Industriefunkuhren

hopf

Elektronik GmbH

Technical Manual

GPS - NTP Time Server with LAN Interface

Model 8029NTS-V2/GPS

For DIN Rail Installation
(DIN EN 60715 TH35)

ENGLISH

Version: 08.02 – 15.06.2021

	SET	IMAGE (8029)	FIRMWARE (8024)
Valid for	Version: **08.xx**	Version: **08.xx**	Version: **01.xx**

Version Numbers (Firmware / Description)

The Term **SET** defines the fixed relationship between the Image Version and the associated H8 Firmware Version.

the first two Digits of the Technical Description Version Number, the **SET** Version and the Image Version **Must Be The Same**! They designate the shared functional Identity between Device, Software and Technical Description.

The Version Number of the Image and the H8 Software can be read in the WebGUI of Time Server 8029NTS/GPS (see ***Chapter 7.3.5.1 Device Information*** and ***Chapter 7.3.5.2 Hardware Information)***.

The two Digits after the Dot in the Version Number designates Corrections to the Firmware and/or Description which have no Effect on Functionality.

Downloading Technical Manuals

All current manuals of our products are available free of charge via our homepage on the Internet.

Homepage:	http://www.hopf.com
E-mail:	info@hopf.com

Symbols and Characters

⚠ **Operational Reliability**

Disregard may cause damages to persons or material.

❗ **Functionality**

Disregard may impact function of system/device.

ℹ **Information**

Notes and Information.

Safety regulations

The safety regulations and observance of the technical data serve to ensure trouble-free operation of the device and protection of persons and material. It is therefore of utmost importance to observe and compliance with these regulations.

If these are not complied with, then no claims may be made under the terms of the warranty. No liability will be assumed for any ensuing damage.

Safety of the device

This device has been manufactured in accordance with the latest technological standards and approved safety regulations

The device should only be put into operation by trained and qualified staff. Care must be taken that all cable connections are laid and fixed in position correctly. The device should only be operated with the voltage supply indicated on the identification label.

The device should only be operated by qualified staff or employees who have received specific instruction.

If a device must be opened for repair, this should only be carried out by employees with appropriate qualifications or by ***hopf*** Elektronik GmbH.

Before a device is opened or a fuse is changed all power supplies must be disconnected.

If there are reasons to believe that the operational safety can no longer be guaranteed the device must be taken out of service and labelled accordingly.

The safety may be impaired when the device does not operate properly or if it is obviously damaged.

CE-Conformity

This device fulfils the requirements of the EU directive 2014/30/EU "Electromagnetic Compatibility" and 2014/35/EU "Low Voltage Equipment".

Therefore the device bears the CE identification marking
(CE = Communautés Européennes = European communities)

The CE indicates to the controlling bodies that the product complies with the requirements of the EU directive - especially with regard to protection of health and safety for the operator and the user - and may be released for sale within the common markets.

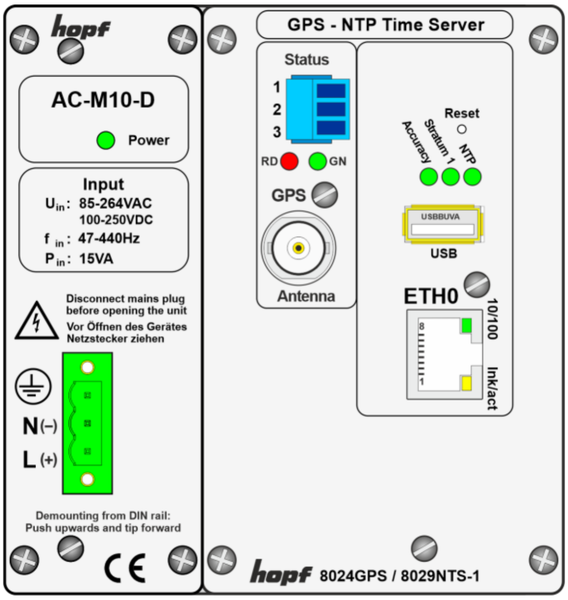
Contents Page

1 GPS - NTP Time Server 8029NTS/GPS

By GPS time synchronization and the worldwide used time protocol **NTP (Network Time Protocol)** the Time Server 8029NTS/GPS turns into a highly accurate **NTP Stratum 1** Time Server. It is used for the synchronization of computers and industrial networks.

The Time Server supports the following synchronization protocols:

- NTP (incl. SNTP)
- Daytime
- Time
- SINEC H1 time datagram (**Activation Key necessary**)



The Time Server is integrated into a compact DIN Rail housing and is characterized by its easy and simple operation, although it offers a **broad range of functions**. Some of the practice-oriented functionalities are:

- **Complete parameterisation via protected WebGUI access**
  All required settings for operation can be executed via a password proteded WebGUI also giving an overview of the status of the Time Server 8029NTS/GPS.

- **Monitoring of GPS antenna circuit**
  An error message is generated when there is a short circuit in the GPS antenna circuit or an open antenna input.

- **Automatic switch-over of summer/winter time** (initial setting required)
  After initial commissioning there is no user intervention for a correct summer/winter time changeover for the following years required.

- **Automatic handling of the leap second**
  Insertion of a leap second in UTC time is automatically recognised and executed by the the Time Sever 8029NTS/GPS.

A superior security is guaranteed via available coding procedures such as symmetric keys, autokey and access restrictions and deactivation of non-used protocols.

Diffferent **Managemenet and Monitoring Functions** are availabe **as options** (e.g. SNMP, SNMP-Traps, E-mail notification, Syslog-messages including MIB II and private Enterprise MIB).

Currently the Time Server 8029NTS/GPS offers following unlockable functions:

- SINEC H1 time datagram
- Static Routing Table
- Alarming and management features
- IEEE 802.1Q Tagged VLAN

A few other basic functions of the Time Server 8029NTS/GPS:

- The Time Server 8029NTS/GPS operates as **NTP Server with Stratum 1**
- Easy operation via **WebGUI**
- **Status LEDs** on the front panel
- **Sync status output** via optical coupler
- **High freewhell accuracy** provided by GPS-supported regulation of the internal quartz basis
- Completely **maintance-free** system
- **SyncOFF Timer** (reception failure bypassing) for operation free of fault messages even based on difficult reception conditions
- Redundant **multiple validation** of the synchronization signal for an error-free and leapfree signal evaluation
- Maintefnace-free, buffered **backup clock** for at least three days

Software supplied:

- ***hmc*** Remote Software for the operating systems:
  - Microsoft® Windows® NT/2000/XP/VISTA/7 (32/64 Bit)
  - Microsoft® Windows® Server 2003/2008 (32/64 Bit)
  - Linux® (32/64 Bit)
  - Oracle® Solaris SPARC/x86
  - IBM AIX® (ab Version 5.2)
  - HP-UX 11i (RS232 support only for PA-RISC architecture)

Overview of the functions of the network Time Server 8029NTS/GPS:

Ethernet Interface

- Auto negotiate
- 10 Mbps half-/full duplex
- 100 Mbps half-/full duplex

Time Protocols

- NTPv4 Server
- NTP Broadcast Mode
- NTP Multicast Mode
- NTP Client for additional NTP Servers (redundancy)
- SNTP Server
- NTP Symmetric Key Encryption
- NTP Autokey Encryption
- NTP Access Restrictions
- PPS Time Source
- SINEC H1 time datagram **(Activation Key necessary)**
- RFC-867 DAYTIME Server
- RFC-868 TIME Server

Network Protocols

- HTTP/ HTTPS
- DHCP
- Telnet
- SSH
- SNMPv3, SNMP Traps (MIB II, Private Enterprise MIB) **(Activation Key necessary)**
- NTP (including SNTP)
- SINEC H1 time datagram **(Activation Key necessary)**

Configuration Channel

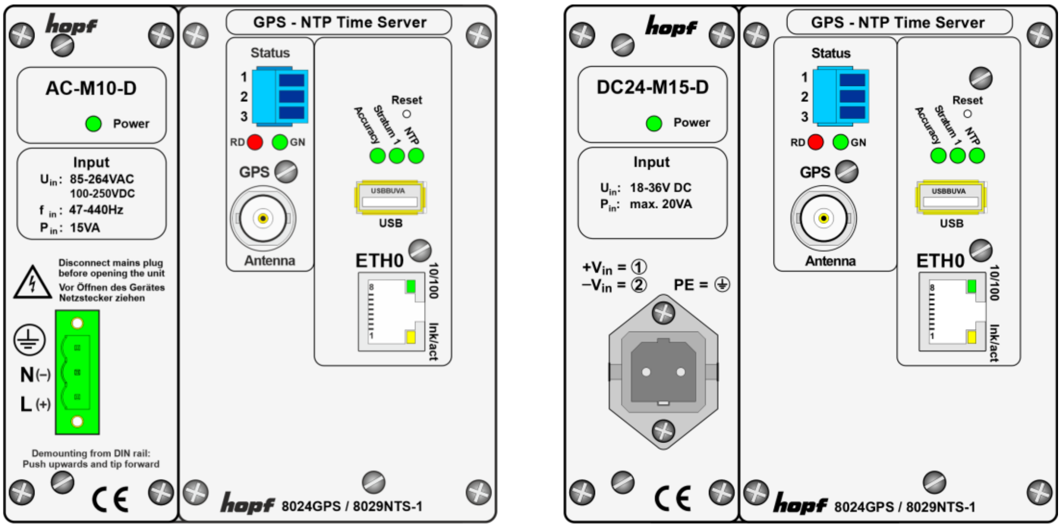
- HTTP/HTTPS WebGUI (browser-based)
- Telnet
- SSH
- External LAN configuration tool (***hmc*** **– Network-Configuration-Assistant**)
- ***hmc*** Remote connection

Additionally Freatures

- E-mail notification **(Activation Key necessary)**
- Syslog messages to external syslog server **(Activation Key necessary)**
- Routing **(Activation Key necessary)**
- Update via TCP/IP
- Fail-safe
- Watchdog circuit
- System management
- Customized security banner

2 System Structure

Views of the Timer Server 8029NTS/GPS with AC and DC power supply.



2.1 Housing

The Time Server 8029NTS/GPS is built into a closed aluminium profile housing for DIN Rail mounting according to DIN EN 60715 TH35.

2.2 Power Supply

Currently the following types of power supplies are available:

- AC/DC wide range power supply 85-264VAC / 100-250VDC

  Type: AC-M10-D
- DC power supply 18-36VDC (nominal voltage 24VDC)

  Type: DC24-M15-D
- DC power supply 36-76 VDC (nominal voltage 48VDC)

  Type: DC48-M15-D

2.3 Functional Overview of the Front Panel Elements

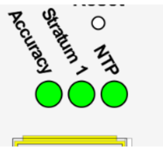
This chapter describes the individual front panel elements and their functions.

2.3.1 Reset-(Default) Button

Reset
Accur
Stratu

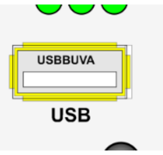
The Reset-(Default) Button is accessible with a thin object through the small drilling in the front panel next to the "Reset" inscription" (see ***Chapter 4.3 Reset-(Default) Button***).

2.3.2 NTP Status LEDs (NTP/Stratum/Accuracy)



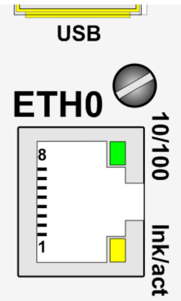
NTP-LED (Green)	NTP sewrvice of the Time Server 8029NTS/GPS
On	**Standard**, running
Off	Not running
Stratum1-LED (Green)	**The NTP service of the Time Server 8029NTS/GPS works with:**
On	Stratum 1
Flashes	Stratum 2-15
Off	Stratum 16 (no synchronization of NTP Clients)
Accuracy-LED (Green)	**The NTP service of the Time Server 8029NTS/GPS works with accuracy of:**
On	high
Flashes	medium
Off	low

2.3.3 USB-Port



On specific problems the USB connection can be used for a system recovery after consulting the ***hopf*** Support.

2.3.4 LAN Interface ETH0



10/100-LED (Green)	Description
Off	10 MBit Ethernet detected
On	100 MBit Ethernet detected

lnk/act-LED (Yellow)	Description
Off	No LAN connection to a network
On	LAN connection available
Flashes	Network activity at ETH0 (transmission / reception)

Pin No.	Assignment
1	Tx+
2	Tx–
3	Rx+
4	Not in use
5	Not in use
6	Rx–
7	Not in use
8	Not in use

2.3.4.1 MAC-Address for ETH0

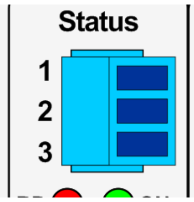
Each LAN interface is clearly identifiable on the Ethermet via a unique MAC Address (hardware address).

The MAC address given for the LAN interface ETH0 can be read in WebGUI of the appropriate board or be evaluated via the ***hmc*** **Network Configuration Assisant.** The MAC address is uniquely assigned for each LAN interface by the company ***hopf*** Elektronik GmbH.

> ℹ The factory set MAC address for the Time Server 8029NTS/GPS is stated on a sticker laterally positioned on the exterior of the housing of the device.

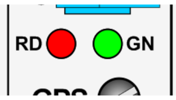
> ℹ ***hopf*** Elektronik GmbH MAC addresses begin with **00:03:C7**:xx:xx:xx.

2.3.5 Sync Status Optical Coupler



Sync Status Optical Coupler	
3-pole pluggable Connector	
Pin	**Signal**
1	Collector
2	n.c.
3	Emitter

2.3.6 Sync Status LEDs

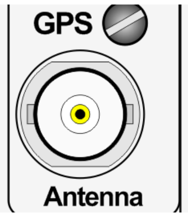


Sync Status LEDs	
LED	**Meaning**
RD	Status LED red
GN	Status LED green

The Status LEDs on the front panel signal the current (synchronization) status of the Sync Source (here Module 8024GPS). The meanings of the LEDs are as follows:

LED RD - Red	LED GN - Green	Status	STATUS Code
Off	ON	**Sync** (radio-synchronous) with quartz regulation	**SYNC**
Off	Flashes	**Sync** (radio-synchronous) - SyncOFF timer running	**SYOF**
Flashes	ON	**Sync** (radio-synchronous) - simulation mode	**SYSI**
Flashes	Flashes	**Quarz** - SyncON timer running	**QUON**
ON	ON	**Quarz** - time was set via synchronization source	**QUEX**
ON	Flashes	**Quarz** - time set manually or after reset	**QUSE**
ON	**Off**	**No valid time**	**INVA**
Off	**Off**	No operating voltage / faulty	---
3Hz	**Off**	**General Module Error (PCID)**	**INVA**
3Hz	**Invert 3Hz**	**User-Settings missing (Difference time / ST-WT changeover)**	**INVA**

2.3.7 GPS Antenna Input



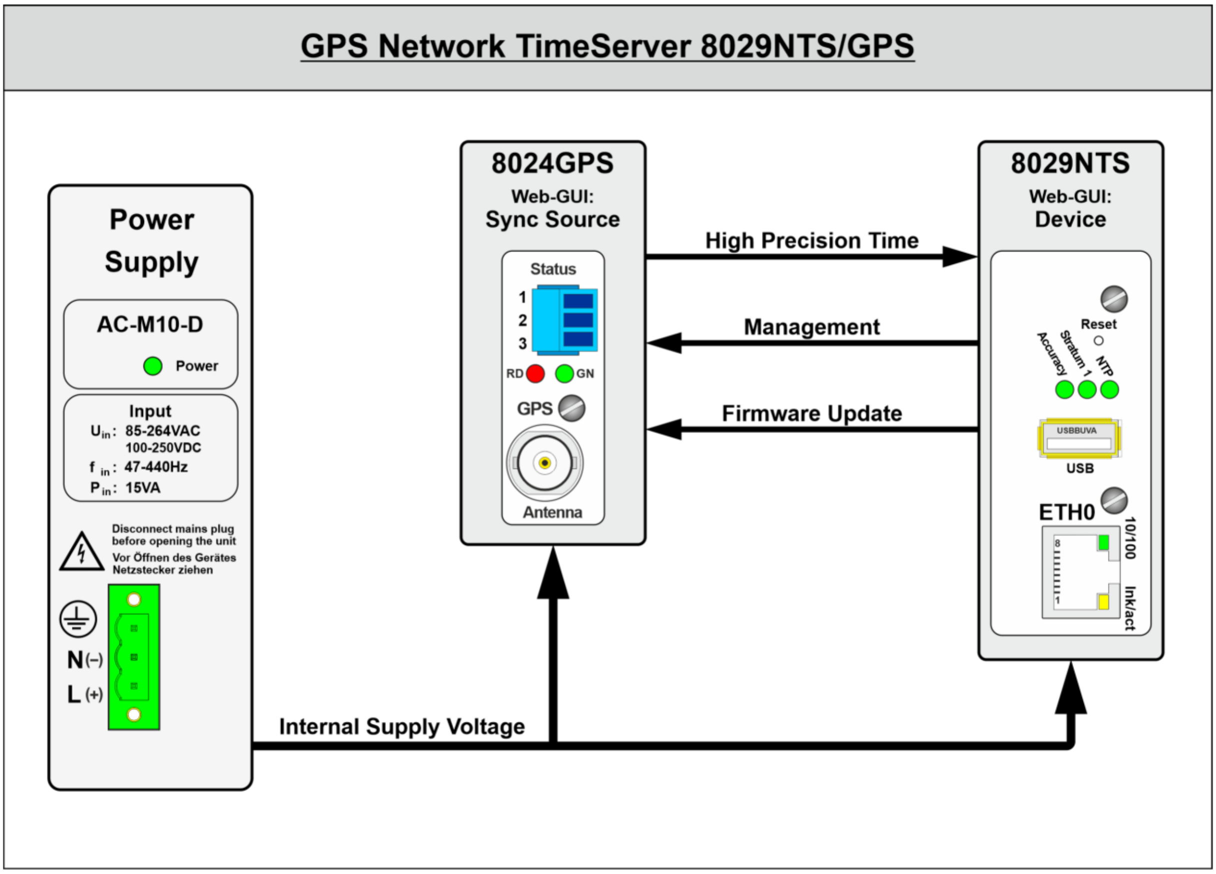
GPS Antenna	
BNC connector	
GPS	Antenna input

ℹ The antenna input provides an internal monitoring for “short-circuit“and “open input“.

3 Function Principle

This chapter describes the function principle of the Time Server 8029NTS/GPS and the internal relations between the different functional groups.

3.1 Block Diagram



- **Internal Supply Voltage**
  The individual functional components are supplied with the required operating voltage via the implemented power supply unit.

- **Firmware Update**
  A H8 firmware update of the Sync Souce (here Module 8024GPS) is completey controlled by Module 8029NTS.
  The update file for Module 8024GPS is loaded into Module 8029NTS via LAN through the WebGUI. Then Module 8029NTS performs the update of the Sync Source (here Module 8024GPS) independently.

- **Management**
  The entire control of the Sync Source (here Module 8024GPS) is done by Module 8029NTS. All data of the Sync Source, indicated via WebGUI, are demanded cyclically by Module 8029NTS from the Sync Source (here Module 8024GPS) or if necessary. These data are then prepared for the display in WebGUI. After activation settings for the Sync Source are transferred to the Sync Source immediately.

- **High Precision Time**
  The Sync Source provides a high-precision time information and the according synchronization status to Module 8029NTS. This time and status information is used for synchronization of the NTP service and if applicable other signal generations running on 8029NTS.

3.2 Function 8029NTS (WebGUI: Device)

The Module 8029NTS is the "heart" of the Time Server 8029NTS/GPS. A complete LINUX operating system is running on this Module providing all functions such as NTP, WebGUI etc. The Module also controls the connected Sync Source (here Module 8024GPS). Using the high-precise time information of Module 8024GPS the NTP service running on Module 8029NTS is also adjusted with high-precision. Thus the Module 8029NTS is a very precise **NTP STRATUM 1 - Time Server**.

3.3 Function 8024GPS (WebGUI: Sync Source)

The Module 8024GPS is in principle an independent Module with GPS receiver and its own µProcessor. In synchronous status it provides a high-precise time information to the Module 8029NTS. The control of Module 8024GPS in this system is completely done via Module 8029NTS. Parameters required by Module 8024GPS or provided are entered into WebGUI of Module 8029NTS or rather be output.

The Module 8024GPS has an own failsafe memory in which all required data for operation after generation via WebGUI are stored.

As the data of the Sync Source for the WebGUI indication need to be received by the Module 8029NTS at first, it is **no real-time indication** in **WebGUI**.

4 System Behaviour

This chapter describes the behaviour of the system in special operational phases and conditions.

4.1 Boot Phase

The boot process of the Time Server 8029NTS/GPS starts after turning on the system or a reset.

During the boot process the Module 8029NTS boots its LINUX operation system and is therefore not available via LAN.

The end of the boot process is reached when the green NTP LED is shining and thereby indicates that the NTP service on Module 8029NTS has been started and enabled. The boot process lasts approx. 1-1.5 minutes.

4.2 NTP Adjustment Process (NTP/Stratum/Accuracy)

NTP is a regulation process. After start of the NTP services, automatically processed during booting, the Time Server 8029NTS/GPS requires approximately 5-10 minutes after synchronization of the Sync Source (Status "SYNC") until NTP is set to the high accuracy of the Sync Source (here Module 8024GPS) and reaches the optimized operation condition of **STRATUM = 1** and **ACCURACY = High**.

The decisive factors here are accuracy of the synchronization source and the appropriate synchronization condition of the Sync Source.

4.3 Reset-(Default) Button

The Time Server 8029NTS/GPS can be reset by the Reset-(Default) Button behind the front panel of the board. The Reset-(Default) Button is accessible with a thin object through the small drilling in the front panel.

The button triggers different functions depending on how long it is pressed:

Duration	Function
< 1 sec.	No action
1 - 9 sec.	After releasing a systemwide **hardware reset** is triggered
>= 10 sec.	After releasing a **FACTORY DEFAULT** followd by a **REBOOT** is triggered after approx. 10 seconds

4.4 Firmware Update

The Time Server 8029NTS/GPS is a multi processor system. For this reason a firmware update always consists of a so called Software SET including up to three (3) program releases defined by the SET version needed to be loaded into the board.

ATTENTION
In order to select the correct image update, *Chapter 7.3.5.5.1 Select Image Update* must be checked!

An update is a critical process.
The device should not be turned off during the update and the network connection to the device not be interrupted.

All programs of a SET needed to be uploaded to ensure a defined operation condition.

The progam releases assigned to a SET version may be taken from the release notes of the software SETs of the Time Sever 8029NTS/GPS.

4.4.1 Firmware Update 8029NTS (WebGUI: Device)

The general process of a software update of Module 8029NTS is described below:

For selection of the correct update set the identifier **8029NTS-V2** has to be observed obligatory. The extension V2 describes a hardware version of 8029NTS.

8029NTS-V2 can be recognized:

- By the imprint stated on the front panel "***hopf*** **8024GPS / 8029NTS**"
- By the label on the housing cover "**8029NTS-V2**"
- In WebGUI at the Web-banner "**8029NTS-V2**"

The firmware update 8029NTS-V2 has to be performed as a SET.

The software package contained in the ZIP archive has to be unpacked. The following steps have to be executed in the following sequence:

1. **Image Update 8029NTS-V2**
2. **H8 Firmware Update 8029NTS-V2 (optional)**
3. **H8 Firmware Update 8024GPS**

Image Update

1. Log in as Master in WebGUI of the board.
2. Select in **Device** tab the menu item **Image Update**.
3. Select the file with the file **.img** via the selection window.
4. The selected file is shown in the selection window.
5. The update process is started with the button **Upload now**.
6. In WebGUI the successful file transfer and writing to the Module is indicated.
7. In WebGUI the successful update is indicated after 2-3 minutes with the request to release a reboot of the board.
8. After activation and successful reboot of the board the image update process is finished.

H8 Update (Optional – only when in WebGUI available)

9. Log in as Master in WebGUI of the board.
10. Select in the **Device** tab the menu item **H8 Firmware Update**.
11. Select the file with the file extension **.mot for Module 8029** via the selection window.
12. The selected file is shown in the selection window.
13. The update process is started with the button **Upload now**.
14. In WebGUI the successful file transfer to the Module is indicated.
15. Now the update of the board automatically starts after a few seconds.
16. After successful update the board automatically reboots.
17. After approx. 2 minutes the H8 update process is finished and the board is again accessible via WebGUI.

4.4.2 Firmware Update 8024GPS (WebGUI: Sync Source)

H8 Firmware Update 8024GPS

1. Log in as Master in WebGUI of the board.
2. Select in the **GPS SYNC SOURCE** tab the menu item **H8 Firmware Update**.
3. Select the file with the file extension **.mot for Module 8024** via the selection window.
4. The selected file is shown in the selection window.
5. The update process is started with the button **Upload now**.
6. In WebGUI the successful file transfer to the Module is indicated.
7. Now the update of the board automatically starts after a few seconds.
8. After successful update the board automatically reboots.
9. After approx. 2 minutes the H8 update process is finished and the board is again accessible via WebGUI.

4.5 Activation of Functions (Activation Key)

The Time Server 8029NTS/GPS offers several functions that require an "Activation Key".

These functions are only available after entering a valid activation key related to the serial number of the Module 8029NTS (not the serial number of the overall system).

The activation of such function(s) can be done by default and also later by the user if required.

These functions are:

- **IEEE 802.1Q Tagged VLAN**
  By activating this function network interfaces can be configured with additional VLANs (Virtual Bridged Local Area Networks) according to IEEE 802.1q.

- **Static Routing Table**
  This function is suitable for configuring static routes based on special network configuration requirements.

- **Alarming and management features**
  This function enables to use **SNMP (SNMPv2c, SNMPv3), Syslog and Email notification** to monitor the system status. Together with the assets provided in the MIB II by default, the ***hopf*** Private Enterprise MIB is also made available. By using the ***hopf*** Private Enterprise MIB numerous product-specific assets for realizing extended management and control functions are available.

- **SINEC H1 time datagram**
  By activating this function SINEC H1 time datagram can be parameterized and issued via the LAN interface.

> ⚠ The settings for activation keys (e.g. an entered activation key) are neither modified nor influenced by the function FACTORY.

5 Installation

The installation of the Time Server 8029NTS/GPS is described below.

5.1 Installation/Dismounting of the DIN Rail Housing

The Time Server 8029NTS/GPS can be mounted on all rails in accordance with DIN EN 60715 TH35 and is designed for horizontal mounting.

Dimensions

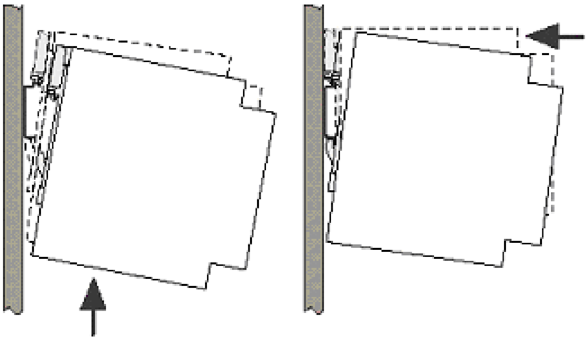
The dimensions of the housing can be found in ***Chapter 11.5 Dimensions – DIN Rail*** Housing.

- **Time Server 8029NNTS/GPS** – **Housing: TYPE 2**

> ⚠ In order to guarantee an adequate convection, we recommend the following minimum distance from other modules:
>
> - 5.0 cm in vertical direction and
> - 1.0 cm in horizontal direction.

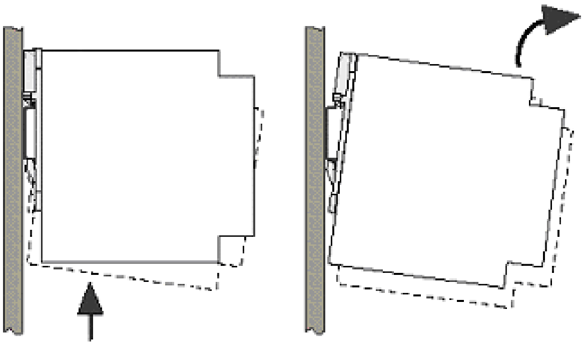
5.1.1 Mounting

Place the module's rail guide bar against the lower edge of the rail, push the module upwards, and clip to the back.



5.1.2 Dismounting

Push the module upwards and then tip forward to remove from the rail.



5.2 Protective Earth Conductor (Grounding)

Grounding of the Time Server 8029NTS/GPS is achieved via the PE line of the power supply wiring.

5.3 Power Connection

Depending on the version of the appliance an AC or DC power feeding is available.

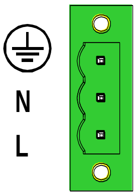
5.3.1 AC Power Supply

The standard AC power supply unit of the Time Server 8029NTS/GPS is described hereunder. However, the connection data on the nameplate of the respective device are always applicable.

Pay attention to the following when connecting the power supply:

- Correct voltage type (AC or DC),
- Voltage amount

The power cable is connected via a 3pole pluggable screw terminal with housing.



Connecting the incorrect voltage can damage the Time Server 8029NTS/GPS.

5.3.1.1 Safety and Warning Instructions

Please read these instructions thoroughly to facilitate safe operation of the device and to use all of its functions!

Warning: Never work on live equipment! Danger to life!

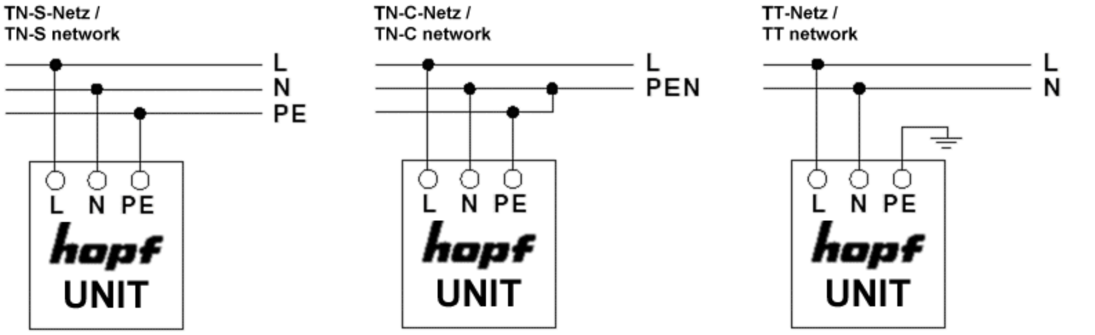
The Time Server 8029NTS/GPS is a built-in device. Installation and commissioning may only be carried out by suitable specialist personnel. In doing so the respective country-specific regulations (e.g. VDE, DIN) must be observed.

In particular, before commissioning please ensure that

- The power connection has been installed correctly and there is guaranteed protection against electric shock!
- The ground wire is connected!
- All power cables are correctly fused and sized!
- All output lines are sized in accordance with the max. output current of the device or are specially fused!
- Sufficient convection is guaranteed!

The device contains components carrying life-threatening voltage and a high amount of stored energy!

5.3.1.2 Connection to various Power Networks



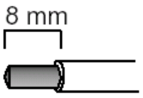
5.3.1.3 Power Cable Connection

The power cable is connected via a 3pole pluggable screw terminal. The following cable cross-sections can be connected to the input plug:

	Fixed [mm^2]	Flexible [mm^2]	AWG	Starting moment [Nm]
L, N, ⏚	0.2-2.5	0.2-2.5	24-12	0.5 – 0.6

For a reliable and secure contact:

Strip the insulation by 8 mm!



The connector must always be mounted using the housing and strain relief fitting provided.

5.3.1.4 Voltage Input / Fuse Protection

The 85-264VAC connection is made via the pluggable screw terminal L, N and ⏚.

Primary Side Fuse Protection

The device must be installed in accordance with the provisions of EN 60950. There must be a suitable isolating device external to the power supply capable of switching the device off.

The primary side line protection, for example, is suitable for this purpose.

Further equipment protection is not required because the device is fused internally.

Recommended External Fuse

When connecting the Time Server 8029NTS/GPS a suitable fuse protection of the power supply needs to be observed.

Accordingly, the performance data should be taken from the nameplate of the device. Currently the standard versions of the Time Server 8029NTS/GPS are supplied with power supplies with power consumption between 6 and 15VA.

Regarding DC applications a suitable fuse must be connected.

> If the internal fuse trips it is highly likely that the device is faulty. In this case the equipment should be checked at the factory!

5.3.1.5 Power Supply Specifications

All specifications regarding the AC power supply can be found in ***Chapter 12.4 Power Supplies***.

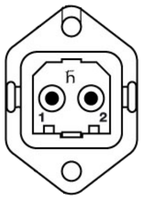
5.3.1.6 Power LED

The green Power LED allows a functional evaluation directly on site at the control cabinet.

LED lights	Normal power supply operation
LED off	No power supply is available or the device is faulty.

5.3.2 DC Power Supply

> Make sure that the external voltage source is switched off. When connecting the power supply, ensure that the polarity and ground connection are correct!



- The power supply cable is connected to the Time Server 8029NTS/GPS by means of a 2-pole plug connector with additional ground connection and interlock:

$+V_{in}$:	Positive pole (contact 1)
$–V_{in}$:	Negative pole (contact 2)
PE:	Ground

Connecting the incorrect voltage can damage the Time Server 8029NTS/GPS.

Grounding:
The negative pole (-Vin) and the ground (PE) are connected together as standard on the system side.

5.3.2.1 Power Supply Unit Specifications

All specifications regarding the DC power supply can be found in ***Chapter 11.4 Power Supplies***.

5.3.2.2 Fuse Protection

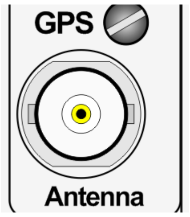
When connecting the Time Server 8029NTS/GPS a suitable fuse protection of the power supply needs to be observed.

Accordingly, the performance data should be taken from the nameplate of the device. Currently the standard versions of the Time Server 8029NTS/GPS are supplied with power supplies with power consumption of max. 20VA.

If the internal fuse (device fuse) blows, it is most probable that the device is defective. In this case the device needs to be checked in the facatory!

5.4 Connection GPS Antenna System

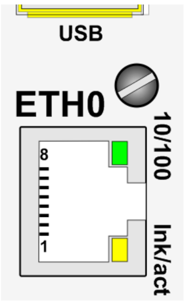
The coaxial line of the GPS antenna system is placed on the BNC female connector with the **"GPS Antenna"** inscription on the front panel of the Time Server 8029NTS/GPS. More detailed descriptions referring to the installation of the antenna system, for example, cable lengths and cable types, are described in the document “Antenna System GPS”.



GPS Antenna	
BNC Connector	
GPS	Antenna input

There is an antenna input monitoring for “open“ and “short-ciruit“ on the the system side.

5.5 Connection LAN Interface ETH0



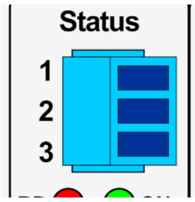
10/100-LED (Green)	Description
Off	10 MBit Ethernet detected
On	100 MBit Ethernet detected

lnk/act-LED (Yellow)	Description
Off	No LAN connection to a network
On	LAN connection available
Flashes	Network activity at ETH0 (transmission / reception)

Pin No.	Assignment
1	Tx+
2	Tx–
3	Rx+
4	Not in use
5	Not in use
6	Rx–
7	Not in use
8	Not in use

5.6 Connection Sync Status Optical Coupler

The Sync Status Optical Coupler connection is a 3-pole pluggable screw terminal.



Sync Status Optokoppler	
3-pole pluggable Connector	
Pin	Signal
1	Collector
2	n.c.
3	Emitter

6 Commissioning

This chapter describes commissioning of the Time Server 8029NTS/GPS.

6.1 General Procedure

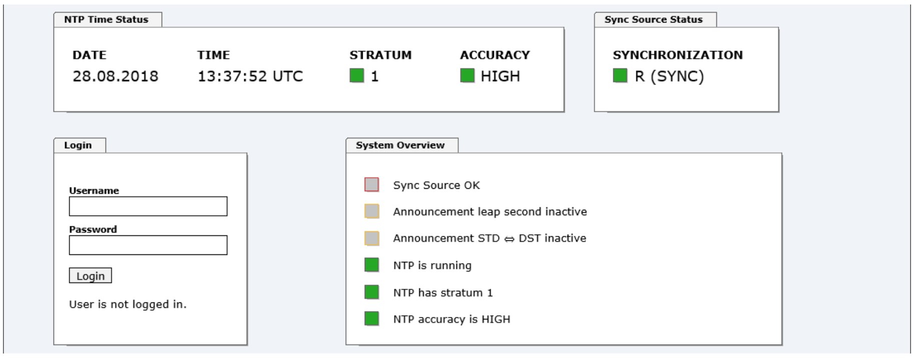
Overview of the general commissioning procedure:

- Finish the installation process completely
- Switch on the device
- Wait until the booting phase is finsihed (Duration approx. 2 min. – finished when the green NTP LED is lit on)
- Using the SEARCH Function of the ***hmc*** **- Network Configuration Assistant** in order to access the Time Server 8029NTS/GPS and set the basis LAN parameters (e.g. DHCP). Afterwards connect to the WebGUI of the Time Server 8029NTS/GPS via Web browser
  OR
  connect directly with the factory default IP-address (192.168.0.1) to the WebGUI of the Time Server 8029NTS/GPS via Web browser
- Log in as **"master"**
- Change default passwords for **"master"** and **"device"** In the **DEVICE tab**
- Set all required LAN parameters (e.g. entry of DNS server) in **NETWORK tab** if necessary
- Check current settings in **NTP tab** and modify according to individual needs as necessary
- Parametrize following values of the Sync Source (here Module 8024GPS) in **GPS SYNC SOURCE** tab:
  - Set current UTC time
  - Set the local difference time to UTC
  - Set or deactivate the changeover times for summer/winter time
  - Set local position (if not known as 0)
  - Check values for reception mode, SyncON/SyncOFF Timer and status OC

  Trigger a **Module Reset** after the above mentioned entries

> During first commissioning it is mandatory required to configure the difference time to UTC and the changeover times for summer/winter time respectively to deactivate them one time. Otherwise synchronization via GPS will not be possible and a "Sync Source Error" is indicated.

- Check for **Module Error** in register **GPS SYNC SOURCE**
- Parametrize optional functions e.g. SNMP or SINEC H1 time datagram
- If all base settings are carried out correctly and there is GPS reception, the **GENERAL** tab should look like this after approx. 30 min.:



NTP Time Status

DATE	TIME	STRATUM	ACCURACY
28.08.2018	13:37:52 UTC	🟩 1	🟩 HIGH

Sync Source Status

SYNCHRONIZATION
🟩 R (SYNC)

Login

Username
Password

User is not logged in.

System Overview

□ Sync Source OK
□ Announcement leap second inactive
□ Announcement STD ⇔ DST inactive
🟩 NTP is running
🟩 NTP has stratum 1
🟩 NTP accuracy is HIGH

6.2 Switching on the Operating Voltage

The Time Server 8029NTS/GPS has no own switch for the power supply. The converter is activated by switching on the external power supply source.

6.3 Establish the Network Connection via Web Browser

Ensure that the network parameters of the Time Server 8029NTS/GPS are configured in accordance with the local network before connecting the device to the network.

Connecting a network to an incorrectly configured Time Server 8029NTS/GPS (e.g. duplicate IP address) may cause interference on the network.

The Time Server 8029NTS/GPS is supplied with a static IP-address (equivalent to the factory default setting).

IP-address:	**192.168.0.1**
Network mask:	**255.255.255.0**
Gateway:	**not set**

In case it is not known whether the Time Server 8029NTS/GPS with a Factory Default setting causes problems in the network, the basis network parameterization should be executed via a "Peer to Peer" network connection.

Request the required network parameters from your network administrator if those are unknown.

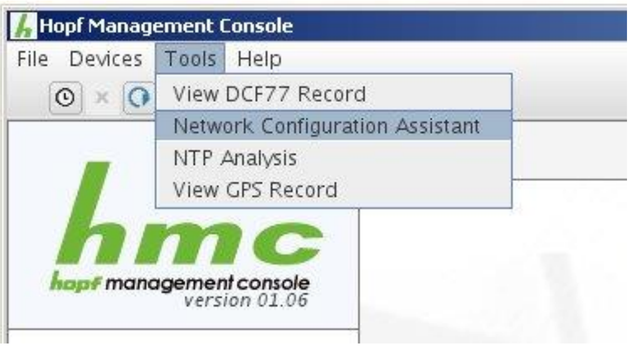
The network connection is made via a LAN cable and RJ45 plug (recommended cable type: CAT5 or better).

6.4 Network Configuration for ETH0 via LAN through ***hmc***

After connecting the system to the power supply and creating the physical network connection to LAN interface of the Time Server 8029NTS/GPS, the device can be searched for on the network via the ***hmc*** (***hopf*** **Management Console**). Then the base LAN parameters (IP address, netmask and gateway or DHCP) may be adjusted in order to allow accessibility of the Time Server 8029NTS/GPS for other systems on the network.

The SEARCH Function of the ***hmc*** - **Network Configuration Assistant** **requires** for location and recognition of the desired Time Server 8029NTS/GPS the ***hmc***-computer and the Time Server 8029NTS/GPS **in the same SUB Net**.

The base LAN parameters can be set via the ***hmc*** integrated **Network Configuration Assistant**.

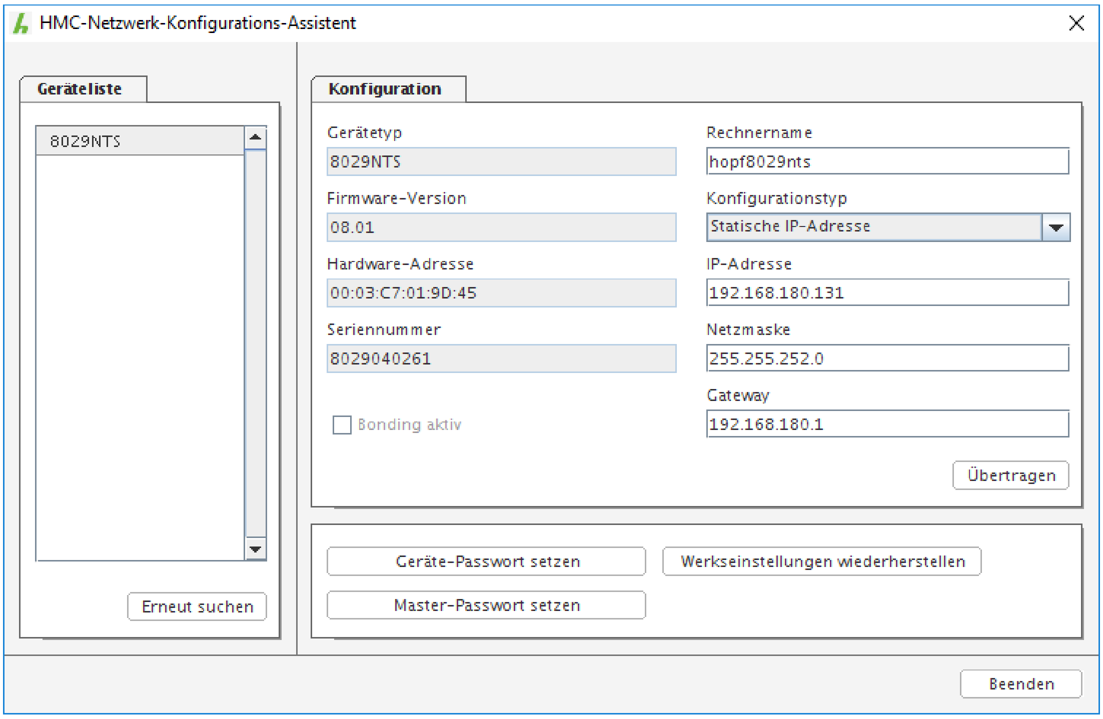


After a successful start of the ***hmc*** **Network Configuration Assistant** and completed search of the ***hopf*** LAN devices, the configuration of the base LAN parameters can be done.

The Time Server 8029NTS/GPS is stated as **8029NTS in the Device List.**

The determination of different Time Server 8029NTS/GPS (or other products variants) is made via **Hardware Address** (MAC Address).

> The factory set MAC address for the Time Server 8029NTS/GPS is stated on a sticker laterally positioned on the exterior of the housing of the device.



HMC-Netzwerk-Konfigurations-Assistent

Geräteliste: 8029NTS

Konfiguration

Gerätetyp: 8029NTS	Rechnername: hopf8029nts
Firmware-Version: 08.01	Konfigurationstyp: Statische IP-Adresse
Hardware-Adresse: 00:03:C7:01:9D:45	IP-Adresse: 192.168.180.131
Seriennummer: 8029040261	Netzmaske: 255.255.252.0
□ Bonding aktiv	Gateway: 192.168.180.1

For an extended configuration of the Time Server 8029NTS/GPS through a browser via WebGUI the following base parameters are required:

• **Host Name**	⇨ e.g. hopf8029nts
• **Network Configuration Type**	⇨ e.g. Static IP Address or DHCP
• **IP Address**	⇨ e.g. 192.168.100.149
• **Netmask**	⇨ e.g. 255.255.255.0
• **Gateway**	⇨ e.g. 192.168.100.1

The **hostname <u>must</u>** meet the following conditions:

- The hostname may only contain the characters 'A'-'Z', '0'-'9', '-' and '.' . There should be no distinction between upper-and lower-case letters.
- The character '.' may only appear as a separator between labels in domain names.
- The sign '-' must not appear as first or last character of a label.

The network parameters being assigned should be pre-determined with the network administrator in order to avoid problems on the network (e.g. duplicate IP address).

IP Address (IPv4)

An IP address is a 32 bit value divided into four 8 bit numbers. The standard presentation is 4 decimal numbers (in the range 0...255) separated from each other by dots (dotted quad notation).

Example: 192.002.001.123

The IP address consists of a leading network ID followed by the host ID. Four common network classes were defined in order to cover different requirements. Depending on the network class, the last one, two or three bytes define the host while the rest define the network (network ID) in each case.

In the following text the "x" stands for the host part of the IP address.

Class A Networks

IP addresses 001.xxx.xxx.xxx to 127.xxx.xxx.xxx

There is a maximum of 127 different networks in this class. This allows the possibility to connect a very high number of devices (max. 16.777.216)

Example: 100.000.000.001, (Network 100, Host 000.000.001)

Class B Networks

IP addresses 128.000.xxx.xxx to 191.255.xxx.xxx

Each of these networks can consist of up to 65534 devices.

Example: 172.001.003.002 (Network 172.001, Host 003.002)

Class C Networks

IP addresses 192.000.000.xx to 223.255.255.xxx

These network addresses are the most commonly used. Up to 254 devices can be connected.

Class D Networks

The addresses from 224.xxx.xxx.xxx - 239.xxx.xxx.xxx are used as multicast addresses.

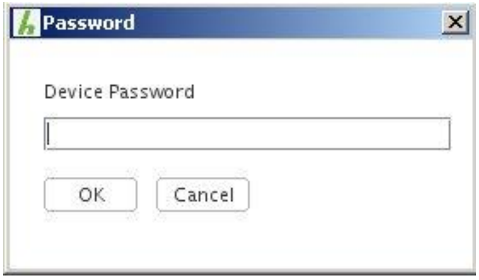
Class E Networks

The addresses from 240.xxx.xxx.xxx - 254.xxx.xxx.xxx are designated as "Class E" and are reserved.

Gateway Address

The gateway or router address is required in order to be able to communicate with other network segments. The standard gateway must be set to the router address which connects these segments. This address must be within the local network.

After entering the above mentioned LAN parameters, they needed to be transferred to the Time Server 8029NTS/GPS via the `Apply` button. Afterwards the entry of the **Device Password** is requested:



The Time Server 8029NTP/GPS is supplied with the default device password <**device**> on delivery. After entry click on the `OK` button to confirm.

The LAN parameters thus set are directly adopted (without reboot) by the Time Server 8029NTS/GPS and are immediately active.

7 HTTP/HTTPS WebGUI – Web Browser Configuration Interface

For the correct display and function of the WebGUI, JavaScript and Cookies must be enabled in the browser.

7.1 Quick Configuration

This chapter gives a brief description of the basic operation of the WebGUI installed on the module.

7.1.1 Requirements

- Ready-for-operation ***hopf*** NTP Time Server 8029NTS/GPS
- PC with installed web browser (e.g. Internet Explorer) in the sub-network of Time Server 8029NTS/GPS

7.1.2 Configuration Steps

- Create the connection to the Time Server with a web browser
- Login as a **'master'** user (default password <master> is set by delivery)
- Switch to "Network" tab if available and enter the DNS Server (required for NTP and the alarm messages depending of network)
- Save the configuration
- Switch to "Device" tab and restart Network Time Server via "Reboot Device"
- NTP Service is now available with the standard settings
- NTP specified settings can be done in the "NTP" tab
- Alarm messages via Syslog/SNMP/Email can be configured in "Alarm" tab – only if this function is enabled by an activation key

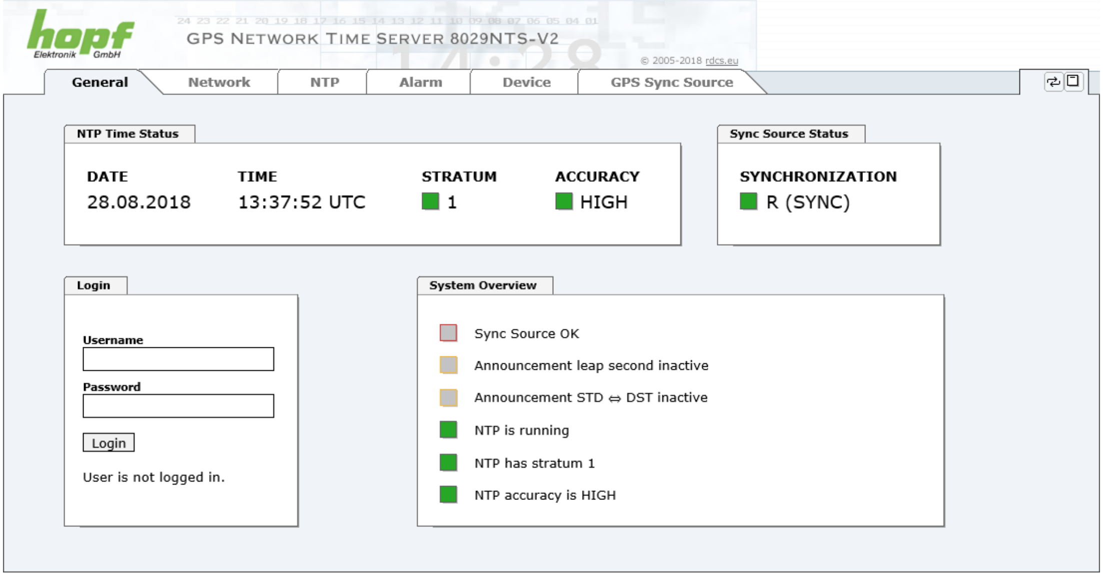
The following detailed explanatory information should be read if anything is unclear while executing the configuration steps.

7.2 General – Introduction

The Time Server 8029NTS/GPS should be accessible to a web browser if it has been set up correctly. Enter the IP address - as set up in the Time Server 8029NTS/GPS earlier - or the DNS name on the address line <http://xxx.xxx.xxx.xxx> and the following screen should appear.

When using IPv6, it is mandatory to enclose the IPv6 address with [ ]
e.g..: `http://[2001:0db8:85a3:08d3::0370:7344]/`

The complete configuration can only be completed via the modules WebGUI!



NTP Time Status

DATE	TIME	STRATUM	ACCURACY
28.08.2018	13:37:52 UTC	🟩 1	🟩 HIGH

Sync Source Status

SYNCHRONIZATION
🟩 R (SYNC)

Login

Username

Password

Login

User is not logged in.

System Overview

- □ Sync Source OK
- □ Announcement leap second inactive
- □ Announcement STD ⇔ DST inactive
- 🟩 NTP is running
- 🟩 NTP has stratum 1
- 🟩 NTP accuracy is HIGH

The WebGUI was developed for multi-user read access but not for multi-user write access. It is the responsibility of the user to pay attention to this issue.

7.2.1 LOGIN and LOGOUT as User

All of the modules data can be read without being logged on as a special user. However, the configuration and modification of settings and data can only be carried out by an authorised user! Two types of user are defined:

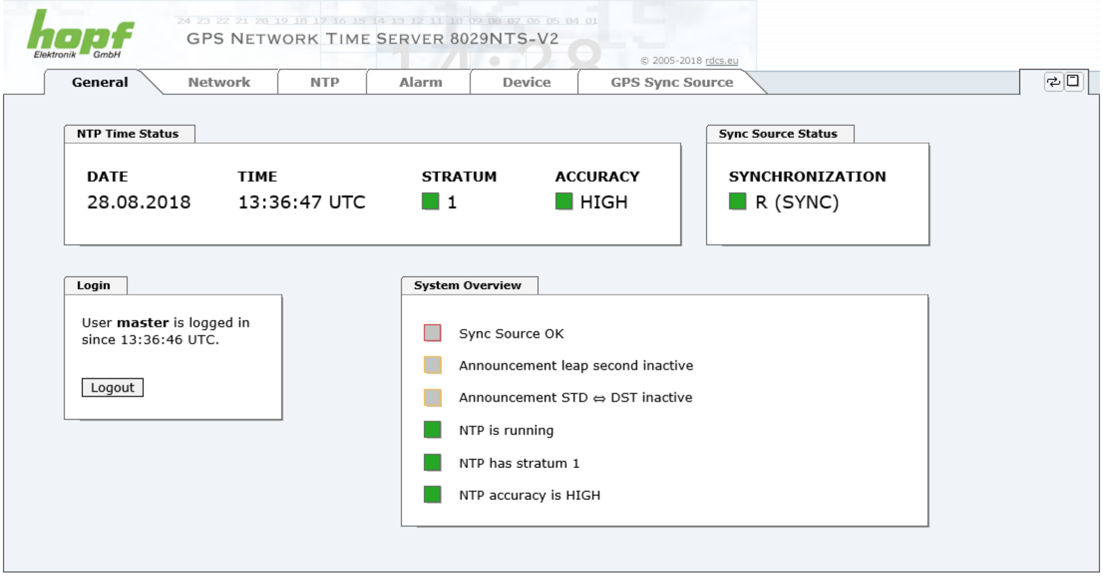
- "**master**" user (default password on delivery: <**master**>)
- "**device**" user (default password on delivery: <**device**>)

Differentiation is made between **upper and lower case** characters in the password. Alphanumeric characters and the following symbols can be used: **. , ! " $ % & / { } [ ] ( ) = ? \ + - @ * ~ # ' < > | ; : _**

The password must be between 6 and 20 characters long and contain at least one uppercase letter, one lowercase letter and one digit!

The password should be changed after the first login for security reasons.

The following screen should be visible after logging in as a "master" user:



NTP Time Status

DATE	TIME	STRATUM	ACCURACY
28.08.2018	13:36:47 UTC	🟩 1	🟩 HIGH

Sync Source Status

SYNCHRONIZATION
🟩 R (SYNC)

Login

User **master** is logged in since 13:36:46 UTC.

Logout

System Overview

- ⬜ Sync Source OK
- ⬜ Announcement leap second inactive
- ⬜ Announcement STD ⇔ DST inactive
- 🟩 NTP is running
- 🟩 NTP has stratum 1
- 🟩 NTP accuracy is HIGH

Click on the **Logout** button to log out.

The WebGUI is equipped with a session management. If the user does not conduct a logout, the logout is automatically made after 10 minutes of inactivity (idle time).

After successful login, depending on the access level (device or master user), changes can be made to the configuration and saved.

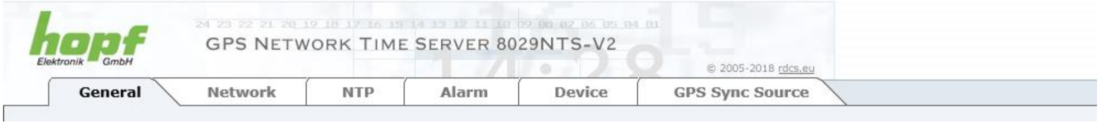
Users logged in as "**master**" have all access rights to the Time Server 8029NTS/GPS.

Users logged in as "**device**" do **not** have access to:

- Trigger reboot
- Trigger factory defaults
- Carry out image update
- Carry out H8 firmware update
- Upload certificate
- Change master password
- Diagnostics
- Download configuration files

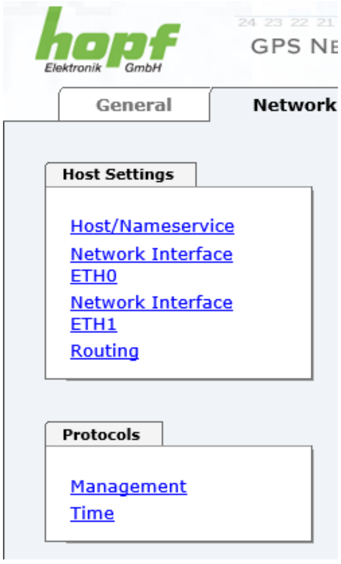
7.2.2 Navigation via the Web Interface

The WebGUI is divided into functional tabs. Click on one of these tabs to navigate through the board. The selected tab is identified by a darker background colour, see the following image (General in this case).



User login is not required in order to navigate through the board configuration options.

JavaScript and Cookies should be enabled in the browser in order to guarantee the correct operation of the web interface.



All the links within the tabs on the left hand side lead to corresponding detailed display or setting options.

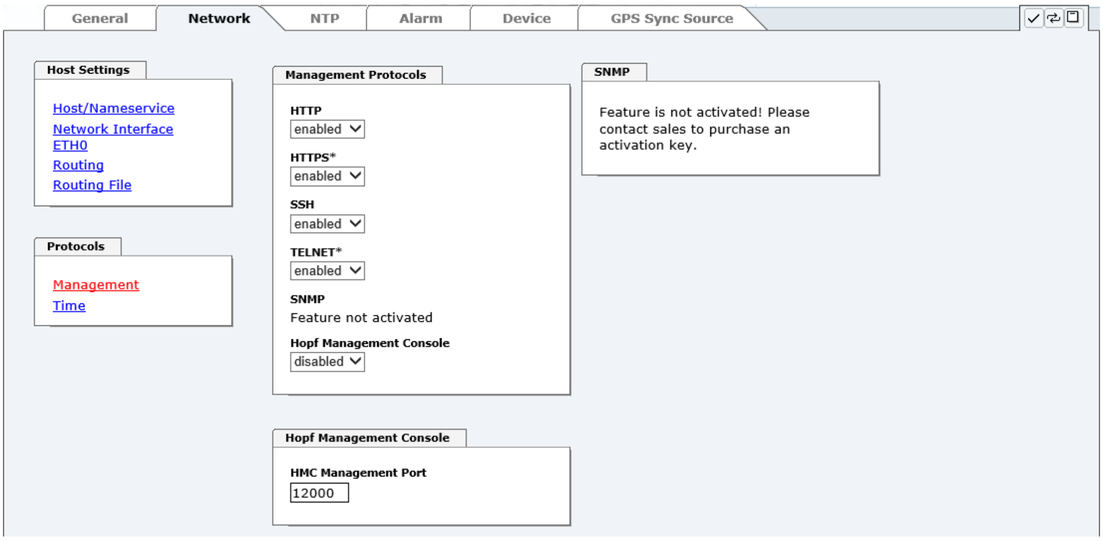
7.2.3 Enter or Changing Data

It is necessary to be logged on as one of the users described above in order to enter or change data.

7.2.3.1 Changing of Data in 8029NTS (WebGUI: Device)

All changeable data, except those in GPS SYNC SOURCE tab, are saved in Module 8029NTS. For these data the value saving is divided into two steps.

For a permanent saving the modified value MUST first be accepted with **Apply** from the module and then be stored with **Save**. Otherwise the modifications get lost after a reboot of the module or switching the system off.



Host Settings

Host/Nameservice
Network Interface
ETH0
Routing
Routing File

Protocols

Management
Time

Management Protocols

HTTP
enabled

HTTPS*
enabled

SSH
enabled

TELNET*
enabled

SNMP
Feature not activated

Hopf Management Console
disabled

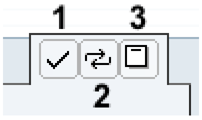
SNMP

Feature is not activated! Please contact sales to purchase an activation key.

Hopf Management Console

HMC Management Port
12000

After an entry with **Apply** is made, the configured field is marked with a star ' * '. This means that a value has been entered or changed but not yet been stored in the flash memory.



Meaning of the symbols from left to right:

No.	Symbol	Description
1	**Apply**	Acceptance of changes and entered data
2	**Reload**	Restoring the saved data
3	**Save**	Fail-save storage of the data in the flash configuration

If the data should only be tested it is sufficient to accept the changes with **Apply**.

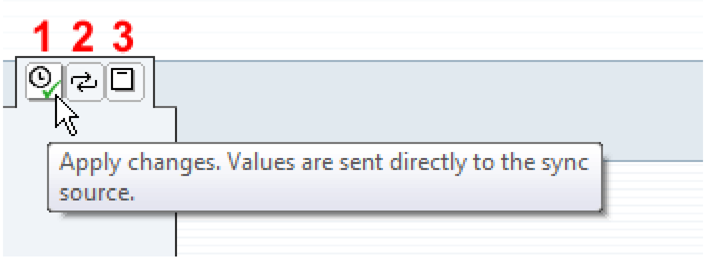
Changing Network Parameters

Modifications of the network parameters (e.g. IP address) are immediately effective clicking on **Apply** to confirm.
However, the modifications are not permanently saved yet. This requires to access the WebGUI with the new network paramters again and to save the data with **Save** permanently.

For adopting changes and entering values only the respective buttons in the WebGUI can be used.

7.2.3.2 Changing of Data in 8024GPS (WebGUI: Sync Source)

The modified data in the GPS SYNC SOURCE tab are diretly transferred to the Module 8024GPS by pushing the button 1 and stored failsafe in Module 8024GPS. Tabs with settings and values modified in this manner can also be recognized by the modified display of the **Apply** button. The buttons 2 and 3 in GPS SYNC SOURCE tab are disabled and are not required.

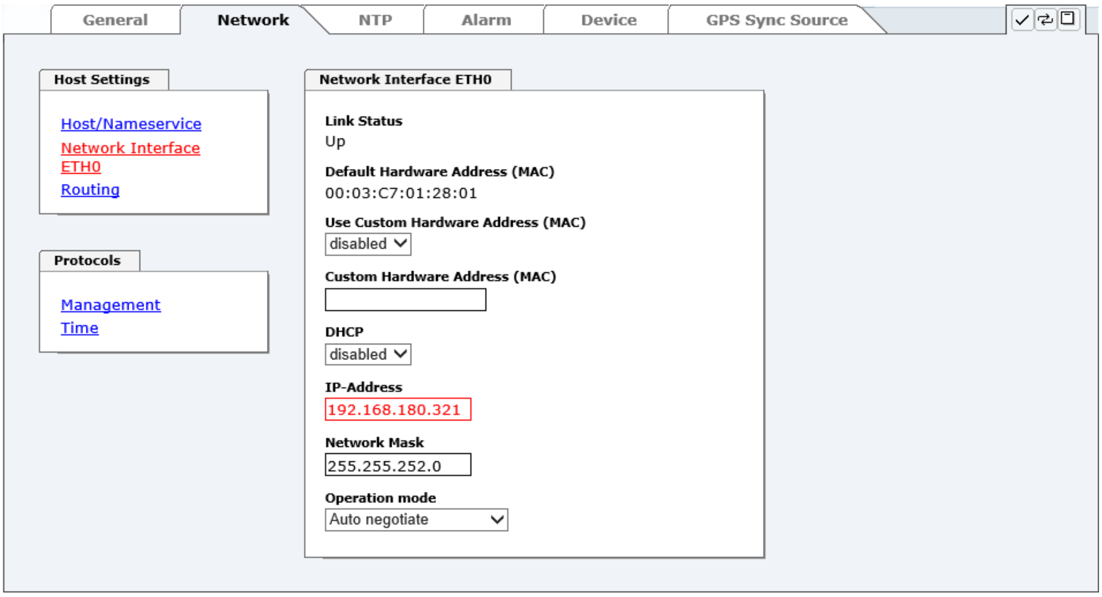


Apply changes. Values are sent directly to the sync source.

The new reading of the modified data from Module 8029NTS for the WebGUI indication can take up to 30 seconds after data transfer to Module 8024GPS.
However, this has no effect on the function of the appropriate setting/value.

7.2.4 Plausibility Check during Input

A plausibility check is generally carried out during input.



Link Status
Up

Default Hardware Address (MAC)
00:03:C7:01:28:01

Use Custom Hardware Address (MAC)
disabled

Custom Hardware Address (MAC)

DHCP
disabled

IP-Address
192.168.180.321

Network Mask
255.255.252.0

Operation mode
Auto negotiate

As illustrated in the above image, an invalid value (e.g. text where a number should be entered, IP address not within the range etc.) is identified by a red border when an attempt is made to accept these settings. It should be noted here that this is only a semantic check and not to test whether an entered IP address can be used on the own network or in the configuration! As long as an error message is displayed it is not possible to save the configuration in the flash memory.

The error check only verifies semantics and the validity of ranges. It is **NOT a logic or network check** for entered data.

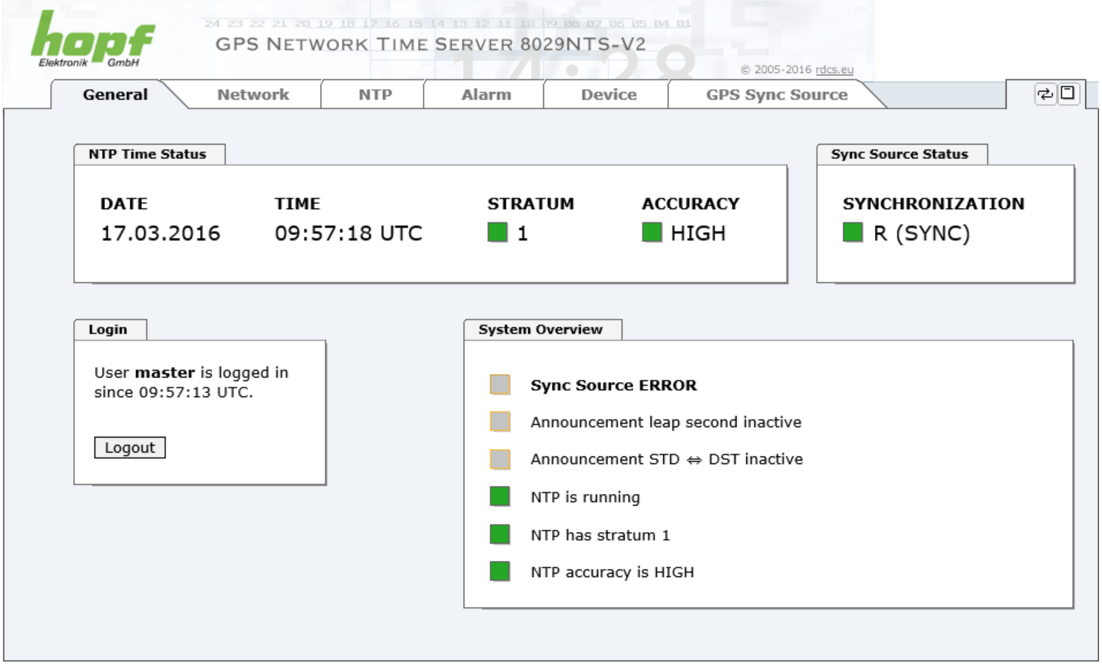
7.3 Description of the Tabs

The WebGUI is divided into the following tabs:

- General
- Network
- NTP
- Alarm
- Device
- GPS Sync Source

7.3.1 GENERAL Tab

This is the first tab displayed when using the web interface.



NTP Time Status

DATE	TIME	STRATUM	ACCURACY
17.03.2016	09:57:18 UTC	🟩 1	🟩 HIGH

Sync Source Status

SYNCHRONIZATION
🟩 R (SYNC)

Login

User **master** is logged in since 09:57:13 UTC.

Logout

System Overview

⬜ **Sync Source ERROR**
⬜ Announcement leap second inactive
⬜ Announcement STD ⇔ DST inactive
🟩 NTP is running
🟩 NTP has stratum 1
🟩 NTP accuracy is HIGH

NTP Time Status

This area shows basic information about the current time and date of the Time Server 8029NTS/GPS. The time **always** corresponds to UTC. The reason for this is that NTP always works with UTC and not with local time.

Stratum displays the actual NTP stratum value of the Time Server 8029NTS/GPS with the value range from 1-16.

The **ACCURACY** field (accuracy of NTP) can contain the values LOW - MEDIUM - HIGH. The meaning of these values is explained in ***Chapter 13.5 Accuracy & NTP Basic Principles***.

Sync Source Status

Display of the actual status of synchronization of the Sync Source (here Module 8024GPS) with these possible values:

SYNC	Time synchronized + Quartz regulation started/running
SYOF	Time synchronized + SyncOFF running
SYSI	Time synchronized as simulation mode (without actual GPS reception)
QUON	Quartz/Crystal time + SyncON running
QUEX	Quartz/Crystal time (in freewheel after synchronization failure ⇨ Board was already synchronized)
QUSE	Quartz/Crystal time after reset or manual setting
INVA	Invalid time

Login

The login box is described in ***Chapter 7.2.1 LOGIN and LOGOUT as User***.

System Overview

This table gives a direct overview of the Time Server's 8028NTS/GPS current operating states.

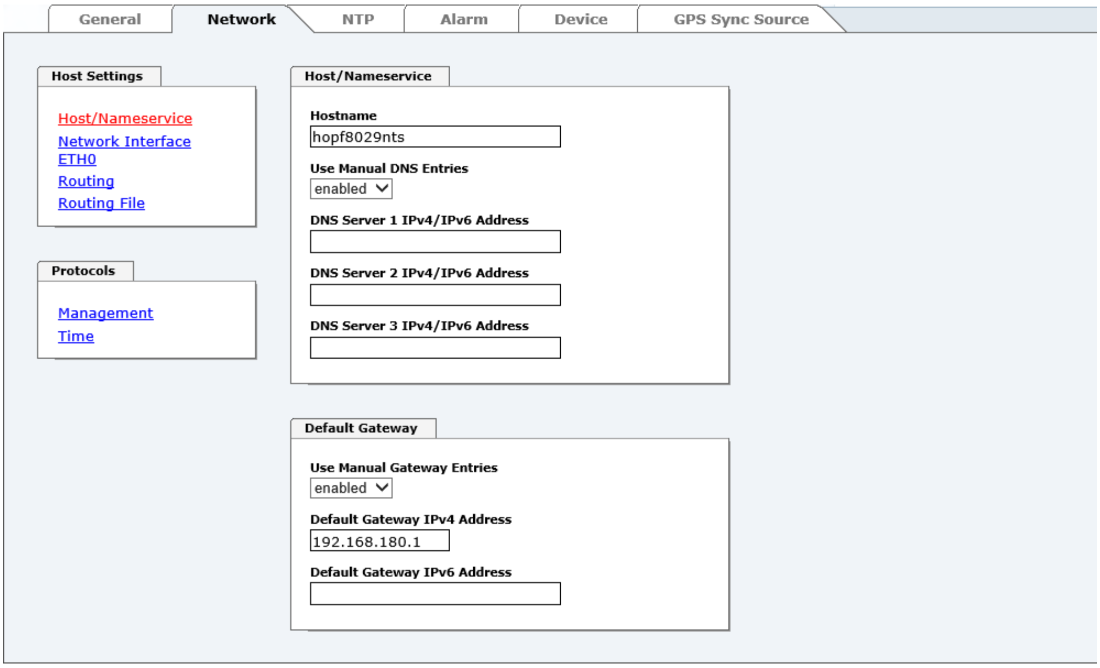
WebGUI	**Description**
Sync Source OK	When active (RED) there is a Sync Souce failure. For details please go to **GPS SYNC SOURCE** tab **- Module Errors.**
Announcement leap second inactive	When active (ORANGE) there is an announcement for a leap-second.
Announcement STD ⇔ DST inactive	When active (ORANGE) there is an announcement for a summer / winter time change-over.
NTP is running	The NTP process on Module 8029NTS is running
NTP has stratum 1	Shows the appropriate stratum the NTP process works with.
NTP Accuracy is High	Shows the appropriate accuracy the NTP process works with.

Announcements

The display fields LEAP SECOND and STD ⇔ DST announce a corrosponding event to the next hour (insertion of a leap-second or rather switchover of summer/winter time).

7.3.2 NETWORK Tab

All the links within the tab on the left hand side lead to corresponding detailed setting options.



Host/Nameservice

Hostname: hopf8029nts

Use Manual DNS Entries: enabled

DNS Server 1 IPv4/IPv6 Address:

DNS Server 2 IPv4/IPv6 Address:

DNS Server 3 IPv4/IPv6 Address:

Default Gateway

Use Manual Gateway Entries: enabled

Default Gateway IPv4 Address: 192.168.180.1

Default Gateway IPv6 Address:

<u>Changing Network Paramaters</u>

Modifications of the network parameters (e.g. IP address) are immediately effective clicking on **Apply** to confirm.
However, the modifications are not permanently saved yet. This requires to access the WebGUI with the new network paramters again and to save the data with **Save** permanently.

7.3.2.1 Host/Nameservice

Setting for the clear network detection.

7.3.2.1.1 Hostname

The standard setting for the Hostname is "**hopf8029nts**". This name should also be adapted to the respective network infrastructure.

If in doubt, simply leave the standard value in place or ask your network administrator.

The **hostname** **<u>must</u>** meet the following conditions:

- The hostname may only contain the characters 'A'-'Z', '0'-'9', '-' and '.' . There should be no distinction between upper-and lower-case letters.
- The character '.' may only appear as a separator between labels in domain names.
- The sign '-' must not appear as first or last character of a label.

For a correct operation a hostname is required. The field for the hostname **<u>must not</u>** be left blank.

7.3.2.1.2 Use Manual DNS Entries

With this setting you can select whether the manually entered DNS servers (DNS servers 1 to 3) should be used.

If "enabled" is selected here, the entries in DNS Server 1 to 3 are used.

If "disabled" is selected, the entries in DNS Server 1 to 3 are ignored.

If a DHCP server is used to distribute the network configuration and if this also distributes the DNS servers used in the network, then **Use Manual DNS Entries** should be set to disabled.

7.3.2.1.3 DNS Server 1 to 3

The IP address (IPv4 or IPv6) of the DNS server should be entered if you wish to use the Fully-Qualified Host Name (hostname.domainname) or work with reverse lookup

Contact your network administrator for details of the DNS server if not known.

If no DNS server is available (special case), enter 0.0.0.0 in the input field or leave the field blank.

7.3.2.1.4 Use Manual Gateway Entries

With this setting, you can select whether the manually entered gateways (Default Gateway IPv4 and Default Gateway IPv6) should be used.

If "enabled" is selected here, the entries in Default Gateway IPv4 and Default Gateway IPv6 are used.

If "disabled" is selected, the entries in Default Gateway IPv4 and Default Gateway IPv6 are ignored.

If a DHCP server is used to distribute the network configuration and if this also distributes the address of the default gateway used in the network, then Use Manual Gateway Entries should be set to disabled.

7.3.2.1.5 Default Gateway IPv4

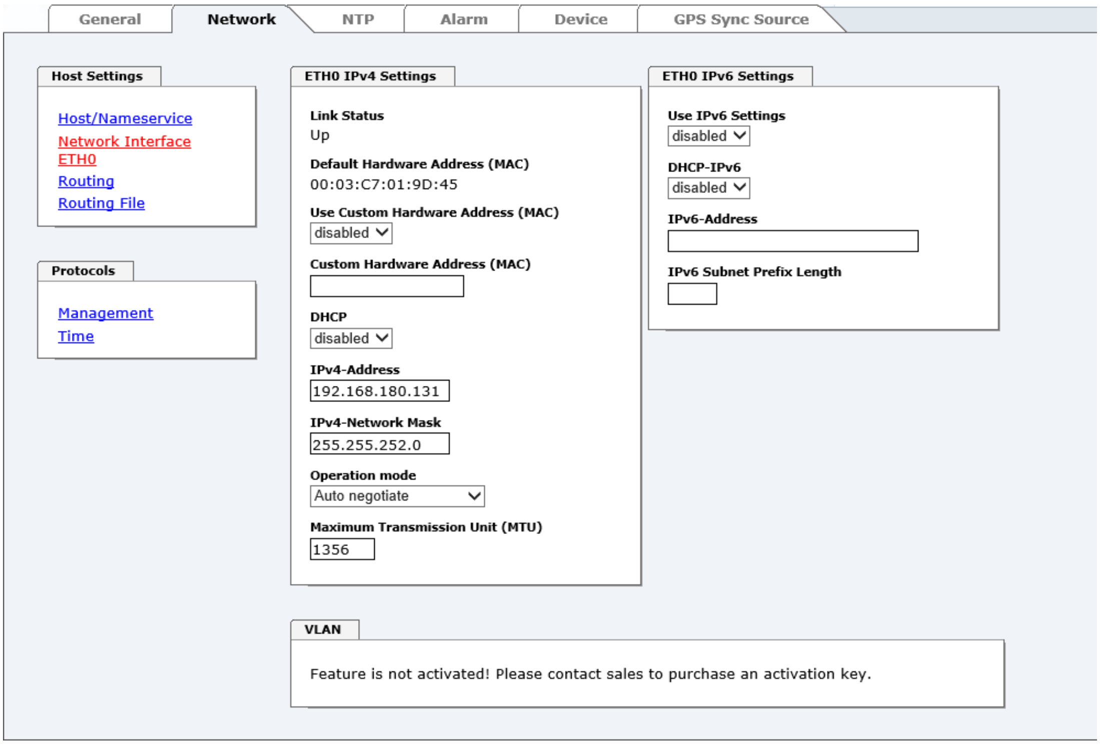
If the IPv4 default gateway is not known, it must be requested by the network administrator. If no standard gateway is available (special case), enter 0.0.0.0 in the input field or leave the field blank.

7.3.2.1.6 Default Gateway IPv6

If the Ipv6 default gateway is not known, it must be requested by the network administrator. If no standard gateway is available (special case), enter :: in the input field or leave the field blank.

7.3.2.1.7 Network Interface ETH0

Configuration of the Ethernet interface ETH0 of the Time Server 8029NTS/GPS.



Host Settings

- Host/Nameservice
- Network Interface ETH0
- Routing
- Routing File

Protocols

- Management
- Time

ETH0 IPv4 Settings

Link Status
Up

Default Hardware Address (MAC)
00:03:C7:01:9D:45

Use Custom Hardware Address (MAC)
disabled

Custom Hardware Address (MAC)

DHCP
disabled

IPv4-Address
192.168.180.131

IPv4-Network Mask
255.255.252.0

Operation mode
Auto negotiate

Maximum Transmission Unit (MTU)
1356

ETH0 IPv6 Settings

Use IPv6 Settings
disabled

DHCP-IPv6
disabled

IPv6-Address

IPv6 Subnet Prefix Length

VLAN

Feature is not activated! Please contact sales to purchase an activation key.

7.3.2.1.8 Default Hardware Address (MAC)

The factory default MAC address can only be read and cannot be changed by the user. It is assigned once only by ***hopf*** Elektronik GmbH for each Ethernet interface.

For further information about the MAC address refer to ***Chapter 2.3.4.1 MAC-Address for ETH0*** for the Time Server 8029NTS/GPS.

ℹ ***hopf*** Elektronik GmbH MAC addresses begin with **00:03:C7**:xx:xx:xx.

7.3.2.1.9 Customer Hardware Address (MAC)

The MAC address assigned from ***hopf*** can be changed to any user-defined MAC address. The board identifies itself with the user-defined MAC address to the network. The default hardware address shown in WebGUI remains unchanged.

Double assignment of MAC addresses on the Ethernet referring to customers MAC addresses should be avoided.
If the MAC address is not known, please contact your network administrator.

The use of customers MAC address needs to be activated by the function **Use Custom Hardware Address (MAC**) with **enable**.

The customers MAC address has to be entered in hexadecimal form with a colon to separateas described in the below example, e.g. **00:03:c7:55:55:02**

The MAC address assigned by ***hopf*** can be activated at any time by disabling this function.

There are no MAC multicast addresses allowed!

7.3.2.1.10 DHCP

If DHCP is to be used, activate this with **enabled**.

7.3.2.1.11 IPv4 Address

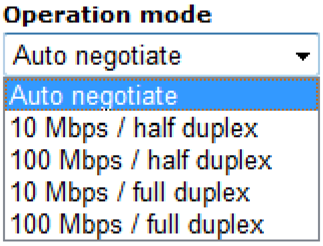
If DHCP is not used, the IPv4 address needed to be entered here. Contact your network administrator for details of the used IPv4 address if not known.

7.3.2.1.12 IPv4 Network Mask

If DHCP is not used, the network mask needed to be entered here. Contact your network administrator for details of the used network mask if not known.

7.3.2.1.13 Operation Mode

The network device usually adjusts the data stream and duplex mode to the device to which it is connected (e.g. HUB, SWITCH) automatically. If the network device requires a certain speed or duplex mode, this can be configured via the web interface. The value should only be changed in special cases. The automatic setting is normally used.



Operation mode

Auto negotiate

- Auto negotiate
- 10 Mbps / half duplex
- 100 Mbps / half duplex
- 10 Mbps / full duplex
- 100 Mbps / full duplex

In individual cases an enabled "Auto negotiate" might lead to problems between the network components and the adjustment process fails.

In such cases it is recommended to set the network speed of the Time Server 8029NTS/GPS **and** the connected network components manually to the same value.

7.3.2.1.14 Maximum Transmission Unit (MTU)

The Maximum Transmission Unit describes the maximum size of a data packet of a protocol of the network layer (layer 3 of OSI model), measured in octets which can be transferred into the frame of a net of the security layer (layer 2 of OSI model) without fragmentation.

The Time Server 8029NTS is going to be delivered with default setting 1356.

7.3.2.1.15 IPv6

The Time Server 8030NTS/GPS can also be operated in an IPv6 network.

To enable IPv6, **Use IPv6 Settings** must be set to **enable**.

IPv6 addresses are 128 bits long and they are recorded in eight 4-character hexadecimal blocks. For example: **2001:0db8:0000:08d3:1319:8a2e:0370:7344**

Leading zeroes in a 4-character hexadecimal block can be omitted. For the above example, this results in the notation: **2001:db8:0:8d3:1319:8a2e:370:7344**

In addition, **once** per IPv6 address a consecutive sequence of blocks containing all zeros may be omitted. But this must be recorded with two consecutive colons. For the above example, this gives the notation: **2001:db8::8d3:1319:8a2e:370:7344**

Another example: **2001:0:0:0:1319:8a2e:0:7344** may be represented

as **2001::1319:8a2e:0:7344**

or **2001:0:0:0:1319:8a2e::7344**

7.3.2.1.16 DHCP-IPv6

If DHCP is to be used, this function is activated with **enabled**.

7.3.2.1.17 IPv6 Address

If DHCP is not used, enter the IPv6 address here. If the IPv6 address to be used is unknown, it must be requested by the network administrator.

7.3.2.1.18 IPv6 Subnet Prefix Lengh

If no DHCP is used, the length of the network address must be entered here. If the length of the network address is not known, it must be requested by the network administrator.

7.3.2.1.19 VLAN (Activation Key necessary)

A VLAN (Virtual Local Area Network) is a logical sub-network within a network switch or a whole physical network. VLANs are used to separate the logical network infrastructure from the physical wiring, thus to virtualize the Local Area Network. The technology of VLAN is standardized by IEEE Standard 802.1q. Network applications like Time Server 8030NTS/GPS, implementing the standard IEEE 802.1q, are able to allocate individual network interfaces to specific VLANs. To transfer data packets of several VLANs via a single network interface the data packets are marked with a related VLAN ID. This method is called VLAN-Tagging. The network application at the other end of the line (e.g. network switch, router etc.) can allocate the data packet to the correct VLAN by checking the marking / tag.

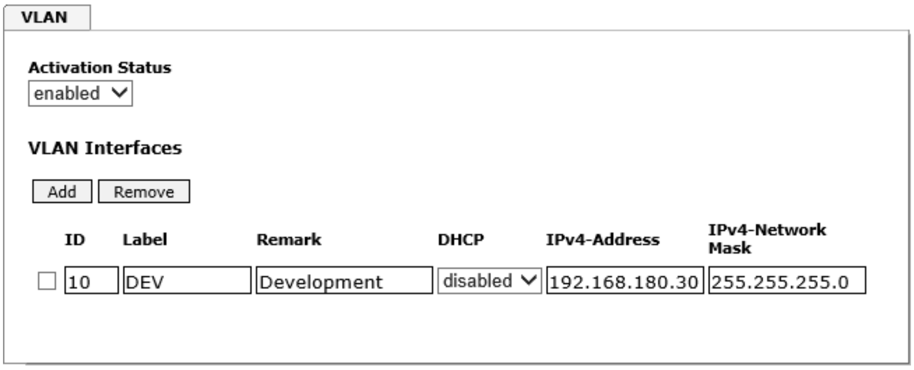
WebGUI with activated VLAN

To be able to configure VLANs the activation status must be set to "enabled" first. Afterwards up to 32 different VLANs per network interface can be configured by clicking the button "Add".

An explicit VLAN ID must be configured for each VLAN interface.

The boxes "Label" and "Remark" can be filled out with a designation or a comment to easily keep the configured VLANs apart.

Determination of the IP-address for the configured VLAN interface can either be done automatically via DHCP or by filling out the boxes "IP-Address" and "Network Mask".



Activation Status
enabled

VLAN Interfaces

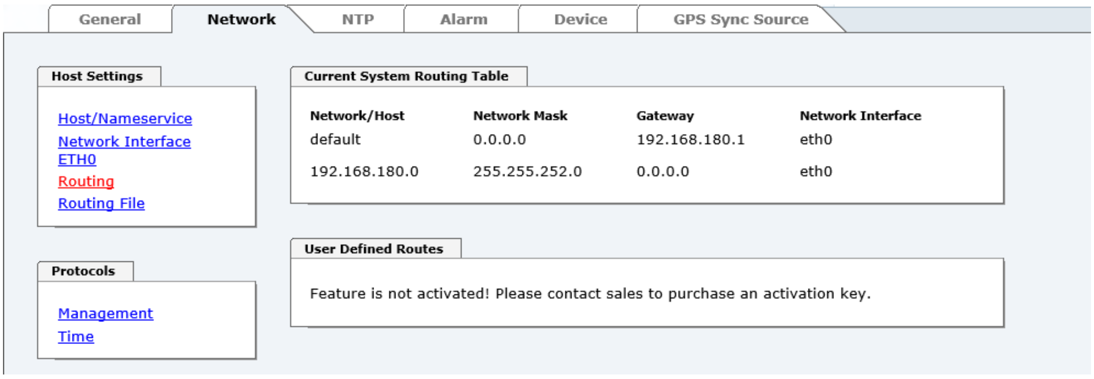
	ID	Label	Remark	DHCP	IPv4-Address	IPv4-Network Mask
□	10	DEV	Development	disabled	192.168.180.30	255.255.255.0

To ensure the correct function the network appliance must be connected with Time Server 8030NTS/GPS via the network interface. Furthermore it must be ensured that the network appliance is accurately configured with the same VLANs.

VLAN ID one (1) and two (2) are reserved and are therefore not permitted!

7.3.2.2 Routing (Activation Key necessary)

A route must be configured if the module is not only be used in the local sub-network.



Current System Routing Table

Network/Host	Network Mask	Gateway	Network Interface
default	0.0.0.0	192.168.180.1	eth0
192.168.180.0	255.255.252.0	0.0.0.0	eth0

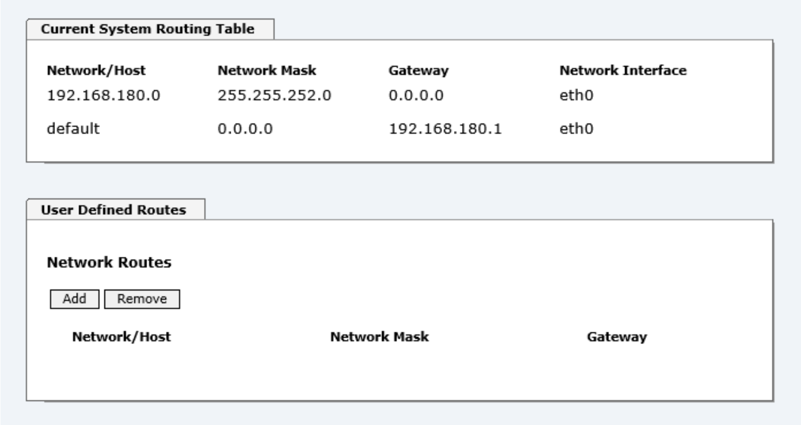
User Defined Routes

Feature is not activated! Please contact sales to purchase an activation key.

The gateway / gateway host need to be in the local sub-network range of the module in order to use the routes.

The parameterization of this feature is a critical process as an incorrect configuartion may lead to considerable problems on the network!

WebGUI with Routing activated



Current System Routing Table

Network/Host	Network Mask	Gateway	Network Interface
192.168.180.0	255.255.252.0	0.0.0.0	eth0
default	0.0.0.0	192.168.180.1	eth0

User Defined Routes

Network Routes

Network/Host	Network Mask	Gateway

The image above shows every configured route of the base system routing table as well as the user's defined routes.

The module cannot be used as a router!

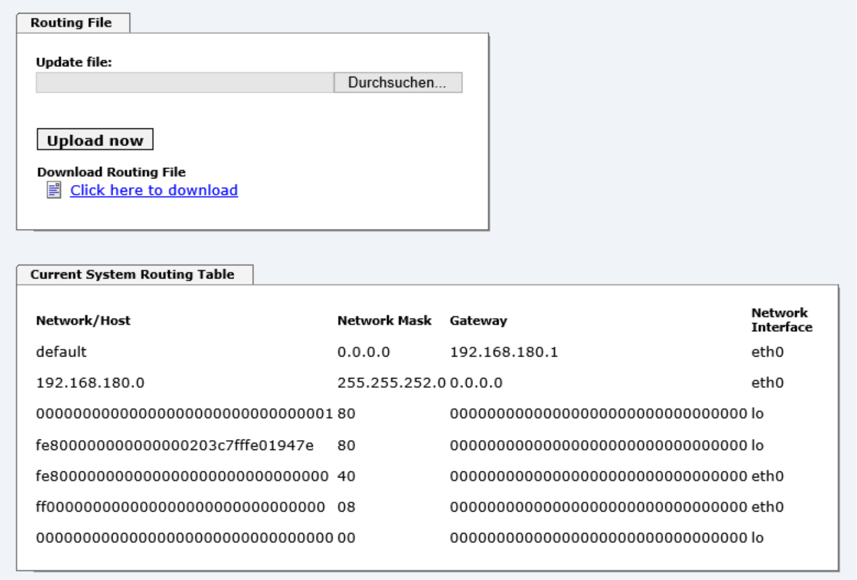
Select **Use Route File** to set whether the routing configuration set under **User Defined Routes** should be used, or routing configuration using a routing file.

If IPv6 routes are required, the routes must be made using the settings in ***Chapter 7.3.2.3 Routing File***.

7.3.2.3 Routing File

In order to activate this function, **Use Route File** must be set to **enabled** on the Routing Page.

The routing file also makes it possible to configure IPv6 routes.



Network/Host	Network Mask	Gateway	Network Interface
default	0.0.0.0	192.168.180.1	eth0
192.168.180.0	255.255.252.0	0.0.0.0	eth0
00000000000000000000000000000001	80	00000000000000000000000000000000	lo
fe800000000000000203c7fffe01947e	80	00000000000000000000000000000000	lo
fe800000000000000000000000000000	40	00000000000000000000000000000000	eth0
ff000000000000000000000000000000	08	00000000000000000000000000000000	eth0
00000000000000000000000000000000	00	00000000000000000000000000000000	lo

Via the selection window under Update file and the button Upload now a new routing file can be uploaded. When uploading the file is checked whether the file is error-free and only then it is used.

If a routing file has already been uploaded, the uploaded routing file can be downloaded under **Download Routing File**.

Routing File Syntax

Each line of the routing file must be either a valid routing line or a comment line. A comment line starts with a hash sign (#) and can contain any text behind it.

A routing line has the format [destination address] [tab] [length of the destination mask in bits] [tab] [gateway address for the specified destination].

If the host 192.168.20.11 is to be reached using the gateway 192.168.0.2, then the routing file must look like this:

```
192.168.20.11    32   192.168.0.2
```

Example of a Routing File:

```
# Host 192.168.20.11 via Gateway 192.168.0.2
192.168.20.11    32   192.168.0.2
#Net 192.168.180.0 Netmask 255.255.255.0 via Gateway 192.168.0.2
192.168.180.0    24   192.168.0.2
#Net 2001:0db8:0:f102:: Subnet Prefix Length 64 via Gateway 2001:0db8:0:f101::1
2001:0db8:0:f102::   64    2000::1
```

Current **System Routing Table**

This table shows all active IPv4 and IPv6 routes.

For IPv6 routes, the colons of the destination and gateway addresses are not displayed, and the **Network Mask** column displays the length in hexadecimal

7.3.2.4 Management (Management-Protocols – HTTP, SNMP etc.)

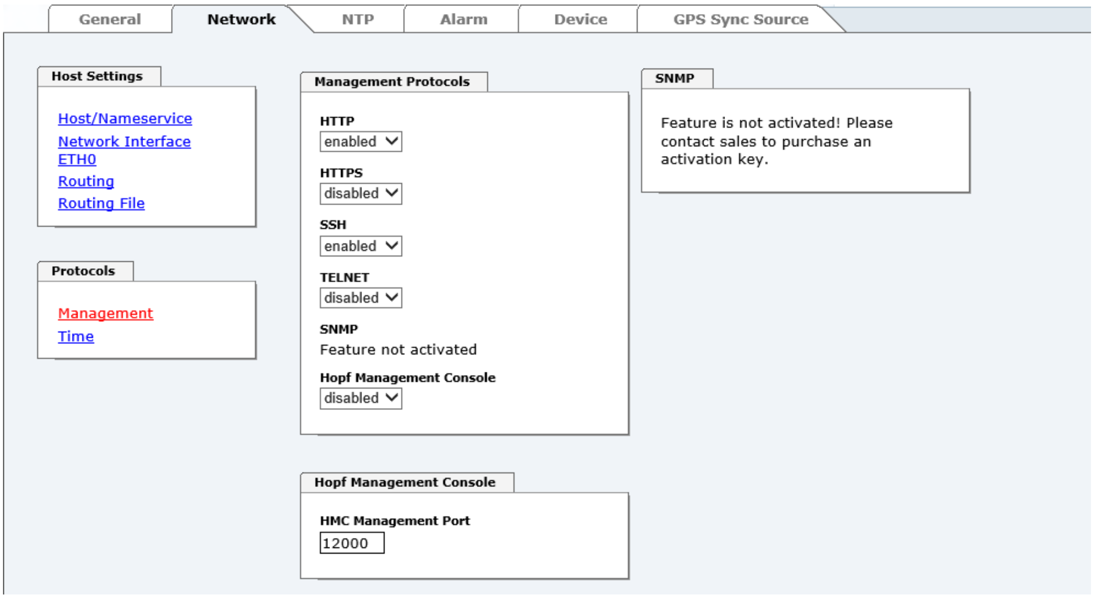
Protocols that are not required should be disabled for security reasons. A correctly configured module is always accessible via the web interface.

Changes to the availability of a protocol (enable/disable) take effect immediately.

For SNMP functionality an activation key is necessary.

If by mistake all protocol channels become "disabled", the SSH channel is automatically "enabled" after the attempt to save.

After a Factory Default the HTTP and SSH channels are "enabled".



HTTP
enabled

HTTPS
disabled

SSH
enabled

TELNET
disabled

SNMP
Feature not activated

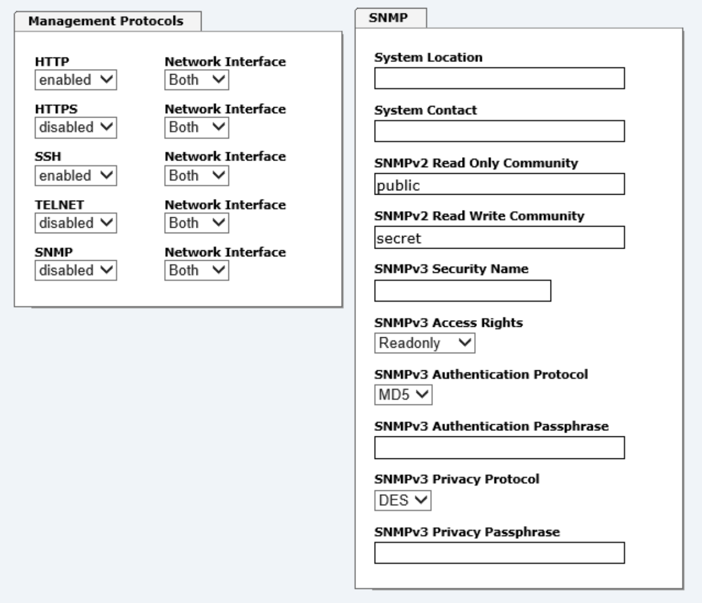
Hopf Management Console
disabled

Feature is not activated! Please contact sales to purchase an activation key.

HMC Management Port
12000

These service settings are valid globally! Services with “disabled” status are not externally accessible and are not made externally available by the module!

WebGUI with Alarming activated



Management Protocols

HTTP: enabled — Network Interface: Both
HTTPS: disabled — Network Interface: Both
SSH: enabled — Network Interface: Both
TELNET: disabled — Network Interface: Both
SNMP: disabled — Network Interface: Both

SNMP

System Location:
System Contact:
SNMPv2 Read Only Community: public
SNMPv2 Read Write Community: secret
SNMPv3 Security Name:
SNMPv3 Access Rights: Readonly
SNMPv3 Authentication Protocol: MD5
SNMPv3 Authentication Passphrase:
SNMPv3 Privacy Protocol: DES
SNMPv3 Privacy Passphrase:

Using SNMP and SNMP- traps the protocol SNMP should be enabled.

All fields must be filled in for a correct operation of SNMP. Contact your network administrator for details of data not known.

7.3.2.4.1 SNMPv2 / SNMPv3 (Activation Key required)

Both protocols SNMPv2 and SNMPv3 are supported and can be configured and enabled independently from each other.

System Location and System Contact are global settings and are valid for both protocols (SNMPv2 / SNMPv3).

In order to disable SNMPv2 both fields **SNMP Read Only Community** and **SNMP Read Write Community** must remain empty.

SNMPv2	SNMPv2 enabled	SNMPv2 disabled
Read Only Community:	set (e.g. public)	empty
Read/Write Community:	set (e.g. secret)	empty

In order to enable SNMPv3 the following fields must be set:

SNMPv3	Description
Security Name:	SNMPv3 is enabled (identical to the username)
Access Rights:	Equivalent to the Read/Write Communities in SNMPv2
Authentication Protocol:	Authentication (MD5 or SHA Hash)
Privacy Protocol:	Encryption (DES or AES Algorithm)

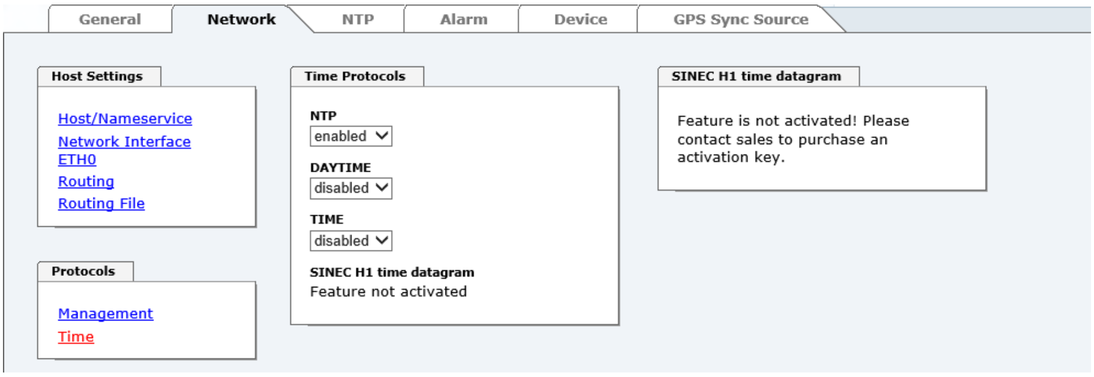
There are three security levels in SNMPv3 that can be adjusted by the removal of the passphrases:

SNMPv3	noAuthNoPriv	authNoPriv	authPriv
Authentication Passphrase:	empty	set	set
Privacy Passphrase:	empty	empty	set

Right now only one user is supported.

7.3.2.5 Time

Activation and configuration of different synchronization protocols



NTP: enabled

DAYTIME: disabled

TIME: disabled

SINEC H1 time datagram: Feature not activated

Feature is not activated! Please contact sales to purchase an activation key.

All protocols can be enabled at the same time.

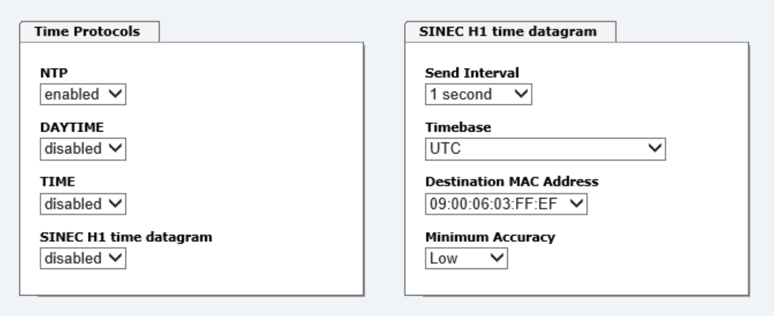
7.3.2.5.1 Synchronization Protocols (Time Protocols – NTP, SNTP etc.)

Needed time protocols can be enabeld here.

- NTP (incl. SNTP)
- DAYTIME
- TIME
- SINEC H1 time datagram (Activation key necessary)

7.3.2.5.2 SINEC H1 time datagram (Activation Key necessary)

Configuration of the SINEC H1 time datagram



Time Protocols

NTP: enabled

DAYTIME: disabled

TIME: disabled

SINEC H1 time datagram: disabled

SINEC H1 time datagram

Send Interval: 1 second

Timebase: UTC

Destination MAC Address: 09:00:06:03:FF:EF

Minimum Accuracy: Low

Broadcast transmission intervals of the SINEC H1 time datagram (Send Interval):

- every second
- every 10 second
- every 60 second

Timebase see also *Chapter 13.2.1 Time-specific expressions:*

- Local time
- UTC
- Standard time
- Standard time with daylight / standard time status

Destination MAC Address:

- 09:00:06:03:FF:EF
- 09:00:06:01:FF:EF
- FF:FF:FF:FF:FF:FF

Synchronization Status based on Starting Transmission (Minimum Accuracy)

This setting defines at which internal accuracy status the SINEC H1 time datagram should be transmitted (see ***Chapter 13.5 Accuracy & NTP Basic Principles*** and ***Chapter 11 Technical Data***):

- LOW
- MEDIUM
- HIGH

The setting Minimum Accuracy = LOW may lead to the output of non-synchronised (thus possibly wrong) time information.

7.3.3 NTP Tab

This tab shows information and adjustment possiblities of the NTP services of the Time Server 8029NTS/GPS. The NTP service is the significant main service of the Time Server 8029NTS/GPS.

If you are not familiar with the subject of NTP you can find a short description in the Glossary. More details are also available at http://www.ntp.org/.

NTP functionality is provided by an NTP-Demon running on the embedded Linux of the Time Server 8029NTS/GPS.

Depending on the receiving conditions and under unfavourable circumstances it may take several hours until long-term accuracy is obtained (normally 5-10 minutes). During this time the NTP algorithm adjusts the internal accuracy parameters.

The NTP time protocol must be enabled in order to use NTP
(see ***Chapter 7.3.2.5 Time***)

After all changes relating to NTP a restart of the NTP service must be performed (see ***Chapter 7.3.3.6 (Restart NTP)***).

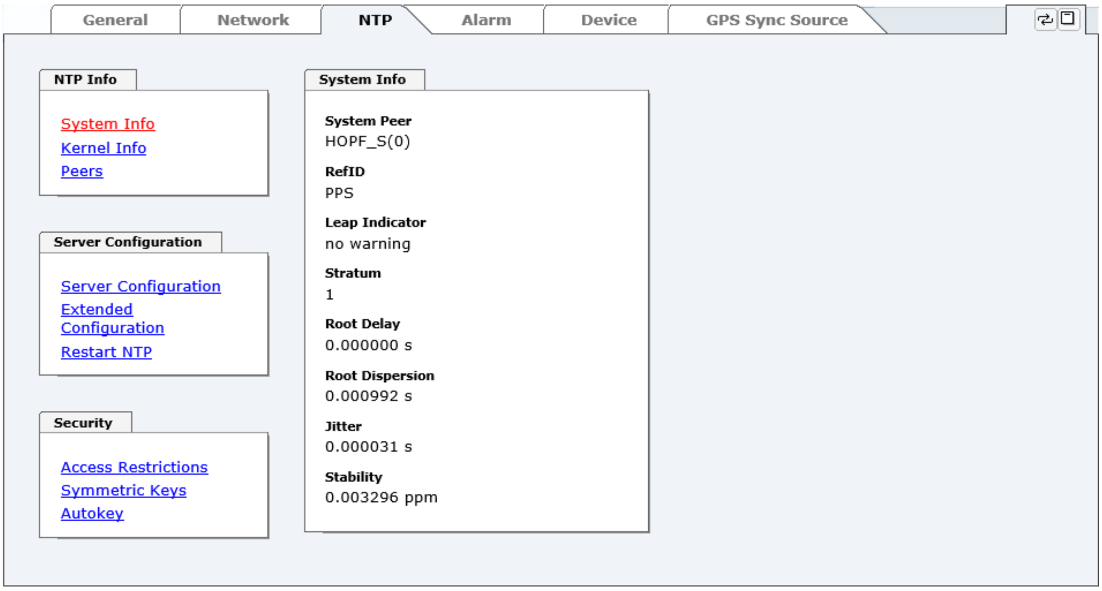
Via the NTP protocol SNTP Clients can also be synchronized. In contrast to NTP in SNTP Clients delay times are not evaluated on the network. For this reason the accuracy reached in SNTP Clients is lower than in NTP Clients.

7.3.3.1 System Info

In the window "System Info" the current NTP values of the NTP service running on the embedded Linux of the Time Server 8029NTS/GPS are indicated. In addition to the NTP calculated values for root delay, root dispersion, jitter, and stability the stratum value of the Time Server 8029NTS/GPS, the status to the leap second, and the current system peer are also found here.

The NTP version used adjusts the leap second correctly.

The Time Server 8029NTS/GPS works as NTP Server with stratum 1 and belongs to the best available class of NTP server, as it has a reference clock with direct access.



System Info

System Peer
HOPF_S(0)

RefID
PPS

Leap Indicator
no warning

Stratum
1

Root Delay
0.000000 s

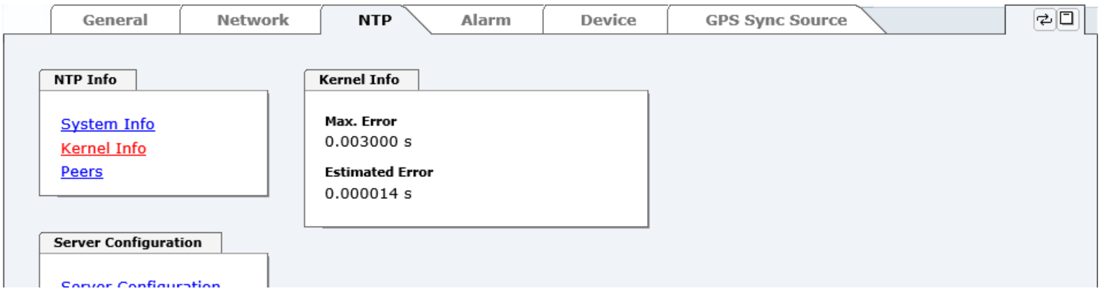
Root Dispersion
0.000992 s

Jitter
0.000031 s

Stability
0.003296 ppm

7.3.3.2 Kernel Info

The “Kernel Info” overview shows the current error values of the internal embedded Linux clock. Both values are internally updated every second.



Kernel Info

Max. Error
0.003000 s

Estimated Error
0.000014 s

This screenshot shows a maximum kernel clock error of 3.000 msec (milliseconds). The estimated error value is 14 µs (microseconds).

The values indicated here are based on the calculation of the NTP service and have no significance for the accuracy of the Sync Source (here Module 8024GPS).

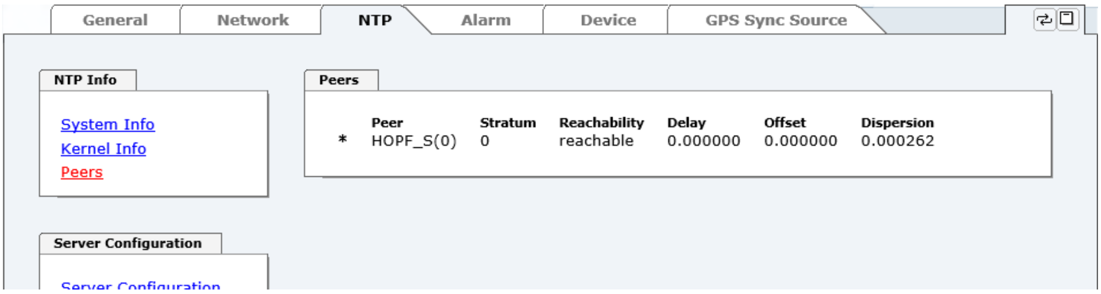
7.3.3.3 Peers

The “Peers summary” is used to track the performance of the configured NTP server/driver and the NTP algorithm itself.

The information displayed is identical with the information available via NTPQ or NTPDC programes.

Each NTP server/driver that has been set up in the NTP server configuration is displayed in the peer information.

The connection status is displayed in the reachability column (not reachable, bad, medium, and reachable).



Peers

	Peer	Stratum	Reachability	Delay	Offset	Dispersion
*	HOPF_S(0)	0	reachable	0.000000	0.000000	0.000262

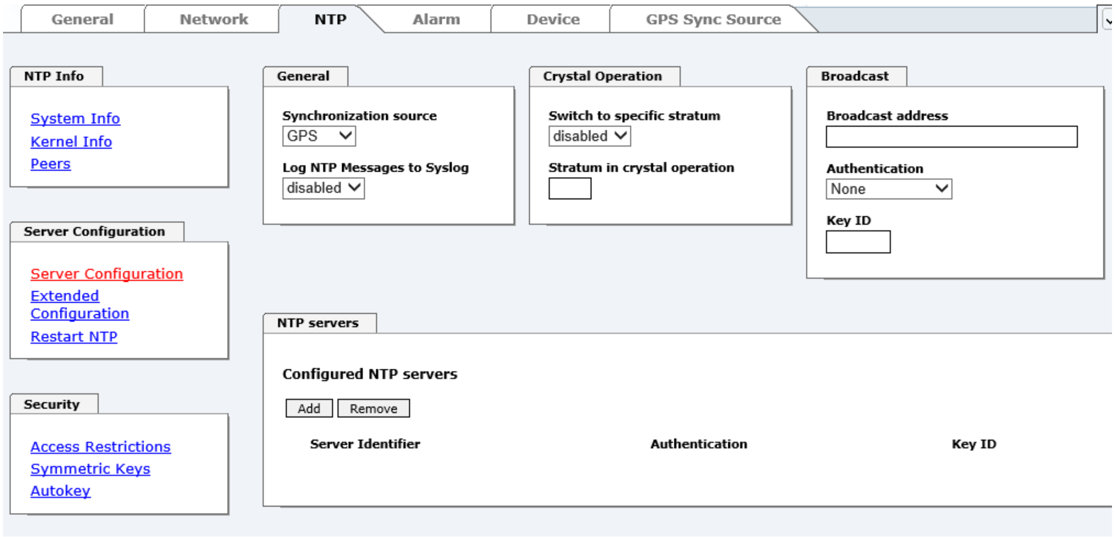
The first line displays the ***hopf* - refclock ntp driver** that gets the time information directly from the Sync Source.

A short explanation and definition of the displayed values can be found in ***Chapter 13.5 Accuracy & NTP Basic Principles***.

The character in the first column on the left presents the current status of the NTP association in the NTP selection algorithm. A list and description of possible characters can be found in the Glossary (see ***Chapter 13.2 Tally Codes (NTP-specific)***).

7.3.3.4 Server Configuration

The basic settings for NTP base functionality are displayed selecting the “Server Configuration” link.



General | Network | NTP | Alarm | Device | GPS Sync Source

NTP Info
- System Info
- Kernel Info
- Peers

Server Configuration
- Server Configuration
- Extended Configuration
- Restart NTP

Security
- Access Restrictions
- Symmetric Keys
- Autokey

General
Synchronization source: GPS
Log NTP Messages to Syslog: disabled

Crystal Operation
Switch to specific stratum: disabled
Stratum in crystal operation:

Broadcast
Broadcast address:
Authentication: None
Key ID:

NTP servers
Configured NTP servers
Add | Remove

Server Identifier	Authentication	Key ID

The NTP-hopf-refclock driver is already configured as standard (127.127.38.0 in the “Peers Summary”) and is not explicitly displayed here.

7.3.3.4.1 Synchronization Source (General / Synchronization source)

As *"Synchronization source"* either GPS or DCF77, depending on the appropriate Sync Source, has to be selected. This is reuiqred in order to align the NTP algorithm for the calculation of the accuracy with the synchronization source.

Based on the selection of GPS, even though GPS is not the source of the Sync Source (different product option) the value **HIGH** for **Accuracy** may never be reached.

7.3.3.4.2 NTP Syslog Messages (General / Log NTP Messages to Syslog)

This option enables or disables Syslog messages which are generated from the NTP service.

This value has no effect if Syslog is not configured in the ALARM tab (see ***Chapter 7.3.4.1 Syslog Configuration***).

7.3.3.4.3 Crystal Operation

Crystal Operation / Switch to Specific Stratum

If the Sync Source (here Module 8024GPS) runs in crystal operation (status "crystal") the NTP service of the Time Server 8029NTS/GPS usually behaves in the way that the receipt of time information is stopped from the Sync Source and the stratum value reset to 16 (defined as invalid in NTP).

NTP Clients do not accept time information from a NTP Time Server with stratum 16 (invalid). Briefly, as long as the Time Server 8029NTS/GPS indicates the stratum value 16, NTP Clients are not synchronized.

This behaviour of NTP during crystal operation of the Sync Source can be changed. Therefore the function "*Switch to specific stratum*" should be enabled by setting the value to "*enabled*" and the so-called downgrading stratum (= stratum value of the Time Server 8029NTS/GPS during crystal operation of the Sync Source).

For the sychronization of NTP Clients during crystal operation of the Sync Source or for testing the system without connected synchronization source, in the setting "*enabled*" any stratum value between 1 and 15 can be set.

Crystal Operation / Stratum in Crystal Operation

The value defined here (range 1-15) designates the transmitted fallback NTP stratum level of the module in "*Quartz*" synchronization status. Stratum 1 should be configured if downgrading is not desired in status "Quartz".

The NTP service MUST also be restarted (see ***Chapter 7.3.3.6 Restart NTP***).

Using the option "*Switch to specific stratum*" the NTP Clients are synchronized with time information indicated in the general menu of the WebGUI of the Sync Source (here Module 8024GPS) during crystal operating. Whether this time information (e.g. through drift) is imprecise or the time is manually set (wrong) cannot be detected by the NTP Client!

In case the value 1 is used for *"Stratum in crystal operation"*, the NTP Client cannot not verify whether the Time Server 8029NTS/GPS is synchronised or runs in crystal operation. Should a differentiation be wished between synchronized and crystal operation the downgrading stratum needs to be set to a value between 2 and 15.

The value is only adjustable if the "*Switch to specific stratum*" function is enabled.

7.3.3.4.4 Broadcast / Broadcast Address

This section is used to configure the Time Server 8029NTS/GPS as a broadcast or multicast server.

The broadcast mode in NTPv3 and NTPv4 is limited to clients on the same sub-network and Ethernets which support broadcast technology.

This technology does not generally extend beyond the first hop (network node - such as router or gateway).

The broadcast mode is provided for configurations which are designed to facilitate one or more servers and as many clients as possible in a sub-network. The server continuously generates broadcast messages at defined intervals, corresponding to 16 seconds (minpoll 4) for Time Server 8029NTS/GPS. Care should be taken to ensure that the correct broadcast address is used for the sub-network, usually xxx.xxx.xxx.255 (e.g. 192.168.1.255). If the broadcast address is not known, this can be requested from the network administrator.

This section can also be used to configure the Time Server 8029NTS/GPS as a multicast server. The configuration of a multicast server is similar to that of a broadcast server. However, a multicast group address (class D) is used instead of the broadcast address.

An explanation of multicast technology goes beyond the scope of this document.

In principle, a host or router sends a message to an IPv4 multicast group address and expects all hosts and routers to receive this message. In doing so, there is no limit to the number of senders and receivers and a sender may also be a receiver and vice-versa. The IANA has assigned the multicast group address IPv4 224.0.1.1 to the NTP, however this should only be used if the multicast range can be safely limited in order to protect neighbouring networks. As a basic principle, administratively manageable IPv4 group addresses should be used as described in RFC-2365 or GLOP group addresses as described in RFC-2770.

7.3.3.4.5 Broadcast / Authentication / Key ID

Broadcast packets can be protected by authentication for security reasons.

If a security method is selected here, this must be configured **additionally** in the security settings of the NTP tab. A key must be defined if the Symmetric Key is selected.

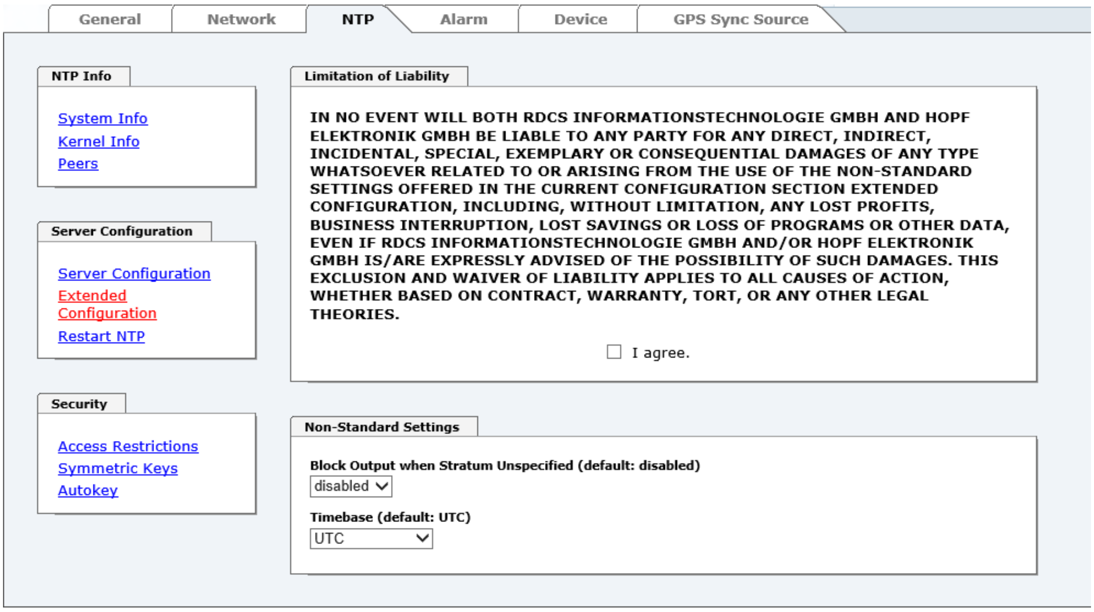
7.3.3.4.6 Additional NTP SERVERS

Adding further NTP servers provides the opportunity to implement a security system for the time service. However, this affects the accuracy and stability of the Time Server 8029NTS/GPS.

Detailed information on this subject can be found in the NTP documentation (http://www.ntp.org/).

7.3.3.5 Extended NTP Configuration

NTP is a standard for synchronising clocks in computer systems via packet-based communication networks. For special applications a NON standard setting can be configured.



Limitation of Liability

IN NO EVENT WILL BOTH RDCS INFORMATIONSTECHNOLOGIE GMBH AND HOPF ELEKTRONIK GMBH BE LIABLE TO ANY PARTY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY TYPE WHATSOEVER RELATED TO OR ARISING FROM THE USE OF THE NON-STANDARD SETTINGS OFFERED IN THE CURRENT CONFIGURATION SECTION EXTENDED CONFIGURATION, INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOST SAVINGS OR LOSS OF PROGRAMS OR OTHER DATA, EVEN IF RDCS INFORMATIONSTECHNOLOGIE GMBH AND/OR HOPF ELEKTRONIK GMBH IS/ARE EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS EXCLUSION AND WAIVER OF LIABILITY APPLIES TO ALL CAUSES OF ACTION, WHETHER BASED ON CONTRACT, WARRANTY, TORT, OR ANY OTHER LEGAL THEORIES.

☐ I agree.

Non-Standard Settings

Block Output when Stratum Unspecified (default: disabled)
disabled

Timebase (default: UTC)
UTC

For activation of this special NTP setting, the customer's approval shown in the WebGUI needed to be declared by checking the field "I agree".

7.3.3.5.1 Suppression of unspecified NTP Outputs (Block Output when Stratum Unspecified)

Unspecified NTP outputs that e.g. are generated by NTP at a restart are suppressed when this function is enabled.

7.3.3.5.2 NTP Timebase

For custom applications this function enables adjustment of the time base of the NTP output.

Entering this function the transmitted time protocol of the modul 8029NTS is not conform to the NTP standard anymore.
According to the NTP standard NTP uses only the UTC time base. The NTP time protocol does not allow any leaps in time.

This function is only allowed for the Output of NTP
In case of activated function the output of the module 8029NTS for *SINEC H1 TIME DATAGRAM / TIME / DAYTIME* is released with a wrong time basis. Therefore this datagram should be deactivated for security reasons.

Following configuration steps for the activation of the NTP time basis are required:

- Select the wished NTP time base.
- Transfer the setting with **Apply Changes** to the modul 8029NTS.
- Fail-save storage of the configuration by pressing **Save to Flash within 10 seconds**.
  Depending on the activated time base leap a board reset might be released after transfer with Apply Changes eliminating non saved configurations.

UTC - NTP with Time Basis UTC

According to the RFC standard NTP uses only the UTC time base.

Standard Time - NTP with the Time Base Standard Time

Using the NTP time protocol with the standard time base the released time information correspond with UTC plus the time difference, adjusted in the base system **without** considering the daylight saving time changeover.

Local Time - NTP with the Time Base Local Time

Output of the NTP time protocol with the local time base the released time information correspond with UTC plus the time difference and the additional offset for the possible summer time, adjusted in the base system.

NTP does not allow any leaps in time. Using the NTP time protocol with the local time base the internal NTP process of a board is restarted based on a summer-/winter time adjustment.

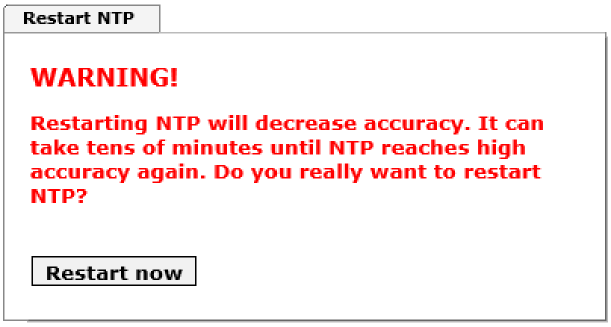
Using the NTP time protocol with the local time base the summer-/winter time adjustment is released one to two minutes belated.

Afterwards the local time is correctly available in the NTP time protocol. Therefore, within this transition period a requested NTP time protocol is replied by the former time base.

Changing the time base for the output of the protocol for NTP is only designed for customized applications and does not correspond with the standard of NTP. The synchronisation of a standard NTP-Client with a time basis deviating from UTC results in a wrong time information in the standard NTP-Client and might cause time leaps!

7.3.3.6 Restart NTP

The following screen appears after clicking on the Restart NTP option:



WARNING!

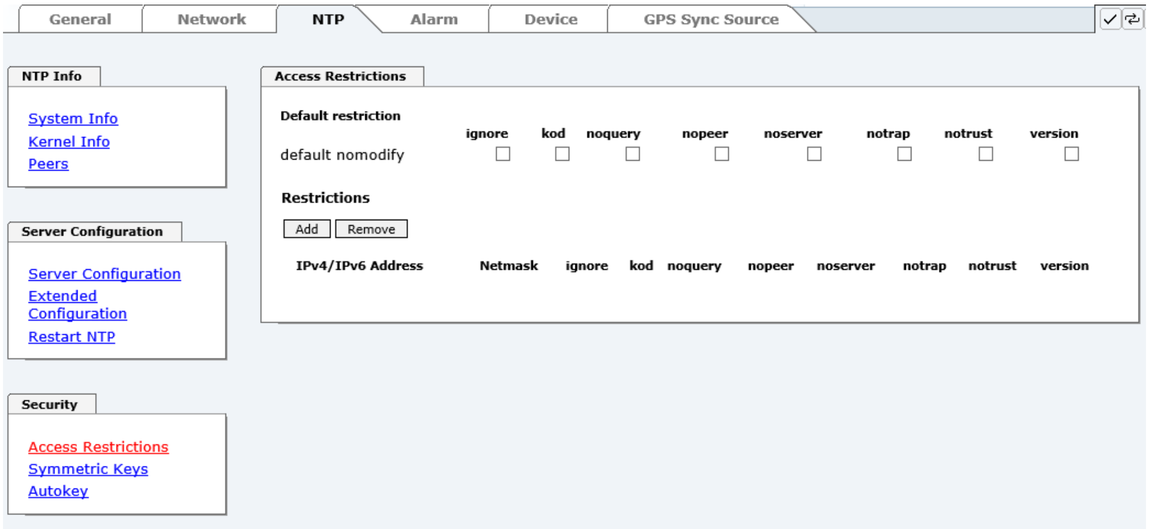
Restarting NTP will decrease accuracy. It can take tens of minutes until NTP reaches high accuracy again. Do you really want to restart NTP?

Restarting NTP services is the only possibility of making NTP changes effective without having to restart the entire Time Server 8029NTS/GPS. As can be seen from the warning message, the currently reachable stability and accuracy get lost caused by this restart.

⚠ After a restart of the NTP service it takes up to 10 minutes until the NTP service on the Time Server 8029NTS/GPS is completely adjusted.

7.3.3.7 Configuring the NTP Access Restrictions

One of the extended configuration options for NTP is the "Access Restrictions" (NTP access restictions).



Default restriction

	ignore	kod	noquery	nopeer	noserver	notrap	notrust	version
default nomodify	☐	☐	☐	☐	☐	☐	☐	☐

Restrictions

Add Remove

IPv4/IPv6 Address	Netmask	ignore	kod	noquery	nopeer	noserver	notrap	notrust	version

Restrictions are used in order to control access to the System's NTP service and these are regrettably the most misunderstood options of the NTP configuration.

If you are not familiar with these options, a detailed explanation can be found at http://www.ntp.org/.

IP addresses should be used when configuring the restrictions – no Hostnames!

The following steps show how restrictions can be configured - should these not be required it is sufficient to retain the standard settings.

The standard restrictions tell the NTP service how to handle packets of hosts (including remote time servers) and sub-network which otherwise have no special restrictions.

The NTP configuration can simplify the selection of the correct standard restrictions while making the required security available.

Before beginning the configuration the points ***7.3.3.7.1*** to ***7.3.3.7.4*** must be checked by the user:

7.3.3.7.1 NAT or Firewall

Are incoming connections to the NTP Service blocked by NAT or a Stateful Inspection Firewall?	
No	Proceed to ***Chapter 7.3.3.7.2 Blocking Unauthorised Access***
Yes	No restrictions are required in this case. Proceed further to ***Chapter 7.3.3.7.4 Internal Client Protection / Local Network Threat Level***

7.3.3.7.2 Blocking Unauthorised Access

Is it really necessary to block all connections from unauthorised hosts if the NTP Service is openly accessible?	
No	Proceed to ***Chapter 7.3.3.7.3 Allowing Client Requests***
Yes	In this case the following restrictions are to be used: **ignore in the default restrictions** ☑ If a standard restriction is selected in this area, exceptions can be declared in separate lines for each authorised server, client or sub-network. See ***Chapter 7.3.3.7.5 Addition of Exceptions to Standard***

7.3.3.7.3 Allowing Client Requests

Are clients to be allowed to see the server status information when they receive the time information from the NTP service (even if this is information about the module, operating system and NTPD version)?	
No	In this case select from the following standard restrictions: See ***Chapter 7.3.3.7.6 Access Control Options*** **kod** ☑ **notrap** ☑ **nopeer** ☑ **noquery**. ☑
Yes	In this case select from the following standard restrictions: See ***Chapter 7.3.3.7.6 Access Control*** Options: **kod** ☑ **notrap** ☑ **nopeer** ☑ If a standard restriction is selected in this area, exceptions can be declared in separate lines for each authorised server, client or sub-network. See ***Chapter 7.3.3.7.5 Addition of Exceptions to Standard .***

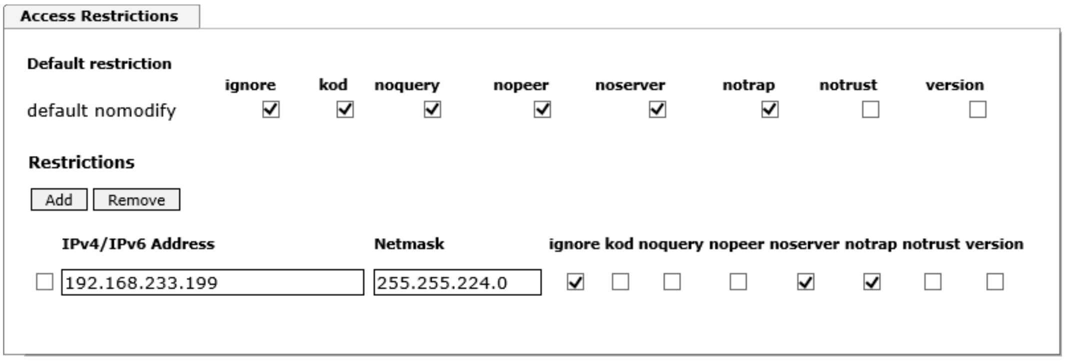
7.3.3.7.4 Internal Client Protection / Local Network Threat Level

How much protection from internal network clients is required?	
Yes	The following restrictions can be enabled if greater security settings than the installed authentication are required in order to protect the NTP service from the clients see ***Chapter 7.3.3.7.6 Access Control Options.*** **kod** ☑ **notrap** ☑ **nopeer** ☑

7.3.3.7.5 Addition of Exceptions to Standard Restrictions

After the standard restrictions have been set once, certain exceptions may be necessary for special hosts/sub-networks in order to allow remote time servers and client hosts/sub-networks to contact the NTP service.

These standard restrictions are to be added in the form of restriction lines.



Access Restrictions

Default restriction

	ignore	kod	noquery	nopeer	noserver	notrap	notrust	version
default nomodify	☑	☑	☑	☑	☑	☑	☐	☐

Restrictions

Add | Remove

	IPv4/IPv6 Address	Netmask	ignore	kod	noquery	nopeer	noserver	notrap	notrust	version
☐	192.168.233.199	255.255.224.0	☑	☐	☐	☐	☑	☑	☐	☐

An unrestricted access of the Time Server 8029NTS/GPS to its own NTP service is always allowed, irrespective of whether standard restrictions are ignored or not. This is necessary in order to be able to display NTP data on the web interface.

Add restriction exception: (for each remote time server)

Restrictions: Press **ADD**

Enter the IP address of the remote time server.

Enable restrictions: e.g.

notrap / nopeer / **noquery** ☑

Allow **unrestricted access** to a special host (e.g. System administrator's workstation):

Restrictions: Press **ADD**

IP address 192.168.1.101

Do not enable any restrictions

Allow a **sub-network** to receive time server and query server statistics:

Restrictions: Press **ADD**

IP address 192.168.1.0

Network mask 255.255.255.0

notrap / nopeer ☑

The entry of exceptions also works for IPv6 addresses. For this, the IPv6 address must be entered in the column IPv4/IPv6 Address and the length of the IPv6 net mask must be entered in the Netmask column.

7.3.3.7.6 Access Control Options

The official documentation concerning the current implementation of the restriction instructions can be found on the "Access Control Options" page at http://www.ntp.org/.

Numerous access control options are used. The most important of these are described in detail here.

nomodify – "Do not allow this host/sub-network to modify the NTPD settings unless it has the correct key."

> **Default Settings**:
> Always active. Can't be modified by the user.

As standard, NTP requires authentication with a symmetric key in order to carry out modifications with NTPDC. If a symmetric key is not configured for the NTP service, or if this is kept in a safe place, it is not necessary to use the nomodify option unless the authentication procedure appears to be unsafe.

noserver – "Do not transmit time to this host/sub-network."
This option is used if a host/sub-network is only allowed access to the NTP service in order to monitor or remotely configure the service.

notrust – "Ignore all NTP packets which are not encrypted."
This option tells the NTP service that all NTP packets which are not encrypted should be ignored (it should be noted that this is a change from ntp-4.1.x). The notrust option MUST NOT be used unless NTP Crypto (e.g. symmetric key or Autokey) has been correctly configured on both sides of the NTP connection (e.g. NTP service and remote time server, NTP service and client).

noquery – "Do not allow this host/sub-network to request the NTP service status."
The ntpd status request function, provided by ntpd/ntpdc, declassifies certain information over the running ntpd Base System (e.g. operating system version, ntpd version) which under certain circumstances ought not to be made known to others. It must be decided whether it is more important to hide this information or to give clients the possibility of seeing synchronization information over ntpd.

ignore – "In this case ALL packets are refused, including ntpq and ntpdc requests".

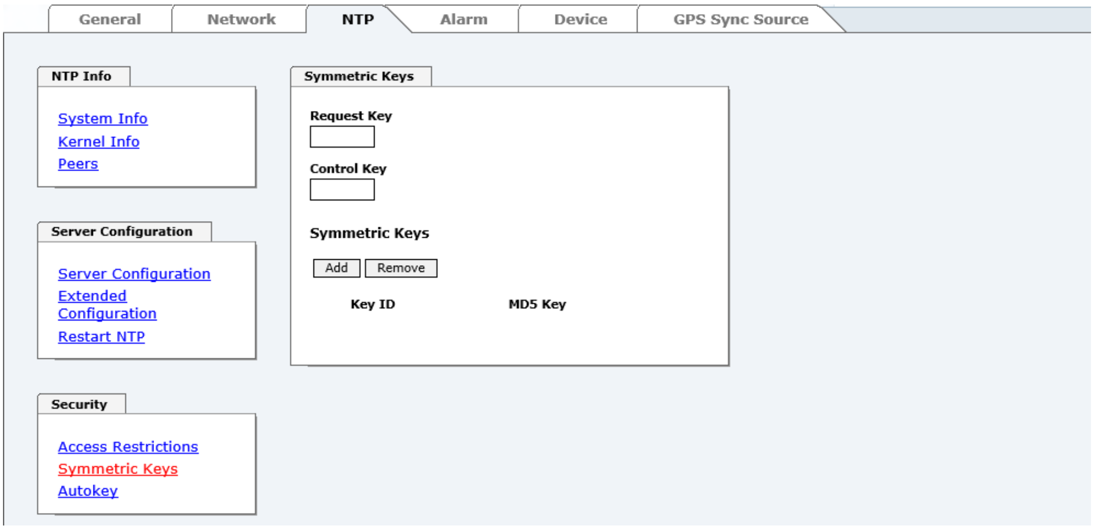
kod – "A kiss-o'-death (KoD) packet is transmitted if this option is enabled in the case of an access error."
KoD packets are limited. They cannot be transmitted more frequently than once per second. Any KoD packet which occurs within one second from the last packet is removed.

notrap – "Denies support for the mode 6 control message trap service in order to synchronise hosts."
The trap service is a sub-system of the ntpq control message protocols. This service logs remote events in programmes.

version – "Denies packets which do not correspond to the current NTP version."

> Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service MUST also be restarted (see ***Chapter 7.3.3.6 Restart NTP***).

7.3.3.8 Symmetric Key



7.3.3.8.1 Why Authentication?

Most NTP users do not require authentication as the protocol contains several filters (for bad time).

Despite this, however, the use of authentication is common. There are certain reasons for this:

- Time should only be used from safe sources
- An attacker broadcasts false time signals
- An attacker poses as another time server

7.3.3.8.2 How is Authentication used in the NTP Service?

Client and server can execute an authentication whereby a code word is used on the client side and a restriction on the server side.

NTP uses keys to implement the authentication. These keys are used when data are exchanged between two machines.

In principle both sides must know this key. The key can generally be found in the "*.*/etc/ntp.keys" directory. It is unencrypted and hidden from public view. This means that the key has to be distributed on a safe route to all communication partners. The key can be downloaded for distribution under "Downloads / Configuration Files" on the DEVICE tab. It is necessary to be logged in as "Master" in order to access this.

The keyword key of a client’s ntp.conf determines the key that is used to communicate with the designated server (e.g. the Time Server 8029NTS/GPS). The key must be reliable if time is to be synchronised. Authentication causes a delay. This delay is automatically taken into account and adjusted in the current versions.

7.3.3.8.3 How is a key created?

A key is a sequence of up to 31 ASCII characters. Some characters with special significance cannot be used (alphanumeric characters and the following symbols can be used: **. , ! " $ % & / { } [ ] ( ) = ? \ + - @ * ~ # ' < > | ; : _**

A new line can be inserted by pressing the **ADD** key. The key which is stored in the key file is entered on this line. The key ID is used to identify the key and is in the range from 1 – 65534. This means that 65534 different keys can be defined.

Duplicate key ID's are not allowed. Having now explained the principles of keys, it should be possible to use a key in practically the same way as a password.

The value of the request key field is used as the password for the ntpdc tool while the value of the control key field is used as the password for the ntpq tool.

More information is available at http://www.ntp.org/.

7.3.3.8.4 How does authentication work?

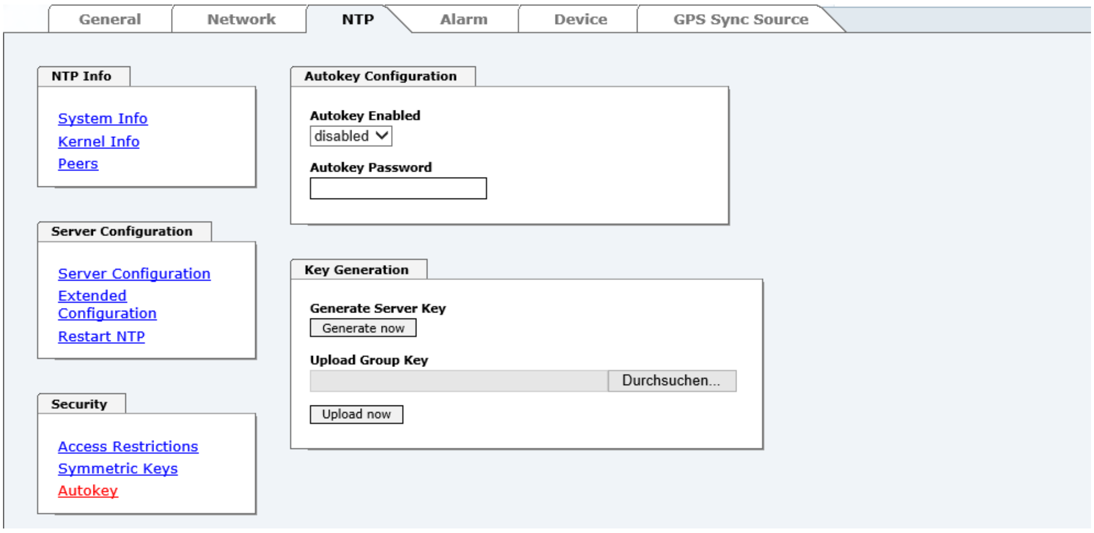
The basic authentication is a digital signature and no data encryption (if there are any differences between the two). The data packet and the key are used to create a non-reversible number which is attached to the packet.

The receiver (which has the same key) carries out the same calculation and compares the results. Authentication has been successful if the results agree.

7.3.3.9 Autokey

NTPv4 offers a new Autokey scheme based on **public key cryptography**.

As a basic principle, **public key cryptography** is safer than **symmetric key cryptography** as protection is based on a private value which is generated by each host and is never visible.



Autokey Configuration

Autokey Enabled: disabled

Autokey Password:

Generate Server Key

Upload Group Key

In order to enable Autokey v2 authentication, the “Autokey Enabled” option must be set to "enabled" and a password specified (may not be blank).

A new server key and certificate can be generated by pressing the "Generate now" button.

> **Generate now**
> This should be carried out regularly as these keys are only valid for one year.

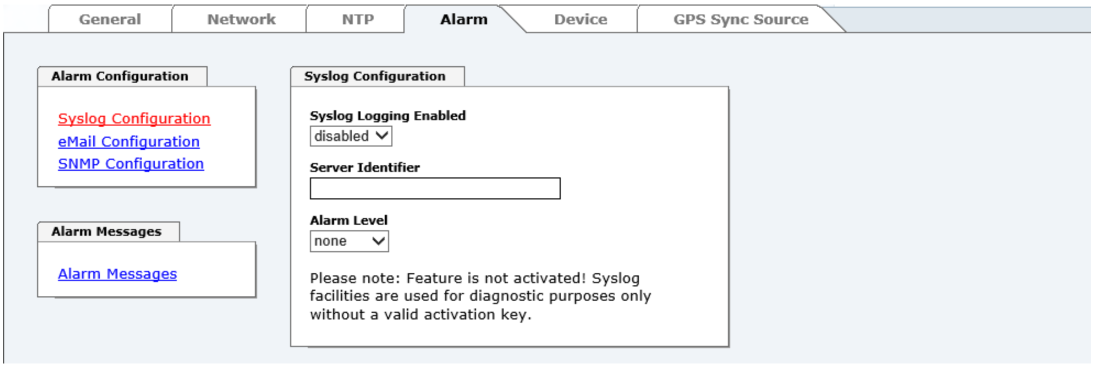
If the Time Server 8029NTS/GPS is to form part of an NTP trust group, a group key can be defined and uploaded with the "Upload now" button.

Detailed information about the NTP Autokey scheme can be found in the NTP documentation (http://www.ntp.org/).

> Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service MUST also be restarted (see ***Chapter 7.3.3.6 Restart NTP***).

7.3.4 ALARM Tab (Activation Key necessary)

All the links within the tab on the left hand side lead to corresponding detailed setting options.



Syslog Logging Enabled: disabled

Server Identifier:

Alarm Level: none

Please note: Feature is not activated! Syslog facilities are used for diagnostic purposes only without a valid activation key.

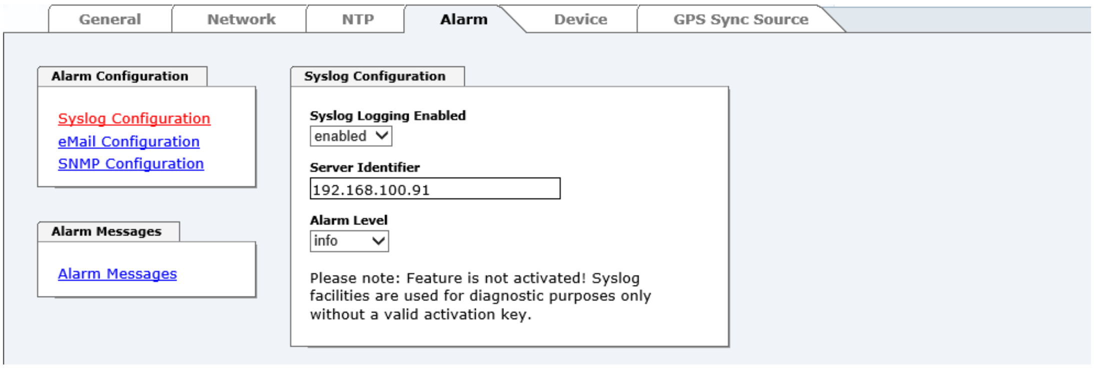
7.3.4.1 Syslog Configuration

It is necessary to enter the name or IPv4 or IPv6 address of a Syslog server in order to store every configured alarm situation which occurs on the module in a Linux/Unix Syslog. If everything is configured correctly and enabled (depending on the Syslog level), every message is transmitted to the Syslog server and stored in the Syslog file there.

Syslog uses Port 514.

Co-logging in the system itself is not possible as therefore the internal memory is not of sufficient size.

It should be noted that the standard Linux/Unix Syslog mechanism is used for this functionality. This is not the same as the Windows System Event mechanism!



Syslog Logging Enabled: enabled

Server Identifier: 192.168.100.91

Alarm Level: info

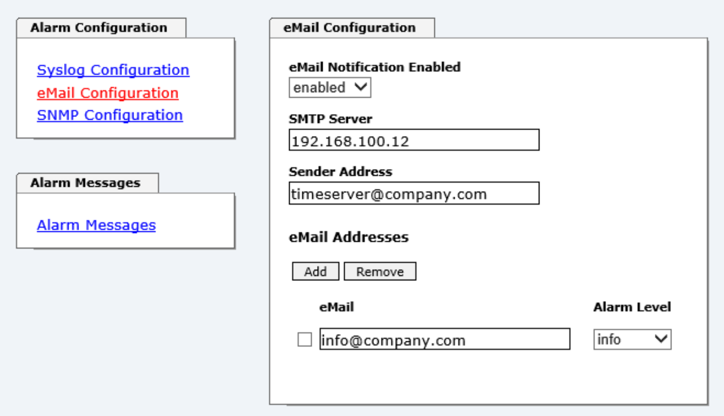
Please note: Feature is not activated! Syslog facilities are used for diagnostic purposes only without a valid activation key.

The alarm level designates the priority level of the messages to be transmitted and the level from which transmission should take place (see ***Chapter 7.3.4.4 Alarm Messages***).

Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm

The NTP service implemented in the system can transmit its own Syslog messages (see ***Chapter 7.3.3.4.2 NTP Syslog Messages (General / Log NTP Messages to Syslog)***).

7.3.4.2 E-mail Configuration



eMail Notification Enabled: enabled

SMTP Server: 192.168.100.12

Sender Address: timeserver@company.com

eMail Addresses

	eMail	Alarm Level
□	info@company.com	info

E-mail notification is one of the important features of this device which offers technical personnel the opportunity to monitor and/or control the IT environment.

It is possible to configure various, independing E-mail addresses which each have different alarm levels.

Dependending on the configured level, an E-mail is sent after an error has occurred on the respective receiver.

A valid E-mail server (SMTP server) must be entered for the purpose of correct configuration.

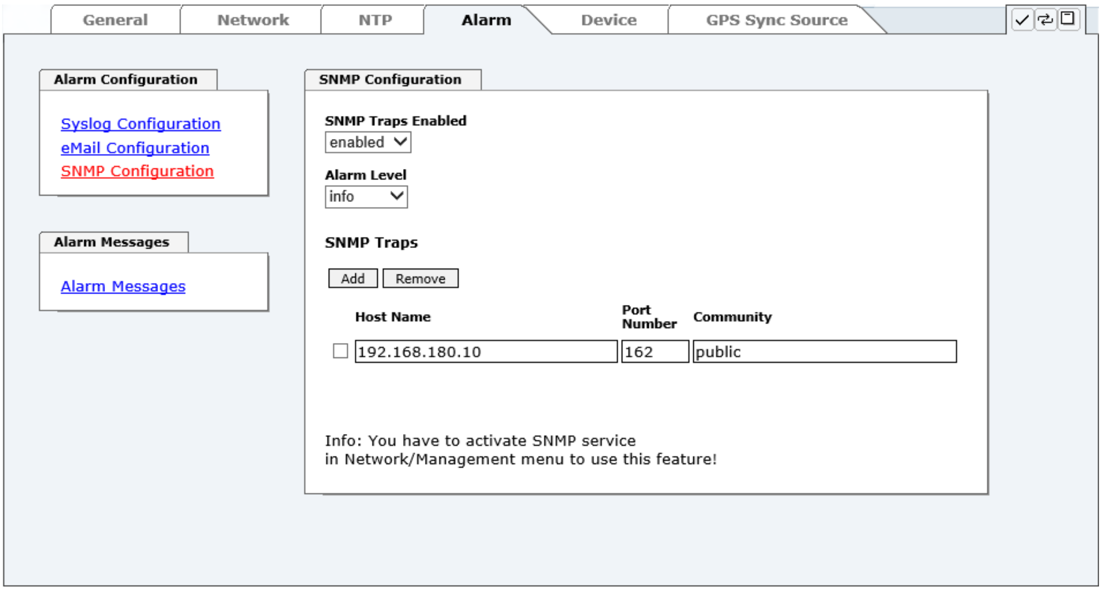
Some E-mail servers only accept messages if the sender address entered is valid (spam protection). This can be inserted in the “Sender Address” field.

The Alarm Level designates the priority level of the messages to be sent and determines from which level the message should be sent (see ***Chapter 7.3.4.4 Alarm Messages***).

Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm

7.3.4.3 SNMP Configuration / TRAP Configuration

It is possible to use an SNMP agent (with MIB) or to configure SNMP traps in order to monitor the module over SNMP.



SNMP Traps Enabled: enabled

Alarm Level: info

SNMP Traps

	Host Name	Port Number	Community
□	192.168.180.10	162	public

Info: You have to activate SNMP service
in Network/Management menu to use this feature!

SNMP traps are sent to the configured hosts over the network. It should be noted that these are based on UDP and therefore it is not certain that they will reach the configured host!

Several hosts can be configured. However, all have the same alarm level.

The private ***hopf*** enterprise MIB is also available over the web (see ***Chapter 7.3.5.6 Downloading Configuration Files / SNMP*** MIB).

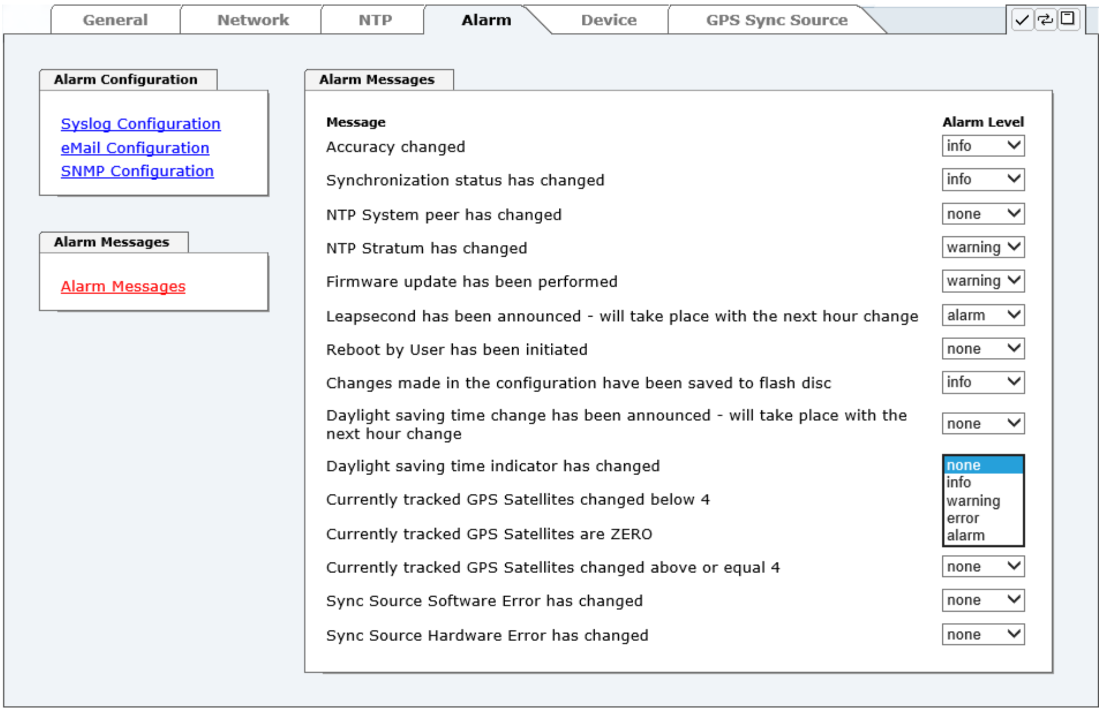
The Alarm Level designates the priority level of the messages to be sent and determines from which level the message should be sent (see ***Chapter 7.3.4.4 Alarm Messages***).

Alarm Level	**Transmitted Messages**
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm

The SNMP protocol must be enabled in order to use SNMP (see ***Chapter 7.3.2.4 Management (Management-Protocols – HTTP, SNMP etc.)***).

7.3.4.4 Alarm Messages

Every message shown in the image can be configured with the displayed alarm levels. Selection of the level NONE means that this message is completely ignored.



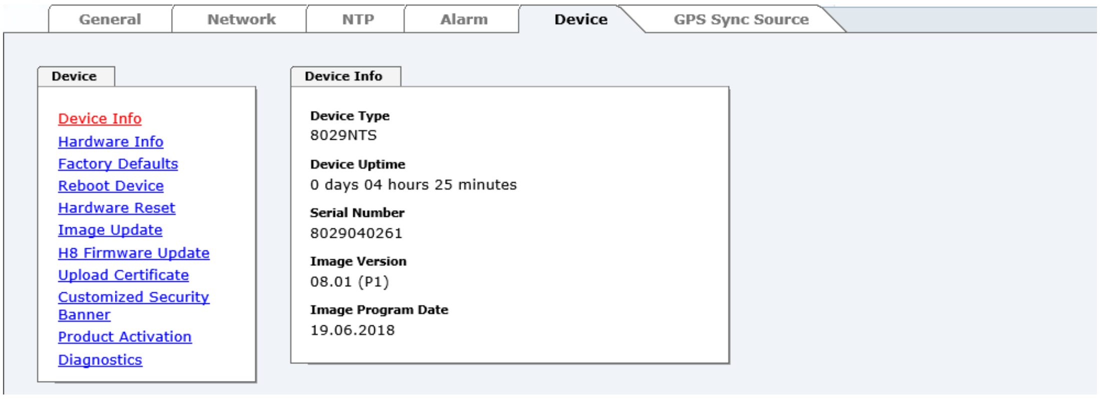
Message	Alarm Level
Accuracy changed	info
Synchronization status has changed	info
NTP System peer has changed	none
NTP Stratum has changed	warning
Firmware update has been performed	warning
Leapsecond has been announced - will take place with the next hour change	alarm
Reboot by User has been initiated	none
Changes made in the configuration have been saved to flash disc	info
Daylight saving time change has been announced - will take place with the next hour change	none
Daylight saving time indicator has changed	none info warning error alarm
Currently tracked GPS Satellites changed below 4	
Currently tracked GPS Satellites are ZERO	
Currently tracked GPS Satellites changed above or equal 4	none
Sync Source Software Error has changed	none
Sync Source Hardware Error has changed	none

Depending on the messages, their configured levels and notifications levels of the E-mails, a corresponding action is carried out if an event occurs.

Modified settings are failsafe stored after **Apply** and **Save** only.

7.3.5 DEVICE Tab

All the links within the tab on the left hand side lead to corresponding detailed setting options.



Device Type
8029NTS

Device Uptime
0 days 04 hours 25 minutes

Serial Number
8029040261

Image Version
08.01 (P1)

Image Program Date
19.06.2018

This tab provides the basic information about the hardware of Module 8029NTS as well as software/firmware. Password administration and the update services for the module are also made accessible via this website. The complete download zone is also a component of this site.

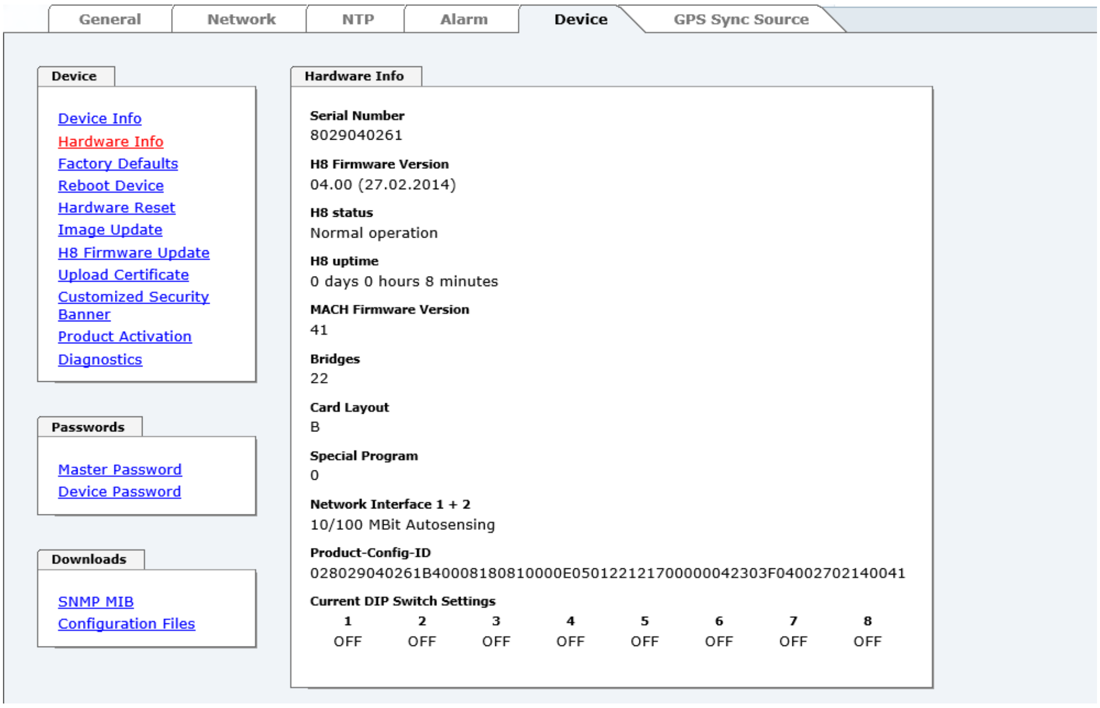
7.3.5.1 Device Information

All information is available exclusively in write-protected and read-only form. Details on the board type, serial number and current software versions are provided to the user for service and enquiry purposes.

7.3.5.2 Hardware Information

Read-only access is provided here in the same way as for device information.

The user requires this information in the case of service requests, e.g. MACH version, hardware status etc.



Serial Number
8029040261

H8 Firmware Version
04.00 (27.02.2014)

H8 status
Normal operation

H8 uptime
0 days 0 hours 8 minutes

MACH Firmware Version
41

Bridges
22

Card Layout
B

Special Program
0

Network Interface 1 + 2
10/100 MBit Autosensing

Product-Config-ID
028029040261B40008180810000E050122121700000042303F04002702140041

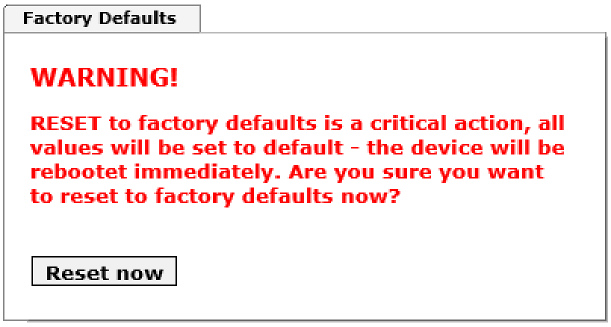
Current DIP Switch Settings

1	2	3	4	5	6	7	8
OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF

The display "Current DIP Switch Settings" is not applicable for this device.

7.3.5.3 Restoring the Factory Defaults Settings

In some cases it may be necessary or wished to reset all settings of module 8029NTS to factory settings (factory defaults).



Factory Defaults

WARNING!

RESET to factory defaults is a critical action, all values will be set to default - the device will be rebootet immediately. Are you sure you want to reset to factory defaults now?

This function serves to reset all values in the flash memory to their factory default values. This also includes passwords (see ***Chapter 12.1 Factory Default Values of Module 8029NTS (Device)***).

Please log in as a “Master” user in accordance with the description in ***Chapter 7.2.1 LOGIN and LOGOUT as User***

Pressing the "**Reset now**" button releases setting of the factory default values.

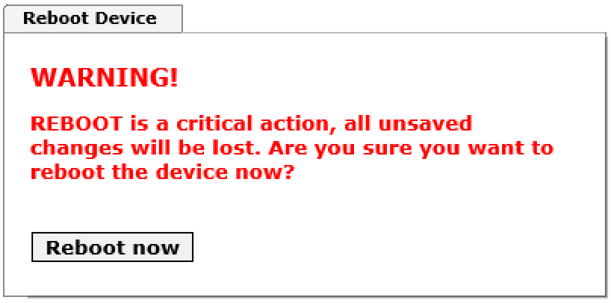
Once this procedure has been triggered there is NO possibility of restoring the deleted configuration.

A **Factory Default** requires a complete check and optionally a new configuration of the Module 8029NTS. In particulary the default MASTER and DEVICE passwords should be reset.

7.3.5.4 Restarting the Module (Reboot Device / Hardware Reset)

The restart concerns the Module 8029NTS only but **not** the Sync Source (here Module 8024GPS).

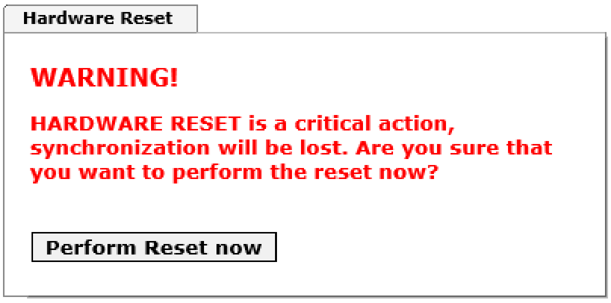
Reboot Device: Restart of the internal Operating System



WARNING!

REBOOT is a critical action, all unsaved changes will be lost. Are you sure you want to reboot the device now?

Hardware Reset: Board Reset including all Hardware components



WARNING!

HARDWARE RESET is a critical action, synchronization will be lost. Are you sure that you want to perform the reset now?

All settings **not** saved with "**Save**" are lost on reboot (see ***Chapter 7.2.3 Enter or Changing Data***).

Moreover the **NTP service** implemented in the system is restarted. This leads to a renewed alignment phase with the loss of the stability and accuracy reached up to this point.

Log in is carried out as "Master" user in accordance with the description in ***Chapter 7.2.1 LOGIN and LOGOUT as User***.

Press the "**Reboot now**" button and wait until the restart has been perfomed.

7.3.5.5 Image Update for Module 8029NTS (WebGUI: Device)

Patches and Bug Fixes are provided for the individual boards by means of updates.

The embedded image is loaded only via the web interface in the Time Server 8029NTS/GPS (log in as “master” user required). See also ***Chapter 4.4 Firmware Update***.

The following points should be considered regarding updates:

- Only experienced users or trained technical personnel should carry out a board update after checking all necessary preconditions.
- Important: **Faulty updates** or **update attempts** may, under certain circumstances, require the module to be returned to the factory for repair at customer’s expense.
- Is the update on hand suitable for the module? If there are any doubts please consult the support of the ***hopf*** company.
- In order to guarantee a correct update, the "***New version of saved site***" function must be set to "***On each access to the site***" on the Internet browser used.
- During the update procedure, the device **must not be switched off** not **settings be saved to the flash memory**!
- Updates are **<u>always</u>** carried out as Software SETs. That means that all programmes included in the SET must be downloaded to the system.
- For the update pay attention to point described in ***Chapter 4.4 Firmware Update***

In order to carry out an update, enter the name and the folder in which the update / firmware image is located in the text field or open the file selection dialogue by pressing the "Browse" button.

Correct firmware and image designations are (e.g.):

8024A_v0101_128**.mot**

for the **H8 firmware** (update takes approx. 1-1.5 minutes)

upgrade_8029-SERI_gen_rel_v06xx**.img**

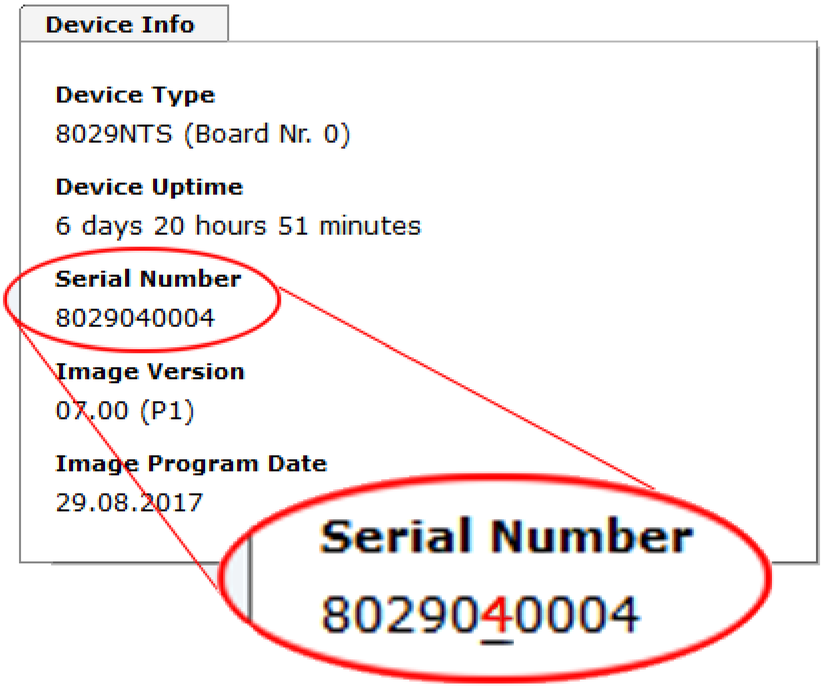
or upgrade_8029-NAND_gen_rel_v0800**.img**

for the **embedded image** (update takes approx. 2-3 minutes)

7.3.5.5.1 Select Image Update

ATTENTION
Important note for the identification of the required image update!

In order to select the correct image update, the **digit marked red** of the serial number must be checked!



Device Info

Device Type
8029NTS (Board Nr. 0)

Device Uptime
6 days 20 hours 51 minutes

Serial Number
8029040004

Image Version
07.00 (P1)

Image Program Date
29.08.2017

Required ZIP archive for the Image Update:

Red marked digit = 1	**Red marked digit = 4**
hopf8029NTS-V2-SERI_GPS_SET_v06xx.zip	**hopf8029NTS-V2-NAND_GPS_SET_v08xx.zip**
Content of the ZIP archive • 8024A_128_v01xx.mot • readme_8029NTS-V2-SERI_GPS.txt • release-notes_8029NTS-V2-SERI_GPS.html • **upgrade_8029-SERI_gen_rel_v06xx.img**	Content of the ZIP archive • 8024A_128_v01xx.mot • readme_8029NTS-V2-NAND_GPS.txt • release-notes_8029NTS-V2-NAND_GPS.html • **upgrade_8029-NAND_gen_rel_v08xx.img**

7.3.5.5.2 Installation Image Update

The update process is started by pressing the "**Update now**" button. The update is installed if the transfer and checksum test are successful. A success page is displayed and shows the number of bytes that have been transferred and installed.

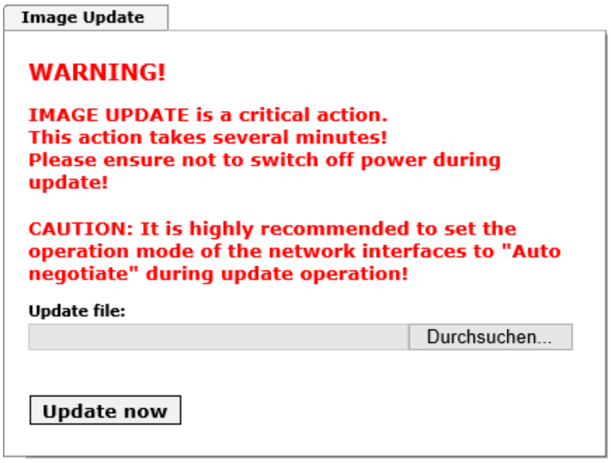


Image Update

WARNING!

IMAGE UPDATE is a critical action.
This action takes several minutes!
Please ensure not to switch off power during update!

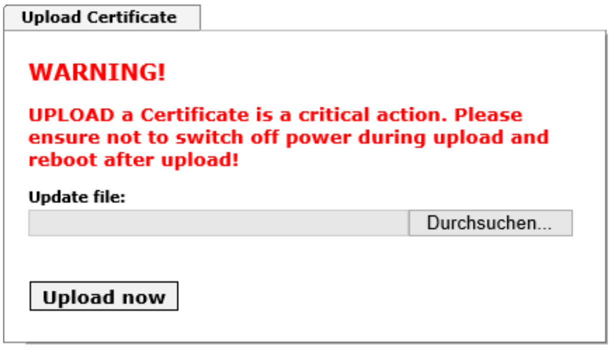
CAUTION: It is highly recommended to set the operation mode of the network interfaces to "Auto negotiate" during update operation!

Update file:

After the image-update the WebGUI displays a window to confirm the reboot of the Time Server 8029NTS/GPS.

7.3.5.1 Upload von Anwender SSL-Server-Zertifikat (Upload Certificate)

Hiermit besteht die Möglichkeit die https-Verbindungen zum Gerät mit einem vom Anwender zur Verfügung gestellten SSL-Server-Zertifikat zu verschlüsseln.



Upload Certificate

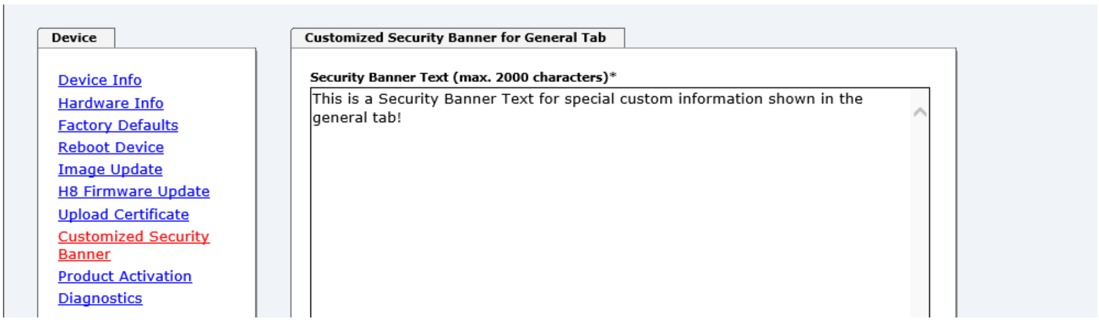
WARNING!

UPLOAD a Certificate is a critical action. Please ensure not to switch off power during upload and reboot after upload!

Update file:

7.3.5.2 Customized Security Banner

Special security information displayed in the General tab can be entered here by the user.



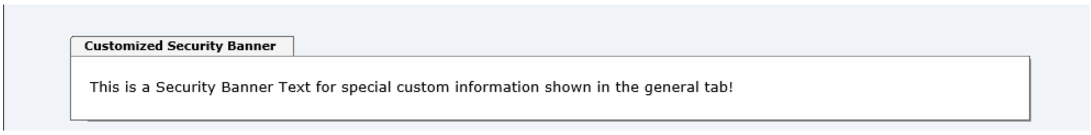
Security Banner Text (max. 2000 characters)*

This is a Security Banner Text for special custom information shown in the general tab!

The security information can be written as 'unformatted' text. There are 2000 characters available to write failsafe into the device.

When saving the text, only the following characters are accepted (all other characters are discarded and therefore not displayed on the General page!):

- Capital letters (A…Z)
- Lowercase letters (a…z)
- Numbers (0…9)
- The following special characters: space (" "), exclamation mark ("**!**"), Comma ("**,**"), dot ("**.**"), Colon ("**:**"), question mark ("**?**")



This is a Security Banner Text for special custom information shown in the general tab!

After a successful storage the "Customized Security Banner" with the saved security information is displayed in the General-Tab.

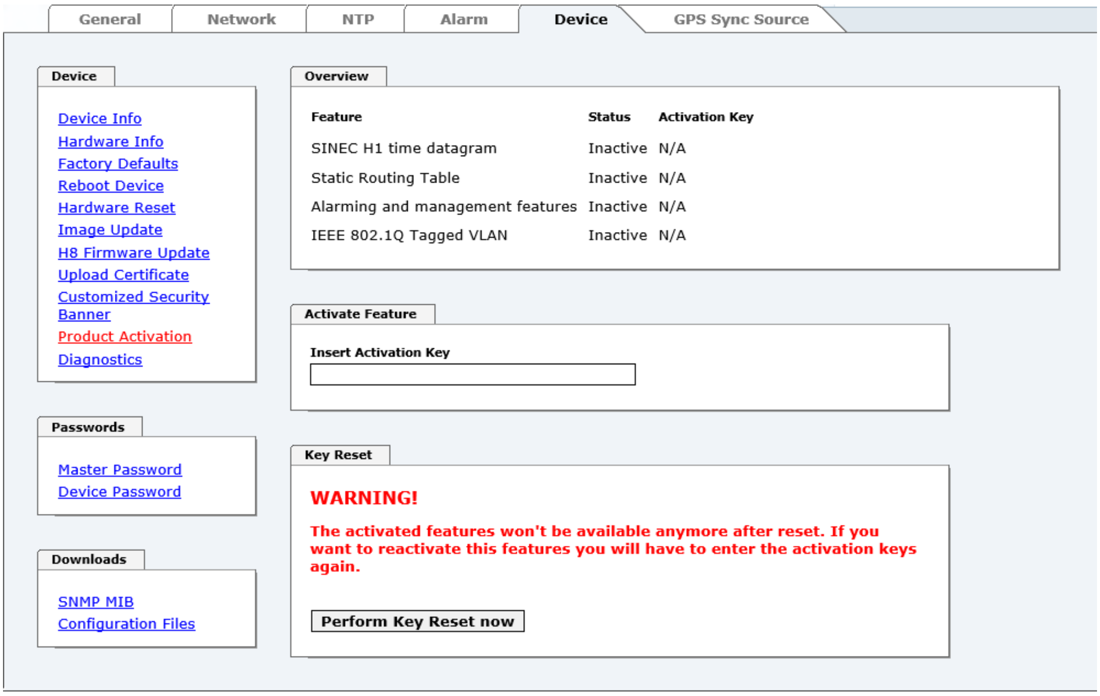
To delete the "Customized Security Banner" the inserted text must be deleted and saved again.

7.3.5.3 Product Activation

For the activation of optional functions, e.g "alarming" or "SINEC H1 time datagram", a special activation key is required for which an order with the ***hopf*** Elektronik GmbH can be placed. Each activation key is related to a special board with an appropriate serial number and cannot be used for several boards.

For a subsequent order of an activation key the serial number of the Module 8029NTS (device) needs to be provided. The serial number can be found under the tab DEVICE – Device info (serial number 8029…).

The settings for activation keys (e.g. an entered activation key) are neither deleted nor restored via the function FACTORY DEFAULTS.



Overview

Feature	Status	Activation Key
SINEC H1 time datagram	Inactive	N/A
Static Routing Table	Inactive	N/A
Alarming and management features	Inactive	N/A
IEEE 802.1Q Tagged VLAN	Inactive	N/A

Activate Feature

Insert Activation Key

Key Reset

WARNING!

The activated features won't be available anymore after reset. If you want to reactivate this features you will have to enter the activation keys again.

Overview

Full listening of all optional functions with the current activation status and stored activation key

Activate Feature

Input field to enter a new activation key. After entering the feature is activated by pressing the ☑ Apply button.

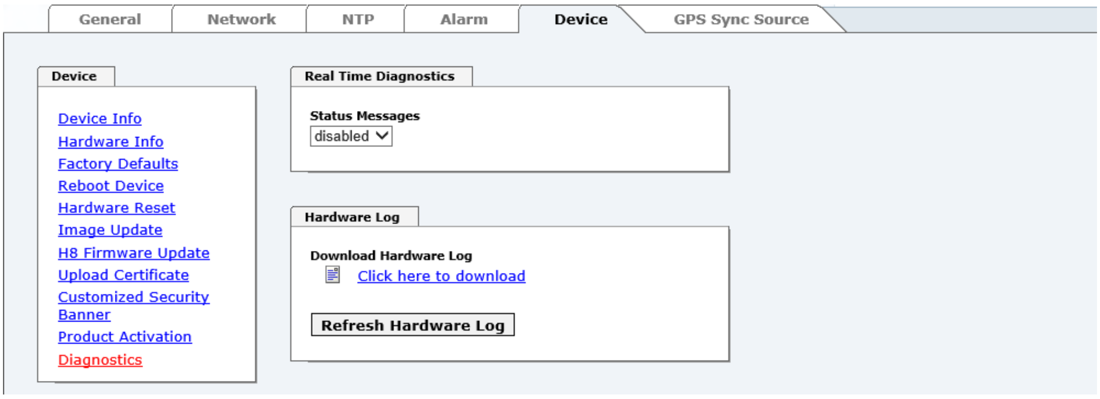
If the activation was successful the new feature is listed in the overview with status “Active” and can be used immediately.

Key Reset

Clears all activation keys and sets all optional features to status “Inactive”. All other non-optinal features are still available after peforming the key reset. If an optional feature is enabled again, the last stored configuration for this feature is restored.

7.3.5.4 Diagnostics Function

It "status messages" is enabled the output is processed as SYSLOG message. This function should only be used/enabled in case a problem arises and after consulting the ***hopf*** support.



Status Messages: disabled

7.3.5.5 Passwords (Master/Device)

Differentiation is made between upper and lower case characters in passwords. In principle, all alphanumeric characters and the following symbols are allowed in passwords:

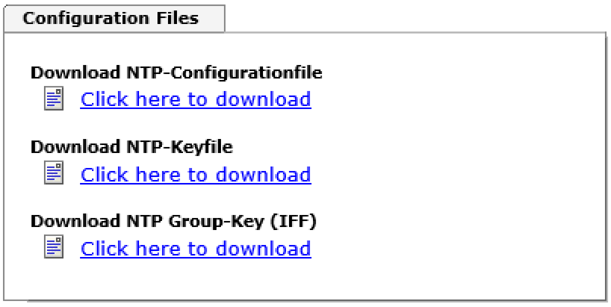
. , ! " $ % & / { } [ ] ( ) = ? \ + - @ * ~ # ' < > | ; : _

(See also ***Chapter 7.2.1 LOGIN and LOGOUT as User***)

A new password must contain at least one capital letter and lowercase letter, a number, and six characters.

7.3.5.6 Downloading Configuration Files / SNMP MIB

In order to be able to download certain configuration files via the web interface, it is necessary to be logged on as a **"master"** user.

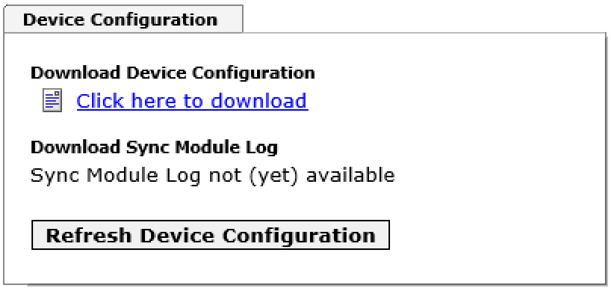


Configuration Files

Download NTP-Configurationfile
Click here to download

Download NTP-Keyfile
Click here to download

Download NTP Group-Key (IFF)
Click here to download



Device Configuration

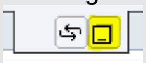
Download Device Configuration
Click here to download

Download Sync Module Log
Sync Module Log not (yet) available

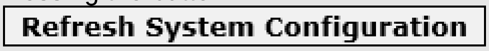
The loaded files **System Configuration** and **Sync Module Log** from the module is only used for support purposes and cannot be reloaded for adjusting the settings in the Time Server 8029NTS/GPS.

For the download of the files **System Configuration** and **Sync Module Log** the following process is mandatory:

1. Pressing the button **SAVE**

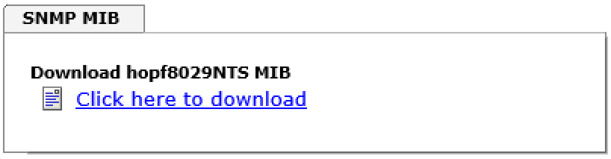


2. Pressing the button



3. Perform the download of the file

The "private ***hopf*** enterprise MIB" is also available via the WebGUI in this area.



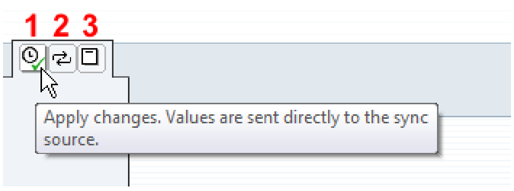
SNMP MIB

Download hopf8029NTS MIB
Click here to download

7.3.6 GPS SYNC SOURCE Tab

The complete display and parameterization of the Sync Source (here Module 8024GPS) takes place in this tab.

The modified values in the tab GPS SYNC SOURCE are directly transferred to the Module 8024GPS (Sync Source) by pressing the button 1 and failsafe stored in Module 8024GPS. This behaviour is indicated on the modified display of the Apply button. The buttons 2 and 3 are without function in the tab GPS SYNC SOURCE and are not required.

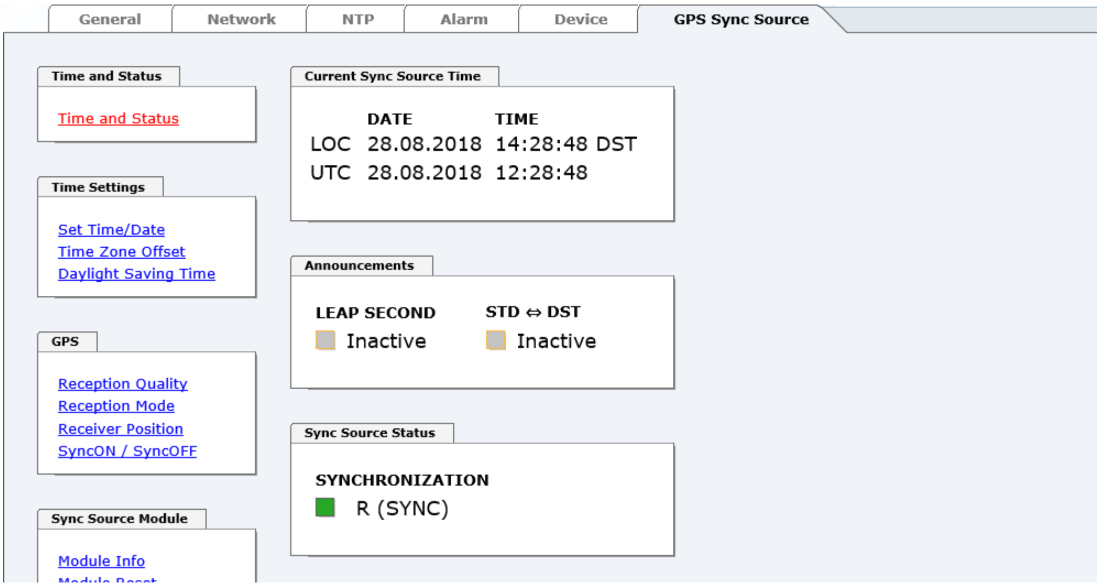


After the data transfer to 8024GPS it can take up to 30 seconds until the modified data are re-read from 8029NTS for the WebGUI indication.

This delayed indication has no effect on the functionality.

Generally it is recommended to perform a restart of the the Sync Source (here Module 8024GPS) with a **Module Reset** after performing all modifications. This ensures that the Module 8024GPS will be operated with the new and failsafe stored data.

7.3.6.1 Time and Status



Current Sync Source Time

	DATE	TIME
LOC	28.08.2018	14:28:48 DST
UTC	28.08.2018	12:28:48

Announcements

LEAP SECOND	STD ⇔ DST
□ Inactive	□ Inactive

Sync Source Status

SYNCHRONIZATION
🟩 R (SYNC)

Current Sync Source Time

This area indicates the curent time and date of the Sync Source. Both the local and UTC time are displayed.

> ❗ In theory, depending on the synchronization status of the Sync Source, the time displayed here can differ from the NTP time since two independent time systems are involved.

Announcements

The display fields LEAP SECOND and STD ⇔ DST announce a corrosponding event to the next hour (insertion of a leap-second or rather switch-over of summer/winter time).

Sync Source Status

Display of the actual status of synchronization of the Sync Source with these possible values:

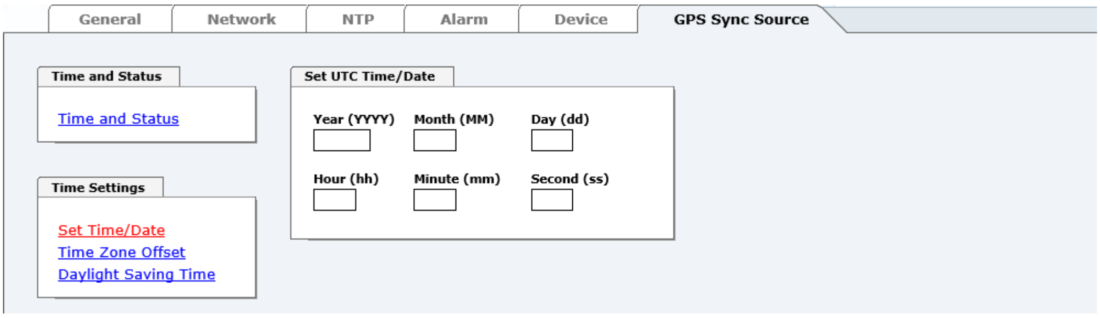
SYNC	Time synchronized + Quartz regulation started/running
SYOF	Time synchronized + SyncOFF running
SYSI	Time synchronized as simulation mode (without actual GPS reception)
QUON	Quartz/Crystal time + SyncON running
QUEX	Quartz/Crystal time (in freewheel after synchronization failure ⇨ Board was already synchronized)
QUSE	Quartz/Crystal time after reset or manual setting
INVA	Invalid time

7.3.6.2 Set Sync Source Time

Adjustment of UTC including the date in the Sync Source (here Module 8024GPS)

After entering the plausibility of these values are directly checked by clicking on the **Apply** button and then sent to the Sync Source (here Module 8024GPS).

> ❗ Always the UTC time must be set. The local time is internally calculated from the difference time (Time Zone Offset) and the summer / winter time changeover (Daylight Saving Time).



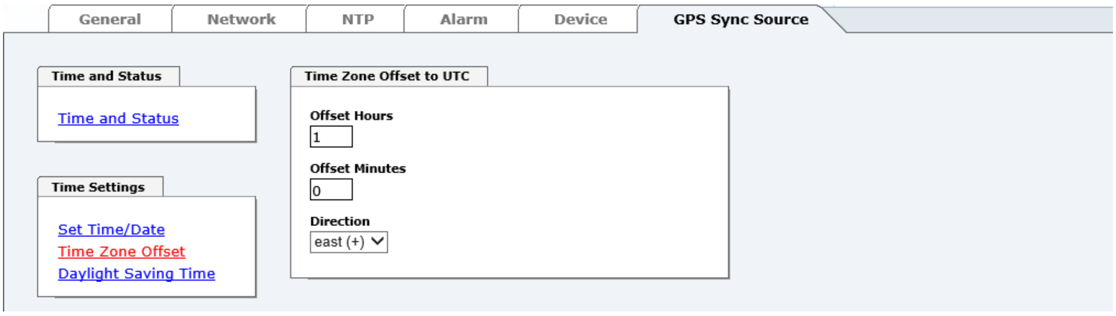
- **Year** Input of the current UTC year (2000-2099)
- **Month** Input of the current UTC month (01-12)
- **Day** Input of the current UTC day (01-31)
- **Hour** Input of the current UTC hour (00-23)
- **Minute** Input of the current UTC minute (00-59)
- **Second** Input of the current UTC second (00-59)

The input must be complete and according to the stated format.

7.3.6.3 Time Zone Offset

Setting of the difference time (Time Zone Offset) from UTC to the local standard time (winter time) in the Sync Source (here Module 8024GPS)

The difference time to be entered **always** relates to **the local standard time (winter time)** even though the commissioning or rather the input of the difference time takes place during daylight saving time.



Offset Hours: 1

Offset Minutes: 0

Direction: east (+)

- **Offset Hours** Time Zone Offset input of the full hour (0-13)
- **Offset Minutes** Time Zone Offset input of minutes (0-59)

Example:

Time Offset for Germany ⇨ East, 1 hour and 0 minutes (+ 01:00)

Time Offset for Peru ⇨ West, 5 hours and 0 minutes (- 05:00)

Direction relating to Prime Meridian – Direction of the Difference Ttime

Entering the direction the local time deviates from world time:

'East' corresponds to east,
'West' corresponds to west of the Prime-Meridian (Greenwich)

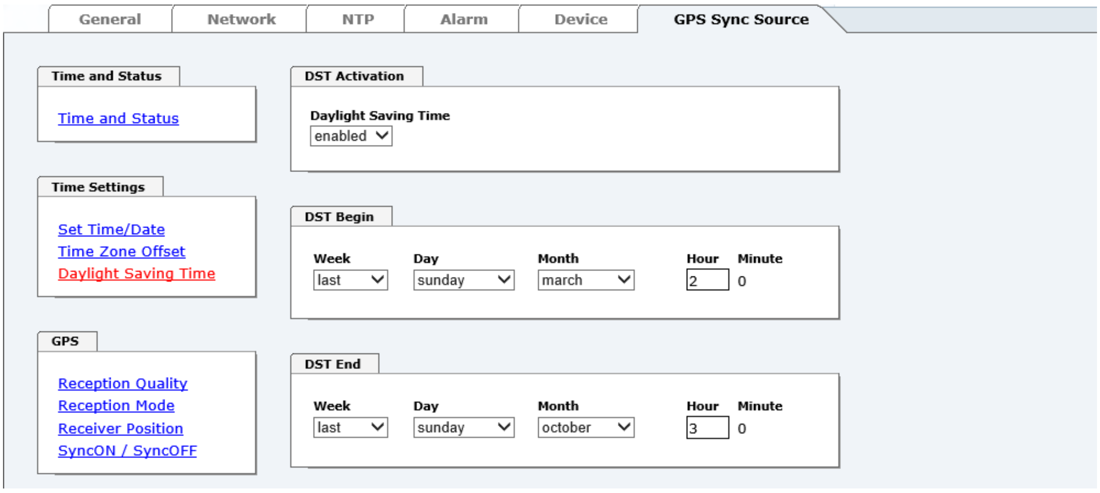
7.3.6.4 Daylight Saving Time (DST)

Setting of the changeover times for summer/winter time in the Sync Source (here Module 8024GPS).

This input is used to define the point of time at which the changeover to Daylight Saving Time or winter time occurs during the course of the year. The hour, day of the week, week of the month and month at which the the Daylight Saving Time begins and ends are determined.

So the exact times are automatically calculated for the running year.

> i After the turn of the year the changeover times for summer/winter time are **automatically** recalculated, without any user intervention.



Daylight Saving Time: enabled

DST Begin — Week: last, Day: sunday, Month: march, Hour: 2, Minute: 0

DST End — Week: last, Day: sunday, Month: october, Hour: 3, Minute: 0

- **DST Activation (enabled/disabled) – Changeover times for summer/winter time**
- **DST Begin – Changeover time for standard time to Daylight Saving Time**
- **DST End – Changeover time for Daylight Saving Time to standard time**

The individual items have the following meanings:

Week	How often the changeover should be processed per day of the week in the month	First - 1st week Second - 2nd week Third - 3th week Fourth - 4th week Last - last week
Day	The day of the week when the changeover should be processed	Sunday, Monday … Saturday
Month	the month when the changeover should be processed	January, February ... December
Hour **Minute**	The time in hour and minute when the changeover should be processed	00h ... 23h 00min ... 59min

> ! The data are entered on the basis of the local time.

7.3.6.5 Receiption Quality

In this tab following information is indicated with read-only access:

Satellites in View

Number of available satellites detected by the GPS receiver

Satellites Tracked

Effective number of received satellites used for synchronization

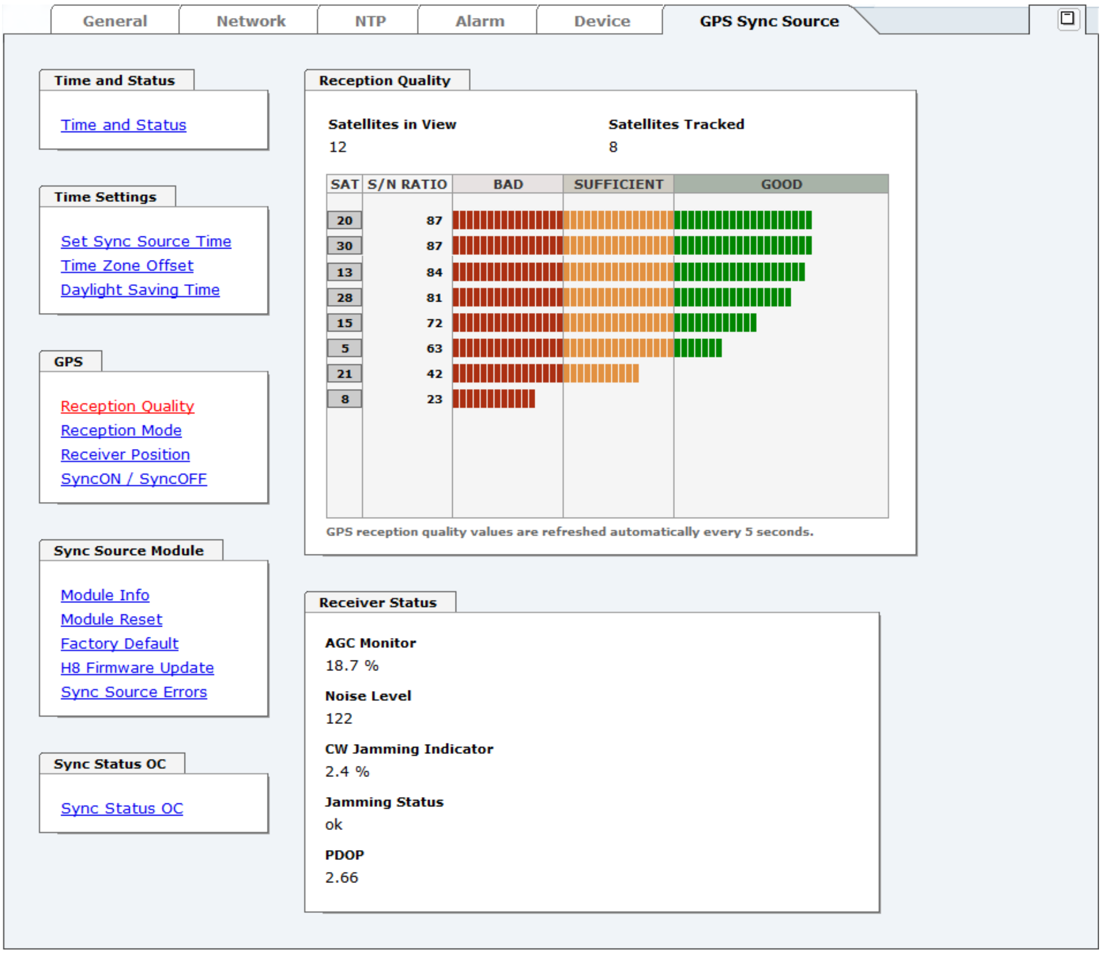
Satellites Number – S/N Ratio

Overview of actually received GPS satellites with their number and reception quality and the pertinent interpretation

green	≥ 48	Good reception quality
yellow	31-47	Sufficient reception quality
red	0-30	Poor reception quality

Receiver Status

Display of the actual GPS receiver values. For analysing the GPS receiver in case of support.



Reception Quality

Satellites in View
12

Satellites Tracked
8

SAT	S/N RATIO	BAD	SUFFICIENT	GOOD
20	87	🟥	🟨	🟩
30	87	🟥	🟨	🟩
13	84	🟥	🟨	🟩
28	81	🟥	🟨	🟩
15	72	🟥	🟨	🟩
5	63	🟥	🟨	🟩
21	42	🟥	🟨	
8	23	🟥		

GPS reception quality values are refreshed automatically every 5 seconds.

Receiver Status

AGC Monitor
18.7 %

Noise Level
122

CW Jamming Indicator
2.4 %

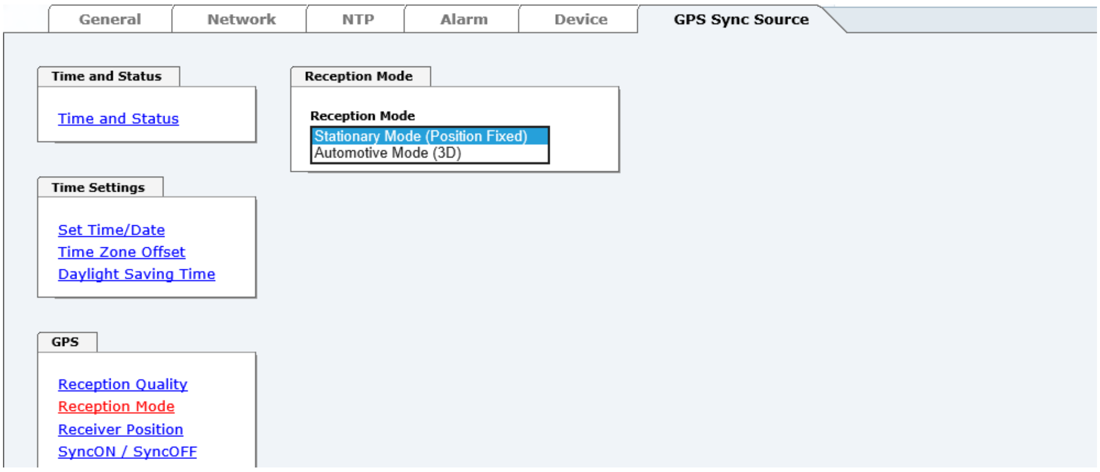
Jamming Status
ok

PDOP
2.66

This page is upated automatically every 5 seconds.

7.3.6.6 Reception Mode

In this tab the GPS reception mode is adjusted and displayed. The accuracy of the time evaluation is defined by the exact position calculation of the installation site. For this calculation (3D evaluation) it is necessary to receive information from at least four (4) satellites. The signal runtime to several satellites is determined from the calculated position and the precise second mark is generated from their mean value.



Reception Mode
Stationary Mode (Position Fixed)
Automotive Mode (3D)

Stationary Mode (Position Fixed) – Standard operation

In Stationary Mode (Fixed position), the GPS receiver calculates its accuracy based on a fixed position. If four or more satellites are received in this mode, the exact location is updated automatically.

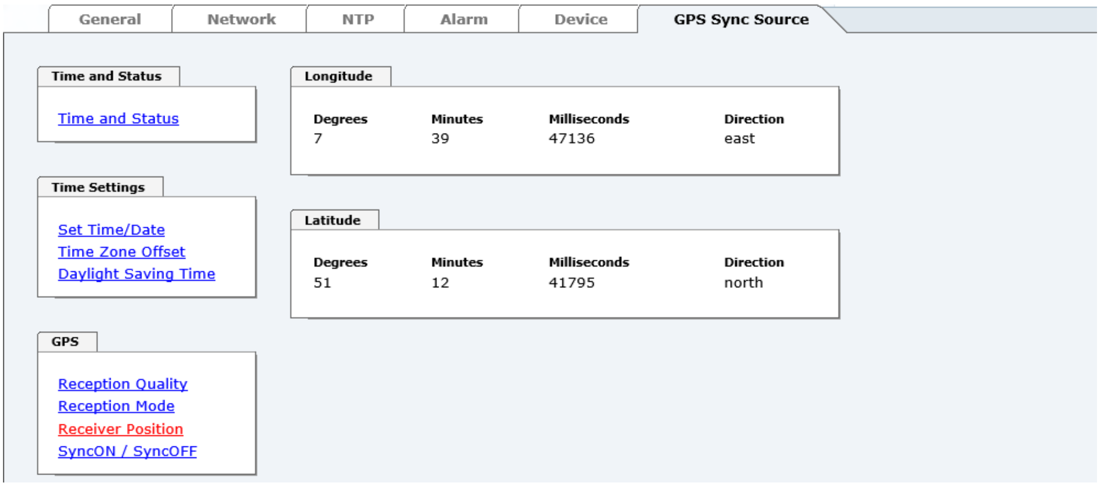
In this mode, a synchronization with a changing position is not possible.

Automotiv (3D)

The automotive (3D) mode allows the use of system 8029NTS at mobile locations (except aircraft).

7.3.6.7 Receiver Position

In this tab the current postion is adjusted and displayed.



Longitude

Degrees	Minutes	Milliseconds	Direction
7	39	47136	east

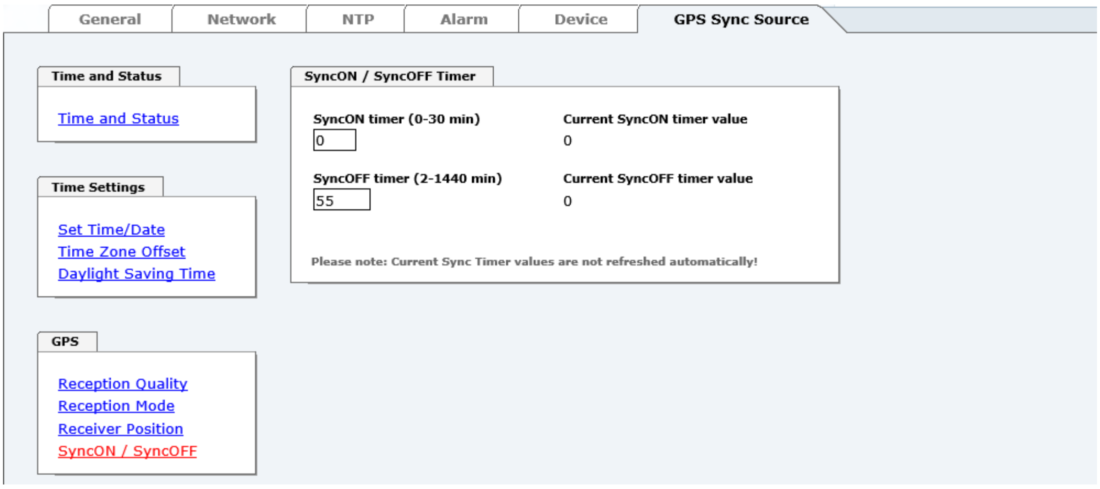
Latitude

Degrees	Minutes	Milliseconds	Direction
51	12	41795	north

Longitude / Latitude – Current Position with Longitude and Latitude

Display of the actual position calculated by the GPS receiver.

7.3.6.8 SyncON / SyncOFF



SyncON timer (0-30 min): 0

Current SyncON timer value: 0

SyncOFF timer (2-1440 min): 55

Current SyncOFF timer value: 0

Please note: Current Sync Timer values are not refreshed automatically!

SyncON Timer

The SyncON timer is used to delay the sync-status “SYNC” by the set time although the GPS receiver is synchronous.

This function is enabled when adjustment processes should be terminated as defined before the sync status is “SYNC”.

This function is not required for this device and should always be set to 0.

SyncOFF Timer

This value is used to provide reception failure bypassing for an error-message free operation even under poor reception conditions.

In the event of a reception failure of the Sync Soure (here Module 8024GPS), the re-synchronization of the Sync Source to **quartz** status is delayed by the set value. The system continues to run in synchronization status **'SYOF'** on the internally regulated, highly accurate quartz base during this period.

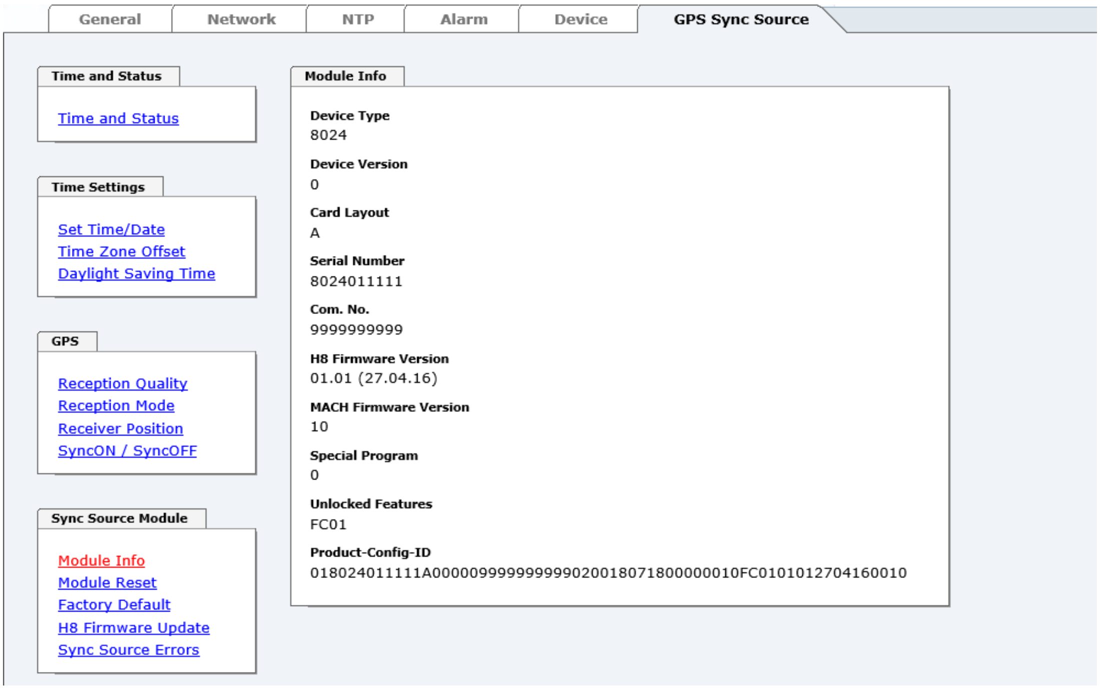
This timer is of special significance when certain system outputs are linked to a specific system status.

The Timer can be set from 2min. to 1440min.

Current Timer values

In case of an active Timer the appropriate value of the timer is displayed here.

7.3.6.9 Module Info



Device Type
8024

Device Version
0

Card Layout
A

Serial Number
8024011111

Com. No.
9999999999

H8 Firmware Version
01.01 (27.04.16)

MACH Firmware Version
10

Special Program
0

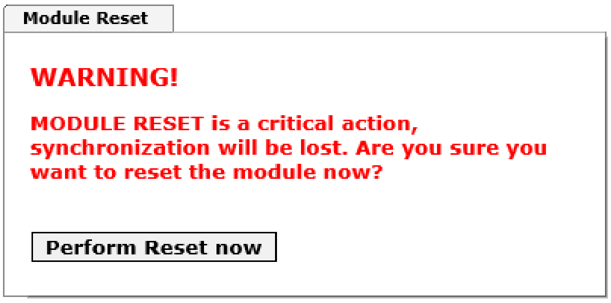
Unlocked Features
FC01

Product-Config-ID
018024011111A000009999999999020018071800000010FC0101012704160010

This tab indicates information about the hardware and software of the Module 8024GPS (Sync Source) implemented in the Time Server 8029NTS/GPS.

> These details might be provided for serive and support puposes.

7.3.6.10 Module Reset



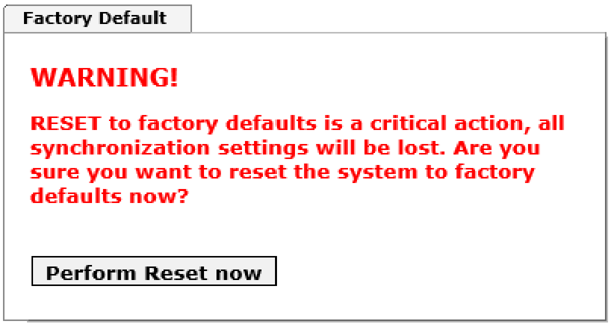
WARNING!

MODULE RESET is a critical action, synchronization will be lost. Are you sure you want to reset the module now?

This function triggers a hardware reset of (just) the Sync Source (here Module 8024GPS).

> This function has no effect on the failsafe stored data.

7.3.6.11 Factory Default



WARNING!

RESET to factory defaults is a critical action, all synchronization settings will be lost. Are you sure you want to reset the system to factory defaults now?

⚠

After setting the Sync Source to factory default values the GPS receiver needs up to 13 minutes of satellite reception in order to generate the correct information on the leap second from the GPS data. Only then the Sync Source (here Module 8024GPS) can be synchronized.

During this time (however only when the GPS receiver really receives satellites) the following message is displayed in the tab **Module Errors**:

GPS Receiver in raw data mode - no sychronisation

⚠

If the changeover times for summer/winter time and the difference time are not initial set after a factory default of the Sync Source (here Module 8024GPS) the following message is displayed in the tab **Module Errors**:

Missing data for Time Zone Offset

and/or

Missing or incomplete data for daylight saving time (DST)

7.3.6.12 H8 Firmware Update (Sync Source)

Patches and Bug Fixes are provided for the Time Server 8029NTS/GPS by means of updates.

The H8 update of the Sync Source is loaded only via the web interface in the Time Server 8029NTS/GPS (log in as “master” user required). See also ***Chapter 4.4 Firmware Update***.

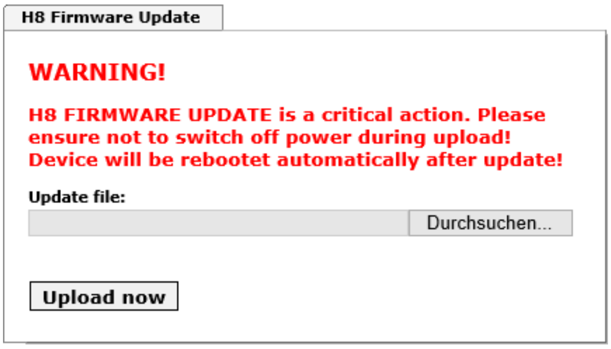
The following points should be considered regarding updates:

- Only experienced users or trained technical personnel should carry out a board update after checking all necessary preconditions.
- Important: **Faulty updates** or **update attempts** may, under certain circumstances, require the module to be returned to the factory for repair at customer’s expense.
- Is the the update on hand suitable for the module? If there are any doubts please consult the support of the ***hopf*** company.
- In order to guarantee a correct update, the "***New version of saved site***" function must be set to "***On each access to the site***" on the Internet browser used.
- During the update procedure, the device **must not be switched off** not **settings be saved to the flash memory**!
- Updates are **always** carried out as Software SETs. That means that all programmes included in the SET must be downloaded to the system.
- For the update pay attention to point described in ***Chapter 4.4 Firmware Update***

In order to carry out an update, enter the name and the folder in which the update / firmware image is located in the text field or open the file selection dialogue by pressing the "Browse" button.

A correct image designation is (e.g.):

8024_v0101_128.**mot**	for **H8 firmware** (Update takes approx. 1-1.5 minutes)



H8 Firmware Update

WARNING!

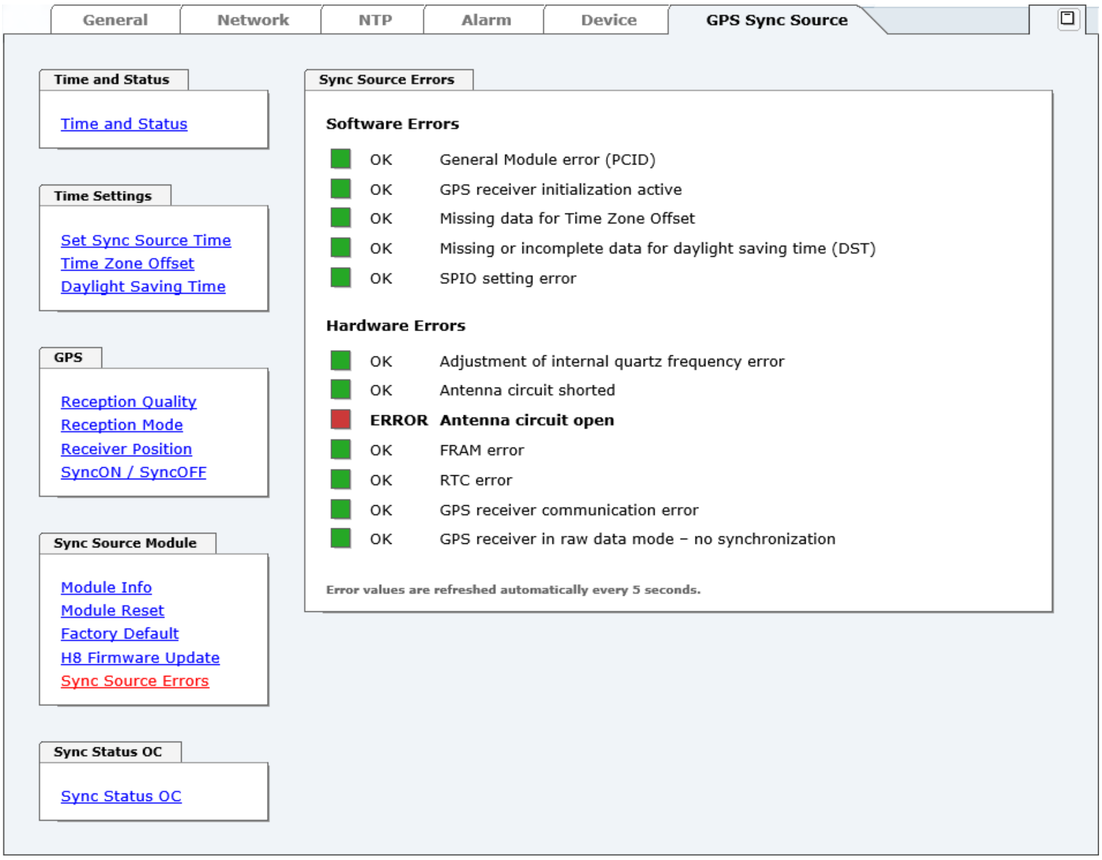
H8 FIRMWARE UPDATE is a critical action. Please ensure not to switch off power during upload! Device will be rebootet automatically after update!

Update file:

7.3.6.13 Sync Source Errors

This tab displays the currrent failure status of the Sync Source (here Module 8024GPS):

> If a collected error message is displayed in the GENERAL tab, there is at least one error (Sync Source Error).



Software Errors

🟩	OK	General Module error (PCID)
🟩	OK	GPS receiver initialization active
🟩	OK	Missing data for Time Zone Offset
🟩	OK	Missing or incomplete data for daylight saving time (DST)
🟩	OK	SPIO setting error

Hardware Errors

🟩	OK	Adjustment of internal quartz frequency error
🟩	OK	Antenna circuit shorted
🟥	**ERROR**	**Antenna circuit open**
🟩	OK	FRAM error
🟩	OK	RTC error
🟩	OK	GPS receiver communication error
🟩	OK	GPS receiver in raw data mode – no synchronization

Error values are refreshed automatically every 5 seconds.

> This page is updated automatically every 5 seconds.

Overview Software Errors

- **General Module error (PCID)**

  If this error occurs even after a Power down, the device is damaged.

- **GPS receiver initialization active**

  This condition might last for max. 1 minute after particular actions.

- **Missing data for Time Zone Offset**

  Difference time (Time Zone Offset) must be an inital entry by the user.

  Otherwise there is no synchronization of the Sync Source (here Module 8024GPS).

- **Missing or incomplete data for daylight saving time (DST)**

  The switchover times for summer/winter time must be initially set / disabled by the user.

  Otherwise there is no synchronization of the Sync Source (here Module 8024GPS).

- **SPIO setting error**

  If this error occurs even after a voltage reset, the support team of company ***hopf*** needs to be contacted for further actions.

Overview Hardware Errors

- **Adjustment of internal quartz frequency error**

  Problems with the internal quartz regulation of the Sync Source (here Module 8024GPS) have occured. So the specified accuracy of the Sync Source cannot be guaranteed anymore.

- **Antenna circuit shorted**

  The Sync Source (here Module 8024GPS) has detected a short circuit in the antenna system. The antenna system should be checked.

- **Antenna circuit open**

  The Sync Source (here Module 8024GPS) has detected an open antenna input. The antenna system should be checked.

- **FRAM error**

  If this error occurs even after a voltage reset, the support team of company ***hopf*** needs to be contacted for further actions.

- **RTC error**

  If this error with set or synchronized time (not sync.-status INVA) and a successive reset of the sync. source still maintains the internal backup clock may be defective.

- **GPS receiver communication error**

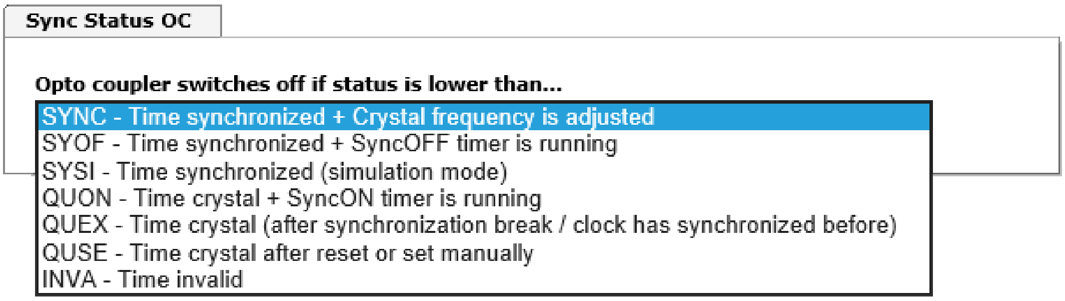
  If this error occurs even after a Power down, the support team of company ***hopf*** needs to be contacted for further actions.

- **GPS receiver in raw data mode – no synchronization**

  If this condition is indicated, the GPS receiver requires special data from the GPS signal for which it needs up to 13 minutes signal receiption of satellites. Only then the Sync Source (here Module 8024GPS) can be synchronized.

  This happens e.g. after resetting the Sync Source paramaters to factory default values.

7.3.6.14 Sync Status OC



Sync Status OC

Opto coupler switches off if status is lower than...

SYNC - Time synchronized + Crystal frequency is adjusted
SYOF - Time synchronized + SyncOFF timer is running
SYSI - Time synchronized (simulation mode)
QUON - Time crystal + SyncON timer is running
QUEX - Time crystal (after synchronization break / clock has synchronized before)
QUSE - Time crystal after reset or set manually
INVA - Time invalid

The output of the status optical coupler (on the front panel of the Time Server 8029NTS/GPS) can be configured by the use of this function.

The time states are listed in this selection window in rising quality from the bottom to the top (**SYNC** = optimal condition).

Behaviour of Optical Coupler:

- Selected status achieved or better – Optical coupler switched through
- Selected status not achieved – Optical coupler blocked

Value range

Optical Coupler Status	**SYNC**	Time synchronized + Quartz regulation started/running
	SYOF	Time synchronized + SyncOFF running
	SYSI	Time synchronized as simulation mode (without actual GPS reception)
	QUON	Quartz/Crystal time + SyncON running
	QUEX	Quartz/Crystal time (in freewheel after synchronization failure ⇨ Board was already synchronized)
	QUSE	Quartz/Crystal time after reset or manual setting
	INVA	Invalid time

8 SSH and Telnet Basic Configuration

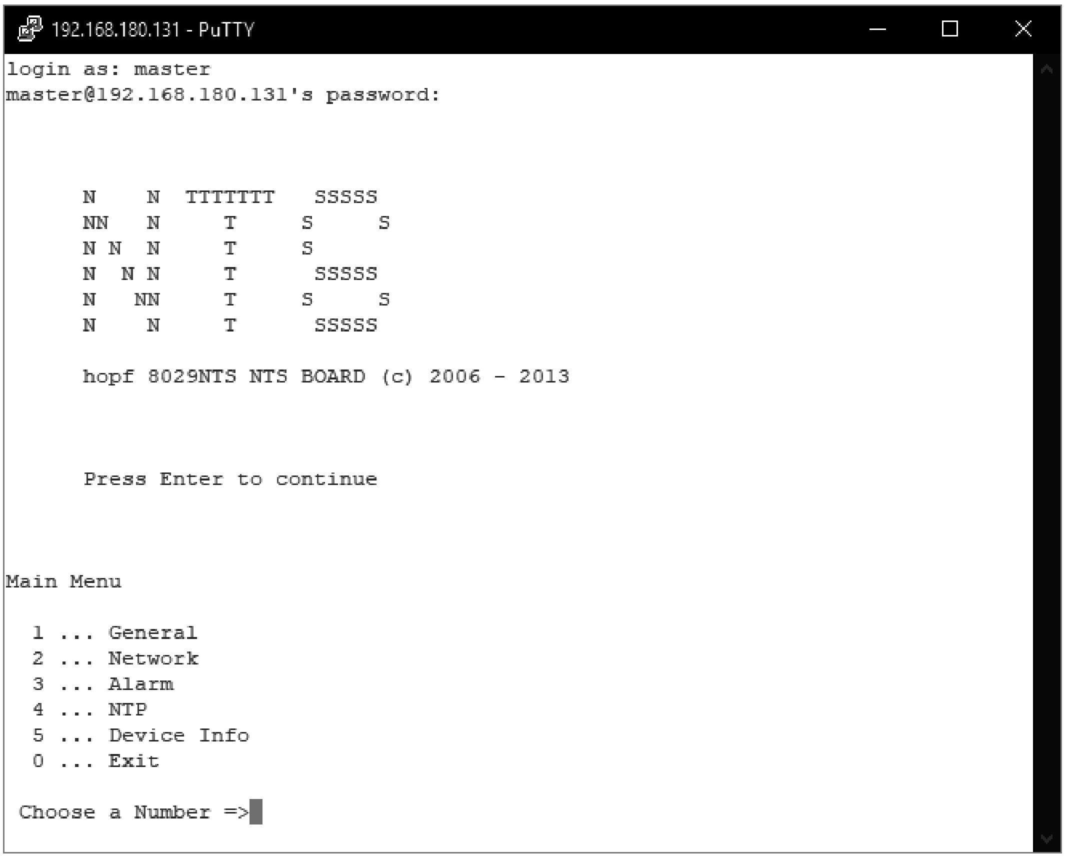
Only basic configuration is possible via SSH or Telnet. The complete configuration of the Time Server 8029NTS/GPS takes place exclusively via the WebGUI.

It is just as easy to use SSH (Port 22) or Telnet (Port 23) as the WebGUI. Both protocols use the same user interface and menu structure.

The user names and passwords are the same as on the WebGUI and are kept in alignment (see ***Chapter 7.3.5.5 Passwords (Master/Device)***).

SSH does not allow blank passwords for safety reasons.

The corresponding protocols should be enabled for the use of Telnet or SSH (see ***Chapter 7.3.2.4 Management (Management-Protocols – HTTP, SNMP etc.)***).



```
login as: master
master@192.168.180.131's password:



      N    N  TTTTTTT   SSSSS
      NN   N     T     S     S
      N N  N     T     S
      N  N N     T      SSSSS
      N   NN     T     S     S
      N    N     T      SSSSS

      hopf 8029NTS NTS BOARD (c) 2006 - 2013



      Press Enter to continue



Main Menu

  1 ... General
  2 ... Network
  3 ... Alarm
  4 ... NTP
  5 ... Device Info
  0 ... Exit

 Choose a Number =>
```

The navigation through the menu takes place by entering the respective number associated with the menu option (as can be seen in the above image).

9 Fault Analysis / Troubleshooting

This chapter explains different error patterns and the process to contact the ***hopf*** support team.

9.1 Error Patterns

This chapter describes various error patterns which enable the customer to make a preliminary problem analysis. In addition they also provide assistance in describing the error when contacting the ***hopf*** support.

> ℹ If possible, for each problem the entire status in the tabs **GENERAL** and **GPS SYNC SOURCE** page "**Module Errors**" via WebGUI should always be checked.

9.1.1 Complete Failure

Description

- The Status LEDs on the front panel are off

Cause / Problem Solution

- Device is switched off
- Voltage supply failure
- Power supply defective

9.1.2 No GPS Reception / No Synchronization

Description

- In WebGUI the status of the SYNC SOURCE is **not** displayed with **SYNC** or **SYOF**
- The Status LEDs of Module 8024GPS on the front panel do not indicate **SYNC** or **SYOF** status

Cause / Problem Solution

- System was not correctly/completely initialized

The following describes various effects and their possible causes on a non-synchronizing system:

Case 1:

Effect: After the first installation, no satellite appears on the display after several hours and **00** is displayed under **Satellites in View**.

Possible Errors:

- The antenna cable is too long
- An incorrect cable type was used for the length of the antenna equipment
- The antenna cable is faulty
- The antenna cable is not connected
- The antenna is defective
- The indirect lightning protection is defective

Case 2:

Effect: There are 7 satellites in the visibility range (**V=07**) but a maximum of 2 appear on the display frame. However, the value of these satellites is 70 or above.

Possible Errors:

- The visibility range of the antenna to the sky is limited.

Case 3:

Effect: There are 9 satellites in the visibility range (**V=09**) and 6 appear on the display frame. The signal/noise ratios are all below 30. The equipment is not synchronized.

Possible Errors:

- The cable is too long
- An incorrect cable type was used for the length of the antenna equipment
- The BNC connectors are poorly mounted
- The cable is bent or crimped
- Indirect lightning protection was irreversibly damaged by overvoltage
- The antenna is defective

Case 4:

Effect: The equipment was working perfectly but has not been receiving for several days. 7 satellites appear in the visibility range (**V=07**) but no satellite is displayed.

Possible Errors:

- The cable has been damaged
- There was excess voltage on the antenna equipment and the indirect lightning protector is defective
- The antenna is defective
- The GPS receiver of Module 8024GPS is defective
- A building change has had an effect on the antenna equipment (e.g. shading of the antenna caused by subsequent building installation, or the laying of cables with a high electrical alternating field in the immediate vicinity of the GPS antenna cable)
- Electronic equipment with an interference effect on the GPS signal has been put into operation in the vicinity of the GPS antenna equipment / GPS receiver (e.g. transmitter for pagers)

Further information on the subject of the GPS antenna system can be consulted in the manual "Antenna Equipment GPS".

9.1.3 No Daylight Saving Time / Summer Time Switchover

Description

- There is no "DST" for “daylight saving time“ (summer time) displayed in the Sync Source time in WebGUI
- Summer time is not considered in outputs working with it and even in case of availibilty.

Cause / Problem Solution

- Changeover times are not set
- Parameterization failure

9.2 Support by Company *hopf*

Should the system show any other failure description than listed in ***Chapter 9.1 Error Patterns***, please contact the support of company ***hopf*** Elektronik GmbH by providing an exact failure description and the following information:

> If possible, for each problem the **Configuration File** in the tab **DEVICE** should be downloaded from the device and be sent to the ***hopf*** support (see ***Chapter 7.3.5.10 Download of Configurations / SNMP MIB***).

- With the file **System Configuration** or if not possible with the serial number of the System
- When does the error occur: During commissioning or operation
- Exact error description
- In the case of GPS reception/synchronization problems ⇨ description of the antenna equipment used:
  - Components used (antenna, indirect lightning protection, etc.)
  - Cable type used
  - Total length of the antenna system
  - Sequence of components and cable lengths between the components
  - Antenna installation site (e.g. signal shading by building)

Please write to the following E-mail address with the above information:

support@hopf.com

> Providing a detailed error description and above listed information avoid the need for additional clarification and leads to a faster processing by the support team.

10 Maintenance

The Time Server 8029NTS/GPS is generally maintenance-free. The following points should be observed if a cleaning of the system might be necessary.

10.1 General Guidelines for Cleaning

The following **must not** be used to clean the Time Server 8029NTS/GPS:

- Fluids
- Cleaning agents containing solvents
- Cleaning agents containing acids
- Abrasive media

The use of such cleaning agents or media could damage the Time Server 8029NTS/GPS.

Do not use a wet cloth to clean the Time Server 8029NTS/GPS.

There is the danger of an electric shock.

To clean the Time Server 8029NTS/GPS use a cloth that is:

- Antistatic
- Soft
- Non-fabric
- Damp

10.2 Cleaning the Housing

Make sure that connections or cables are not loosened while cleaning the housing of the Time Server 8029NTS/GPS. There is the danger of damage and functionality loss.

11 Technical Data

The company ***hopf*** reserves the right to hardware and software alterations at any time.

11.1 General – 8029NTS/GPS

General Data	
Installation position:	On horizontal 35mm rail in accordance with DIN EN 60715 TH35
Protection type of the housing:	IP30
Protection class:	I, with PE connection
Housing design:	Aluminium, closed
Housing dimensions:	*See **Chapter 11.5 Dimensions – DIN Rail Housing***
Weight:	Approx. 0.8kg

Ambient Conditions		
Temperature range:	Operation:	0°C to +55°C
	Storage:	-20°C to +75°C
Humidtiy:		max. 95%, non condensing

CE Conformity
EMV Directive 2014/30/EU
EN 55022 : 2010 / AC : 2011
EN 61000-3-2 : 2006 / A2 : 2009, EN 61000-3-3 : 2013
EN 55024 : 2010
Low Voltage Directive 2014/35/EU
EN 60950-1 : 2006 / AC : 2011

MTBF	
MTBF	> 250,000h

Power Consumption - internal	
Normal operation	Typical: 550mA (max. 600mA) at 5VDC
Boot phase	Typical: 550mA (max. 600mA) at 5VDC

11.2 Module 8029NTS

LAN - ETH0	
Network connection	Via a LAN cable with RJ45 connector, male (recommended cable type CAT5 or better)
Request per second	Max. 1000 requests
Number of connectable Clients	Theoretically unlimited
Network interface ETH0	10/100 Base-T
Ethernet compatibility	Version 2.0 / IEEE 802.3
Isolation voltage (Network- to system side)	1500 Vrms

GPS-System - Accuracy		
Lambda < 15ms and Stratum 1-15	Stability: < 0,2ppm	HIGH
Lambda < 15ms and Stratum 1-15	Stability: 0,2ppm to 2ppm, Offset < 1ms	HIGH
Lambda < 15ms and Stratum 1-15	Stability: > 2ppm or Offset >= 1ms	MEDIUM
Lambda >= 15ms or Stratum 16	---	LOW
DCF77-System – Accuracy		
Lambda < 15ms and Stratum 1-15	Stability: < 0,6ppm	HIGH
Lambda < 15ms and Stratum 1-15	Stability: 0,6ppm to 2ppm, Offset < 2ms	HIGH
Lambda < 15ms and Stratum 1-15	Stability: > 2ppm or Offset >= 2ms	MEDIUM
Lambda >= 15ms or Stratum 16	---	LOW

Time Protocols

- NTPv4 Server
- NTP Broadcast Mode
- NTP Multicast Mode
- NTP Client for additional NTP Servers (Redundancy)
- SNTP Server
- NTP Symmetric Key Encryption
- NTP Autokey Encryption
- NTP Access Restrictions
- PPS Time Source
- RFC-867 DAYTIME Server
- RFC-868 TIME Server
- SINEC H1 time datagram (Activation key required)

TCP/IP Network Protocols

- HTTP/ HTTPS
- DHCP
- Telnet
- SSH
- SNMP (Activation Key required)
- NTP (incl. SNTP)
- SINEC H1 time datagram (Activation key required)

Configuration Channels

- HTTP/HTTPS-WebGUI (Browser Based)
- Telnet
- SSH
- ***hmc*** Remote Access
- ***hmc*** Network Configuration Assistent

11.3 Module 8024GPS

Accuracy	
Internal PPS pulse on GPS reception (after 5min. continuously GPS reception):	Standard Quartz: < ± 30ns VCTCXO: < ± 15ns
VCO control of the internal quartz base (after 5min. continuously GPS reception):	Standard Quartz: < ±0.030ppm VCTCXO: < ±0.015ppm
Freewheel accuracy:	Standard Quartz: < ±0.1ppm after 5min. GPS reception / T = +20° C Drift for T = +20° C (constant): - after 1h: 0.36msec. - after 24h: 8.64msec. VCTCXO: < ±0.02ppm after 5min. GPS Empfang/ T=+20°C Drift für T=+20°C (konstant): - nach 1h: 0.72µsec - nach 24h: 1.73msec
Internal back-up clock (RTC):	±25ppm / for T = +10° C to +50° C

GPS Data	
Receiver type:	22 channel phase tracking receiver, C/A code
Evaluation:	L1 frequency (1575.42MHz)
Sensitivity:	Tracking: -161dBm Cold Start: -148dBm
Synchronization time TTF (Time to First Fix):	• Warm start: < 1min. • Cold start: < 5min. • First inizialising: < 12.5min. (without valid leap second information)
Antenna connection:	• Via BNC connector, female • For active antennas, Ub = 5VDC • Antenna power feed via BNC connector, female of Module 8024GPS

Signal Outputs	
Status optical coupler:	Via 3-pole pluggable screw terminal Resistive circuit-breaking capacity: max. 50mA / 80VDC

Tailor-made products:

Modifications can be made to hardware and software in accordance with customer specifications.

> The ***hopf*** company reserves the right to modify hardware and software at any time.

11.4 Power Supplies

AC Wide-Range Power Supplies

Internal **Power Supply** (Only wide input range)	***hopf*** Type: **AC-M05-D**	***hopf*** Type: **AC-M10-D**

Input Data		
Input voltage range	85-264VAC 100-250VDC	85-264VAC 100-250VDC
Frequency	47-440Hz 0 Hz	47-440Hz 0 Hz
Current consumption (at nominal values)	approx. 0.15A (100VAC) 0.10A (200VAC)	approx. 0.30A (100VAC) 0.20A (200VAC)
Inrush current	typ. 15A (I_O = 100%) 100VAC typ. 30A (I_O = 100%) 200VAC	typ. 15A (I_O = 100%) 100VAC typ. 30A (I_O = 100%) 200VAC
Hold-up time at nominal laod	> 20msec. (> 100VAC)	> 20msec. (> 100VAC)
Start-up time after connected mains voltage	< 1 sec.	< 1 sec.
Transient overvoltage protection	Overvoltage protection III (EN 60664-1)	Overvoltage protection III (EN 60664-1)
Protection supply, internal	400 mA slow blow (device protection)	400 mA slow blow (device protection)
Recommended back-up fuse (AC)	Circuit breaker 6A, 10A charakteristics B (EN 60898)	Circuit breaker 6A, 10A charakteristics B (EN 60898)
Leakage current against PE	< 0.5mA (60Hz, according to EN 60950)	< 0.5mA (60Hz, according to EN 60950)
Input isolation voltage / PE	2000VAC, 1 minute, leakage current = 10mA, 500VDC, 50MOhm min. (at room temperature)	2000VAC, 1 minute, leakage current = 10mA, 500VDC, 50MOhm min. (at room temperature)

Output Data (only internal)		
Internal nominal output voltage	5VDC	5VDC
Nominl output current I_N 0° C ... +55° C	1A (U_{OUT} = 5VDC)	2A (U_{OUT} = 5VDC)
Efficiency	> 77%	> 74%
Function Display (Power LED)	LED green	LED green

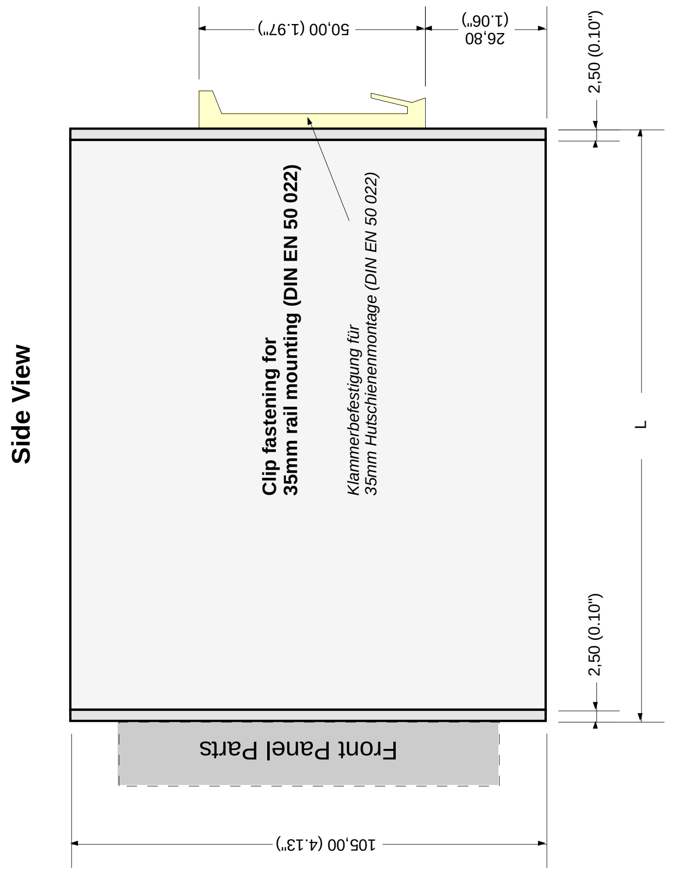
DC Power Supplies

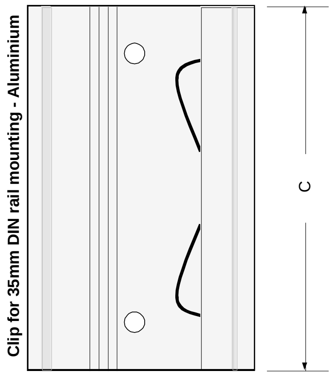
Internal Power Supply	***hopf*** Type: **DC24-M15-D**	***hopf*** Type: **DC48-M15-D**

Input Data		
Input voltage range	18-36VDC	36-76VDC
Current consumption (at nominal values)	approx. 0.69A	Approx. 0.35A
Start-up time after connected mains voltage	< 200msec.	< 200msec.
Protection supply internal (Device protection)	2A fast blow	1A fast blow
Input isolation voltage Input / Output	1,500VDC 1 minute, 500VDC 50MΩ min. (20°C ±15°C)	1,500VDC 1 minute, 500VDC 50MΩ min. (20°C ±15°C)

Output Data (only internal)		
Internal nominal output voltage	5VDC	5VDC
Nominl output current I_N 0° C ... +55° C	3A (U_{OUT} = 5VDC)	3A (U_{OUT} = 5VDC)
Efficiency	> 90%	> 90%
Function Display (Power LED)	LED green	LED green

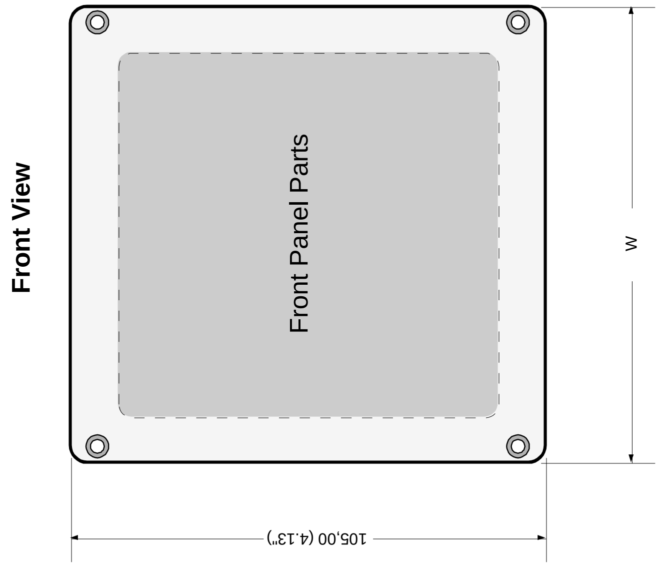
11.5 Dimensions – DIN Rail Housing


Side View
50,00 (1.97")
26,80 (1.06")
2,50 (0.10")
Clip fastening for 35mm rail mounting (DIN EN 50 022)
Klammerbefestigung für 35mm Hutschienenmontage (DIN EN 50 022)
L
2,50 (0.10")
Front Panel Parts
105,00 (4.13")



Material: Aluminium

All dimensions in mm (inch)



TYPE	(L)ength	(W)idth	(C)lip
1	130 (5.12")	64,5 (2.54")	40,0 (1.57")
2	130 (5.12")	100,0 (3.94")	80,0 (3.15")
3	130 (5.12")	135,0 (5.31")	80,0 (3.15")
4	175 (6.89")	64,5 (2.54")	40,0 (1.57")
5	175 (6.89")	100,0 (3.94")	80,0 (3.15")
6	175 (6.89")	135,0 (5.31")	80,0 (3.15")

12 Factory Defaults of Time Server 8029NTS/GPS

This chapter lists the factory default values of the individual components integrated in the Time Server 8029NTS/GPS.

12.1 Factory Default Values of Module 8029NTS (Device)

The default delivery status of the Time Server 8029NTS/GPS meets the factory default values when using GPS synchronization sources. In case of DCF77 synchronization (different product variant) the function **"NTP / General / Sync Source"** is factrory-set to **"DCF77"** on delivery.

> Using the board in DCF77 sytems (different product variant) the setting for **NTP / General / Sync Source"** needs to be re-configured to **"DCF77"** after a factory default.

NTP Server Configuration	**Setting**	**WebGUI**
Sync Source	DCF77	DCF77

12.1.1 Network

Host/Name Service	**Setting**	**WebGUI**
Hostname	hopf8029nts	hopf8029nts
Use Manual DNS Entries	Enabled	Enabled
DNS Server 1 IPv4/IPv6 Address	Blank	---
DNS Server 2 IPv4/IPv6 Address	Blank	---
DNS Server 3 IPv4/IPv6 Address	Blank	---
Use Manual Gateway Entries	Enabled	Enabled
Default Gateway IPv4 Address	Blank	---
Default Gateway IPv6 Address	Blank	---
Network Interface ETH0	**Setting**	**WebGUI**
Use Custom Hardware Address (MAC)	Disabled	Disabled
Custom Hardware Address (MAC)	Blank	---
DHCP	Disbabled	Disabled
IPv4	192.168.0.1	192.168.0.1
IPv4-Netmask	255.255.255.0	255.255.255.0
Operation mode	Auto negotiate	Auto negotiate
VLAN Interfaces	deaktiviert	disabled
IPv6 Settings	deaktiviert	disabled
Routing	**Setting**	**WebGUI**
Use Route File	Disabled	Disabled
User Defined Routes	Blank	---
Management	**Setting**	**WebGUI**
HTTP	Enabled	Enabled
HTTPS	Disabled	Disabled
SSH	Enabled	Enabled
TELNET	Disabled	Disabled
SNMP	Disabled	Disabled
System Location	Blank	---
System Contact	Blank	---

Read Only Community	Blank	---
Read/Write Community	Blank	---
Security Name	Blank	---
Access Rights	Readonly	Readonly
Authentication Protocol	MD5	MD5
Authentication Passphrase	Blank	---
Privacy Protocol	DES	DES
Privacy Passphrase	Blank	---
Time	**Setting**	**WebGUI**
NTP	Enabled	Enabled
DAYTIME	Disabled	Disabled
TIME	Disabled	Disabled
SINEC H1 time datagram	**Setting**	**WebGUI**
Send Interval	Every second	1 second
Timebase	UTC	UTC
Destination MAC Address	09:00:06:03:FF:EF	09:00:06:03:FF:EF
Minimum Accuracy	LOW	LOW

12.1.2 NTP

NTP Server Configuration	**Setting**	**WebGUI**
Sync Source	GPS	GPS
NTP to Syslog	Disabled	Disabled
Switch to specific stratum	Disabled	Disabled
Stratum in crystal operation	Blank	---
Broadcast address	Blank	---
Authentication	Disabled	None
Key ID	Blank	---
Additional NTP Servers	Blank	---
NTP Extended Configuration	**Setting**	**WebGUI**
Limitation of Liability	Blank	---
Block Output when Stratum Unspecified	Disabled	Disabled
NTP Access Restrictions	**Setting**	**WebGUI**
Access Restrictions		Default nomodify
NTP Symmetric Keys	**Setting**	**WebGUI**
Request Key	Blank	---
Control Key	Blank	---
Symmetric Keys	Blank	---
NTP Autokey	**Setting**	**WebGUI**
Autokey	Disabled	Disabled
Password	Blank	---

12.1.3 ALARM

Syslog Configuration	Setting	WebGUI
Syslog	Disabled	Disabled
Server Name	Blank	---
Alarm Level	Disabled	None
E-mail Configuration	**Setting**	**WebGUI**
E-mail Notifications	Disabled	Disabled
SMTP Server	Blank	---
Sender Address	Blank	---
E-mail Addresses	Blank	---
SNMP Traps Configuration	**Setting**	**WebGUI**
SNMP Traps	Disabled	Disabled
Alarm Level	Disabled	None
SNMP Trap Receivers	Blank	---
Alarm Messages	**Setting**	**WebGUI**
Alarms	All disabled	All none

12.1.4 DEVICE

User Passwords	Settings	WebGUI
Master Password	master	---
Device Password	device	---
Diagnostic	**Settings**	**WebGUI**
Real Time Diagnostics	Disabled	Disabled
Product Activation	**Settings**	**WebGUI**
Activate Feature	No changes	No changes

12.2 Factory Default Values of Module 8024GPS (Sync Source)

After triggering a factory default of Module 8024GPS two steps are carried out.

1. **Deleting the current leap second information in the GPS receiver**

2. **Following parameters are set to default values:**

Difference time	**00h 00min east**
Changeover times: Begin of Daylight Saving Time:	**disabled** Week □ first Day □ Monday Month □ January Hour □ 0
End of Daylight Saving Time:	Week □ first Day □ Monday Month □ January Hour □ 0
SyncON / SyncOFF Timeout:	**0000** / **0055** (minutes)
GPS Position: Longitude: Latitude:	 **E 000° 00' 0000** **N 00° 00' 0000**
GPS reception mode:	**Position Fixed**
Sync Status OC:	**SYNC**

13 Glossary and Abbreviations

13.1 NTP-specific Terminology

Stability	The average frequency stability of the clock system.
Accuracy	Specifies the accuracy in comparison to other clocks.
Precision of a clock	Specifies how precisely the stability and accuracy of a clock system can be maintained.
Offset	This value represents the time difference between two clocks. It is the offset by which the local time would have to be adjusted in order to keep it congruent with the reference clock.
Clock skew	The frequency difference between two clocks (first derivative of offset over time).
Drift	Real clocks vary in frequency difference (second derivative of offset over time). This variation is known as drift.
Roundtrip delay	Roundtrip delay of an NTP message to the reference and back.
Dispersion	Represents the maximum error of the local clock relative to the reference clock.
Jitter	The estimated time error of the system clock measured as the average exponential value of the time offset.

13.2 Tally Codes (NTP-specific)

space	**reject**	Rejected peer – either the peer is not reachable or its synchronization distance is too great.
x	**falsetick**	The peer was picked out by the NTP intersection algorithm as a false time supplier.
.	**excess**	The peer was picked out by the NTP sort algorithm as a weak time supplier on the basis of synchronization distance (concerns the first 10 peers).
-	**outlyer**	The peer was picked out by the NTP clustering algorithm as an outlyer.
+	**candidate**	The peer was selected as a candidate for the NTP combining algorithm.
#	**selected**	The peer is of good quality but not among the first six peers selected by the sort algorithm on the basis of synchronization distance.
*****	**sys.peer**	The peer was selected as a system peer. Its characteristics are transferred to the Base System.
o	**pps.peer**	The peer was selected as a system peer. Its characteristics are transferred to the Base System. The current synchronization is derived from a PPS (pulse-per-second) signal either indirectly via PPS reference clock driver or directly via kernel interface.

13.2.1 Time-specific expressions

UTC	**UTC Time** (**U**niversal **T**ime **C**oordinated) was depending on the Greenwich Mean Time (GMT) definition of the zero meridian. While GMT follows astrological calculations, UTC is based on the stability and accuracy of the Caesium standard. The leap second was defined in order to cover this deviation.
Time Zone	The globe was originally divided into 24 longitudinal segments or time zones. Today, however, there are a number of time zones which in part apply specifically to certain individual countries only. In relation to the time zones, consideration was given to the fact that local daylight and sunlight coincide at different times in the individual time zones. The zero meridian runs through the British city of Greenwich.
Time Offset	This is the difference between UTC and the valid standard time of the current time zone. The Time Offset will be commit from the local time zone.
Local Standard Time **(winter time)**	**Standard Time = UTC + Time Offset** The time offset is defined by the local time zone and the local political regulations.
Daylight Saving Time **(summer time)**	**Offset of Daylight Saving Time = + 1h** Daylight Saving Time was introduced to reduce the energy requirement in some countries. In this case one hour is added to the standard time during the summer months.
Local Time	Local Time = Standard Time if exists with summer / winter time changeover
Leap Second	A leap second is a second which is added to the official time (UTC) in order to synchronise this with Greenwich Mean Time when required. Leap seconds are defined internationally by the **International Earth Rotation and Reference Systems Service (IERS)**.

13.3 Abbreviations

D, DST	Daylight Saving Time
ETH0	Ethernet Interface 0
ETH1	Ethernet Interface 1
FW	Firmware
GPS	Global Positioning System
HW	Hardware
IF	Interface
IP	Internet Protocol
LAN	Local Area Network
LED	Light Emitting Diode
NTP	Network Time Protocol
NE	Network Element
OEM	Original Equipment Manufacturer
OS	Operating System
RFC	Request for Comments
SNMP	Simple Network Management Protocol (handled by more than 60 RFCs)
SNTP	Simple Network Time Protocol
S, STD	Standard Time
TCP	Transmission Control Protocol http://de.wikipedia.org/wiki/User_Datagram_Protocol
ToD	Time of Day
UDP	User Datagram Protocol http://de.wikipedia.org/wiki/User_Datagram_Protocol
UTC	Universal Time Coordinated
WAN	Wide Area Network
msec	millisecond (10^{-3} seconds)
µsec	microsecond (10^{-6} seconds)
ppm	parts per million (10^{-6})

13.4 Definitions

An explanation of the terms used in this document.

13.4.1 DHCP (Dynamic Host Configuration Protocol)

DHCP makes it possible to integrate a new computer into an existing network with no additional configuration. It is only necessary to set the automatic reference of the IP address on the client. Without DHCP, relatively complex settings need to be made. Beside the IP address, further parameters such as network mask, gateway and DNS server have to be entered. A DHCP server can assign these parameters automatically by DHCP when starting a new computer (DHCP client).

DHCP is an extension of the BOOTP protocol. A valid IP address is allocated automatically if a DHCP server is available on the network and DHCP is enabled.

ℹ See RFC 2131 Dynamic Host Configuration Protocol for further information.

13.4.2 NTP (Network Time Protocol)

Network Time Protocol (NTP) is a standard for the synchronization of clocks in computer systems via packet-based communication networks. Although it is processed mainly over UDP, it can also be transported by other layer 4 protocols such as TCP. It was specially developed to facilitate reliable timing via networks with variable packet runtime.

NTP uses the Marzullo algorithm (devised by Keith Marzullo of the San Diego University in his dissertation) with a UTC timescale and supports leap seconds from Version 4.0. NTP. It is one of the oldest TCP/IP protocols still in use. It was developed by David Mills of the University of Delaware and published in 1985. The protocol and UNIX implementation continue to be developed under his direction. Version 4 is the up to date version of the protocol. This uses UDP Port 123.

NTPv4 can maintain the local time of a system to an accuracy of some 10 milliseconds via the public Internet. Accuracies of 500 microseconds and better are possible under ideal conditions on local networks.

With a sufficiently stable, local clock generator (oven-stabilised quartz, rubidium oscillator, etc.) and using the kernel PLL (see above), the phase error between reference clock generator and local clock can be reduced to something of the order of a few hundred microseconds. NTP automatically compensates for the drift of the local clock.

NTP can be installed over firewalls and offers a range of security functions.

ℹ See RFC 5905 for further information.

13.4.3 SNMP (Simple Network Management Protocol)

Simple Network Management Protocol (SNMP) is a network protocol which was developed by the IETF in order to be able to monitor and control network elements from a central station. This protocol regulates the communication between the monitored devices and the monitoring station. SNMP describes the composition of the data packets which can be transmitted and the communication procedure. SNMP was designed in such a way that can be provided by SNMP include:

- Monitoring of network components
- Remote control and configuration of network components
- Fault detection and notification

Due to its simplicity, SNMP has become the standard which is supported by most management programmes. SNMP Versions 1 and 2c hardly offer any safety mechanisms. The safety mechanisms have been significantly expanded in the current Version 3.

Using description files, so-called MIB's (Management Information Base), the management programmes are able to represent the hierarchical structure of the data of any SNMP agent and to request data from them. In addition to the MIB's defined in the RFC's, every software and hardware manufacturer can define his own so-called private MIB's which reflect the special characteristics of his product.

13.4.4 TCP/IP (Transmission Control Protocol / Internet Protocol)

TCP and IP are generally used concurrently and thus the term TCP/IP has become established as the standard for both protocols.

IP is based on network layer 3 (layer 3) in the OSI Layer Model whereas TCP is based on layer 4, the transport layer. In other words, the expression TCP/IP signifies network communication in which the TCP transport mechanism is used to distribute or deliver data over IP networks. As a simple example: Web browsers use TCP/IP to communicate with web servers.

13.5 Accuracy & NTP Basic Principles

NTP is based on the Internet protocol. Transmission delays and errors as well as the loss of data packets can lead to unpredictable accuracy data and time synchronization effects.

NTP protocol neither defines nor guarantees the accuracy or correctness of the time server.

Thus the QoS (Quality of Service) used for direct synchronization with GPS or serial interface does not apply to synchronization via NTP.

In simplified terms, accuracies of between 1msec and 1sec can be expected, depending on the accuracies of the servers used.

The accuracy of IP-based time synchronization is depending on the following criteria:

- Characteristics and accuracy of the time server / time signal used
- Characteristics of the sub-network
- Characteristics and quality of the synchronization client
- The algorithm used

NTP has a variety of algorithms to equalise the possible characteristics of IP networks. Algorithms also exist to equalise the offset between reference time source and the local clock.

However, under some circumstances it is not possible to provide an algorithmic solution.

For example:

1. Time servers which do not deliver any correct time cannot be detected at all. The only option available to NTP is to mark these time servers as FALSETICKERS in comparison to other time servers and to disregard them. However, this means that if only 2 time servers are configured, NTP has no way of determining the correctness of the individual times and clearly identifying which time is incorrect.
2. Asymmetries in the transmission between NTP servers and NTP clients can neither be measured nor calculated by NTP. NTP works on the assumption that the transmission path to the NTP server is exactly as long as the return path. The NTP algorithm can only filter out changes on a statistical basis. The use of several servers makes it possible for the combining algorithm to pick up and filter out any such errors. However, there is no possibility of filtering if this asymmetry is present on all or most of the NTP servers (faulty routing etc).
3. It goes without saying that the accuracy of the synchronised time cannot be better than the accuracy resolution of the local clock on the NTP server and NTP client.

With reference to the above mentioned error circumstances, the delivered **time offset** of the NTP should be considered to be at best the most favourable case and in no way to be a value that takes account of all possible errors.

In order to resolve this problem, NTP delivers the maximum possible error in relation to the offset. This value is designated as the synchronization distance ("**LAMBDA**") and is the sum of the **Root Dispersion** and half of the **Root Delay** of all NTP servers used. This value describes the worst possible case and thus the maximum error that can be expected.

Finally, please note that the user of the Time Server is responsible for the network conditions between the Time Server and the NTP clients.

As an example, we mention the case where a network has a delay of 500msec and an accuracy shift (asynchronization.) of 50msec occurs. The synchronised clients will therefore NEVER achieve accuracy values of one millisecond or even microseconds!

The accuracy value in the GENERAL tab of the WebGUI is designed to help the user to estimate the accuracy.

14 List of RFCs

- NTPv4 - Protocol and Algorithms Specification (RFC 5905)
- NTPv4 - Autokey Specification (RFC 5906)
- PPS API (RFC 2783)
- DHCP (RFC 2131)
- Time Protocol (RFC 868)
- Daytime Protocol (RFC 867)
- HTTP (RFC 2616)
- HTTPS (RFC 2818)
- SSH-2 (RFC 4250-4256, 4335, 4344, 4345, 4419, 4432, 4716, 5656)
- TELNET (RFC 854-861)
- SNMPv2 (RFC 1213, RFC1901-1908)
- SNMPv3 (RFC 3410-3418)
- SYSLOG (RFC 5424)
- SMTP (RFC 5321)

15 List of Open Source Packages Used

Third Party Software

The ***hopf*** Time Server 8029NTS/GPS includes a numerous of software packages subject to other license conditions. In case the use of such a software package might violate the licence conditions immediately after written notice it is ensured that the underlying licence conditions are met again.

If the underlying licence conditions relating to a specific software package require availibility of the source code the package is provided electronically (email, download etc.) on requested.

The following table includes all used software packages with the applicable underlying software license conditions:

Package name	Version	License	License details	Patches
arp-scan	1.9	GPL	v3	no
arptables	0.0.4			no
at91bootstrap3	3.8.7			no
busybox	1.28.1	GPL	v2	no
bzip2	1.0.6	BSD		no
cifs-utils	6.7	GPL	v3	no
ethtool	4.13	GPL	v2	no
libevent	2.1.8-stable	3-clause BSD		no
libopenssl	1.0.2n	Dual	http://www.openssl.org/source/license.html	no
libpcap	1.8.1	BSD		no
libzlib	1.2.11		Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution.	no
lighttpd	1.4.48		Copyright (c) 2004, Jan Kneschke, incremental All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:	no

Package name	Version	License	License details	Patches
			- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. - 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. - Neither the name of the 'incremental' 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 COPYRIGHT HOLDERS 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 COPYRIGHT OWNER 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.	
linux	4.8.6	GPL	v2	no
linux-headers	4.8.6	GPL	v2	no
lzo	2.10	GPL	v2	no
mtd	2.0.1	GPL	v2	no
netsnmp	5.7.3	BSD (mehrere)	http://net-snmp.sourceforge.net/about/license.html	no
ntp	4.2.8p11		Copyright (c) University of Delaware 1992-2011 Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or Publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.	yes
openssh	7.6p1	BSD		no
pcre	8.41	BSD		no
pps-tools	47333f24af8 78f67ce480 22e8af1641 9713aa1ac	GPL	v2	no
uboot	2016.09.01	GPL	v2+	no

Package name	Version	License	License details	Patches
uboot-tools	2018.01	GPL	v2+	no
uclibc	1.0.28	GPL	v2	no
util-linux	2.31.1	GPLv2+ GPLv2 LGPLv2+ BSD		no
zip	3.0		Copyright (c) 1990-2007 Info-ZIP. All rights reserved. For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals: Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White. This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions: 1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions. 2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled. 3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions. 4. Info-ZIP retains the right to use the names "Info-ZIP," Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for ist own source and binary releases.	no