Industrial mobile router with integrated firewall and VPN

User manual

UM EN TC ROUTER ... 3G/4G

INSPIRING INNOVATIONS

User manual

Industrial mobile router with integrated firewall and VPN

UM EN TC ROUTER ... 3G/4G, Revision 01 2018-09-07

This user manual is valid for:

Designation	Software release	Order No.
TC ROUTER 3002T-4G	2.04.11	2702528
TC ROUTER 3002T-3G	2.04.11	2702529
TC ROUTER 2002T-4G	2.04.11	2702530
TC ROUTER 2002T-3G	2.04.11	2702531
TC ROUTER 3002T-4G VZW	2.04.11	2702532
TC ROUTER 3002T-4G ATT	2.04.11	2702533

107025_en_01

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Table of contents

1 For your safety

Read this user manual carefully and keep it for future reference.

1.1 Identification of warning notes

⚠ This symbol indicates hazards that could lead to personal injury.

There are three signal words indicating the severity of a potential injury.

DANGER
Indicates a hazard with a high risk level. If this hazardous situation is not avoided, it will result in death or serious injury.

WARNING
Indicates a hazard with a medium risk level. If this hazardous situation is not avoided, it could result in death or serious injury.

CAUTION
Indicates a hazard with a low risk level. If this hazardous situation is not avoided, it could result in minor or moderate injury.

ⓘ This symbol together with the **NOTE** signal word warns the reader of actions that might cause property damage or a malfunction.

ℹ Here you will find additional information or detailed sources of information.

1.2 Qualification of users

The use of products described in this user manual is oriented exclusively to:

- Electrically skilled persons or persons instructed by them. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.
- Qualified application programmers and software engineers. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

1.3 Field of application of the product

The devices are industrial mobile routers for 3G and 4G mobile networks.

1.3.1 Intended use

- The devices are designed for use in industrial environments.
- The devices are intended for installation in a control cabinet.
- Operation of the wireless system is only permitted if accessories available from Phoenix Contact are used. The use of other accessory components could invalidate the operating license.

You can find the approved accessories for this wireless system listed with the product at phoenixcontact.net/products.

1.3.2 Product changes

Modifications to hardware and firmware of the device are **not** permitted.

Incorrect operation or modifications to the device can endanger your safety or damage the device. Do not repair the device yourself. If the device is defective, please contact Phoenix Contact.

1.4 Safety notes

WARNING:
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 the generally recognized codes of practice, must be observed. The technical data is provided in the packing slip and on the certificates (conformity assessment, additional approvals where applicable).
- Do not open or modify the device. Do not repair the device yourself; replace it with an equivalent device instead. Repairs may only be carried out by the manufacturer. The manufacturer is not liable for damage resulting from non-compliance.
- The IP20 degree of protection (IEC 60529/EN 60529) of the device is intended for use in a clean and dry environment. Do not subject the device to mechanical and/or thermal loads that exceed the specified limits.
- The device is designed exclusively for operation with safety extra-low voltage (SELV) in accordance with IEC 60950/EN 60950/VDE 0805. The device may only be connected to devices that meet the requirements of EN 60950.
- The device complies with the EMC regulations for industrial areas (EMC class A). When used in residential areas, the device may cause radio interference.

1.5 UL warning notes (only TC ROUTER 3002T-4G VZW and TC ROUTER 3002T-4G ATT)

- 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

⚠

2 Installation

2.1 Product description

The **TC ROUTER...** mobile routers enable high-performance high-speed data links via mobile networks. The integrated firewall and VPN (Virtual Private Network) protect your application against unauthorized access.

The focus is on EMC, electrical isolation, and surge protection for reliable and secure communication. The data link and quality of the mobile network are also monitored. If required, the device sends a message or re-establishes the mobile network connection.

Features

- Virtual permanent line to connect networks via mobile network
- Stateful inspection firewall for dynamic filtering
- VPN remote start via SMS or call
- Two switching inputs and one switching output
- XML interface
- Alarm sent via SMS or e-mail directly via the integrated switching input
- Configuration via web-based management or microSD card
- Two local Ethernet connections
- Switchable energy-saving mode
- Integrated logbook
- Extended temperature range of -40°C ... +70°C

Table 2-1 Overview product versions

Designation	Mobile communication	Fallback	VPN function	Area of application
TC ROUTER 3002T-4G	4G (LTE)	3G (UMTS/HSPA) 2G (GPRS/EDGE)	IPsec and OpenVPN, up to three VPN tunnels	Europe
TC ROUTER 3002T-3G	3G (UMTS/HSPA)	2G (GPRS/EDGE)		
TC ROUTER 2002T-4G	4G (LTE)	3G (UMTS/HSPA) 2G (GPRS/EDGE)	-	
TC ROUTER 2002T-3G	3G (UMTS/HSPA)	2G (GPRS/EDGE)		
TC ROUTER 3002T-4G VZW	4G (LTE)	-	IPsec and OpenVPN, up to three VPN tunnels	USA (HazLoc approval)
TC ROUTER 3002T-4G ATT		3G (UMTS/HSPA)		

2.2 Structure

2.2.1 4G router

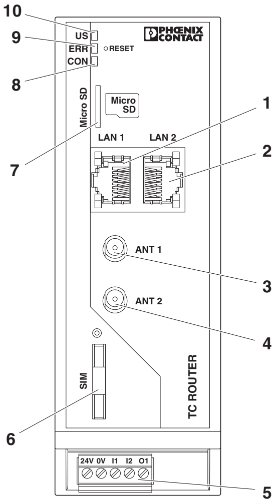


Figure 2-1 4G router

1 LAN interface 1
2 LAN interface 2
3 SMA antenna connection 1, primary antenna
4 SMA antenna connection 2, secondary antenna
5 COMBICON plug-in screw terminal block
6 SIM interface
7 Slot for microSD card
8 CON LED
9 ERR LED
10 US LED

2.2.2 3G router

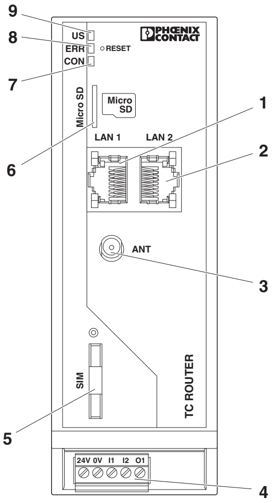


Figure 2-2 3G router

1	LAN interface 1
2	LAN interface 2
3	SMA antenna socket
4	COMBICON plug-in screw terminal block
5	SIM interface
6	Slot for microSD card
7	CON LED
8	ERR LED
9	US LED

2.2.3 Status and diagnostics indicators

U_S	Power	Green
	On	Supply voltage is present
ERR	Error	Red
	Off	Logged into the network
	Flashing	SIM card not inserted, SIM error (e.g., PIN or PUK locked)
	On	Searching for cellular network
CON	Connect	Yellow
	On	Connection established

In the case of the TC ROUTER 3002T..., the CON LED can be configured via web-based management. You can therefore monitor the mobile IP connection or the VPN tunnel.

2.3 Mounting and removal

NOTE: Device damage

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

The device is intended for installation in a control cabinet.

- Snap the device onto a 35 mm DIN rail according to EN 60715.
- Connect the DIN rail to protective earth ground.

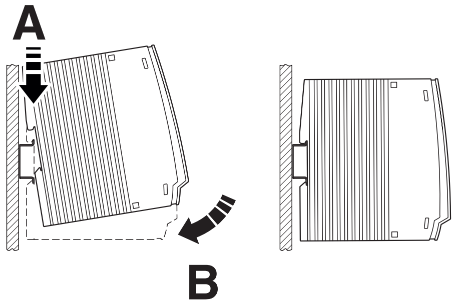


Figure 2-3 Mounting on the DIN rail

Removal

- Pull down the locking latch using a screwdriver, needle-nose pliers or similar.
- Pull the bottom edge of the device slightly away from the mounting surface.
- Pull the device away from the DIN rail.

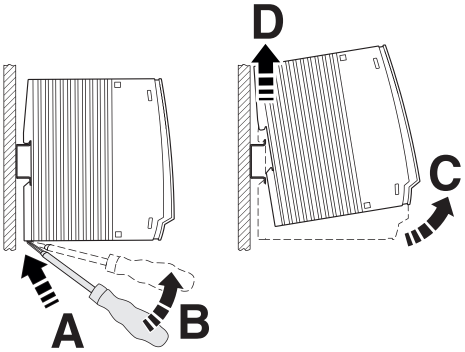


Figure 2-4 Removal

2.4 Inserting the SIM card

NOTE: Electrostatic discharge!

The device contains components that can be damaged or destroyed by electrostatic discharge. When handling the device, observe the necessary safety precautions against electrostatic discharge (ESD) in accordance with EN 61340-5-1 and IEC 61340-5-1.

The device only supports 1.8 V and 3 V SIM cards. In the event of older SIM cards, please contact your provider.

You will receive a SIM card from the provider on which all data and services for your connection are stored. The SIM card can be protected with a 4 or 5-digit PIN code. We recommend that you enter the PIN code and the APN settings as described in "SIM" on page 30.

A packet data connection via the mobile network is required for the core functions (VPN router). Select an appropriate SIM card. You must activate the package data connection before the operation (see "Packet data setup" on page 36).

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

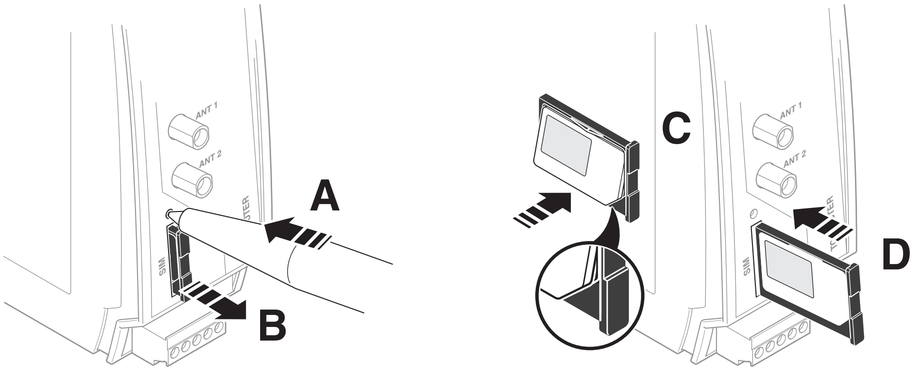


Figure 2-5 Removing the SIM card holder, inserting the SIM card

2.5 Connection

2.5.1 Antenna

> You can find the approved accessories for this wireless system listed with the product at phoenixcontact.net/products.

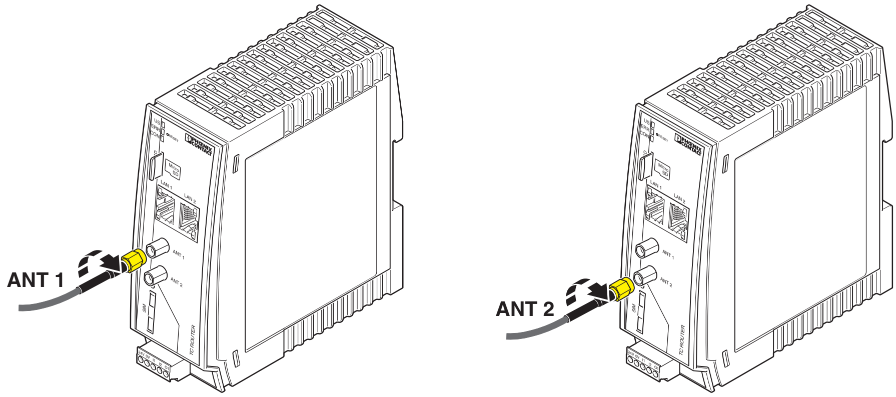


Figure 2-6 Connecting the antenna (4G router)

The 4G routers have two antenna connections. To achieve optimum LTE reception, always connect two antennas for 4G routers. The 3G routers only have one antenna connection.

We recommend the multiband mobile antenna with mounting bracket for outdoor installation (TC ANT MOBILE WALL 5M, Order No. 2702273). Please also refer to the documentation for the antenna at phoenixcontact.net/product/2702273.

- Connect one or two suitable antennas to the antenna connection.
- The antenna cable must not be longer than 5 meters in length.
- Check the signal quality in the web-based management software under “Device Information, Status, Radio”.
- Fix the antenna in place when reception is good or very good.
- Screw the antenna hand-tight on to the device (1.7 Nm).

2.5.2 Ethernet network

- Only twisted pair cables with an impedance of 100 Ω may be connected to the RJ45 Ethernet interfaces.
- Only use shielded twisted pair cables and corresponding shielded RJ45 connectors.
- Push the Ethernet cable with the RJ45 connector into the TP interface until the connector engages with a click. Observe the connector coding.

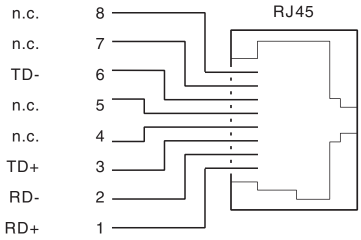


Figure 2-7 RJ45 interface

2.5.3 Supply voltage

CAUTION: Electrical voltage

The device is designed exclusively for operation with safety extra-low voltage (SELV) in accordance with IEC 60950/EN 60950/VDE 0805.

– Provide overcurrent protection (I ≤ 5 A) in the installation.

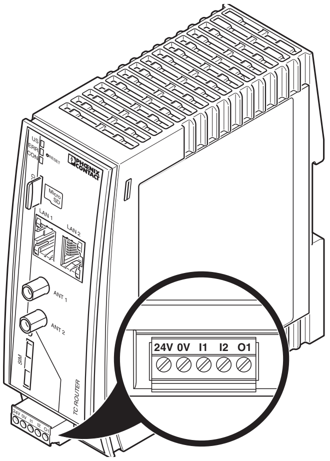


Figure 2-8 Connecting the supply voltage

- Connect the supply voltage to 24 V and 0 V at the plug-in screw terminal block. Ensure the correct polarity when doing so.
- The device is ready for operation as soon as the US LED lights up.

2.5.4 Switching inputs and switching outputs

Two configurable switching inputs for the following functions:

- Sending an SMS, including to multiple recipients
- Sending an e-mail, including to multiple recipients
- Controlling an output at a remote station via SMS
- Restarting the router
- Starting or stopping a mobile data connection
- Switching the IPsec or OpenVPN connection
- Automatically loading a configuration from a microSD card
- Activating energy-saving mode

One configurable switching output, activated by:

- Activation by the input at a remote station
- SMS
- Web-based management
- Incoming call
- Connection abort
- Status of the mobile network connection
- Status of the mobile data connection
- Status of a VPN connection

Connecting

- You can connect 10 ... 30 V DC to switching inputs I1 and I2.
- Switching output O1 is designed for a maximum of 50 mA at 10 ... 30 V DC.
- The connecting cables for the switching inputs and the switching output must not be longer than 30 meters in length.
- The 0 V potential of the switching inputs and outputs must be connected to the “0 V” terminal block of the power supply connection.

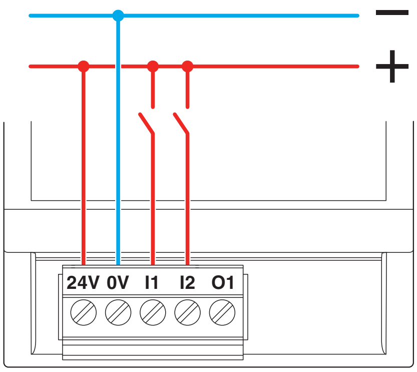


Figure 2-9 Wiring inputs

2.6 Resetting the router

The routers have a reset button on the front to the right of the LEDs. The reset button can be used to temporarily reset the router's IP address and the passwords to the default settings upon delivery.

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

The IP address is now reset to its default address (192.168.0.1).

3 Configuration via web-based management

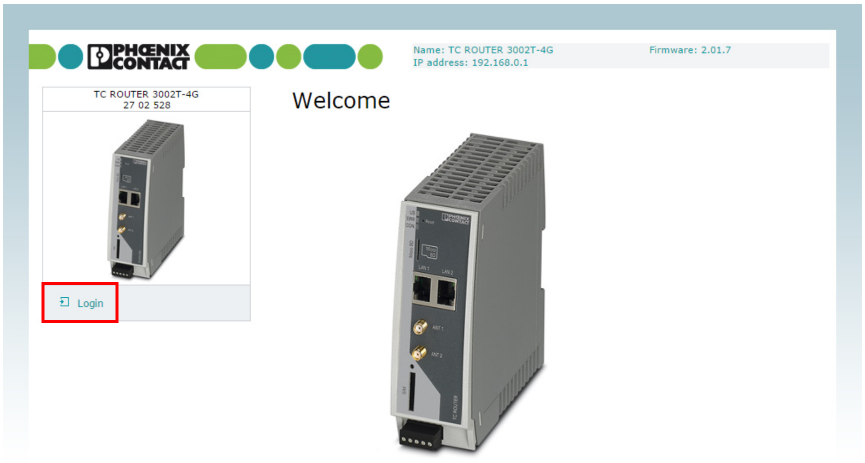
3.1 Connection requirements

– The device must be connected to the power supply.
– The computer that is to be used for configuration must be connected to one of the LAN ports on the router.
– A browser, e.g., Mozilla Firefox, Microsoft Internet Explorer or Apple Safari, must be installed on the configuration computer.

3.2 Starting web-based management (WBM)

The router is configured via web-based management (WBM).

- Establish an Ethernet connection from the device to a PC.
- If necessary, adjust the IP parameters of your computer.
- Open a browser on the PC.
- Enter the IP address 192.168.0.1 in the address field of your browser.
- The following page opens in the browser.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Welcome

Figure 3-1 Login window

This page protects the area in web-based management where router settings are modified. To log into the router, click on “Login”. You need the user name and the password.

– User name: admin
– Password: admin

For security reasons, we recommend you change the password during initial configuration (see “User (password change)” on page 85).

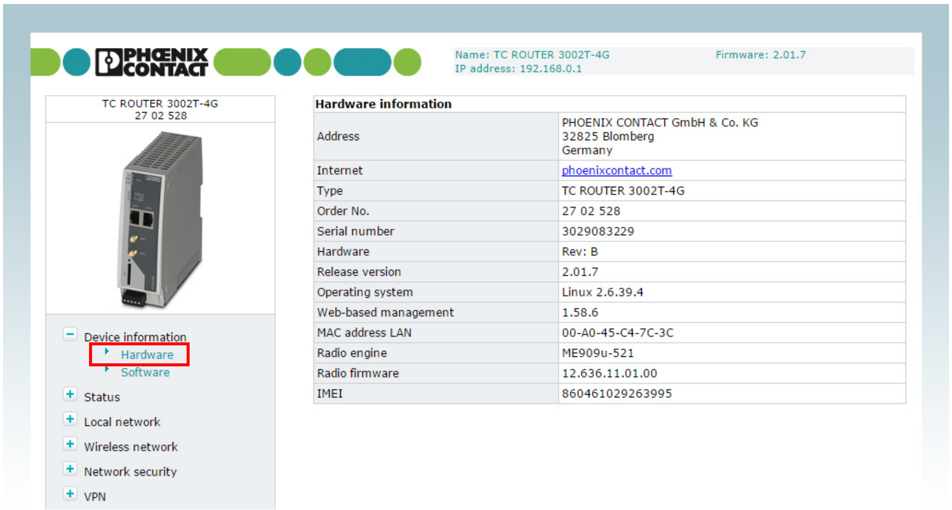
There are two user levels:

– **user:** read-only access to the “Device Information” menu item
– **admin:** full access to all areas

3.3 Device information (viewing the device status)

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

3.3.1 Hardware



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Hardware information	
Address	PHOENIX CONTACT GmbH & Co. KG 32825 Blomberg Germany
Internet	phoenixcontact.com
Type	TC ROUTER 3002T-4G
Order No.	27 02 528
Serial number	3029083229
Hardware	Rev: B
Release version	2.01.7
Operating system	Linux 2.6.39.4
Web-based management	1.58.6
MAC address LAN	00-A0-45-C4-7C-3C
Radio engine	ME909u-521
Radio firmware	12.636.11.01.00
IMEI	860461029263995

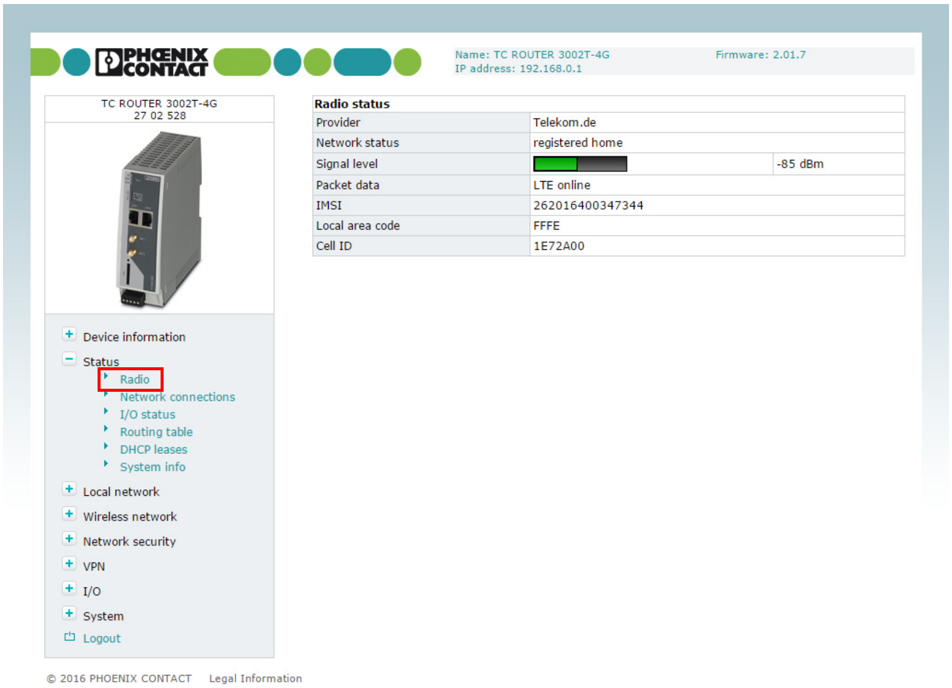
Figure 3-2 Device information, Hardware

Device information, Hardware		
Hardware information	**Address**	Address of the manufacturer
	Internet	Website address of the manufacturer
	Type	Order designation of the router
	Order No.	Order number of the router
	Serial number	Serial number of the router
	Hardware	Hardware version of the router
	Release version	Release version of the router 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	Type of radio engine used
	Radio firmware	Firmware version of the radio engine
	IMEI	IMEI = International Mobile Station Equipment Identity 15-digit serial number that can be used to clearly identify each mobile network device

3.4 Status

The current status information about the mobile network and the network connections is displayed here.

3.4.1 Radio



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

Radio status		
Provider	Telekom.de	
Network status	registered home	
Signal level	🟩	-85 dBm
Packet data	LTE online	
IMSI	262016400347344	
Local area code	FFFE	
Cell ID	1E72A00	

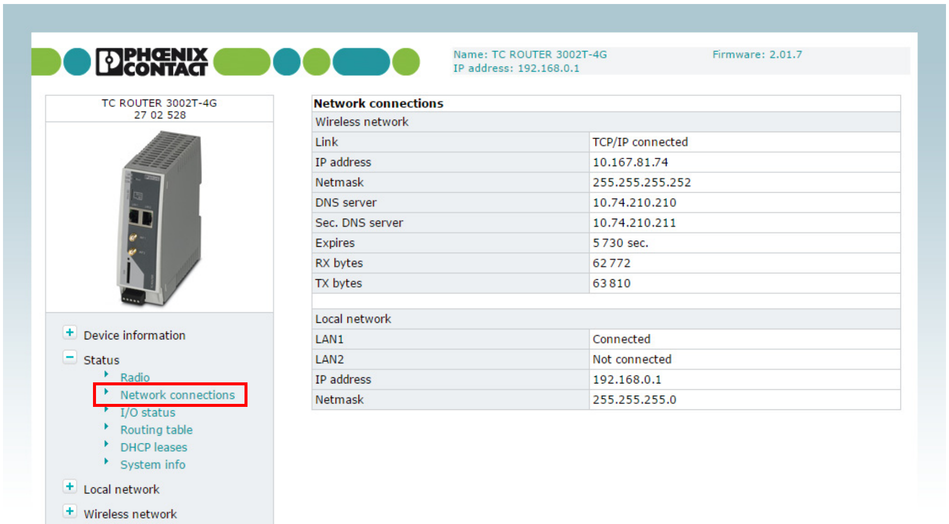
Figure 3-3 Status, Radio

Device information, Status, Radio		
Radio status	**Provider**	Provider name
	Network status	Status of the mobile network – **Registered home:** logged in to 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

Device information, Status, Radio [...]		
	Packet data	– **Offline**: no packet data connection in the mobile network – **GPRS online**: active packet data connection in the mobile network via GPRS. GPRS is a GSM service which provides packet-based wireless access for mobile GSM users. – **EDGE online**: active packet data connection in the mobile network via EDGE. EDGE is a further development of the GPRS data service and has a higher data transmission speed. – **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	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

3.4.2 Network connections

This page displays status information about the local Ethernet interface and the packet data interface in the mobile network.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

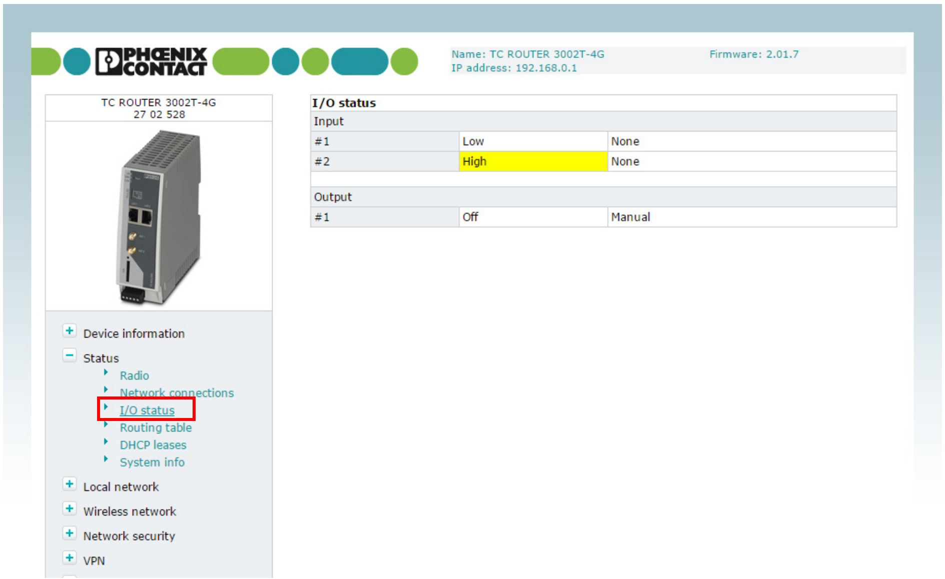
Network connections	
Wireless network	
Link	TCP/IP connected
IP address	10.167.81.74
Netmask	255.255.255.252
DNS server	10.74.210.210
Sec. DNS server	10.74.210.211
Expires	5 730 sec.
RX bytes	62 772
TX bytes	63 810
Local network	
LAN1	Connected
LAN2	Not connected
IP address	192.168.0.1
Netmask	255.255.255.0

Figure 3-4 Status, Network connections

Status, Network connections		
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 Ethernet IP address
	Netmask	Netmask of the local Ethernet network

3.4.3 I/O status

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



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

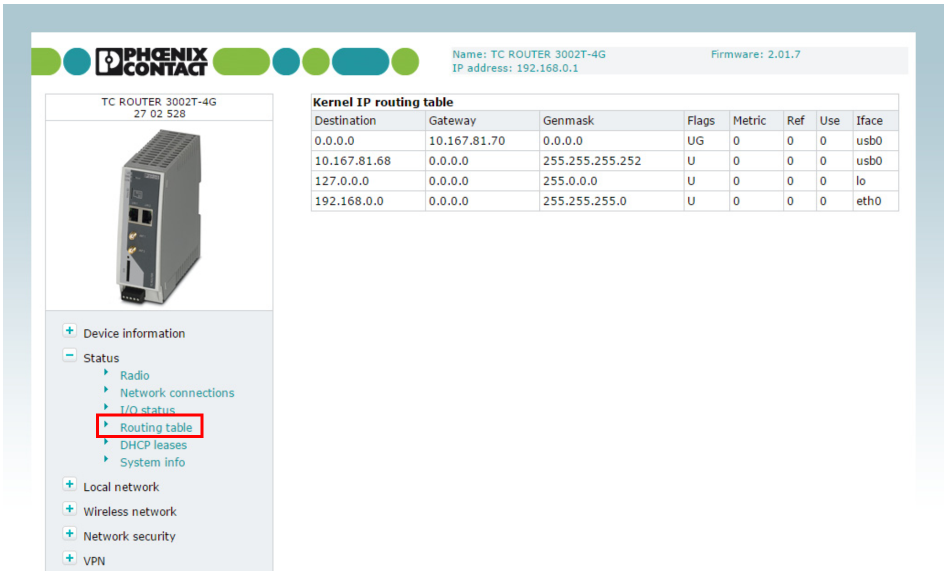
I/O status

Input		
#1	Low	None
#2	High	None
Output		
#1	Off	Manual

Figure 3-5 Status, I/O status

3.4.4 Routing table

This page shows all entries of the routing table.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

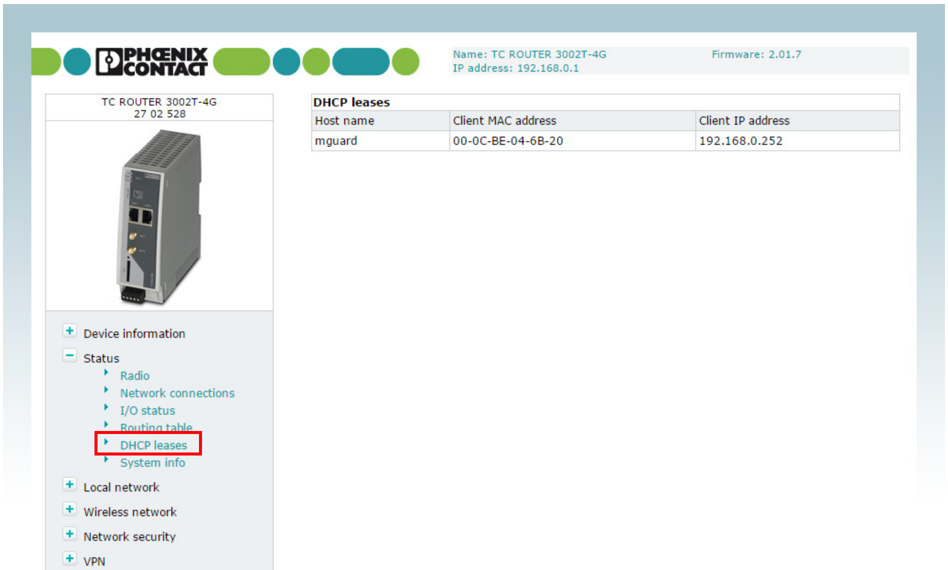
Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	10.167.81.70	0.0.0.0	UG	0	0	0	usb0
10.167.81.68	0.0.0.0	255.255.255.252	U	0	0	0	usb0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

Figure 3-6 Status, Routing table

3.4.5 DHCP leases

This page shows the IP addresses that the mobile router has currently assigned to the DHCP clients.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

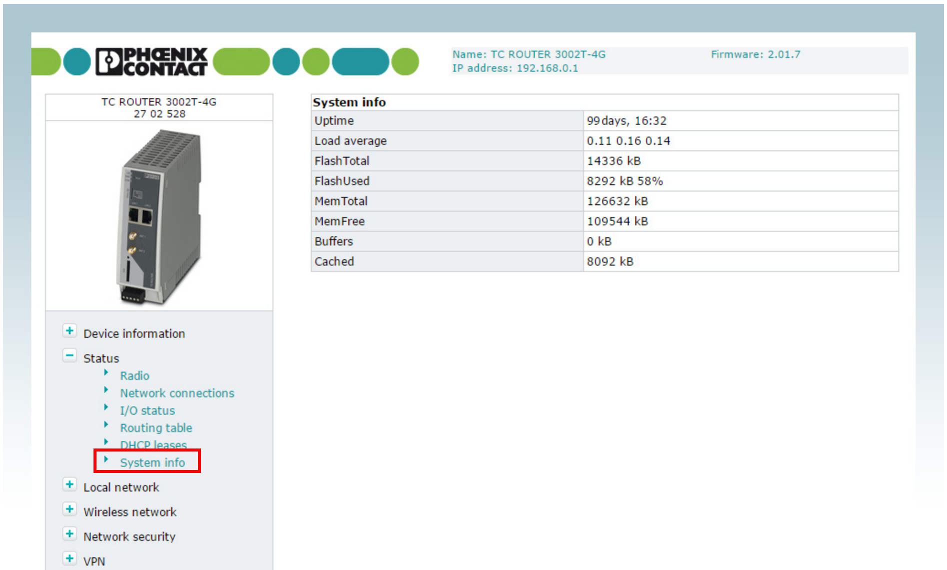
DHCP leases

Host name	Client MAC address	Client IP address
mguard	00-0C-BE-04-6B-20	192.168.0.252

Figure 3-7 Status, DHCP leases

3.4.6 System info

This page shows the current system utilization.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

System info	
Uptime	99days, 16:32
Load average	0.11 0.16 0.14
FlashTotal	14336 kB
FlashUsed	8292 kB 58%
MemTotal	126632 kB
MemFree	109544 kB
Buffers	0 kB
Cached	8092 kB

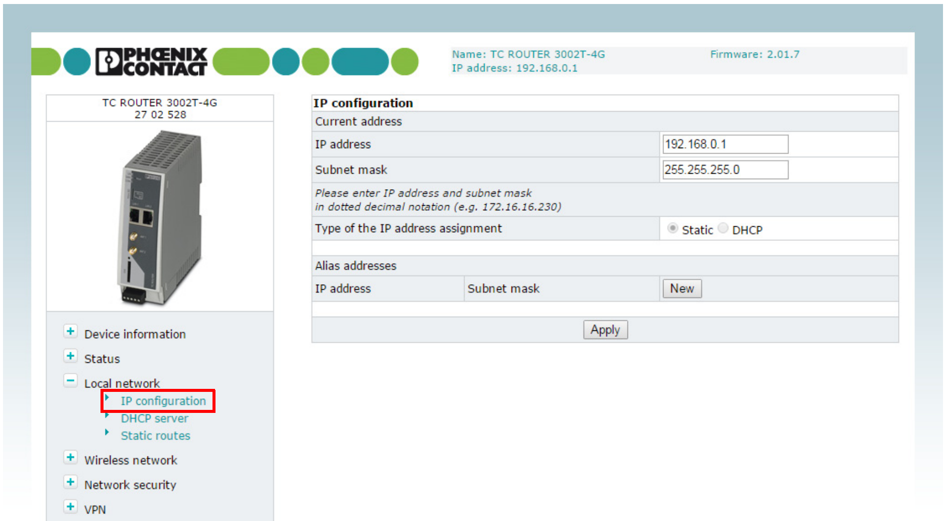
Figure 3-8 Status, System info

3.5 Local network (local network setup)

3.5.1 IP configuration (connection setup)

The connection from the router to the local Ethernet network can be set up here. You can modify the IP configuration, e.g., the IP address, the subnet mask, and the type of address assignment.

Confirm your changes to the IP configuration with “Apply”. The changes only take effect after a restart.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

IP configuration

Current address

IP address	192.168.0.1
Subnet mask	255.255.255.0

Please enter IP address and subnet mask in dotted decimal notation (e.g. 172.16.16.230)

Type of the IP address assignment: ● Static ○ DHCP

Alias addresses

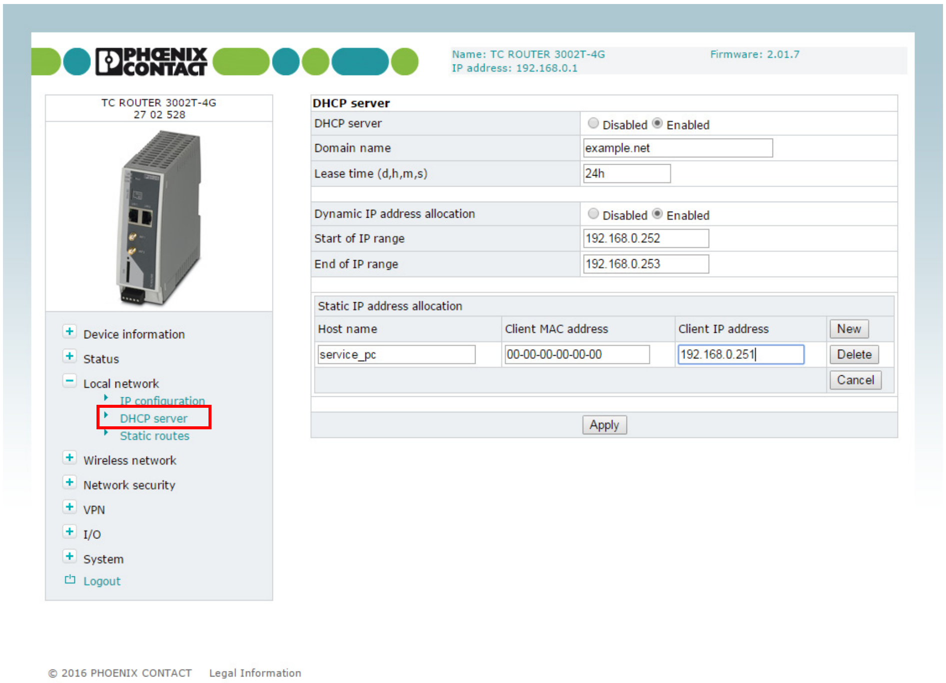
IP address	Subnet mask

Figure 3-9 Local network, IP configuration

Local network, IP configuration		
IP configuration		
Current address	**IP address**	Current IP address of the router Computers that are connected to the LAN interfaces access the router using this address. You can use the reset button to reset the IP address to the default address 192.168.0.1 (see “Resetting the router” on page 17).
	Subnet mask	Subnet mask for the current IP address
	Type of the IP address assignment	– **Static** (default): the IP address is assigned permanently (fixed IP). – **DHCP:** when the router is started, the IP address and the subnet mask are assigned dynamically by a DHCP server.
Alias addresses		Using alias addresses, you can assign up to 8 additional IP addresses to the router. This means that the router can be accessed from various subnetworks. Click on “New” and enter the desired IP address and subnet mask.

3.5.2 DHCP server

You can use the Dynamic Host Configuration Protocol (DHCP) to assign the set network configuration to the devices. The devices must be connected directly to the router.



DHCP server

DHCP server	○ Disabled ● Enabled
Domain name	example.net
Lease time (d,h,m,s)	24h
Dynamic IP address allocation	○ Disabled ● Enabled
Start of IP range	192.168.0.252
End of IP range	192.168.0.253

Static IP address allocation

Host name	Client MAC address	Client IP address
service_pc	00-00-00-00-00-00	192.168.0.251

Figure 3-10 Local network, DHCP server

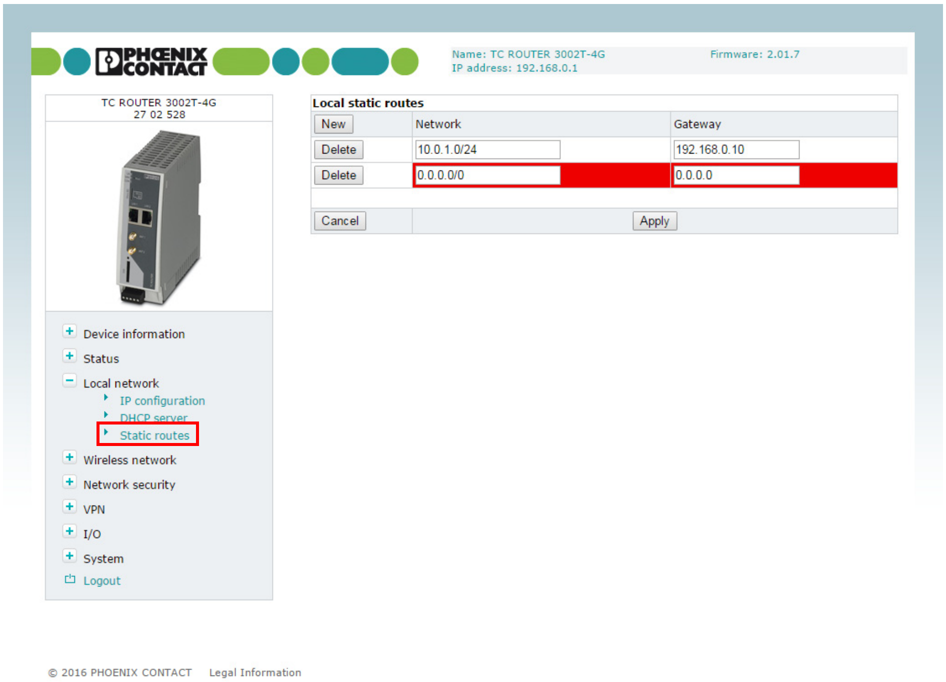
Local network, DHCP server		
DHCP server	**DHCP server**	– **Enabled:** router acts as the DHCP server
	Domain name	Domain name that will be distributed via DHCP
	Lease time (d,h,m,s)	Time for which the network configuration assigned to the client is valid The client should renew its assigned configuration shortly before this time expires. Otherwise it may be assigned to other computers.
	Dynamic IP address allocation	Dynamic IP address pool: when the DHCP server and the dynamic IP address pool have been activated, you can specify the network parameters to be used by the client.
	Start of IP range	Start of DHCP area: the start of the address area from which the DHCP server should assign IP addresses to locally connected devices.
	End of IP range	End of DHCP area: the end of the address area from which the DHCP server should assign IP addresses to locally connected devices.

Local network, DHCP server [...]		
Static IP address allocation		Static assignment based on the MAC address: the static IP of the client to which the MAC address should be assigned.
	Client MAC address	MAC of the client with dashes
	Client IP address	Client IP address Static assignments must not overlap with the dynamic IP address pool. Do not use one IP address in multiple static assignments, otherwise this IP address will be assigned to multiple MAC addresses.

3.5.3 Static routes (redirection of data packets)

With local static routes, you can specify alternative routes for data packets from the local network via other gateways in higher-level networks. You can define up to eight static routes.

If the entries for the network and gateway are logically incorrect, the incorrect entries will be displayed with a red frame.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Local static routes

New	Network	Gateway
Delete	10.0.1.0/24	192.168.0.10
Delete	0.0.0.0/0	0.0.0.0
Cancel	Apply	

© 2016 PHOENIX CONTACT Legal Information

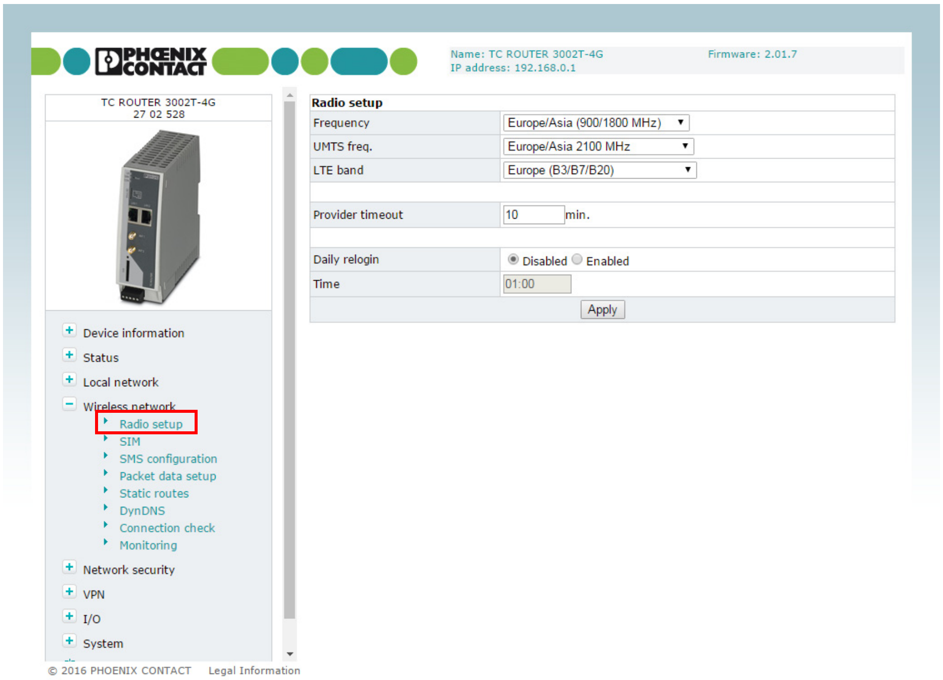
Figure 3-11 Local network, Static routes

Local network, Static routes		
Local static routes	**Network**	Network in CIDR format, see “CIDR (Classless Inter-Domain Routing)” on page 136
	Gateway	Gateway via which this network can be accessed

3.6 Wireless network (mobile network settings)

You can integrate remote stations into an IP network, e.g., the Internet, via a mobile network connection. The mobile network connection and frequencies can be configured here.

3.6.1 Radio setup



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Radio setup

Frequency	Europe/Asia (900/1800 MHz) ▾
UMTS freq.	Europe/Asia 2100 MHz ▾
LTE band	Europe (B3/B7/B20) ▾
Provider timeout	10 min.
Daily relogin	● Disabled ○ Enabled
Time	01:00

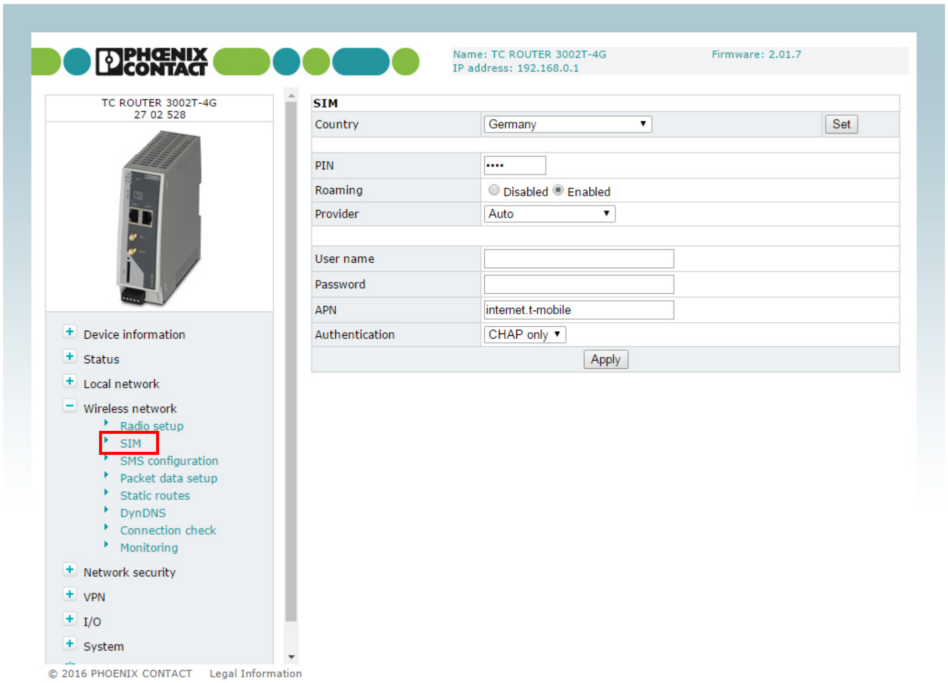
Apply

Figure 3-12 Wireless network, Radio setup

Wireless network, Radio setup		
Radio setup	**Frequency**	GSM frequency range in which the router should operate
	UMTS freq.	Frequency range for UMTS in which the router should operate In addition, you can deactivate UMTS: “UMTS off”
	LTE band	Frequency range for LTE in which the router 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 router logs out of the mobile network under controlled conditions and logs in again.

3.6.2 SIM

Settings for the European devices (TC ROUTER ... 3G/4G)



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

SIM

Country	Germany ▾
PIN	••••
Roaming	○ Disabled ● Enabled
Provider	Auto ▾
User name	
Password	
APN	internet.t-mobile
Authentication	CHAP only ▾

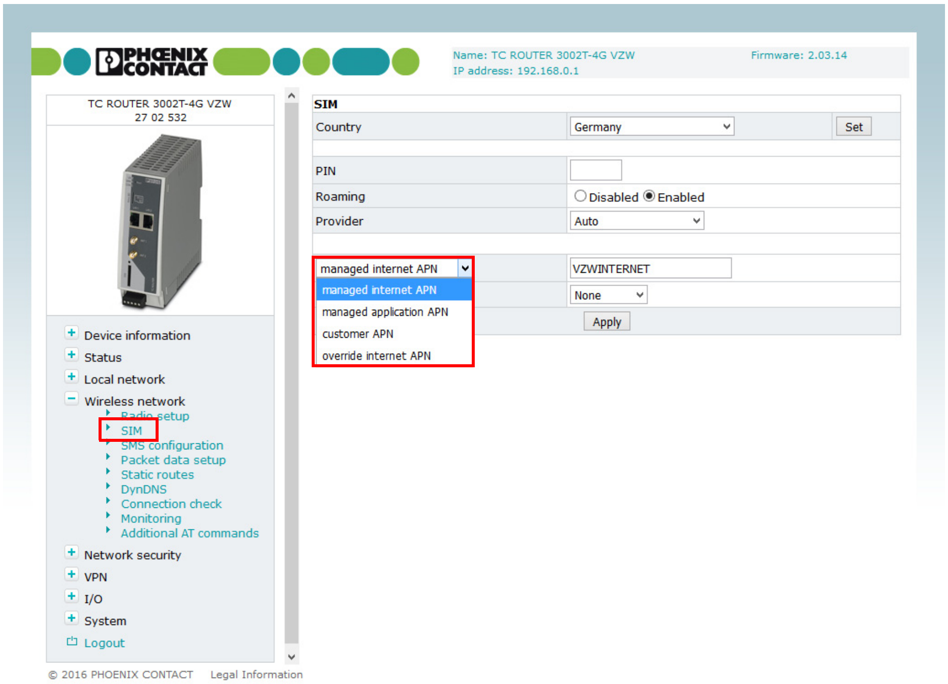
Figure 3-13 Wireless network, SIM (Europe)

Wireless network, SIM	Settings for the primary mobile network connection, Europe	
SIM	**Country**	Select the country in which the router is dialing into the GSM network. This setting limits the selection among the providers.
	PIN	Enter the PIN for the SIM card here. The PIN cannot be read back, it can only be overwritten.
	Roaming	If roaming is activated (default), you can select a specific provider from the drop-down 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 and only the provider's home network is used. If this network is unavailable, the router cannot establish an Internet connection.

Wireless network, SIM [...]	Settings for the primary mobile network connection, Europe	
	Provider	Select a provider via which the router is to establish the Internet connection. The country selected under “Country” limits the list of providers. – **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 the packet data access. This field may be left empty if the provider does not require a password.
	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 is to 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 in to 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.

Settings for the US devices (TC ROUTER 3002T-4G VZW and TC ROUTER 3002T-4G ATT)

The devices for the American market require special APN settings.



Name: TC ROUTER 3002T-4G VZW
IP address: 192.168.0.1
Firmware: 2.03.14

TC ROUTER 3002T-4G VZW
27 02 532

SIM		
Country	Germany	Set
PIN		
Roaming	○ Disabled ● Enabled	
Provider	Auto	
managed internet APN	VZWINTERNET	
	None	
	Apply	

Figure 3-14 Wireless network, SIM (US)

Wireless network, SIM	Settings for the primary mobile network connection, US	
SIM	**Country**	Select the country in which the router is dialing into the GSM network. This setting limits the selection among the providers.
	PIN	Enter the PIN for the SIM card here. The PIN cannot be read back, it can only be overwritten.
	Roaming	If roaming is activated (default), you can select a specific provider from the drop-down 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 and only the provider's home network is used. If this network is unavailable, the router cannot establish an Internet connection.

Wireless network, SIM [...]	Settings for the primary mobile network connection, US	
	Provider	Select a provider via which the router is to establish the Internet connection. The country selected under “Country” limits the list of providers. – **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 the packet data access. This field may be left empty if the provider does not require a password.
	APN	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 is to be established. In the case of a public APN, the connection is usually established to the Internet. The device supports public and private APNs. – **managed Internet APN:** default, no manual input The device autonomously logs in to the network. The APN is set automatically. When the router has logged in to the network, the standard APN used is displayed. – **managed application APN (only Verizon Wireless):** enter an application APN. The standard APN remains stored in the device. – **customer APN:** enter a customer-specific APN. The standard APN remains stored in the device. – **overwrite APN:** the standard APN will be deleted if you enter your APN here. This is only possible after the router has successfully made a connection with the mobile network by using the default setting (managed Internet APN). Only use "overwrite APN" if the default APN of your provider changed and the router does not adapt automatically. Contact your provider if you have accidentally overwritten the default APN.
	Authentication	Select the protocols for logging in to 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.

3.6.3 SMS configuration (SMS settings)

You can operate the device remotely via SMS.

- Open “Wireless network, SMS configuration”. Activate “SMS control” and enter the “SMS password”. The password can contain up to seven alphanumeric characters.

In addition, the device can forward received SMS messages to a recipient as a UDP packet via Ethernet.

- Activate the “SMS forward” function.
- Enter the recipient IP address and port with which you would like to communicate. The default value for the server is port 1432. Alternatively, incoming SMS messages can be accessed from the local Ethernet network via XML and socket server (see “Socket server” on page 75).

The received SMS is forwarded in the following format:

```
<?xml version="1.0"?>
<cmgr origaddr="+49172123456789" timestamp="10/05/21,11:27:14+08">
SMS message</cmgr>
```

– origaddr = Sender telephone number

– timestamp = Time stamp of the service center in GSM 03.40 format

The SMS syntax for switching inputs, outputs, and functions contains the following information:

– Password

– Function command

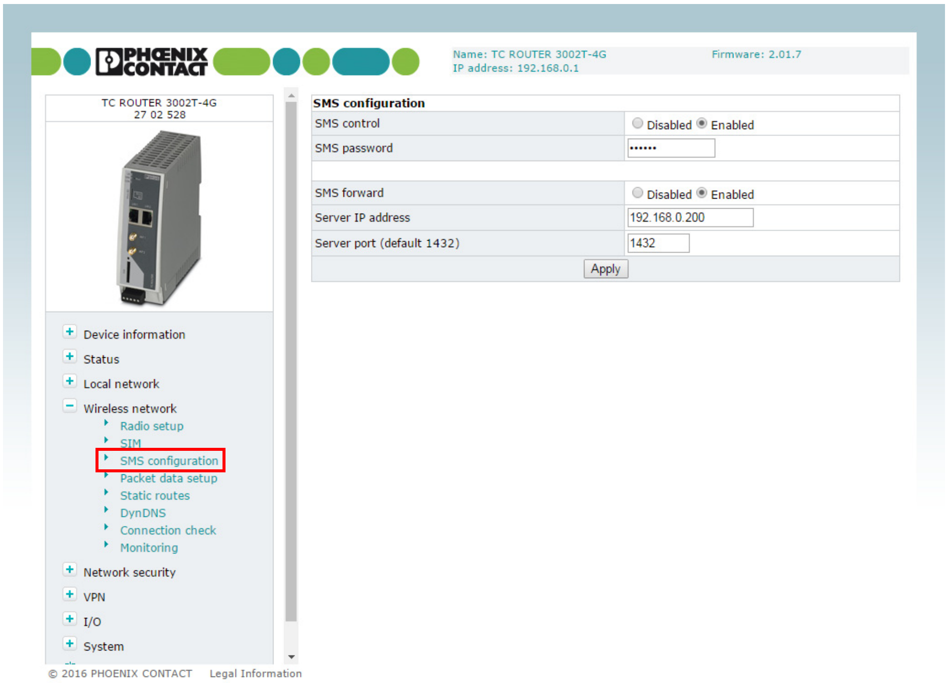
– Additional subcommands

Table 3-1 Supported function commands

Function command	Description
SET:<sub_cmd>	General command for starting functions (ON), must be supplemented with subcommand
CLR:<sub_cmd>	General command for stop functions (OFF), must be supplemented with subcommand
SEND:STATUS	Query status of the mobile router
RESET	Reset alarms
REBOOT	Restart mobile router

Table 3-2 Subcommands <sub_cmd> for the function commands “SET” and “CLR”

Subcommand <sub_cmd>	Description
GPRS	Start or stop packet data connection
OUTPUT	Switch output 1: ON/OFF
OUTPUT:n	Switch output n: ON/OFF, n={1...4}
IPSEC	Start or stop IPsec VPN 1: ON/OFF
IPSEC:n	Start or stop IPsec VPN n: ON/OFF, n={1...3}
OPENVPN	Start or stop VPN 1: ON/OFF
OPENVPN:n	Start or stop VPN n: ON/OFF, n={1...3}



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

SMS configuration

SMS control	○ Disabled ● Enabled
SMS password	••••••
SMS forward	○ Disabled ● Enabled
Server IP address	192.168.0.200
Server port (default 1432)	1432

Figure 3-15 Wireless network, SMS configuration

Wireless network, SMS configuration		
SMS configuration	**SMS control**	– **Disabled**: remote operation of router via SMS not possible – **Enabled**: remote operation of router via SMS activated
	SMS password	SMS password for remote operation
	SMS forward	– **Disabled**: **not** possible to forward SMS messages via Ethernet – **Enabled**: forwarding of SMS messages via Ethernet activated
	Server IP address	IP address to which the SMS message should be forwarded
	Server port (default 1432)	Port to which the SMS message should be forwarded

Example

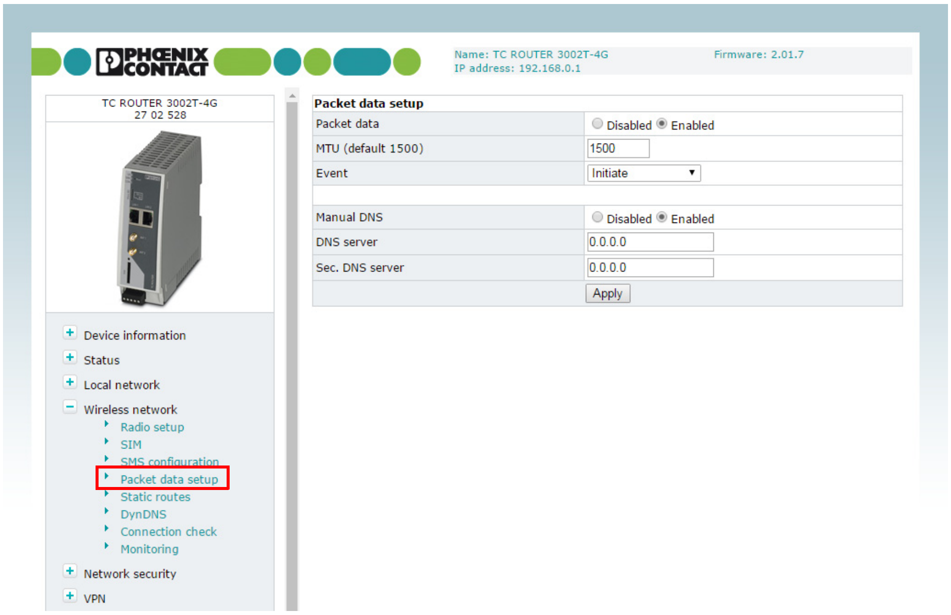
SMS message text for starting IPsec tunnel #2 with the password 1234:

#1234:SET:IPSEC:2

To stop this connection, you must send the following SMS message:

#1234:CLR:IPSEC:2

3.6.4 Packet data setup



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Packet data setup

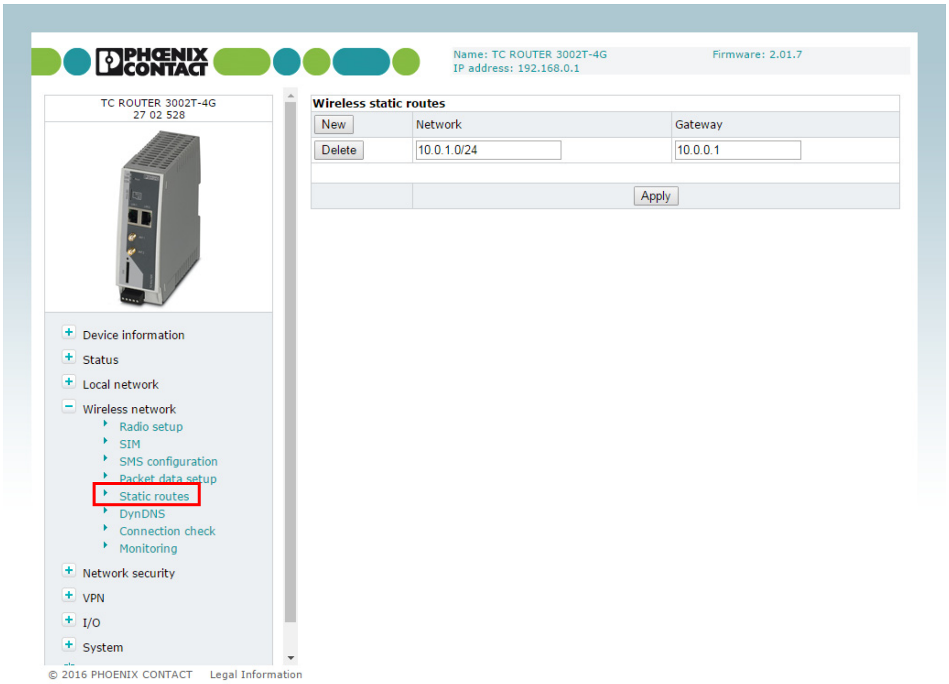
Packet data	○ Disabled ● Enabled
MTU (default 1500)	1500
Event	Initiate
Manual DNS	○ Disabled ● Enabled
DNS server	0.0.0.0
Sec. DNS server	0.0.0.0

Figure 3-16 Wireless network, Packet data setup

Wireless network, Packet data setup		
Packet data setup	**Packet data**	– **Disabled**: packet data connection deactivated – **Enabled**: access enabled to LTE / UMTS / HSPA / GPRS / EDGE If this packet data connection is activated, there is only a virtual permanent connection to the partner. This wireless area is not used until data is actually transmitted, e.g., via VPN tunnel.
	MTU (default 1500)	Maximum Transmission Unit (MTU) is the maximum packet size, in bytes, in the mobile network
	Event	Event that starts the packet data connection: – **Initiate**: automatic start after router boots up – **Initiate on Input #1 ... #2**: manual start via switching input – **Initiate on SMS:** manual start via SMS message – **Initiate on XML:** manual start via XML socket server
	Manual DNS	– **Disabled**: manual DNS setting is deactivated. The DNS settings are received automatically from the provider. – **Enabled**: manual DNS setting is enabled.
	DNS server	IP address of the primary DNS server in the mobile network
	Sec. DNS server	IP address of the alternative DNS server in the mobile network

3.6.5 Wireless static routes (redirection of data packets)

With static routes, you can specify alternative routes for data packets in the mobile network. If the entries for the network and gateway are logically incorrect, the incorrect entries will be displayed with a red frame.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Wireless static routes

New	Network	Gateway
Delete	10.0.1.0/24	10.0.0.1

Figure 3-17 Wireless network, Wireless static routes

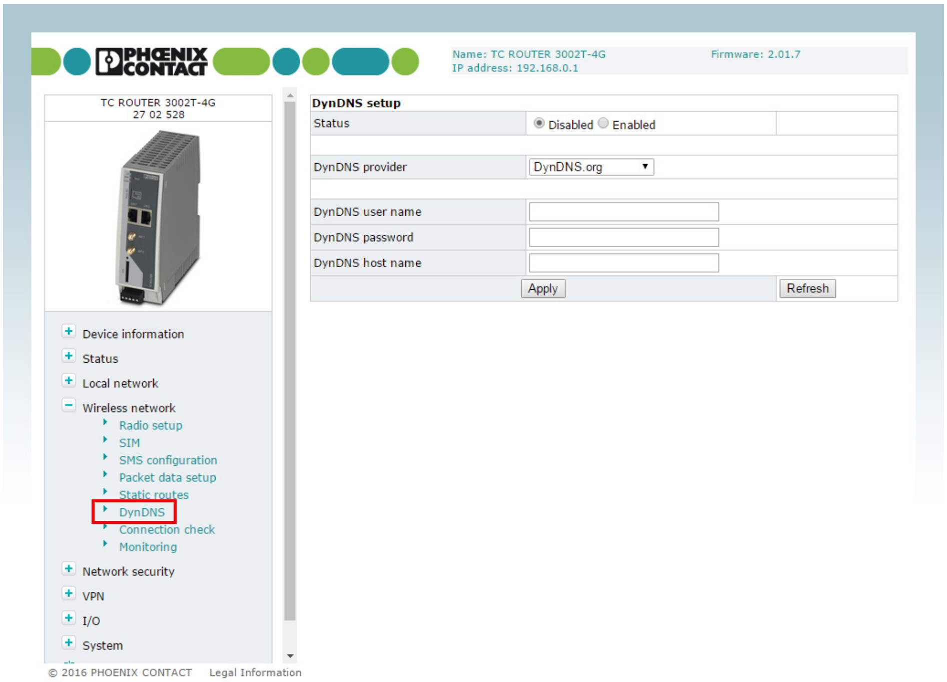
Wireless network, wireless static routes		
Wireless static routes	**Network**	The network in CIDR format, see “CIDR (Classless Inter-Domain Routing)” on page 136
	Gateway	Gateway via which this network can be accessed

3.6.6 DynDNS (address management via dynamic DNS)

Each mobile router is dynamically assigned an IP address by the provider. The address changes from session to session.

If the mobile router is to be accessed via the Internet, you can specify a fixed host name with the help of a DynDNS provider for the dynamic IP address. The router can in the future be accessed via this host name.

> Check whether your mobile network provider supports dynamic DNS in the mobile network.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

DynDNS setup

Status: ● Disabled ○ Enabled

DynDNS provider: DynDNS.org ▾

DynDNS user name:

DynDNS password:

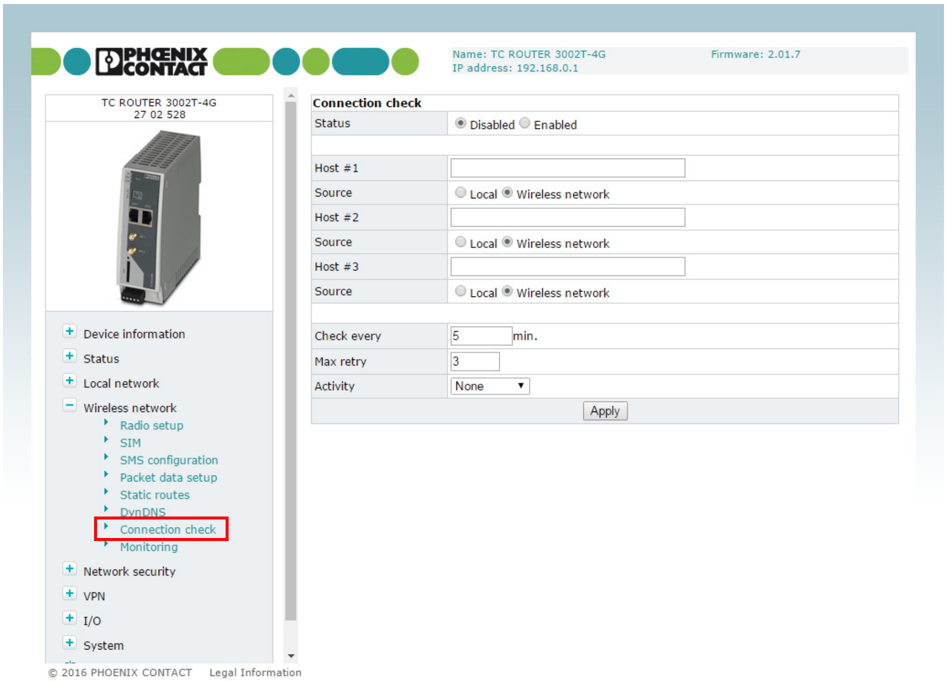
DynDNS host name:

Figure 3-18 Wireless network, DynDNS

Wireless network, DynDNS		
DynDNS setup	**Status**	– **Disabled**: DynDNS client deactivated – **Enabled**: DynDNS client activated
	DynDNS provider	Select the name of the provider with whom you are registered, e.g., DynDNS.org, TZO.com, dhs.org
	DynDNS user name	User name for your DynDNS account
	DynDNS password	Password for your DynDNS account
	DynDNS host name	Host name that was specified for this router with the DynDNS service The router can be accessed via this host name.

3.6.7 Connection check (connection monitoring)

Connection monitoring enables you to check whether the packet data connection in the mobile network is functioning correctly. In order to maintain the packet data connection in the mobile network, connection monitoring also acts as a Keep Alive function.



Connection check	
Status	● Disabled ○ Enabled
Host #1	
Source	○ Local ● Wireless network
Host #2	
Source	○ Local ● Wireless network
Host #3	
Source	○ Local ● Wireless network
Check every	5 min.
Max retry	3
Activity	None

Apply

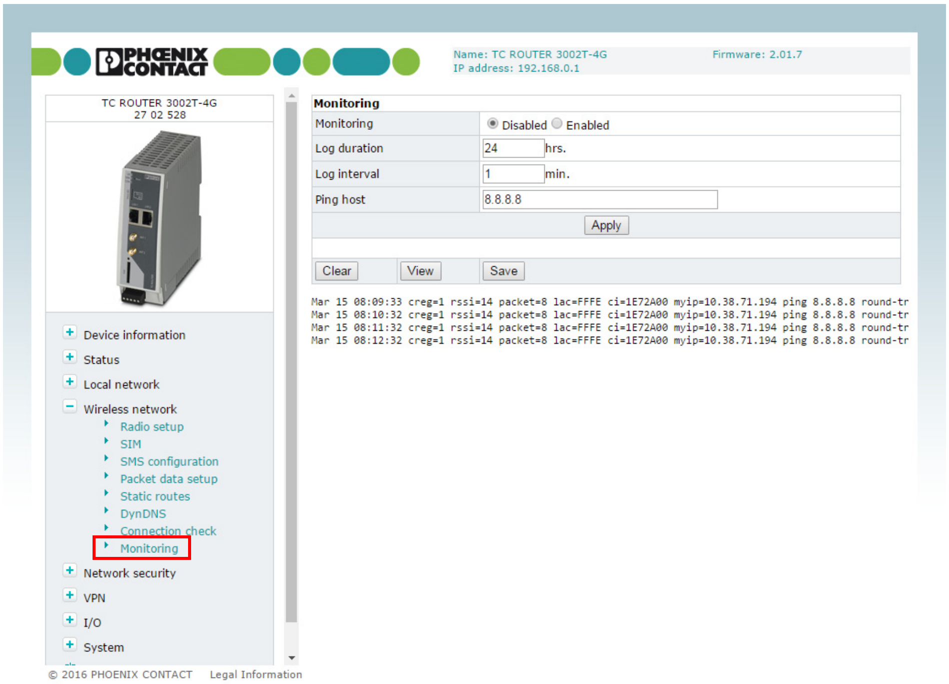
Figure 3-19 Wireless network, Connection check

Wireless network, connection check		
Connection check	**Status**	– **Disabled**: connection monitoring of the packet data connection is deactivated (default) – **Enabled**: connection monitoring of the packet data connection is activated
	Host #1 ... #3	IP address or host name of the reference point for connection monitoring
	Source	– **Local:** the local network interface sends the connection monitoring IP packets with the IP address of the local interface (LAN). – **Wireless network:** the mobile network interface sends the connection monitoring IP packets with the IP address assigned by the provider.
	Check every	Check interval in minutes
	Max. retry	Number of times to retry until the configured action is performed

Wireless network, connection check [...]		
	Activity	– **Reboot**: restart router – **Reconnect**: re-establish packet data connection – **Relogin**: shut down mobile network interface and restart by logging into the mobile network again. – **None**: no action As an option, you can configure information regarding the status of connection monitoring via a switching output.

3.6.8 Monitoring

Monitoring records mobile network parameters. You can use the function **temporarily** for startup or troubleshooting. The function is not intended for permanent use. All parameters are stored in a separate log file: “logradio.txt”. At the end of the monitoring period, monitoring must be disabled.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

Monitoring

Monitoring: ● Disabled ○ Enabled

Log duration: 24 hrs.

Log interval: 1 min.

Ping host: 8.8.8.8

Apply

Clear | View | Save

```
Mar 15 08:09:33 creg=1 rssi=14 packet=8 lac=FFFE ci=1E72A00 myip=10.38.71.194 ping 8.8.8.8 round-tr
Mar 15 08:10:32 creg=1 rssi=14 packet=8 lac=FFFE ci=1E72A00 myip=10.38.71.194 ping 8.8.8.8 round-tr
Mar 15 08:11:32 creg=1 rssi=14 packet=8 lac=FFFE ci=1E72A00 myip=10.38.71.194 ping 8.8.8.8 round-tr
Mar 15 08:12:32 creg=1 rssi=14 packet=8 lac=FFFE ci=1E72A00 myip=10.38.71.194 ping 8.8.8.8 round-tr
```

Figure 3-20 Wireless network, Monitoring

Wireless network, Monitoring		
Monitoring	**Monitoring**	– **Disabled**: mobile network monitoring deactivated (default) – **Enabled**: mobile network monitoring activated
	Log duration	Monitoring duration in hours, we recommend a maximum of 30 hours
	Log interval	Monitoring interval in minutes (at least one minute)
	Ping host	IP address or host name of the reference point for monitoring
	Clear	Clear log file in the router for a new monitoring session
	View	View current log file
	Save	Save log file on local computer

Structure of the “logradio.txt” log file:

Date and time

Network status	creg=
0	Not logged in, not searching for cellular network
1	Logged in, home network
2	Not logged in, searching for cellular network
3	Not logged in, login rejected
4	Status unknown
5	Logged in, external network

Reception strength	rssi=
0	-113 dBm or worse
1	-111 dBm
2...30	-109 dBm ... -53 dBm
31	-51 dBm or better

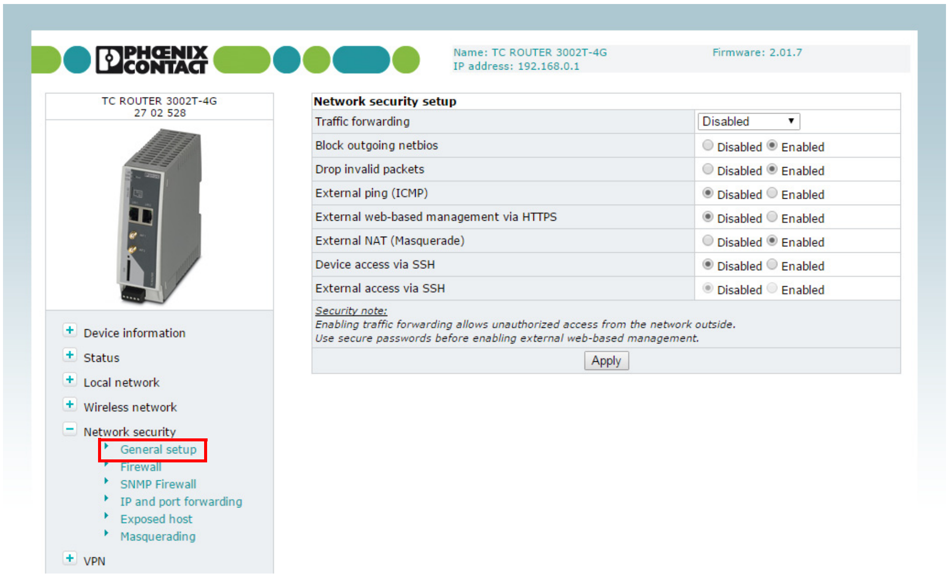
Packet data connection	packet=
0	OFFLINE
1	ONLINE
2	GPRS ONLINE
3	EDGE ONLINE
4	WCDMA ONLINE
5	WCDMA HSDPA ONLINE
6	WCDMA HSUPA ONLINE
7	WCDMA HSDPA+HSUPA ONLINE
8	LTE ONLINE

Location	lac= Location Area Code
	ci= mobile phone cell ID
Current own IP address	myip=
Reference IP	ping=
Ping times in msd	round-trip min/avg/max= (minimum/average/maximum)

3.7 Network security (security settings)

3.7.1 General setup

General settings for network security can be made on this page.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

Network security setup	
Traffic forwarding	Disabled ▾
Block outgoing netbios	○ Disabled ● Enabled
Drop invalid packets	○ Disabled ● Enabled
External ping (ICMP)	● Disabled ○ Enabled
External web-based management via HTTPS	● Disabled ○ Enabled
External NAT (Masquerade)	○ Disabled ● Enabled
Device access via SSH	● Disabled ○ Enabled
External access via SSH	● Disabled ○ Enabled

Security note:
Enabling traffic forwarding allows unauthorized access from the network outside.
Use secure passwords before enabling external web-based management.

Apply

Figure 3-21 Network security, General setup

Network security, general setup		
Network security setup	**Traffic forwarding**	– **Disabled:** port forwarding from the mobile network to the local network is deactivated (default) – **Port forwarding:** port forwarding from the mobile network to the local network is activated – **Exposed host:** forwarding of all data traffic from the mobile network to an Ethernet device in the local network is activated. This access **cannot** be restricted via the firewall in the mobile router.
	Block outgoing netbios	If Windows-based systems are installed in the local network, NetBIOS requests can result in data traffic and the associated costs, where applicable. – **Disabled**: outgoing NetBIOS requests are permitted. – **Enabled**: outgoing NetBIOS requests are blocked (default).
	Drop invalid packets	The firewall of the mobile router can filter and drop invalid or damaged IP packets. – **Disabled**: invalid IP packets are also sent. – **Enabled**: invalid IP packets are dropped (default).

Network security, general setup [...]		
	External ping (ICMP)	A ping can be used to check whether a device in an IP network can be accessed. During normal operation, responding to external ping requests results in data traffic and its associated costs, where applicable. – **Disabled**: if a ping request is sent from the external IP network to the router, it is ignored (default). – **Enabled**: if a ping request is sent from the external IP network to the router, it is sent back.
	External web-based management via HTTPS	Select whether the router may be configured via the mobile network or the external network using the web-based management (WBM). – **Disabled**: external configuration via WBM is not possible. Set this option if you wish to configure and maintain the router locally (default). – **Enabled**: the router can be configured externally via WBM. Remote maintenance of the router is therefore possible. The router can be accessed from any external IP address. Access **cannot** be restricted via the firewall.
	External NAT (Masquerade)	For outgoing data packets, the router can rewrite the specified sender IP addresses from its internal network to its own external address. This method is used if the internal addresses cannot be routed externally. This is the case, for example, if a private address area such as 192.168.x.x is used. This method is referred to as IP masquerading. – **Disabled**: IP masquerading is deactivated – **Enabled**: IP masquerading is activated. You can communicate via the Internet from a private, local network (default).
	Device access via SSH	This option can be used to specify whether the router can be accessed via the SSH service. – **Disabled:** the SSH service is not available. No access to the router via SSH (default). – **Enabled:** access to the router via the SSH service is possible, from the local network or via a VPN tunnel.
	External access via SSH	This option can be used to specify whether the router can be accessed via the mobile network or the external network via the SSH service. – **Disabled:** the SSH service is not available. No external access to the router via SSH (default) – **Enabled:** external access to the router via the SSH service is possible, from the local network or via a VPN tunnel.

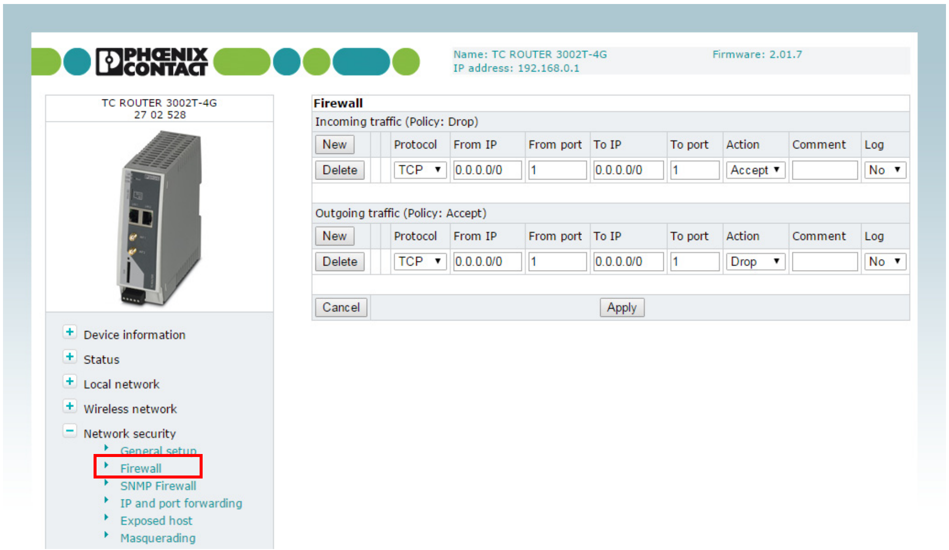
3.7.2 Firewall (definition of firewall rules)

The device includes a stateful packet inspection firewall. The connection data of an active connection is recorded in a database (connection tracking). Rules therefore only have to be defined for one direction. This means that data from the other direction of the relevant connection, and only this data, is automatically allowed through.

The firewall is active by default upon delivery. It blocks incoming data traffic and only permits outgoing data traffic.

> If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied.
>
> If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

The device supports a maximum of 32 rules for incoming data traffic and 32 rules for outgoing data traffic.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Firewall

Incoming traffic (Policy: Drop)

	Protocol	From IP	From port	To IP	To port	Action	Comment	Log
New								
Delete	TCP	0.0.0.0/0	1	0.0.0.0/0	1	Accept		No

Outgoing traffic (Policy: Accept)

	Protocol	From IP	From port	To IP	To port	Action	Comment	Log
New								
Delete	TCP	0.0.0.0/0	1	0.0.0.0/0	1	Drop		No

Cancel Apply

Figure 3-22 Network security, Firewall

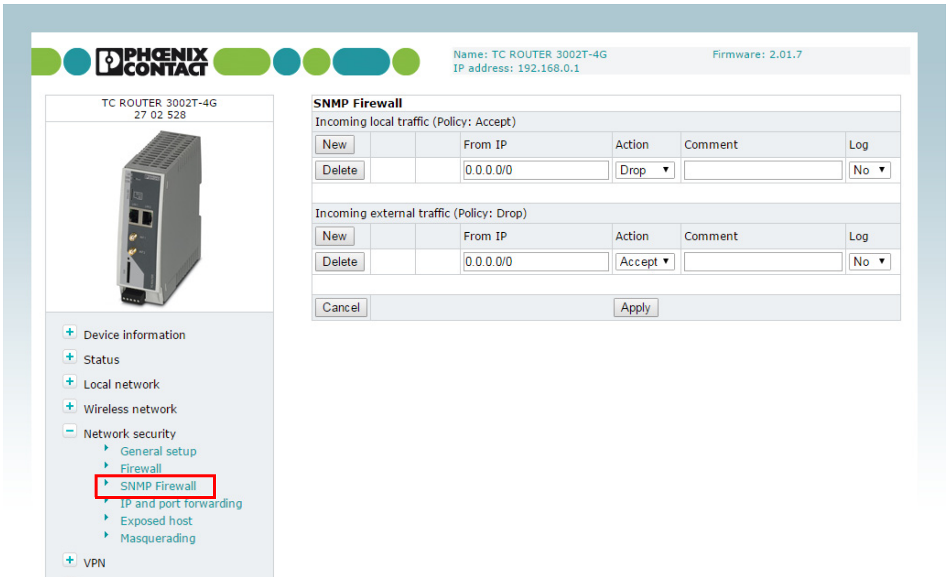
Network security, firewall		
Firewall	Lists the firewall rules that have been set up. They apply for incoming data links that have been initiated externally.	
Incoming traffic	**Protocol**	TCP, UDP, ICMP, all
	From IP / To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 136).
	From port / To port	(Only evaluated for TCP and UDP protocols) – **any:** any port – **startport-endport:** a port range (e.g., 110 ... 120)

Network security, firewall [...]		
	Action	– **Accept**: the data packets may pass through. – **Reject**: the data packets are sent back. The sender is informed of their rejection. – **Drop**: the data packets are blocked. They are discarded, which means that the sender is not informed of their whereabouts.
	Log	For each individual firewall rule you can specify whether the event is to be logged if the rule is applied. – **Yes:** event is logged. – **No:** event is not logged (default).
	New	– **New**: add a new firewall rule below the last rule. – **Delete:** delete rule from the table. The arrows can be used to move the respective rule one row up/down.
Outgoing traffic	Lists the firewall rules that have been set up. They apply for outgoing data links that have been initiated internally in order to communicate with a remote peer. **Default:** a rule is defined by default that allows all outgoing connections. If no rule is defined, all outgoing connections are prohibited (excluding VPN).	
	Protocol	TCP, UDP, ICMP, all
	From IP / To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 136).
	From port / To port	(Only evaluated for TCP and UDP protocols) – **any:** any port – **startport-endport:** a port range (e.g., 110 ... 120)
	Action	– **Accept**: the data packets may pass through. – **Reject**: the data packets are sent back. The sender is informed of their rejection. – **Drop**: the data packets are blocked. They are discarded, which means that the sender is not informed of their whereabouts.
	Log	For each individual firewall rule you can specify whether the event is to be logged if the rule is applied. – **Yes:** event is logged. – **No:** event is not logged (default).
	New	– **New**: add a new firewall rule below the last rule. – **Delete:** delete rule from the table. The arrows can be used to move the respective rule one row up/down.

3.7.3 SNMP Firewall

The device has an additional firewall for SNMP connections. It can be used to restrict SNMP access. The firewall is active by default upon delivery. It blocks external access (incoming external traffic) and only allows access from the local network (incoming local traffic).

The device supports a maximum of 32 rules for local access and 32 rules for external access.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

SNMP Firewall

Incoming local traffic (Policy: Accept)

New		From IP	Action	Comment	Log
Delete		0.0.0.0/0	Drop ▼		No ▼

Incoming external traffic (Policy: Drop)

New		From IP	Action	Comment	Log
Delete		0.0.0.0/0	Accept ▼		No ▼

Cancel Apply

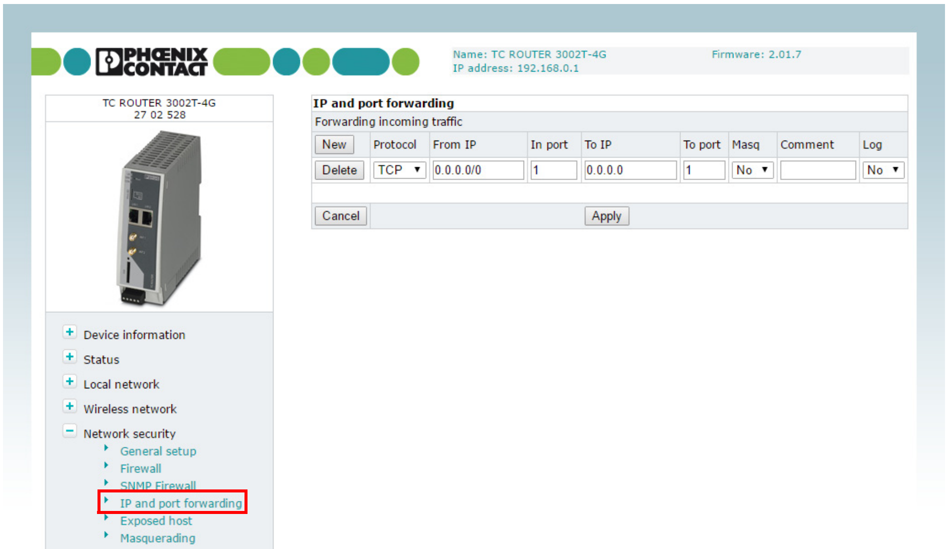
Figure 3-23 Network security, SNMP Firewall

Network security, SNMP Firewall		
SNMP Firewall	**From IP**	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 136).
	Action	– **Accept**: the data packets may pass through. – **Reject**: the data packets are sent back. The sender is informed of their rejection. – **Drop**: the data packets are blocked. They are discarded, which means that the sender is not informed of their whereabouts.
	Log	For each individual firewall rule you can specify whether the event is to be logged if the rule is applied. – **Yes**: event is logged. – **No**: event is not logged (default).

3.7.4 IP and port forwarding (port forwarding setup)

The table contains the rules defined for IP and port forwarding. The device has one IP address, which can be used to access the device externally. For incoming data packets, the device can convert the specified sender IP addresses to internal addresses. This technique is referred to as NAT (Network Address Translation). Using the port number, the data packets can be redirected to the ports of internal IP addresses.

The device supports a maximum of 32 rules for port forwarding.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

IP and port forwarding

Forwarding incoming traffic

New	Protocol	From IP	In port	To IP	To port	Masq	Comment	Log
Delete	TCP ▾	0.0.0.0/0	1	0.0.0.0	1	No ▾		No ▾

Cancel Apply

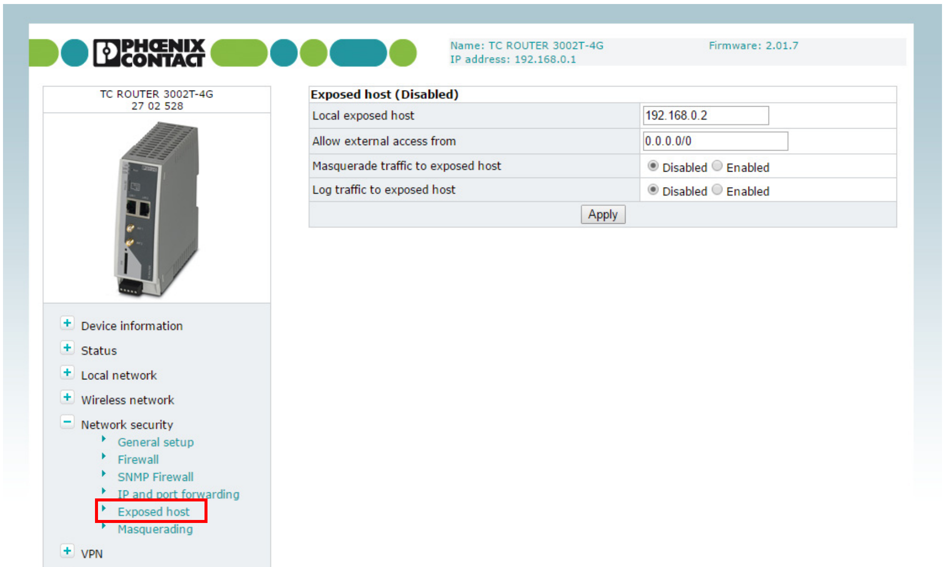
Figure 3-24 Network security, IP and port forwarding

Network security, IP and port forwarding		
IP and port forwarding	**Protocol**	TCP, UDP, ICMP
	From IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 136).
	In port / To port	Only evaluated for TCP and UDP protocols – **any:** any port – **startport-endport:** a port range (e.g., 110 ... 120)
	To IP	IP address from the local network, incoming packets are forwarded to this address
	Masq	For each individual rule you can specify whether IP masquerading is to be used. – **Yes**: IP masquerading is activated, incoming packets from the Internet are given the IP address of the router. A response via the Internet is possible, even without a default gateway. – **No**: a response via the Internet is only possible with the default gateway (default).

Network security, IP and port forwarding [...]		
	Log	For each individual rule, you can specify whether the event is to be logged if the rule is applied. – **Yes:** event is logged. – **No:** event is not logged (default).
	New	– **New**: add a new firewall rule below the last rule. – **Delete:** delete rule from the table. The arrows can be used to move the rule one row up or down.

3.7.5 Exposed host (server setup)

With this function, the router forwards all received external packets that do not belong to an existing connection to an IP address in the LAN. The device can therefore be accessed directly from the Internet as an “exposed host”. You can use the device as a server.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Exposed host (Disabled)	
Local exposed host	192.168.0.2
Allow external access from	0.0.0.0/0
Masquerade traffic to exposed host	● Disabled ○ Enabled
Log traffic to exposed host	● Disabled ○ Enabled

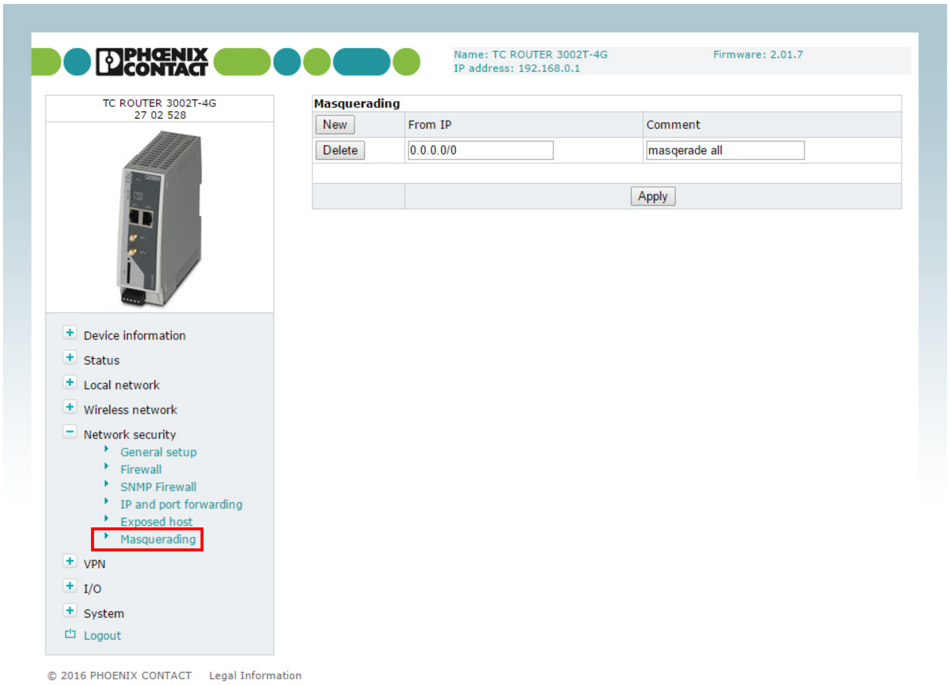
Figure 3-25 Network security, Exposed host

Network security, exposed host		
Exposed host	**Local exposed host**	IP address of the exposed host (server)
	Allow external access from	IP addresses for incoming data links **0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 136).
	Masquerade traffic to exposed host	Specify whether IP masquerading is to be used. – **Enabled**: IP masquerading is activated, incoming packets from the Internet are given the IP address of the router. A response via the Internet is possible, even without a default gateway. – **Disabled**: a response via the Internet is only possible with the default gateway (default).
	Log traffic to exposed host	Specify whether IP connections are logged. – **Enabled**: IP connections are logged. – **Disabled:** IP connections are not logged (default).

3.7.6 Masquerading

For certain networks you can specify whether IP masquerading is to be used. If IP masquerading is activated, all incoming packets from the Internet are given the IP address of the router. The response in the configured networks is possible even without a default gateway.

The device supports a maximum of 16 rules for IP masquerading.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Masquerading

	From IP	Comment
New		
Delete	0.0.0.0/0	masqerade all

© 2016 PHOENIX CONTACT Legal Information

Figure 3-26 Network security, Masquerading

Network security, masquerading		
Masquerading	**From IP**	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 136).

3.8 VPN

Requirements for a VPN connection

A general requirement for a VPN connection is that the IP addresses of the VPN partners are known and can be accessed. The device supports up to three IPsec connections and up to two OpenVPN connections. When a VPN connection is active, the VPN LED on the device is illuminated.

In order to successfully establish an IPsec connection, the VPN peer must support IPsec with the following configuration:

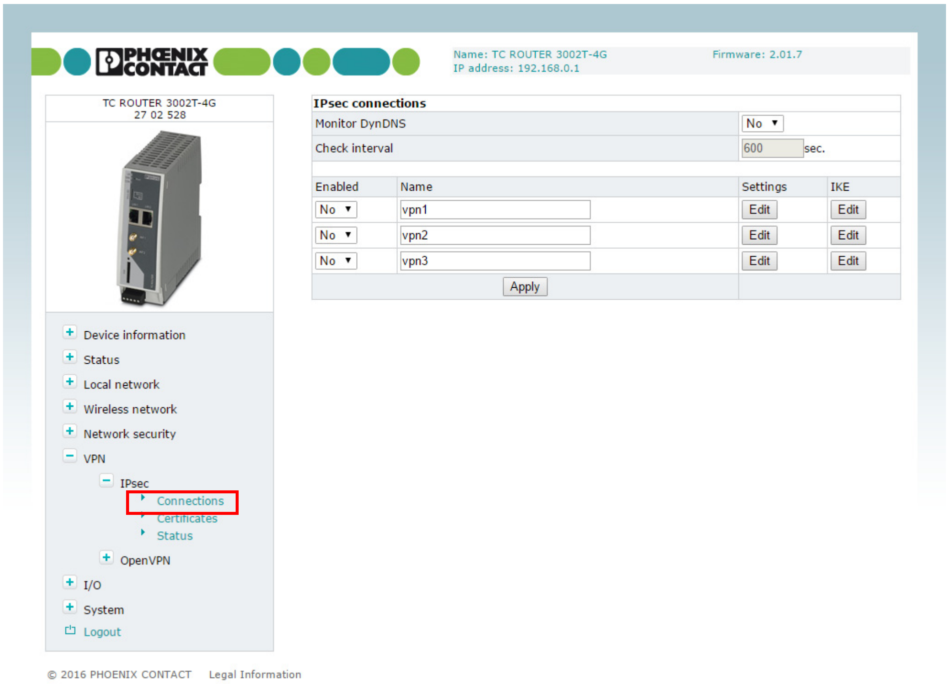
- Authentication via X.509 certificate or pre-shared secret key (PSK)
- Diffie-Hellman group 2 or 5
- 3DES or AES encryption
- MD5 or SHA-1 hash algorithms
- Tunnel mode
- Quick mode
- Main mode
- SA lifetime (one second to 24 hours)

The following functions are supported for OpenVPN connections:

- OpenVPN Client
- TUN device
- Authentication via X.509 certificate or pre-shared secret key (PSK)
- Static key
- TCP and UDP transmission protocol
- Keep Alive

3.8.1 IPsec connections (IPsec connection setup)

IPsec (Internet Protocol Security) is a secure VPN standard that is used for communication via IP networks.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

IPsec connections

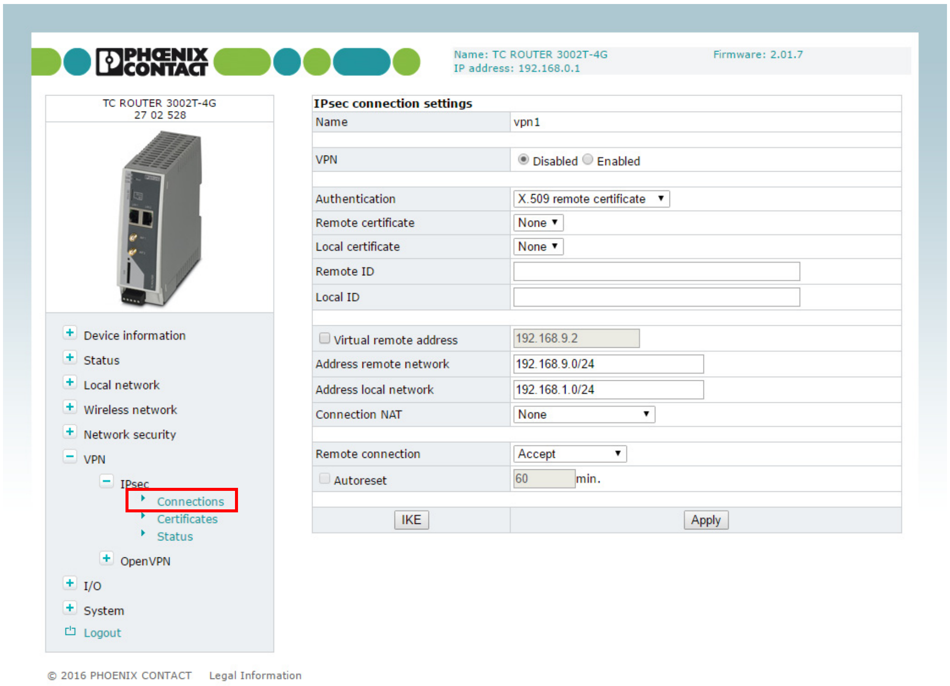
Monitor DynDNS	No ▾
Check interval	600 sec.

Enabled	Name	Settings	IKE
No ▾	vpn1	Edit	Edit
No ▾	vpn2	Edit	Edit
No ▾	vpn3	Edit	Edit

Figure 3-27 VPN, IPsec, Connections

VPN, IPsec, Connections		
IPsec connections	**Monitor DynDNS**	Activate this function to check accessibility. – If the VPN peer does not have a fixed IP address – if a DynDNS name is used as the “Remote host”.
	Check interval	Enter the check interval in seconds.
	Enabled	– **Yes:** VPN connection activated – **No**: VPN connection deactivated
	Name	Assign a descriptive name to each VPN connection. The VPN connection can be freely named or renamed.
	Settings	Click on **Edit** to specify the settings for IPsec (see Page 54).
	IKE	Internet Key Exchange protocol for automatic key management for IPsec Click on **Edit** to specify the settings for IKE (see Page 58).

Settings, Edit



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

IPsec connection settings	
Name	vpn1
VPN	● Disabled ○ Enabled
Authentication	X.509 remote certificate ▾
Remote certificate	None ▾
Local certificate	None ▾
Remote ID	
Local ID	
□ Virtual remote address	192.168.9.2
Address remote network	192.168.9.0/24
Address local network	192.168.1.0/24
Connection NAT	None ▾
Remote connection	Accept ▾
□ Autoreset	60 min.

Figure 3-28 VPN, IPsec, Connections, Settings, Edit

VPN, IPsec, Connections, Settings, Edit		
IPsec connection settings	**Name**	Name of the VPN connection entered under “IPsec connections“
	VPN	– **Yes:** VPN connection activated – **No**: VPN connection deactivated
	Remote host	IP address or URL of the peer to which (or from which) the tunnel will be created. “Remote host” is only used if “Initiate” has been selected under “Remote connection” (the router establishes the connection). If “Remote connection” is set to “Accept”, the value “%any” is set internally for “Remote host”. It therefore waits for a connection.

VPN, IPsec, Connections, Settings, Edit [...]

Authentication

X.509 remote certificate: authentication method with X.509 certificate

With the X.509 certificate option, each VPN device has a private secret key and a public key. The certificate contains additional information about the certificate's owner and the certification authority (CA).

> The procedure for creating an X.509 certificate is described in Section “Creating certificates” on page 101.

Preshared secret key (PSK): authentication method

With a preshared secret key, each VPN device knows one shared private key, one password. Enter this shared key in the “Preshared Secret Key” field.

Remote certificate

Certificate the router uses to authenticate the VPN peer (remote certificate, .pem).

The selection list contains the certificates that have been loaded on the router (see “IPsec certificates (certificate upload)” on page 60).

Local certificate

Certificate used by the router to authenticate itself to the VPN peer (machine certificate, PKCS#12)

The selection list contains the certificates that have been loaded on the router (see “IPsec certificates (certificate upload)” on page 60).

Remote ID

Default: empty field

The **Remote ID** can be used to specify the name the router uses to identify itself to the partner. The name must match the data in the router certificate. If the field is left empty, the data from the certificate is used.

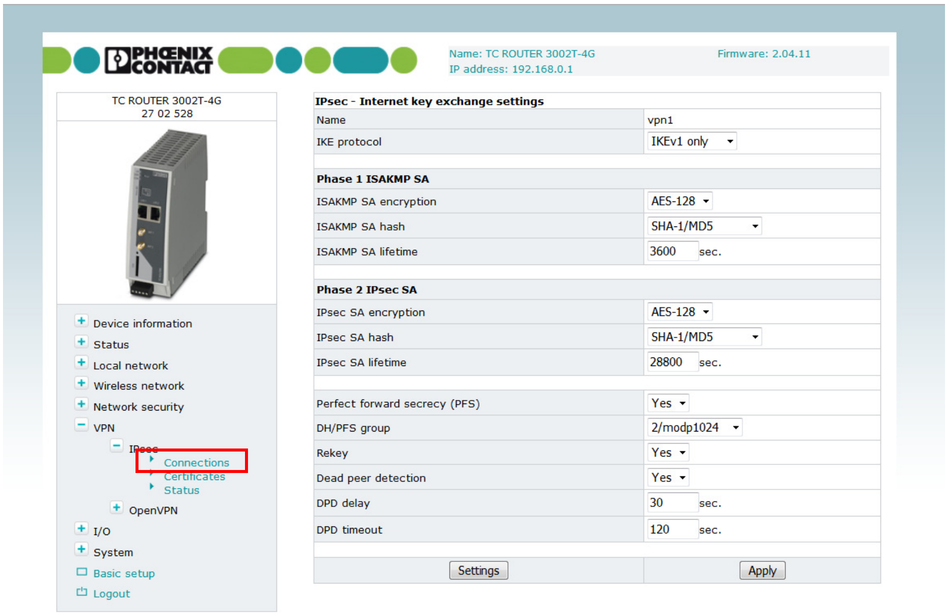
Valid values:

- No entry (default). The “Subject” entry (previously Distinguished Name) in the certificate is used.
- Subject entry in the certificate
- One of the “Subject Alternative Names”, if they are listed in the certificate. If the certificate contains “Subject Alternative Names”, these are specified under “Valid values”. These can include IP addresses, host names with “@” prefix or e-mail addresses, for example.

VPN, IPsec, Connections, Settings, Edit [...]		
	Local ID	Default: empty field The “Local ID” can be used to specify the name the router uses to identify itself to the peer. For additional information, see “Remote ID“.
	Virtual remote address	Virtual address of software VPN clients that are to establish the VPN connection. If your software VPN client requires this virtual address, activate this function.
	Address remote network	IP address/subnet mask of the remote network to which the VPN connection is to be established
	Address local network	IP address/subnet mask of the local network Specify the address of the network or computer which is connected locally to the router here. – “NAT to local network” set to “None” (default) Actual IP address or subnet mask of the local network. Specify the address of the network that is connected locally to the router here. – “Local 1:1 NAT” and “Remote masquerading” activated This virtual IP address/subnet mask enables the IP addresses for the remote network to be accessed through the VPN tunnel. You must enter the same settings as the remote network on the remote VPN router.
	Connection NAT	– **None:** no NAT within the VPN tunnel (default) – **Local 1:1 NAT:** virtual IP addresses are used for communication via a VPN tunnel. These addresses are linked to the real IP addresses for the set network that has been connected. The subnet mask remains unchanged. – **Remote masquerading:** as with “Local 1:1 NAT”, virtual IP addresses are used for communication via a VPN tunnel. In addition, the sender IP address (source IP) is replaced with the IP address of the router for all incoming packets via a VPN tunnel. Devices in the local network that cannot use a default gateway can therefore be accessed via a VPN tunnel.
	NAT to local network	Enter the real IP address area for the local network here. Using this address area, the local network can be accessed from the remote network via 1:1 NAT. You can use this function, for example, to access two machines with the same IP address via a VPN tunnel.

VPN, IPsec, Connections, Settings, Edit [...]		
	Remote connection	Side from which the connection can be established – **Initiate:** VPN connection is started by the router. – **Accept:** VPN connection is initiated by the peer. Additional settings: – **Initiate on Input...:** VPN tunnel is started or stopped via a digital input. – **Initiate on SMS:** VPN tunnel is started via SMS. You must also specify the number of minutes until the VPN tunnel is to be stopped via Autoreset. – **Initiate on call:** VPN tunnel is started via a call. You must also specify the number of minutes until the VPN tunnel is to be stopped via Autoreset. – **Initiate on XML:** VPN tunnel is started or stopped via an XML command via socket server.

IKE, Edit



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.04.11

IPsec - Internet key exchange settings	
Name	vpn1
IKE protocol	IKEv1 only
Phase 1 ISAKMP SA	
ISAKMP SA encryption	AES-128
ISAKMP SA hash	SHA-1/MD5
ISAKMP SA lifetime	3600 sec.
Phase 2 IPsec SA	
IPsec SA encryption	AES-128
IPsec SA hash	SHA-1/MD5
IPsec SA lifetime	28800 sec.
Perfect forward secrecy (PFS)	Yes
DH/PFS group	2/modp1024
Rekey	Yes
Dead peer detection	Yes
DPD delay	30 sec.
DPD timeout	120 sec.

Figure 3-29 VPN, IPsec, Connections, IKE, Edit

VPN, IPsec, Connections, IKE, Edit		
IPsec - Internet Key Exchange settings	**Name**	Name of the VPN connection entered under "“IPsec connections“
	IKE protocol	Select an IKE version. – **initiate IKEv2:** IKEv2 is preferred. A switch back to IKEv1 takes place in case of an erroneous connection attempt.
Phase 1 ISAKMP SA Key exchange	**ISAKMP SA encryption**	Encryption algorithm Internet Security Association and Key Management Protocol (ISAKMP) is a protocol for creating Security Associations (SA) and exchanging keys on the Internet. **AES128** is preset as default. The following generally applies: the more bits an encryption algorithm has (specified by the appended number), the more secure it is. The relatively new **AES-256** method is therefore the most secure, however it is still not used that widely. The longer the key, the more time-consuming the encryption procedure.
	ISAKMP SA hash	Leave this set to **SHA-1/MD5**. It then does not matter whether the peer works with **MD5** or **SHA-1**.

VPN, IPsec, Connections, IKE, Edit [...]		
	ISAKMP SA lifetime	The keys of an IPsec connection are renewed at defined intervals in order to increase the difficulty of an attack on an IPsec connection. ISAKMP SA lifetime: lifetime in seconds of the keys agreed for ISAKMP SA. Default: 3600 seconds (1 hour) The maximum lifetime is 86400 seconds (24 hours).
Phase 2 IPsec SA Data exchange		In contrast to Phase 1 ISAKMP SA (key exchange), the procedure for data exchange is defined here. It does not necessarily have to differ from the procedure defined for key exchange.
	IPsec SA encryption	See “ISAKMP SA encryption“
	IPsec SA hash	See “ISAKMP SA encryption“
	IPsec SA lifetime	Lifetime in seconds of the keys agreed for IPsec SA Default: 28800 seconds (8 hours) The maximum lifetime is 86400 seconds (24 hours).
	Perfect forward secrecy (PFS)	– **Yes**: PFS activated – **No**: PFS deactivated
	DH/PFS group	Key exchange procedure, defined in RFC 3526 – More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) Perfect Forward Secrecy (PFS): method for providing increased security during data transmission. With IPsec, the keys for data exchange are renewed at defined intervals. With PFS, new random numbers are negotiated with the peer instead of being derived from previously agreed random numbers. **5/modp1536 – 2/modp1024** The following generally applies: the more bits an encryption algorithm has (specified by the appended number), the more secure it is. The longer the key, the more time-consuming the encryption procedure.
	Dead peer detection	If the peer supports the Dead Peer Detection (DPD) protocol, the relevant peers can detect whether or not the IPsec connection is still valid and whether it needs to be established again. Behavior in the event that the IPsec connection is aborted: – **Off**: no DPD – **On**: DPD activated – in “Restart” mode for VPN Initiate – in “Clear” mode for VPN Accept

VPN, IPsec, Connections, IKE, Edit [...]		
	DPD delay	Delay between requests for a sign of life Duration in seconds after which DPD Keep Alive requests should be transmitted. These requests test whether the peer is still available. Default: 30 seconds
	DPD timeout	Duration after which the connection to the peer should be declared dead if there has been no response to the Keep Alive requests. Default: 120 seconds.

3.8.2 IPsec certificates (certificate upload)

A certificate that has been loaded on the router is used to authenticate the router at the peer. The certificate acts as an ID card for the router, which it shows to the relevant peer.

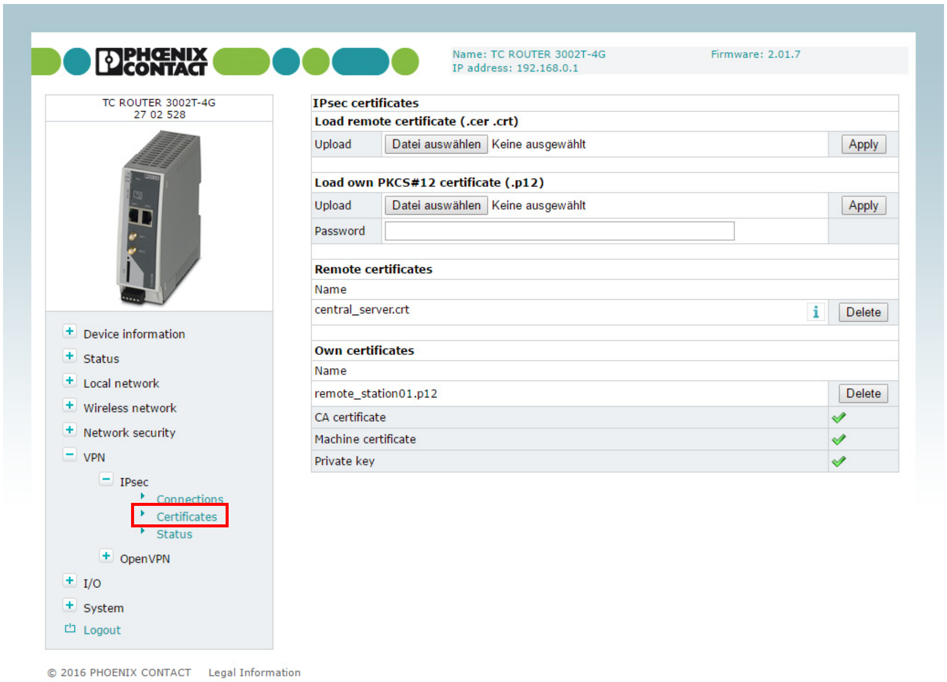
> The procedure for creating an X.509 certificate is described under "CIDR (Classless Inter-Domain Routing)" on page 136.

There are various types of certificate:

- Remote or peer certificates contain the public key used to decode the encrypted data.
- Own or machine certificates contain the private key used to encrypt the data. The private key is kept private. A PKCS#12 file is therefore protected by a password.
- The CA certificate or root certificate is the "mother of all certificates used". It is used to check the validity of the certificates.

By importing a PKCS#12 file, the router is provided with a private key and the corresponding certificate. You can load several PKCS#12 files on the router. This enables the router to show the desired machine certificate to the peer for various connections. This can be a self-signed or CA-signed machine certificate.

To use a certificate that is installed, the certificate must be assigned under "VPN, IPsec, Connections, Settings, Edit". Click on "Apply" to load the certificate onto the router.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

IPsec certificates

Load remote certificate (.cer .crt)

Upload	Datei auswählen Keine ausgewählt	Apply

Load own PKCS#12 certificate (.p12)

Upload	Datei auswählen Keine ausgewählt	Apply
Password		

Remote certificates

Name		
central_server.crt	i	Delete

Own certificates

Name	
remote_station01.p12	Delete
CA certificate	✓
Machine certificate	✓
Private key	✓

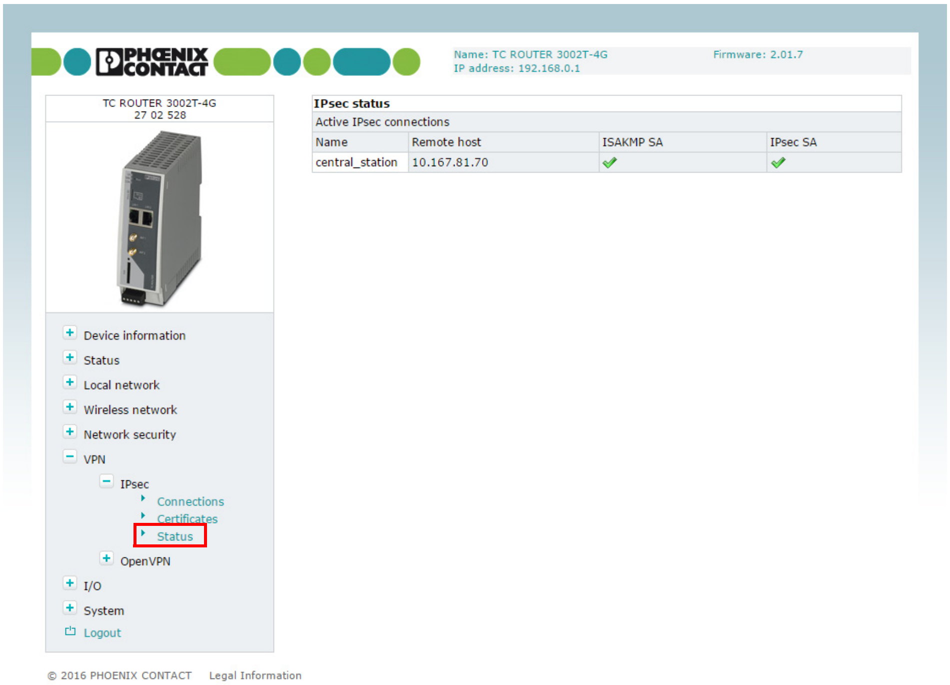
© 2016 PHOENIX CONTACT Legal Information

Figure 3-30 VPN, IPsec, Certificates

VPN, IPsec, Certificates		
IPsec certificates	**Load remote certificate (.cer .crt)**	Here you can upload certificates which the router can use for authentication with the VPN peer. The procedure for creating an X.509 certificate is described under Section 4.5, “Creating certificates”. – **Upload:** import certificate. Click on the “Browse” button to select the certificate to be imported. Under **“VPN, IPsec, Connections, Settings, Edit“**, one of the certificates listed under “Remote certificate“ or “Local certificate“ can be assigned to each VPN connection.
	Load own PKCS#12 certificate (.p12)	**Upload:** import the certificate you have received from your provider. The file must be in PKCS#12 format. Click on the “Browse” button to select the certificate to be imported. Under **“VPN, IPsec, Connections, Settings, Edit“**, one of the certificates listed under “Remote certificate“ or “Local certificate“ can be assigned to each VPN connection. **Password:** password used to protect the private key of the PKCS#12 file. The password is assigned when the key is exported.

VPN, IPsec, Certificates [...]		
	Remote certificates	Overview of the imported .cer/.crt certificates of the peers
		Click on “Delete” to delete a certificate.
	Own certificates	Overview of own imported PKCS#12 certificates
		Click on “Delete” to delete a certificate.
		The green ticks indicate whether the PKCS#12 file contains a CA certificate, a machine certificate or a private key.

3.8.3 IPsec status (status of the VPN connection)



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

IPsec status

Active IPsec connections

Name	Remote host	ISAKMP SA	IPsec SA
central_station	10.167.81.70	✓	✓

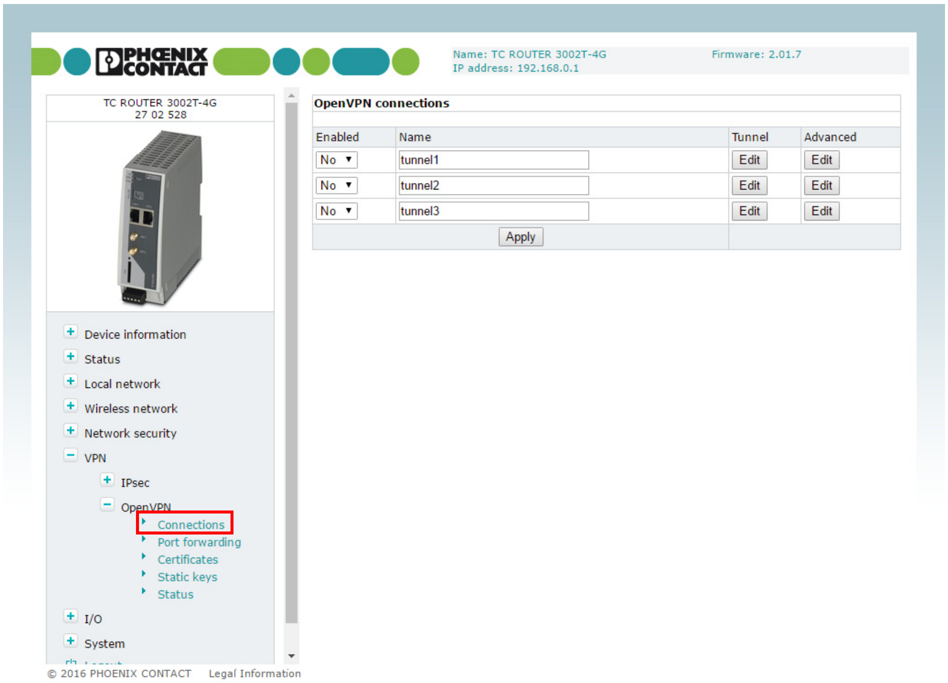
© 2016 PHOENIX CONTACT Legal Information

Figure 3-31 VPN, IPsec, Status

VPN, IPsec, Status		
IPsec status	**Active IPsec connections**	Status of the active VPN connection

3.8.4 OpenVPN connections (OpenVPN connection setup)

OpenVPN is a program for creating a virtual private network (VPN) via an encrypted connection. The device supports two OpenVPN connections.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

OpenVPN connections

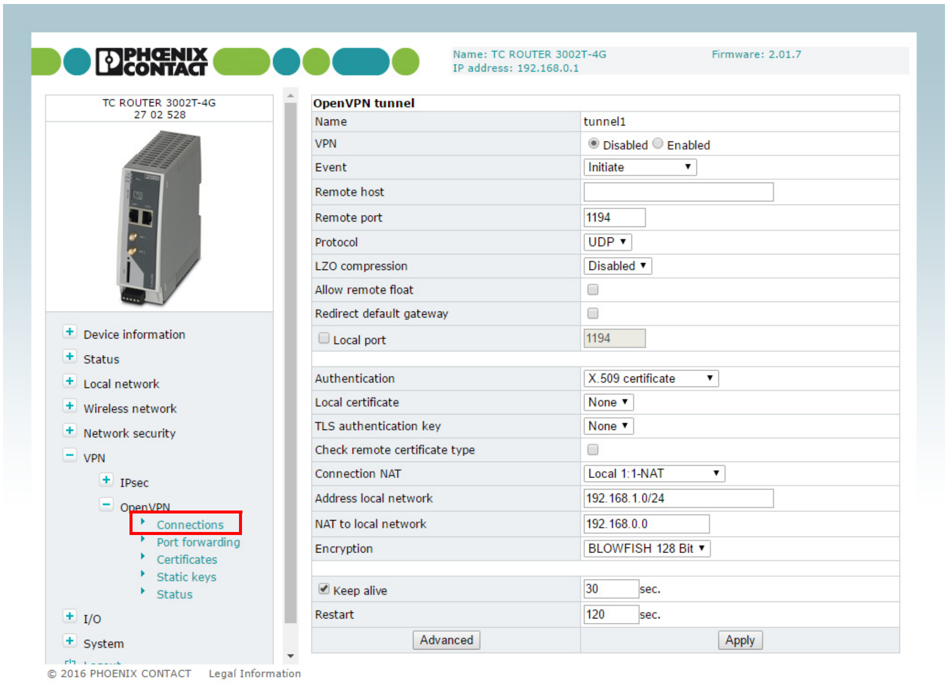
Enabled	Name	Tunnel	Advanced
No ▾	tunnel1	Edit	Edit
No ▾	tunnel2	Edit	Edit
No ▾	tunnel3	Edit	Edit

Apply

Figure 3-32 VPN, OpenVPN, Connections

VPN, OpenVPN, Connections		
OpenVPN connections	**Enabled**	– **Yes:** defined VPN connection active – **No:** defined VPN connection not active
	Name	Assign a descriptive name to each VPN connection. The VPN connection can be freely named or renamed.
	Tunnel	Click on “Edit” to specify the settings for OpenVPN (see “Tunnel, Edit” on page 64).
	Advanced	Click on “Edit” to specify advanced settings for OpenVPN (see “Advanced, Edit” on page 67).

Tunnel, Edit



OpenVPN tunnel	
Name	tunnel1
VPN	● Disabled ○ Enabled
Event	Initiate
Remote host	
Remote port	1194
Protocol	UDP
LZO compression	Disabled
Allow remote float	□
Redirect default gateway	□
□ Local port	1194
Authentication	X.509 certificate
Local certificate	None
TLS authentication key	None
Check remote certificate type	□
Connection NAT	Local 1:1-NAT
Address local network	192.168.1.0/24
NAT to local network	192.168.0.0
Encryption	BLOWFISH 128 Bit
☑ Keep alive	30 sec.
Restart	120 sec.

Figure 3-33 VPN, OpenVPN, Connections, Tunnel, Edit

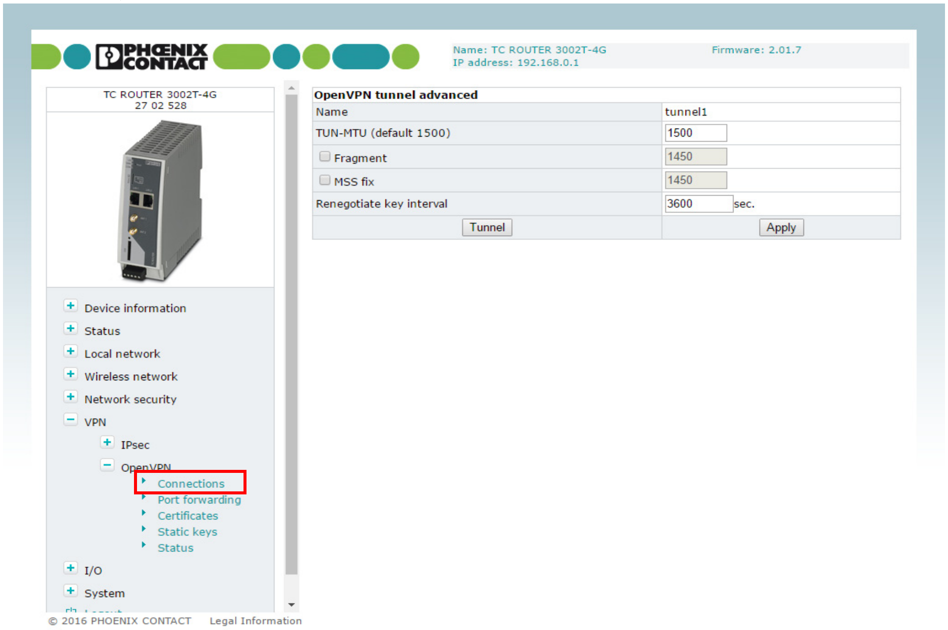
VPN, OpenVPN, Connections, Tunnel, Edit		
OpenVPN tunnel	**Name**	Assign a descriptive name to each VPN connection. The VPN connection can be freely named or renamed.
	VPN	– **Yes:** VPN connection activated – **No**: VPN connection deactivated
	Event	Event for starting the OpenVPN connection – **Initiate**: automatic start after router boots up – **Initiate on SMS:** manual start via SMS message. You must also specify the number of minutes until the VPN connection is to be stopped via Autoreset. – **Initiate on call:** start via a call. You must also specify the number of minutes until the VPN connection is to be stopped via Autoreset. – **Initiate on XML:** manual start via XML socket server – **Initiate on Input #1 ... #2**: manual start via switching input
	Remote host	IP address or URL of the peer to which the tunnel will be created.
	Remote port	Port of the peer to which the tunnel will be created (default: 1194)

VPN, OpenVPN, Connections, Tunnel, Edit		
	Protocol	Choose whether UDP or TCP will be used for transport.
	LZO compression	Choose whether data transmission for the OpenVPN connection will be compressed. – **Disabled**: no OpenVPN compression – **Adaptive**: adaptive OpenVPN compression – **Yes**: OpenVPN compression
	Allow remote float	Activate this option in order to accept authenticated packets from each IP address for the OpenVPN connection. This option is recommended when dynamic IP addresses are used for communication.
	Redirect default gateway	Activate this option in order to redirect all network communication to external networks, e.g., requests via the Internet, via this tunnel. The OpenVPN tunnel is used as the default gateway of the local network.
	Local port	Local port from which the tunnel is created (default: 1194)
	Authentication	**X.509 certificate - authentication method:** each VPN device has a private secret key in the form of an X.509 certificate. The certificate contains additional information about the certificate's owner and the certification authority (CA). **Pre-shared secret key:** each VPN device knows one shared private key. Load this shared key as a “Static key” (see Page 69).
	Local certificate	Certificate used by the router to authenticate itself to the VPN peer
	TLS authentication key	TLS key used to encrypt communication
	Check remote certificate type	Activate this option to check the OpenVPN connection certificates.
	Connection NAT	– **None:** no NAT within the VPN tunnel (default) – **Local 1:1 NAT:** virtual addresses are used for communication via a VPN tunnel. The virtual addresses are linked to the real IP addresses for the set network that has been connected. The subnet mask remains unchanged.
	Address local network[1]	Virtual IP address/subnet mask of the local network. This virtual IP address enables the IP addresses for the remote network to be accessed through the VPN tunnel. You must enter the same settings as the remote network on the remote VPN router.

VPN, OpenVPN, Connections, Tunnel, Edit		
	NAT to local network[1]	Enter the real IP address area for the local network here. Using this address area, the local network can be accessed from the remote network via 1:1 NAT. You can use this function, for example, to access two machines with the same IP address via a VPN tunnel.
	Encryption	Choose the encryption algorithm for the OpenVPN connection.
	Keep alive	Duration in seconds after which Keep Alive requests will be transmitted. These requests test whether the peer is still available. Default: 30 seconds
	Restart	Duration in seconds after which the connection to the peer should be restarted if there has been no response to the Keep Alive requests. Default: 120 seconds

[1] Only if “Local 1:1 NAT” is activated.

Advanced, Edit



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

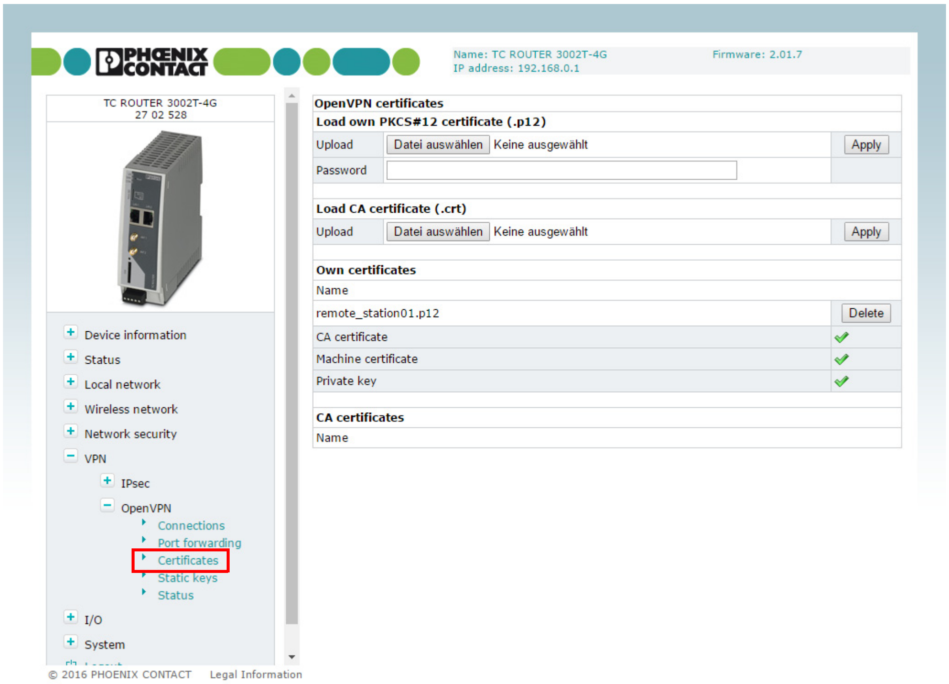
OpenVPN tunnel advanced	
Name	tunnel1
TUN-MTU (default 1500)	1500
□ Fragment	1450
□ MSS fix	1450
Renegotiate key interval	3600 sec.
Tunnel	Apply

Figure 3-34 VPN, OpenVPN, Connections, Advanced, Edit

VPN, OpenVPN, Connections, Advanced, Edit		
OpenVPN tunnel advanced	**Name**	Name of the VPN connection entered under “OpenVPN connections”
	TUN-MTU	Maximum IP packet size that may be used for the OpenVPN connection. Default: 1500 MTU = Maximum Transfer Unit
	Fragment	Maximum size for unencrypted UDP packets that are sent through the tunnel. Larger packets are sent in fragments. Default: 1450 “Fragment” is deactivated if the box is unchecked (default).
	MSS fix	Maximum size for TCP packets that are sent via a UDP tunnel. The maximum packet size in bytes is used for the TCP connection through the OpenVPN tunnel. “MSS fix” is deactivated if the box is unchecked (default). When “Fragment” and “MSS fix” are activated, the value for MSS fix is specified automatically. The value cannot be modified manually.
	Renegotiate key interval	Lifetime in seconds of the agreed keys. Default: 3600 seconds (one hour) The keys of the OpenVPN connection are renewed at defined intervals in order to increase the difficulty of an attack on the OpenVPN connection.

3.8.5 OpenVPN certificates (certificate upload)

A certificate that has been loaded on the router is used to authenticate the router at the peer. The certificate acts as an ID card for the router, which it shows to the relevant peer.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

OpenVPN certificates		
Load own PKCS#12 certificate (.p12)		
Upload	Datei auswählen Keine ausgewählt	Apply
Password		
Load CA certificate (.crt)		
Upload	Datei auswählen Keine ausgewählt	Apply
Own certificates		
Name		
remote_station01.p12		Delete
CA certificate		✓
Machine certificate		✓
Private key		✓
CA certificates		
Name		

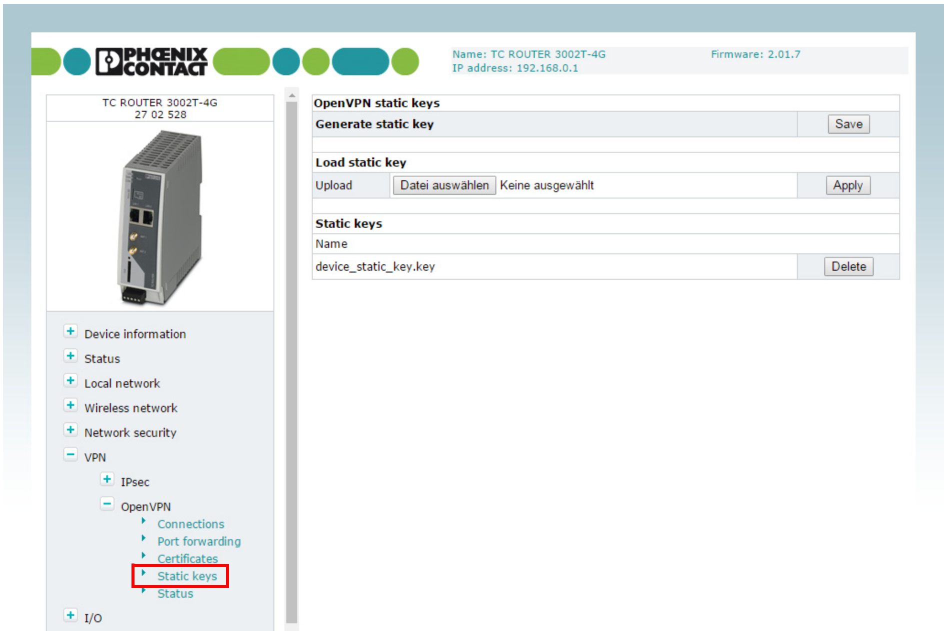
Figure 3-35 VPN, OpenVPN, Certificates

VPN, OpenVPN, Certificates		
OpenVPN certificates		
Load own PKCS#12 certificate (.p12)	**Upload**	Certificate that you have received from your provider. The file must be in PKCS#12 format. Click on the “Browse” button to select the certificate to be imported. Under **“VPN, OpenVPN, Connections, Tunnel, Edit“**, **Local Certificate**, one of these certificates can be assigned to each VPN connection.
	Password	Password used to protect the private key of the PKCS#12 file. The password is assigned when the key is exported.
Load CA certificate (.crt)	**Upload**	The CA certificate must be in crt format. Click on the “Browse” button to select the certificate to be imported. Under **“VPN, OpenVPN, Connections, Tunnel, Edit“**, **Local Certificate**, one of these certificates can be assigned to each VPN connection.

VPN, OpenVPN, Certificates [...]		
Own certificates	Name	Overview of the imported PKCS#12 certificates Click on “Delete” to delete a certificate. The green ticks indicate whether the PKCS#12 file contains a CA certificate, a machine certificate or a private key.
CA certificates	Name	Overview of the imported CA certificates Click on “Delete” to delete a certificate.

3.8.6 Static keys (pre-shared secret key authentication)

Static key authentication is based on a symmetrical encryption method where the communication partners first exchange a shared key via a secure channel. All tunnel network traffic is then encrypted using this key. Network traffic can then be decoded by anyone who has this key.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

OpenVPN static keys

Generate static key

Load static key

Upload Keine ausgewählt

Static keys

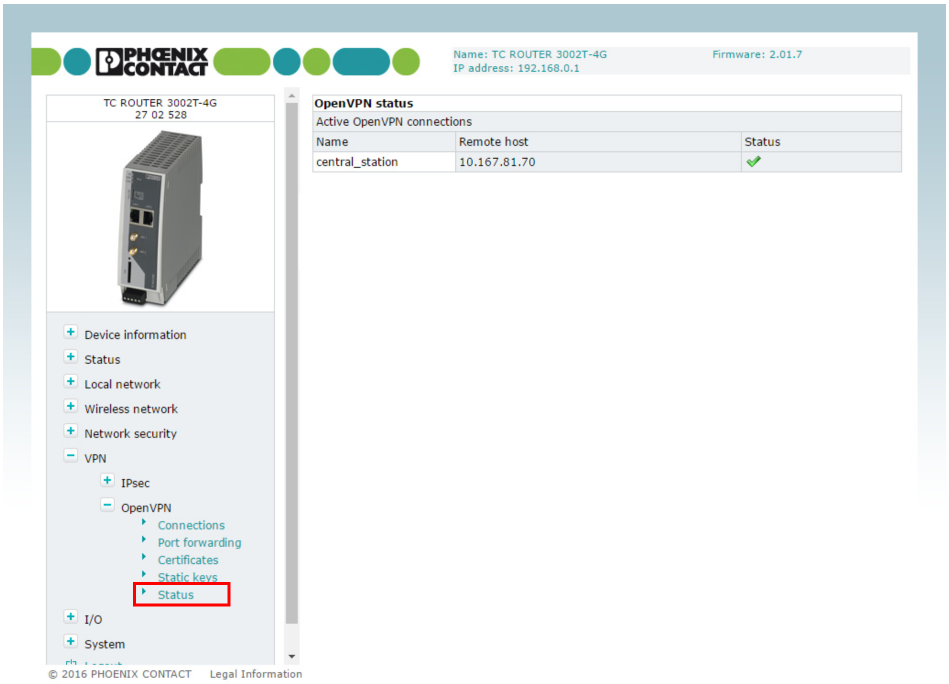
Name

device_static_key.key

Figure 3-36 VPN, OpenVPN, Static keys

VPN, OpenVPN, Static keys		
Open VPN static keys	Generate static key	Generates a key for the OpenVPN connection. You can store this key locally on the computer.
	Load static key	Loads the key on the mobile router.
	Static keys	Keys stored in the router

3.8.7 OpenVPN status (status of the VPN connection)



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

OpenVPN status

Active OpenVPN connections

Name	Remote host	Status
central_station	10.167.81.70	✓

Figure 3-37 VPN, OpenVPN, Status

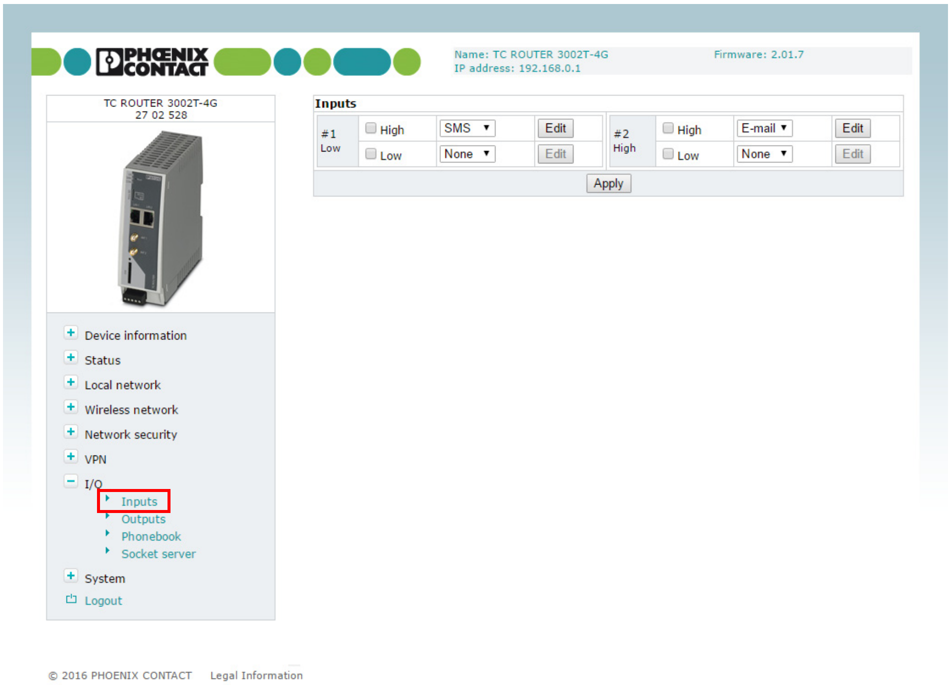
VPN, OpenVPN, Status		
Open VPN status	**Active OpenVPN connections**	Status of the active VPN connection

3.9 I/O

The router has two integrated digital switching inputs and one integrated digital switching output for alarms and switching.

3.9.1 Inputs (input configuration)

The inputs can be used to send alarms by SMS or e-mail. Each input can be configured individually. Please note that inputs that are used to start a VPN connection, for example, cannot also be used to send alarms.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Inputs

#1 Low	□ High	SMS ▾	Edit	#2 High	□ High	E-mail ▾	Edit
	□ Low	None ▾	Edit		□ Low	None ▾	Edit

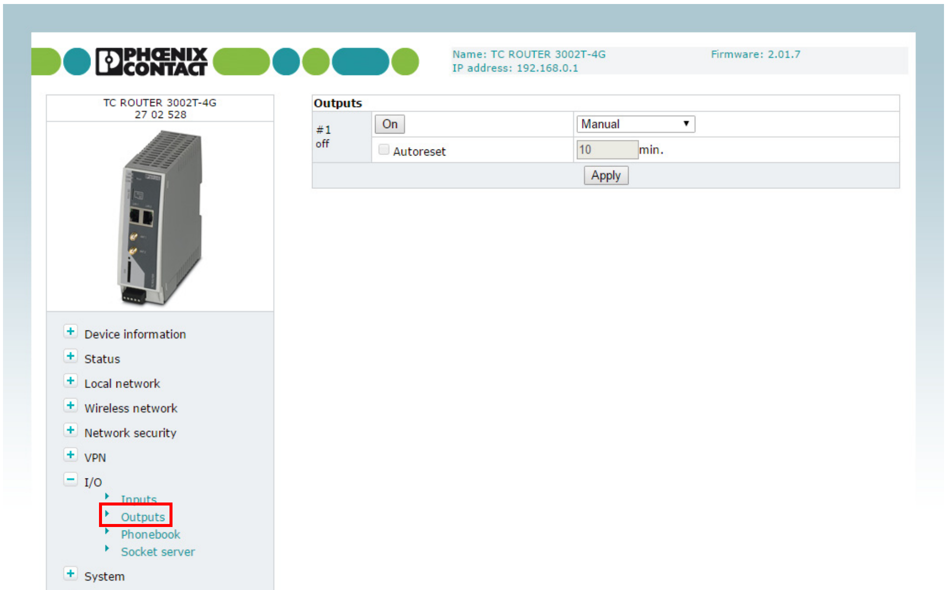
© 2016 PHOENIX CONTACT   Legal Information

Figure 3-38 I/O, Inputs

I/O, Inputs		
Inputs	**High**	If a message should be sent at a “High” input level, activate “High”. Click on “Apply” for acceptance. Choose whether you want to be alerted by SMS or e-mail. Click on “Edit”. Enter the following for an SMS message: – Recipient from the phonebook – Message text Enter the following for an e-mail alert: – To: recipient – Cc: recipient of a copy – Subject – Message text
	Low	If a message should be sent at a “Low” input level, activate “Low”. Click on “Apply” and choose whether you want to be alerted by SMS or e-mail. Click on “Edit”. Enter the following for an SMS message: – Recipient from the phonebook – Message text Enter the following for an e-mail alert: – To: recipient – Cc: recipient of a copy – Subject – Message text

3.9.2 Outputs (output configuration)

The outputs can be switched remotely or, alternatively, provide information about the status of the router. Each output can be configured individually.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Outputs

#1
off

On

Manual

□ Autoreset

10 min.

Apply

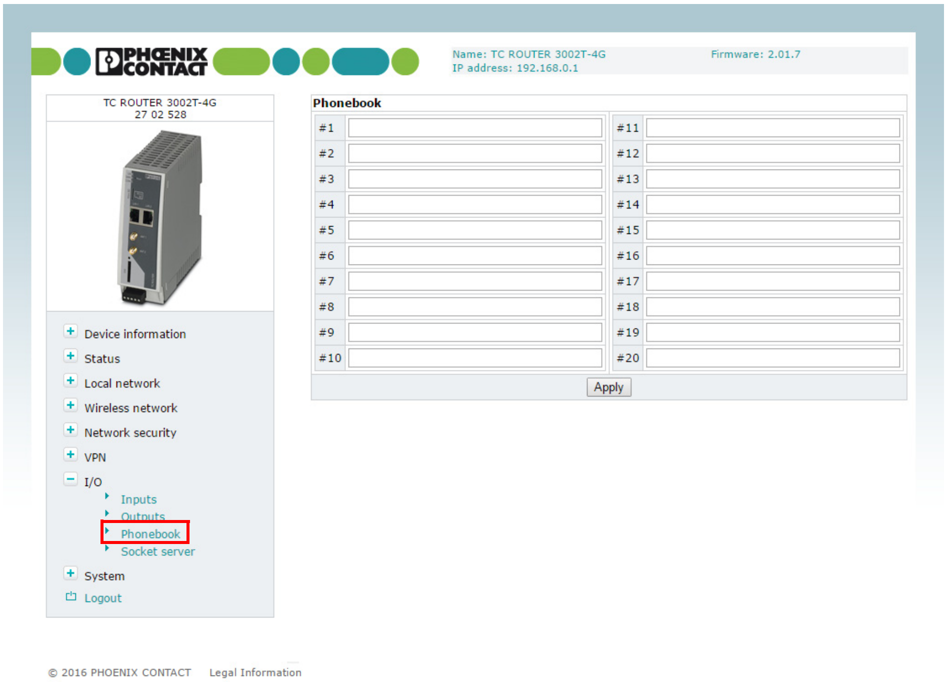
Figure 3-39 I/O, Outputs

I/O, Outputs		
Outputs		– **Manual**: manual switching of the output via the web-based Management – **Remote controlled**: remote switching via SMS or socket server. Automatic reset of the output can be used as an option. To do this, activate “Autoreset” and specify the duration in minutes. – **Radio network**: the output is switched if the router is logged in to a mobile network. – **Packet service**: the output is switched if the router has established a packet data connection and received a valid IP address from the provider. – **VPN service**: the output is switched if the router has established a VPN connection. – **Incoming call**: the output is switched if the router is called by a phone number listed in the phonebook. – **Connection lost**: the output is switched if the router connection check does **not** reach the configured reference address.
	Autoreset	Duration in minutes until the output is reset automatically

3.9.3 Phonebook

Enter phone numbers here:

- For the recipients of alarm SMS messages
- For those authorized to switch the outputs



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Phonebook

#1		#11	
#2		#12	
#3		#13	
#4		#14	
#5		#15	
#6		#16	
#7		#17	
#8		#18	
#9		#19	
#10		#20	

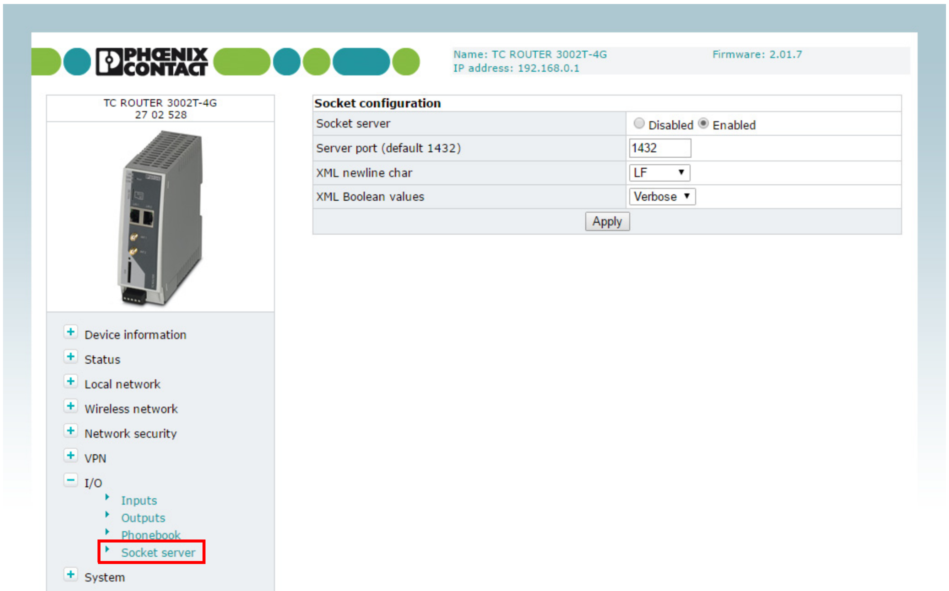
© 2016 PHOENIX CONTACT Legal Information

Figure 3-40 I/O, Phonebook

3.9.4 Socket server

The router has a socket server, which can accept operating commands via the Ethernet interface. These commands must be sent in XML format.

A client from the local network initiates basic communication. To do this, a TCP connection is established to the set server port. The socket server responds to the client's requests. It then terminates the TCP connection. A TCP connection is established again for another request. Only one request is permitted per connection.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

TC ROUTER 3002T-4G
27 02 528

Socket configuration	
Socket server	○ Disabled ● Enabled
Server port (default 1432)	1432
XML newline char	LF
XML Boolean values	Verbose

Figure 3-41 I/O, Socket server

I/O, Socket server		
Socket configuration	**Socket server**	– **Disabled**: operation via Ethernet interface not possible – **Enabled**: operation via Ethernet interface possible
	Server port (default 1432)	Socket server port (default: 1432) Please note that port 80 cannot be used for the socket server. To use the router, a TCP socket connection must be established to the configured port. The data format must conform to XML Version 1.0.
	XML newline char	Character which creates a line break in the XML file – **LF:** line feed, line break after 0x0A (hex) – **CR:** carriage return, line break after 0x0D (hex) – **CR+LF:** line break after carriage return, followed by a line feed

I/O, Socket server		
	XML Boolean values	Format in which requests are answered via XML – **Verbose:** response in words, e.g., on/off – **Numeric:** short numerical response, e.g., 1/0

Every XML file generally begins with the header <?xml version="1.0"?> or <?xml version="1.0" encoding="UTF-8"?> followed by the basic entry.

Basic entries

<io>	....	</io>	I/O system
<info>	....	</info>	Request general device information
<cmgs>	....	</cmgs>	Send SMS messages
<cmgr>	....	</cmgr>	Receive SMS messages
<cmga>	....	</cmga>	Confirm receipt of SMS
<email>	....	</email>	Send e-mails

I/O system

Using the XML socket server, you can:

- query outputs and inputs
- switch outputs

The outputs used must have been previously configured to “Remote controlled”. Depending on the setting of “XML Boolean values”, on/off or 0/1 can be output as “value”.

> Make sure that the XML data does not contain any line breaks.

Query outputs and inputs

```
<?xml version="1.0"?>
 <io>
  <output no="1"/>       Request state of output 1
  <input no="1"/>        Request state of input 1
 </io>
```

Response from the router (shown with line break):

```
<?xml version="1.0" encoding="UTF-8"?>
 <result>
  <io>
   <output no="1" value="off"/>        State output 1
   <input no="1" value="off"/>         State input 1
  </io>
 </result>
```

Switch outputs

```
<?xml version="1.0"?>
 <io>
  <output no="1" value="on"/>        Switch output 1
  </io>
```

Response from the router (shown with line break):

```
<?xml version="1.0" encoding="UTF-8"?>
 <result>
  <io>
   <output no="1" value="on"/>        Output 1 switched
  </io>
 </result>
```

Switch on data connection

First, set the following in the web-based Management:

- Switch on the data connection under "Packet data setup" (enabled see Page 36).
- Under "Event", select the option "Initiate on XML".

⇒ You can now switch on the data connection of the router through XML.

```
<?xml version="1.0"?>
 <io>
  <gprs value="on"/>        Switch on data connection
 </io>
```

Response from the router (shown with line break):

```
<?xml version="1.0" encoding="UTF-8"?>
 <result>
  <io>
   <gprs value="on"/>                Connection on
  </io>
 </result>
```

Request general device information

You can read status information from the device:

```
<?xml version="1.0"?>
 <info>
  <device/>              Request device data
  <radio/>               Data for the wireless connection (mobile devices only)
  <inet/>                Request data for the Internet connection
  <io/>                  Logical states at the connections
 </info>
```

Response from the router (shown with line break):

```
<?xml version="1.0" encoding="UTF-8"?>
 <result>
  <info>
   <device>
    <serialno>13120004</serialno>
    <hardware>A</hardware>
    <firmware>1.04.9</firmware>
    <wbm>1.40.8</wbm>
    <imei>359628023404123</imei>
  </device>
   <radio>
    <provider>Vodafone.de</provider>
    <rssi>15</rssi>
    <creg>1</creg>
    <lac>0579</lac>
    <ci>26330CD</ci>
    <packet>7</packet>
    <simstatus>5</simstatus>
    <simselect>1</simselect>
   </radio>
   <inet>
    <ip>1.2.3.4</ip>
    <rx_bytes>24255</rx_bytes>
    <tx_bytes>1753</tx_bytes>
    <mtu>1500</mtu>
   </inet>
   <io>
    <gsm>1</gsm>
    <inet>1</inet>
    <vpn>0</vpn>
   </io>
  </info>
 </result>
```

To read just one single value, you can use the “Select” attribute to select it. Here is a request for the RSSI value as an example:

```
<?xml version="1.0" encoding="UTF-8"?>
  <info>
   <radio select="rssi" />
  </info>
```

Send SMS messages

Send XML data with the following structure to the device IP address via Ethernet:

```
<?xml version="1.0"?>
  <cmgs destaddr=“0172 123 4567“>SMS message</cmgs>
```

> For this purpose, make sure that the XML data does not contain any line breaks. The text must be UTF-8-coded.
>
> ASCII characters 34_{dec}, 38_{dec}, 39_{dec}, 60_{dec}, and 62_{dec} must be entered as &quot; &apos; &amp; &lt; and &gt;.

If the XML data was received correctly, the device responds with the transmission status:

```
<?xml version="1.0"?>
  <result>
  <cmgs length=“17“>SMS transmitted</cmgs>
  </result>
```

Receive SMS messages

To receive SMS messages via Ethernet, enter the following:

```
<?xml version="1.0"?>
 <cmgr/>
```

Response from the router (shown with line break):

```
<?xml version="1.0" encoding="UTF-8"?>
 <result>
  <cmgr error="1">empty</cmgr>
 </result>
```

The response means that an SMS message has not been received yet. The following error codes are possible:

1	Empty = no SMS message received
2	Busy = try again later
3	System error = communication problem with the radio engine

If the router has received an SMS message and if it is available, then the message is output:

```
<?xml version="1.0" encoding="UTF-8"?>
 <result>
  <cmgr origaddr="+49123456789"
timestamp="14/06/30,10:01:05+08">SMS message</cmgr>
 </result>
```

Confirm receipt of SMS

Successful receipt of the SMS via Ethernet must be confirmed with the following command:

```
<?xml version="1.0" encoding="UTF-8"?>
 <cmga/>
```

Response from the router (shown with line break):

```
<?xml version="1.0" encoding="UTF-8"?>
 <result>
  <cmga>ok</cmga>
 </result>
```

This SMS message is then marked as read on the router.

Send e-mails

Send XML data with the following structure to the device IP address via Ethernet:

```
<?xml version="1.0"?>
 <email to="x.yz@diesunddas.de" cc="info@andere.de">
  <subject>Test Mail</subject>
  <body>
   This is an e-mail text with several lines.
   Best regards,
    your router
  </body>
 </email>
```

Response from the router (shown with line break):

```
<?xml version="1.0" encoding="UTF-8"?>
 <result>
  <email>done</email>
 </result>
```

Response from the router in the event of an error:

```
<?xml version="1.0" encoding="UTF-8"?>
 <result>
  <email error="3">transmisson failed</email>
 </result>
```

Start and stop VPN connections

To start and stop IPsec and OpenVPN connections, send XML data with the following structure to the device IP address via Ethernet:

```
<?xml version="1.0"?>
 <vpn>
  <ipsec no="2" value="on">       Start IPsec connection 2
  <openvpn no="1" value="on"/>    Start OpenVPN connection
<vpn/>
```

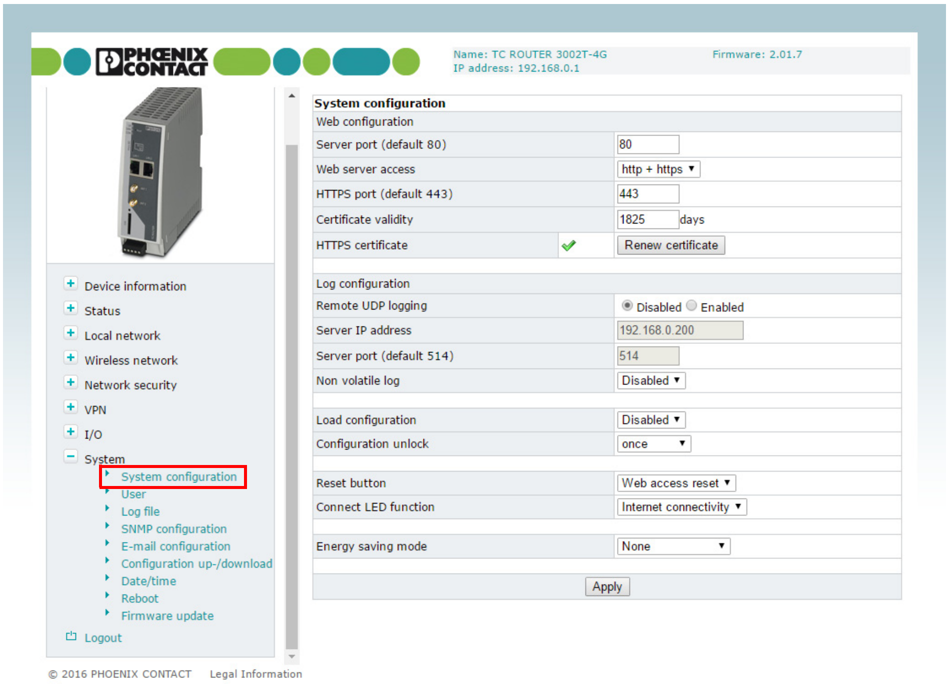
Response from the router (shown with line break):

```
<?xml version="1.0">
 <result>
  <vpn>
   <ipsec no="2" value="on"/>
   <openvpn no="1" value="on"/>
  <vpn/>
```

3.10 System

3.10.1 System configuration

Set the basic options for web-based management and router logging here. The router can store log files on an external log server via UDP.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

System configuration	
Web configuration	
Server port (default 80)	80
Web server access	http + https
HTTPS port (default 443)	443
Certificate validity	1825 days
HTTPS certificate	✓ Renew certificate
Log configuration	
Remote UDP logging	● Disabled ○ Enabled
Server IP address	192.168.0.200
Server port (default 514)	514
Non volatile log	Disabled
Load configuration	Disabled
Configuration unlock	once
Reset button	Web access reset
Connect LED function	Internet connectivity
Energy saving mode	None

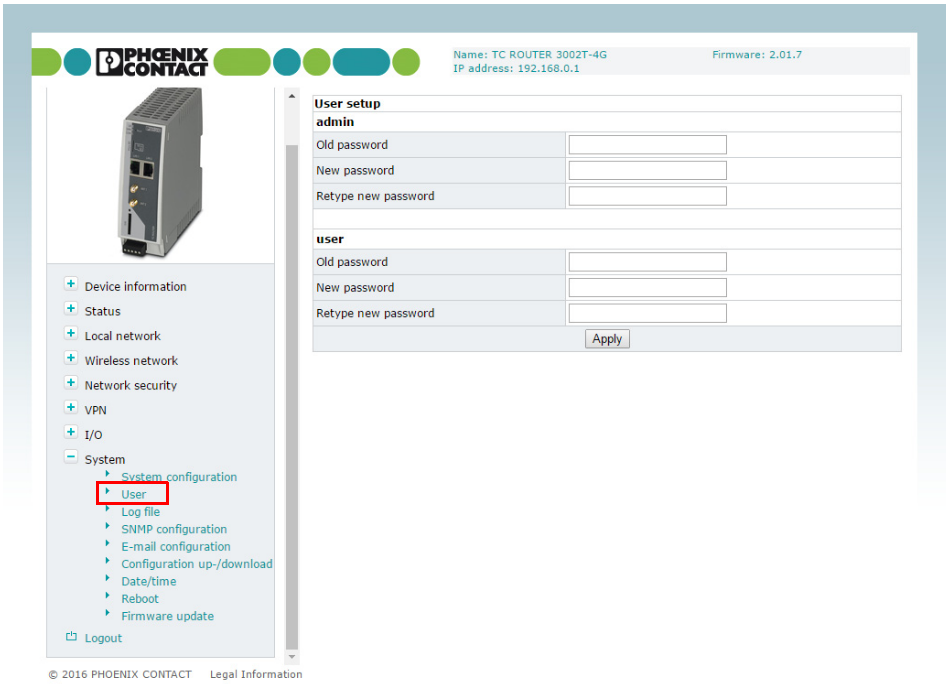
Figure 3-42 System, System configuration

System, system configuration		
System configuration		
Web configuration	**Server port**	The web-based management of the router can be accessed via this port using HTTP (default: 80).
	Web server access	Choose how web-based management can be accessed: – Using the HTTP and HTTPS protocol (default) – Using HTTP only – Using HTTPS only For security reasons, external access via the mobile network is only possible using the HTTPS protocol.
	HTTPS port	The web-based management of the router can be accessed via this port using HTTPS (default: 443).
	Certificate validity	Specify the validity period of the certificate for HTTPS access to web-based management here (default: 1825 days).

System, system configuration		
	HTTPS certificate	To create a new certificate for HTTPS access to web-based management, click on “Renew certificate”. This certificate is valid for the period set under “Certificate validity”.
Log configuration	**Remote UDP logging**	– **Disabled**: no external logging – **Enabled**: logging on external server activated.
	Server IP address	IP address of the log server
	Server port	Log server port (default: 514)
	Non volatile log	– **Disabled**: temporary logging – **Enabled**: permanent logging on microSD card
	Load configuration	– **Disabled**: configuration is not loaded automatically when the router is started – **SD card**: configuration is loaded automatically when the router is started. The configuration is loaded from a microSD card.
	Configuration unlock	– **Once**: a configuration is loaded once next time the router is started. The configuration is loaded from a microSD card. – **Always**: a configuration is loaded every time the router is started. The configuration is loaded from a microSD card. – **By input 1:** a configuration is loaded from a microSD card, controlled via switching input 1 – **By input 2:** a configuration is loaded from a microSD card, controlled via switching input 2
	Reset button	– **Web access reset**: the IP address and access data for the administrator are reset to the default settings via the reset button. The configuration is retained. – **Factory reset**: the device is completely reset to the delivery state via the reset button. The configuration will be deleted.
	Connect LED function	– **Internet connectivity:** packet data connection via mobile network active – **VPN connectivity:** VPN connection active (IPsec or OpenVPN)

System, system configuration		
	Energy saving mode	– **None**: no energy-saving mode – **Initiate on input 1**: energy-saving mode, activated via switching input 1. – **Initiate on input 2**: energy-saving mode, activated via switching input 2. **Radio engine:** energy-saving mode deactivates the radio engine. If energy-saving mode is active, mobile communication is no longer possible. **Ethernet LAN1/2:** energy-saving mode deactivates Ethernet interface LAN 1/2. If energy-saving mode is active, communication is no longer possible via this interface.

3.10.2 User (password change)



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

User setup

admin

Old password	
New password	
Retype new password	

user

Old password	
New password	
Retype new password	

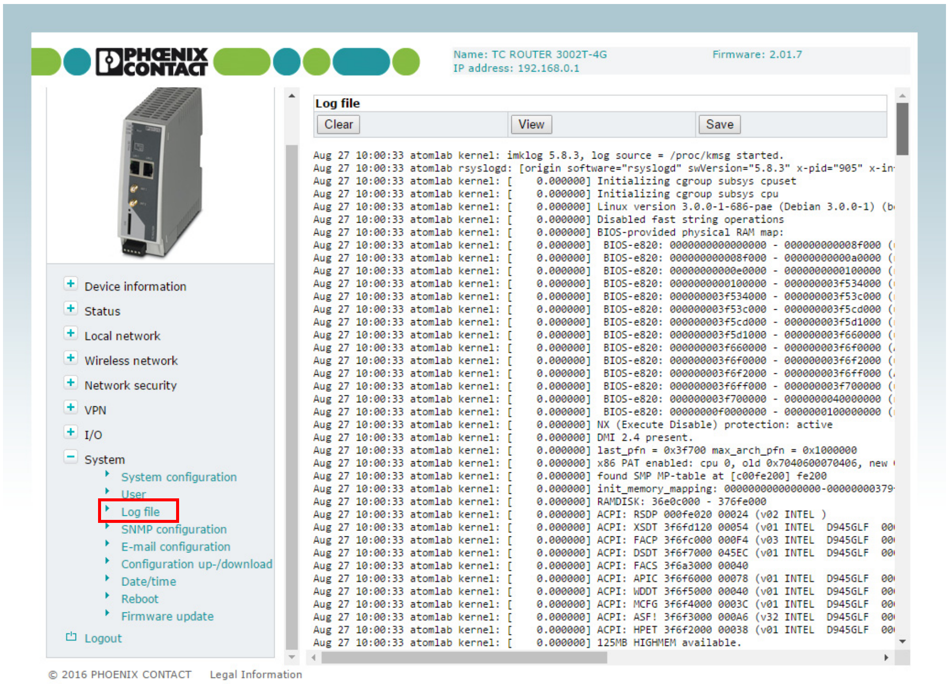
Apply

Figure 3-43 System, User

System, user		
User setup	**Admin**	Unrestricted access to all areas – **Old password** – **New password** – **Retype new password**
	User	Restricted access (read-only) Default: public – **Old password** – **New password** – **Retype new password**

3.10.3 Log file

The router 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.



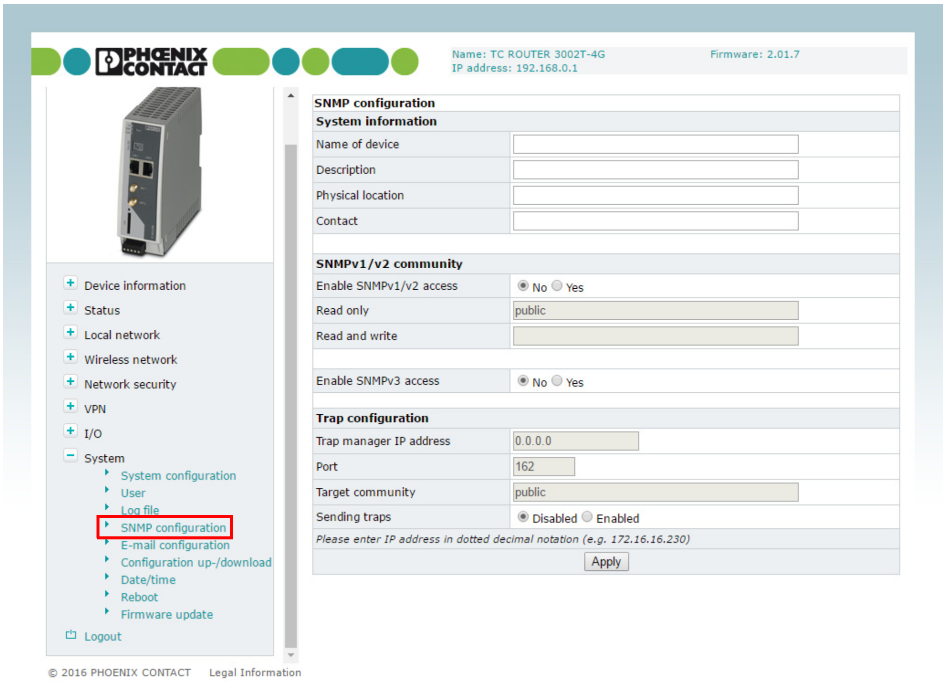
```
Aug 27 10:00:33 atomlab kernel: imklog 5.8.3, log source = /proc/kmsg started.
Aug 27 10:00:33 atomlab rsyslogd: [origin software="rsyslogd" swVersion="5.8.3" x-pid="905" x-in
Aug 27 10:00:33 atomlab kernel: [    0.000000] Initializing cgroup subsys cpuset
Aug 27 10:00:33 atomlab kernel: [    0.000000] Initializing cgroup subsys cpu
Aug 27 10:00:33 atomlab kernel: [    0.000000] Linux version 3.0.0-1-686-pae (Debian 3.0.0-1) (b
Aug 27 10:00:33 atomlab kernel: [    0.000000] Disabled fast string operations
Aug 27 10:00:33 atomlab kernel: [    0.000000] BIOS-provided physical RAM map:
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 0000000000000000 - 000000000008f000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000000008f000 - 00000000000a0000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 00000000000e0000 - 0000000000100000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 0000000000100000 - 000000003f534000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f534000 - 000000003f53c000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f53c000 - 000000003f5cd000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f5cd000 - 000000003f5d1000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f5d1000 - 000000003f660000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f660000 - 000000003f6f0000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f6f0000 - 000000003f6f2000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f6f2000 - 000000003f6ff000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f6ff000 - 000000003f700000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f700000 - 0000000040000000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 00000000f0000000 - 0000000100000000 (
Aug 27 10:00:33 atomlab kernel: [    0.000000] NX (Execute Disable) protection: active
Aug 27 10:00:33 atomlab kernel: [    0.000000] DMI 2.4 present.
Aug 27 10:00:33 atomlab kernel: [    0.000000] last_pfn = 0x3f700 max_arch_pfn = 0x1000000
Aug 27 10:00:33 atomlab kernel: [    0.000000] x86 PAT enabled: cpu 0, old 0x7040600070406, new
Aug 27 10:00:33 atomlab kernel: [    0.000000] found SMP MP-table at [c00fe200] fe200
Aug 27 10:00:33 atomlab kernel: [    0.000000] init_memory_mapping: 0000000000000000-0000000379
Aug 27 10:00:33 atomlab kernel: [    0.000000] RAMDISK: 36e0c000 - 376fe000
Aug 27 10:00:33 atomlab kernel: [    0.000000] ACPI: RSDP 000fe020 00024 (v02 INTEL )
Aug 27 10:00:33 atomlab kernel: [    0.000000] ACPI: XSDT 3f6fd120 00054 (v01 INTEL  D945GLF  00
Aug 27 10:00:33 atomlab kernel: [    0.000000] ACPI: FACP 3f6fc000 000F4 (v03 INTEL  D945GLF  00
Aug 27 10:00:33 atomlab kernel: [    0.000000] ACPI: DSDT 3f6f7000 045EC (v01 INTEL  D945GLF  00
Aug 27 10:00:33 atomlab kernel: [    0.000000] ACPI: FACS 3f6a3000 00040
Aug 27 10:00:33 atomlab kernel: [    0.000000] ACPI: APIC 3f6f6000 00078 (v01 INTEL  D945GLF  00
Aug 27 10:00:33 atomlab kernel: [    0.000000] ACPI: WDDT 3f6f5000 00040 (v01 INTEL  D945GLF  00
Aug 27 10:00:33 atomlab kernel: [    0.000000] ACPI: MCFG 3f6f4000 0003C (v01 INTEL  D945GLF  00
Aug 27 10:00:33 atomlab kernel: [    0.000000] ACPI: ASF! 3f6f3000 000A6 (v32 INTEL  D945GLF  00
Aug 27 10:00:33 atomlab kernel: [    0.000000] ACPI: HPET 3f6f2000 00038 (v01 INTEL  D945GLF  00
Aug 27 10:00:33 atomlab kernel: [    0.000000] 125MB HIGHMEM available.
```

Figure 3-44 System, Log file

System, log file		
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

3.10.4 SNMP configuration (router monitoring)

The router supports the reading of information via SNMP (Simple Network Management Protocol). SNMP is a network protocol that can be used to monitor and control network elements from a central station. The protocol controls communication between the monitored devices and the central station.



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

SNMP configuration	
System information	
Name of device	
Description	
Physical location	
Contact	
SNMPv1/v2 community	
Enable SNMPv1/v2 access	● No ○ Yes
Read only	public
Read and write	
Enable SNMPv3 access	● No ○ Yes
Trap configuration	
Trap manager IP address	0.0.0.0
Port	162
Target community	public
Sending traps	● Disabled ○ Enabled

Please enter IP address in dotted decimal notation (e.g. 172.16.16.230)

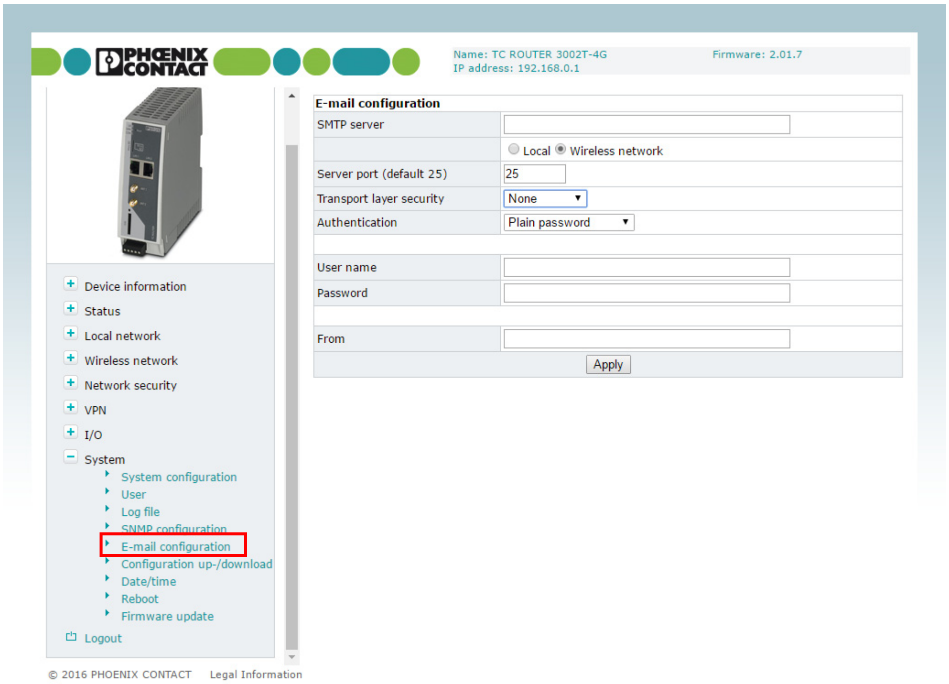
Figure 3-45 Local network, SNMP configuration

Local network, SNMP configuration		
SNMP configuration		
System information		
	Name of device	Name for management purposes, can be freely assigned
	Description	Description of the router
	Physical location	Designation for the installation location, can be freely assigned
	Contact	Contact person responsible for the router
SNMPv1/v2 community		
	Enable SNMPv1/2 access	– **Yes:** SNMP Version 1 and Version 2 are used. – **No:** the service is deactivated (default).
	Read only	Password for read access via SNMP
	Read and write	Password for read and write access via SNMP
	Enable SNMPv3 access	– **Yes:** SNMP Version 3 is used. – **No:** the service is deactivated (default).

Local network, SNMP configuration [...]		
Trap configuration		In certain cases, the router can send SNMP traps. The traps correspond to SNMPv1. They are part of the standard MIB.
	Trap manager IP address	IP address to which the trap will be sent
	Port	Port to which the trap will be sent
	Target community	Name of the SNMP community to which the trap is assigned.
	Sending traps	– **Disabled**: it is not possible to send traps to the IP address of the trap manager. – **Enabled**: the sending of traps to the IP address of the trap manager is activated.

3.10.5 E-mail configuration

To send alarms by e-mail, the e-mail server via which these alerts are sent can be configured here. The e-mail server must support the SMTP protocol.



Name: TC ROUTER 3002T-4G
Firmware: 2.01.7
IP address: 192.168.0.1

E-mail configuration

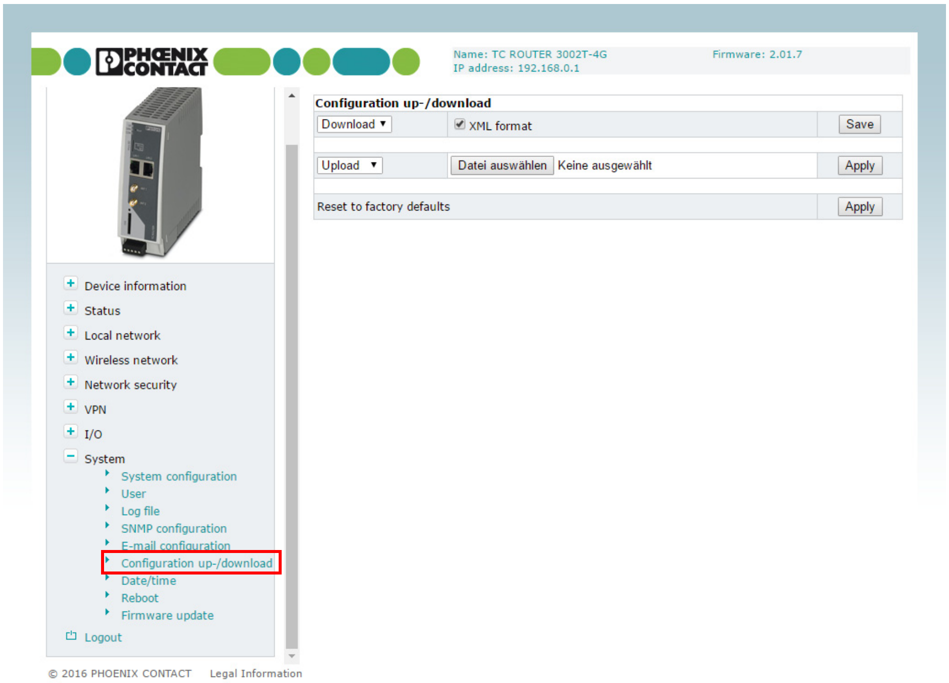
SMTP server	
	○ Local ● Wireless network
Server port (default 25)	25
Transport layer security	None
Authentication	Plain password
User name	
Password	
From	

Figure 3-46 System, E-mail configuration

System, E-mail configuration		
E-mail configuration	**SMTP server**	Host name or IP address of the e-mail server – **Local:** the IP packets for the SMTP server are sent from the local network interface with the IP address of the local interface (LAN). – **Wireless network:** the IP packets for the SMTP server are sent from the mobile network interface with the IP address assigned by the provider.
	Server port	E-mail server port (default: 25)
	Transport layer security	– **None**: unencrypted connection to e-mail server – **STARTTLS**: STARTTLS-encrypted connection to the e-mail server – **SSL/TLS**: SSL/TLS-encrypted connection to the e-mail server
	Authentication	– **No authentication**: no authentication required. – **Plain password**: authentication with user name and password. User name and password are transmitted in unencrypted form. – **Encrypted password**: authentication with user name and password. User name and password are transmitted in encrypted form.
	User name	User name for login to the e-mail server
	Password	Corresponding password for login to the e-mail server
	From	E-mail address of the sender

3.10.6 Configuration up-/download

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



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

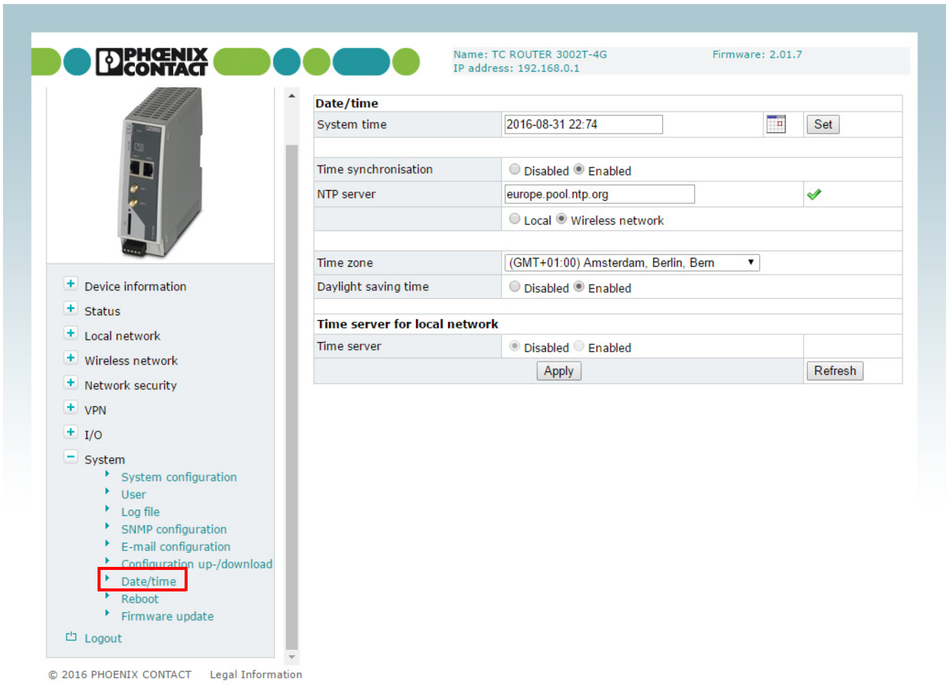
Configuration up-/download

Download ▾	☑ XML format	Save
Upload ▾	Datei auswählen Keine ausgewählt	Apply
Reset to factory defaults		Apply

Figure 3-47 System, Configuration up-/download

System, Configuration up-/download		
Configuration up-/download	**Download**	To save the active configuration to a microSD card, select the “SD card” option under “Download”. Click on “Save” to save the active configuration locally to a file. Enable the “XML format” option to save the router configuration as an editable XML structure.
	Upload	To load a configuration from the microSD card, select the “SD card” option under “Upload”. Import a saved configuration. Click on the “Browse” button to select the configuration that is to be imported. Click on “Apply” to load the selected configuration (cfg format or XML format).
	Reset to factory defaults	Click on “Apply” to reset the router to the default state upon delivery. This will reset all settings, including IP settings. Imported certificates remain unaltered.

3.10.7 Date/time



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

Date/time

System time	2016-08-31 22:74	Set
Time synchronisation	○ Disabled ● Enabled	
NTP server	europe.pool.ntp.org	✓
	○ Local ● Wireless network	
Time zone	(GMT+01:00) Amsterdam, Berlin, Bern	
Daylight saving time	○ Disabled ● Enabled	

Time server for local network

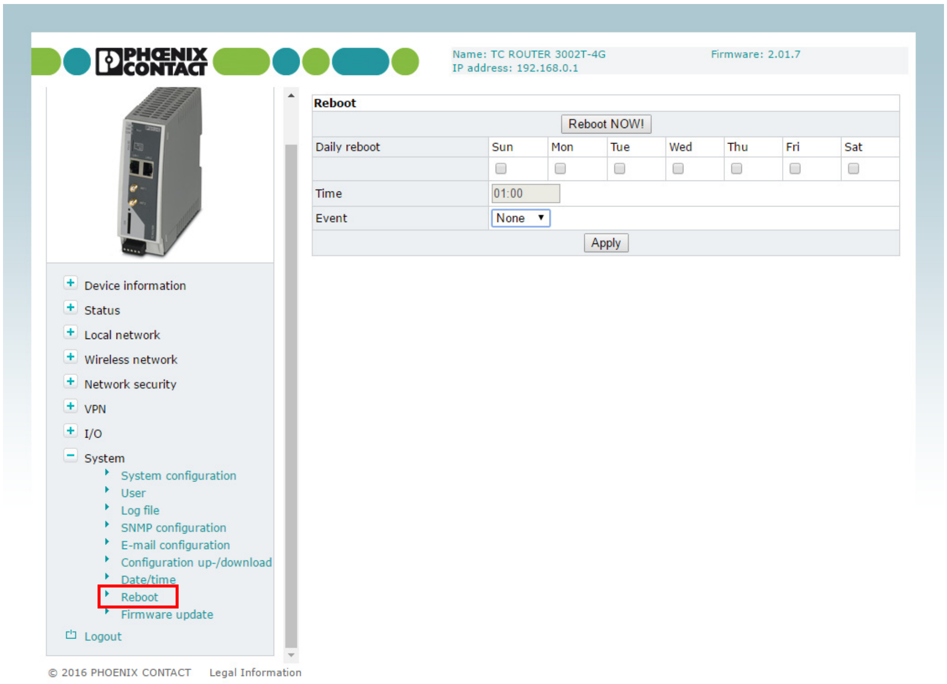
Time server	● Disabled ○ Enabled

Figure 3-48 System, Date/time

System, date/time		
Date/time	**System time**	You can set the time manually if no NTP server (time server) has been set up or the NTP server cannot be reached.
	Time synchronisation	– **Enabled:** the router synchronizes the time and date with a time server. Initial time synchronization can take up to 15 minutes. During this time, the router 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 router act as the NTP server for the devices connected to the LAN interface. The router then provides the system time.

System, date/time [...]		
	NTP server	NTP = Network Time Protocol The router can act as the NTP server for the devices connected to the LAN interface. In this case, the devices should be configured so that the local address of the router is specified as the NTP server address. For the router to act as the NTP server, it must obtain the current date and time from an NTP server (time server). In order to do this you must specify the address of a time server. In addition, NTP synchronization must be set to “Enabled”. A green tick is displayed following successful time synchronization with the time server. – **Local:** the specified NTP server can be accessed with the IP address of the local interface (LAN). Activate this option if the NTP server can be accessed in the local LAN or via a VPN tunnel. – **Wireless network:** activate this option if the NTP server is on the Internet (default).
	Time zone	Select the time zone.
	Daylight saving time	– **Enabled**: daylight savings is taken into account. – **Disabled**: daylight savings is not taken into account.
	Time server for local network	Time server for the local network

3.10.8 Reboot (router restart)



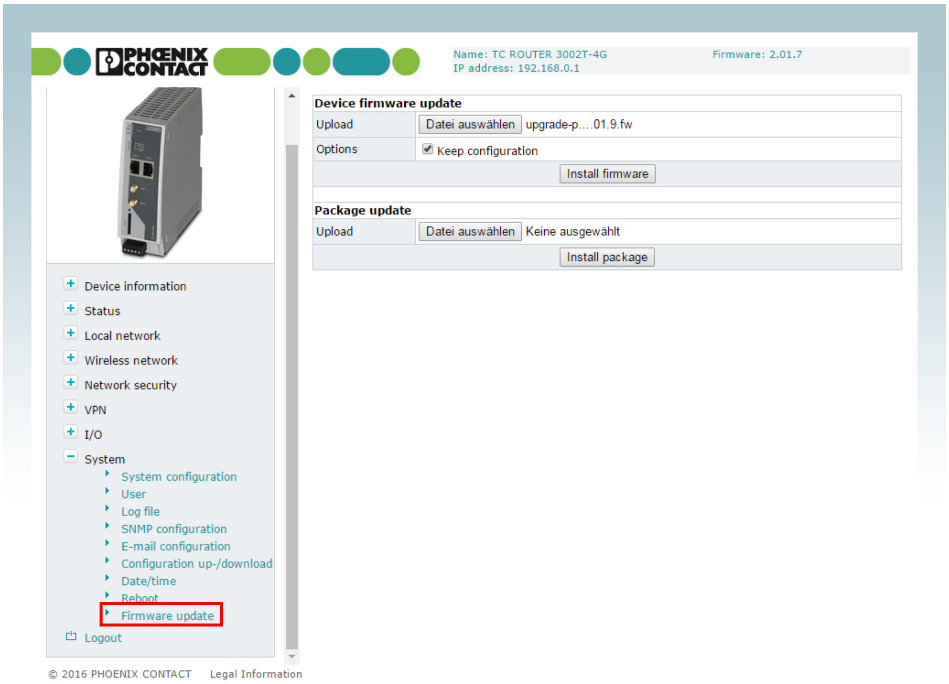
Name: TC ROUTER 3002T-4G Firmware: 2.01.7
IP address: 192.168.0.1

Reboot							
	Reboot NOW!						
Daily reboot	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	□	□	□	□	□	□	□
Time	01:00						
Event	None						
	Apply						

Figure 3-49 System, Reboot

System, reboot		
Reboot	**Reboot NOW!**	Restarting the router 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 router will be restarted at the specified time. Following a reboot, it is necessary to log in to the mobile network again. The provider resets the data link and calculates charges. Regular rebooting provides protection against the provider aborting and re-establishing the connection at an unforeseeable point in time.
	Time	Time specified in Hours:Minutes
	Event	Choose the digital input with the “High” signal which will be used to restart the router if required. Make sure that following a restart the signal is “Low” again. This ensures that the router starts up normally.

3.10.9 Firmware update



Name: TC ROUTER 3002T-4G
IP address: 192.168.0.1
Firmware: 2.01.7

Device firmware update	
Upload	Datei auswählen upgrade-p....01.9.fw
Options	☑ Keep configuration
	Install firmware

Package update	
Upload	Datei auswählen Keine ausgewählt
	Install package

Figure 3-50 System, Firmware update

System, Firmware update

Device firmware update

Updates ensure that you can benefit from function extensions and product updates.

Updates can be downloaded at: phoenixcontact.net/products.

Install firmware update:

- Click on “Select file” and select the update file with the extension *.fw. To ensure that the active configuration is retained following the update, select the “Keep configuration” option.
- Click on “Install firmware”.
- The ERR LED and CON LED flash alternately during the update. Wait until the update is completed and the router restarts automatically.

> Do **not** start the router manually.
>
> Do **not** interrupt the power supply during the update process.

Package update

If necessary you can also just update individual router functions.

4 Creating X.509 certificates

Certificates are required for a secure VPN connection. Certificates can be acquired from certification bodies or you can create them using the appropriate software. In this example, X.509 certificates are created using Version 0.9.3 of the XCA program.

The XCA program can be downloaded at http://xca.sourceforge.net.

4.1 Installation

- Start the setup file. Follow the instructions in the setup program.

4.2 Creating a new database

- Start the XCA program.
- Create a new database via “File, New Database”.

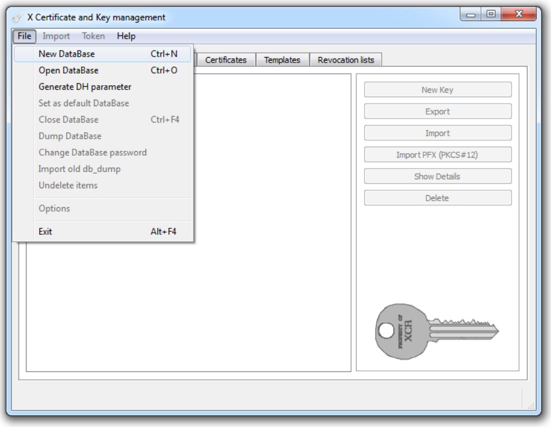
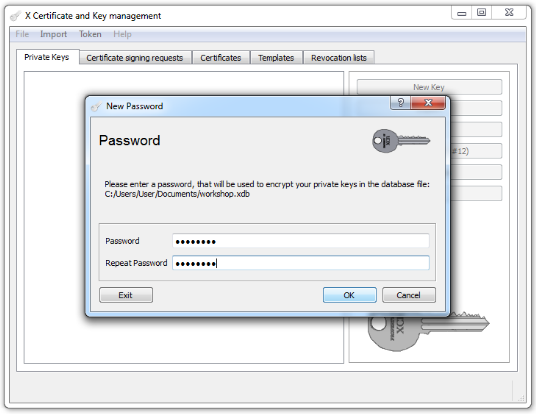


Figure 4-1 Creating a new database

- Assign a password to encrypt the database.



Password

Please enter a password, that will be used to encrypt your private keys in the database file:
C:/Users/User/Documents/workshop.xdb

Password ••••••••

Repeat Password ••••••••

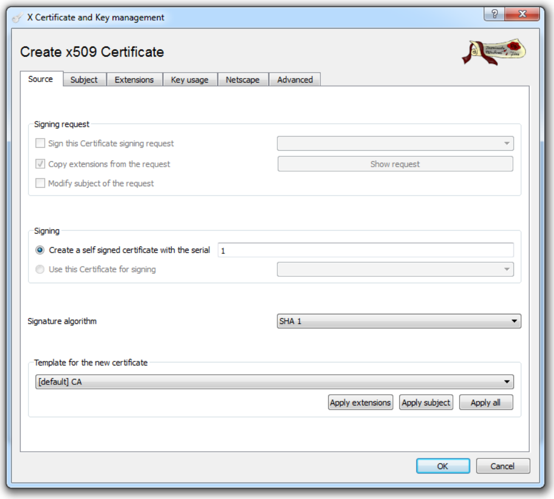
Figure 4-2 Assigning a password

4.3 Creating a CA certificate

First of all, create a Certification Authority (CA) certificate. This root certificate acts as an entity that certifies and authenticates the signing of all certificates that are derived from it and thus guarantees the authenticity of these certificates.

- Switch to the “Certificates” tab and create a new certificate.

In the program window shown, there is already a preset self-signed certificate with the signature algorithm SHA-1.



Create x509 Certificate

Signing request

☐ Sign this Certificate signing request

☑ Copy extensions from the request

☐ Modify subject of the request

Signing

● Create a self signed certificate with the serial 1

○ Use this Certificate for signing

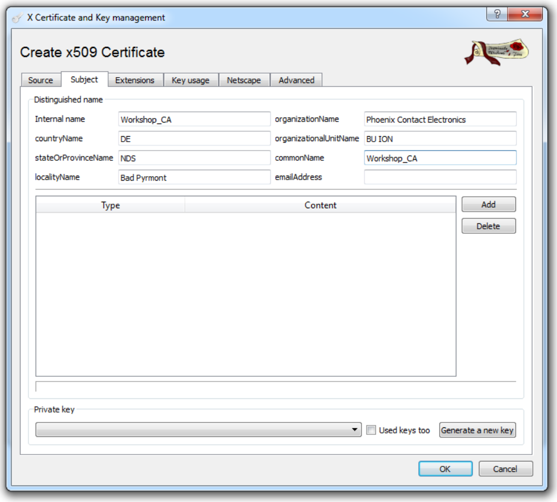
Signature algorithm SHA 1

Template for the new certificate

[default] CA

Figure 4-3 Creating a new CA certificate

- On the “Subject” tab, enter the information about the owner of the root certificate.



Create x509 Certificate

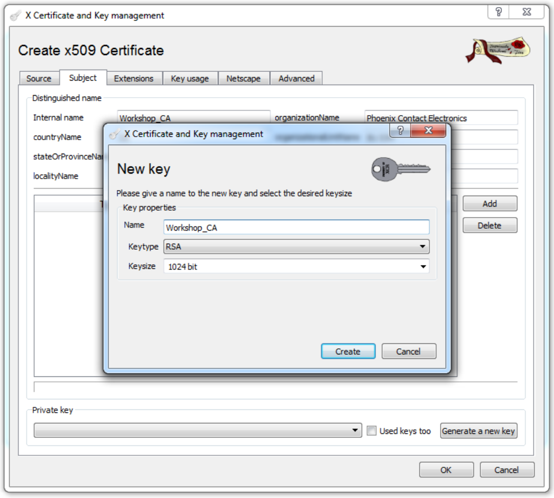
Distinguished name

Internal name	Workshop_CA	organizationName	Phoenix Contact Electronics
countryName	DE	organizationalUnitName	BU ION
stateOrProvinceName	NDS	commonName	Workshop_CA
localityName	Bad Pyrmont	emailAddress	

☐ Used keys too

Figure 4-4 Entering information about the owner

- Create a key for this certificate. The default name, key type, and key size can be retained.



New key

Please give a name to the new key and select the desired keysize

Key properties

Name: Workshop_CA

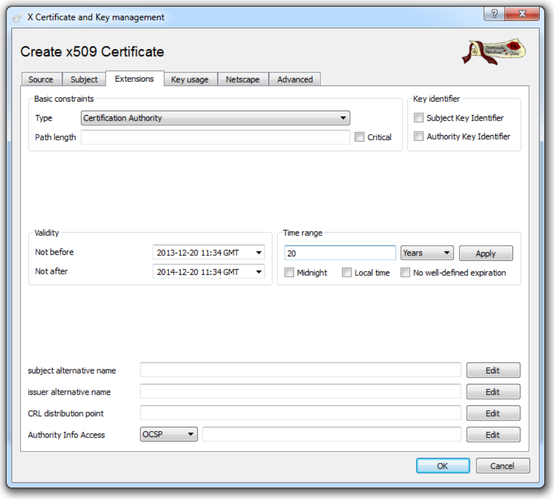
Keytype: RSA

Keysize: 1024 bit

Figure 4-5 Creating a key

The period of validity of the certificate is specified on the “Extensions” tab. The root certificate must be valid for longer than the machine certificates that are to be created later. In this example, the validity is set to ten years.

- Set the certificate type to “Certification Authority”.
- Activate all the options as shown in Figure 4-6.



Basic constraints
Type: Certification Authority
Path length: □ Critical

Key identifier
□ Subject Key Identifier
□ Authority Key Identifier

Validity
Not before: 2013-12-20 11:34 GMT
Not after: 2014-12-20 11:34 GMT

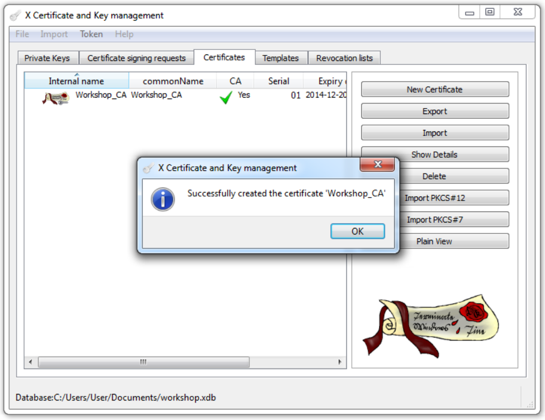
Time range
20 Years Apply
□ Midnight □ Local time □ No well-defined expiration

subject alternative name
issuer alternative name
CRL distribution point
Authority Info Access: OCSP

Figure 4-6 Setting the validity and type for the CA certificate

- Click OK.

The certificate is created. A new root certificate from which further machine certificates can be derived now appears in the overview.



Internal name	commonName	CA	Serial	Expiry
Workshop_CA	Workshop_CA	✓ Yes	01	2014-12-20

Successfully created the certificate 'Workshop_CA'

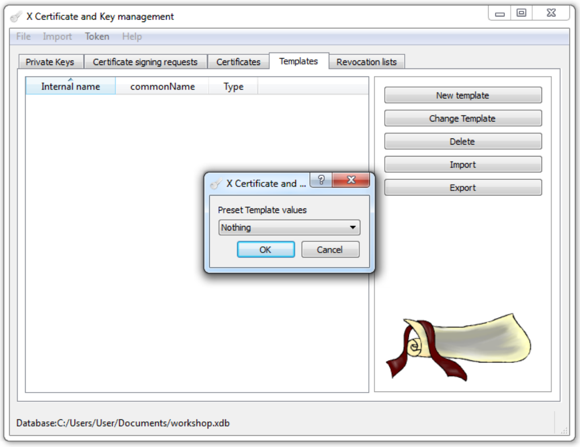
Database:C:/Users/User/Documents/workshop.xdb

Figure 4-7 CA certificate created

4.4 Creating templates

By using templates, you can create machine certificates quickly and easily.

- Switch to the “Templates” tab and create a new template for a terminal certificate.
- When prompted about template values, select “Nothing”.

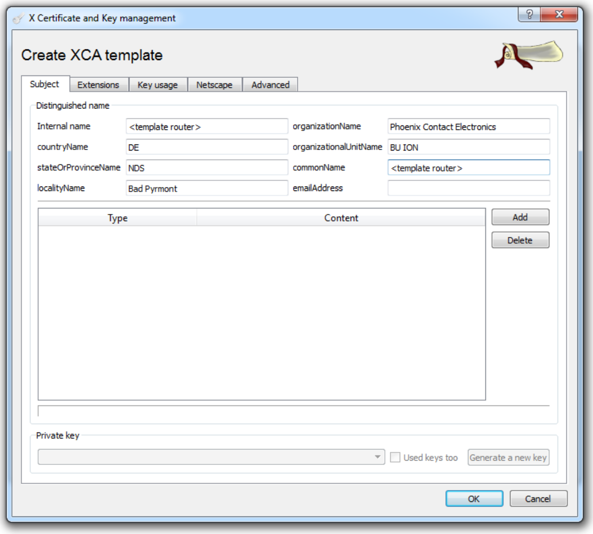


Preset Template values: Nothing

Database:C:/Users/User/Documents/workshop.xdb

Figure 4-8 Creating a new template

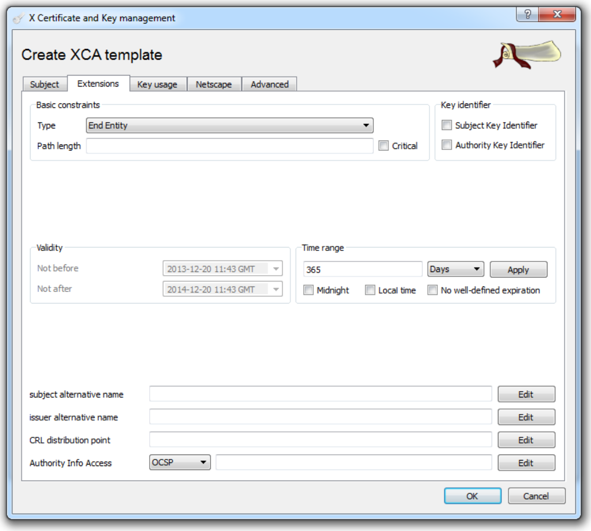
- Default settings for the certificates to be created later can be made on the “Subject” tab. The name must be specified in the relevant certificates. The text specified in the angle brackets is a placeholder which is replaced when the template is applied.



Internal name	<template router>	organizationName	Phoenix Contact Electronics
countryName	DE	organizationalUnitName	BU ION
stateOrProvinceName	NDS	commonName	<template router>
localityName	Bad Pyrmont	emailAddress	

Figure 4-9 Creating a template, entering information about the owner

- On the “Extensions” tab, set the certificate type to “End Entity” as the template should be valid for machine certificates.
- The validity of the certificates to be created is 365 days in this example. Once the end date has elapsed, the certificates can no longer be used.



X Certificate and Key management

Create XCA template

Subject | Extensions | Key usage | Netscape | Advanced

Basic constraints

Type: End Entity

Path length: □ Critical

Key identifier

□ Subject Key Identifier

□ Authority Key Identifier

Validity

Not before: 2013-12-20 11:43 GMT

Not after: 2014-12-20 11:43 GMT

Time range

365 Days Apply

□ Midnight □ Local time □ No well-defined expiration

subject alternative name: Edit

issuer alternative name: Edit

CRL distribution point: Edit

Authority Info Access: OCSP Edit

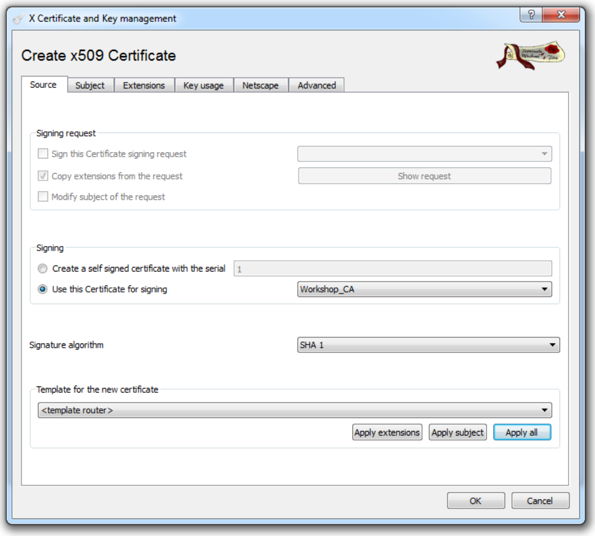
Figure 4-10 Creating a template, entering the validity and type of certificate

- Click OK.

The template is created. You can now use the template as a basis to create certificates signed by the root certificate.

4.5 Creating certificates

- To create certificates based on the template, switch to the “Certificates” tab.
- Create a new certificate.
- A program window opens. On the “Source” tab, the root certificate that is to be used for signing is specified. In addition, you can select a template that was created earlier. The data is imported when you click on “Apply all”.



Signing request

□ Sign this Certificate signing request

☑ Copy extensions from the request

□ Modify subject of the request

Signing

○ Create a self signed certificate with the serial: 1

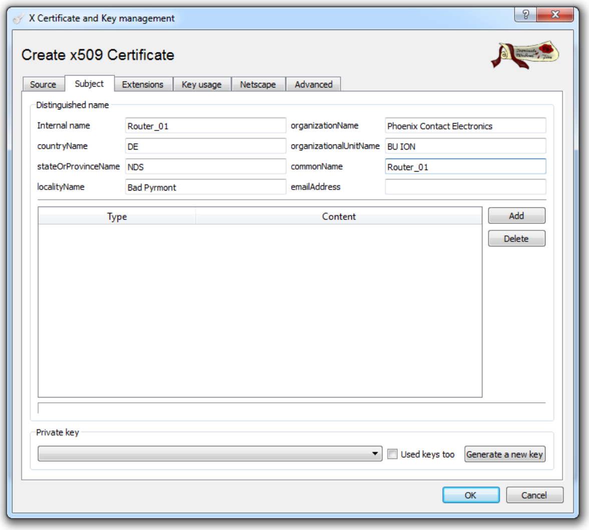
● Use this Certificate for signing: Workshop_CA

Signature algorithm: SHA 1

Template for the new certificate: <template router>

Figure 4-11 Creating a certificate

The fields on the “Subject” tab will now either be empty or they will contain the defaults from the imported template. When entering information on this tab, please note that the certificates must differ at least with regard to their name (internal name and common name). For example, the equipment identification of the machine or the location can be specified as the name here.



X Certificate and Key management

Create x509 Certificate

Distinguished name

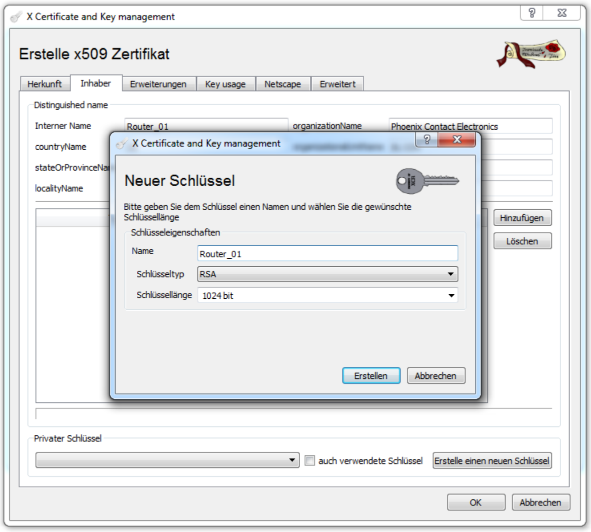
Internal name: Router_01
countryName: DE
stateOrProvinceName: NDS
localityName: Bad Pyrmont
organizationName: Phoenix Contact Electronics
organizationalUnitName: BU ION
commonName: Router_01
emailAddress:

Private key

□ Used keys too

Figure 4-12 Creating a certificate, “Subject” tab

- Create a new private key for this certificate.



X Certificate and Key management

Erstelle x509 Zertifikat

Distinguished name

Interner Name: Router_01
organizationName: Phoenix Contact Electronics

X Certificate and Key management

Neuer Schlüssel

Bitte geben Sie dem Schlüssel einen Namen und wählen Sie die gewünschte Schlüssellänge

Schlüsseleigenschaften

Name: Router_01
Schlüsseltyp: RSA
Schlüssellänge: 1024 bit

Privater Schlüssel

□ auch verwendete Schlüssel

Figure 4-13 Creating a key for a certificate

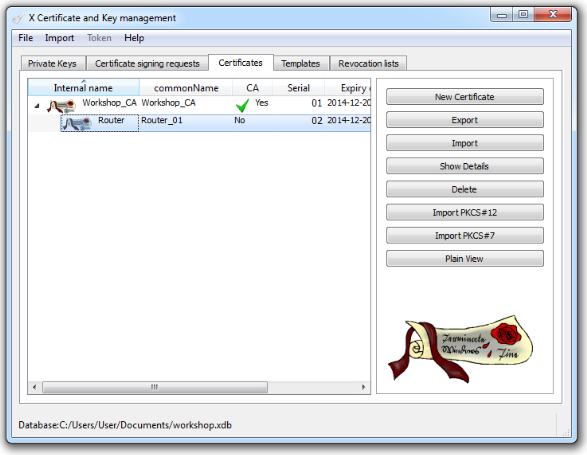
- Click OK.

You have now created a machine certificate signed by the Certification Authority (CA).

4.6 Exporting certificates

In order to use the machine certificate in a router, you must export the certificate.

- Select the desired certificate from the list. Click on “Export”.

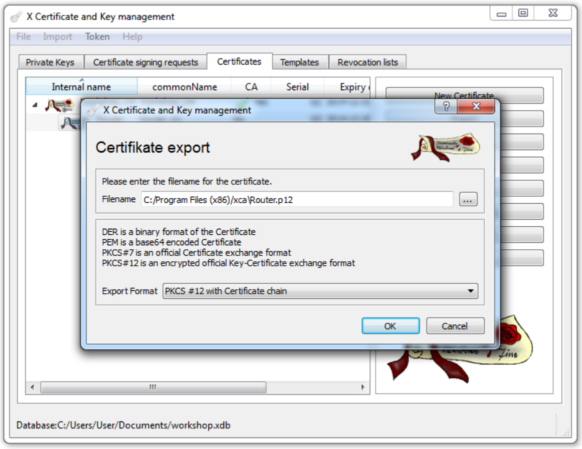


Internal name	commonName	CA	Serial	Expiry
Workshop_CA	Workshop_CA	✓ Yes	01	2014-12-20
Router	Router_01	No	02	2014-12-20

Database:C:/Users/User/Documents/workshop.xdb

Figure 4-14 Selecting a certificate for export

The complete certificate, including the private key and the CA certificate, must be in “PKCS #12 with Certificate Chain” format. You can then upload it to the relevant device as a machine certificate.



Certifikate export

Please enter the filename for the certificate.

Filename C:/Program Files (x86)/xca\Router.p12

DER is a binary format of the Certificate
PEM is a base64 encoded Certificate
PKCS#7 is an official Certificate exchange format
PKCS#12 is an encrypted official Key-Certificate exchange format

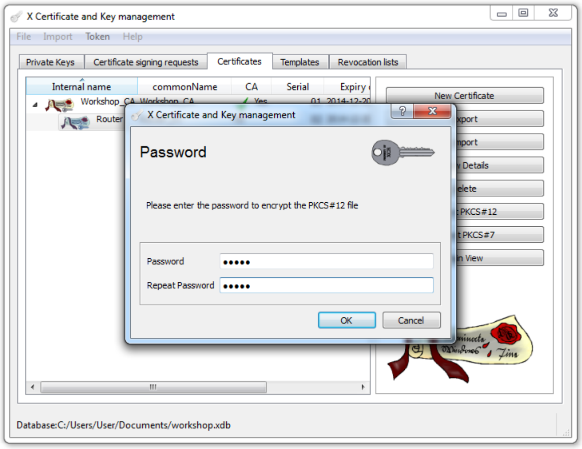
Export Format PKCS #12 with Certificate chain

Database:C:/Users/User/Documents/workshop.xdb

Figure 4-15 Exporting a certificate

For security reasons, the machine certificate is protected with a password of your choice.

- Enter the password. You need the password in order to load the machine certificate on the relevant device.



Password

Please enter the password to encrypt the PKCS#12 file

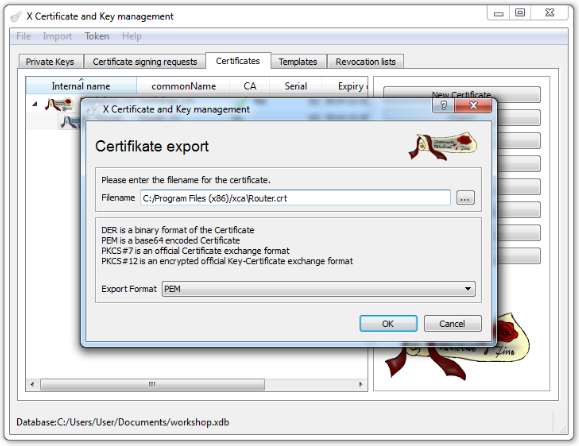
Password •••••

Repeat Password •••••

Database:C:/Users/User/Documents/workshop.xdb

Figure 4-16 Entering the password

- The certificate for the partner must also be exported. This certificate is stored in PEM format without the private key.



Certifikate export

Please enter the filename for the certificate.

Filename C:/Program Files (x86)/xca\Router.crt

DER is a binary format of the Certificate
PEM is a base64 encoded Certificate
PKCS#7 is an official Certificate exchange format
PKCS#12 is an encrypted official Key-Certificate exchange format

Export Format PEM

Database:C:/Users/User/Documents/workshop.xdb

Figure 4-17 Exporting the partner certificate

5 Technical data

5.1 Ordering data

Description	Type	Order No.	Pcs./Pkt.
Industrial LTE 4G router, European version, fallback to 3G UMTS/HSPA and 2G GPRS/EDGE, 2 Ethernet interfaces, firewall, NAT, 2x SMA-F antenna socket	TC ROUTER 3002T-4G	2702528	1
Industrial LTE 3G router, European version, fallback to 2G GPRS/EDGE, 2 Ethernet interfaces, firewall, NAT, SMA-F antenna socket	TC ROUTER 3002T-3G	2702529	1
Industrial LTE 4G router, European version, fallback to 3G UMTS/HSPA and 2G GPRS/EDGE, 2 Ethernet interfaces, firewall, NAT, 2x SMA-F antenna socket	TC ROUTER 2002T-4G	2702530	1
Industrial LTE 3G router, European version, fallback to 2G GPRS/EDGE, 2 Ethernet interfaces, firewall, NAT, SMA-F antenna socket	TC ROUTER 2002T-3G	2702531	1
Industrial LTE 4G router, version for Verizon Wireless (US), 2 Ethernet interfaces, firewall, NAT, IPsec and OpenVPN support, 2x SMA-F antenna socket	TC ROUTER 3002T-4G VZW	2702532	1
Industrial LTE 4G router, version for AT&T (US), fallback to 3G UMTS/HSPA, 2 Ethernet interfaces, firewall, NAT, IPsec and OpenVPN support	TC ROUTER 3002T-4G ATT	2702533	1

Accessories	Type	Order No.	Pcs./Pkt.
Primary-switched TRIO POWER power supply with push-in connection for rail mounting, input: 1-phase, output: 24 V DC/3 A C2LPS	TRIO-PS-2G/1AC/24DC/3/C2LPS	2903147	1
Multiband mobile communication antenna, with mounting bracket for outdoor installation, 5 m antenna cable with SMA circular connector	TC ANT MOBILE WALL 5M	2702273	1
License for mGuard Secure VPN Client v10.0x	MGUARD SECURE VPN CLIENT LIC	2702579	1
Mobile network antenna cable, 5 m in length, SMA (male) -> SMA (female), 50 ohm impedance	PSI-CAB-GSM/UMTS- 5M	2900980	
Mobile network antenna cable, 10 m in length, SMA (male) -> SMA (female), 50 ohm impedance	PSI-CAB-GSM/UMTS-10M	2900981	
Attachment plug with LAMBDA/4 technology as surge protection for coaxial signal interfaces. Connection: plug/socket SMA connectors	CSMA-LAMBDA/4-2.0-BS-SET	2800491	1

5.2 Technical data

Power supply	TC ROUTER ...-4G...	TC ROUTER ...-3G
Supply voltage range	10 V DC ... 30 V DC (SELV, via COMBICON plug-in screw terminal block)	
Typical current consumption	< 200 mA (24 V DC) 65 mA (with activated energy-saving mode)	
Maximum current consumption	1.7 A	
Electrical isolation	VCC // LTE // Ethernet // PE	VCC // UMTS // Ethernet // PE

Functions	TC ROUTER 3002T...	TC ROUTER 2002T...
Management	Web-based management, SNMP	
Firewall rules	Stateful inspection firewall	
Filtering	IP, port, protocol	
Number of VPN tunnels	3	-
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) according to IEEE 802.3u	
Number of channels	2 (SELV)
Connection method	RJ45 socket, shielded
Serial transmission speed	10/100 Mbps, auto-negotiation
Transmission length	100 m (twisted pair, shielded)
Supported protocols	TCP/IP, UDP/IP, FTP, HTTP(S)
Secondary protocols	ARP, DHCP, PING (ICMP), SNMP V1/V2, SMTP(S), NTP, SSL/TLS, STARTTLS

Wireless interface	TC ROUTER 3002T -4G TC ROUTER 2002T -4G	TC ROUTER 3002T -3G TC ROUTER 2002T -3G	TC ROUTER 3002T -4G VZW	TC ROUTER 3002T -4G ATT
Interface description	GSM / GPRS / EDGE / UMTS / HSPA / LTE (FDD)	GSM / GPRS / EDGE / UMTS / HSPA	LTE (FDD)	LTE (FDD) / UMTS / HSPA
Frequency	850 MHz (EGSM, 2 W) 900 MHz (EGSM, 2 W) 1800 MHz (EGSM, 1 W) 1900 MHz (EGSM, 1 W) 850 MHz (UMTS/HSPA B5) 900 MHz (UMTS/HSPA B8) 1900 MHz (UMTS/HSPA B2) 2100 MHz (UMTS/HSPA B1) 800 MHz (LTE B20) 850 MHz (LTE B5) 900 MHz (LTE B8) 1800 MHz (LTE B3) 1900 MHz (LTE B2) 2100 MHz (LTE B1) 2600 MHz (LTE B7)	850 MHz (EGSM, 2 W) 900 MHz (EGSM, 2 W) 1800 MHz (EGSM, 1 W) 1900 MHz (UMTS/HSPA B2) 2100 MHz (UMTS/HSPA B1)	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))	≤ 21.6 Mbps (HSPA (DL)) ≤ 5.76 Mbps (HSPA (UL))	≤ 150 Mbps (LTE (DL)) ≤ 50 Mbps (LTE (UL))	
Antenna	50 Ω impedance SMA antenna socket			
SIM interface	1.8 V, 3 V			
GPRS	Class 12, Class B CS1 ... CS4		-	
EDGE	Multislot Class 10		-	
UMTS	HSPA 3GPP R9	HSPA 3GPP R7	-	HSPA 3GPP R9
LTE	CAT4	-	CAT4	CAT4

Digital input	
Number of inputs	2
Voltage input signal	10…30 V DC
Switching level “1” signal	10…30 V DC

Digital output	
Number of outputs	1 (resistive load)
Voltage output signal	10 V DC ... 30 V DC (depending on the operating voltage)
Current output signal	≤50 mA (not short-circuit-proof)

General data	
Management	Web-based management, SNMP
Degree of protection	IP20 (manufacturer's declaration)
Pollution degree	2 (indoor use only)
Dimensions (W/H/D)	45 mm x 130 mm x 126 mm
Housing material	Plastic gray
Vibration resistance according to EN 60068-2-6/IEC 60068-2-6	5g, 10 ... 150 Hz, 2,5 h, in XYZ direction
Shock according to EN 60068-2-27/IEC 60068-2-27	15g
Noise immunity according to	EN 61000-6-2
Electromagnetic compatibility	Conformance with EMC directive 2014/30/EU

Ambient conditions	TC ROUTER ...-4G...	TC ROUTER ...-3G
Ambient temperature (operation)	-40°C ... 70°C (maximum transmission power of 5 dBm)	-40°C ... 70°C (maximum transmission power of 10 dBm)
	-40°C ... 60°C (maximum transmission power of 23 dBm)	-40°C ... 60°C (maximum transmission power of 23 dBm)
Ambient temperature (storage/transport)	-40°C ... 85°C	
Permissible humidity (operation)	30% ... 95% (non-condensing)	
Permissible humidity (storage/transport)	30% ... 95% (non-condensing)	
Altitude	5000 m (for restrictions see manufacturer's declaration)	

Approvals	TC ROUTER 3002T-4G TC ROUTER 3002T-3G TC ROUTER 2002T-4G TC ROUTER 2002T-3G	TC ROUTER 3002T-4G VZW TC ROUTER 3002T-4G ATT
Conformance	CE-compliant	
Noxious gas test	ISA-S71.04-1985 G3 Harsh Group A	
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

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 intensity 3)
	Air discharge	±8 kV (test intensity 3)
	Comment	Criterion B
Electromagnetic HF field	EN 61000-4-3	
	Frequency range	80 MHz ... 3 GHz (test intensity 3)
	Field strength	10 V/m
	Comment	Criterion A
Fast transients (burst)	EN 61000-4-4	
	Input	±2 kV (test intensity 3)
	Signal	±2 kV (Ethernet)
	Comment	Criterion B
Surge current loads (surge)	EN 61000-4-5	
	Input	±0.5 kV (symmetrical) ±1 kV (asymmetrical)
	Signal	±1 kV (data cable, asymmetrical)
	Comment	Criterion B
Conducted interference	EN 61000-4-6	
	Frequency range	0.15 MHz ... 80 MHz
	Voltage	10 V
	Comment	Criterion A

Noise emission in accordance with EN 61000-6-4	
Radio interference voltage according to EN 55011	Class B, industrial and residential applications
Emitted radio interference according to EN 55011	Class B, industrial and residential applications

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

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	Official Journal of the European Communities 1999/519/EC	Recommendation of the Council of the European Community from July 12,1999
Radio - effective use of the frequency spectrum and avoidance of radio interference	DIN EN 301511	

5.3 Dimensions

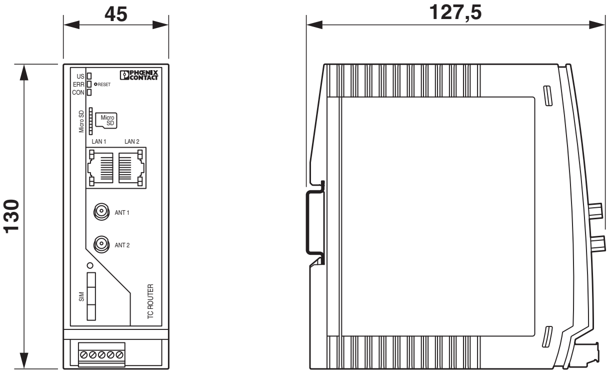


Figure 5-1 Dimensions

A Technical appendix

A 1 XML elements

Table A-1 Data definitions of the XML elements used

Category	XML element	Description
Info	**Device group**	
	serialno	Serial number of the device
	hardware	Hardware version of the device
	firmware	Firmware release
	wbm	Web-based management version
	imei	IMEI of the SIM card
Info	**Radio group**	
	provider	Name of the provider (text)
	rssi	Received signal strength (decimal number 0 ... 99)
	0	-113 dBm or less
	1	-111 dBm
	2 ... 30	-109 dBm ... -53 dBm
	31	-51 dBm or more
	99	Not measured yet or not to be determined
	creg	Status of registration in the mobile network (decimal number 0 ... 5)
	0	Not registered, not searching for cellular network
	1	Registered in home network
	2	Not registered yet, searching for cellular network
	3	Registration rejected
	4	Not used
	5	Registered in another network (roaming)
	lac	Location Area Code (LAC) of the device in a mobile network (hexadecimal number, maximum of 4 digits)
	ci	Cell ID, unique identification of the radio cell within the LAC (hexadecimal number, maximum of 8 digits)

Table A-1 Data definitions of the XML elements used

Category	XML element [...]		Description [...]
Info	packet		Packet data status (decimal number 0 ... 8)
		0	Offline (no Internet connection)
		1	Online (Internet connection)
		2	GPRS online
		3	EDGE online
		4	UMTS online
		5	HSDPA online
		6	HSUPA online
		7	HSDPA+HSUPA online
		8	LTE online
	simstatus		Status of the SIM card (decimal number 0 ... 5)
		0	Unknown
		1	No SIM card
		2	Waiting for PIN
		3	Incorrect PIN entered
		4	Waiting for PUK
		5	Ready
Info	**Inet group**		
	ip		IP address of the packet data connection on the Internet
	rx_bytes		Number of data bytes received so far (decimal number 0 ... 4294967295)
	tx_bytes		Number of data bytes transmitted so far (decimal number 0 ... 4294967295)
	mtu		Maximum Transmission Unit (MTU), the maximum packet size, in bytes, in the packet data network (decimal number 128 ... 1500)
Info	**IO group**		Returned data type, depends on server configuration
		Verbose	Response in words, e.g., on/off
		Numeric	Short numerical response, e.g., 1/0
	gsm		Binary status of the GSM/UMTS connection
	inet		Binary status of the Internet connection (packet data connection)
	vpn		Binary status of the VPN tunnel
SMS	**Send SMS (cmgs)**		
	destaddr		National or international telephone number of the recipient (160 characters maximum) The UTF-8 coded text is specified in the element content. The text may consist of characters that are defined in the GSM 03.38 6.2.1 default alphabet. However, coding must be in UTF-8 as per XML rules.

Table A-1 Data definitions of the XML elements used

Category	XML element [...]	Description [...]
SMS	**Receive SMS (cmgr, UTF-8 text)**	
	origaddr	National or international telephone number of the sender
	timestamp	Time of SMS transmission
	error	Error type (decimal number 1 ... 3)
	1	Empty = no SMS message received
	2	Busy = try again later
	3	System error = communication problem with the radio engine
SMS	**Acknowledge SMS receipt (cmga, text)**	If communication with the GSM/UMTS control program is possible, “ok” is always returned.
	error	Error type (decimal number 8) Only returned if an error is present. In this case “system error” is returned in the cmga element of the error test.
E-mail	**E-mail**	
	to	E-mail address
	cc	E-mail subject, UTF-8 coded text
	body	E-mail message, UTF-8 coded text
IO	**Input element (input)**	
	no	Decimal number 1 ... 6
IO	**Output element (output)**	
	no	Decimal number 1 ... 6
	value	Returned data type depending on server configuration. Both variants are recognized to set or reset outputs:
	Verbose	Response in words, e.g., on/off
	Numeric	Short numerical response, e.g., 1/0

A 2 Structure of the XML configuration file

You can configure the device using an XML file. The device can output and also read in XML files.

A 2.1 XML file format

A valid XML file contains:

- A header which distinguishes the file as XML
- A <config> “root” element

After the <config> element, only the <entry> element is used to specify settings:

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
<entry name="...">...</entry>
...
</config>
```

Only “name” is used as an attribute in the <entry> element. This attribute determines where the data is placed in the file tree. As defined in the header, all data must be specified in the UTF-8 character set.

Line breaks in the data are specified as escape sequences: “&#10;”.

A 2.2 Reference to <entry> element

The described reference is valid as of release 2.01.8.

A 2.3 Local network settings

LAN interface

```
<entry name="conf/network/interface/lan/ipaddr">192.168.0.1</entry>
<entry name="conf/network/interface/lan/netmask">255.255.255.0</entry>
<entry name="conf/network/interface/lan/proto">static</entry>
<entry name="conf/network/interface/lan/ipalias"># IP alias
&#10;#&#10;let alias_cnt=0</entry>
<entry name="conf/network/interface/lan/devlist"></entry>
<entry name="conf/network/interface/lan/ifname">eth0</entry>
<entry name="conf/network/interface/lan/mode">auto</entry>
<entry name="conf/network/interface/lan/type">ethernet</entry>
```

The ./devlist, ./ifname, ./mode, and ./type elements must not be modified. They are also not modified by settings on the configuration page.

./ipaddr	IPv4 address of the device
./netmask	IPv4 netmask
./proto	Type of address assignment: “static” or “dhcp”
./ipalias	This value represents a special list and should only be modified via the configuration page.

DHCP server

```
<entry name="conf/network/dhcp/lan/enable">0</entry>
<entry name="conf/network/dhcp/lan/domain">example.net</entry>
<entry name="conf/network/dhcp/lan/lease">24h</entry>
<entry name="conf/network/dhcp/lan/dynamic">0</entry>
<entry name="conf/network/dhcp/lan/addr1">192.168.0.10</entry>
<entry name="conf/network/dhcp/lan/addr2">192.168.0.30</entry>
<entry name="conf/network/dhcp/lan/hosts"># DHCP hosts&#10;#</entry>
<entry name="conf/network/dhcp/lan/names"># DHCP names&#10;#</entry>
<entry name="conf/network/dhcp/lan/options"># DHCP options&#10;#</entry>
```

./enable		DHCP server
	0	Off
	1	On
./domain		Local domain name, maximum of 64 characters
./lease		Time after which the IP address is automatically renewed
./dynamic		Dynamic address assignment in the specified area
	0	Off
	1	On
./addr1		Area for dynamic address assignment
./addr2		Area for dynamic address assignment
./hosts		List of static MAC at IP assignments This list should only be modified via the configuration page.
./names		Not used at present, must not be modified
./options		Not used at present, must not be modified

Static routes

```
<entry name="conf/network/route/lan/sroute"># static routes
&#10;#</entry>
```

./sroute	List of local static routes This list should only be modified via the configuration page.

SNMP

```
<entry name="conf/snmp/device"></entry>
<entry name="conf/snmp/description"></entry>
<entry name="conf/snmp/location"></entry>
<entry name="conf/snmp/contact"></entry>
<entry name="conf/snmp/rocommunity">public</entry>
<entry name="conf/snmp/rwcommunity"></entry>
<entry name="conf/snmp/rwuser">admin</entry>
<entry name="conf/snmp/secretpass">Snmpadmin</entry>
<entry name="conf/snmp/trap_addr">0.0.0.0</entry>
<entry name="conf/snmp/trap_port">162</entry>
<entry name="conf/snmp/trap_community">public</entry>
<entry name="conf/snmp/trap_enable">0</entry>
<entry name="conf/snmp/v12_enable">0</entry>
<entry name="conf/snmp/v3_enable">0</entry>
<entry name="conf/snmp/fw_local"></entry>
<entry name="conf/snmp/fw_external"></entry>
```

./device	Text descriptions of the same name with a maximum of 250 characters each
./description	Text descriptions of the same name with a maximum of 250 characters each
./location	Text descriptions of the same name with a maximum of 250 characters each
./contact	Text descriptions of the same name with a maximum of 250 characters each
./rocommunity	Password for read access. If the password is left empty, the SNMP service will not be started.
./rwcommunity	Password for write access
./rwuser	User name for SNMPv3 access
./secretpass	Password for SNMPv3 access
./trap_addr	IPv4 trap manager address
./trap_port	IPv4 trap manager port
./trap_community	Password for traps
./trap_enable	Send traps
0	No
1	Yes
./v12_enable	Activate SNMPv1/v2
0	No
1	Yes
./v3_enable	Activate SNMPv3
0	No
1	Yes

The values represent a special list and should only be modified via the configuration page

./fw_local	List of firewall rules for local data
./fw_external	List of firewall rules for external data

A 3 Wireless network

General settings

```
<entry name="conf/gsm/band_setup">515</entry>
<entry name="conf/gsm/sim_timeout">10</entry>
<entry name="conf/gsm/relogin">0</entry>
<entry name="conf/gsm/time">01:00</entry>
```

./band_setup		Bit mask for band selection of the GSM/UMTS/LTE engine
./sim_timeout		Provider timeout in minutes
./relogin		Daily (new) login into the network
	0	No
	1	Yes
./time		Time for daily (new) login into the network

SIM card

```
<entry name="conf/sim1/mcc">262</entry>
<entry name="conf/sim1/cpin"></entry>
<entry name="conf/sim1/roaming">1</entry>
<entry name="conf/sim1/provider">0</entry>
<entry name="conf/sim1/username"></entry>
<entry name="conf/sim1/password"></entry>
<entry name="conf/sim1/apn">web.vodafone.de</entry>
<entry name="conf/sim1/auth_allow">0</entry>
```

./mcc		Code for country selection
./cpin		PIN of the SIM card
./roaming		Roaming allowed
	0	No
	1	Yes
./provider		Code of the selected provider
	0	Auto
./username		User name for packet data network access
./password		Password for packet data network access
./apn		APN access point of the provider
./authallow		Bit mask for permitted access protocols

SMS configuration

```
<entry name="conf/gsm/sms_control">0</entry>
<entry name="conf/gsm/sms_password"></entry>
<entry name="conf/gsm/sms_forward">0</entry>
<entry name="conf/gsm/sms_server">192.168.0.200</entry>
<entry name="conf/gsm/sms_port">1432</entry>
```

./sms_control		Control device via SMS
	0	No
	1	Yes
./sms_password		Password used for control
./sms_forward		Forward received SMS message to a server
	0	No
	1	Yes
./sms_server		IP address of the SMS server
./sms_port		SMS server port

Packet data

```
<entry name="conf/gprs/enable">0</entry>
<entry name="conf/gprs/debug">0</entry>
<entry name="conf/gprs/noccp">0</entry>
<entry name="conf/network/interface/wwan/mtu">1500</entry>
<entry name="conf/gprs/restart">5</entry>
<entry name="conf/gprs/echo-interval">30</entry>
<entry name="conf/gprs/echo-failure">4</entry>
<entry name="conf/gprs/event">0</entry>
```

./enable		Activate packet data
	0	No
	1	Yes
./debug		Activate debug mode for PPP connection establishment
	0	No
	1	Yes
./noccp		Allow data compression
	0	No
	1	Yes
./mtu		Selected MTU (Maximum Transmission Unit) on the PPP interface
./restart		Restart interval in seconds
./echo-interval		Echo interval in seconds
./echo-failure		Number of missing echo responses after which the connection is terminated
./event		Start selection for packet data connection
	0	Start immediately
	1	Control via SMS message
	2	Reserved (do not use)
	3	Control via XML server
	4 ... 5	Control via input 1 ... 2

Static routes

```
<entry name="conf/network/route/wwan/sroute"># static routes
&#10;#</entry>
```

./sroute	List of local static routes. This list should only be modified via the configuration page.

DynDNS

```
<entry name="conf/ddns/enable">0</entry>
<entry name="conf/ddns/provider">0</entry>
<entry name="conf/ddns/server">members.dyndns.org</entry>
<entry name="conf/ddns/username"></entry>
<entry name="conf/ddns/password"></entry>
<entry name="conf/ddns/hostname"></entry>
```

./enable		Activate DynDNS client
	0	No
	1	Yes
./provider		Selection list of supported providers
	0	DynDNS.org
	1	TZO.com
	3	selfHOST.de
	4	custom DynDNS
	5	FesteIP.net
	6	FreeDNS.afraid.org
	7	Hurricane Electric
./server		Server URL for the custom DynDNS server
./username		User name for the DynDNS service
./password		Password for the DynDNS service
./hostname		Own host name which is registered for the DynDNS service

Connection check (connection monitoring)

```
<entry name="conf/conchk/enable">0</entry>
<entry name="conf/conchk/host1"></entry>
<entry name="conf/conchk/host2"></entry>
<entry name="conf/conchk/host3"></entry>
<entry name="conf/conchk/local1">0</entry>
<entry name="conf/conchk/local2">0</entry>
<entry name="conf/conchk/local3">0</entry>
<entry name="conf/conchk/interval">5</entry>
<entry name="conf/conchk/retry">3</entry>
<entry name="conf/conchk/event">0</entry>
```

./enable		Activate connection monitoring
	0	No
	1	Yes
./host[n]		URL or IP address of the host that should respond to the echo request
./local[n]		Wireless network or local network as transmitting interface
	0	Wireless
	1	Local
./interval		Transmission interval in minutes
./retry		Maximum number of missing responses after which an action is triggered
./event		Action selection
	0	None
	1	Restart device (Reboot)
	2	Reconnect packet data (Reconnect)
	3	Reconnect to GSM/UMTS network (Relogin)

Monitoring

```
<entry name="conf/gsm/log_enable">0</entry>
<entry name="conf/gsm/log_duration">24</entry>
<entry name="conf/gsm/log_interval">1</entry>
<entry name="conf/gsm/log_ping"></entry>
```

./log_enable		Activate monitoring
	0	No
	1	Yes
./log_duration		Monitoring duration in hours
./log_interval		Time between two echo requests
./log_ping		URL or IP address of a host that should respond to the echo requests

A 3.1 Network security

General settings

```
<entry name="conf/iptables/fw_enable">1</entry>
<entry name="conf/iptables/nat_enable">0</entry>
<entry name="conf/iptables/fw_netbios">1</entry>
<entry name="conf/iptables/icmp">0</entry>
<entry name="conf/iptables/masq_enable">1</entry>
<entry name="conf/iptables/xssh">0</entry>
<entry name="conf/iptables/xwbm">0</entry>
<entry name="conf/dropbear/enable">0</entry>
<entry name="conf/dropbear/port">22</entry>
```

./fw_enable		State of the overall firewall function
	0	Off
	1	On
./nat_enable		State of the NAT table (port forwarding)
	0	Off
	1	On
./fw_netbios		Block outgoing NetBIOS broadcasts
	0	No
	1	Yes
./icmp		Respond to echo requests at the external interface
	0	No
	1	Yes
./masq_enable		Perform IP masquerading at the external interface
	0	No
	1	Yes
./xssh		External device access via SSH
	0	No
	1	Yes
./xwbm		External device access via HTTP or HTTPS
	0	No
	1	Yes
./enable		Device access via SSH
	0	No
	1	Yes
./port		Port used for SSH access, normally 22

Firewall

```
<entry name="conf/iptables/fw_in"># Firewall incoming
&#10;#</entry>
<entry name="conf/iptables/fw_out"># Firewall outgoing
&#10;#</entry>
```

The values represent a special list and should only be modified via the configuration page.

./fw_in	List of firewall rules for incoming data
./fw_out	List of firewall rules for outgoing data

NAT table

```
<entry name="conf/iptables/nat_fw"># NAT firewall
&#10;#</entry>
<entry name="conf/iptables/nat_vs"># NAT virtual server
&#10;#</entry>
```

The values represent a special list and should only be modified via the configuration page.

./nat_fw	List of firewall rules for the NAT table (port forwarding)
./nat_vs	List of forwarding rules for the NAT table (port forwarding)

A 3.2 VPN

A 3.2.1 IPsec

Higher-level settings

```
<entry name="conf/ipsec/enableupdate">0</entry>
<entry name="conf/ipsec/autoupdate">600</entry>
```

./enableupdate		Monitoring of IP address changes
	0	Off
	1	On
./autoupdate		Monitoring interval in seconds

Connection settings 1 ... n

```
<entry name="conf/ipsec/vpn1/name">vpn1</entry>
<entry name="conf/ipsec/vpn1/enable">0</entry>
<entry name="conf/ipsec/vpn1/rightallowany">0</entry>
<entry name="conf/ipsec/vpn1/host"></entry>
<entry name="conf/ipsec/vpn1/auth">0</entry>
<entry name="conf/ipsec/vpn1/remote_cert">mGuard.crt</entry>
<entry name="conf/ipsec/vpn1/local_cert">test.p12</entry>
<entry name="conf/ipsec/vpn1/remote_id"></entry>
<entry name="conf/ipsec/vpn1/local_id"></entry>
<entry name="conf/ipsec/vpn1/remote_addr">192.168.9.0/24</entry>
<entry name="conf/ipsec/vpn1/local_addr">192.168.0.0/24</entry>
<entry name="conf/ipsec/vpn1/psk">complicated_like_5Dy0qoD_and_long</entry>
<entry name="conf/ipsec/vpn1/nat">0</entry>
<entry name="conf/ipsec/vpn1/local_net">192.168.1.0</entry>
<entry name="conf/ipsec/vpn1/mode">0</entry>
<entry name="conf/ipsec/vpn1/autoreset">0</entry>
<entry name="conf/ipsec/vpn1/resettime">60</entry>
```

./name		Description of the connection
./enable		Connection active
	0	No
	1	Yes
./rightallowany		Accept connection from any partner
	0	No
	1	Yes
./host		URL or IP address of the partner
./auth		Selected authentication method
	0	X.509 certificates
	1	Pre-shared key
./remote_cert		Partner certificate
./local_cert		Local certificate
./remote_id		Partner ID
./local_id		Own ID
./remote_addr		Partner tunnel end
./local_addr		Local tunnel end
./psk		Pre-shared key
./nat		Connection NAT
	0	None
	1	Local 1:1 NAT
	5	Remote masquerading
./local_net		Target of local NAT

./mode		Type of connection
	0	Waiting for connection
	1	Always establish connection
	2	Control via SMS message
	3	Control via call
	4	Control via XML server
	5 ... 6	Control via input 1 ... 2
./autoreset		Automatic connection release
	0	No
	1	Yes
./resettime		Time in minutes after which the connection is re-established

IKE settings (1 ... n)

```
<entry name="conf/ipsec/vpn1/ike_crypt">aes128</entry>
<entry name="conf/ipsec/vpn1/ike_hash">0</entry>
<entry name="conf/ipsec/vpn1/ike_life">3600</entry>
<entry name="conf/ipsec/vpn1/esp_crypt">aes128</entry>
<entry name="conf/ipsec/vpn1/esp_hash">0</entry>
<entry name="conf/ipsec/vpn1/esp_life">28800</entry>
<entry name="conf/ipsec/vpn1/pfs">1</entry>
<entry name="conf/ipsec/vpn1/pfsgroup">modp1024</entry>
<entry name="conf/ipsec/vpn1/rekey">1</entry>
<entry name="conf/ipsec/vpn1/dpd">1</entry>
<entry name="conf/ipsec/vpn1/dpddelay">30</entry>
<entry name="conf/ipsec/vpn1/dpdtimeout">120</entry>
<entry name="conf/ipsec/vpn1/keyingtries">0</entry>
<entry name="conf/ipsec/vpn1/rekeyfuzz">100</entry>
<entry name="conf/ipsec/vpn1/rekeymargin">540</entry>
```

./ike_crypt		Phase 1 ISAKMP encryption, valid values: 3des, aes128, aes192, aes256
./ike_hash		Phase 1 ISAKMP hash
	0	All
	1	MD5
	2	SHA-1
./ike_life		Time in seconds after which the key is renegotiated
./esp_crypt		Phase 2 IPsec SA encryption, valid values: 3des, aes128, aes192, aes256
./esp_hash		Phase 2 IPsec SA hash
	0	All
	1	MD5
	2	SHA-1
./esp_life		Time in seconds after which the key is renegotiated

./pfs		Perfect forward secrecy
	0	No
	1	Yes
./pfsgroup		DH/PFS group, valid values: modp1024, modp1536, modp2048
./rekey		Renew key
	0	No
	1	Yes
./dpd		Dead Peer Detection (DPD)
	0	No
	1	Yes
./dpddelay		Time in seconds between requests
./dpdtimeout		Time in seconds after which the connection is deemed interrupted
./keyingtries		Number of attempts to establish a connection
	0	Unlimited
./rekeyfuzz		Value as a percentage
./rekeymargin		Time in seconds

A 3.2.2 Certificates

```
<entry name="ipsec.d/cacerts/test.crt">
-----BEGIN CERTIFICATE--...</entry>
<entry name="ipsec.d/certs/local/test.crt">
-----BEGIN CERTIFICATE--...</entry>
<entry name="ipsec.d/certs/remote/mGuard.crt">
-----BEGIN CERTIFICATE--...</entry>
<entry name="ipsec.d/private/test.pem">
-----BEGIN RSA PRIVATE KEY--...</entry>
<entry name="ipsec.d/ldir/test.p12">7</entry>
```

./cacerts/*	CA certificates
./certs/local/*	Local certificates
./certs/remote/*	Partner certificates
./private/*	Private key
./ldir/*	Bit mask for certificate validity

A 3.2.3 OpenVPN

Connections 1 ... n

```
<entry name="conf/openvpn/tunnel1/name">tunnel1</entry>
<entry name="conf/openvpn/tunnel1/enable">0</entry>
<entry name="conf/openvpn/tunnel1/event">0</entry>
<entry name="conf/openvpn/tunnel1/host"></entry>
<entry name="conf/openvpn/tunnel1/rport">1194</entry>
<entry name="conf/openvpn/tunnel1/proto">0</entry>
<entry name="conf/openvpn/tunnel1/complzo">0</entry>
<entry name="conf/openvpn/tunnel1/float">0</entry>
<entry name="conf/openvpn/tunnel1/redir">0</entry>
<entry name="conf/openvpn/tunnel1/bind">0</entry>
<entry name="conf/openvpn/tunnel1/lport">1194</entry>
<entry name="conf/openvpn/tunnel1/auth">0</entry>
<entry name="conf/openvpn/tunnel1/certificate">test-server.p12</entry>
<entry name="conf/openvpn/tunnel1/nscert">0</entry>
<entry name="conf/openvpn/tunnel1/psk">my_static.key</entry>
<entry name="conf/openvpn/tunnel1/username"></entry>
<entry name="conf/openvpn/tunnel1/password"></entry>
<entry name="conf/openvpn/tunnel1/remote_ifc">172.16.0.2</entry>
<entry name="conf/openvpn/tunnel1/local_ifc">172.16.0.1</entry>
<entry name="conf/openvpn/tunnel1/remote_addr">192.168.9.0/24</entry>
<entry name="conf/openvpn/tunnel1/nat">0</entry>
<entry name="conf/openvpn/tunnel1/local_masq">0</entry>
<entry name="conf/openvpn/tunnel1/local_addr">192.168.0.0/24</entry>
<entry name="conf/openvpn/tunnel1/local_net">192.168.1.0</entry>
<entry name="conf/openvpn/tunnel1/cipher">BF-CBC</entry>
<entry name="conf/openvpn/tunnel1/keepalive">1</entry>
<entry name="conf/openvpn/tunnel1/ping">30</entry>
<entry name="conf/openvpn/tunnel1/restart">120</entry>
```

./name		Description of the connection
./enable		Connection active
	0	No
	1	Yes
./event		Start selection for the tunnel
	0	Start immediately
	1	Control via SMS message
	2	Control via call
	3	Control via XML server
	4...5	Control via input 1 ... 2
./host		URL or IP address of the partner
./rport		Used partner port
./proto		Protocol
	0	UDP
	1	TCP

./complzo		Settings for data compression
	0	Disabled
	1	Adaptive compression
	2	No compression active
	3	Compression active
	4	Compression allowed
./float		Partner may change its IP address
	0	No
	1	Yes
./redir		All data traffic is routed through the tunnel.
	0	No
	1	Yes
./bind		Specify outgoing port
	0	No
	1	Yes
./lport		Outgoing port
./auth		Authentication
	0	X.509 certificates
	1	Pre-shared key
	2	User name and password
./certificate		Certificate name
./nscert		Check partner certificate type
	0	No
	1	Yes
./psk		Pre-shared key
./username		User name
./password		Password
./remote_ifc		Partner tunnel end
./local_ifc		Local tunnel end
./remote_addr		Partner tunnel network
./nat		Connection NAT
	0	None
	1	Local 1:1 NAT
	4	Local masquerading
	5	Remote masquerading
	6	Port forwarding
	7	Host forwarding

./local_masq		Activate masquerading in the port and host forwarding settings. Otherwise, the value must be set to 0.
	0	Off
	1	On
./local_addr		Local tunnel network
./local_net		Target of local NAT
./cipher		Type of encryption, valid values: BF-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, DES-CBC, DES-EDE-CBC, DES-EDE3-CBC, DESX-CBC, CAST5-CBC, RC2-40-CBC, RC2-64-CBC, RC2-CBC, none
./keepalive		Send Keep Alive packets
	0	No
	1	Yes
./ping		Time in seconds between packets
./restart		Time in minutes after which the connection is re-established

Additional connection settings (1 ... n)

```
<entry name="conf/openvpn/tunnel1/tun_mtu">1500</entry>
<entry name="conf/openvpn/tunnel1/frag_enable">0</entry>
<entry name="conf/openvpn/tunnel1/frag_size">1450</entry>
<entry name="conf/openvpn/tunnel1/mssfix_enable">0</entry>
<entry name="conf/openvpn/tunnel1/mssfix_size">1450</entry>
<entry name="conf/openvpn/tunnel1/reneg_sec">3600</entry>
```

./tun_mtu		MTU (Maximum Transmission Unit) for the TUN device
./frag_enable		Fragmentation of data packets
	0	No
	1	Yes
./frag_size		Size of fragmented packets
./mssfix_enable		MSSFIX option
	0	No
	1	Yes
./mssfix_size		Size of packets with MSSFIX
./reneg_sec		Time in seconds for renewing the key

Port forwarding

```
<entry name="conf/openvpn/napt"># NAPT port forwarding
&#10;#</entry>
```

The values represent a special list and should only be modified via the configuration page.

.napt	List of settings for port forwarding

Certificates

```
<entry name="openvpn/cacerts/test-server.crt">
-----BEGIN CERTIFICATE--...</entry>
<entry name="openvpn/certs/test-server.crt">
-----BEGIN CERTIFICATE--...</entry>
<entry name="openvpn/private/test-server.pem">
-----BEGIN RSA PRIVATE KEY--...</entry>
<entry name="openvpn/ldir/test-server.p12">7</entry>
<entry name="openvpn/casonly/test-ca.crt">
-----BEGIN CERTIFICATE--...</entry>
```

./cacerts/*	CA certificates
./certs/	Certificates
./private/	Private key
./ldir/*	Bit mask for certificate validity
./casonly/*	CA certificates for authentication with user name and password

Static keys

```
<entry name="openvpn/keys/my_static.key">
#&#10;# 2048 bit OpenVPN static key... </entry>
```

./ keys/*	Static keys

Diffie-Hellman parameters

```
<entry name="openvpn/dh1024.pem">
-----BEGIN DH PARAMETERS--...</entry>
<entry name="openvpn/dh2048.pem">
-----BEGIN DH PARAMETERS--...</entry>
```

./dh1024.pem	DH parameter, 1024 bits
./dh2048.pem	DH parameter, 2048 bits

A 3.3 Inputs and outputs

Inputs 1 ... 2

```
<entry name="conf/alerts/in_1/0/enable">0</entry>
<entry name="conf/alerts/in_1/0/action">0</entry>
<entry name="conf/alerts/in_1/0/sms/phonebook">0</entry>
<entry name="conf/alerts/in_1/0/sms/message"></entry>
<entry name="conf/alerts/in_1/0/email/to"></entry>
<entry name="conf/alerts/in_1/0/email/cc"></entry>
<entry name="conf/alerts/in_1/0/email/subject"></entry>
<entry name="conf/alerts/in_1/0/email/message"></entry>
<entry name="conf/alerts/in_1/1/enable">0</entry>
<entry name="conf/alerts/in_1/1/action">0</entry>
<entry name="conf/alerts/in_1/1/sms/phonebook">0</entry>
<entry name="conf/alerts/in_1/1/sms/message"></entry>
<entry name="conf/alerts/in_1/1/email/to"></entry>
<entry name="conf/alerts/in_1/1/email/cc"></entry>
<entry name="conf/alerts/in_1/1/email/subject"></entry>
<entry name="conf/alerts/in_1/1/email/message"></entry>
<entry name="conf/alerts/in_1/alarm_enable">0</entry>
<entry name="conf/alerts/in_1/alarm_time">0</entry>
```

./in_[n]/0/*		Refers to input [n], falling edge
./in_[n]/1/*		Refers to input [n], rising edge
./enable		Enable action for the input
	0	No
	1	Yes
./action		Action on the event
	0	No action
	1	Send SMS message
	3	Send e-mail
./sms/phonebook		Bit mask for phonebook selection
./sms/message		SMS text
./email/to		Recipient of the message
./email/cc		Recipient of a copy
./email/subject		Subject
./email/message		Text message
./alarm_enable		Activate alarm
	0	No
	1	Yes
./alarm_time		Automatic reset time for the alarm in minutes

Output 1

```
<entry name="conf/leds/out_1/function">0</entry>
<entry name="conf/leds/out_1/autoreset">0</entry>
<entry name="conf/leds/out_1/time">10</entry>
```

./out_1		Refers to output 1
./function		Function linked to the output
	0	Manual
	1	Remote controlled
	2	Radio Network
	3	Packet Service
	4	VPN Service
	5	Incoming Call
	6	Connection Lost
	9	Alarm
./autoreset		Automatically reset alarm
	0	No
	1	Yes
./time		Time in minutes to reset the alarm

Phonebook

```
<entry name="conf/phonebook/n01"></entry>
<entry name="conf/phonebook/n02"></entry>
<entry name="conf/phonebook/n03"></entry>
<entry name="conf/phonebook/n04"></entry>
<entry name="conf/phonebook/n05"></entry>
<entry name="conf/phonebook/n06"></entry>
<entry name="conf/phonebook/n07"></entry>
<entry name="conf/phonebook/n08"></entry>
<entry name="conf/phonebook/n09"></entry>
<entry name="conf/phonebook/n10"></entry>
<entry name="conf/phonebook/n11"></entry>
<entry name="conf/phonebook/n12"></entry>
<entry name="conf/phonebook/n13"></entry>
<entry name="conf/phonebook/n14"></entry>
<entry name="conf/phonebook/n15"></entry>
<entry name="conf/phonebook/n16"></entry>
<entry name="conf/phonebook/n17"></entry>
<entry name="conf/phonebook/n18"></entry>
<entry name="conf/phonebook/n19"></entry>
<entry name="conf/phonebook/n20"></entry>
```

./n[xx]	Telephone number in national or international format

Socket server

```
<entry name="conf/alerts/sock_enable">0</entry>
<entry name="conf/alerts/sock_port">1432</entry>
<entry name="conf/alerts/sock_xml_nl">1</entry>
<entry name="conf/alerts/sock_xml_io">0</entry>
```

./sock_enable		Socket server
	0	Off
	1	On
./sock_port		Server listener port
./sock_xml_nl		Character which creates a line break in the XML file
	0	None
	1	Line feed
	2	Carriage return
	3	Carriage return + line feed
./sock_xml_io		Representation of Boolean values
	0	Text
	1	Numeric

A 3.4 System

General system configuration

```
<entry name="conf/system/httpaccess">2</entry>
<entry name="conf/system/httpport">80</entry>
<entry name="conf/system/httpsport">443</entry>
<entry name="conf/system/logremote">0</entry>
<entry name="conf/system/logserver">192.168.0.200</entry>
<entry name="conf/system/logport">514</entry>
<entry name="conf/system/lognvm">0</entry>
```

./httpaccess		HTTP access via:
	0	HTTP
	1	HTTPS
	2	HTTP and HTTPS
./httpport		Port used for the web server for HTTP
./httpsport		Port used for the web server for HTTPS
./logremote		Send log data to a log server
	0	No
	1	Yes
./logserver		IP address of the log server
./logport		Log server port
./lognvm		Reserved, must be set to 0

User authentication

```
<entry name="conf/auth/admin">admin</entry>
<entry name="conf/auth/user">public</entry>
```

For users “admin” and “user”, the passwords are stored in plain text by default. When a new password is assigned, only the hash values are stored here.

E-mail configuration (SMTP)

```
<entry name="conf/smtp/server"></entry>
<entry name="conf/smtp/port">25</entry>
<entry name="conf/smtp/auth">1</entry>
<entry name="conf/smtp/tls">0</entry>
<entry name="conf/smtp/username"></entry>
<entry name="conf/smtp/password"></entry>
<entry name="conf/smtp/from"></entry>
```

./server		Address of the SMTP server
./port		SMTP server port
./auth		Authentication for the server
	0	None
	1	STARTTLS
	2	Encrypted Password
./tls		Reserved, must be set to 0

Default AT commands

```
<entry name="conf/gsm/at1cmd"></entry>
<entry name="conf/gsm/at2cmd"></entry>
<entry name="conf/gprs/at1cmd"></entry>
<entry name="conf/gprs/dialup">*99***1#</entry>
```

./gsm/at1cmd	Commands before PIN entry (without prefixed AT)
./gsm/at2cmd	Commands after PIN entry (without prefixed AT)
./gprs/at1cmd	Commands before PPP dial-in (without prefixed AT)
./gprs/dialup	Dial-in into the packet data network that is used (not used at present)

Date and time

```
<entry name="conf/system/newtime">1388534400</entry>
<entry name="conf/system/ntpenable">0</entry>
<entry name="conf/system/ntpserver">europe.pool.ntp.org</entry>
<entry name="conf/system/ntpiface">0</entry>
<entry name="conf/system/timezone">6+0100</entry>
<entry name="conf/system/daylight">1</entry>
<entry name="conf/system/ntplocal">0</entry>
```

./newtime		Time at device start in seconds, since January 1, 1970 00:00 (UNIX time)
./ntpenable		Synchronize with a time server
	0	No
	1	Yes
./ntpserver		URL or IP address of an Internet time server
./ntpiface		Wireless network or local network as transmitting interface
	0	Wireless
	1	Local
./daylight		Take daylight savings into account
	0	No
	1	Yes
./timezone		Select the time zone
./ntplocal		Make own time available to the local network
	0	No
	1	Yes

Reboot

```
<entry name="conf/system/rebootenable">0</entry>
<entry name="conf/system/reboottime">01:00</entry>
<entry name="conf/system/rebootevent">0</entry>
```

./rebootenable		Bit mask of weekdays on which a reboot should be performed
./reboottime		Time for the reboot
./rebootevent		Selected event for a reboot
	0	None
	1 ... 2	Triggered by the relevant input

A 4 CIDR (Classless Inter-Domain Routing)

IP netmasks and CIDR are methods of notation that combine several IP addresses to create a single address area. An area comprising consecutive addresses is handled like a network.

To specify an area of IP addresses for the router, it may be necessary to specify the address area in CIDR notation. This may be necessary when configuring the firewall, for example. In the table below, the left-hand column shows the IP netmask, while the far right-hand column shows the corresponding CIDR notation.

IP netmask	binary	CIDR
255.255.255.255	11111111 11111111 11111111 11111111	32
255.255.255.254	11111111 11111111 11111111 11111110	31
255.255.255.252	11111111 11111111 11111111 11111100	30
255.255.255.248	11111111 11111111 11111111 11111000	29
255.255.255.240	11111111 11111111 11111111 11110000	28
255.255.255.224	11111111 11111111 11111111 11100000	27
255.255.255.192	11111111 11111111 11111111 11000000	26
255.255.255.128	11111111 11111111 11111111 10000000	25
255.255.255.0	11111111 11111111 11111111 00000000	24
255.255.254.0	11111111 11111111 11111110 00000000	23
255.255.252.0	11111111 11111111 11111100 00000000	22
255.255.248.0	11111111 11111111 11111000 00000000	21
255.255.240.0	11111111 11111111 11110000 00000000	20
255.255.224.0	11111111 11111111 11100000 00000000	19
255.255.192.0	11111111 11111111 11000000 00000000	18
255.255.128.0	11111111 11111111 10000000 00000000	17
255.255.0.0	11111111 11111111 00000000 00000000	16
255.254.0.0	11111111 11111110 00000000 00000000	15
255.252.0.0	11111111 11111100 00000000 00000000	14
255.248.0.0	11111111 11111000 00000000 00000000	13
255.240.0.0	11111111 11110000 00000000 00000000	12
255.224.0.0	11111111 11100000 00000000 00000000	11
255.192.0.0	11111111 11000000 00000000 00000000	10
255.128.0.0	11111111 10000000 00000000 00000000	9
255.0.0.0	11111111 00000000 00000000 00000000	8
254.0.0.0	11111110 00000000 00000000 00000000	7
252.0.0.0	11111100 00000000 00000000 00000000	6
248.0.0.0	11111000 00000000 00000000 00000000	5
240.0.0.0	11110000 00000000 00000000 00000000	4
224.0.0.0	11100000 00000000 00000000 00000000	3
192.0.0.0	11000000 00000000 00000000 00000000	2
128.0.0.0	10000000 00000000 00000000 00000000	1
0.0.0.0	00000000 00000000 00000000 00000000	0

Example: 192.168.1.0/255.255.255.0 corresponds to CIDR: 192.168.1.0/24

B Appendixes

B 1 List of figures

B 2 Index

Please observe the following notes

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

PHOENIX CONTACT Development and Manufacturing, Inc.
586 Fulling Mill Road
Middletown, PA 17057
USA

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com