TAINY iQ

User Manual

Dr. Neuhaus

Sagemcom Dr. Neuhaus GmbH

Papenreye 65

22453 Hamburg

Germany

Internet: http://www.neuhaus.de

Product no.:	3201
Doc. no.:	3202AD010 Version 1.4 / August 2017
Compatible with:	Firmware Version 1.001

Table of Contents

1 Introduction

1.1 Product Overview

Products

This manual provides security instructions and describes the installation and operation of all types of TAINY iQ.

Type		
	Type 4GDSE6	**Type 3GDSE6**
Data	4G / 3G / 2G 6 x Ethernet 24 V DC power supply	3G / 2G 6 x Ethernet 24 V DC power supply
Type		
	Type 4GDSE2	**Type 3GDSE2**
Data	4G / 3G / 2G 2 x Ethernet 24 V DC power supply	3G / 2G 2 x Ethernet 24 V DC power supply

Wireless WAN Connectivity

The TAINY iQ provides a wireless connection to the internet or to a private network.

The TAINY iQ provides this connection anywhere a UMTS network (Universal Mobile Telecommunication System = 3rd generation mobile communications network), a LTE network (Long Term Evolution = 4th generation mobile communications network) or a GSM network (Global System for Mobile Communication = mobile communications network) which provides IP-based data service is available. For UMTS, this means the HSDPA data service (High-Speed Downlink Packet Access), the HSUPA data service (High-Speed Uplink Packet Access), or the UMTS Data Service. For GSM, this means EGPRS (Enhanced General Packet Radio Service = EDGE) or GPRS (General Packet Radio Service).

For HSDPA and HSUPA the term HSPA+ is used in this manual.

Wired WAN Connectivity

The TAINY iQ can also establish WAN connection via Ethernet lines provided it is connected to a router with WAN access or a DSL modem.

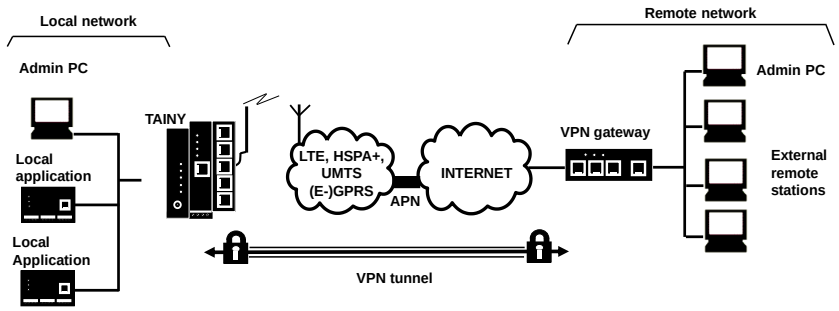
The TAINY iQ connects via up to 6 Ethernet ports locally connected applications or entire networks to the internet. Therefore it uses wireless or wired IP connections. Direct connection can also be made to an intranet which the external remote stations are connected to.

It can establish also a VPN (Virtual Private Network) between a locally connected application/network and an external network using a wireless or wired IP connection and can protect this connection from third party access using IPsec (Internet Protocol Security).

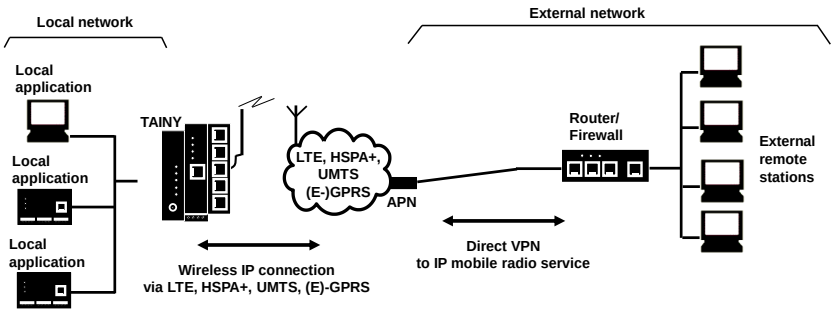
Dual SIM

Being equipped with two SIM card slots, the TAINY iQ enables alternative operation with a second SIM card, i.e. with a second operator, which takes over the communication if a connection over the first SIM card should be interrupted.

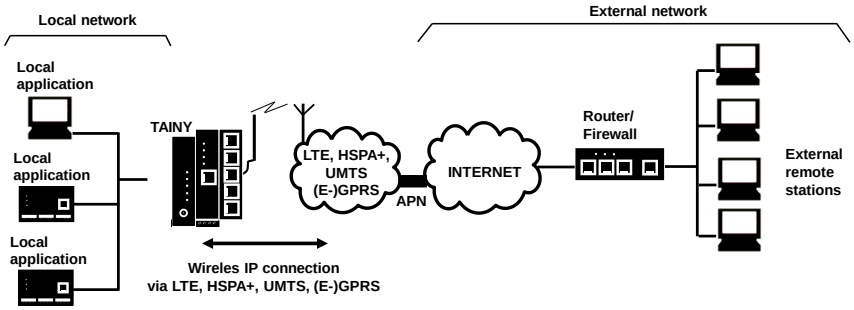
Scenario 1: Virtual Private Network (VPN) with IPsec



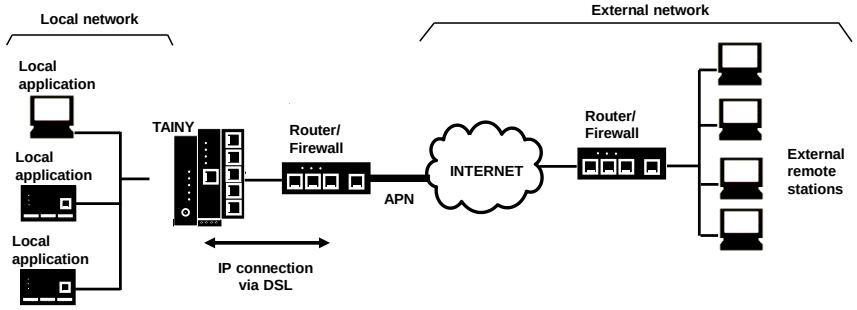
Scenario 2: Connection via HSPA+, UMTS, EGPRS or GPRS or LTE or DSL and a direct VPN to an external network:



Scenario 3: Connection via HSPA+, UMTS, EGPRS or GPRS or LTE or DSL and the Internet to an external network:



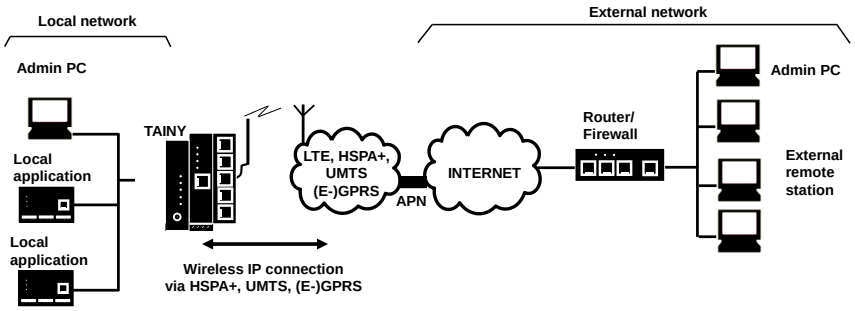
Scenario 4: Connection via DSL and the Internet to an external network.



Local applications could be, for example, a programmable controller, a machine with an Ethernet interface for remote monitoring, or a notebook or desktop PC. These applications use the TAINY iQ to access an external network just as if they had a direct, local connection to the external network.

1.2 Terms

In this section definitions frequently used of terms in this manual are listed:



Local network — Network connected to the local interface of the TAINY iQ. The local network contains at least one local application.

Local interfaces ETH 0, ETH 1, ETH 2, ETH 3, ETH 4, ETH 5 (10/100-Base-T) — Interfaces of the TAINY iQ for connecting the local network. The interfaces are labelled ETH 0 to ETH 5 (10/100 Base-T) on the device. These are Ethernet interfaces with a data rate of 10Mbit/s or 100Mbit/s (Autosensing MDI/MDIX). ETH 0 is directly linked to the router function of the TAINY iQ while ETH 1 to ETH 5 is connected via a switch to the router function. You can route data between ETH 0 and all other ports (see chapter 9.4) or you can use ETH 0 as a wired WAN connection (see chapter 7.5). ETH 1 to ETH 5 can be grouped to VLANs.

Local application — Local applications are network components of the local network, for example a programmable controller, a machine with an Ethernet interface for remote monitoring, or a notebook or desktop PC or the Admin PC.

Admin PC — Computer with Web browser (e.g. Windows Internet Explorer version 11 or later or Mozilla Firefox version 37 or later) connected to the local network or the external network; used to configure the TAINY iQ. The Web browser must support HTTPS.

External network	External network the TAINY iQ is connected to via HSPA+, UMTS, EGPRS or GPRS. External networks are the internet or a private intranet.
External remote stations	External remote stations are network components in an external network, e.g. web servers in the internet, routers in an intranet, a central server of a company, an admin PC, and many more.
(E-)GPRS	EGPRS or GPRS depending on what services are available.
VPN gateway	Component of the external remote network that supports DM VPN and IPsec and which is compatible with the TAINY iQ.
Remote network	External network with which the TAINY iQ is establishing a VPN connection.
Mobile communications network	Infrastructure and technology for wireless mobile verbal and data communication. The TAINY iQ is designed for use in LTE, UMTS mobile communications networks and GSM mobile communications networks.
Certificates Management	Management of TAINY iQ certificates as well external CA Certificates. Possibility to upload, export and mail certificates as well as generate device keys.

2 Safety

The product TAINY iQ complies with the European standard EN60950-1, Safety of Information Technology Equipment.

2.1 Intended Use

The device may only be used as described in this manual and in accordance with the technical data as mentioned in the data sheets.

The device may only be used for intended application in the data sheets and in this document. Proper transport, storage, set-up and assembly, as well as careful operation and service are prerequisite for a fault-free and safe operation of the product.

2.2 Unintended Use

Do not use TAINY iQ without a secure backup in any application which malfunctions could lead to property damage, fatal injuries or death.

2.3 Qualified Personnel

This device may only be installed, operated, commissioned and decommissioned by an electrically skilled person. An electrically skilled person provides sufficient knowledge and experience due to technical training to:

- Turn on, turn off, disconnect, ground and short-circuit electric circuits and devices,
- Duly apply and maintain safety guards in accordance with effective safety requirements,
- Take emergency care of injured

Classification of safety instructions

This manual contains instructions which you must follow for your own personal safety and to prevent property damage. A warning triangle is provided to draw your attention to instructions for your personal safety; no warning triangle is provided for instructions for general property damage. Warning notices are provided in the following sequence according to the decreasing severity of the hazard.

Danger

Indicates a hazardous situation that, if not avoided, will result in death or serious injury.

Warning

Indicates a hazardous situation that, if not avoided, could result in death or serious injury.

Caution

Indicates a hazardous situation that, if not avoided, will result in minor or moderate injury.

Caution

Indicates a hazardous situation, that if not avoided could result in property damage or loss.

Attention

Indicates that an undesired result could occur, if the given instructions are not followed.

Note

Indicates help and advice to improve the operation or set up process.

In the event of multiple hazard levels simultaneously, the warning notice of the highest respective level always applies. If a warning of personal injury is provided in a warning notice with a warning triangle, a warning of property damage can also be added.

2.4 Safety Instructions

The product TAINY iQ complies with the European standard EN60950-1, Safety of Information Technology Equipment. Read the installation instructions carefully before using the device.

General

Danger

Risk of fatal injury by electric shock

- Never install or operate a damaged device.
- Never install or operate if the cables connected to the device are damaged.
- Never connect the device to damaged cables.
- Do not install or operate device outdoors.
- Do not install or operate device in a damp environment.
- Never use device for any other then the intended use.
- Keep device out of reach of children.

Qualified personnel

Danger

Risk of fatal injury by electric shock due to lack of knowledge

- Installation and operation must be carried out by skilled personnel only.
- Also the installation of joining devices such as the antenna must be carried out by skilled personnel only.
- Read manual carefully before installation and operation.
- Follow the safety instructions at all times.
- Make sure the device is electrically isolated before inserting the SIM card.

Intended use

Warning

Risk of injury or damaged device

- Only use device for its intended purpose.
- Operate the device in accordance with the electrical data as stated in the data sheet.
- Only assemble and disassemble device as described in the manual.
- Transport and store device with great care.

Handling cables

Warning

Risk of electric shock due to wrong handling of cables

- Never remove the plug from the socket by pulling the cable, always pull the plug.
- Never route cables over sharp edges or corners without an edge guard.
- Ensure sufficient strain relief for the cable.

Antenna assembly

Attention

Risk of diminished transmission and reception

- Mind the bending radii when routing the antenna cable.
- The minimum bending radius of the cable may not exceed:
  - statically 5 times its diameter
  - dynamically 15 times its diameter

HF exposure

Warning

Risk of interference and damage of other devices due to radio transmitters

- Never use the device in an environment in which the operation of radio equipment is prohibited.
- People with hearing aids or pacemakers may not get near the device. If in doubt ask a medical doctor or the manufacturer of medical device for advice.
- The internal/external antennas of this device must always be placed and operated at least 20 cm away from people.

Warning

Risk of property damage due to demagnetization

- Do not store diskettes, credit cards or any other magnetic data carrier in the vicinity of the device

Caution

Risk of breach legal regulations and interference with other transmitters

- Mind the limit of public exposure to electromagnetic fields (0 hertz to 300 gigahertz) when using a directional antenna. See the council recommendation 199/519/EG dated July, 12, 1999 for details.
- The internal/external antennas of this device must always be placed and operated at least 20 cm away from people
- The antennas must be commissioned and operated in a way they could not interact with other antennas or transmitters.

Warning

Risk of data loss due to demagnetization

- Do not store diskettes, credit cards or any other magnetic data carrier in the vicinity of the device.

External Power Supply

Warning

Risk of damaging the device due to false voltage

- Use only power supplies that are conforming with the EN 60950-1 standard.
- The output voltage of the supply must not exceed 60 V DC.
- The output of the external power supply must be short circuit proofed.

Warning

Risk of damaging the device due false battery connection

- Ensure that an all-pole disconnecting device (battery main switch) with sufficient disconnecting capacity and fuse with sufficient disconnecting capacity (fuse set 32 V, 3A) is provided between the device and the battery or rechargeable battery.

Warning

Risk of damaging the device due to false supply

- Use only power supplies that are conform to the standard IEV/EN 60950 2.5 “Limited Power Source”.
- The external power supply must also comply with the requirements for NEC Class 2 circuit as defined in the National Electric Code (ANSI/NFPA 70).

In port and switching output

Warning

Risk of property damage or injuries due to false voltage

- The in port and switching output are both galvanic insulated against all other terminals of the TAINY iQ. If the external installation being connected to the TAINY iQ connects a signal of the in port and switching output galvanically to a power supply signal of the TAINY iQ, the voltage between each signal of the in port and switching output and each signal of the power supply may not exceed 60V.

Caution: Costs

Caution

Risk of additional financial costs

- Bear in mind that the exchange of data packages is subject to charges whether a connection to a remote station is maintained or re-established.
- Unsuccessful attempts to connect to incorrect addresses or switch off remote stations are subject to charges.

Firmware with open source GPL/LGPL

The firmware for TAINY iQ contains open source software under GPL/LGPL conditions. We provide you with the source code in accordance with Section 3b of GPL and Section 6b of LGPL. You can find the source code on our webpage, www.neuhaus.de.

As an alternative, you can also request the source code from us on CD-ROM. Send your email to Kundendienst@neuhaus.de. Please enter "Open Source iQ" in the subject line of your email so that we can easily filter out your message.

The license conditions for the open source software can be found in the source code on the product CD.

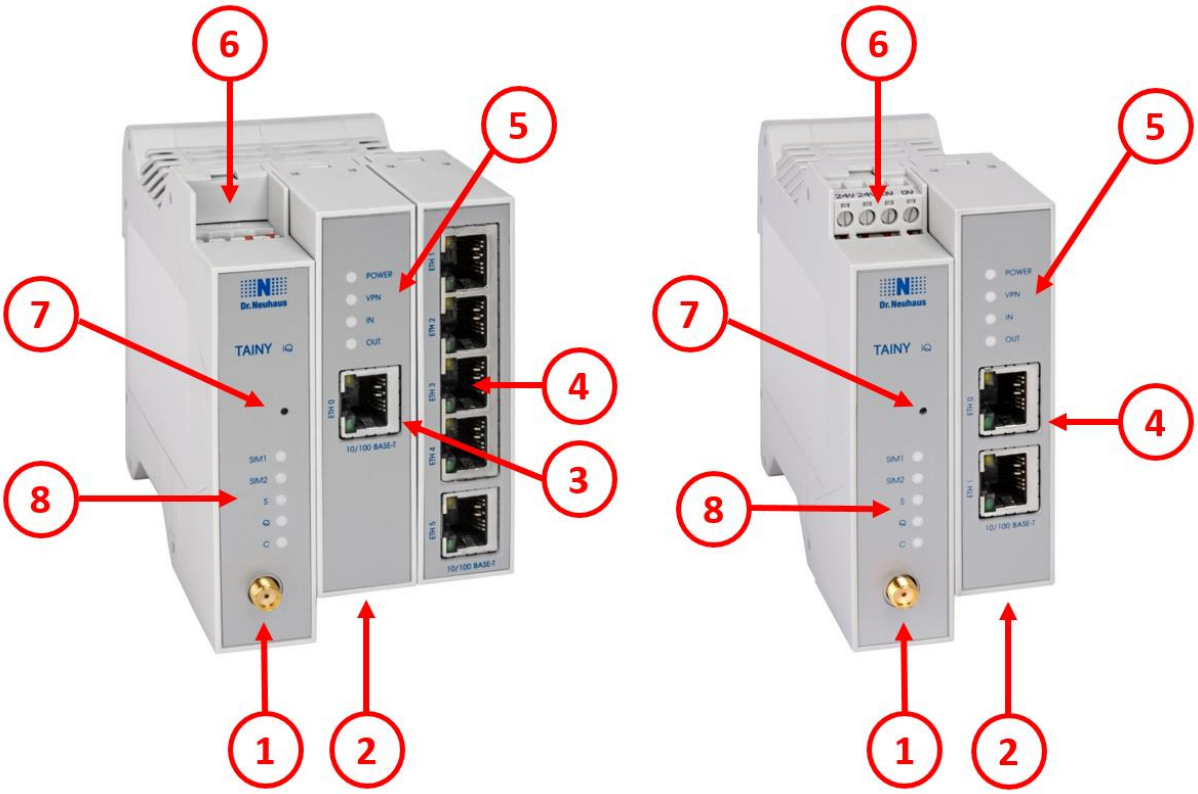
Firmware with OpenBSD

The firmware of the TAINY iQ contains parts from the OpenBSD software. Whenever OpenBSD software is used, the following copyright note must be reproduced:

```
* Copyright (c) 1982, 1986, 1990, 1991, 1993
* The Regents of the University of California. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    This product includes software developed by the University of
*    California, Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
* WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
```

3 Product Description

3.1 Controls



1	Antenna socket
2	Digital Input / Output
3,4	Ethernet Ports
5,8	Signal lamps
6	24V Power Input
7	Service Button

3.2 Functions

Functions

Communication

Wireless modem for flexible data communication in LTE networks

Wireless modem for flexible data communication in UMTS networks

- via HSPA+, UMTS

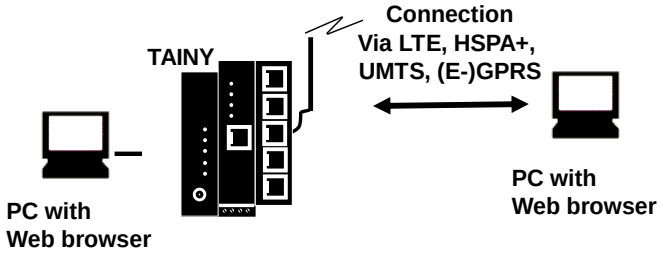
Wireless modem for flexible data communication in GSM networks

- EGPRS, GPRS

Configuration

The device can be configured via a Web user interface that can simply be displayed using a Web browser. It can be accessed by means of the following:

- the local interface, or
- LTE, HSPA+, UMTS, EGPRS, GPRS



VPN functions

The TAINY iQ provides the following VPN features

- VPN router for secure data transfer via public networks
- Dynamic Multipoint VPN
- Protocols: GRE, NHRP, IPsec
- IPsec-3DES encryption with 192 bit
- IPsec-AES encryption with 128, 192 and 256 bit
- Package authentication: MD5, SHA-1
- Internet Key Exchange (IKE) with main and aggressive mode
- Authentication: Pre shared Key (PSK)
- NAT-T
- Dead Peer Detection (DPD)
- Authentication by certificates
- Status display of established IPsec connections

Firewall functions

The TAINY iQ provides the following firewall functions to protect the local network and itself from external attacks:

- Stateful inspection firewall
- Anti-spoofing
- Port forwarding
- Activation of HTTP-,SSH-, ICMP- and SNMP-services for WAN
- Unknown data packets are written in the logbook

Additional functions

The TAINY iQ provides the following additional functions:

- Alternative login via TACACS+
- DNS cache
- DHCP server
- NTP
- In Port, Switching Output
- Web user interface for configuration
- SNMP for control and configuration
- Management of certificates
- Sending emails and snapshots

4 Installation

4.1 Step by step

Please always also refer to the mentioned chapter. This is not to be seen as a brief instruction and replacement for this manual. The TAINY iQ is set up by the following steps:

Step		Chapter
1.	First familiarise yourself with the preconditions for operating the TAINY iQ.	3.1
2.	Read the safety instructions and other instructions at the beginning of this user manual **very carefully** and make sure to understand and follow them.	1.11, 2, 3
3.	Also familiarise yourself with the control elements, connections and operating state indicators of the TAINY iQ before installation.	3
4.	Connect the web browser of your pc to one of the local interfaces (10/100 BASE-T) of the TAINY iQ.	5.4
5.	Enter the PIN(s) –personal identification number – of the SIM card(s) into the web user interface of TAINY iQ.	7.4
6.	Disconnect the TAINY iQ from the power supply.	4.3
7.	Insert the SIM card(s) into the device.	4.9
8.	Connect the antenna.	4.5
9.	Connect the TAINY iQ to a power supply.	4.3
10.	Set up the TAINY iQ according to your requirements.	5 to 13
11.	Configure ETH0 port to get six LAN ports (if required).	9.4
12.	Connect your local application.	4.4

4.2 Preconditions and Information

To operate the TAINY iQ, the following information must be on hand and the following preconditions must be fulfilled:

Antenna	An antenna as described in chapter 4.5.
Power supply	A 24 V installation. See chapter 4.3.
SIM card	A SIM card from the chosen GSM network operator.
PIN	The PIN for the SIM card.
HSPA+ / UMTS EGPRS / GPRS activation	The services LTE, HSPA+, UMTS data and / or EGPRS or GPRS must be enabled on the SIM card by your mobile communications network provider. The access data must be known: - Access Point Name (APN) - User name - Password

4.3 Connection to 24V/0V power supply

Please read the safety instruction carefully before installation.

The TAINY iQ operates with direct current of from 12-60 V DC, nominally 24 V DC.

The external power supply is connected at the screw terminals on the left-hand side of the device.

The current consumption is round about 450 mA at 12 V and 100 mA at 60 V (I_{Burst}>1.26 A)

Warning

Risk of injuries or property damage due to false voltage

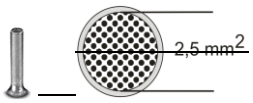
- The In port and switching outport are both galvanically insulated against all other terminals of the TAINY iQ. If the external installation being connected to the TAINY iQ connects a signal of the In port and switching output galvanically to a power supply signal of the TAINY iQ, the voltage between each signal of the In port and switching output and each signal of the power supply may not exceed 60V.

Terminals

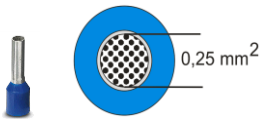
Cross-section rigid/flexible	0,2-2,5 mm² (see Note)
AWG	24-14
Isolation stripped length L	7 mm
Locked torque	0,5-0,6 Nm / 4,4-5,3 lb in

To ensure a reliable and finger-safe connection, strip the isolations as written in the table above and use end sleeves for flexible cables. Close unused terminals.

The maximum valid cross-section of flexible cables using end sleeves **without** plastic shells is 2,5 mm².



The maximum valid cross-section for flexible cables using end sleeves **with** plastic shells is 0,25 mm².



4.4 Ethernet Ports (ETH0, ETH1, ETH2, ETH3, ETH4, ETH5)

4 3

The Ethernet Ports ETH1 to ETH5 (10/100 Base-T) for the E 6 variants and ETH1 for the E 2 variants are used to connect the local network with local applications e.g. a programmable controller, a machine with an Ethernet interface for remote monitoring, or a notebook or desktop PC.

The TAINY iQ acts as a switch between the available interfaces.

To set up the TAINY iQ, connect the Admin PC with Web browser here.

The Ethernet Ports ETH0 is dedicated to establish wired WAN-DSL/LAN connections, however it can also be used as an additional port to connect the local network with local applications. See chapter 9.4

CAT5 cables shall be used. All interfaces supports auto negotiation. It is thus detected automatically whether a transmission speed of 10 Mbit/s or 100 Mbit/s is used on the Ethernet. It is also automatically detected whether cross-over or one-to-one cables are used.

4.5 Antenna socket

1

The TAINY iQ has one SMA type antenna jack to connect an antenna.

Please make sure, that during operation always an antenna is connected to the TAINY iQ.

Requirements for the antenna::

Passive, azimuthally, omnidirectional, vertical polarisation, gain < 1,5 dBi, VSWR < 2,0:1, impedance 50 Ω, matched for the used frequency bands. See chapter 17 for a list of supported frequency bands.

Which frequency bands are actually used at the location is dependent on the country and the network operator. Contact your network operator for this information Please obtain this information from your network operator.

Caution

Risk of property damage and interference with other devices

- Please use only antennas from the accessories line for TAINY iQ. These antennas have been tested by us and guarantee the described product features.

Attention

Risk of diminished transmission and reception

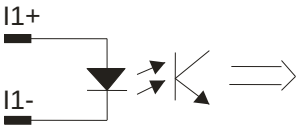
- When installing the antenna, a sufficiently good signal quality must be ensured (CSQ > 11).
- Use the signal lamps of the TAINY iQ which show the signal quality or the webpage *Status Overview*, see chapter 5.1.
- Make sure that there are no large metal objects (e.g. reinforced concrete) close to the antenna.
- Read the antenna's installation and user guide before operating it.

4.6 Digital Input / Output

Digital Input

2

The TAINY iQ has an In port. The screw terminals are designated I1+/I1-.



U_{In} = 5 …30V; ON: $U_{In} \geq$ 5 V; OFF: $U_{In} \leq$ 1,2 V

This port is the Gate Input for WAN Setup Operation Rules, see chapter 7.3.

Warning:

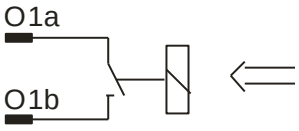
Risk of injuries or property damage due to false voltage

- The In port is galvanically insulated against all other terminals of the TAINY iQ. If the external installation being connected to the TAINY iQ connects a signal of the In port galvanically to a power supply signal of the TAINY iQ, the voltage between each signal of the In port and each signal of the power supply may not exceed 60V.

Switching output O1a/ O1b

2

The TAINY iQ has a switching output. The screw terminals are designated O1a/O1b.



U_{Max} = 30 V; I_{Max} = 20 mA

This port is the Switching Output for WAN Setup Operation Rules, see chapter 7.3. When the switching output is active the switch is closed.

Warning

Risk of injuries or property damage due to false voltage

- The switching output is galvanically insulated against all other terminals of the TAINY iQ. If the external installation being connected to the TAINY iQ connects a signal of the switching output galvanically to a power supply signal of the TAINY iQ, the voltage between each signal of the switching output and each signal of the power supply may not exceed 60V.

4.7 Signal lamps

The TAINY iQ is equipped with a set of signal lamps for display of the operating status.

5

Power Supply Signal

LED	Status	Meaning
POWER	Always OFF	No supply voltage available or defect.
	Always ON	In operation

8

WAN Status Signals

LED	Status	Meaning
SIM 1	Constantly OFF	Not in use
	Constantly ON	Active SIM
SIM 2	Constantly OFF	Not in use
	Constantly ON	Active SIM
S (Status)	Flashing	Not registered to mobile net
	Constantly ON	WAN IP connection available (Cellular or Ethernet)
Q (Quality)	Flashing slowly	Logging into the GSM network
	Flash 1 time with interval	Field strength poor
	Flash 2 times with interval	Field strength moderate
	Flash 3 times with interval	Field strength good
	Constantly ON	Field strength very good
	Constantly OFF	Field strength info not available
C (Connect)	Always OFF	No connection
	Flash 1 time with interval	GPRS/EDGE connection
	Flash 2 times with interval	UMTS connection
	Flash 3 times with interval	LAN connection

5

VPN and IO Status Signals

LED	Status	Meaning
VPN	Constantly OFF	No VPN tunnel established
	Constantly ON	One or more VPN tunnel established
IN	Constantly OFF	Input not active
	Constantly ON	Input active
Out	Constantly OFF	Output not active
	Constantly ON	Output active

4

Ethernet Ports Status Signals

Each Ethernet Port ETH is equipped with a yellow and green LED which indicates the operational status of the port.

LED	Status	Meaning
Green	Constantly ON	Link established
	Constantly Off	No link established
Yellow	Flashing	Data transfer

4.8 Service button

7

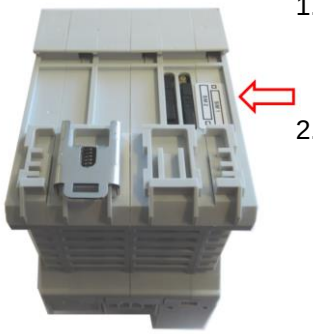
There is a small hole on the front side of the TAINY iQ where a button is located. Use a thin object, such as a straightened paper clip, to press the button.

➲ When you press the button during operation for longer than 5 seconds the factory configuration is loaded.

4.9 SIM card holder

Attention

Before inserting a SIM card, enter the PIN of the SIM card in the TAINY iQ via the Web user interface. See Chapter 7.4



1. After you have entered the PIN of the SIM card, disconnect the TAINY iQ completely from the power supply.

2. The drawer(s) for the SIM card(s) is located on the back of the device. Right next to each drawer for the SIM card in the housing aperture there is a small yellow button. Press on this button with a pointed object, for example a pencil.

   When the button is pressed the SIM card drawer comes out of the housing.

3. Place the SIM card in the drawer so that its gold-plated contacts remain visible.

4. Then push the drawer with the SIM card completely into the housing.

Caution

Risk of damage or loss of SIM card or the entire device

- Do not under any circumstances insert or remove the SIM card during operation.

4.10 Mounting

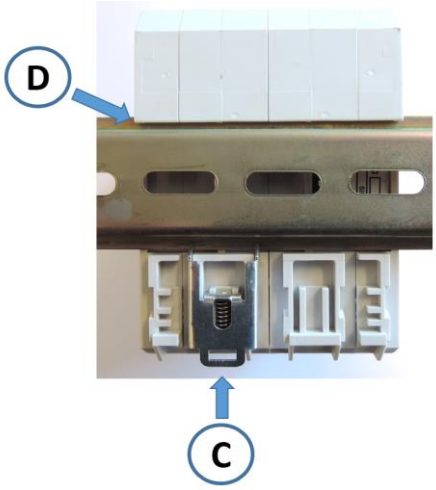
The TAINY iQ is suitable for mounting on cap rails in accordance with DIN EN 50022 (3.5mm). The corresponding mount is located on the rear side of the device.

Warning

Risk of injury and property loss due to touching voltage-carrying parts

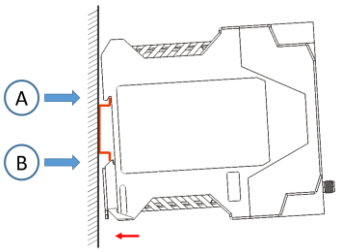
- After installation, the TAINY iQ, especially the screw terminal area (Digital Input / Output terminal or 24V terminal) must be covered to avoid accidental touch of voltage-carrying parts.
- Prohibit the intrusion of foreign bodies, e.g. screws, paper clips or other metal parts.

At the rear side the TAINY iQ has a notch (D) to hook it at the top of the cap rail. One metal spring fastener (C) lock the TAINY iQ at the bottom of the cap rail. It can be released again by pulling the down with a screw driver.



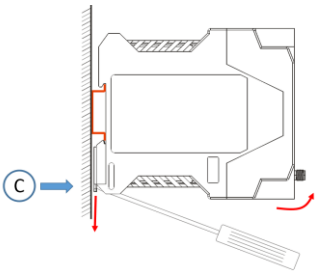
Mounting:

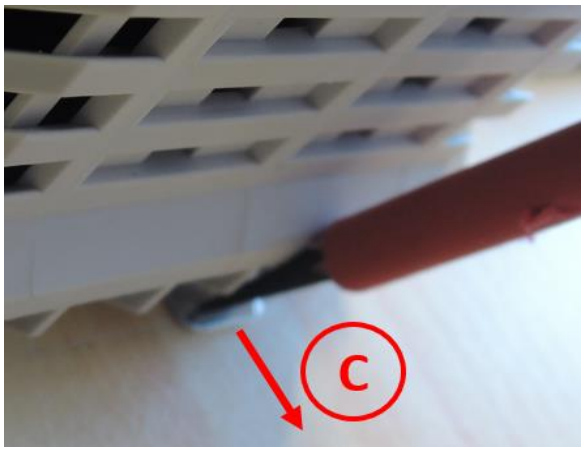
Hook the TAINY iQ at the cap rail (A) and push the lower part of the TAINY iQ carefully in direction to the cap rail (B) until it snap-in the cap rail.



Unmounting:

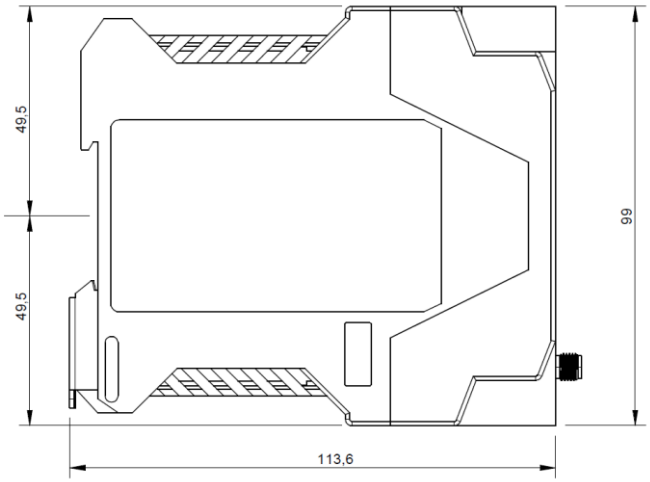
Use a flat-head screw driver to pull down the cap rail fixation (C) until the TAINY iQ is detached.





Mounting:

Position of the cap rail:



[mm]

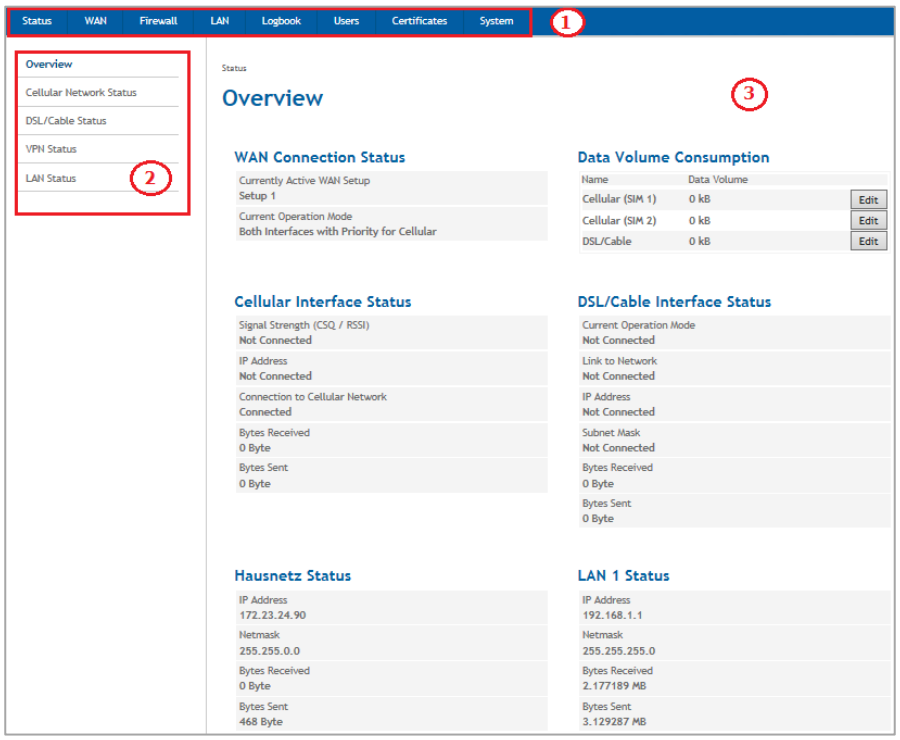
5 Configuration

5.1 Overview Screens

The settings for TAINY iQ are configured on various tabs. All tabs consist of a tab bar (1) at the top, a menu (2) on the left and the dialog box (3).

For illustration purposes the tab bar as shown in the left text column throughout this manual only reflects the tab in question.

Please also bear in mind that not all tabs of all TAINY iQ types contain the same information or configuration possibilities in the dialog box. Again see the left text column of this manual for the corresponding device types.



Note

Please remember that the names you enter for a new network i.e. in the entry field “`Name`” might not exceed 20 digits.

5.2 Overview

Configuration of TAINY iQ functions is carried out locally or remotely via the Web-based administration interface of the TAINY iQ.

Remote configuration

Remote access to the web server is possible by either a particular setting of the firewall or the default setting of a VPN tunnel via HTTPS.

Configuration via the local interface

The preconditions for the initial configuration via the local interface are:

- The computer (Admin PC) that you use to carry out configuration must be either:
  - connected directly to one of the Ethernet ports of TAINY iQ via a network cable

  or
  - it must have direct access to the TAINY iQ via the local network.

By default the LAN ports ETH1 to ETH5 of TAINY iQ are part of one local network with the IP address 192.168.1.1 and Subnet mask 255.255.255.0. So you have to do the following settings for your PC:

- The network adapter of the computer (Admin PC) that you use to carry out configuration must have the following TCP/IPconfiguration:

  IP address: **192.168.1.2**

  Subnet mask: **255.255.255.0**

  Instead of the IP address **192.168.1.2** you can also use other IP addresses from the **range 192.168.1.x**. except the addresses 192.168.1.0, 192.168.1.1 und 192.168.1.255.

- If you also wish to use the Admin PC to access the external network via the TAINY iQ, the following additional settings are necessary:

  Standard gateway: **192.168.1.1**

  Preferred DNS server: **Address of the domain name server**

See chapter 9.4 if ETH0 shall be used as a LAN port too.

5.3 Valid characters for user names, passwords and other inputs

Valid characters

For user names, passwords, host names, APN and PIN the following ASCII characters may be used:

usernames and passwords	# @ ~ % $, * ' = ! + - \ / ? ( ) { } . : ; [ ] _ | 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z
hostnames and APN	. – 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z
PIN	PINs support numeric characters only 0 1 2 3 4 5 6 7 8 9

Some parameters accept additional special characters.

5.4 Establishing a configuration connection

Set up a Web browser

Proceed as follows:

Open the start page of the TAINY iQ

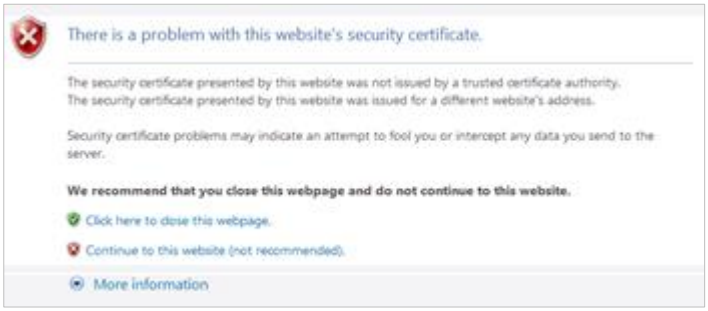
Launch the Web browser (e.g. MS Internet Explorer Version 11 or later or Mozilla Firefox Version 37 or later).

Enter the full TAINY iQ address in the address line of the browser.

The factory setting is: https://192.168.1.1

Result: A security message appears. In Internet Explorer 7, for example, it is the following:

Confirm the security message



Acknowledge the corresponding safety message with "Continue loading this page …"

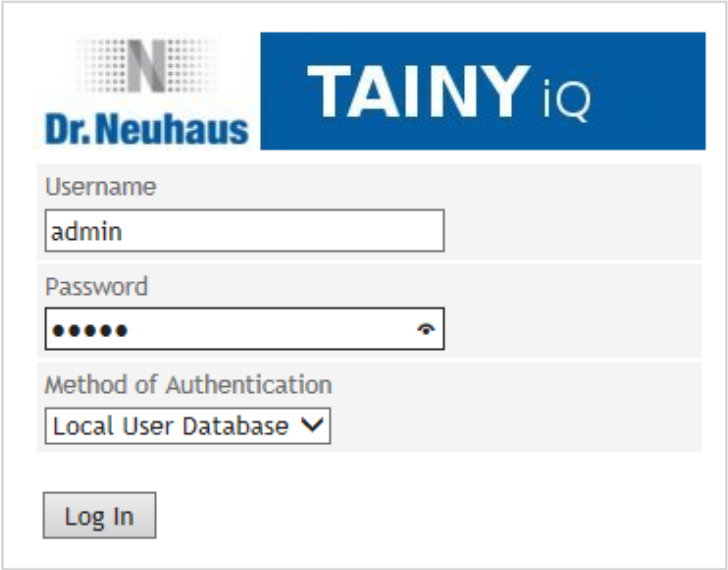
Note

Because the device can only be administered via encrypted access, it is delivered with a self-signed certificate. In the case of certificates with signatures that are unknown to the operating system, a security message is generated. You can display the certificate.

It must be clear from the certificate that it was issued for Sagemcom Dr. Neuhaus GmbH. Since the web user interface is addressed via an IP address and not a name, the name specified in the security certificate, is different from the one in the certificate.

Enter the user name and password

You will be asked to enter the user name and the password:



The factory settings are:

User name:	**admin**
Password:	**<serial number of the device>**
Example	*15044201/28/2015*

Note

You should change the password in any event. The factory settings are general knowledge and do not provide sufficient protection. Refer to chapter 11 on how to change the password.

Open the start page by clicking on “Log In”.

Note

To register successfully on the TAINY iQ activate the cookies in your browser.

Note

The registration screen will open a selection menu, in which the registration can be made via TACACS+ or the normal, local registration. The initial local registration process is described below, which is used when commissioning the device. For further information on registration via TACACS+, see Chapter 11.2 and the Glossary.

The start page is displayed

After entering the user name and password the start page of the TAINY iQ appears in the Web browser. It provides an overview of the operating state, see Chapter 6.

5.5 Terminating a configuration connection (Logging out)

Log Out

Click the *Log Out* button at the top right of the screen to sign out manually. This will terminate the configuration connection to TAINY iQ. The webserver will return to the start screen.

In order to re-establish the configuration connection, you have to enter your user name and password again.

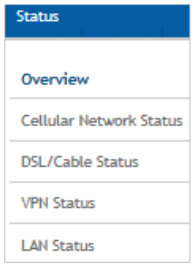
Please refer to chapter 5.4.

6 Status overview

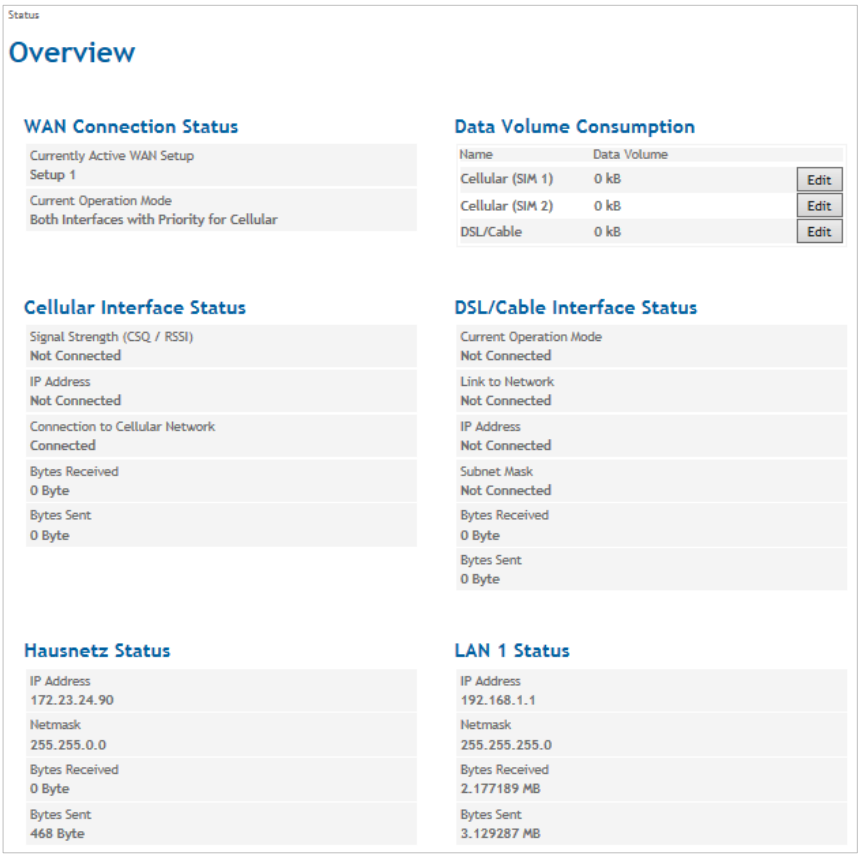
6.1 Get a Status Overview

Overview

4GDSE6
3GDSE6

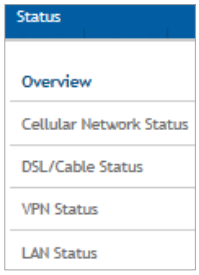


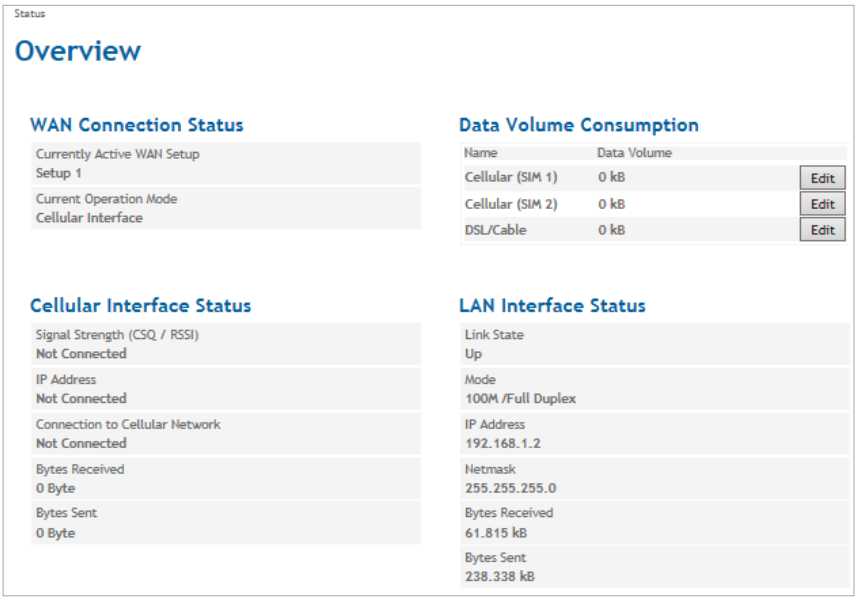
Click on the **`Status`** tab and select "**`Overview`**" to open the screen.



Overview

3GDSE2
4GDSE2





After a successful log-in to the TAINY iQ's web user interface select "**Status**" from the menu bar at the top left. An overview of the current operating status of TAINY iQ appears. It displays the status of the:

- WAN connection
- Cellular Interface
- Data Volume Consumption
- DSL/Cable Interface
- Active LAN Interface

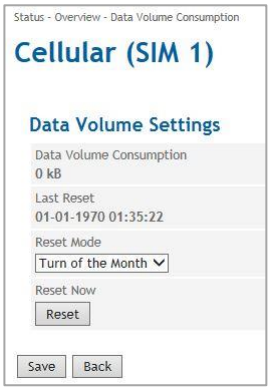
Note

The displayed values are automatically refreshed by the TAINY iQ.

Signal strength: Indicates the strength of the received signal of cellular network as a CSQ value (see Glossary) and a RSSI value.

Bytes Received / Bytes Sent: Indicates the number of received or sent bytes since the connection has been established. They will be reset when the connection is re-established.

Data Volume Consumption

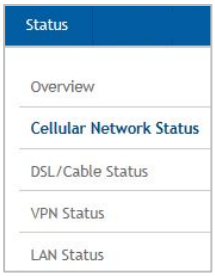


Define in which time interval the value of the data volume consumption is set back to zero. The default setting is monthly (at the first day of each month). To change the settings select another interval from the dropdown list "Reset Mode".

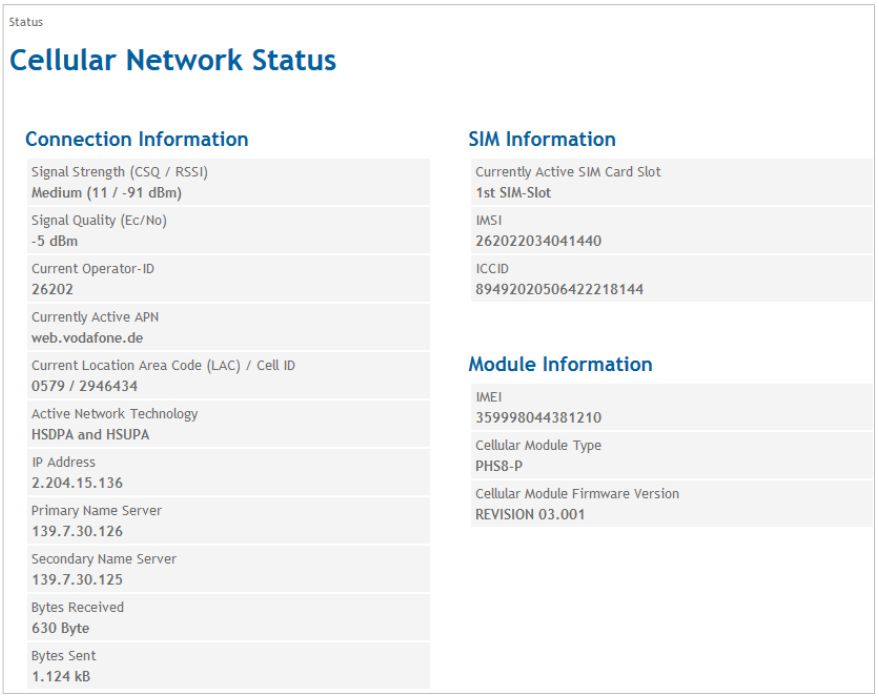
To reset the value to zero right away click the "Reset" button.

6.2 Get the Cellular Network Status

Cellular Network Status



Click on the **`Status`** tab and select "**`Cellular Network Status`**" to open the screen.



Indicates the signal strength, signal quality, information about the used cellular network, the SIM card and the cellular engine embedded in the TAINY iQ.

For CSQ, LAC (Cell ID), IMCI, ICCID, IMEI, see Glossary

Note

The displayed values are automatically refreshed by the TAINY iQ.

`Bytes Received / Bytes Sent`: Indicates the number of received or sent bytes since the connection has been established. The counters will be reset when the connection will be re-established.

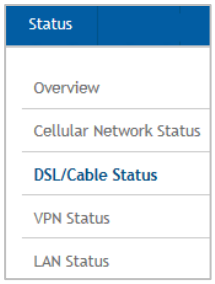
`Cellular Module Type / Cellular Module Firmware Version`: The TAINY iQ is equipped with a cellular module which acts as the radio interface. It handles all the communication over the radio network.

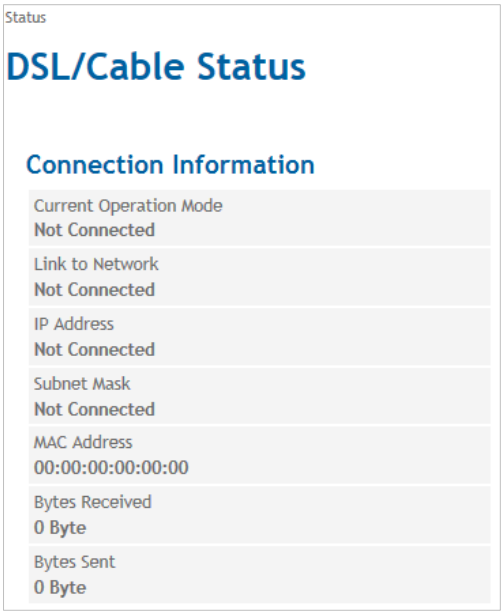
Also the type and firmware version of the cellular module is displayed here.

6.3 Get the DSL/Cable Status

DSL/Cable Status

Click on the **`Status`** tab and select "**`DSL/Cable Status`**" to open the screen.





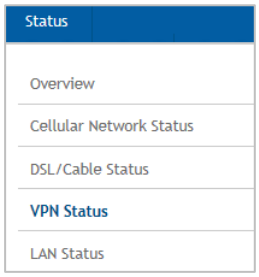
Indicates the status and settings of the WAN connection, if it is established over a wired DSL/Cable connection.

`Bytes Received / Bytes Sent`: Indicates the number of received or sent bytes since the connection has been established. The counters will be reset when the connection is re-established.

6.4 Get the VPN Status

VPN Status

Click on the **`Status`** tab and select "**`VPN Status`**" to open the screen.



Displays a list of the existing ISAKMP SAs (Security Associations).

`Remote IP`: IP address of the other (opposite) party.

`Connected`: "`Yes`" connection is established or "`No`" connection is not established.

SA Type: Defines the convention (connection) two communicating entities use within a secure network.

Static: Indicates a connection that is configured and established by TAINY iQ.

Dynamic: Indicates a connection that is established externally by the other entity.

Connected Since: Displays the timestamp of the connection.

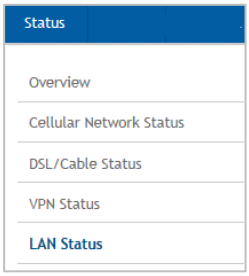
Remote ID: Identifier of the other party/entity.

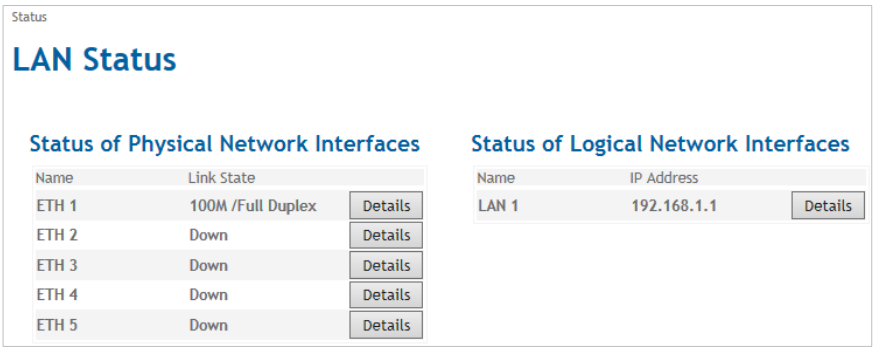
6.5 Get the LAN Status

LAN Status

4GDSE6
3GDSE6

Click on the **Status** tab and select "**LAN Status**" to open the screen.





Indicates the status and settings of the LAN interfaces on physical and logical level.

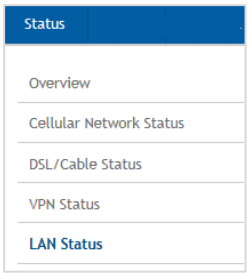
Status of Physical Network Interfaces

Link State: Indicates which type of link is established, e.g. "100M/Full Duplex". If no link via this interface is established it will display "Down".

IP Address: Indicates the IP Address which has been configured for this interface.

ETH x Details

Click on "**Details**" in the Physical Network Interface column to get more information on the selected Physical Network Interface.



Interface Status

Indicates the status of the Link - up / down and the operating mode, e.g. 100M /Full Duplex.

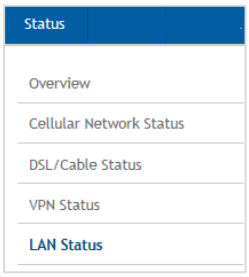
`Dynamic MAC Table`

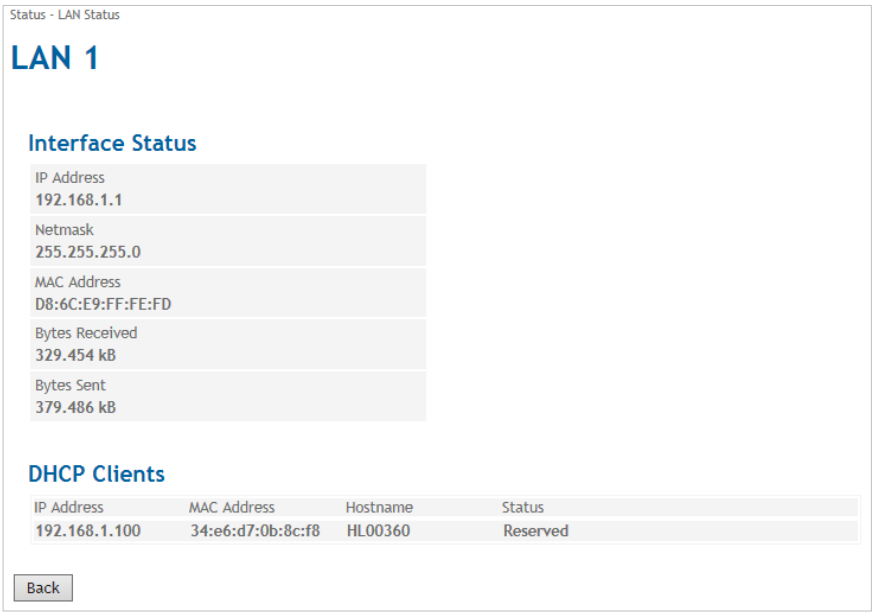
Indicates the MAC address(es) of connected clients or the static MAC table.

`Status of Logical Network Interfaces`

Click on "**`Details`**" in the Logical Network Interface column to get more information about the selected `Logical Network Interface`.

LAN x Details





`Interface Status`

Indicates the IP Address, Netmask and MAC Address which are assigned to this interface.

Bytes Received / Bytes Sent: Indicates the number of received or sent bytes since the connection has been established. They will be reset when the connection is re-established.

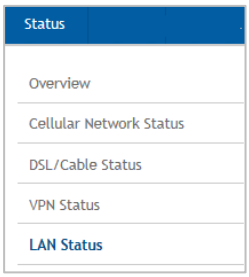
`DHCP Clients`

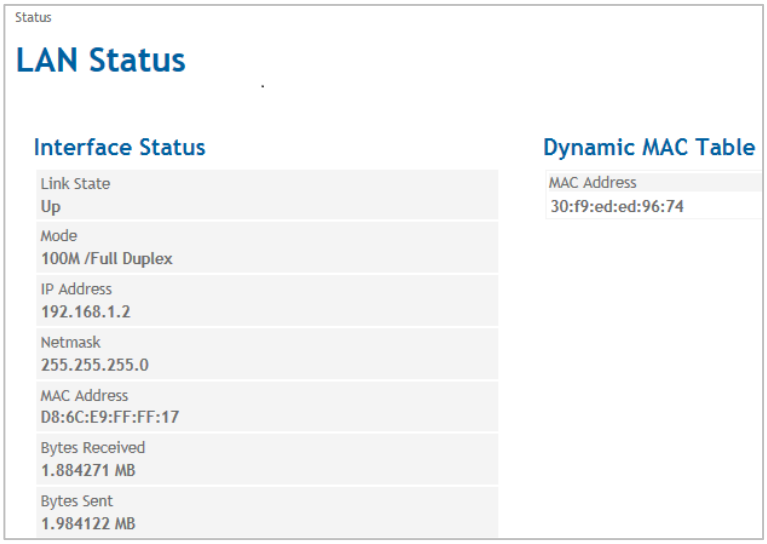
Indicates LAN devices, which have retrieved an IP address from the TAINY iQ DHCP server, if this server is activated (see Chapter 9.5). For each device the assigned IP address, the MAC address, the Hostname and the status is indicated.

LAN Status

3GDSE2
4GDSE2

Click on the **`Status`** tab and select "**`LAN Status`**" to open the screen.





`Interface Status`

Indicates the IP Address, Netmask and MAC Address which are assigned to this interface.

Bytes Received / Bytes Sent: Indicates the number of received or sent bytes since the connection has been established. They will be reset when the connection is re-established.

`Dynamic MAC Table`

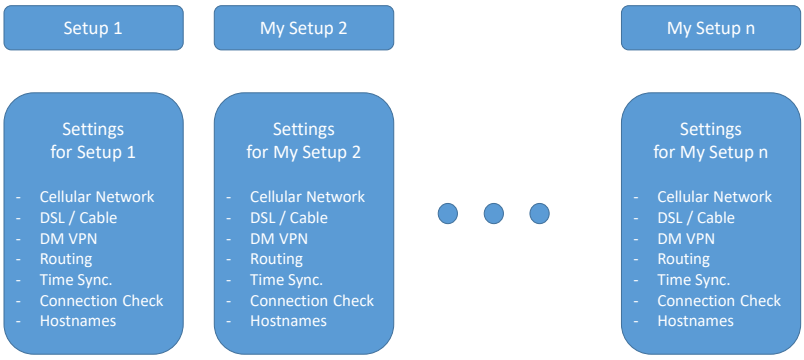
Indicates the MAC address(es) of connected clients or the static MAC table.

7 WAN Settings

7.1 Select the Default WAN Setup

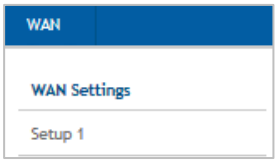
WAN Settings

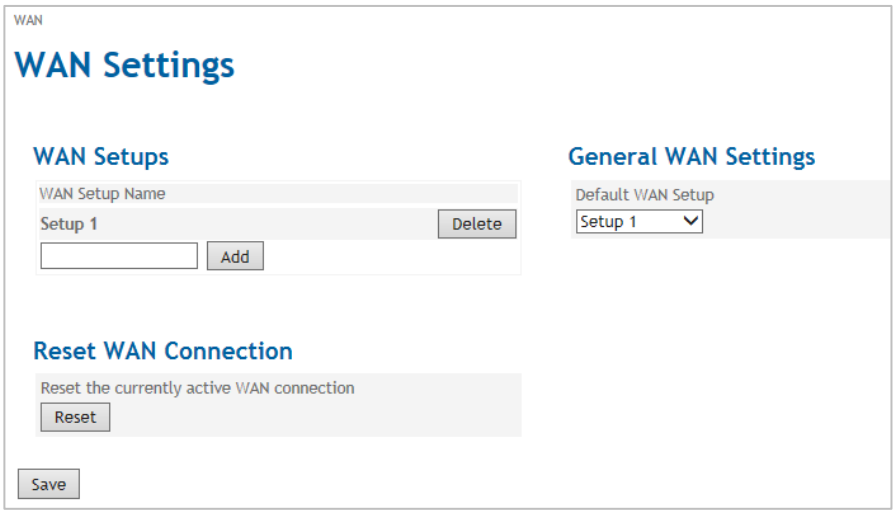
A WAN setup, e.g. Setup 1 comprises a group of WAN interface related settings. See figure below.



You may organize several WAN setups with different settings and select one of it as the default setting.

Click on the **`WAN`** tab and select "**`WAN Settings`**" to open the screen.





`Reset WAN Connection`

This configuration page provides options to create different WAN Setups, select the default WAN Setup and reset a WAN Connection.

`General WAN Settings`

In the "`General WAN Settings`" column you select the "`Current Default WAN Setup`". The selected WAN Setup will be used once you start-up the TAINY iQ.

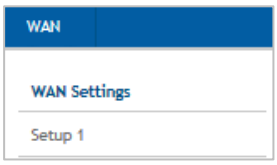
To change the current WAN Setup you select the desired setup from the list of "`Current Default WAN Setups`" and click the "`Save`" button below. The newly selected WAN Setup is immediately active.

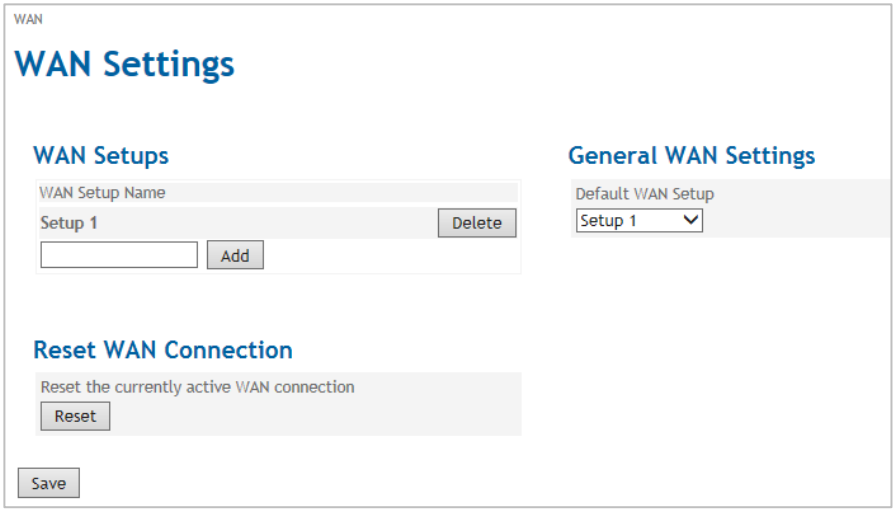
On how to create new WAN Setups see chapter 7.2.

7.2 List, Add, Delete WAN Setups

WAN Setup

Click on the **WAN** tab and select "**WAN Settings**" to open the screen





Setup 1
(or created Setups)

WAN Setups

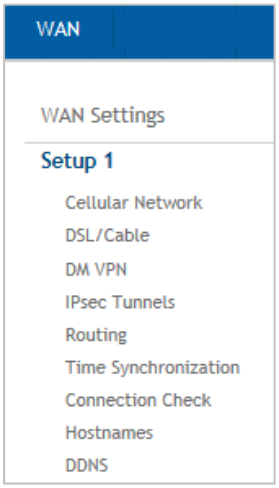
All existing WAN Setups are listed in this column.

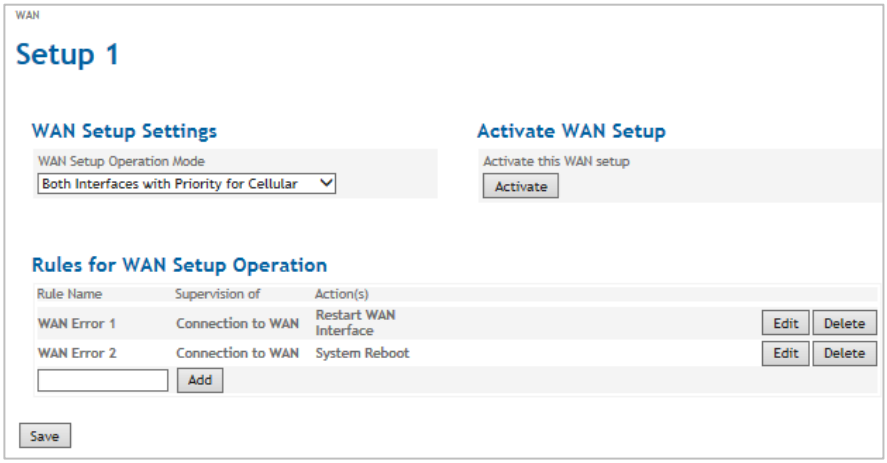
You can add or delete WAN Setups.

To add a new WAN Setup:

Enter a name in the "Setup" entry field and press the "Add" button.

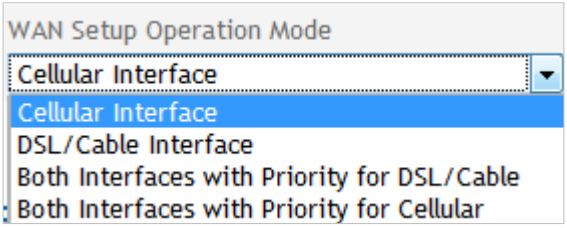
The new WAN Setup will appear in this list and in the menu.





WAN Setup Operation Mode

You can either select one of the interfaces (Cellular or DSL/Cable) to be responsible for establishing the WAN Connection. Or you select both interfaces in parallel. Having selected both however you need to priorities either Cellular or DSL Cable. TAINY iQ will then always try the prioritised interface first to establish the WAN Connection. In case it fails it will use the second one as an alternative.



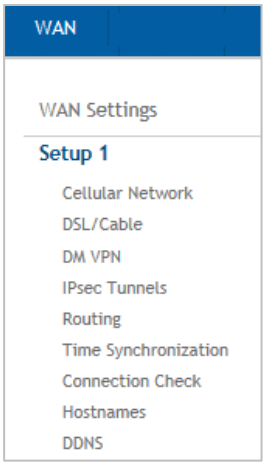
Note

If the ETH0 port shall be used as a LAN port, it is necessary to select "`Both Interfaces with Priority for Cellular`". Otherwise the ETH0 port is powered down.

Additionally to the definition of `Rules for WAN Setup Operation` and the `WAN Setup Operation Mode` you can define for each WAN Setup its own settings for the:

- Cellular Network interface,
- DSL/Cable interface
- DM VPN
- Routing
- Time Synchronization
- Connection Check
- Hostnames

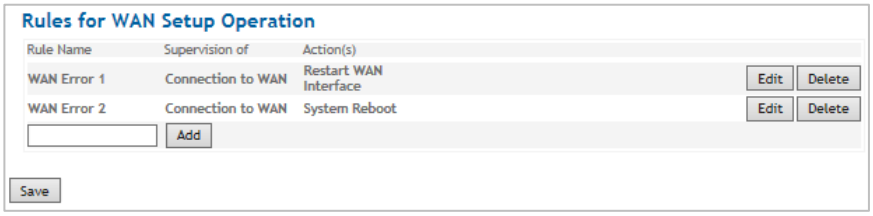
7.3 Configure Rules for WAN Setup Operations



Rules for WAN Setup Operation

You can define TAINY iQ's reaction in case of an incident on the WAN connection, e.g. in case of connection loss or general incident like a transition at the In Port.

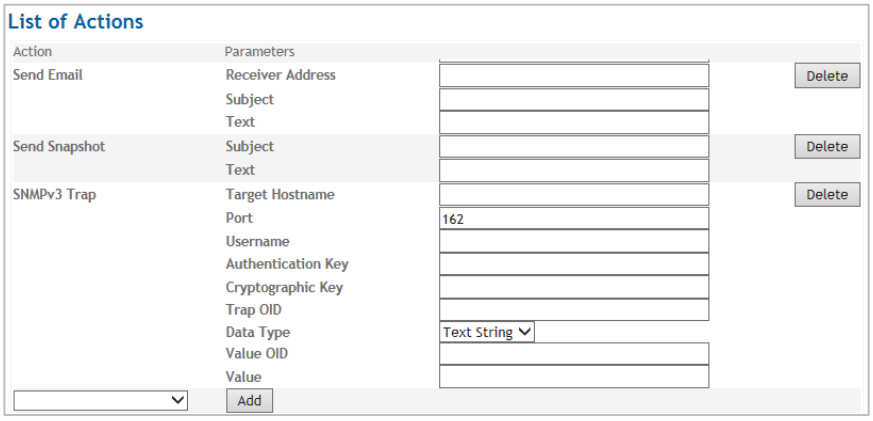
Add, edit or delete Rules for WAN Setup Operations in this section:



To add a new rule enter a name and click the „Add" button. The new rule will appear in this list.

To define or modify the rule click the "Edit" button.

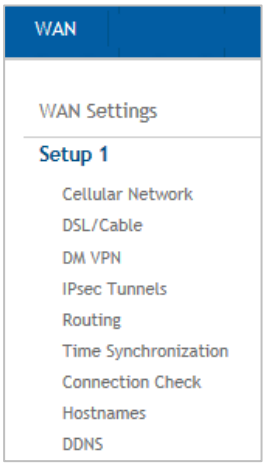
Select the desired action from the List of Actions e.g. Send Email/ SNMP Trap/Send Snapshot.

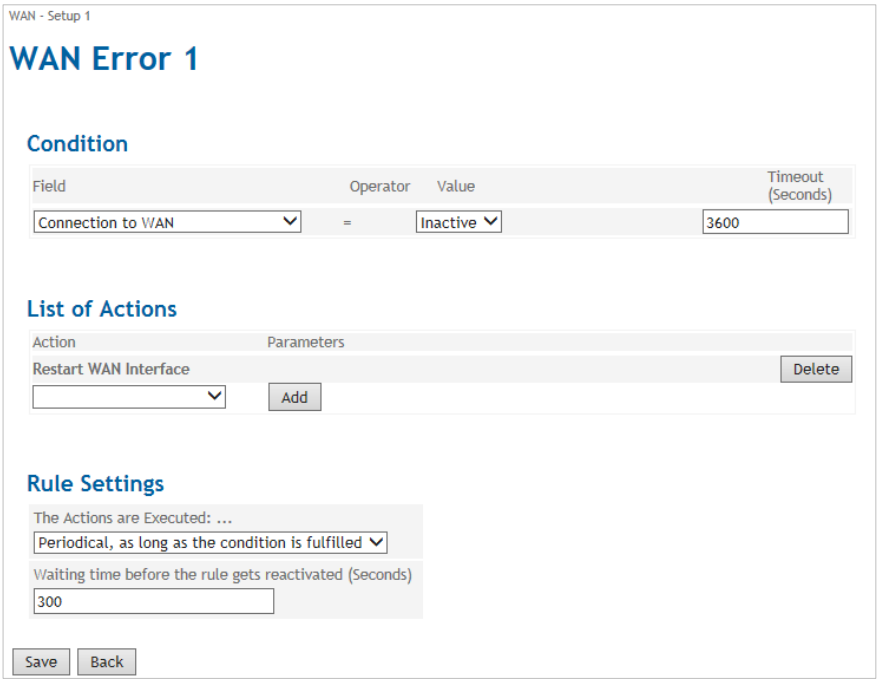


You will find the parameters you need to set explained in the tables „*Selectable Conditions*", "*Selectable Actions*" and "*Selectable Rules*" below.

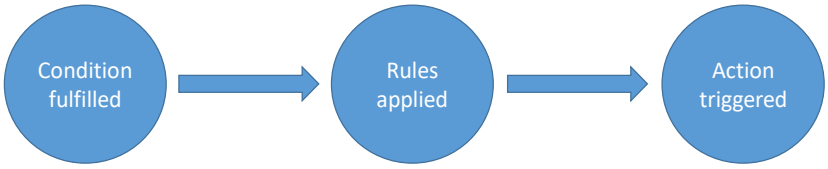
WAN Error 1

(or created Rules)





Next select the **Condition** on which the rule shall be applied, the **Actions** which should be executed, and the **Rule Settings** for the Action.



Example (as shown above):

Condition:	If the *Connection to WAN* is *Inactive* for *3600* seconds.
Action:	*Restart the WAN Interface*
Rule Settings:	*Periodically, as long as the condition is fulfilled* within a waiting time of *300* seconds

If the WAN connection is inactive for 3600 seconds, the TAINY iQ resets the WAN interface. This will be done periodically each 300 seconds, until the WAN connection is no longer inactive.

Selectable Conditions

Condition	Parameter	Action is triggered …
General		
Without Condition	Timeout	… whenever the Timeout expires.
Connection to WAN	Operator/ Value/ Timeout	…in case the connection to WAN is active or inactive for the period (Timeout) defined.
Gate Input	Operator/ Value/ Timeout	…in case the Input Gate is active or inactive for the period (Timeout) defined.
Connection Check		
Check failed	n/a	…in case the Connection Check failed (see …)
Lost Packets (%)	Operator/ Value/ Timeout	…in case the percentage of Lost Data Packets is equal, higher or lower the entered value or within the entered range for the defined period of time (Timeout). Only data exchange of the connection check is qualified.
Mean Response Time (ms)	Operator/ Value/ Timeout	…in case the Mean Response Time (ms) is equal, higher or lower the entered value or within the entered range for the defined period of time (Timeout). Only data exchange of the connection check is qualified.
WAN Data Volume		
SIM 1 Data Volume (kB)	Counter Value Cellular	…in case the value is equal, higher or lower than the entered value or within the entered range for the defined period of time (Timeout).
SIM 2 Data Volume (kB)	Counter Value Cellular	…in case the value is equal, higher or lower than the entered value or within the entered range for the defined period of time (Timeout).
DSL/Cable Data Volume (kB)	Counter Value DSL/Cable	…in case the value is equal, higher or lower than the entered value or within the entered range for the defined period of time (Timeout).
Cellular Connection		
Signal Strength (CSQ)	Operator/ Value/ Timeout	…in case is equal, higher or lower the entered value or within the entered range for the defined period of time (Timeout).
Signal Strength (RSSI (dBm))	Operator/ Value/ Timeout	…in case is equal, higher or lower the entered value or within the entered range for the defined period of time (Timeout).
Signal Strength 3G (RSCP (dBm))	Operator/ Value/ Timeout	…in case is equal, higher or lower the entered value or within the entered range for the defined period of time (Timeout).
Signal Quality (Ec/No (dBm))	Operator/ Value/ Timeout	…in case is equal, higher or lower the entered value or within the entered range for the defined period of time (Timeout).
DM VPN		
No Default Gateway Available	n/a	…in case none of the Default Gateways configured for Dynamic Multipoint VPN is reachable.
Dead Peer Detection (DPD)	n/a	…in case the Dead Peer Detection (DPD) failed.
IPsec Phase 1 Timeout	n/a	Action is triggered, in case of an IPsec Phase 1 Timeout.
Connection to VPN	Operator/ Value/	Action is triggered, in case the connection to VPN is active or inactive for the period

	Timeout	(Timeout) defined.

Time		
System Uptime (Seconds)	n/a	…in case the System Uptime is equal, higher or lower the entered value or within the entered range for the defined period of time (Timeout).
Time of Day	Value	…at the entered moment of time (hh:mm:ss)
Reliable Time Base	Operator/ Value/ Timeout	…in case the Reliable Time Base of the TAINY iQ is active or inactive for the period (Timeout) defined. The Reliable Time Base is active as long as the latest successful NTP Synchronization is not older than 48h
LAN Link State		
Any LAN Interface Up	n/a	...in case a network cable is plugged into Any Interface.
Any LAN Interface Down	n/a	...in case a network cable is removed from Any Interface.
ETH 1…ETH 5 Up	n/a	...in case a network cable is plugged into ETH1..ETH5 interface.
ETH 1…ETH 5 Down	n/a	...in case a network cable is removed from ETH1..ETH5 interface.
Counters Influenced by Rules		
Counter 1 …5	Operator/ Value/ Timeout	...in case the Counter is equal, higher or lower the entered value or within the entered range for the defined period of time (Timeout).

Selectable Actions

Action	Parameter	Description
System Reboot	n/a	The TAINY iQ performs a system reboot
Changeover WAN Setup	WAN Setup Name	The TAINY iQ switches to the WAN Setup determined by the parameter.
Restart WAN Interface	n/a	The WAN interface will be restarted and the connection will be established again according to the default WAN setup.
Restart VPN	n/a	The VPN service will be restarted; the VPN connections are dropped and established again according to the setup.
Log Entry	Log Level Event Text	A Log Entry with configured text and Log Level will be generated.
SNMPv3 Trap	Destination Address/ Destination/ Username/ Password/ Authentication key/ Cryptography key/ Trap-OID/ Datatype/ Value-OID/Value	A SNMPv3 trap is sent in case one of the above described conditions applied. ***Note***: The receiver address is configured on the System tab, submenu Device Information
Send Email	Recieveraddress/ Subject/Text	An Email is sent
Send Snapshot	Subject/Text	A snapshot is sent by email. ***Note***: The receiver address is configured on the System tab, submenu Device Information

Switching Output	Output State	The Switching Output will be set to the state as configured by the parameter.
Increase Counter	Counter	The selected Counter (1..5) will be increased by 1.
Decrease Counter	Counter	The selected Counter (1..5) will be decreased by 1.
Set Counter	Counter Value	The selected Counter (1..5) will set to the value, determined by the value parameter.

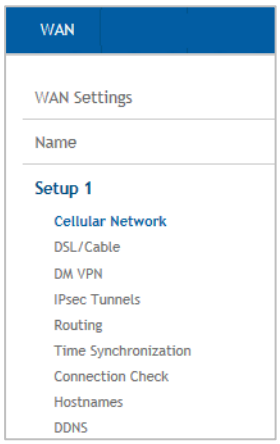
Selectable Rules

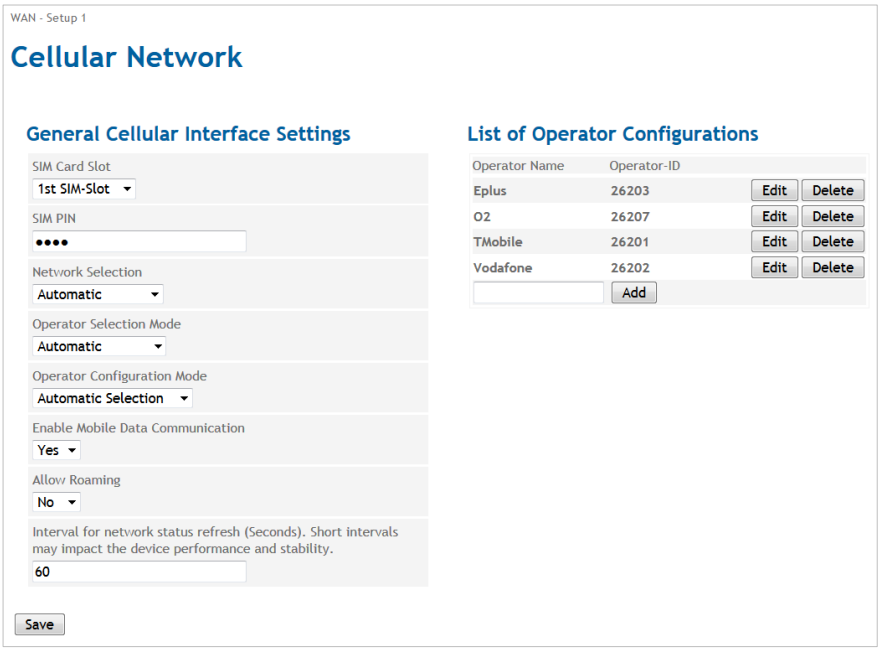
Rule	Parameter	Description
Every time the condition is fulfilled	n/a	The action will be performed when the condition switches from not fulfilled to fulfilled.
The first time the condition is fulfilled	n/a	The action will be performed the first time after start-up or after saving the rule.
Periodically, as long as the condition is fulfilled	Waiting time	The action is performed periodically as long as the conditions are fulfilled. The next execution of the action is locked until the Waiting time is expired.

7.4 Configure the WAN Cellular Network Interface

Cellular Network

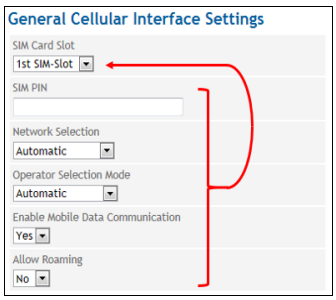
Click on the **WAN** tab and select "**Cellular Network**" to open the screen





General Cellular Interface Settings

Select the SIM Card Slot and configure the parameter being applied to the selected SIM.

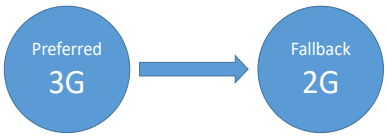


SIM PIN: Enter the PIN of the SIM in the selected SIM-Slot.

Network Selection: Select if the TAINY iQ shall automatically register to the most advanced network type being supported and available:

Type 4GDSEx

Type 3GDSEx



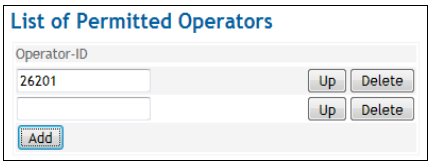
Or it should register to 4G, 3G or to 2G networks only.

Operator Selection Mode: Select the list of allowed network operators, that shall be applied searching for a network:

Automatic: TAINY iQ searches automatically for the best network option and tries to register to it.

SIM Card List: TAINY iQ attaches only networks of operators stored at the SIM card.

User Defined List: TAINY iQ attaches only networks of operators entered in the List of Permitted Operators. You may enter here the preferred operators. The first entry in the list is tried first. You can move the ranking by pressing the „Up" button.



Operator Configuration Mode: Select if the access parameter shall be selected automatically according to an Operator-ID stored at the used SIM card (see Automatic Operator Configuration) or manually (see Manual Operator Configuration) according to fixed settings.

Enable Mobile Data Communication: Enable / Disable the communication with this SIM via the cellular interface. The device registers into network but does not attach to the data service.

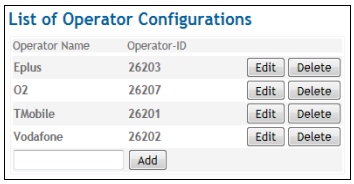
Allow Roaming: Enable / Disable roaming.

Intervall for network status refresh: Intervall for refreshing of the quality data of the radio connection (value range: 5 – 300 seconds)

List of Operator Configurations

The list is only visible, if the `Operator Configuration Mode` is set to Automatic Selection

The list shows which access configurations for which network operators are stored on TAINY iQ.



To add a new operator configuration, enter the name of the desired operator into the entry field and click the "`Add`" button.

To view or modify an existing configuration click the "`Edit`" button.

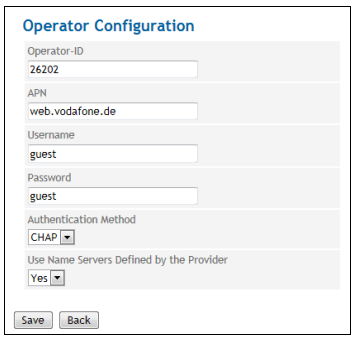
To delete an existing configuration click the "`Delete`" button in the corresponding line of "`Operator Name`".

Operator Configuration (for Automatic Selection)

Only applicable, if the Operator Configuration Mode is set to Automatic Selection

The TAINY iQ reads from the active SIM card the Operator-ID and selects the corresponding Operator Configuration that has been predefined for the Operator-ID.

The Operator Configuration is required to access the IP data service (GPRS, EDGE or HSPA+).



Operator-ID: This ID is used to assign the right Operator Configuration to the used SIM Card. The TAINY iQ reads the Operator-ID from the SIM Card (part of the IMSI) and searches the List of Operator Configuration for a matching entry.

When the Operator IDs of SIM and Operator List match, the corresponding Operator Configuration is used to attach to the IP data service.

Note

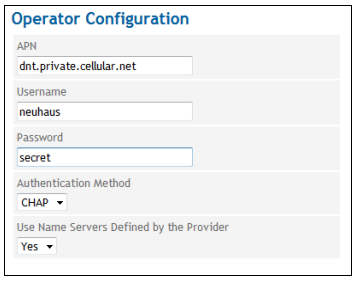
You find the Operator-ID at our website www.neuhaus.de, in the information documents of your UMTS or GSM/GPRS provider or on the provider's homepage. You can also ask the provider's hotline (Kwan Interface keyword: MCC/MNC).

Operator Configuration (for Manual Configuration)

Only applicable, if the Operator Configuration Mode is set to Manual Configuration.

The Operator Configuration is required to access the IP data service (GPRS, EDGE or HSPA+).

Independent of the Operator-ID at the SIM card, the entered Operator Configuration is applied.



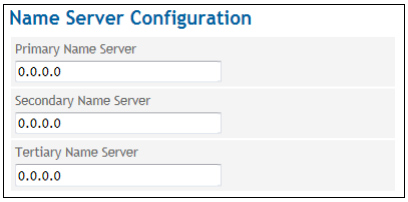
Parameter for Operator Configuration

Enter the **APN**, the **Username** and the **Password**. You can find the APN, Username and Password in your mobile radio network operator's documentation, on your operator's Website, or ask your operator's hotline.

Some mobile radio network operators do not use access control with user names and/or passwords. In this case enter *guest* in the corresponding entry field.

To register with the wireless data service (HSPA+, UMTS, EGPRS or GPRS), two different **Authentication Methods** (PAP and CHAP) are used. Generally the method is selected automatically. If however a particular method shall be used, the selection may be done manually. Select either PAP or CHAP.

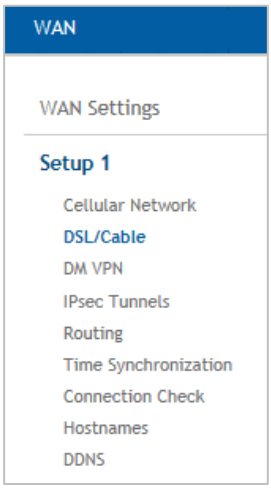
Use Name Servers Defined by the Provider: Select Yes, if Name Servers offered by the Operator shall be used. Select No to determine up to 3 Name Servers manually.

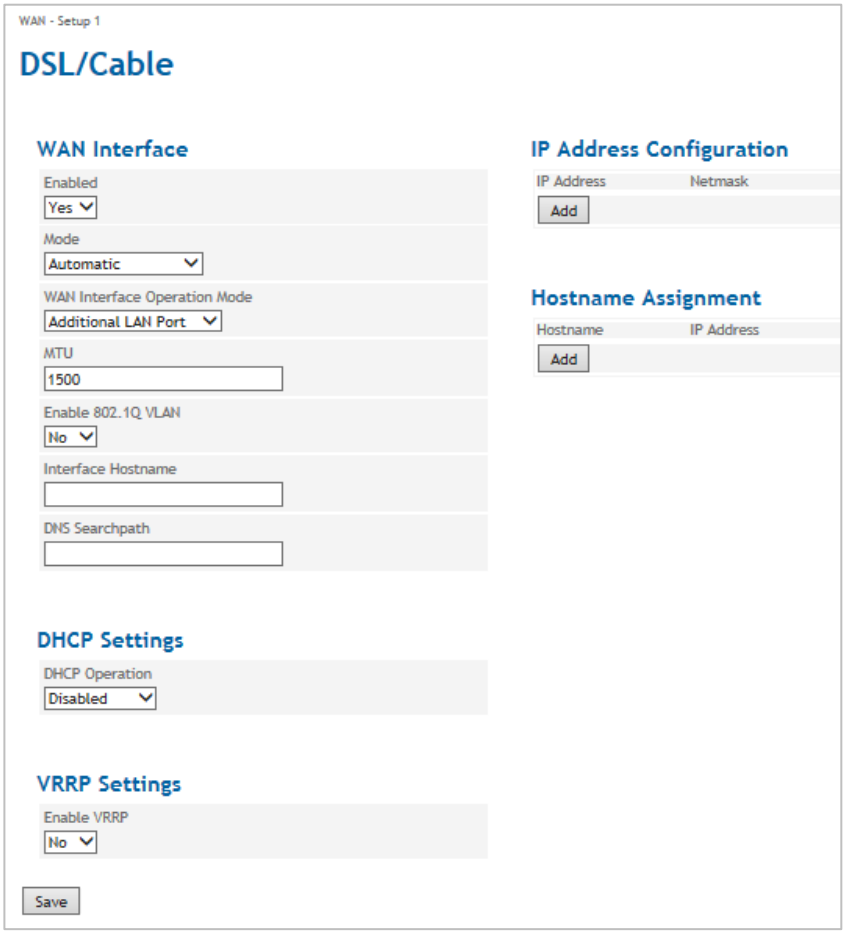


7.5 Configure the WAN DSL/Cable Interface

DSL/Cable

4GDSE6
3GDSE6





`WAN Interface`

To establish WAN communication via a Ethernet communication the following parameters set the following parameters:

Select the correct "**`WAN Interface Operation Mode`**" from the list:

- Select PPPoE. to connect the TAINY iQ to DSL modems providing a PPPoE logical interface,
- Select DHCP to connect the TAINY iQ to routers.
- Select PPPoE > DHCP or DHCP > PPPoE if the TAINY iQ shall automatically select the right logical interface. With PPPoE > DHCP will first try to connect with PPPoE, if this fails it will try DHCP. With DHCP > PPPoE it will work vice versa.
- In case of a PPPoE connection, enter the Username and the Password.

It is possible to change the **`Mode`** of the interface. Select the required mode from the dropdown list:

- `Automatic`
- `100M Full Duplex` or `100M Half Duplex`
- `10M Full Duplex` or `10M Half Duplex`

To shut down the entire interface set the **`Enabled`** to "`No`".

MTU

Enter the MTU (Maximum Transmission Unit) to determine the maximum size of IP packets.

Enable VLAN Tags (802.1Q)

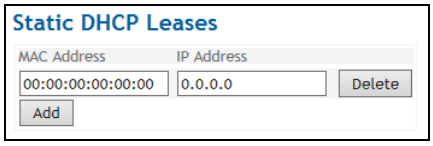
Select “Yes”, if the VLAN Tags shall be forwarded via this Physical Interface towards the connected application. Otherwise the VLAN Tags will be removed for outbound communication.

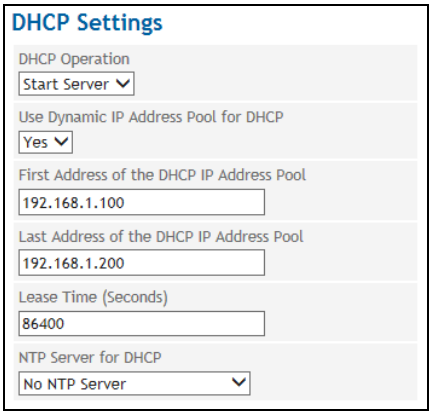
DHCP Settings

DHCP Operation

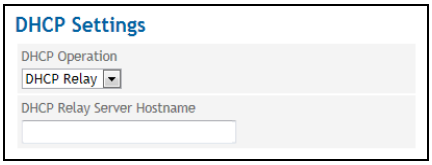
The TAINY iQ provides a DHCP server function or a DHCP relay function.

If the DHCP server function is activated, the TAINY iQ itself assigns IP addresses to applications connected to the LAN interface. Define the range of address the assigned IP addresses shall be taken from and/or static IP leases.





If the DHCP relay function is activated, the TAINY iQ routes the DHCP requests of applications connected to the LAN interface to a remote DHCP relay server which provides the IP addresses. Enter the hostname or the IP address of the DHCP Relay Server.



VRRP Settings

VRRP (Virtual Router Redundancy Protocol) secures the availability of important gateways within the network by utilising a number of TAINY iQs.

To configure the VRRP setting set **Enable VRRP** to “Yes”.

`Virtual Router ID`

ID for the group of utilised TAINY iQs.

`VRRP Priority`

Defines, which TAINY acts as master and which as the backup. The TAINY iQ which has the highest priority acts as the master. Enter values between 1 (lowest prio) and 254 (highest prio). The VRRP priority can be adjusted automatically to a new value

`Adjusted VRRP Priority`

In case of an active WAN or VPN connection

`VRRP IP Address List`

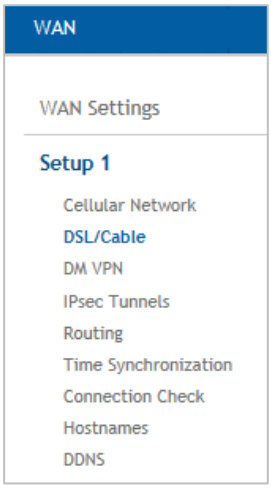
IP addresses of the VRRP (TAINY iQs)

`IP Address Configuration/ Hostname Assignment`

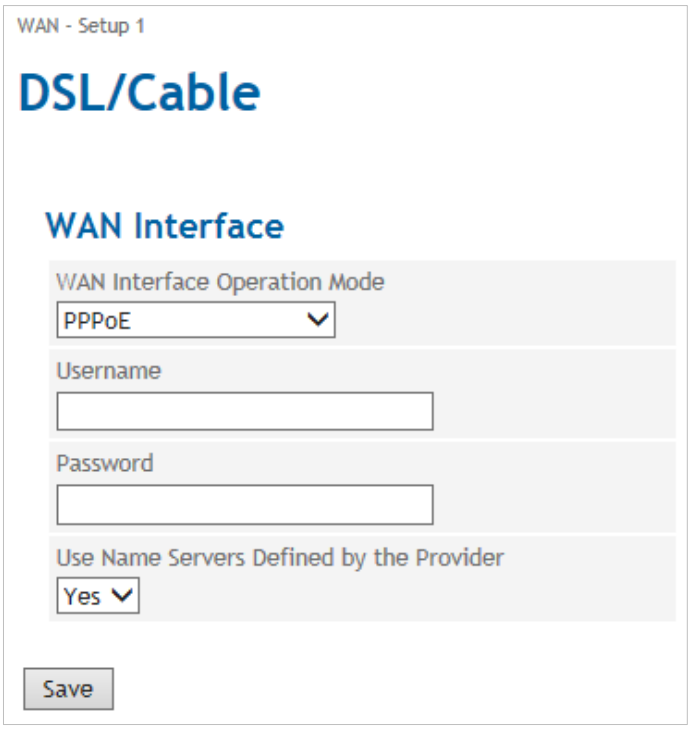
`Hostname, IP Address:` The TAINY iQ allows assigning IP addresses of remote stations to hostnames. Using this function, applications connected to TAINY iQ's LAN interfaces address these remote stations by the entered hostnames. TAINY iQ functions (e.g. NTP) also use this feature.

DSL/Cable

3GDSE2-dc
4GDSE2-dc



Click on the **`WAN`** tab and select "**`DSL/Cable`**" to open the screen



`WAN Interface`

To establish the WAN communication via a wired Ethernet connection, the following parameters need to be set.

Select the correct "`WAN Interface Operation Mode`" from the list:

- To connect the TAINY iQ to DSL modems providing a PPPoE logical interface, select PPPoE.
- To connect the TAINY iQ to routers, select DHCP.

If the TAINY iQ shall automatically select the right logical interface, select PPPoE > DHCP or DHCP > PPPoE. With PPPoE > DHCP will first try to

connect with PPPoE, if this fails it will try DHCP. With DHCP > PPPoE it will work vice versa.

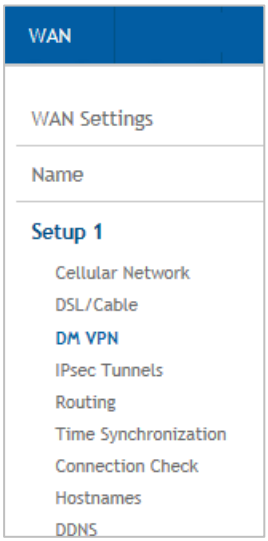
In case of a PPPoE connection, enter the `Username` and the `Password`.

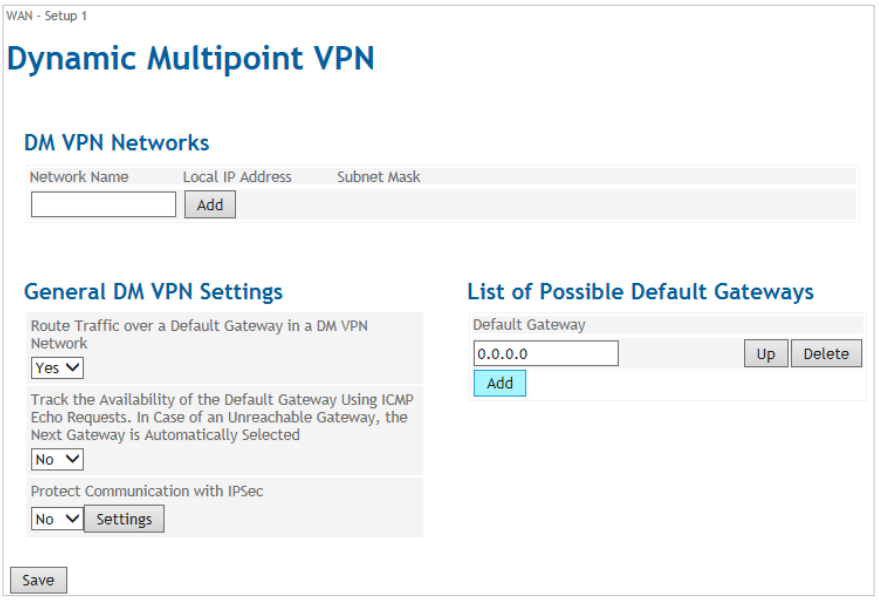
Click on “`Save`”.

7.6 Configure Dynamic Multipoint VPN

DM VPN

Click on the **`WAN`** tab and select “**`Dynamic Multipoint VPN`**” to open the screen





`DM VPN Networks`

Network definitions of the existing networks (see next page)

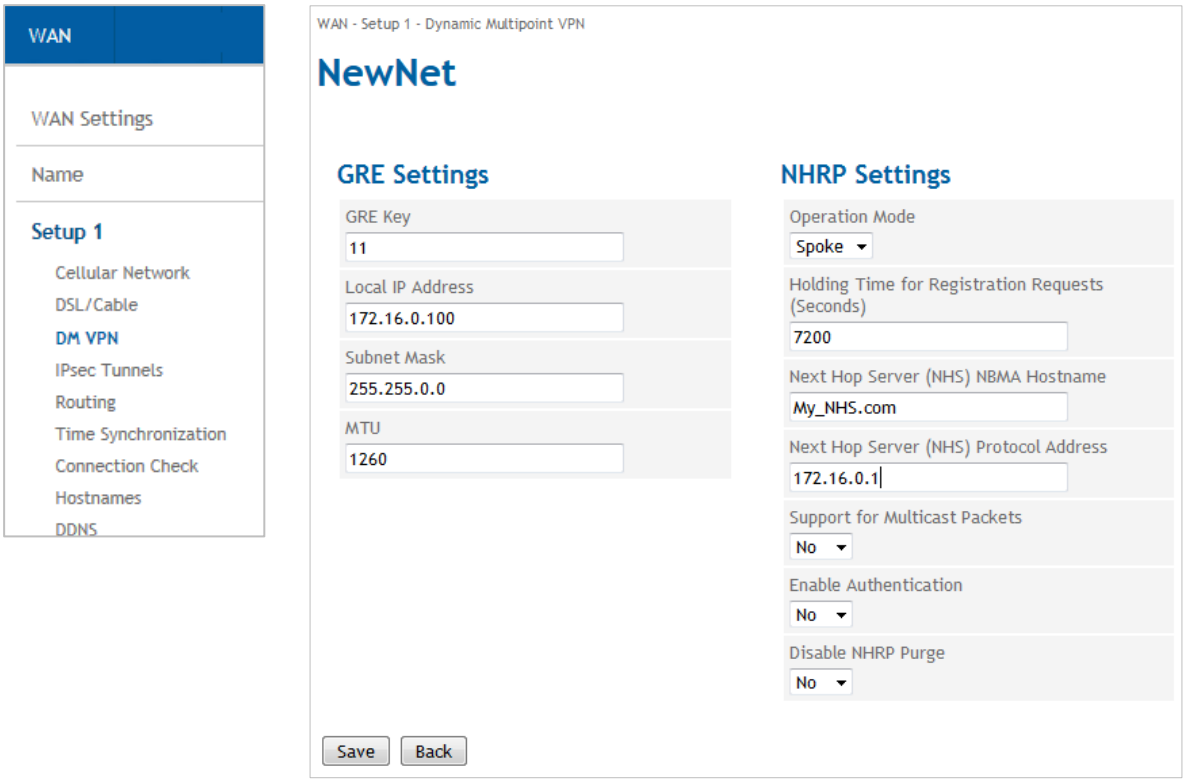
`General DM VPN Settings / List of Possible Default Gateways`

Select “`Yes`” to “`Route all WAN traffic over a Default Gateway`” in a DM VPN Network. The Default Gateway needs to be part of the “`List of Possible Default Gateways`”.

Select “`Yes`” if the TAINY iQ shall monitor the availability of the Default Gateway by ICMP pings and switch to the next gateway in case the used one is not reachable.

`DM VPN Networks`

Click the “`Add`” button to define a new `DM VPN Network`. Define the network characteristics for the new network.



GRE Settings

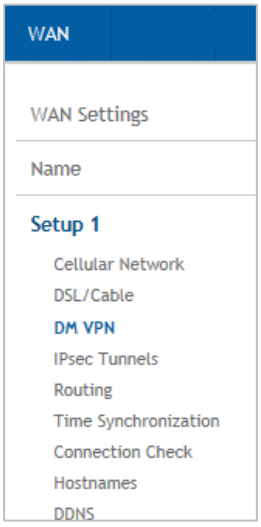
Local IP Address	Enter the IP address of the TAINY iQ within the DM VPN. The IP address is provided by the operator of the DM VPN.
Subnet Mask	Enter the Subnet Mark of the DM VPN. The Subnet Mask is provided by the operator of the DM VPN.
MTU	Enter the MTU (Maximum Transmission Unit) to determine the maximum size of IP packets used in the DM VPN. This may differ from the MTU size defined in chapter 9.1. Please observe that the GRE protocol increases the size of data packets.

NHRP Settings

Operating Mode	Select whether the TAINY iQ shall act as a NHRP spoke or hub. Please observe that there may only be one hub in the DM VPN.
Holding Time	Only applicable if Spoke mode is selected: The holding time for registration requests defines the period of time the Next Hop Server will keep the address information.
Next Hop Server NBMA address	Only applicable if Spoke mode is selected: Enter the WAN IP address of the Next Hop Server NBMA (the next hub).
Next Hop	Only applicable if Spoke mode is selected:

Server Protocol address	Enter the DM VPN IP address of the Next Hop Server NBMA (the next hub).
Support for Multicast Packets	Enables / Disables distribution of Multicast Packets in the DM VPN.
Enable Authentication	Select “Yes” if the TAINY iQ shall authenticate itself at the remote NHRP station. In this case enter an authentication key.
Disable NHRP Purge	If “No” is selected the TAINY iQ in Spoke mode sends after a (re-) registration a request to the hub to clean-up formerly stored routing data of the TAINY (standard implementation). If “Yes” is selected the request is not sent.

7.7 Configure IPsec for Dynamic Multipoint VPN

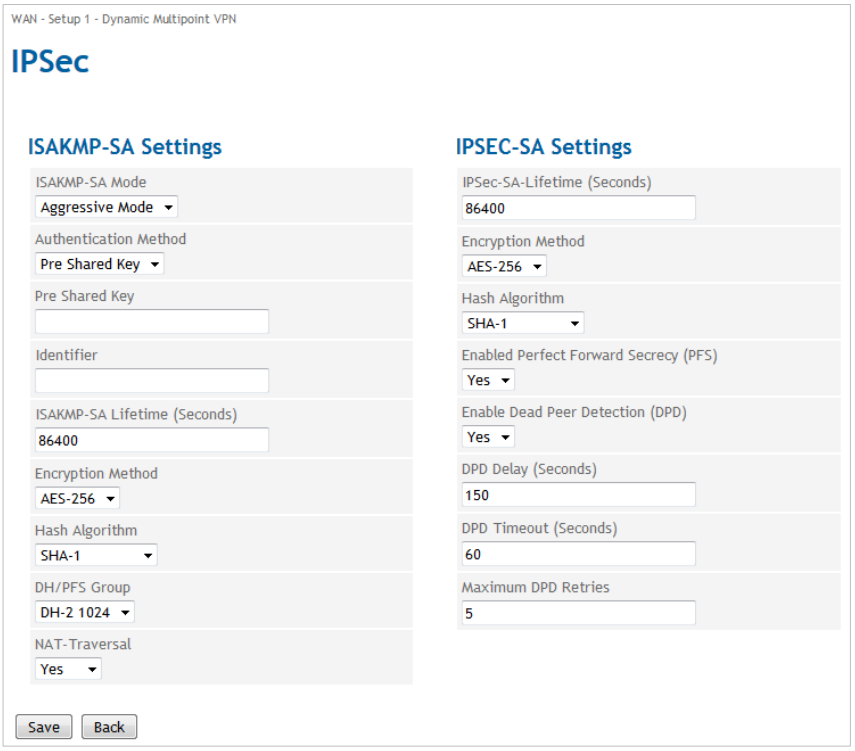


Click on the **WAN** tab and select "**DM VPN**" to open the screen.

IPsec

The DM VPN has no encryption and authentication mechanism by its own. However, it is possible to add these features using IPsec technology.

Select "Yes" if the communication shall be protected by IPsec and click the "Settings" button to define the IPsec.



If the IPsec function is activated, each dynamically established GRE tunnel will be protected by a corresponding IPsec tunnel, which is also dynamically established.

ISAKMP-SA Settings

The ISAKMP-SA settings define the procedures and packet formats to establish, negotiate, modify and delete the Security Associations (SA) for the IPsec tunnel(s).

IPsec-SA Settings

The IPsec-SA settings define the timeouts, encryption methods, packet formats etc. of the Security Association (SA) of the IPsec tunnel(s).

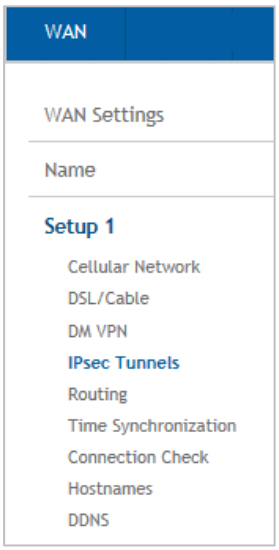
It also enables/disables the dead peer detection (DPD) and its behaviour.

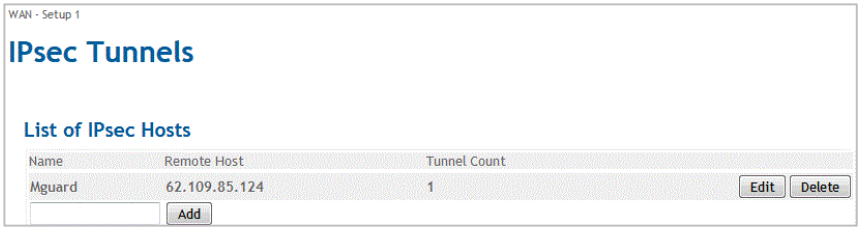
The settings that shall be applied for ISAKMP-SA and IPsec-SA settings have to be agreed with the administrator of the remote station as well as the DM VPN. The settings shall be the same for all possible communication partners of the TAINY iQ in this DM VPN.

7.8 Configure IPsec Tunnels

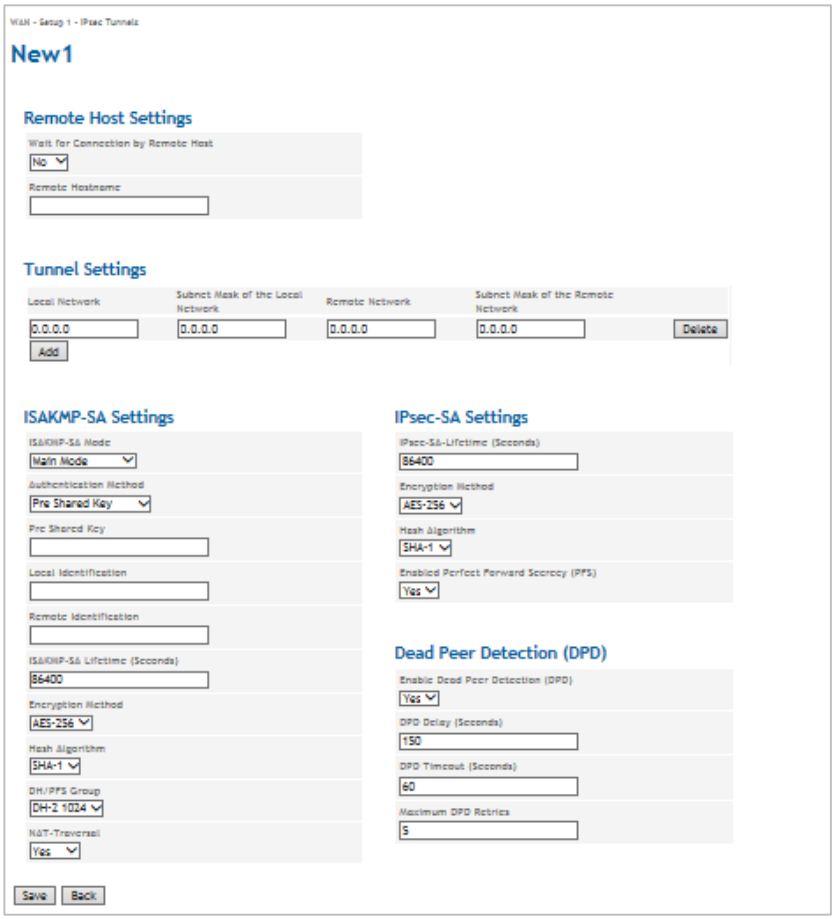
IPsec Tunnels

Click on the **WAN** tab and select "**IPsec Tunnels**" to open the screen.



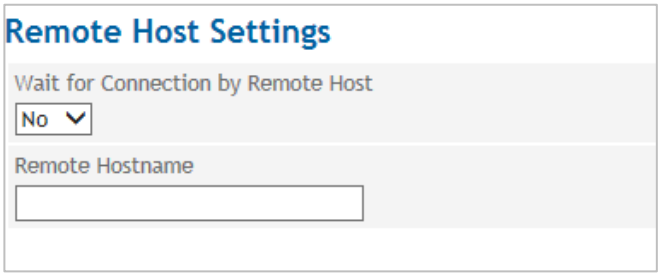


All configured `IPsec Hosts` are listed in this view. You can see the `Name`, `Remote Host` and `Tunnel Count`. To edit an IPsec Tunnel click the "Edit" button. To configure a new IPsec Host enter the name in the "`Name`" entry field and click "`Add`". The following screen opens.



Set the follwoing parameters to edit an exsisting or configure a new IPsec Tunnel:

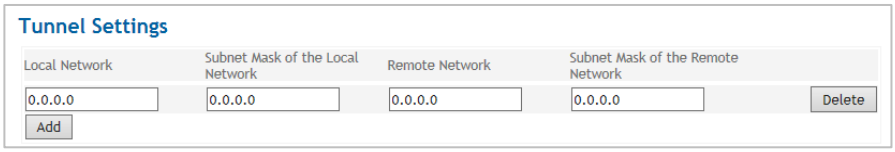
Remote Host Settings



If you set the parameter **Wait for Connections by Remote Host** to "Yes" make sure the remote station is available continuously and must answer pings.

Enter the name of the host station in the **Remote Hostname** entry field.

Tunnel Settings



View, add or delete tunnels settings.

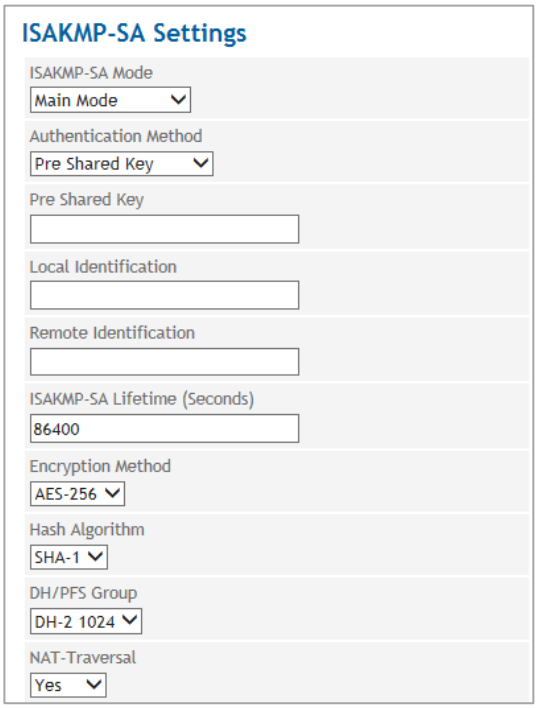
To add new tunnel settings the following parameters are required:

IPs of the **Local Network** and Subnet **Mask of the Local Network** that TAINY uses to establish a connection to the remote network

The actual IPs of the **Remote Network** and **Subnet Mask of the Remote Network**.

You could leave these fields empty.

ISAKMP-SA Settings



ISAKMP SA Mode

ISAKMP (Internet Security Association and Key Management) establishes the SA (Security Association) for the key exchange between TAINY iQ and the VPN gateway of the opposite network.

Select either Main Mode or Aggressive Mode.

Main Mode protects the identified peers in any case whereas the Aggressive Mode will not protect the identified peers.

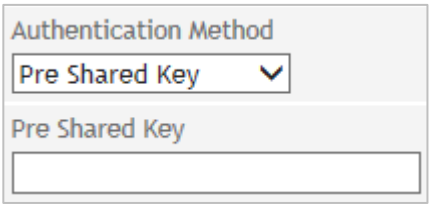
Authentication Method

To be able to select the desired settings in this section you have to make sure, that the required certificates are already available on TAINY iQ, see chapter 12 for further information.

Select the preferred **Authentication Method** from the three options:

Pre Shared Key

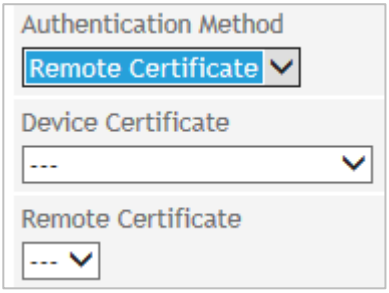
If pre shared keys is selected enter a password for of the keys into the Pre Shared Key entry field.



Remote Certificate

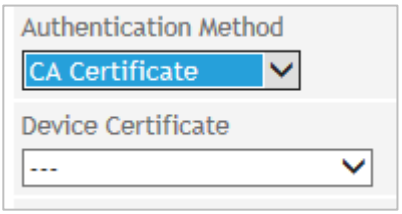
If the authentication method is set to Remote Certificate select the desired certificate from the dropdown list **Device Certificate.**

Select the corresponding **Remote Certificate.**



CA Certificate

If the authentication method is set to CA Certificate select the desired certificate from the dropdown list **Device Certificate.**



Local/Remote Identification

Enter the IDs of the local and remote ISAKMP SAs.

ISAKMP-SA Lifetime (seconds)

Enter the validity of the Internet Security Association and Key Management in seconds. Could be between 1 second up to 24 hours.

Encryption Method

Select the required encryption method (algorithm)

AES or 3DES.

Hash Algorithm

Select the used Hash Algorithm.

DH/PFS Group

Select the DH (Dynamic Host)/PFS (Perfect Forward Secrecy) - group that has been agreed on with the administrator of the opposite network for the exchange of keys.

NAT-Traversal

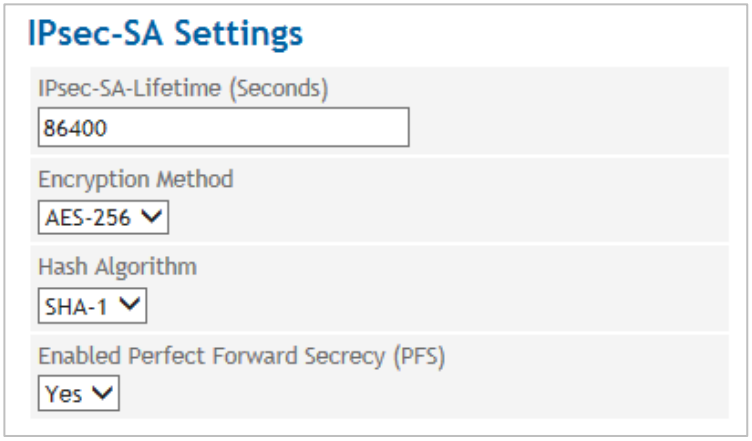
Select:

"Yes" – The use of NAT-Traversal could be arranged when the connecting is established

"No" - The use of NAT-Traversal could not be arranged when the connection is established.

"Force" – NAT-Traversal is used in any case

IPsec-SA Settings



IPsec (Internet Protocol Security) establishes the actual SA (Security Association) for the connection between the TAINY and the opposite network.

IPsec-SA Lifetime (seconds)

Enter the validity of the Internet Protocol Security in seconds. Could be between 1 second up to 24 hours.

Encryption Method

Select the required encryption method (algorithm)

"AES" or "3DES".

Hash Algorithm

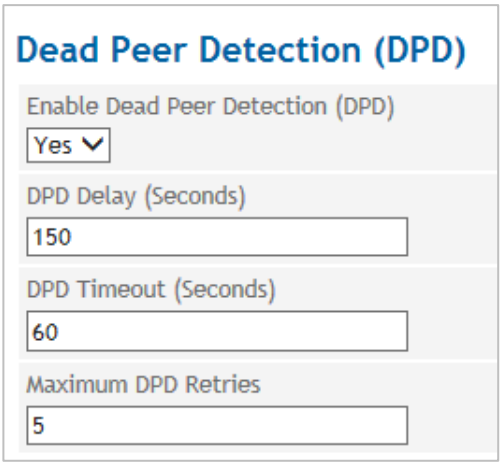
Select the used Hash Algorithm.

Enable Perfect Forward Secrecy (PFS)

If set to "Yes" a new session key will be generated (DH-Key-Exchange), once the ISAKMP-SA is arrange for IPsec-SA.

If set to "No" the ISAKMP-SA is used again.

Dead Peer Detection (DPD)



The Dead Peer Detection identifies whether the IPsec connection between two networks is still valid or if the connection has to be re-established. This function presumes though that it is supported on both sides.

Caution

Risk of additional costs

Due to sending DPD request as well as the use of NAT-T the number of send and receive data will increase. Depending on the selected settings the additional data volume might be 5 MB or more per month. This could lead to additional costs.

Enable Dead Peer Detection

Select “Yes” to use the function. TAINY iQ will now identify the validity of the connection irrespectively data transmission.

Select “No” to switch the function off.

DPD Delay

Lapse of time in seconds the DPD-requests are send.

DPD Timeout

Lapse of time (in seconds) after which the DPD-request is considered failed if no answer is received. This is also the interval after which the next request is send until the connection is finally interrupted.

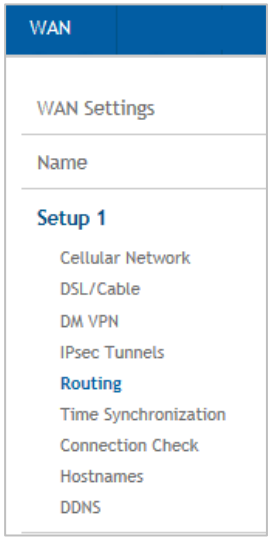
Maximum DPD Retries

Number of permitted retries until the IPsec connection is considered interrupted.

7.9 Configure User defined WAN Routes and RIPv2

Routing

Click on the **WAN** tab and select "**Routing**" to open the screen.



User Defined WAN Routes

Select the logical interface which shall be used to route data traffic from/to a remote station via the WAN:

- Route over Cable/DSL Connection
- Route over Cellular Connection
- Route over IP Gateway

Enter the IP address of the remote station as well as a corresponding netmask.

RIPv2 Settings

The RIPv2 protocol is used to transmit the configured LAN routing tables repeatedly in fixed intervals to a remote station.

If two routers (e.g. TAINY iQ) provide the same route, you can prioritize one of the routers by entering a lower value for the **Networks Costs**. This router will be prioritised.

Select Yes if **only RIP neighbours behind the active default gateway** shall be used. The TAINY iQ will transmit the routing tables only via the default gateway.

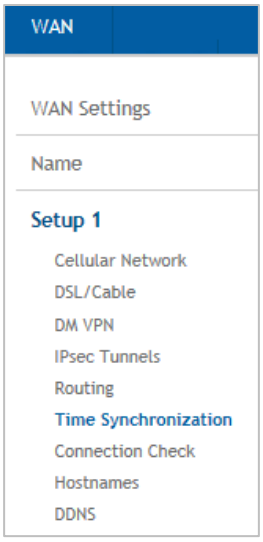
RIPv2 Neighbour IP Addresses

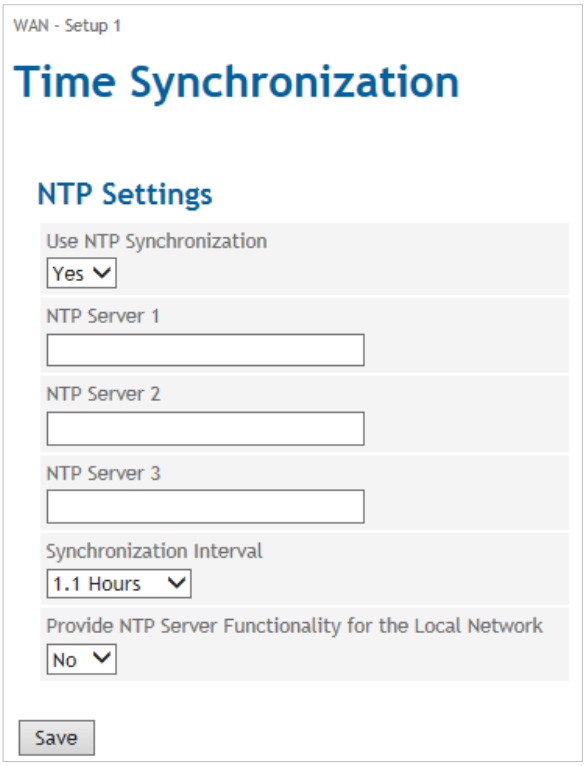
Enter the IP address of the remote station the routing tables shall be sent to.

7.10 Configure the NTP Time Synchronization

Time Synchronization

Click on the **WAN** tab and select "**Time Synchronization**" to open the screen.





NTP Settings

The TAINY iQ can obtain the system time from a time server via NTP (= *Network Time Protocol*). There are a number of time servers on the Internet that can be used to obtain the current time very precisely via NTP.

NTP Server 1..3

You can enter up to 3 time server. Enter either their URL or there IP address.

Synchronization Interval

You can select the interval in which the NTP Servers are requested for the actual time stamp.

Provide NTP Server Functionality for the Local Network

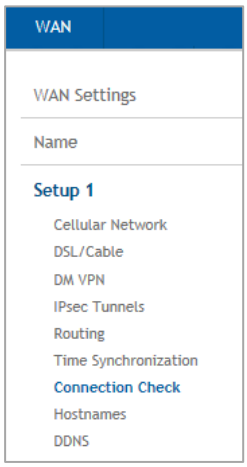
The TAINY iQ can serve itself as an NTP time server for the applications that are connected to its local network interface. To activate this function select *Yes*.

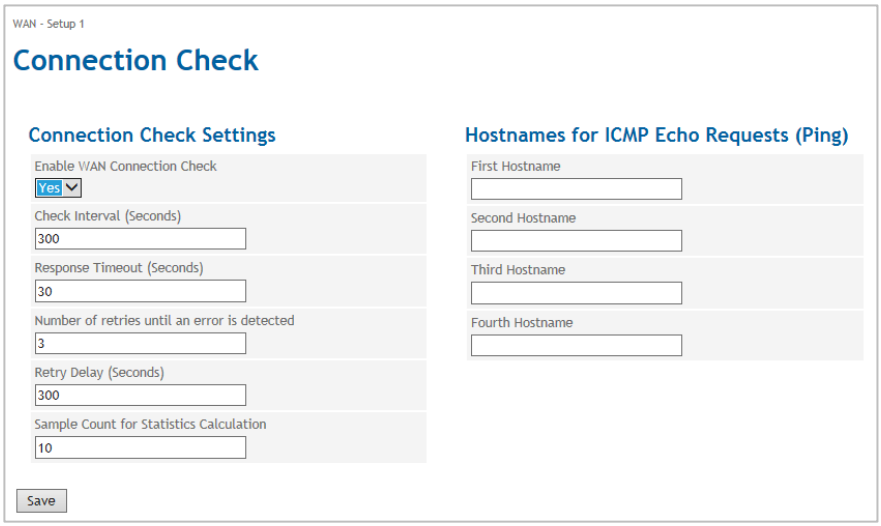
The NTP time server in the TAINY iQ can be reached via the local IP address set for the TAINY iQ.

7.11 Configure the Connection Check

Connection Check

Click on the **WAN** tab and select "**Connection Check**" to open the screen.





With the function *Connection Check* the TAINY iQ checks its connection to UMTS/GPRS and to the connected external networks, such as the internet or an intranet. To do this, the TAINY iQ sends ping packets (ICMP) to up to four remote stations at regular intervals.

Connection Check Settings

Enable the WAN Connection Check

Select Yes to activate the Connection Check

Check Interval (Seconds)

Defines the Interval in which the Connection Check shall be performed.

Response Timeout (Seconds)

Defines the Reponse Timeout. If the TAINY iQ receives within this period of time the ICMP ping answers from the remote stations, the check was successful.

Number of retries until an error is detected

Defines the number of retries until an error is detected. In case the TAINY iQ does not receive ICMP ping answers within the Response Timeout, the check will be repeated the entered number of retries. If all retries fails, the connection check is failed.

Retry Delay

Defines the delay between retries.

Sample Count for Statistics Calculation

Defines the number of samples used to calculate a mean value.

Hostnames for ICMP Echo Requests (Ping)

First … Fourth Hostname

Enter up to four remote stations that the TAINY iQ can ping. The remote stations must be available continuously and must answer pings.

Note

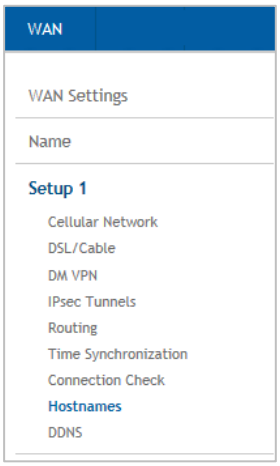
Make sure that the selected remote stations will not feel "harassed".

Note

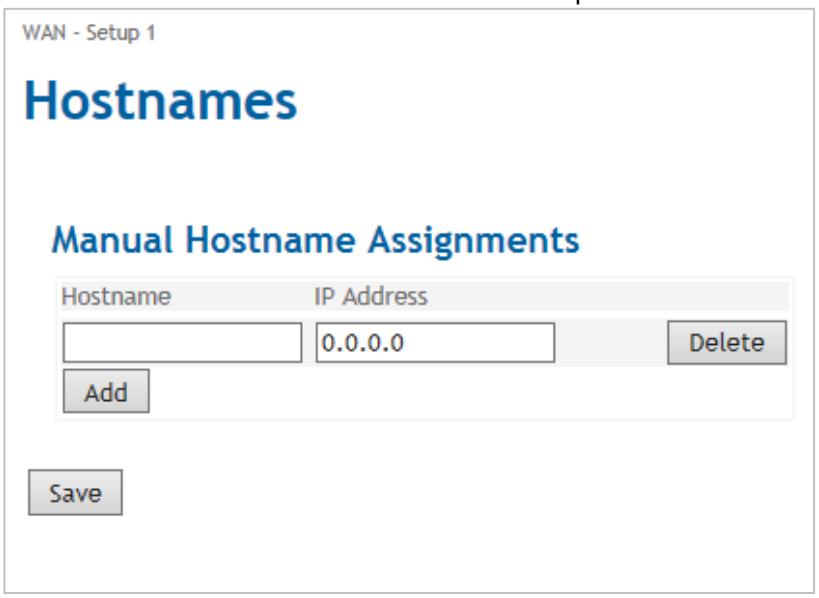
If the connection check is used for checking a VPN-tunnel, only the VPN-host should be entered as ICMP target.
By entering further hosts, which will answer to the ICMP requests, a termination of the VPN-tunnel will not be detected.

7.12 Assign Hostnames to remote IP Addresses

Hostnames



Click on the **WAN** tab and select "**Hostnames**" to open the screen.



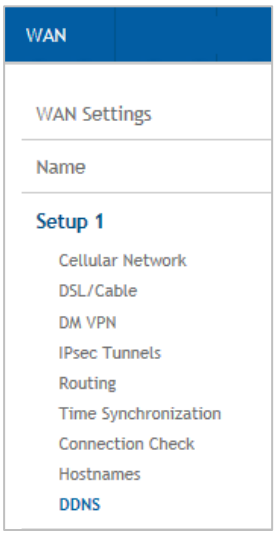
This function allows assigning IP- addresses of remote stations to hostnames. Using this function, applications connected to TAINY iQ's LAN interfaces can address these remote stations by the entered hostnames. TAINY iQ functions (e.g. NTP) can also use this feature.

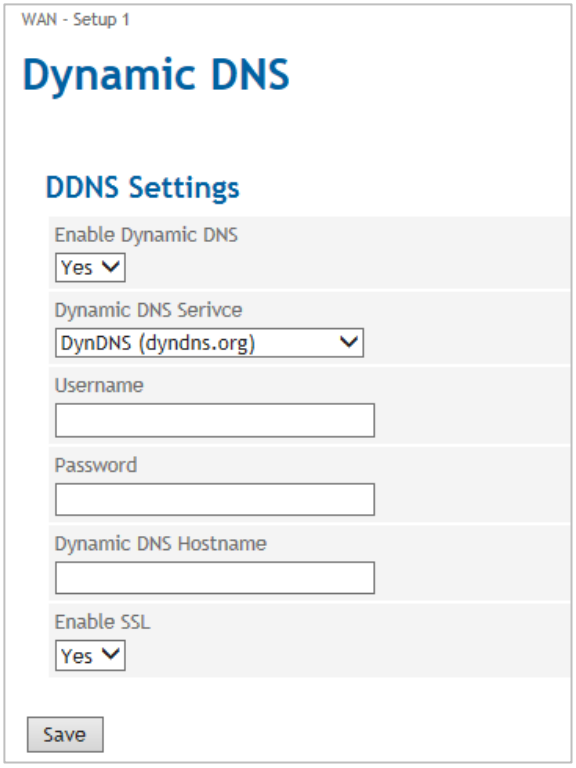
Hostnames configured here are valid only for the selected WAN setup. Hostnames that are independent of the WAN setup can be entered in the LAN section, see 9.1.

7.13 DynDNS Service (DDNS)

DDNS

Click on the **WAN** tab and select "**Hostnames**" to open the screen.

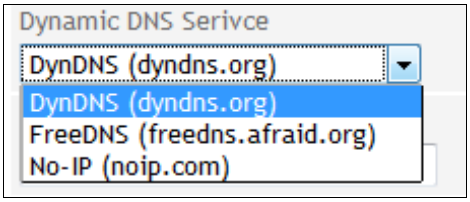




The TAINY iQ can use DynDNS services to be addressable via a DynDNS hostname. You can **enable/disable** this function.

Dynamic DNS Service

Chose one of the three supported function:



Username, Password

Enter the username and password to access the selected DynDNS service.

Dynamic DNS Hostname

Enter the hostname on which the TAINY iQ can be addressed (provided by the DynDNS service).

Enable SSL

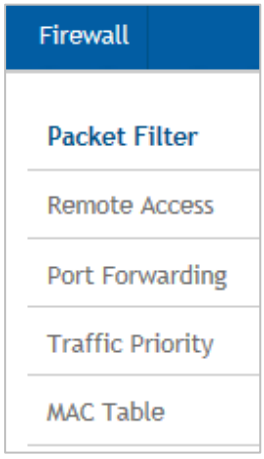
Select if the connection to the DynDNS service shall be SSL-protected.

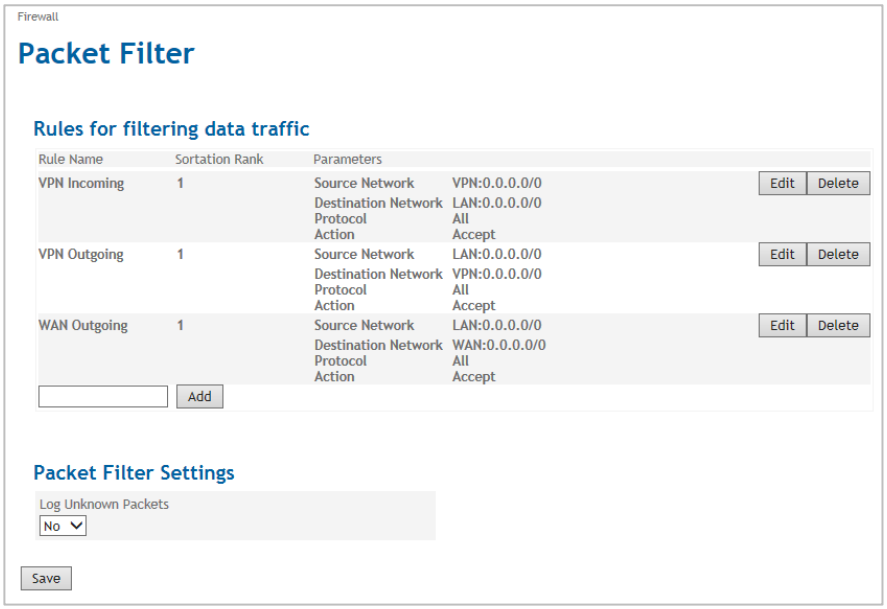
8 Firewall Settings

8.1 Configure the Packet Filter

Packet Filter

Click on the **`Firewall`** tab and select "**`Packet Filter`**" to open the screen.





`Packet Filter`

The firewall prohibits all data traffic through the TAINY iQ, e.g. from LAN to WAN or LAN to LAN if no rules for the Packet Filter are set. Only the internal traffic of data traffic which is terminated inside the TAINY iQ, e.g. for configuration is not blocked.

By default three rules for the Packet Filter are set (VPN Incoming, VPN Outgoing and WAN Outgoing).

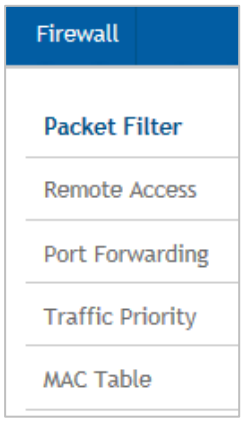
Packet filter can be defined to allow data traffic from/to a specific **Data Source** to a specific **Data Destination**.

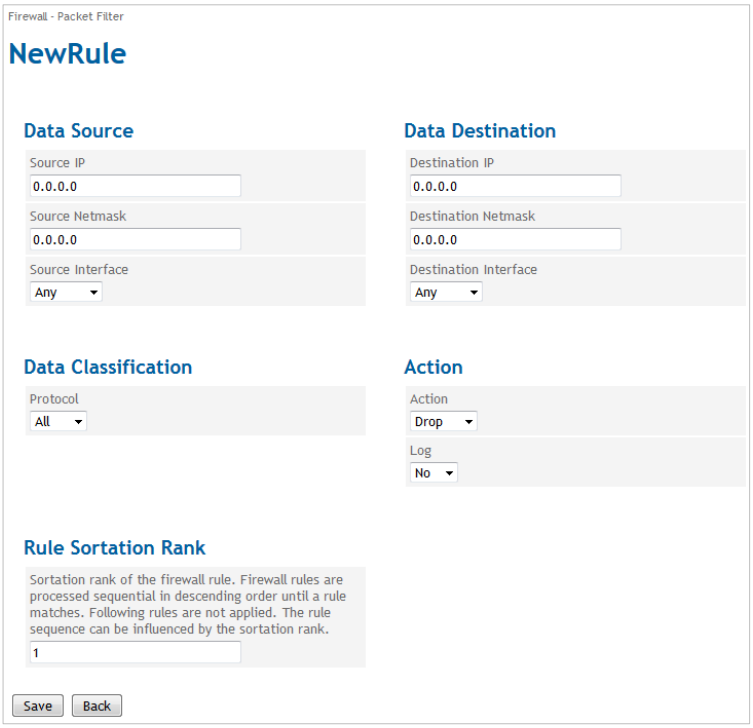
To define a packet filter chose a **Rule Name** and click the "`Add`" or "`Edit`" button.

`Packet Filter Settings`

Set the **`Log Unknown Packets`** to "`Yes`" to display them in the log files for received unidentified data packets.

Define a Rule





Data Source

Enter the IP address and the netmask of the application that shall send the data. Define the **Source Interface** the Data Source is connected to (WAN, LAN, DM VPN or Any).

Data Destination

Enter the IP address and the netmask of the application which shall receive the data. Define the **Destination Interface** the Data Destination is connected to (WAN, LAN, DM VPN or Any).

Data Classification

Define whether only a certain data protocol may pass the packet filter, e.g. TCP, UDP, ICMP or Any.

Action

Define whether data from this Data Source shall be **Accept**ed, **Drop**ped or **Reject**ed.

If Log is enabled (`Yes`) each time the conditions for the rule are fulfilled, an entry will be made to a firewall log, retrievable via the Snapshot (see chapter 13.6).

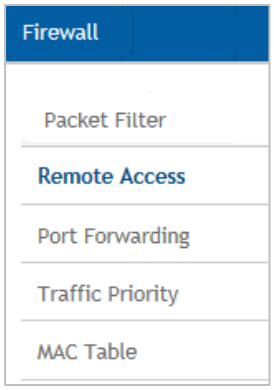
Rule Sortation Rank

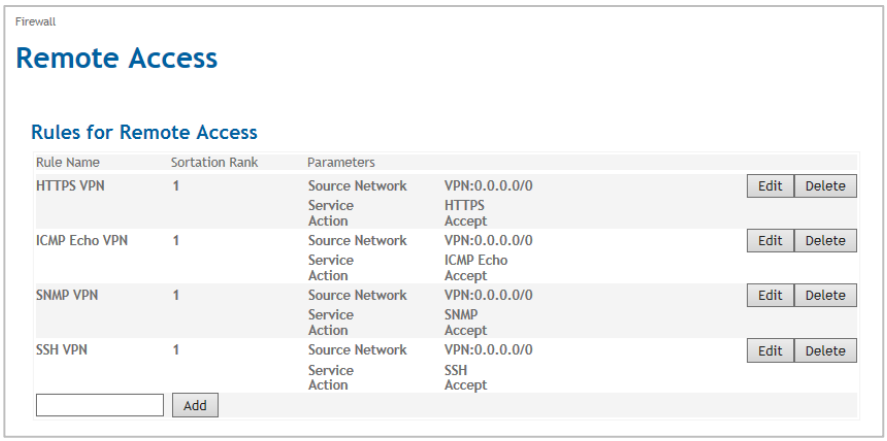
Sortation Rank of the firewall rule. Firewall rules are processed sequential in descending order until a rule matches. Following rules are not applied. The rule sequence can be influenced by the sortation rank. Rank 1 will be processed first, rank 2 second, etc.

8.2 Configure Remote Access

Remote Access

Click on the **`Firewall`** tab and select "**`Remote Access`**" to open the screen.





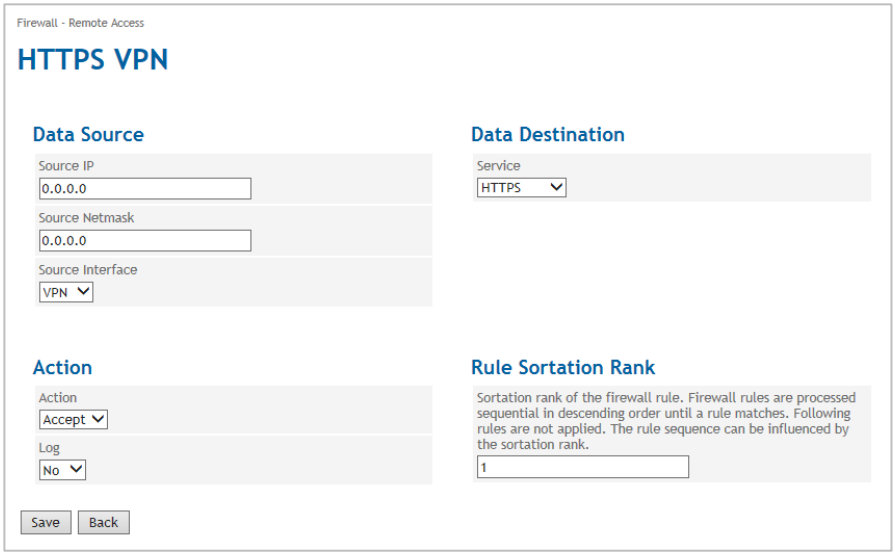
Remote Access

It is possible to activate such services as HTTP, SSH, ICMP or SNMP for WAN settings via the firewall settings.

Define Rules for Remote Access

To define rules for a new remote access or change the rules for an existing remote access click the "`Add`" or "`Edit`" button.

`HTTPS VPN`



`Data Source`

Enter the `IP address` and the `Netmask` of the application that shall send the data.

Define the **`Source Interface`** the Data Source is connected to (WAN, LAN, DM VPN or Any)

`Data Destination`

Select the required **`Service`** (see chapter 16) from the list:

- HTTPS
- SSH
- ICMP
- SNMP

Action

Define whether data from this Data Source shall be **Accept**ed, **Dropp**ed or **Reject**ed.

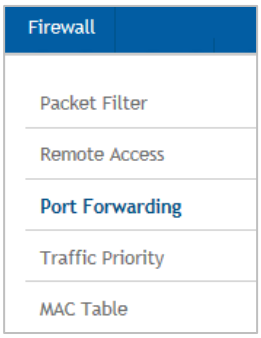
If Log is enabled (Yes) each time the conditions for the rule are fulfilled, an entry will be made to a firewall log, retrievable via the Snapshot (see chapter 13.6)

Rule Sortation Rank

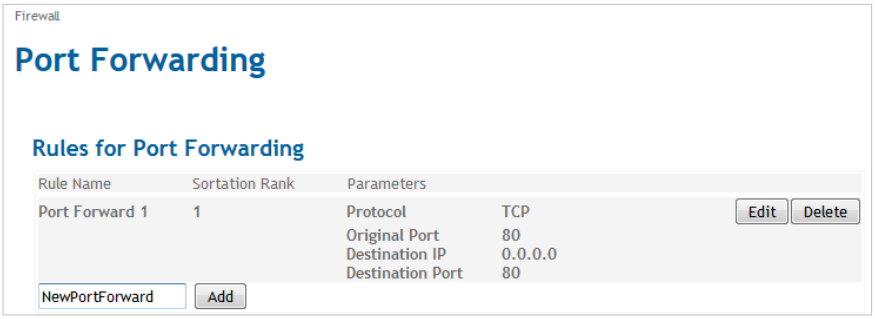
Sortation Rank of the firewall rule. Firewall rules are processed sequential in descending order until a rule matches. Following rules are not applied. The rule sequence can be influenced by the sortation rank. Rank 1 will be processed first, rank 2 second, etc.

8.3 Configure the Port Forwarding

Port Forwarding



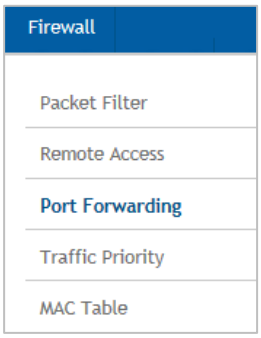
Click on the **Firewall** tab and select "**Port Forwarding**" to open the screen.

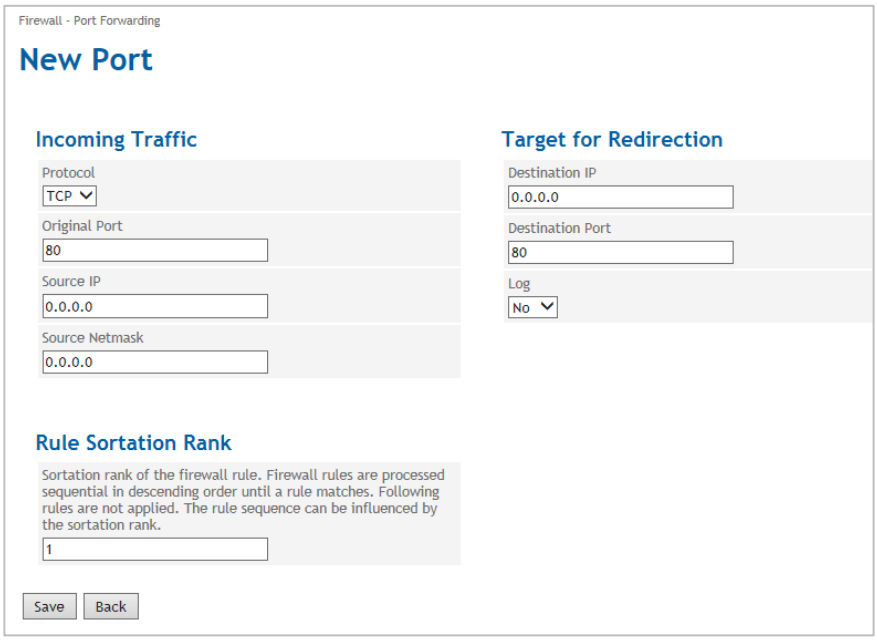


Port Forwarding can be defined to forward data traffic received by the TAINY iQ's WAN interface on a certain IP port to a defined IP address/port.

To define a packet filter chose a **Rule Name** and click the "Add" or "Edit" button.

Define a Rule





`Incoming Traffic`

Defines the protocol type of the incoming data which shall be forwarded (TCP or UDP) and the IP port the incoming data is originally sent to.

By Source IP / Netmask the port forwarding rule can be applied only to data coming from a certain source network.

`Target for Redirection`

Defines by IP address and IP port the destination the data are forwarded to.

If Log is enabled (`Yes`) each time the conditions for the rule are fulfilled, an entry will be made to a firewall log, retrievable via the Snapshot (see chapter 13.6).

`Rule Sortation Rank`

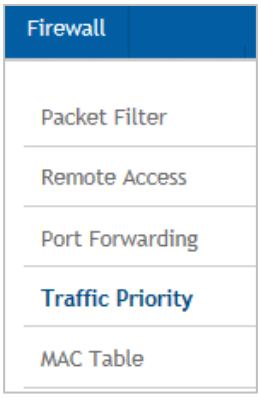
Sortation Rank of the firewall rule. Firewall rules are processed sequential in descending order until a rule matches. Following rules are not applied. The rule sequence can be influenced by the sortation rank. Rank 1 will be processed first, rank 2 second, etc.

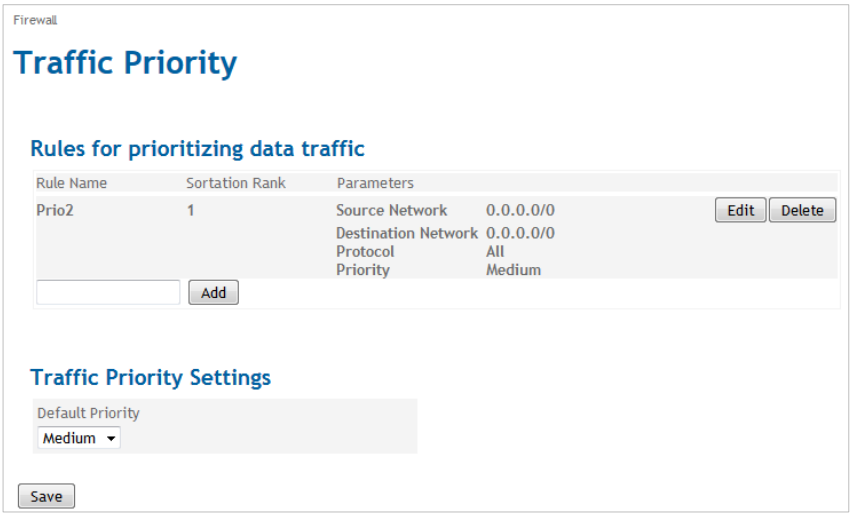
Rule Sortation is not applied for IP ports used by TAINY iQ itself, like 443, 500, 4500.

8.4 Configure the Traffic Priority

Traffic Priority

Click on the **`Firewall`** tab and select "**`Traffic Priority`**" to open the screen.

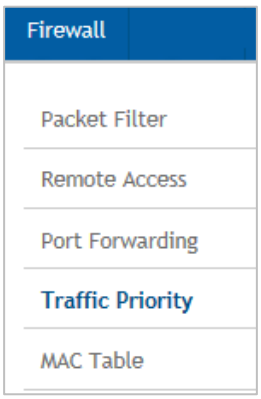


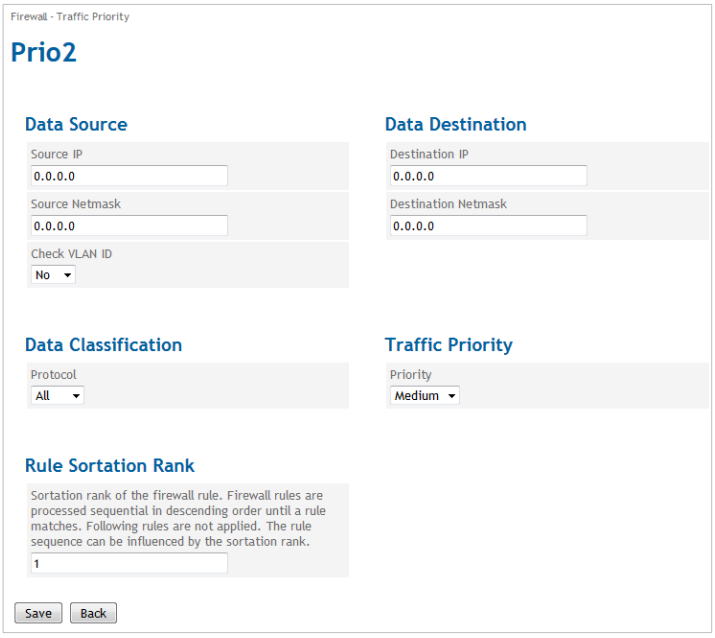


Use this function to prioritize the communication of selected data paths (from LAN to WAN only). If there are data in a path of high priority, they will be transmitted first. They are followed by data in paths of medium priority. Only if there are no data in path of high or medium priority, data in path of low priority are transmitted.

To define a rule for prioritizing data traffic chose a **Rule Name** and click the "`Add`" or "`Edit`" button.

Define a Rule



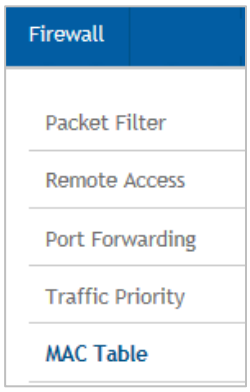


The data paths are defined by the IP address of the source network (**`Source IP/Netmask`**) and the IP range of the destination network (**`Destination IP/Netmask`**). If **`Check VLAN ID`** is enabled, the rule will be only applied to traffic of the specified VLAN.

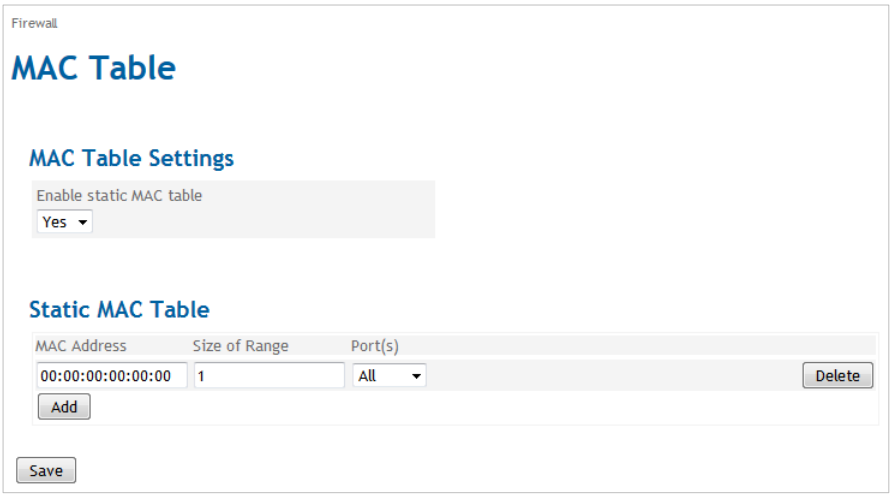
In addition you can prioritize data of a certain type of protocol (TCP, ICMP etc.) as well as data towards a certain destination.

8.5 Configure the MAC Table

MAC Table



Click on the **`Firewall`** tab and select "**`MAC Table`**" to open the screen



If the Static MAC Table function is enabled, only devices may communicate with or via the TAINY iQ, which MAC addresses are entered in the Static MAC Table. You can enable a MAC address to All ports or to a certain Physical Network Interface (ETH0… ETH5) only.

The Size of Range determines the number of MAC Addresses starting with the given MAC Address which will not be blocked.

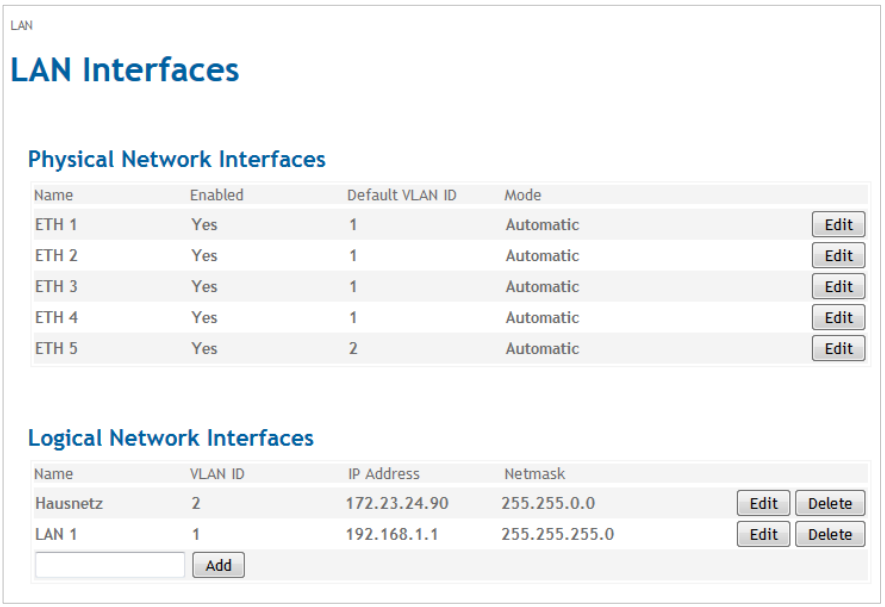
9 LAN Settings

9.1 Configure the Physical Network Interfaces / Create VLANs

LAN Interface

4GDSE6
3GDSE6

Click on the **LAN** tab and select "**LAN Interfaces**" to open the screen.

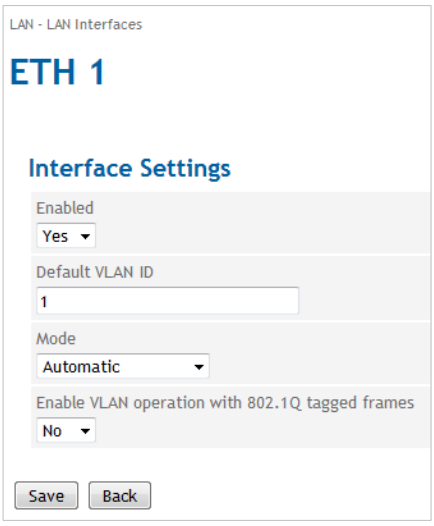


Physical Network Interfaces

The TAINY iQ provides up to 5 Physical Network Interfaces ETH1…ETH5 to connect local applications to. ETH0 can be used as a DSL/Cable WAN port or as an additional LAN port (see chapter 9.4).

To configure each Physical Network Interface separately click the corresponding "Edit" button.

ETH1…ETH5



Interface Settings

Enables or **disables** the Physical Interface. To use the interface select "Yes".

Mode

Selects the data transmission rate (10Mbit/s or 100Mbit/s) and the transmission method (half duplex or full duplex). If the mode is set to "Automatic", the TAINY iQ and the device connected to this Physical Interface determines the settings automatically.

VLAN ID

This ID assigns the Physical Interface to a Virtual Local Area Network (VLAN). All Physical Interfaces which have the same VLAN ID are part of this VLAN.

See Glossary.

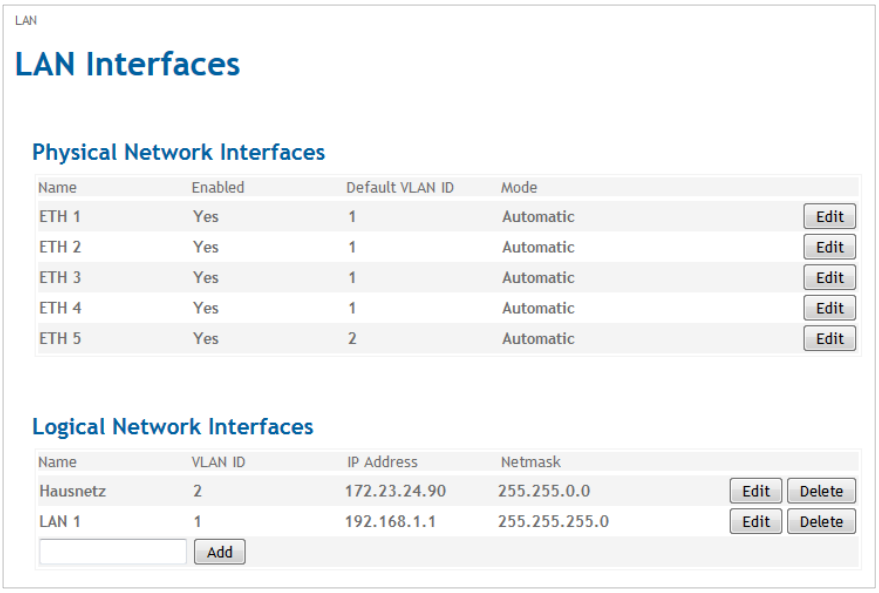
Enable VLAN Tags (802.1Q)

Select "Yes", if the VLAN Tags shall be forwarded via this Physical Interface towards the connected application. Otherwise the VLAN Tags will be removed for outbound communication.

9.2 Configure the Logical Network Interfaces / Address Assignment (DHCP)

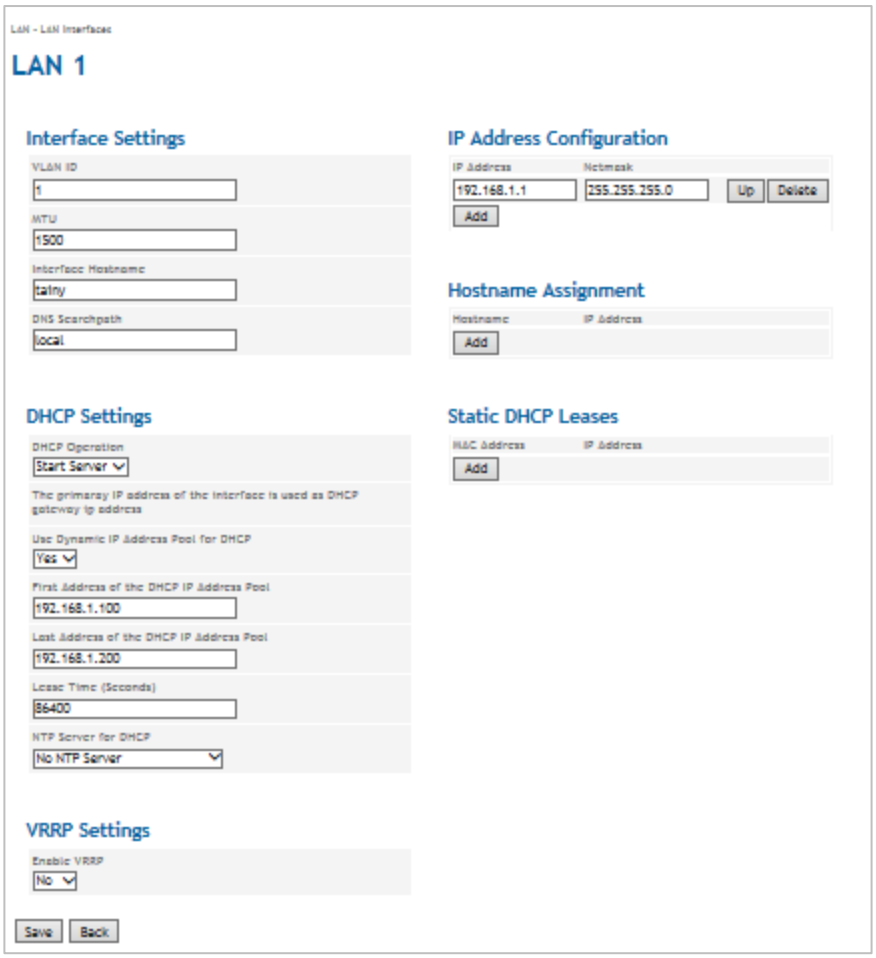
LAN Interface

Click on the **LAN** tab and select "**LAN Interfaces**" to open the screen.



LAN 1

Click the "Add" button to create a new Logical Network Interface, Click the "Edit" button to modify the settings.



Interface Settings

VLAN ID: Enter the ID of the VLAN to which this Logical Network Interface shall relate to. A Logical Network Interface may only relate to one VLAN.

MTU: Enter the MTU (Maximum Transmission Unit) to determine the maximum size of IP packets.

Interface Hostname

The Logical Network Interface can either be addressed by an IP address or a hostname. To address it by hostname enter the hostname in the entry field.

DNS Searchpath

Enter the Domain Name of the search path.

Hostname Assignment

Hostname, IP Address: The TAINY iQ allows assigning IP addresses of remote stations to hostnames. Using this function, applications connected to TAINY iQ's LAN interfaces address these remote stations by the entered hostnames. TAINY iQ functions (e.g. NTP) also use this feature. See also the Hostname Assignment related to the WAN setup, chapter 7.12.

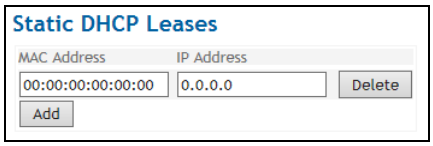
DHCP Settings

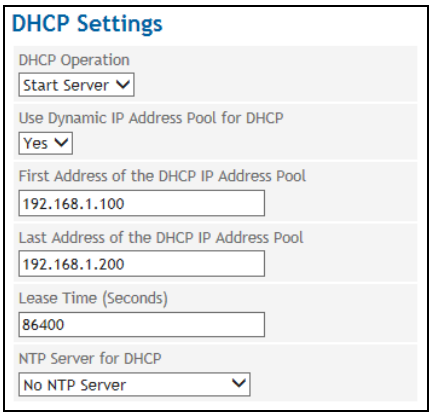
DHCP Operation: The TAINY iQ provides a DHCP server function or a DHCP relay function.

Note

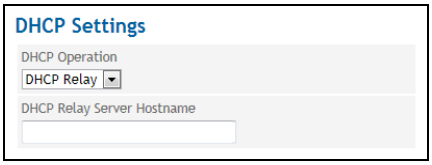
Only the primary IP-address of the interface (e.g. Eth0) is used as DHCP-Gateway-IP.

If the DHCP server function is activated, the TAINY iQ itself assigns IP addresses to applications connected to the LAN interface. Define the range of address the assigned IP addresses shall be taken from and/or static IP leases.





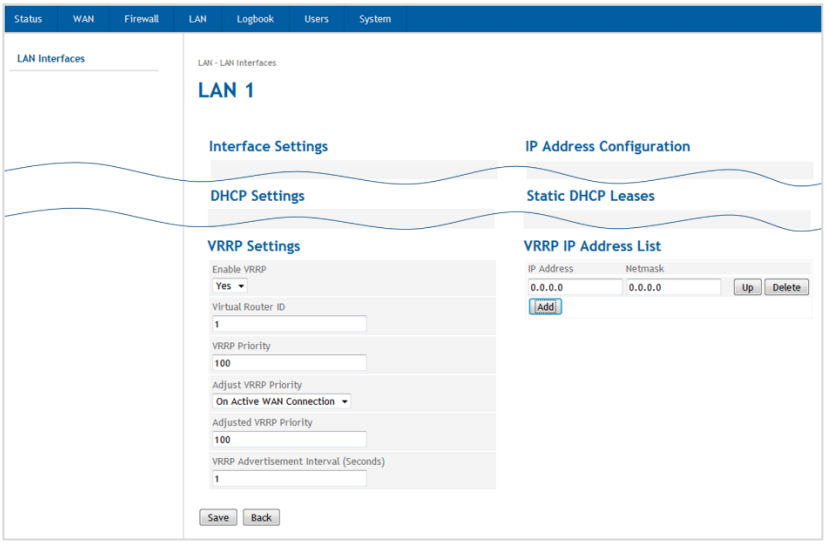
If the DHCP relay function is activated, the TAINY iQ routes the DHCP requests of applications connected to the LAN interface to a remote DHCP relay server which provides the IP addresses. Enter the hostname or the IP address of the DHCP Relay Server.



9.3 Configure VRRP

VRRP Settings

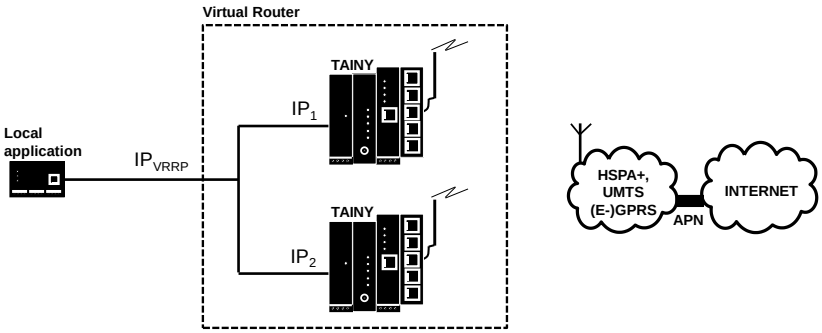
Click on the LAN tab and select "`LAN Interface`" to open the screen.



The TAINY iQ supports the Virtual Router Redundancy Protocol (VRRP). Enable/disable this function in the submenu the LAN tab for Logical Network Interfaces. Two TAINY iQ routers perform as one virtual router. If one TAINY iQ loses the WAN connection (or the VPN connection) the second TAINY iQ takes over/supports the connection.

If you define several virtual routers for a network, make sure to assign different IDs to them.

The **VRRP Priority** defines which TAINY acts as master and which as the backup. The TAINY iQ which has the highest priority acts as the master. Enter values between 1 (lowest prio) and 254 (highest prio). The VRRP priority can be adjusted automatically to a new value (**Adjusted VRRP Priority**) in case of an active WAN or VPN connection.



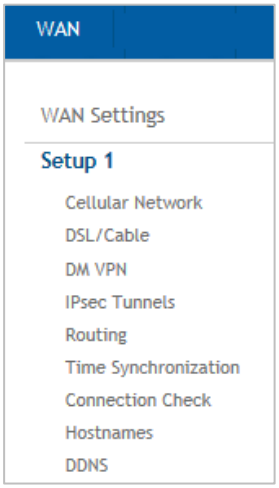
The IP_{VRRP} is the IP address of the Virtual Router. Enter/Add it to the **VRRP IP Address List**. Use this as the standard gateway for the local application. IP_1 and IP_2 are the IP addresses of TAINY iQs as being entered in the **IP Address Configuration** of each TAINY iQ.

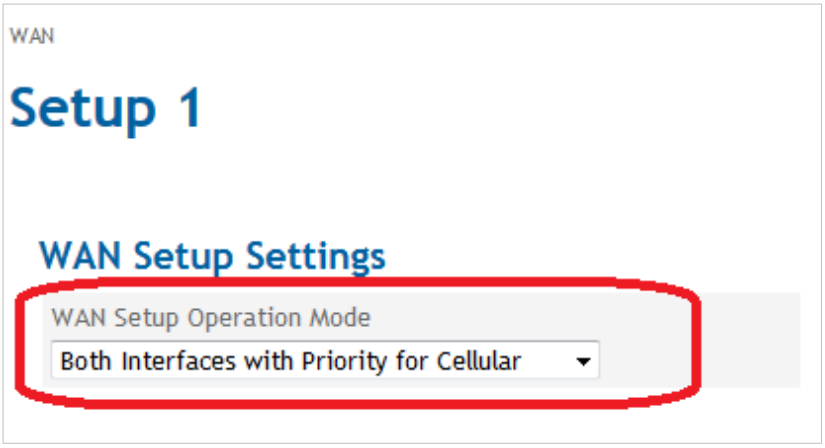
9.4 Using ETH0 as a LAN Port

To use the ETH0 port as the sixth LAN port of the TAINY iQ configure as described below.

WAN Setup Settings

Select the **WAN** tab and click "**Setup 1**" to open the screen.

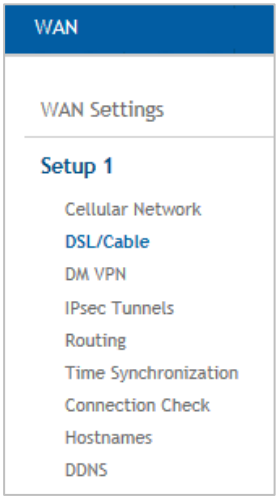


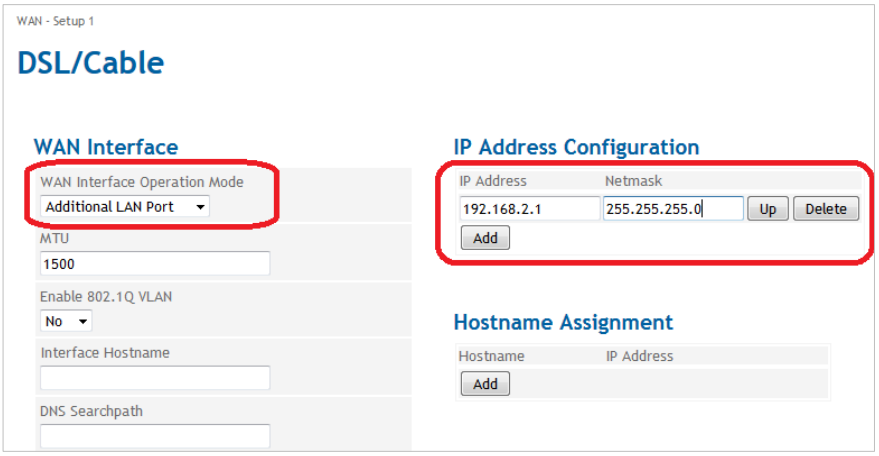


Set the **WAN Setup Operation Mode** to **Both Interfaces with Priority for Cellular** to switch on the ETH0 port. Since it is prioritized the WAN communication will be routed via the cellular.

DSL/Cable Settings

Open the DSL/Cable submenu. Define an IP address and netmask on the Additional LAN Port with a different network to the other 5 ETH ports.

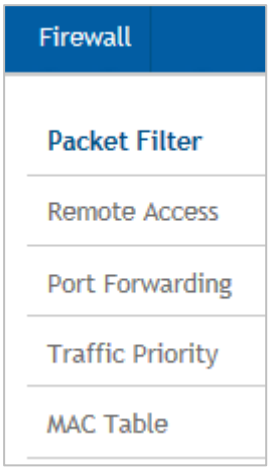


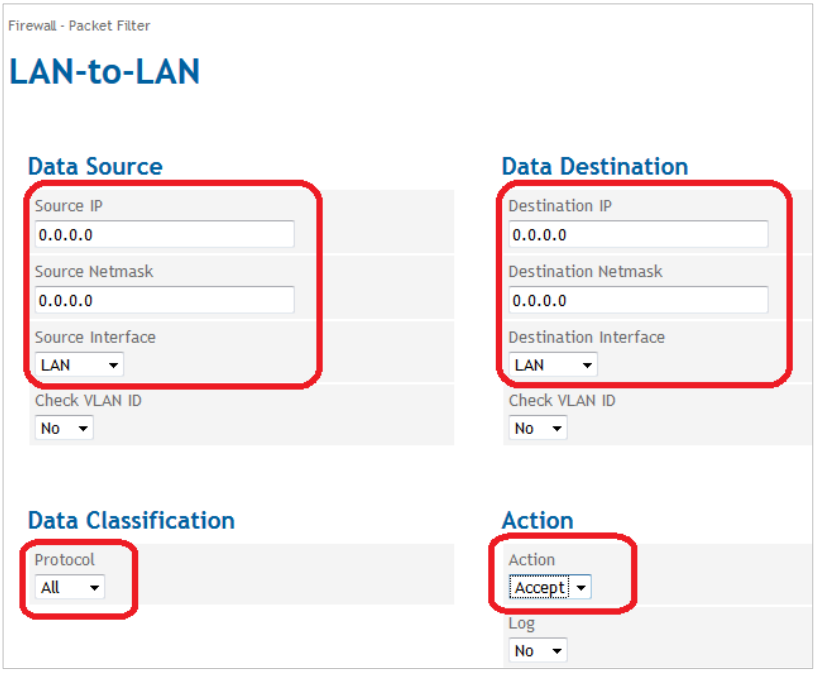


Firewall Packet Filter

Click on the **`Firewall`** tab and select "**`Packet Filter`**" to open the screen.

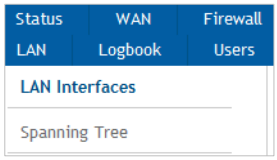
Define a Firewall package filter rule and allow traffic from LAN to LAN.

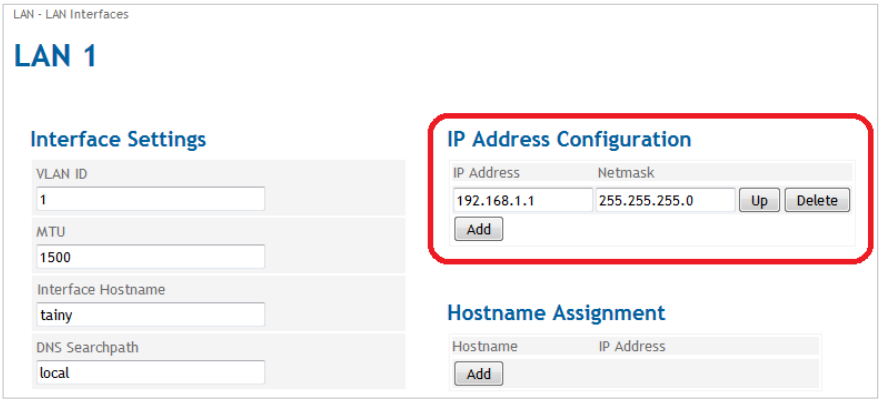




LAN Interfaces

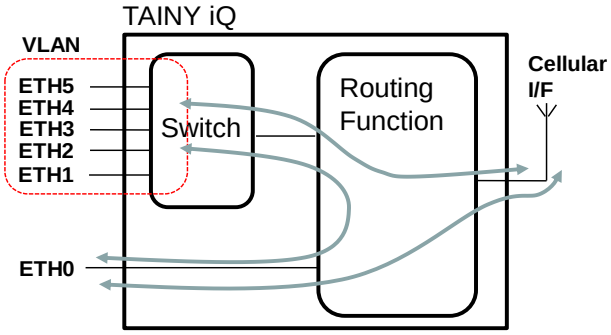
Click on the **`LAN`** tab and select "**`LAN Interfaces`**" to open the screen. Define a different network at the 5 Port Switch





After these configuration steps, the ETH0 port performs as a LAN port of the TAINY iQ.

Data can be routed between the ETH0 and ETH1...5 and the Cellular Interface.



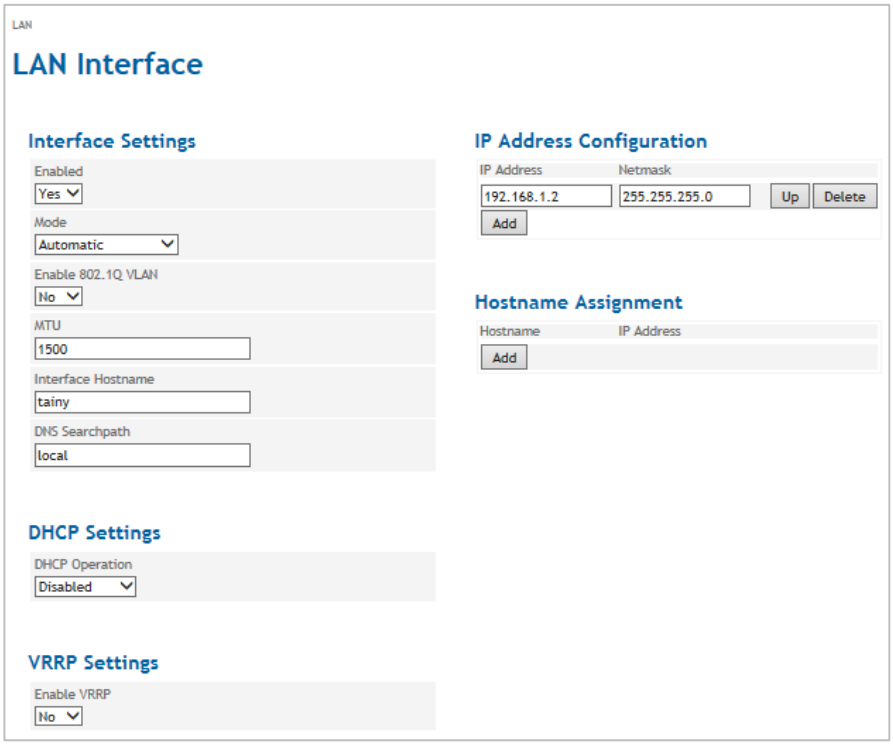
The ports ETH1 to ETH5 can be grouped to VLANs.

9.5 Configure the Interfaces/DHCP/VRRP Settings (3GDSE2, 4GDSE2)

LAN Interface

3GDSE2
4GDSE2

Click on the **LAN** tab and select "**LAN Interfaces**" to open the screen.



Interfaces Settings

Enable

Select "Yes" to enable the interface.

Mode

Set the required mode to select the required data transmission rate (10Mbit/s or 100Mbit/s) and the transmission method (half duplex or full duplex).

If the mode is set to “Automatic”, the TAINY iQ and the device connected to this LAN Interface determines the settings automatically

Enable 802.1Q VLAN

Set to “**Yes**” and enter the ID of the VLAN to enable the communication with 802.1q tagged Ethernet frames.

Set to “No” to disable 802.1q tagges in this interface.

MTU

Enter the MTU (Maximum Transmission Unit) to determine the maximum size of IP packets.

Interface Hostname

The Logical Network Interface can either be addressed by an IP address or a hostname. To address it by hostname enter the hostname in the entry field.

DNS Searchpath

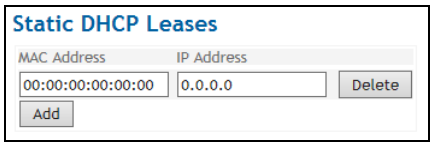
Enter the Domain Name Server oft he search path

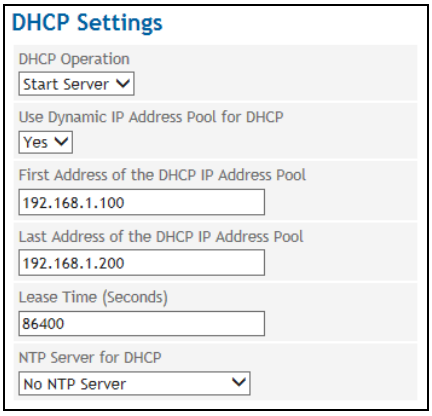
DHCP Settings

DHCP Operation

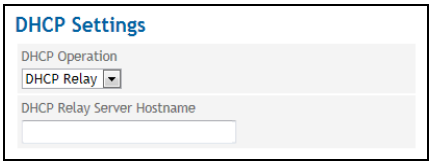
The TAINY iQ provides a DHCP server function or a DHCP relay function

If the DHCP server function is activated, the TAINY iQ itself assigns IP addresses to applications connected to the LAN interface. Define the range of address the assigned IP addresses shall be taken from and/or static IP leases.





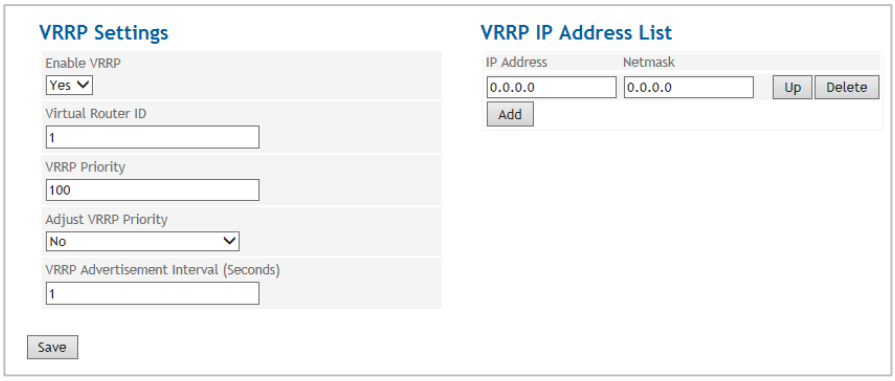
If the DHCP relay function is activated, the TAINY iQ routes the DHCP requests of applications connected to the LAN interface to a remote DHCP relay server which provides the IP addresses. Enter the hostname or the IP address of the DHCP Relay Server.



VRRP Settings

VRRP (Virtual Router Redundancy Protocol) secures the availability of important gateways within the network by utilising a number of TAINY iQs.

To configure the VRRP setting set **Enable VRRP** to “Yes”.



Virtual Router ID

ID for the group of utilised TAINY iQs.

VRRP Priority

Defines, which TAINY iQ acts as master and which as the backup. The TAINY iQ which has the highest priority acts as the master. Enter values between 1 (lowest prio) and 254 (highest prio). The VRRP priority can be adjusted automatically to a new value.

Adjusted VRRP Priority

In case of an active WAN or VPN connection.

VRRP IP Address List

IP addresses of the VRRP (TAINY iQs).

IP Address/ Hostname

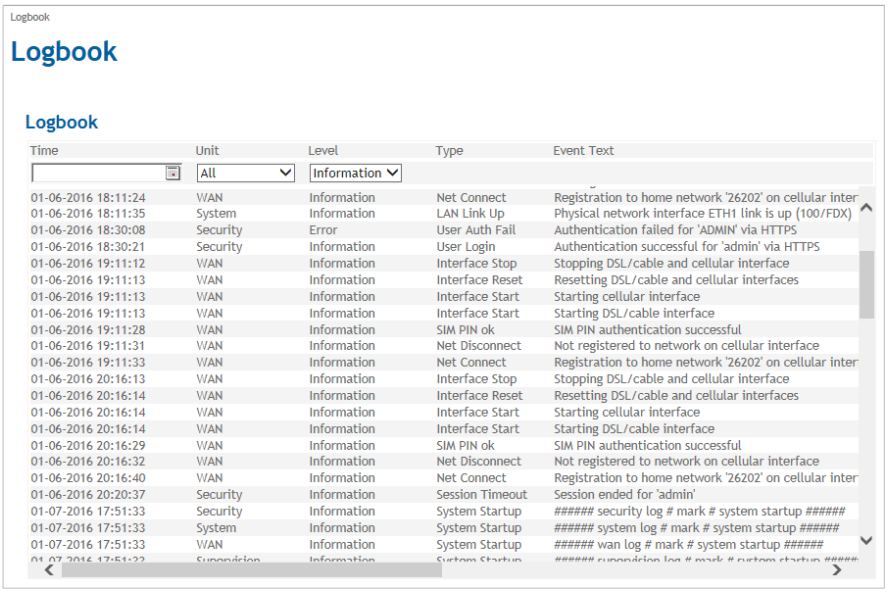
Hostname, IP Address: The TAINY iQ allows assigning IP addresses of remote stations to hostnames. Using this function, applications connected to TAINY iQ's LAN interfaces address these remote stations by the entered hostnames. TAINY iQ functions (e.g. NTP) also use this feature.

10 Logbook

10.1 Read the Logbook

Logbook

Click on the **Logbook** tab and select "**Logbook**" to open the screen.



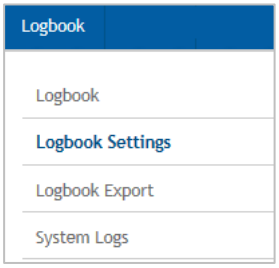
Important incidents of the TAINY iQ are saved and displayed in this view. The entries are refreshed automatically.

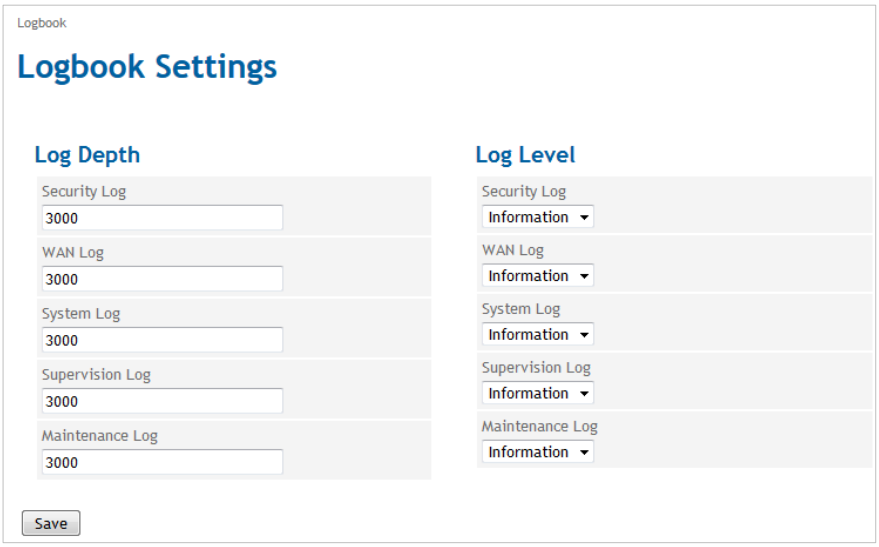
Also Log entries created by rules for the WAN setup operations are written into this logbook (see chapter 7).

10.2 Configure the Logbook Function

Logbook Settings

Click on the **Logbook** tab and select "**Logbook Settings**" to open the screen.





The logbook is cut in five sections (Unit): `Security`, `WAN`, `System`, `Supervision` and `Maintenance`. The number of stored log entries can be selected for each section separately. If the maximum number of log entries is reached, the oldest log entries of this section will be overwritten.

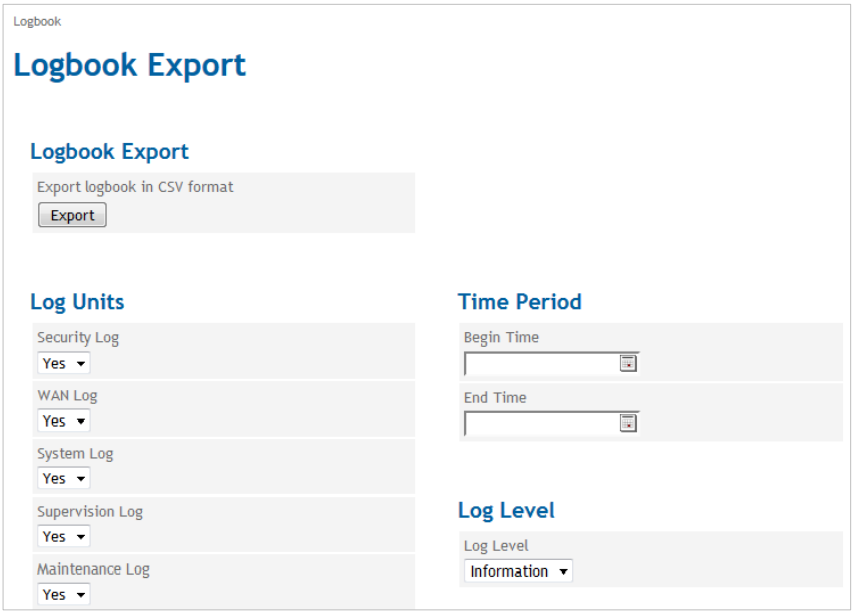
All log entries are characterized by a log level. The lowest level being "`Debug`", the highest level being "`Fatal`".

For each logbook section you can select the minimum Log level which is stored. If you select "Debug", all Log entries are stored, if you select "Error" all Log entries with the level "Error" and "Fatal" are stored.

10.3 Export the Logbook

Logbook Export

Click on the **`Logbook`** tab and select "**`Logbook Export`**" to open the screen.



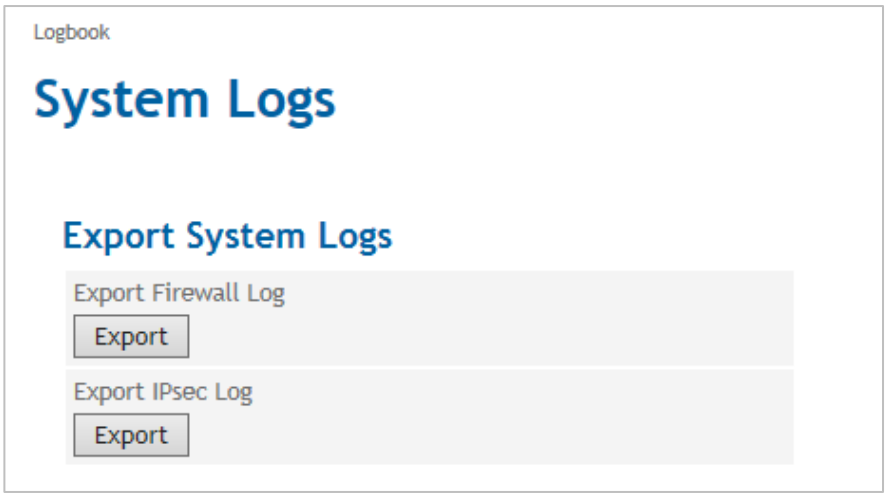
Click on the "`Export`" button to write the logbook data into a CSV file. Select all the **Log Units** and the **Log Level** that shall be included in the export.

It is also possible to select a period of time (`Begin` and `End Time`) for the export.

10.4 System Logs

Export System Logs

Click on the **Logbook** tab and select "**Logbook Export**" to open the screen.



Export Firewall Log

Click "Export" button to export the firewall log file in a zip file to an external pc.

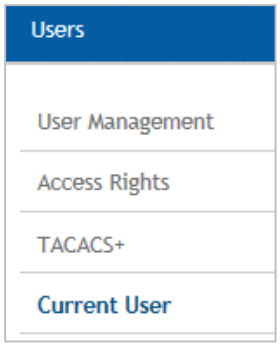
Export IPsec Log

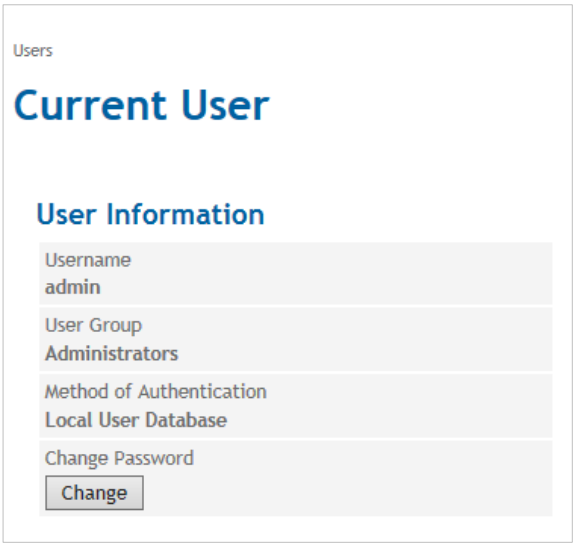
Click "Export" button to export the IPsec Log file in a zip file to an external pc.

11 Manage Users, Enable/Disable SNMP Access

Current User

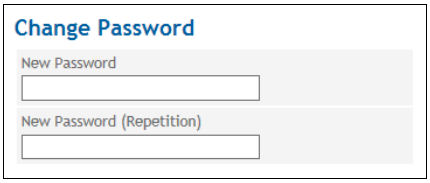
Click on: the **`Users`** tab and select "**`Current User`**" to open the screen.





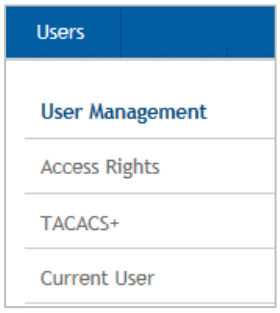
`Change Password`

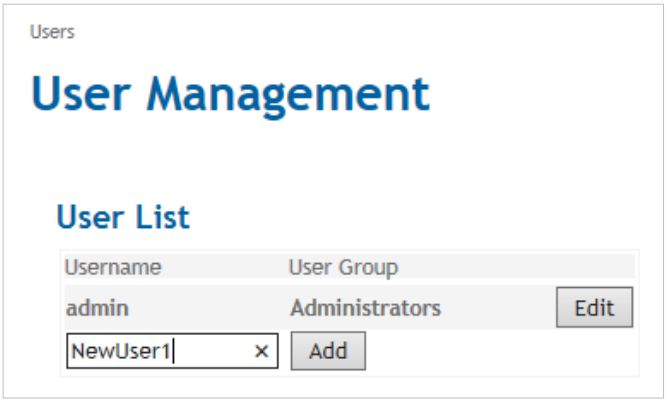
In this screens information about the current user are displayed. Click on the "`Change`" button to change the password of the current user.



User Management

Click on: the **`Users`** tab and select "**`User Management`**" to open the screen.



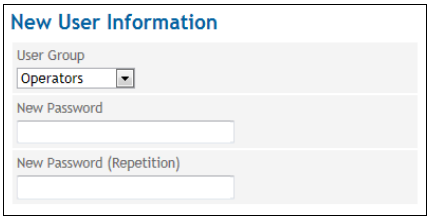


Click the "`Add`" to define an additional user or the "`Edit`" button to change the settings for an existing user.

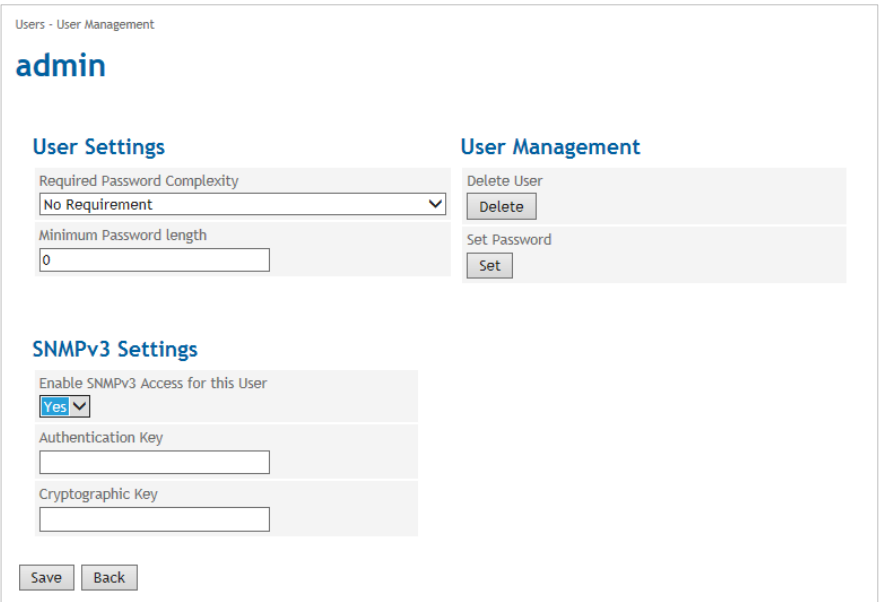
Add User

`User Group`

Select the "`User Group`", the new user belongs to. The user's access rights are defined by the User Group. An Admin has got unlimited rights, whereas the rights of Guest or Operator "`User Groups`" can be limited (see Access Rights below).



Edit User



`User Settings/ Management`

For each user you define the `Required Password Complexity` (numbers, letters, upper case, lower case, special characters) and the `Minimum Password Length`.

Apart from assigning a password you can delete the user in this screen.

`SNMPv3 Settings`

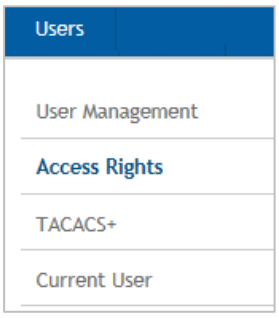
Select "`Yes`" to enable the access via SNMPv3 for the current user.

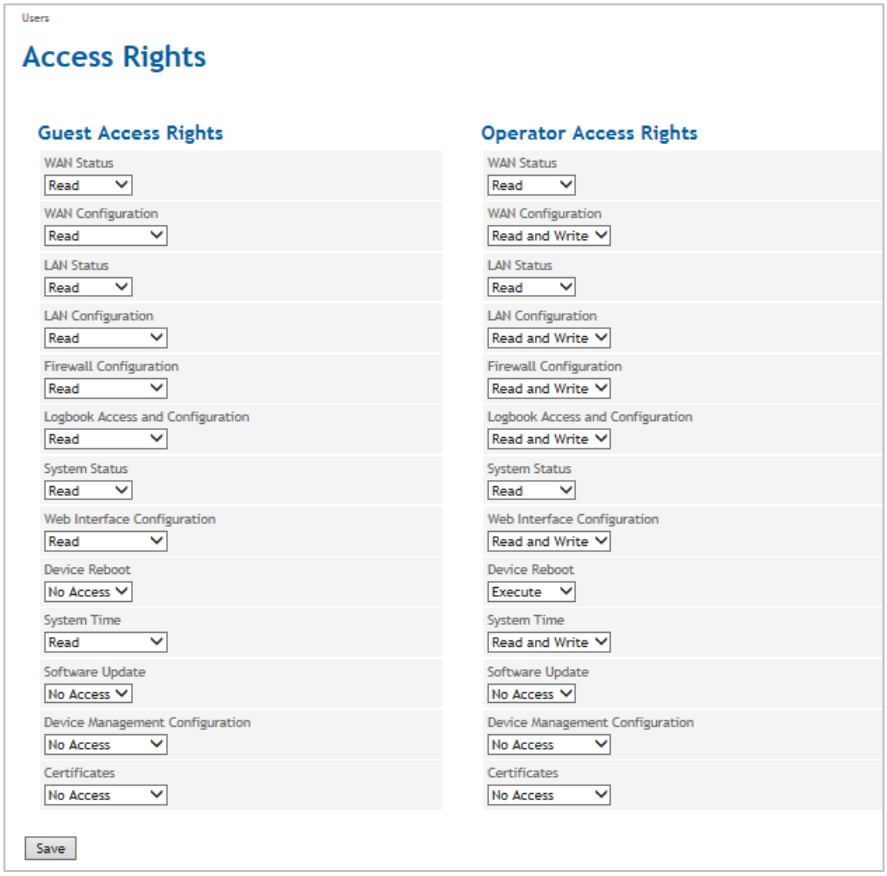
Enter the `Authentication` and a `Cryptographic Key` for this access.

11.1 Configure Operator and Guests Access Rights

Access Rights

Click on the **`Users`** tab and select "**`Access Rights`**" to open the screen.



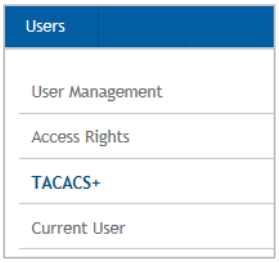


Access Rights

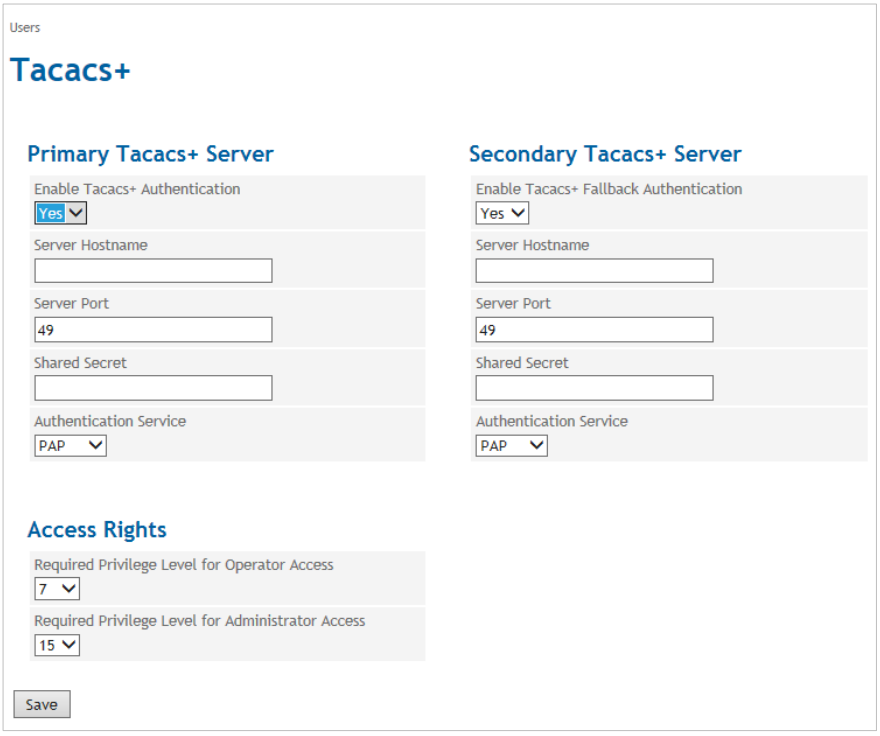
While an Admin always has got full access rights, the access rights of the members of the *Guest* user group and the *Operator* user group are limited. Define the `Access Rights` for the Guest and Operator Group in the corresponding columns of the screen.

11.2 Configure TACACS+

TACACS+



Click on: the **Users** tab and select "**TACACS+**" to open the screen.

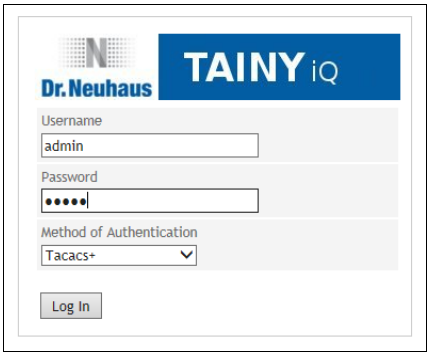


With the authentication method TACACS+ (Terminal Access Controller Access Control System Plus), the access data for the TAINY iQ are not saved on the device itself, but on an external server.

In the event of a registration request, the TAINY iQ forwards the registration data to the TACACS+ server. The server checks the validity of the data and reports the result back to the TAINY iQ, which then either rejects or accepts the registration.

Activate the authentication process TACACS+ in this screen by setting the parameters, the TAINY iQ needs to connect to the TACACS+ server.

As soon as the TACACS+ service is activated, the type of registration can be selected from an additional drop-down list (*TACACS+* or *Local*) in the registration.



Primary /Secondary TACACS+ Server

A primary and a secondary (backup) TACACS+ server can be used.

Enter the Hostname (or IP address), port number, shared secret and authentication protocol to reach and access the TACACS+ server.

Access Rights

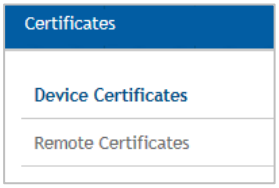
In the TACACS+ protocol the access right levels of a user are numerical coded from 1 to 15. The TAINY iQ provides three access right levels (administrator, operator and guest).

To map the levels of the TACACS+ protocol to the levels of TAINY iQ, define the minimum TACACS+ level the user shall have for TAINY iQ administrator rights and the define the minimum TACACS+ level, the user shall have for TAINY iQ operator rights. Below the operator level, the user has guests' rights only.

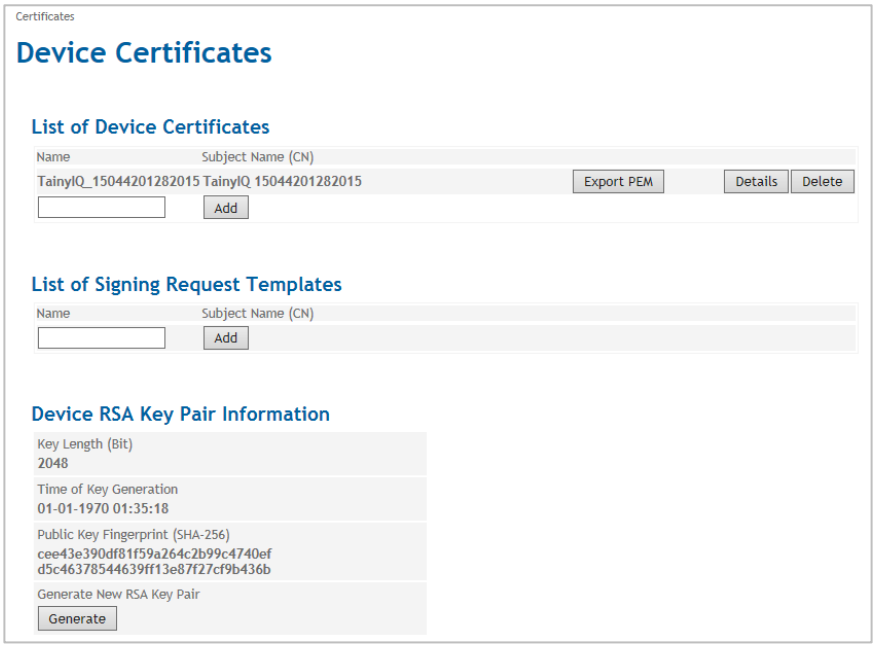
12 Certificates

12.1 Device Certificates

Device Certificates



Click on the **`Certificates`** tab and select "**`Device Certificates`**" to open the screen.



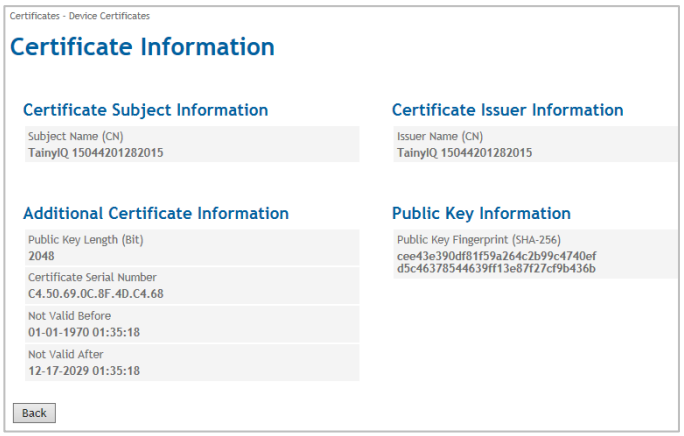
Device Certificates are all certificates of TAINY iQ. The opposite entity certificates are the Remote Certificates as described in the next chapter. See also Glossary for further information. In this view information on the device certificates, the request templates and the currently used RSA Key Pair are displayed.

It is possible to add new certificates and request templates as well as generate a new RSA Key Pair.

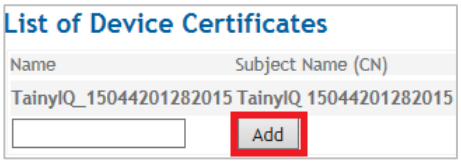
`List of Device Certificates`

View Details/Export Certificate

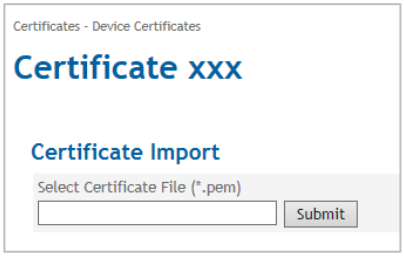
Click the "`Details`" button to display more detailed information on the specific certificate.



Add/Import Device Certificate

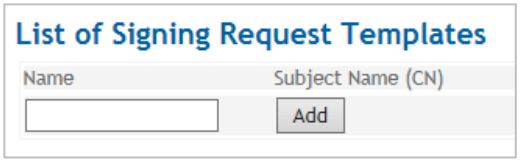


Click the "Add" button in the **List of Device Certificates** and click "Submit" to import the file of the new certificate from the administration pc. The imported certificate requires the file ending ".pem"



The new certificate will now appear in the List of Certificates.

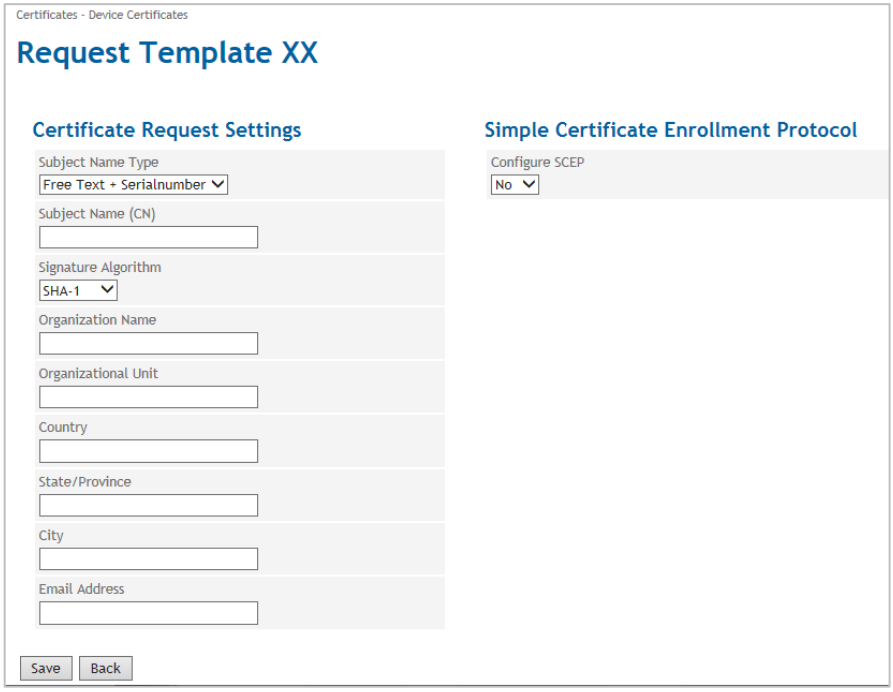
List of Signing Request Templates



All requests templates appear in the **List of Signing Request Templates** with Name and Subject Name (CN).

New Request Templates

To create a new Request Template enter the name of the template in the Name entry field and click the "Add" button. The following screen opens:



Certificate Request Settings

Enter the following parameters:

`Subject Name Type/Subject Name (CN)`

Select `Free Text + Serial number`. The serial number will be automatically attached to the subject name at export.

`Signature Algorithm`

Select either SHA-1 or SHA-256. The latter being more recent and saver.

`Organisation Name/Unit/Address/Email Address`

Enter the name and contact details into the respective entry fields.

`Simple Certificate Enrolment Protocol`

Set to **"`Yes`"** to obtain a device certificate of server that has to be configured.

Device RSA Key Pair Information

This section displays information on the currently used RSA Key Pair such as the `Key Length`, `Time of Key Generation` and the `Public Key Fingerprint.`

The pair consists of a private and a public key, which guarantee a secure data transmission.

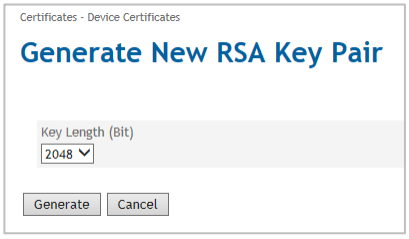
Generate a new Key Pair

To generate a new pair of keys:

Select the **`Key Length`** (in Bit) from the list.

Click "**`Generate`**" to start the process.

Mind that the process could take up to 2 minutes.

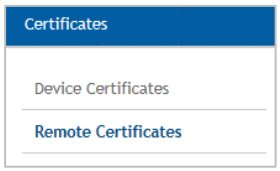


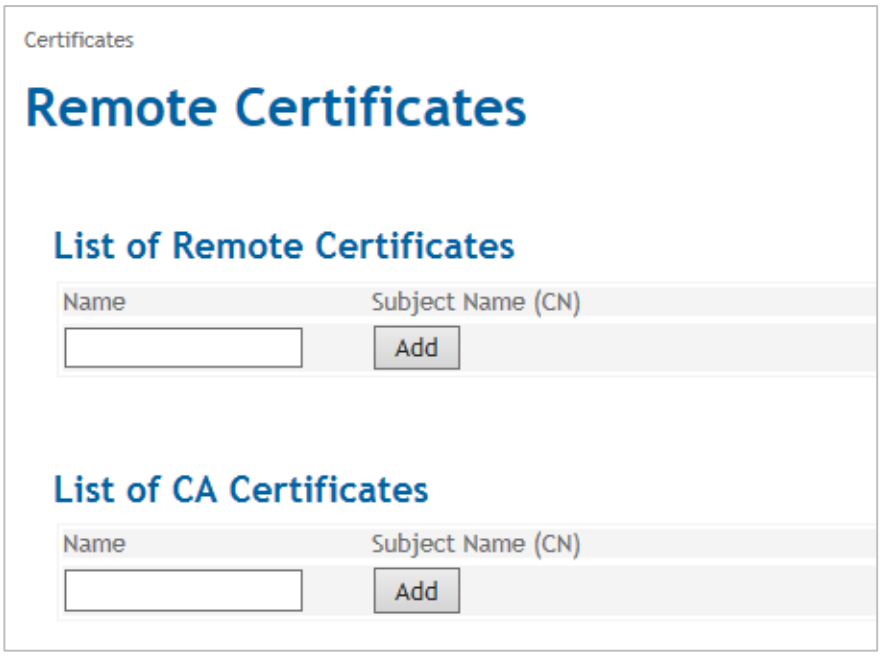
The information on the newly generated key pair appears now in the `Device RSA Key Pair Information`.

12.2 Remote Certificates

Remote Certificates

Click on the **`Certificates`** tab and select "**`Device Certificates`**" to open the screen.

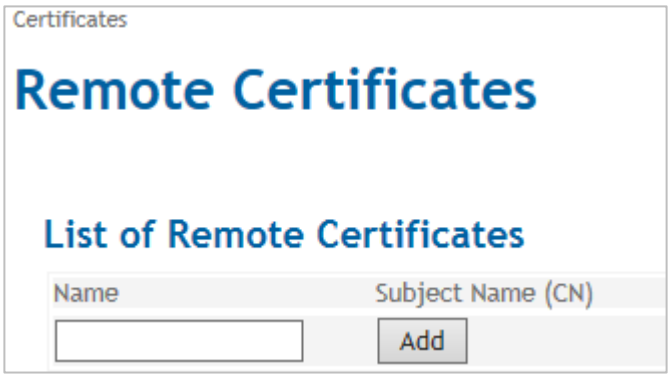




Remote certificates are all certificates that are used to authenticate the opposite entities.

The List of CA certificates contains the certificates of the accepted Certificate Authorities

`List of Remote Certificates`



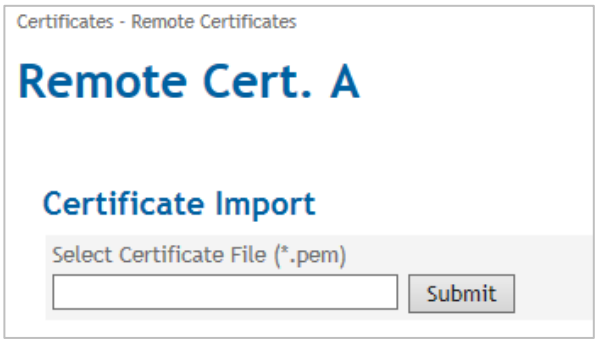
Add Remote Certificate

To upload a certificate from the opposite entity:

Enter a name in the **`Name`** entry field.

Click the "`Add`" button in the `List of Remote Certificates`.

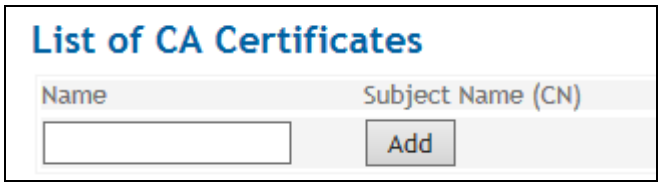
The following screen opens:



Click on "`Submit`" to upload the file of the additional remote certificate from the administration pc.

The new certificate will appear in the List of Remote Certificates.

`List of CA Certificates`



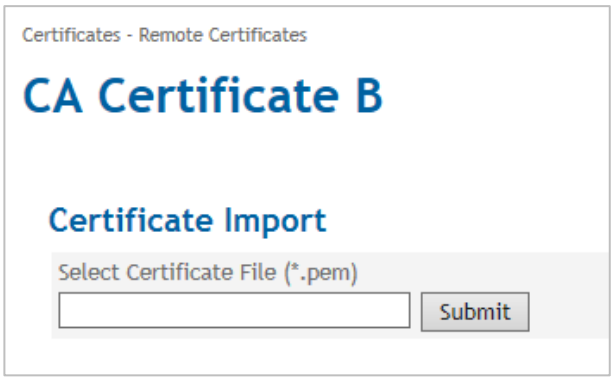
Add CA Certificate/Add Remote Certificate

To upload a certificate from CA:

Enter a name in the `Name` entry field.

Click the "`Add`" button in the `List of CA Certificates`.

The following screen opens:



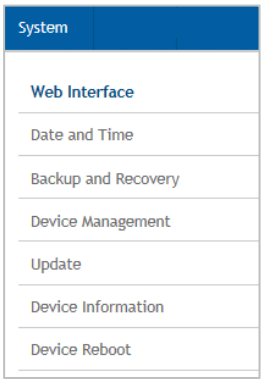
Click on "`Submit`" to upload the file of the additional CA certificate from the administration pc.

The new certificate will appear in the List of CA Certificates.

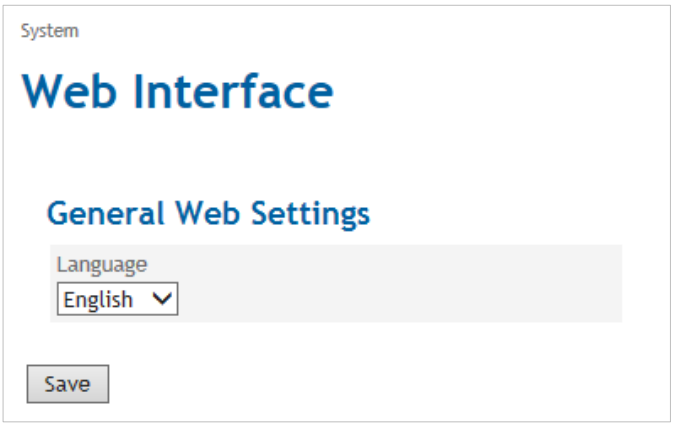
13 System

13.1 Select the System Language

Web Interface



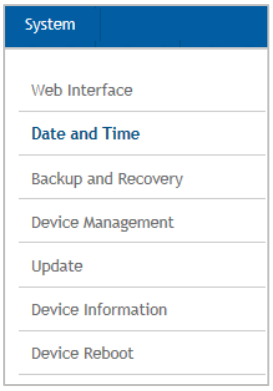
Click on the **`System`** tab and select "**`Web Interface`**" to open the screen.



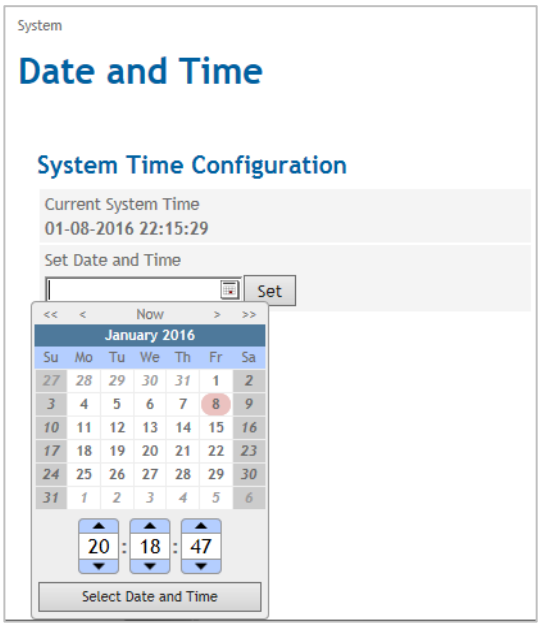
Select the "`Language`" of the Web Interface in the `General Web Settings`.

13.2 Enter manually Date and Time

Date and Time



Click on the **`System`** tab and select "**`Date and Time`**" to open the screen.

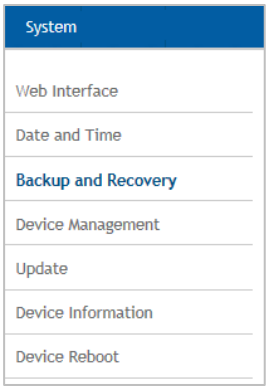


`System Time Configuration`

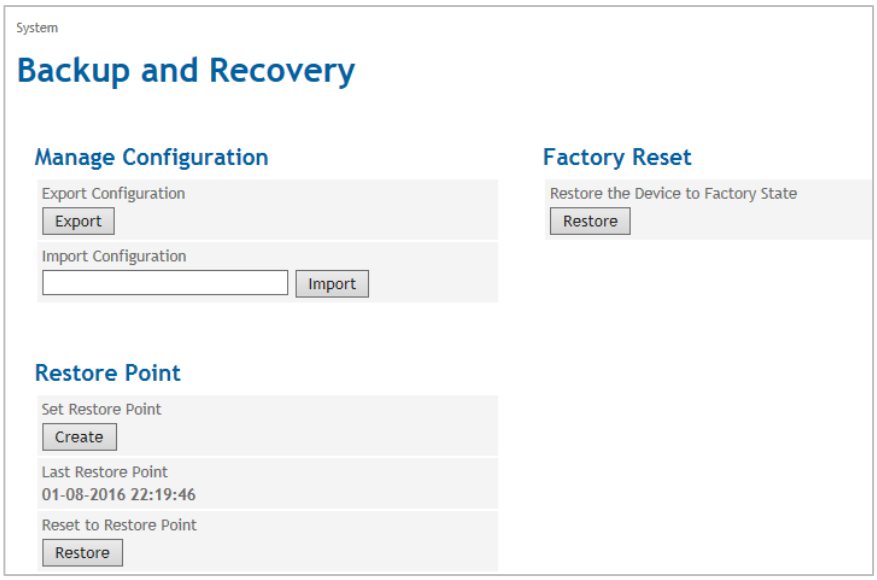
Set the `System Time` of the TAINY iQ. Enter the local time. In case the time synchronisation by NTP is active the entered date and time will be overwritten after the next NTP synchronisation.

13.3 Force a Factory Reset, Manage Device Configuration

Backup and Recovery



Click on the **`System`** tab and select "**`Backup and Recovery`**" to open the screen.

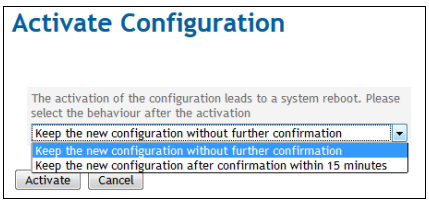


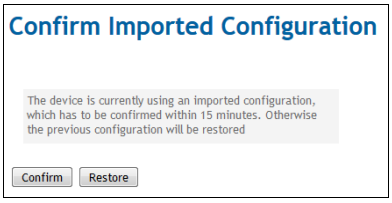
Click the "`Export`" button to write the current configuration of the TAINY iQ into a configuration file.

Select a valid configuration file and click the "`Import`" button to load a new configuration from a file.

Chose if the new configuration shall be kept without further confirmation or if the TAINY iQ should fall back to the configuration used before, in case the new configuration has not been confirmed within 15 minutes.

To create a new configuration, export the current configuration and edit it in a text editor.

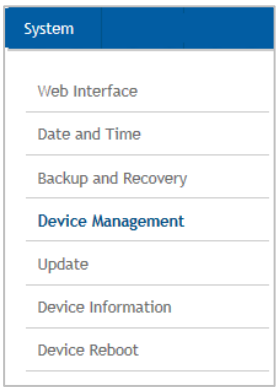


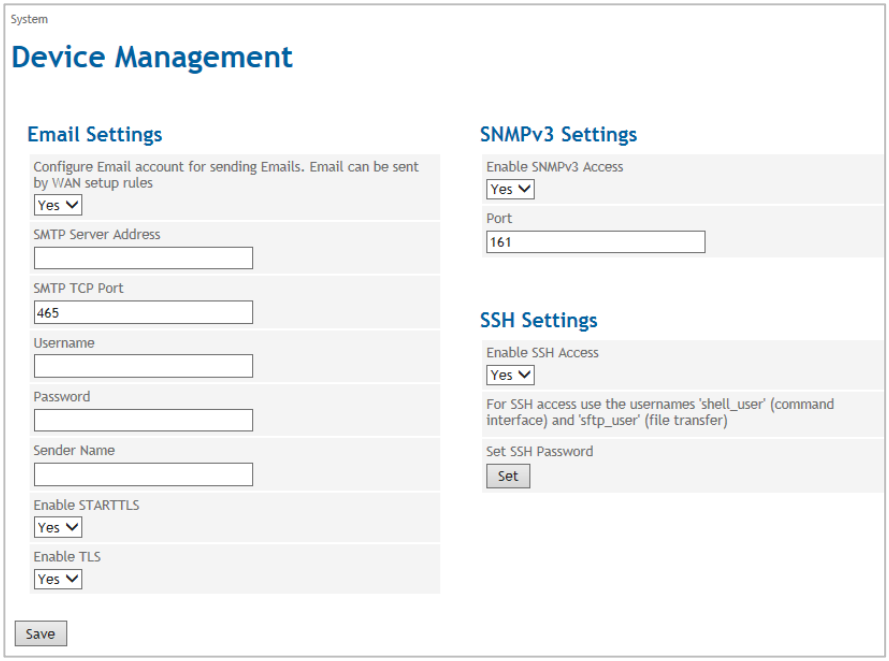


13.4 Device Management

Device Management

Click on the **System** tab and select "**Update**" to open the screen.





Email Settings

Configure an Email account

Set the function to "Yes" to be able to send emails from this device.

SMTP Server Address/ SMTP TCP Port

Enter the SMTP Server Address and the SMTP TC Port

Username/ Password

Enter a username and password for this email account.

Sender Name

Enter the name you intend to appear in the sender's field of the email.

Enable STARTTLS/ Enable TLS

Set to "Yes" to enable the configuration of the encryption via TLS (Transport Layer Security)

SNMPv3 Settings

Enable

To enable the SNMPv3 interface, select "Yes".

Port

Add the port number at which the SNMPv3 service should be accessible.

SSH Settings

Enable SSH Access

Set to “Yes”.

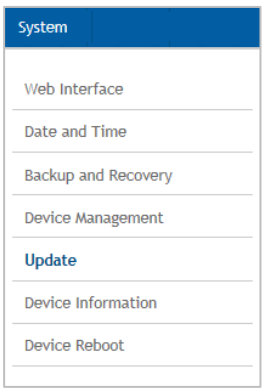
Set SSH Password

Enter a valid password for authentication.

For further information on how to configure conditions and rules on when to send emails see chapter 7.3

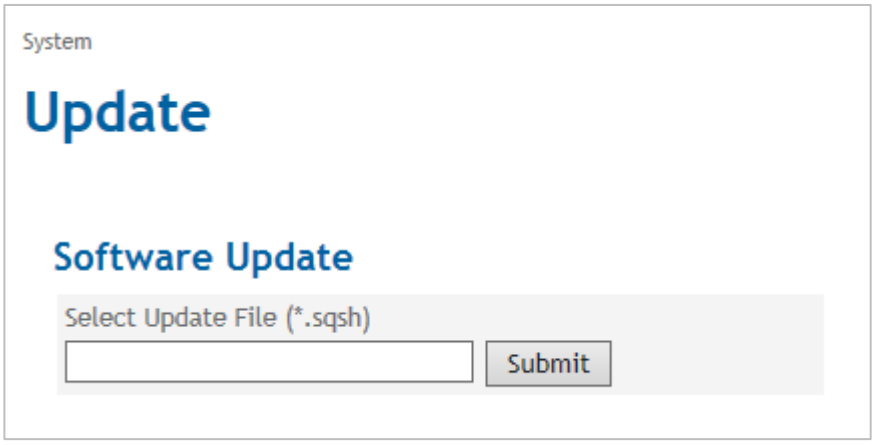
13.5 Perform Software Updates

Update



Software Update

Click on the **System** tab and select “**Update**” to open the screen.

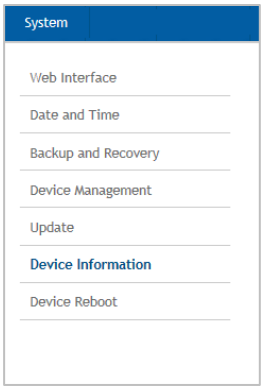


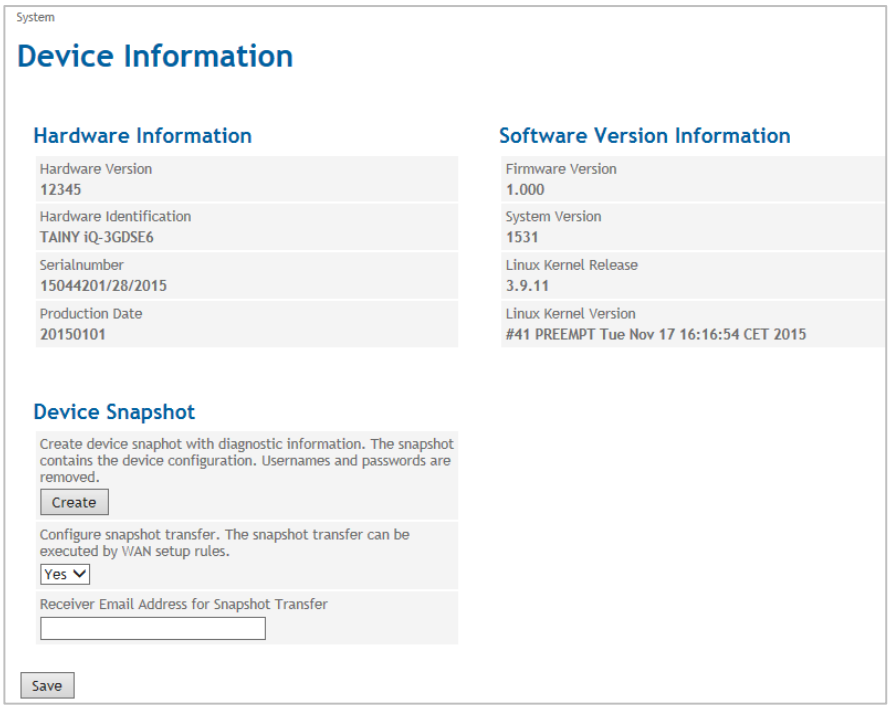
Click the “**Submit**” button to select and upload the required update file from the administration pc.

13.6 Retrieve Device Information

Device Information

Click on the **System** tab and select "**Device Information**" to open the screen.





Hardware Information/ Software Version Information

This screen displays information about the hardware and software versions of the TAINY iQ.

Device Snapshot

The Device Snapshots provides diagnostic information of TAINY iQ for debug purposes. It stores the information in a downloadable "tgz-file". Sensitive information such as usernames and passwords are not included.

The snapshot also contains the log files of the TAINY iQ.

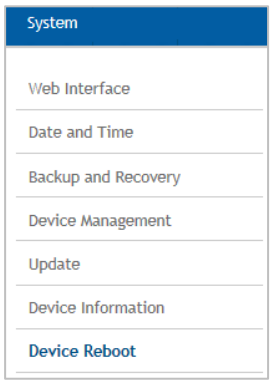
Click "**Create**" to take a snapshot.

Set the Configure Snapshot transfer to "Yes". Mind that the function email function has to be configured beforehand, see chapter Device Management

Enter the email address of receiver of the snapshot in the corresponding entry field.

13.7 Force a Reboot

Device Reboot



Click on the **`System`** tab and select "**`Device Reboot`**" to open the screen.

Click the "`Reboot`" button to force a new system start of the TAINY iQ.

14 Maintenance

14.1 Maintenance

All types of TAINY iQ are maintenance free.

14.2 Troubleshooting

In case you encounter any problems please refer to the table below for advice:

Problem	Cause	Solution
Control lamps are off	Power supply is cut off	Check the connection to the power supply
Device does not log in	Wrong PIN or APN	Check PIN or APN
	SIM card is not activated or in PUK status	Check activation and status
	SIM card is not activated for the selected service (UMTS, LTE)	Check activation and selected service
	Poor reception	Check positioning of antenna
No data-connection from local network to WAN possible	Default gateway configured wrongly in application	Check the gateway settings on the WAN tab
	GRE Tunnel set as default gateway yet no route set (this is also important for DNS, NTP, SNMP and Ping checks)	Check the GRE settings and gateway settings on the WAN tab
	Firewall is not open	Check the Firewall settings
No access from the local network to TAINY	Wrong VLAN parameters set	Check VLAN parameters on WAN and LAN tab
	Logged out by MAC filter	Check the filter settings for MAC
	Logged out by firewall	Check the filter settings for the firewall
IPsec Tunnel does not configure	Incorrect certificates and keys	Check the certificates and keys (Certificate tab)
	The encryption and hash methods do not match	Check the selected methods on the WAN tab
	The networks are not consistently (crisscross)	Check the networks
	Not all network devices and routers between the entities are configured correctly	Check the configuration of all devices and routers again

Problem	Cause	Solution
GRE tunnel does not configure	Not all devices and modems are configured correctly	Check for example the settings for the firewall an port forwarding-rules
	The IPsec encryption is not consistently activated or deactivated	Check the settings for IPsec on the WAN tab
	The encryption- and hash methods of the activated IPsec do not match	Check the IPsec settings on the WAN tab
The GRE tunnel does configure yet the communication between the local networks is not possible	Do both entities use RIPv2	Please check
	Do both entities support RIPv2	Please check
	If not, are the right routes set in both entities tunnels so the packets are routed through the right tunnels	Check the settings for IPsec tunnels on the WAN tab

15 Transport, Storage and Disposal

15.1 Transport

The TAINY iQ will be delivered in an individual box. Keep the packing for later transport purposes.

The TAINY iQ can be carried by public transportation:

Transportation by air, by road on all qualities of road surface, by ship and by train and where some care has been taken with respect to low temperatures.

Temperature range (transport) : -40°C … +70°C

Relative Humidity (transport) : max. 95%

The TAINY iQ must be carried either in its individual box or mounted on a top rail inside a cabinet.

When carried mounted on a top rail it must be ensured, that the TAINY iQ cannot slip along the top rail. The cabinet must be packed inside a layer of material (e.g. Styrofoam), which absorbs shocks and vibrations. The layer of material shall be appropriate to the mass of the cabinet.

15.2 Storage

Please always cut off the power supply before removal and storage. Disconnect all cables. Store the TAINY iQ in weather-protected, not temperature-controlled storage locations:

Temperature range (storage) : -20°C … +70°C

Relative Humidity (transport) : max. 95%

The TAINY iQ must be stored either in its individual box or mounted on a top rail inside a cabinet. The cabinet must be packed inside a layer of material (e.g. Styrofoam), which absorbs shocks and vibrations. The layer of material shall be appropriate to the mass of the cabinet.

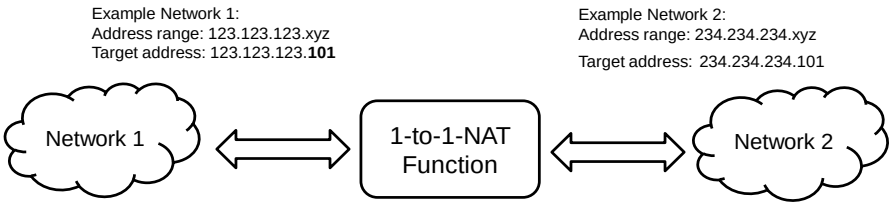
15.3 Disposal

Environmental Information for Customers in the European Union European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the manufacturer where you purchased the product.

16 Glossary

1-to-1 NAT

With 1-to-1 NAT, a network component (e.g. router) maps the address range of one network to the address range of another network.



A component in Network 1 addresses a component in Network 2 through a target address from the address range of Network 1. The 1-to-1 NAT function maps the target address in the address range of Network 2. In turn, responses from Network 2 are received by a sender address from Network 1.

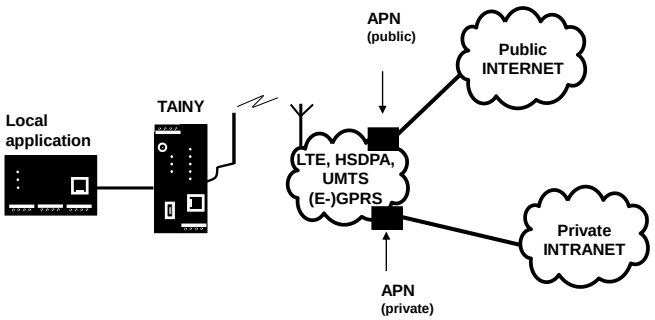
AES

Advanced Encryption Standard.

The NIST (National Institute of Standards and Technology) has developed the AES encryption standard in collaboration with industrial corporations for years. This → symmetric encryption should replace the previous DES standard. The AES standard specified three different key sizes with 128, 192 and 256 bit. In 1997 the NIST started an initiative for AES and revealed its conditions for the algorithm. From the proposed encryption algorithms the NIST narrowed the selection down to five algorithms: MARS, RC6, Rijndael, Serpent and Twofish. In October 2000 Rijndael was chosen as the encryption algorithm.

APN (Access Point Name)

Trans-network connections, e.g. from a wireless network (HSPA+, UMTS, EGPRS or GPRS) to the Internet, are created in the wireless network via so-called APNs.



An end device that wants/tries to establish a connection via the GPRS network specifies an APN to indicate which network it wants to be connected to: the Internet or a private company network that is connected via a dedicated line.

The APN designates the transfer point to the other network. It is communicated to the user by the network operator.

Asymmetric encryption

With asymmetric encryption, data is encrypted with a key and encrypted again with a second key. Both keys are suitable for encryption and decryption. One of the keys is kept secret by its owner (private key) and the other is given to the public (public key), potential communication partners.

A message encrypted with the public key can only be decrypted and read by a recipient who has the corresponding private key. A message encrypted with the private key can only be decrypted and read by any recipient who has the corresponding public key. Encryption with the private key shows that the message actually originated from the owner of the corresponding public key. For that reason, the term “digital signature” is used.

However, asymmetric encryption processes such as RSA are slow and susceptible to certain types of attacks, therefore they are often combined with a symmetric process (→ symmetric encryption). Furthermore concepts which eliminate the elaborate administrative efforts for symmetric keys are also possible.

Cell ID

Unique identifier of a cellular network cell.

CIDR

Classless Inter-Domain Routing

IP netmasks and CIDR are notations for grouping a number of IP addresses into an address space. Thus a range of contiguous addresses is treated as a network.

The CIDR method reduces, for example the routing tables stored in routers by means of a postfix in the IP address. This postfix can be used to designate a network together with its subnetworks. This method is described in RFC 1518.

In order to specify a range of IP addresses to the TAINY iQ, or when configuring the firewall, it may be necessary to specify the address space in the CIDR notation. The following table shows the IP netmask on the left-hand side and to the far right the corresponding CIDR notation.

CIDR (Table)

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

Client / Server

In a client-server environment a server is a program or computer that receives and answers queries from the client program or client computer.

With data communication the computer is also referred to as a client that establishes a connection to a server (or host). This means the client is the calling computer; the server (or host) is the callee.

CSQ / RSSI

The CSQ value is a value defined in the GSM standard to indicate the signal quality. CSQ values correspond to the received field strength RSSI (= Received Signal Strength Indication):

	RSSI
< 6	< -101 dBm
6..10	-101 dBm.. - 93 dBm
11..18	- 91 dBm.. -77 dBm
> 18	> -75 dBm
99	Not logged in

Datagram

With the transfer protocol TCP/IP, data is sent as data packages, so-called IP datagrams. An IP datagram has the following structure:

1. IP header
2. TCP/UDP header
3. Data (payload)

The IP address contains:

- the IP address of the sender (source IP address)
- the IP address of the recipient (destination IP address)
- the protocol number of the protocol of the next higher protocol layer (according to the OSI layer model)
- the IP header check sum (checksum) for verifying the integrity of the header on receipt.

The TCP/UDP header contains the following information:

- Port of the sender (source port)
- Port of the recipient (destination port)
- a check sum over the TCP header and some information from the IP header (including source and destination IP address)

DES / 3DES

The symmetric encryption algorithm (→ symmetric encryption) DES, originating from IBM and tested by the NSA, was established in 1977 by the American National Bureau of Standards, the predecessor of today's National Institute of Standards and Technology (NIST) as a standard for American governmental institutions. Since it was the first standardised encryption algorithm, it was also quickly adopted in industrial applications in the US and beyond.

DES works with a key length of 56bit, which can no longer be considered to be secure due to the increase in computing capability of the computer since 1977.

3DES is a variant of DES. It works with keys three times the size, they are 168 bits long. It is still considered to be secure and is also a part of the IPsec standard, among other things.

DHCP

Dynamic Host Configuration Protocol (DHCP) assumes the automatic dynamic assignment of IP addresses and additional parameters in a network. The Dynamic Host Configuration Protocol uses UDP. It was defined in RFC 2131 and assigned with the UDP ports 67 and 68. DHCP works in the client – server method, wherein the client is assigned the IP address by the server.

DNS

The addressing in IP networks takes place over IP address as a basic rule. However, addressing in the form of a domain address is generally preferred (in the form www.abc.xyz.de). The addressing takes place over the domain address. First the sender sends the domain address to a Domain Name Server (DNS) and receives the corresponding IP address. Only afterwards does the sender address its data to this address.

DPD

The Dead Peer Detection (DPD) identifies whether the IPsec connection between two networks is still valid or if the connection has to be re-established. This function presumes though that it is supported on both sides. Without DPD depending on the configuration the connection has to be manually re-established or the lifetime of the SA has to elapse. To control if the IPsec connection is still valid the DPD sends a DPD-request to the opposite party. If no answer is received the IPsec connection will be interrupted after a number of failed attempts.

DynDNS provider

Also *Dynamic DNS provider*. Every computer that is connected to the internet has an IP address (IP = Internet Protocol). An IP address consists of up to 4 four three-digit numbers, with dots separating each of the numbers. If the computer is online via the telephone line via modem, ISDN or ADSL, then the internet service provider dynamically assigns it an IP address, i.e. the address changes from session to session. Even if the computer is online for more than 24 hours without interruption (e.g. in the case of a flat rate), the IP address is changed periodically.

For a local computer to be accessible via the internet, its address must be known to the external remote station. This is necessary for it to establish a connection to the local computer. This is not possible, however, if the address of the local computer constantly changes. It is possible, however, if the user of the local computer has an account with a DynamicDNS provider (DNS = Domain Name Server).

Then he can specify a host name, under which the computer can be accessed in the future, e.g.: www.xyz.abc.de. Moreover, the DynamicDNS provider makes a small program available that has to be installed and executed on the computer concerned. In each internet session of the local computer this tool reports to the DynamicDNS provider which IP address the computer obtains at the moment. Its domain name server registers the current host name - IP address assignment and reports it to other domain name servers on the internet.

If now an external computer tries to establish a connection with a local computer which is registered with the DynamicDNS provider, the external computer uses the host name of the local computer as the address. This way a connection is established with the responsible DNS (Domain Name Server) to look up the IP address which is currently assigned to this host name. The IP address is transmitted back to the external computer, and then used by it as the destination address. It now leads precisely to the desired local computer.

As a rule, all internet addresses are based on the following method: First a connection is established to a DNS to determine the IP addresses assigned to this host name. Once that has been accomplished, the IP address that was sought after is used to establish the connection to the desired remote station, which could be any Web site.

EDGE

EDGE (= Enhanced Data Rates for GSM Evolution) refers to a method by which the available data rates in GSM mobile phone networks are increased by introducing an additional modulation process. EDGE, GPRS is expanded to become EGPRS (Enhanced GPRS), and HSCSD is expanded to become ECSD.

EGPRS

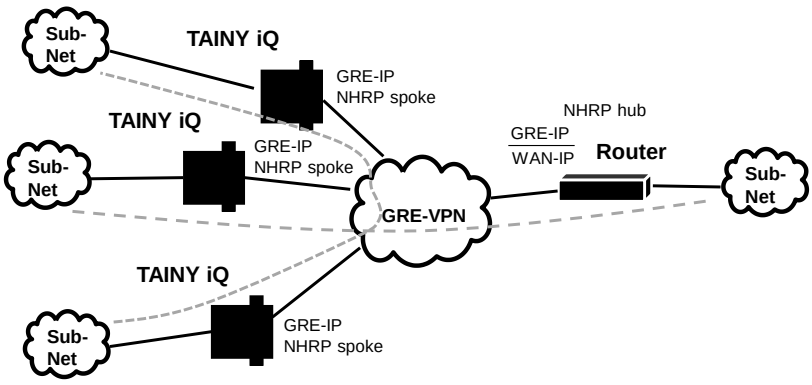
EGPRS stands for "Enhanced General Packet Radio Service", describes a packet-oriented data service based on GPRS, which is accelerated by EDGE technology.

GPRS

GPRS is the abbreviation for "General Packet Radio Service" and a data transfer system of GSM2+ mobile radio systems. GPRS systems use the base station of the GSM network for the radio technology and an internal infrastructure for the networking and coupling to other IP networks, such as the internet. In the process, data is communicated packet-oriented, wherein the internet protocol (IP) is used. GPRS provides data rates of up to 115.2 KBit/s.

GRE

Via the TAINY iQ independent (sub-) networks can be connected. For that purpose the TAINY iQ uses the GRE (=Generic Routing Encapsulation) protocol (RFC 1701; RFC 1702; RFC 2784).



The (sub-) networks require a GRE-capable router (e.g. the TAINY iQ), to create a DM VPN among themselves.

From one (sub-) network an address of another (Sub-) network can be directly addressed provided a corresponding route is configured.

As the GRE protocol establishes 1:1 tunnels between endpoints only, the DM VPN is organized like a NBMA (=Nonbroadcast Multiple Access) network. Inside this virtual network, data are transmitted directly from endpoint to endpoint or across a switching device.

By using the NHRP (=Next Hop Resolution Protocol) the addresses of the endpoints (NHRP spokes) are collected at one endpoint acting as a NHRP hub, which shares this information on request.

In a DM VPN one GRE endpoint (e.g. the router of the central site) must operate in hub mode, while other GRE endpoints (e.g. TAINY iQ) operates in spoke mode.

All spokes in the DM VPN must know the WAN IP address as well as the DM VPN IP address of the hub.

If the hub receives data, which is not addressed to its own directly connected (sub-) network, it either forwards the data to the addressed endpoint in the DM VPN or the hub informs the sender, how to contact the addressed endpoint directly.

The GRE protocol does cover neither authentication nor encryption. This can be done by an additional IPsec layer.

GSM

GSM (= Global System for Mobile Communication) is a worldwide standard for digital mobile radio networks. In addition to the voice service for telephony, GSM supports various data services, such as fax, SMS, CSD and GPRS. Depending on legal regulations in various countries, the frequency bands 900 MHz, 1800 MHz or 850 MHz and 1900 MHz are used.

HSPDA, HSUPA (HSPA+)

HSDPA (=High Speed Downlink Packet Access) and HSUPA (=High Speed Upload Packet Access) are extensions of the UMTS network, which provides higher data rates from the base station to the mobile station (HSDPA) or from the mobile station to the base station (HSUPA).

HTTPS

HTTPS (=Hyper Text Transfer Protocol Secure) is a variant of the familiar HTTP, which is used by any web browser for navigation and data exchange in the Internet. For example, this familiar entry: http://www.neuhaus.de.

In HTTPS the original protocol is supplemented with an additional component for data protection. While in HTTP data are transmitted unprotected in plain text, in HTTPS data are transmitted only after an exchange of digital certificates, and in encrypted form.

ICCID

The ICCID (=Integrated Circuit Card Identifier) identifies each SIM internationally. A full ICCID may have 19 or 20 characters

It includes a country code, an issuer code, the SIM number as well as checksum data.

IMEI

The IMEI (=International Mobile Equipment Identity) is a unique 15-digit serial number of a GSM or UMTS terminal device.

IMSI

The IMSI (=International Mobile Subscriber Identity) is an identifier stored on the SIM card and used to identify the subscriber. An IMSI is usually presented as a 15 digit long number, but could be shorter.

Intranet

An intranet is a private IP network varying in size. For example, the IP network of a company is an intranet, as is also several networked private computers.

The internet, on the other hand, is a public network. Intranet and internet should only be connected to each other over protective devices, such as a firewall.

IP address

Each host or router on the internet/intranet has a unique IP address (IP = internet protocol). The IP address is 32 bits (= 4 bytes) long and is written as 4 number digits (in the range 0 to 255 in each case), which are separated from each other by a period.

An IP address is comprised of two parts: the network address and the host address.

All hosts of a network have the same network address, but different host addresses. Depending on the size of the respective network - varying between networks of the categories class A, B and C - both address parts vary in size:

<table>
<tr><th></th><th>1st byte</th><th>2nd byte</th><th>3rd byte</th><th>4 byte</th></tr>
<tr><td>Class A</td><td>Network add.</td><td colspan="3">Host add.</td></tr>
<tr><td>Class B</td><td colspan="2">Network add.</td><td colspan="2">Host add.</td></tr>
<tr><td>Class C</td><td colspan="3">Network add.</td><td>Host add.</td></tr>
</table>

The first byte of the IP address indicates whether an IP address refers to a device in a network of the category Class A, B or C. The following are defined:

	Value of the 1st byte	Bytes for the network address	Bytes for the host address
Class A	1-126	1	3
Class B	128-191	2	2
Class C	192-223	3	1

In terms of figures, there can only be a maximum of 126 Class A networks in the world; each of these networks can comprise a maximum of 256 x 256 x 256 hosts (address space 3 bytes). There can be a maximum of 64 x 256 Class B networks and each can contain up to 65,536 hosts (address space 2 bytes: 256 x 256). There can be a maximum of 32 x 256 x 256 Class B networks and each can contain up to 256 hosts (address space 1 byte).

IP packet

See Datagram

IPsec

IP security (IPsec) is a standard which uses IP datagrams to ensure the authenticity of the sender as well as the confidentiality and the integrity of the data through encryption. The components of IPsec are the authentication header (AH), the encapsulating security payload (ESP), the security association (SA), the security parameter index (SPI) and the internet key exchanges (IKE).

At the beginning of the communication, the computers participating in the communication clarify the process used as well as its implications, such as transport mode or tunnel mode.

In transport mode, an IPsec header is used between the IP header and TCP or UDP header in each IP datagram. Since the IP header remains unchanged in the process, this mode is only suitable for a host-to-host connection.

In tunnel mode, an IPsec header and a new IP header precede the entire IP datagram. That means the original datagram is encrypted in the payload of the new datagram.

The tunnel mode is used with the VPN: The devices at the tunnel ends encrypt and decrypt the datagrams along the stretch of the tunnel; in a nutshell, the actual datagrams are fully protected along the transport route through the public network.

Location Area Code (LAC),

A location area is a group of adjacent GSM base stations connected to each other in order to facilitate the finding and call signalling for a GSM end device, i.e. the CM-E1P01-GPRS module. The group can comprise between 10 and 100 GSM base stations. Each of these groups has a unique worldwide identifier (Location Area Code = LAC)

Long Term Evolution (LTE)

LTE is the 4th generation of mobile radio network, which allows a significant higher data transmission rate, than the 3nd generation UMTS. It is possible to download up to 300 MB per second. The frequency range used by LTE-providers is solely on UHF-frequency band. Multiple frequencies are used varying regionally between the middle and upper section of the UHF-range from 700 to 2600 MHz

MCC/MNC

The MCC (Mobile Country Code) and the MNC (Mobile Network Code) are unique worldwide identifiers for a mobile radio network.

The MCC is three-digit and the MNC are two- or three-digit long.

There are many websites on the internet with the MCC/MNC of various countries and network operators.

MIB

See SNMP

NAT (Network Address Translation)

With network address translation (NAT), often called IP masquerading, an entire network is "hidden" behind a single device, known as the NAT router. The internal computers of the local network remain concealed with their IP addresses in the local network when they communicate outwardly through the NAT router. Only the NAT router with its own IP address is visible to outside communication partners.

However, in order for internal computers to be able to communicate directly with external computers (on the internet), the NAT router must change the IP datagrams to and from the internal computer to the outside.

If an IP datagram is sent from the internal network to the outside, the NAT router changes the IP and TCP header of the datagram. It switches the source IP address and the source port with its own official IP address and its own, previously unused port. For this purpose, it maintains a table which establishes the allocation of the original with the new values.

Upon receipt of a response datagram, the NAT router recognises that the datagram is actually intended for an internal computer on the basis of the specified target port. Using the table, the NAT router exchanges the target IP address and the target port and forwards the datagram to the internal network.

Network mask / Subnet mask

A company network with access to the internet is normally officially assigned only to a single IP address, e.g. 134.76.0.0. In this example address it can be seen from the 1st byte that this company network is a Class B network, i.e. the last 2 bytes can be used freely for host addressing. Arithmetically that represents an address space of 65,536 possible hosts (256 x 256).

Such a huge network is not very practical. In this case it is necessary to form subnetworks. This is accomplished by using a subnet mask. Like an IP address, this is a 4 bytes long field. The value 255 is assigned to each of the bytes that represent the network address. The main purpose is to "hide" a part of the host address range in order to use it for the addressing of subnetworks. For example, in a Class B network (2 bytes for the network address, 2 bytes for the host address), by means of the subnet mask 255.255.255.0 it is possible to take the 3rd byte, which was actually intended for host addressing, and use it now for subnet addressing. Arithmetically that means that 256 subnets with 256 hosts each could be created.

Packet Filter

Packet filtering is a method of a stateful inspection firewall. Packet filters only let IP packets pass through if this has been defined previously by firewall rules. The following are defined in the firewall rules:

- which protocol (TCP, UDP, ICMP) can go through,
- the permitted source of the IP packets (From IP / From port)
- the permitted destination of the IP packets (To IP / To port)

It is likewise defined here how IP packets are handled that are not allowed to pass through (discard, reject).

For a simple packet filter it is always necessary to create two firewall rules for a connection:

- one rule for the query direction from the source to the destination, and
- a second rule for the query direction from the destination to the source.

It is different for stateful inspection firewall. In this case a firewall rule is only created for the query direction from the source to the destination. The firewall rule for the response direction from the destination to the source results from analysis of the data previously sent. The firewall rule for the responses is closed again after the responses are received or after a short time period has elapsed. Thus responses can only pass through if there was a previous query. This means that the response rule cannot be used for unauthorised access. What is more, special procedures make it possible for UDP and ICMP data to also go through, even though these data were not requested before.

Port Forwarding

If a firewall rule has been created for port forwarding, then data packets received at a defined IP port of the firewall device from the external network will be forwarded. The incoming data packets are then forwarded to a specified IP address and port number in the local network. The port forwarding can be configured for TCP or UDP.

In port forwarding the following occurs: The header of incoming data packets from the external network that are addressed to the external IP address of the firewall device and to a specific port are adapted so that they are forwarded to the internal network to a specific computer and to a specific port of that computer.
This means that the IP address and port number in the header of incoming data packets are modified.

This process is also called Destination NAT or Port Forwarding.

Port number

The port number field is a field of 2-bytes in UDP and TCP headers. The assignment of port numbers serves for identification of the various data streams, which the UDP/TCP process simultaneously. The entire data exchange between UDP/TCP and the application processes takes place over these port numbers. The assignment of port numbers to the application processes take place dynamically and randomly. For specific, frequently used application processes, fixed port numbers are assigned. They are referred to as Assigned Numbers.

PPPoE

Acronym for Point-to-Point Protocol over Ethernet. It is based on the standards PPP and Ethernet. PPPoE is a specification for connecting users to the internet via ethernet using a jointly used broadband medium such as DSL, Wireless LAN or cable modem.

PPTP

Acronym for Point-to-Point Tunnelling Protocol. This protocol was developed by Microsoft, U.S. Robotics and others in order to transmit data securely between two VPN nodes (→ VPN) over a public network.

Private key, public key; certification (X.509)

Two keys are used with asymmetric encryption algorithms: one private (*private key*) and one public (*public key*). The public key is used for the encryption of data and the private key is used for the decryption.

The public key is provided by the future recipient of data to those who encrypt and send data to the recipient. Only the recipient has the private key. It is used for the decryption of the data received.

Certification:

The possibility of certification exists. Therefore the user of the public key (used for encryption) can be certain that the public key really originated from the party who was intended to receive the data to be sent: a certification authority (*CA*) checks the authenticity of the public key and the associated linking of the sender's identity with its key. This is conducted according to the CA's rules, which may require the sender to appear in person. After a successful check, the CA signs the public key of the sender with its (digital) signature. A *certificate* is created.

X.509 certificate establishes a link between an identity in the form of an "X.500 distinguished name" (DN) and an official key, which is certified with the digital signature of an X.509 certification authority (CA). The signature (an encryption with the signature key) can be checked by the public key which the CA issues to the certificate holder.

Protocol, transfer protocol

Devices that communicate with each other must use the same set of rules for this purpose. They must "speak the same language". Such rules and standards are referred to as protocol or transfer protocol. Protocols which are often used include IP, TCP, PPP, HTTP or SMTP. TCP/IP is an umbrella term for all protocols building on IP.

RIPv2

The RIP (Routing Information Protocol) is a routing protocol which is used to generate automatically routing tables of routers. Routers with activated RIPv2-Protocol transmit periodically their routing tables to configured RIP neighbours. A router knows at start only the directly connected networks. Therefore a new router asks all RIP neighbours for their complete routing tables. The answers are used to generate first entries in the own routing table. Afterwards the generated routing table is transmitted to all RIP neighbours.

Service provider

Supplier, company or institutions that offer users access to the internet or to an online service.

SNMP

SNMP (Simple Network Management Protocol) is a widespread mechanism for to control network components such as servers, routers, switches, printers, computers etc. centralized

SNMP defines the communication process and structure of the data packages. UDP via IP is used for transport.

SNMP does not define the values which can be read or changed.

This is done in an MIB (Management Information Base). The MIB is a description file in which the individual values are listed in a table. The MIB is for specific network components or for a class of components, such as switches.

SNMP Trap

SNMP trap is a message which is sent unprompted by the SNMP agent (Simple Network Management Protocol) from a network component.

Spoofing, Anti-Spoofing

In internet terminology, spoofing means to specify a forged address. The forged Internet address is used to pose as an authorised user.

Anti-spoofing means mechanisms to reveal or prevent spoofing.

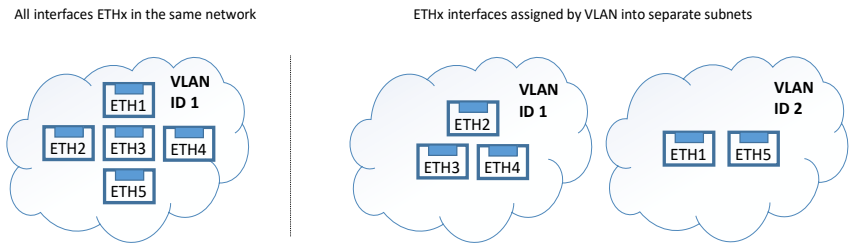
SSH	SSH (Secure SHell) is a protocol that enables secure, encrypted data exchange between computers. Secure SHell is used for remote access to the input console from LINUX-based machines.
Symmetric encryption	With symmetric encryption, data is encrypted and decrypted with the same key. DES and AES are two examples of symmetric encryption algorithms. They are fast, but time-consuming to administer as the number of users increases.
TACACS+	TACACS+ (**T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem Plus) is a standardised protocol, which is used for communication between clients and servers within a network in the areas authentication, authorization and accounting (billing). Like the TAINY iQ, a TACACS+ server can be set up, for example, which manages the access data for all end devices in the network centrally and carries out the authorization for the relevant interested party on behalf of the end devices when registration requests are received. The end device forwards the received registration data to the TACACS+ server, which carries out the necessary checks for the authorization and reports the result of the checks back to the end device.
TCP/IP (Transmission Control Protocol/Internet Protocol)	Network protocols that are used for the connection of two computers over the internet. IP is the base protocol. UDP builds on IP and sends individual packages. These could arrive at the recipient in a different sequence than they were sent, or they could even be lost. TCP serves for securing the connection and ensures, for example, that data packages are forwarded in the correct sequence. UDP and TCP additionally provide port numbers between 1 and 65535 for the IP address, through which the various services can be differentiated. A series of additional protocols build on UDP and TCP, such as HTTP (Hyper Text Transfer Protocol), HTTPS (Secure Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol, Version 3) and DNS (Domain Name Service). ICMP builds on IP and contains control messages. SMTP is an email protocol based on TCP. IKE is an IPsec protocol based on UDP. ESP is an IPsec protocol based on IP. On a Windows PC, WINSOCK.DLL (or WSOCK32.DLL) assumes the development of the two protocols. (see also datagram)
UDP	See TCP/IP
UMTS	UMTS (Universal Mobile Telecommunication System) is a 3rd generation mobile radio network, which allows significant higher data transmission rates, than the 2nd generation GSM networks. UMTS provides beside voice connections also IP-based data connections, SMS transmission and high speed data application like video. Apart from North America UMTS uses a frequency band at 2100 MHz. In North America the frequency bands at 850 MHz and 1900 MHz are used, which are also used for GSM networks.

VLAN

The VLAN function (Virtual Local Area Network) facilitates splitting the LAN interfaces of the TAINY iQ into different, independent virtual networks. Local applications, which are connected to LAN interfaces with identical VLAN ID, can communicate via the TAINY iQ among each other. If the VLAN IDs are different, a communication among one another is not possible.

The separation in VLANs is made by additional tags (marks) to the data packets, which indicates that the data packet belongs to a certain VLAN.

Depending on the configuration, the tags will be removed. Accordingly the data packets leaves the TAINY iQ with or without tags. If the tags are not removed, a connected external application which supports VLAN protocol (802.1Q) can be included in the VLAN.



VPN (Virtual Private Network)

A virtual private network (VPN) connects several physically separate private networks (subnetworks) through a public network, such as the internet to form a common network. The use of cryptographic protocols ensures confidentiality and authenticity. A VPN offers an affordable alternative to standard lines for creating a supraregional company network.

X.509 certificate

A type of "seal" which verifies the authenticity of the public key (→ asymmetric encryption) and corresponding data.

The possibility of certification exists so that the user of the public key (used for encryption) can be certain that the public key really originates from its actual originator and thus from the party who was intended to receive the data to be sent. A certification authority (CA) checks the authenticity of the public key and the associated linking of the originator's identity with its key. This takes place according to the CA's rules, which may require the originator of the public key to appear in person. After a successful check, the CA signs the public key with its (digital) signature. A certificate is created.

X.509 (v3) certificate thus contains a public key, information about the owner of the key (specified by distinguished name [DN]), allowed purposes of use, etc. and the signature of the CA.

The signature is created as follows: The CA creates an individual bit sequence up to 160 bits long known as the HASH value from the public key's bit sequence, the data on its owner and from additional data. The CA encrypts this with its private key and adds the certificate. Encryption with the CA's private key verifies authenticity, meaning that the encrypted HASH character sequence is the CA's digital signature. If the data of the certificate appears to have been manipulated, this HASH value will no longer be correct and the certificate will be worthless.

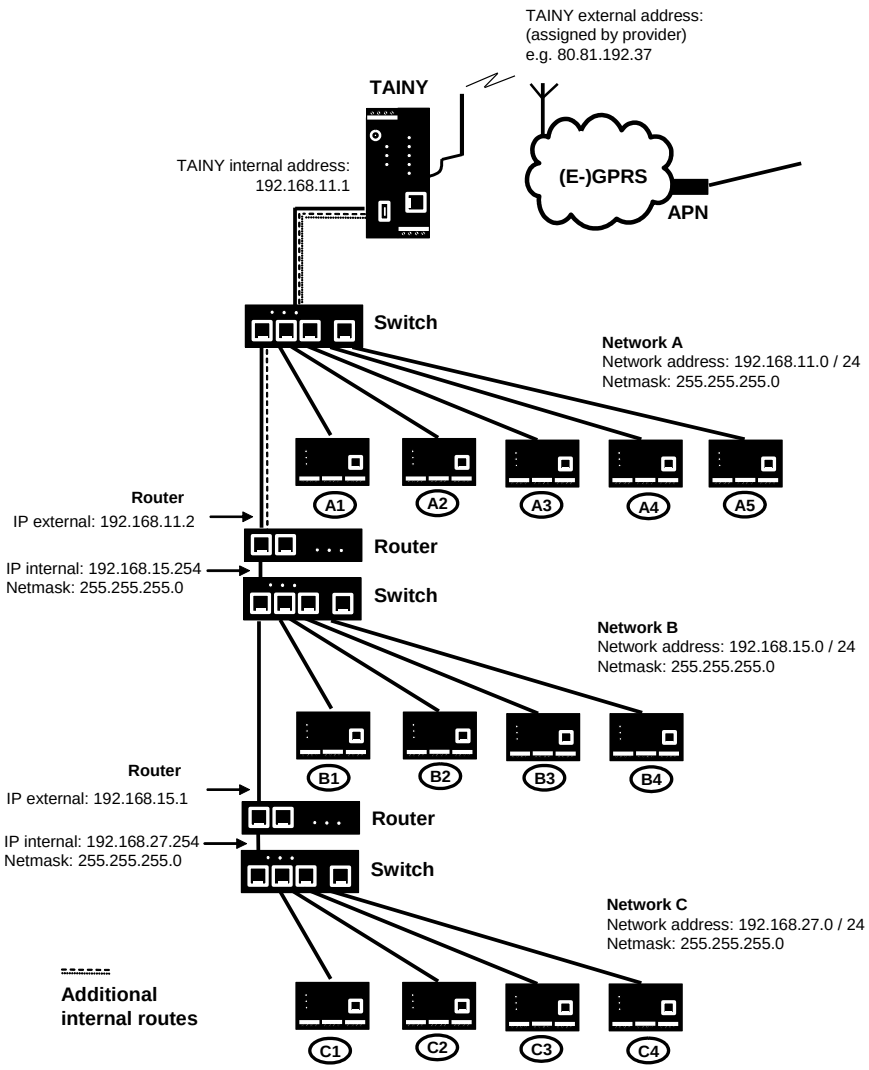
The HASH value is also referred to as a fingerprint. Since it is encrypted with the CA's private key, anyone who has the appropriate public key can encrypt the bit sequence and thus check the authenticity of this fingerprint or this signature.

By using the services of authentication authorities, it is possible that one key owner need not know the other, only the authentication authority. The additional information for the key also simplifies the administrative efforts for the key.

X.509 certificates are used for email encryption, etc. using S/MIME or IPsec.

Additional Internal Routes

The following sketch shows how the IP addresses could be distributed in a local network with subnetworks as well as the kind of network addresses resulting from this, and how the specification for an additional internal route could look like.



Network A is connected to the TAINY iQ and via it to a remote network. Additional internal routes show the path to additional networks (networks B, C), which are connected to each other via gateways (routers). For the TAINY iQ, in the example shown networks B and C can both be reached via gateway 192.168.11.2 and network address 192.168.11.0/24.

17 Technical data

Wired Interfaces	Ethernet (LAN)	5 x 10/100 Base-T (RJ45 plug), Ethernet IEEE802, 10/100 Mbit/s, cross-over or one-to-one, auto-negotiation
	Ethernet (LAN/WAN)	5 x 10/100 Base-T (RJ45 plug), Ethernet IEEE802, 10/100 Mbit/s, cross-over or one-to-one, auto-negotiation
Wireless connection	Frequency bands	*TAINY iQ 4GDSE-2 / TAINY iQ 4GDSE-6:* GSM/GPRS/ EDGE: 900 MHz, 1800 MHz UMTS/ HSPA+: 900 MHz (BdVIII), 1800 MHz (BdIII)* 2100 MHz (BdI) LTE: 800 MHz (Bd20), 900 MHz (Bd8) 1800 MHz (Bd3), 2100 MHz (Bd1) 2600 MHz (Bd7), * Not for use in the EU. *TAINY iQ 3GDSE-2 / TAINY iQ 3GDSE-6* GSM/GPRS/ EDGE: 850 MHz*, 900 MHz, 1800 MHz, 1900 MHz* UMTS/ HSPA+: 800 MHz (BdVI)*, 850 MHz (BdV)*, 900 MHz (BdVIII), 1900 MHz (BdII)*, 2100 MHz (BdI) * Not for use in the EU.
	Max. Transmit Power	*TAINY iQ 4GDSE-2 / TAINY iQ 4GDSE-6:* Class 4 (+33dBm ±2dB) für EGSM900 Class 1 (+30dBm ±2dB) für GSM1800 Class E2 (+27dBm ± 3dB) für GSM 900 8-PSK Class E2 (+26dBm +3 /-4dB) für GSM 1800 8-PSK Class 3 (+24dBm +1/-3dB) für UMTS 2100, FDD BdI Class 3 (+24dBm +1/-3dB) für UMTS 1800, FDD BdIII* Class 3 (+24dBm +1/-3dB) für UMTS 900, FDD BdVIII Class 3 (+23dBm +-2dB) für LTE 2600, LTE FDD Bd7 Class 3 (+23dBm +-2dB) für LTE 2100, LTE FDD Bd1 Class 3 (+23dBm +-2dB) für LTE 1800, LTE FDD Bd3 Class 3 (+23dBm +-2dB) für LTE 900, LTE FDD Bd8 Class 3 (+23dBm +-2dB) für LTE 800, LTE FDD Bd20 * Not for use in the EU.

		TAINY iQ 3GDSE-2 / TAINY iQ 3GDSE-6 Class 4 (+33dBm ±2dB) for EGSM850 Class 4 (+33dBm ±2dB) for EGSM900 Class 1 (+30dBm ±2dB) for GSM1800 Class 1 (+30dBm ±2dB) for GSM1900 Class E2 (+27dBm ± 3dB) for GSM 850 8-PSK Class E2 (+27dBm ± 3dB) for GSM 900 8-PSK Class E2 (+26dBm +3 /-4dB) for GSM 1800 8-PSK Class E2 (+26dBm +3 /-4dB) for GSM 1900 8-PSK Class 3 (+24dBm +1/-3dB) for UMTS 2100, FDD BdI Class 3 (+24dBm +1/-3dB) for UMTS 1900, FDD BdII* Class 3 (+24dBm +1/-3dB) for UMTS 900, FDD BdVIII Class 3 (+24dBm +1/-3dB) for UMTS 850, FDD BdV* Class 3 (+24dBm +1/-3dB) for UMTS 800, FDD BdVI* * Not for use in the EU.	
	HSPA+	HSDPA Cat. 10 / HSUPA Cat.6 data rates DL: max. 14.4 Mbps, UL: max. 5.76 Mbps	
	EDGE (EGPRS)	EDGE class 12 data rates: DL: max. 237 kbps, UL: max. 237 kbps	
	GPRS	GPRS class 12 data rates DL: max. 85.6 kbps, UL: max. 85.6 kbps	
	Antenna connection	SMA jack; nominal impedance: 50 ohms	
Security functions	VPN	Dynamic Multipoint VPN IPsec	
	Firewall	Stateful inspection firewall Anti-spoofing Port forwarding Traffic Priority MAC Table	
Additional functions		VLAN, PPPoE, DNS cache, DHCP server, NTP, Connection check, TACACS+, Spanning Tree,	
Management		Web-based administration user interface SNMPv3, Logbook, Snapshot	
Ambient conditions	Temperature range	Operation: -25 °C to +70 °C *) Storage: -40 °C to +85 °C *) Automatic shut-down of the radio module in case of reaching a critical temperature.	
	Air humidity	0-95 %, non-condensing	
Power Supply	TAINY iQ 4GDSE-6	U (nominal)	12-42 VDC
		I (nominal)	Irms: 590-185 mA; Imax:645 mA
	TAINY iQ 3GDSE-6	U (nominal)	12-42 VDC
		I (nominal)	Irms: 590-185 mA; Imax:645 mA

	TAINY iQ 4GDSE-2	U (nominal)	12-42 VDC
		I (nominal)	Irms: 550-165 mA; Imax:630 mA
	TAINY iQ 3GDSE-2	U (nominal)	12-42 VDC
		I (nominal)	Irms: 550-165 mA; Imax:630 mA
Housing	Design	Top-hat rail housing	
	Material	Plastic	
	Protection class	IP20	
	Dimensions	114,5 mm x 45 mm x 99 mm (d x w xh) *Type 4GDSE2/3GDSE2*	
		114,5 mm x 68 mm x 99 mm (d x w x h) *Type 4GDSE6/3GDSE6*	
	Weight	ca. 250g *Type 4GDSE2/3GDSE2* ca. 340g *Type 4GDSE6/3GDSE6*	
Electrical Safety	Standard	EN 60950-1	
	Classification	Protection class 2, Pollution degree 2, Overvoltage Category 2	
Compliance	CE mark	The devices meet when used as intended the directive 2014/53/EU (RED). The devices meet the 2011/65/EU (ROHS). The CE Declaration of Conformity can be found at www.neuhaus.de www.sagemcom.com, or contact our customer service.	
	Radio	EN 301 511 [v.9.0.2] incl. section 4.2.26 EN 301 908-1 [v.11.1.1] EN 301 908-2 [v.11.1.1] EN 301 908-13 [v.11.1.1] *(TAINY iQ 4GDSE-2/-6 only)*	
	EMC/ESD	EN 301 489-1 [v.1.9.2] Draft EN 301 489-52 [v.1.1.0] EN 61000-6-2 / AC [2005 / 2005]	
	Safety & Health	EN 60950-1 / A11 / A1 / A12 / AC / A2 [2006 / 2009 / 2010 / 2011 / 2011 / 2013] EN 62479 [2010] Protection class 2, Pollution degree 2, Overvoltage category 2	
	Environment	ROHS (EN 50581 [2012]) WEEE	
	Radio Module	GCF and PTCRB certified	

18 Simplified EU Declaration of Conformity

Simplified EU Declaration of Conformity

Hereby, Sagemcom Dr. Neuhaus GmbH declares that the radio equipment:

- TAINY iQ 3GDSE-2,
- TAINY iQ 3GDSE-6,
- TAINY iQ 4GDSE-2,
- TAINY iQ 4GDSE-6

are in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address:

www.neuhaus.de

www.sagemcom.com