use in a clean and dry environment. The device must not be subject to mechanical strain and/or thermal loads, which exceed the limits described.
- The device is designed exclusively for SELV operation according to IEC 60950-1/EN 60950-1/VDE 0805. The device may only be connected to devices, which meet the requirements of EN 60950-1.
- The device complies with the EMC regulations for industrial areas (EMC class A). When using the device in residential areas, it may cause radio interference.
- Operation of the wireless system is only permitted when using accessories available from Phoenix Contact. The use of any other components can lead to the withdrawal of the operating license.
- You will find the approved accessories for this wireless system listed with the product

5.3 UL warning instructions

WARNING: Explosion hazard when used in potentially explosive areas

Please make sure that the following notes and instructions are observed.

- Use copper wires rated 85°C.
- If the equipment is used in a manner not specified, the protection provided by the equipment may be impaired.
- This device has to be built in an enclosure (control box).
- External circuit from SELV supplied
- SELV - Limited energy according to UL/IEC/EN 61010-1 or NEC class II
- This equipment must be mounted in an enclosure certified for use in Class I, Zone 2 minimum and rated IP54 minimum in accordance with IEC 60529 when used in Class I, Zone 2 environment.
- Device shall only be used in an area of not more than pollution degree 2.

c UL us LISTED
IND.CONT.EQ.
FOR.HAZ.LOC.
E366272

Class I, Zone 2, AEx nA IIC T4 / Ex nA IIC T4 Gc
Class I, Division 2, Groups A, B, C and D T4
Input: 10 - 30 V DC, max. 1.7 A ⎓
Amb. Temp. Range: -40°C < Tamb < 70°C

6 Countries of use

USA

The TC CLOUD CLIENT 1002-4G VZW/ATT devices are intended for use in the US 4G mobile networks of Verizon and AT&T.

Europe

The TC CLOUD CLIENT 1002-4G VZW/ATT devices are only for export outside of the European Economic Area.

Use the following devices in Europe:

– TC CLOUD CLIENT 1002-4G, 2702886

Only these devices have all the necessary approvals for use in Europe.

Other countries

If the required general conditions are met, the US devices may be used in other countries.

For an initial idea of which frequency bands are available in your country of use, visit www.frequencycheck.com.

- Verify with your provider whether one of the following frequency bands is available:

TC CLOUD CLIENT 1002-4G VZW
  – LTE, CAT4, B4
  – LTE, CAT4, B13

TC CLOUD CLIENT 1002-4G ATT
  – LTE, CAT4, B2
  – LTE, CAT4, B4
  – LTE, CAT4, B5
  – LTE, CAT4, B13
  – LTE, CAT4, B17

- Verify with your provider whether there is network coverage at the installation location.
- Verify with your provider whether the device is approved for operation at the installation location.

7 Product description

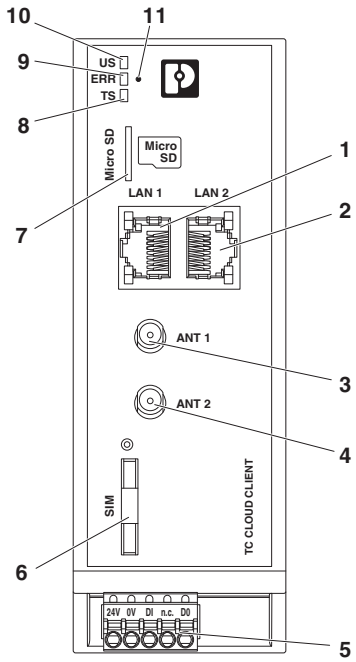

Figure 1 Function elements

1 LAN interface 1
2 LAN interface 2
3 SMA antenna connection 1, primary antenna
4 SMA antenna connection 2, secondary antenna
5 Pluggable Push-in terminal block
6 SIM interface
7 Slot for micro SD card
8 TS-LED
9 ERR-LED
10 US-LED
11 Reset button

Status and diagnostics indicators

U_S	Power	Green
	On	Supply voltage present
ERR	Error	Red
	Off	Registered on the network
	Flashing	SIM card not inserted, SIM error (e.g. PIN or PUK locked)
	On	Searching for cellular network
TS	Teleservice	Yellow
	On	The teleservice connection (VPN) to the mGuard Secure Cloud is established.

Reset button

The reset button can be used to reset the device to the default settings.

IP address:	https://192.168.0.1
Subnet mask:	255.255.255.0
User name:	admin
Password:	admin

- Press and hold down the reset button.
- Disconnect the Ethernet cable from the LAN connection.
- Reconnect the Ethernet cable to the LAN connection.
- Press and hold down the reset button for a further five seconds.

8 Transport and unpacking

- Check the delivery for visible damage caused by transportation.
- Submit claims for any transport damage immediately. Inform Phoenix Contact or your supplier as well as the shipping company without delay.
- Read the complete packing slip carefully.
- Retain the packing slip.
- Keep the packaging for a possible later transport.

9 Mounting

NOTE: device damage

Only mount and remove devices when the power supply is disconnected.

9.1 Mounting on a DIN rail

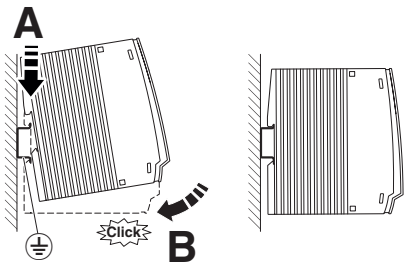

Figure 2 Mounting

The device is intended for installation in a control cabinet.

- To avoid contact resistance, only use clean, corrosion-free 35 mm DIN rails according to DIN EN 60715.
- Place the device onto the DIN rail from above. Push the module from the front toward the mounting surface until it audibly engages.
- Connect the DIN rail to protective earth ground (⏚).

9.2 Removal

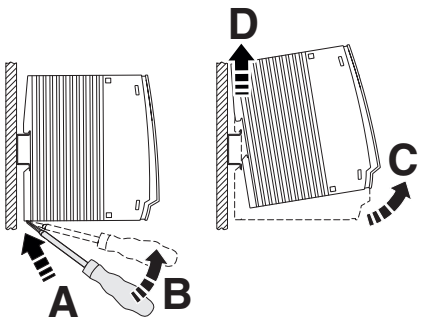

Figure 3 Removal

- Push down the locking tab with a screwdriver, needle-nose pliers or similar.
- Slightly pull the bottom edge of the device away from the mounting surface.
- Pull the device away from the DIN rail.

10 Connecting the cables

10.1 Power supply voltage

CAUTION: Electric shock

The device is only intended for operation with SELV according to IEC 60950/EN 60950/ VDE 0805.

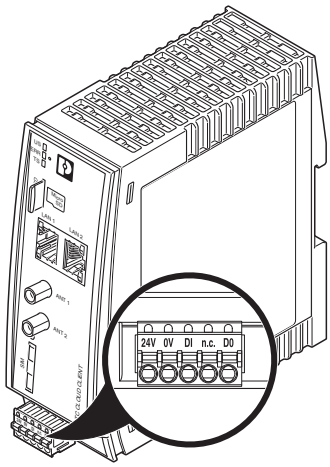

Figure 4 Connecting the supply voltage

- Connect the supply voltage to the push-in terminal block at 24 V and 0 V. Observe the polarity.

10.2 Twisted pair interface (TP port)

- Only twisted pair cables with an impedance of 100 Ω can be connected to the RJ45 Ethernet interfaces.
- Only use shielded twisted pair cables and matching shielded RJ45 connectors.
- Insert the Ethernet cable with the RJ45 plug into the TP interface until the plug engages audibly. Observe the plug keying.

10.3 Switching input and switching output

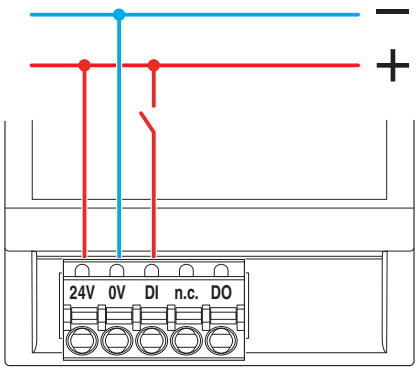

Figure 5 Switching input and switching output

- To start the VPN connection, you can connect to the switching input 10 ... 30 V DC.
- Switching output DO is designed for a maximum of 50 mA at 10 ... 30 V DC. This is how a VPN connection can be signalled.
- The connection cables for the switching input and the switching output must not be longer than 30 meters.
- You must connect the 0 V potential of the switching inputs and outputs to the "0 V" terminal of the voltage supply connection.

10.4 Antennas

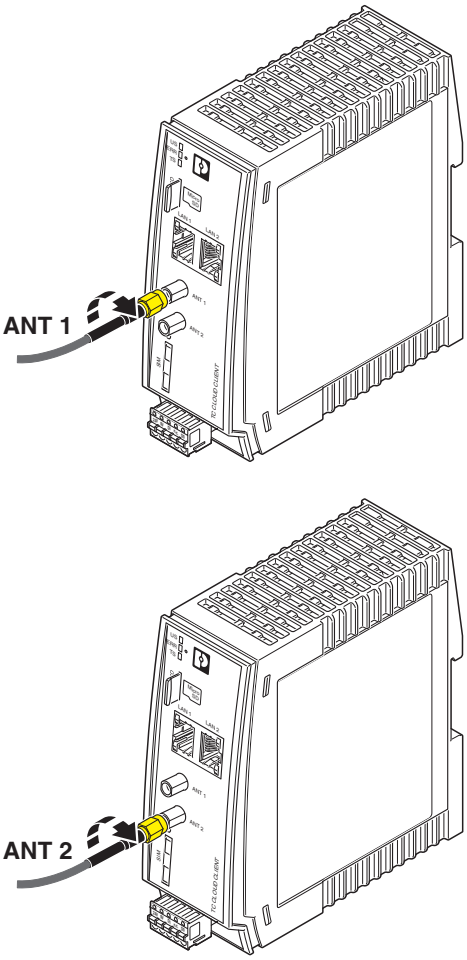

Figure 6 Connect the antenna

- To achieve optimum reception, connect two suitable antennas to the antenna connections.
- The antenna cable must not be longer than 5 meters.
- Fix the antenna in place when reception is good or very good.

11 Insert the SIM card

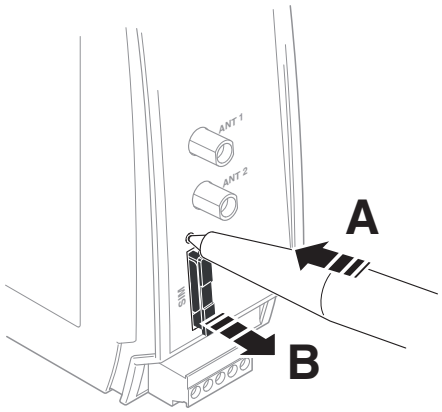

Figure 7 Remove SIM card holder

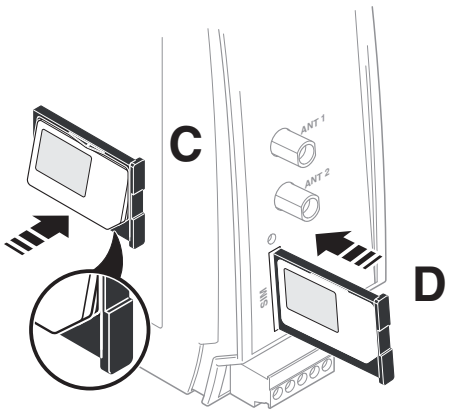

Figure 8 Insert the SIM card

You will receive a SIM card from the provider on which all data and services for your connection are stored.

- Push the yellow release button with a pointed object.
- Remove the SIM card holder.
- Insert the SIM card so that the SIM chip remains visible.
- Insert the SIM card holder together with the SIM card into the device until this ends flush with the housing.

12 Configuration and startup

- Log on to the mGuard Secure Cloud (start.cloud.mguard.com).
- Connect the configuration computer to one of the LAN ports.
- Now establish the connection via the following IP address: https://192.168.0.1 (subnet: 255.255.255.0).

Configure the device in the mGuard Secure Cloud.

Figure 9 Login window

This page protects the area in web-based management where settings are modified. To log into the device, click on “Login”.

– User name: admin
– Password: admin

12.1 Device status (Device information)

You can also access this page with the user login. The page displays information about the hardware, software, and device status.

Hardware

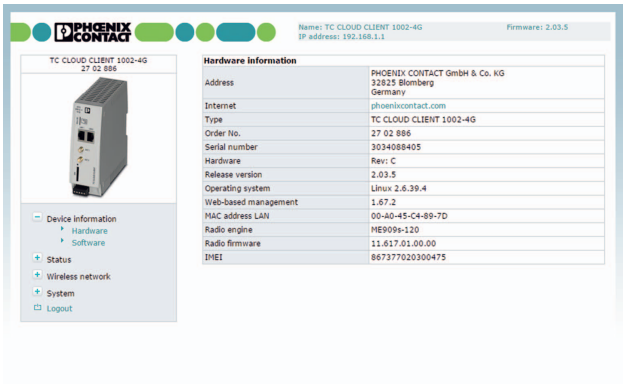

Figure 10 Device information, Hardware

Device information, Hardware	
Address	Address of the manufacturer
Internet	Website address of the manufacturer
Type	Product designation
Order No.	Order No.
Serial number	Serial number
Hardware	Hardware version
Release version	Release version of the software
Operating system	Operating system version
Web-based management	Web-based management version
MAC address LAN	MAC address for unique identification of an Ethernet device in a computer network
Radio engine	Radio engine used
Radio firmware	Firmware version of the radio engine
IMEI	International Mobile Station Equipment Identity, 15-digit serial number that is used to clearly identify each mobile network device

12.2 Status

Radio

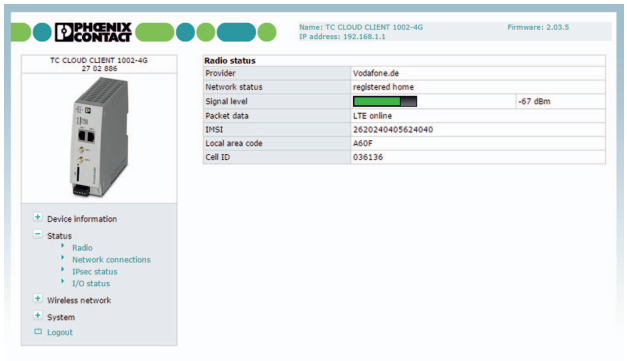

Figure 11 Status, Radio

Status, Radio	
Provider	Name of the provider
Network status	Status of the mobile network
	Registered home: logged into the provider's home network
	Roaming: dial-in via an external mobile network
	Waiting for PIN: enter the PIN.
	Waiting for PUK: SIM card locked because an incorrect PIN was entered three times, PUK entry required
	Wrong PIN: wrong PIN stored in device
	No SIM card: SIM card not inserted
	Busy: radio engine starting
	Power off: radio engine switched off
Signal level	Signal strength as a dBm value and bar
Packet data	**Offline:** no packet data connection in the mobile network
	UMTS online: active packet data connection in the 3G mobile network via UMTS
	HSDPA/UPA online: active packet data connection in the 3G mobile network via HSDPA/UPA HSDPA/UPA is a further development of the UMTS network with a higher data transmission speed.
	LTE online: active high-speed packet connection in the 4G mobile network via LTE
IMSI	International Mobile Subscriber Identity, number used to clearly identify the user of a network
Local area code	Area code in the mobile network
Cell ID	Unique mobile phone cell ID

Network connections

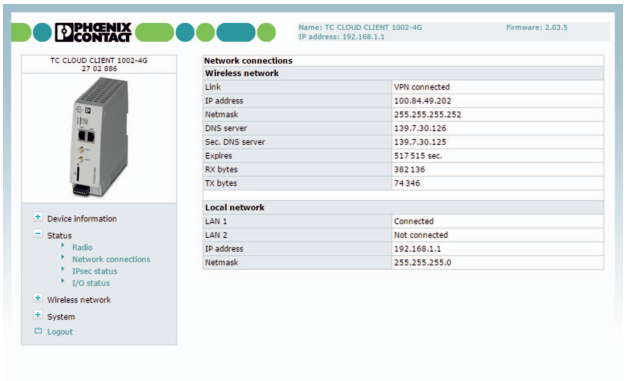

Figure 12 Status, Network connections

Status, Network connections	
Wireless network	
Link	**TCP/IP connected:** active packet data connection in the mobile network You can transmit data via TCP/IP.
	VPN connected: active VPN connection in the mobile network You can transmit encrypted data.
	Not connected: no packet data connection in the mobile network, no data transmission
IP address	IP address assigned by the provider
Netmask	Netmask assigned by the provider
DNS server	IP address of the DNS server
Sec. DNS server	IP address of the alternative DNS server
Expires	Time after which the IP settings assigned by the provider expire (IP address, netmask, DNS server)
RX bytes	Sum of data received since last login to the mobile network
TX bytes	Sum of data sent since last login to the mobile network
Local network	
LAN 1/2	**Connected:** LAN 1/2 connected **Not connected:** LAN 1/2 not connected
IP address	Current IP address
Netmask	Netmask of the local Ethernet network

VPN connection (IPsec status)

Figure 13 Status, IPsec status

Status, IPsec status	
Active IPsec connections	Status of the active teleservice connection (VPN)

I/O status

This page shows current status information and the configuration of the inputs and outputs.

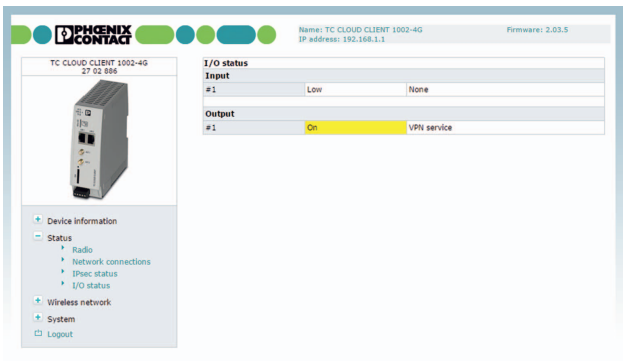

Figure 14 Status, I/O status

12.3 Wireless network

Radio setup

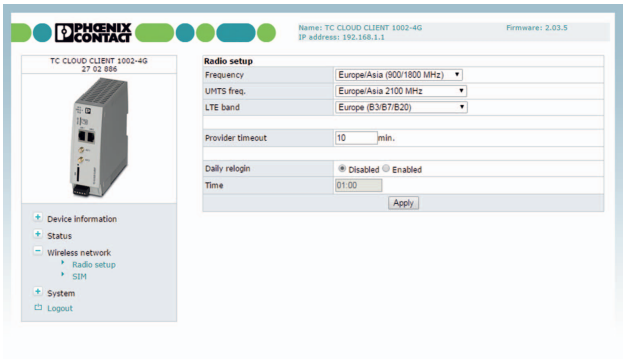

Figure 15 Wireless network, Radio setup

Wireless network, Radio setup	
UMTS freq.	UMTS frequency range in which the device should operate In addition, you can deactivate UMTS: “UMTS off”
LTE band	LTE frequency band in which the device should operate In addition, you can deactivate LTE: “LTE off”
Provider timeout	Period of time after which the radio engine restarts in the event of the failure or unavailability of the mobile network (in minutes)
Daily relogin	**Disabled:** daily login deactivated **Enabled:** daily login activated
Time	Time at which the device logs out of the mobile network under controlled conditions and logs in again

SIM

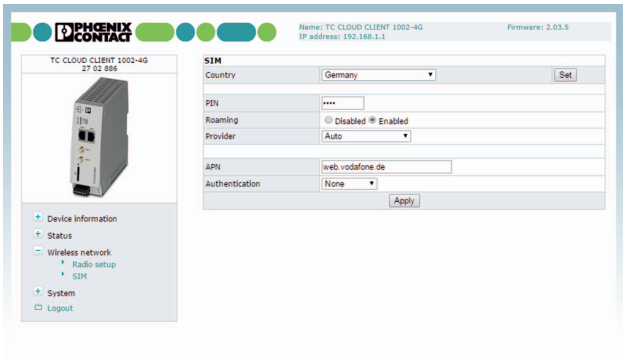

Figure 16 Wireless network, SIM

Wireless network, SIM	
Country	Country in which the device is dialing into the GSM network This setting limits the selection under Provider.
PIN	Enter the PIN for the SIM card. The PIN can be overwritten. It is not possible to read the PIN.
Roaming	If roaming is activated (default), you can select a specific provider from the “Provider” menu.
	Enabled: the router can also dial-in via external networks. If “Auto” is set under “Provider”, the strongest provider is selected. Depending on your contract, this may incur additional costs. Alternatively, you can specify a provider.
	Disabled: roaming is deactivated. The device only uses the provider's home network. If this network is unavailable, the device cannot establish an Internet connection.
Provider	Select a provider via which the device is to establish the Internet connection. If you have selected a country under “Country”, this limits the selection. **Auto:** the router automatically selects the provider using the SIM card.
User name	User name for packet data access The user name and password can be obtained from your provider. This field may be left empty if the provider does not require a special input.
Password	Password for packet data access This field may be left empty if the provider does not require a password.

Wireless network, SIM	
APN	The APN can be obtained from your provider. APN (Access Point Name) is the name of a terminal point in a packet data network. The APN enables access to an external data network. At the same time, the APN specifies the network to which a connection will be established. In the case of a public APN, the connection is usually established to the Internet. The device supports public and private APNs.
Authentication	Select the protocols for logging into the provider:
	None: the provider's APN does not require login (default).
	Refuse MSCHAP: MSCHAP is **not** accepted.
	CHAP only: only CHAP is accepted.
	PAP only: only PAP is accepted.

12.4 System

Connection setup (IP configuration)

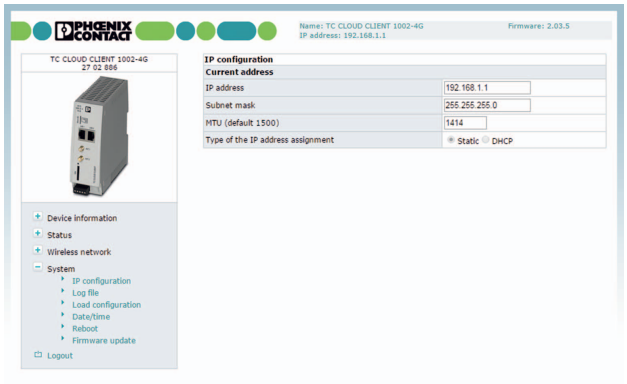

Figure 17 System, IP configuration

System, IP configuration	
IP address	Current IP address
Subnet mask	Subnet mask for the current IP address
MTU (default 1500)	Maximum Transmission Unit (MTU) is the maximum packet size, in bytes, in the mobile network
Type of the IP address assignment	**Static (default):** the IP address is assigned permanently, fixed IP. **DHCP:** when the device is started, the IP address and the subnet mask are assigned dynamically by a DHCP server.

Log file

The log file can be used to diagnose various events and operating states. The log file is a form of circulating storage where the oldest entries are overwritten first.

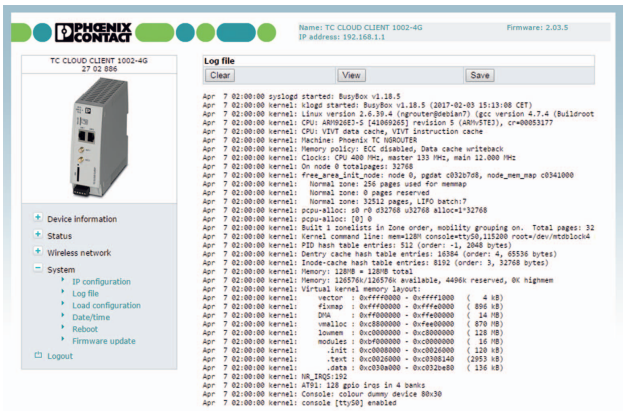

Figure 18 System, Log file

System, Log file	
Clear	Delete all entries in the log file
View	View log file in the browser window
Save	Save log file as text file on local computer

Load configuration

You can save the active configuration to a file and load prepared configurations.

Figure 19 System, Load configuration

System, Load configuration	
Upload	To load a configuration from the microSD card, select the “SD card” option under “Upload”. Import a saved configuration. Click on “Apply” to load the selected configuration.
Reset to factory defaults	Click on “Apply” to reset the device to the default state upon delivery. This will reset all settings, including IP settings. Imported certificates remain unaltered.

Set time and date (Date/time)

Figure 20 System, Date/time

System, Date/time	
System time	Here you can set the time manually if no NTP server has been set up or the NTP server cannot be reached.
Time synchronisation	**Enabled:** the cloud client synchronizes the time and date with a time server. Initial time synchronization can take up to 15 minutes. During this time, the cloud client continuously compares the time data of the external time server and that of its own clock. The time is therefore adjusted as accurately as possible. Only then can the cloud client act as the NTP server for the devices connected to the LAN interface. The cloud client then provides the system time.
NTP server	NTP = Network Time Protocol
Time zone	Select the time zone.
Daylight saving time	**Enabled:** daylight savings is taken into account. **Disabled:** daylight savings is not taken into account.

Restart device (Reboot)

Figure 21 System, Reboot

System, Reboot	
Reboot NOW!	Any active data transmissions will be aborted. Do **not** trigger a reboot while data transmission is active.
Daily reboot	Define the day of the week on which the device will be restarted at the specified time.
Time	Time specified in Hours:Minutes

Firmware update

Updates can be downloaded at:
phoenixcontact.net/products

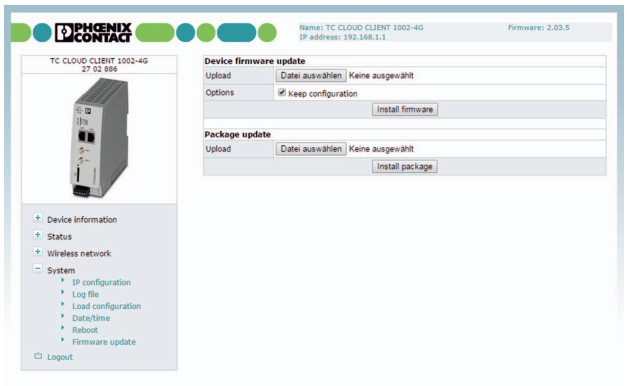

Figure 22 System, Firmware update

System, Firmware update	
Device firmware update	Updates ensure that you can benefit from function extensions and product updates.
Package update	If necessary you can also just update individual functions.

Install firmware update:

- Select the update file with the extension *.fw. To ensure that the device retains the active configuration following the update, select the “Keep configuration” option.
- Click on “Install firmware”.

The ERR LED and TS LED flash alternately during the update. Wait until the update is completed and the device restarts automatically.

13 Disposal

Dispose of the device separately from other waste, i.e., via an appropriate collection site.