The Synchronization Experts.

MANUAL

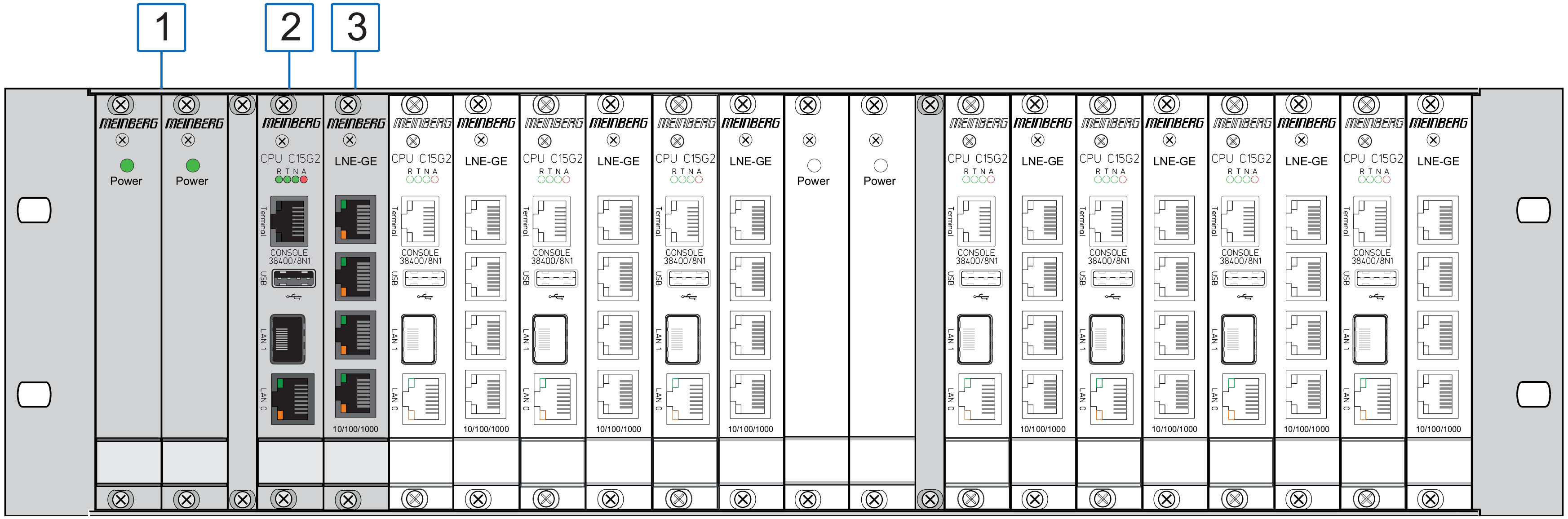
LANTIME CPU Expansion Shelf

LCES/NTP/LNE/RPS/BGT

February 4, 2022

Meinberg Funkuhren GmbH & Co. KG

Front view (Frontansicht) LANTIME CPU Expansion Shelf



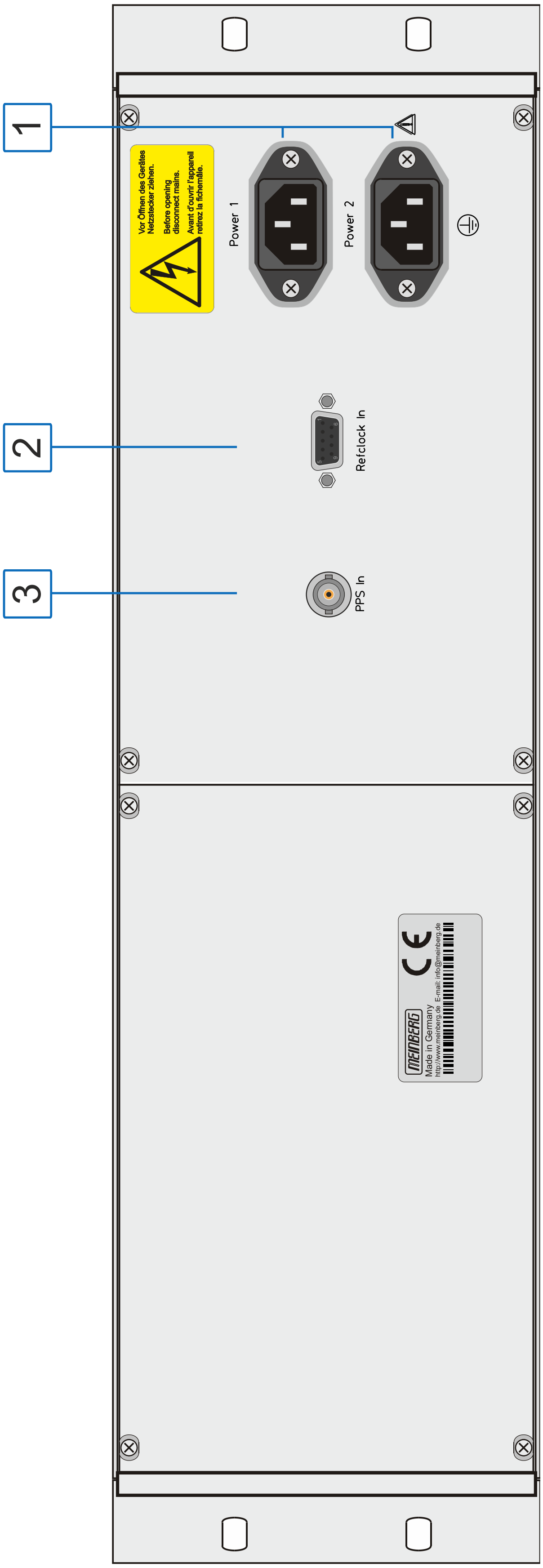
ENGLISH

1. Power supply
2. ***LANCPU***
   - Terminal connector, RJ45 interface (VT100, 38400Baud, 8N1)
   - USB connector
   - Network connectors: LAN 0 - 10/100 Mbit/s, RJ45
     LAN 1 - 1000Base-T, SFP
3. LNE-GE, 4 x network expansion ports 10/100/1000 Mbit/s

DEUTSCH

1. Netzteil
2. ***LANCPU***
   - Terminalanschluss, RS232 Schnittstelle (VT100, 38400 Baud, 8N1)
   - USB Anschluss
   - Netzwerk Anschlüsse: LAN 0 - 10/100 Mbit/s, RJ45
     LAN 1 - 1000Base-T, SFP
3. LNE-GE, 4 x Netzwerk Erweiterung 10/100/1000 Mbit/s

Rear view (Rückansicht) LANTIME CPU Expansion Shelf


1
2
3
Vor Öffnen des Gerätes Netzstecker ziehen.
Before opening disconnect mains.
Avant d'ouvrir l'appareil retirez la fichemâle.
Power 1
Power 2
Refclock In
PPS In
MEINBERG
Made in Germany
http://www.meinberg.de E-mail: info@meinberg.de
CE

ENGLISH

1. Power supply connector
2. Refclock Input, DSUB-9 conncetor
3. PPS Input, BNC female

DEUTSCH

1. Spannungsversorgung
2. Refclock Eingang, DSUB-9 Anschluss
3. PPS Eingang, BNC Buchse

Table of Contents

1 Imprint

Meinberg Funkuhren GmbH & Co. KG
Lange Wand 9, 31812 Bad Pyrmont, Germany

Phone:	+ 49 (0) 52 81 / 93 09 - 0
Fax:	+ 49 (0) 52 81 / 93 09 - 230
Website:	https://www.meinbergglobal.com
Email:	info@meinberg.de
Date:	February 4, 2022

2 Important Safety Information

2.1 Important Safety Information and Safety Precautions

The following safety information must be observed whenever the device is being installed or operated. Failure to observe this safety information and other special warnings or operating instructions in the product manuals constitutes improper usage and may violate safety standards and the manufacturer's requirements.

Depending on the configuration of your device or installed options, some information may not specifically apply to your device.

The device satisfies the requirements of the following EU regulations: EMC Directive,
Low Voltage Directive, RoHS Directive and—where applicable—the Radio Equipment Directive.

If a procedure is marked with the following signal words, you may only proceed with it if you have understood and fulfilled all requirements. Hazard notices and other relevant information are classified and indicated as such in this manual according to the following system:

DANGER!
This signal word indicates a hazard with a high risk level . Such a notice refers to a procedure or other action that will very likely result in serious injury or even death if not observed or if improperly performed.

WARNING!
This signal indicates a hazard with a medium risk level . Such a notice refers to a procedure or other action that may result in serious injury or even death if not observed or if improperly performed.

CAUTION!
This signal word indicates a hazard with a low risk level . Such a notice refers to a procedure or other action that may result in minor injury if not observed or if improperly performed.

ATTENTION!
This signal word refers to a procedure or other action that may result in product damage or the loss of important data if not observed or if improperly performed.

2.2 Used Symbols

The following symbols and pictograms are used in this manual. Pictograms are used in particular to indicate potential hazards in all hazard categories.

Symbol	Beschreibung / Description
⎓	IEC 60417-5031 Gleichstrom / *Direct current*
∼	IEC 60417-5032 Wechselstrom / *Alternating current*
⏚	IEC 60417-5017 Erdungsanschluss / *Earth (ground) terminal*
⏚	IEC 60417-5019 Schutzleiteranschluss / *Protective earth (ground) terminal*
⚠	ISO 7000-0434A Vorsicht / *Caution*
⚡	IEC 60417-6042 Vorsicht, Risiko eines elektrischen Schlages / *Caution, risk of electric shock*
	IEC 60417-5041 Vorsicht, heiße Oberfläche / *Caution, hot surface*
	IEC 60417-6056 Vorsicht, Gefährlich sich bewegende Teile / *Caution, moving parts*
	IEC 60417-6172 Trennen Sie alle Netzstecker / *Disconnect all power connectors*
	IEC 60417-5134 Elektrostatisch gefährdete Bauteile / *Electrostatic Discharge Sensitive Devices*
ⓘ	IEC 60417-6222 Information generell / *General information*
	2012/19/EU Dieses Produkt fällt unter die B2B Kategorie. Zur Entsorgung muss es an den Hersteller übergeben werden. *This product is handled as a B2B-category product. To ensure that the product is disposed of in a WEEE-compliant fashion, it must be returned to the manufacturer.*

2.3 Product Documentation

Detailed product documentation is provided on a USB flash drive delivered with the system. The manuals can also be downloaded from the Meinberg website at https://www.meinbergglobal.com, where you can enter your system name into the search box at the top of the page to find the relevant manual. Alternatively, contact Meinberg Support for further assistance.

The "Docs & Support" tab on the Web Interface also provides user manuals for time server administrators.

⚠

This manual contains important safety instructions for the installation and operation of the device. Please read this manual thoroughly before using the device.

This device may only be used for the purpose described in this manual. In particular, the specified operating limits of the device must be heeded. The person setting up the device is responsible for safety matters in relation to any larger system in which the device is installed!

Failure to observe these instructions may have an adverse impact on device safety!

Please keep this manual in a safe place.

This manual is only intended to be used by qualified electricians, or by persons who have been appropriately instructed by a qualified electrician and who are familiar with applicable national standards and with safety rules & regulations. This device may only be installed, set up, and operated by qualified personnel.

2.4 Safety during Installation

WARNING!

Pre-Operation Procedures and Preparation for Use
This mountable device has been designed and examined in accordance with the requirements of the standard IEC 62368-1 "Audio/Video, Information and Communication Technology Equipment - Part 1: Safety Requirements".

When the mountable device is to be used as part of a larger unit (e.g., electrical enclosure), there will be additional requirements in the IEC 62368-1 standard that must be observed and complied with. General requirements regarding the safety of electrical equipment (such as IEC, VDE, DIN, ANSI) and applicable national standards must be observed in particular.

The device has been developed for use in the industrial sector or in home environments and may only be used in such environments. In environments at risk of high environmental conductivity ("high pollution degree" according to IEC 60664-1), additional measures such as installation of the device in an air-conditioned electrical cabinet may be necessary.

Transport, Unpacking, Installation
If the unit has been brought into the usage area from a cold environment, condensation may develop; in this case, wait until the unit has adjusted to the temperature and is completely dry before setting it up.

When unpacking & setting up, and before operating the equipment, be sure to read the information on installing the hardware and the specifications of the device. These include, for example, dimensions, electrical characteristics, or necessary environmental conditions.

Fire safety standards must be upheld with the device in its installed state.

The device must not be damaged in any way when mounting it. In particular, holes must not be drilled into the housing.

For safety reasons, the device with the highest mass should be installed at the lowest position in the rack. Further devices should be installed from the bottom, working your way up.

The device must be protected against mechanical & physical stresses such as vibration or shock.

Connecting Data Cables

Do not connect or disconnect data cables during a thunderstorm, as doing so presents a risk in the event of a lightning strike.

The device cables must be connected or disconnected in the order specified in the user documentation for the device. Cables should always be held by the connector body when connecting or disconnecting them. Never pull a connector out by pulling on the cable. Doing so may cause the plug to be detached from the cable or cause damage to the plug itself.

Cables must be installed so that they do not represent a health & safety hazard (e.g., tripping) and are not at risk of damage (e.g., kinks).

Connecting the Power Supply

This equipment is operated at a hazardous voltage. Failure to observe the safety instructions in this manual may result in serious injury, death or property damage.

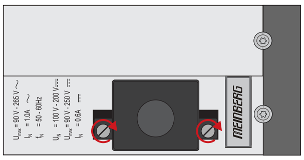
Before the device is connected to the power supply, a grounding conductor must be connected to the earth terminal of the device.

The power supply should be connected with a short, low-inductance cable.

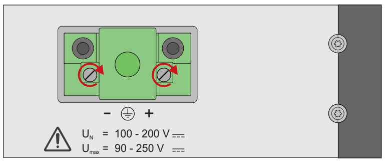
Before operation, check that all cables and lines work properly and are undamaged. Ensure in particular that the cables do not have kinks, that they are not wound too tightly around corners, and that no objects are placed on the cables.

Ensure that all connections are secure—make sure that the lock screws of the power supply plug are tightened when using a 3-pin MSTB or 5-pin MSTB connector (see diagram, LANTIME M300 power supply).

5-Pin MSTB Connector



3-Pin MSTB Connector



Faulty shielding or cabling and improperly connected plugs are a health & safety risk (risk of injury or death due to electrical shock) and may damage or even destroy your Meinberg device or other equipment.

Ensure that all necessary safety precautions have been taken. Connect all cables to the device only while the device is de-energized before turning on the power. Observe the safety instructions on the device itself (see safety symbols).

The metal chassis of the device is grounded. When installing the device in an electrical enclosure, it must be ensured that adequate clearance is provided, creepage distances to adjacent conductors are maintained, and that there is no risk of short circuits.

In the event of a malfunction or if servicing is required (e.g., damage to the chassis or power cable, ingress of fluids or foreign objects), the power supply may be cut off.

Please address any questions regarding your building's electrical, cable or antenna installations to the person or department responsible for that installation within your building.

AC Power Supply	DC Power Supply
• The device is a Protection Class 1 device and may only be connected to a grounded outlet (TN system). • For safe operation, the installation must be protected by a fuse of a rating not exceeding 16 A and equipped with a residual-current circuit breaker in accordance with applicable national standards. • The disconnection of the appliance from the mains power supply must always be performed from the mains socket and not from the appliance itself. • Mains-powered appliances are equipped with a safety-tested mains cable designed for use in the country of operation and may only be connected to a grounded shockproof socket, otherwise electric shock may occur. • Make sure that the mains socket on the appliance or the mains socket of the house installation is readily accessible for the user so that the mains cable can be pulled out of the socket in an emergency.	• In accordance with IEC 62368-1, it must be possible to disconnect the appliance from the supply voltage from a point other than the appliance itself (e.g., from the primary circuit breaker). • The power supply plug may only be fitted or dismantled while the appliance is isolated from the power supply (e.g., disconnected at the primary circuit breaker). • Supply cables must be adequately secured and have an adequate wire gauge size. *Connection Cable Wire Gauge:* *1 mm^2 – 2.5 mm^2* *17 AWG – 13 AWG* • The power supply of the device must have a suitable disconnection mechanism such as a switch. This disconnection mechanism must be readily accessible in the vicinity of the appliance and marked accordingly as a cut-off mechanism for the appliance.

2.5 Connection of Protective Earth Conductor/Grounding

ATTENTION!

In order to ensure that the device can be operated safely and to meet the requirements of IEC 62368-1, the device must be correctly connected to the protective earth conductor via the protective earth connection terminal.

If an external earth terminal is provided on the housing, it must be connected to your bonding busbar (grounding busbar). The parts required to attach the device to a grounding busbar are not included with the shipped product.

Note:
Please use a grounding cable with a core cross-section of $\geq 1.5\ \text{mm}^2$
Always ensure that the connection is properly crimped!

2.6 Safety during Operation

WARNING!

Avoiding Short-Circuits
Protect the device against all ingress of solid objects or liquids. Ingress presents a risk of electric shock or short-circuiting!

Ventilation Slots
Ensure that the ventilation slots are clean and uncovered at all times. Blocked ventilation slots may cause heat to be trapped in the system, resulting in overheating. This may cause your device to malfunction or fail.

Appropriate Usage
The device is only deemed to be appropriately used and EMC limits (electriomagnetic compatibility) are only deemed to be observed if the chassis cover is properly fitted (thus ensuring that the device is properly cooled, fire-safe, and shielded against electrical, magnetic and electromagnetic fields).

Switching the Device Off in the Event of a Malfunction or when Repairs are Required
It is not sufficient to simply switch off the device itself in order to disconnect the power supply.
If the device is malfunctioning, or if repairs become necessary, the device must be isolated from all power supplies immediately.

To do so, follow the procedure below:

- Switch off the device from the unit itself.
- Pull out all power supply plugs.
- Inform the person or department responsible for your electrical installation.
- If your device is connected to an Uninterruptible Power Supply (UPS), it will remain operational even after pulling the UPS power cable from the mains socket. In this case, you will need to shut down your UPS in accordance with the user documentation of your UPS system.

2.7 Safety during Maintenance

WARNING!

The device must never be opened. Repairs to the device may only be performed by the manufacturer or by authorized personnel. Improper repairs may expose the user to considerable safety risks (electric shock, fire hazard).

Opening the device or individual device components in an unauthorized fashion may also expose the user to considerable risks and invalidate your warranty.
Meinberg Funkuhren accepts no liability for consequences arising from such unauthorized actions.

Danger from moving parts—do not touch moving parts.

Parts of the device may become very hot during operation. Do not touch these surfaces!
If necessary, switch off the device before installing or removing any equipment, and allow it to cool down.

2.8 Handling of Batteries

⚠ WARNING!

The lithium battery on the receiver modules has a life of at least ten years. Should it be necessary to replace it, please note the following:

Improper handling of the battery can lead to an explosion or to a leakage of flammable liquids or gases.

- Never short-circuit the battery.
- Never attempt to recharge the battery.
- Never throw the battery into a fire.
- The battery must only be exposed to the barometric pressure range specified by the battery manufacturer.
- The battery must only ever be replaced with one of the same type or a comparable type recommended by the manufacturer. The battery must only be replaced by the manufacturer or an authorized technician.
- Never dispose of the battery in a mechanical crusher or shredder, or in an open fire or furnace.
- Please consult your local waste disposal regulations for information on how to dispose of hazardous waste.

ATTENTION!

The battery is used to power components such as the RAM and the reserve real-time backup clock for the reference clock.

If the battery voltage drops below 3 V DC, Meinberg recommends having the battery replaced. If the battery voltage drops below the specified minimum, the following behavior may be observed in the reference clock:

- The reference clock may have the wrong date or wrong date upon power-up
- The reference clock repeatedly starts in Cold Boot mode
- Some of the configurations saved for the reference clock may be lost

2.9 Cleaning and Care

ATTENTION!

Never clean the device using liquids! Water ingress is a significant safety risk for the user (e.g., electric shock).

Liquids can cause irreparable damage to the electronics of the device! The ingress of liquids into the device chassis may cause short circuits in the electronic circuitry.

Only clean with a soft, dry cloth. Never use solvents or cleaners.

2.10 Prevention of ESD Damage

ATTENTION!

An ESDS device (electrostatic discharge-sensitive device) is any device at risk of damage or malfunction due to electrostatic discharges (ESD) and thus requires special measures to prevent such damage or malfunction. Systems and modules with ESDS devices usually bear the following symbol:

Symbol Indicating Devices with ESDS Components

The following measures will help to protect ESDS components from damage and malfunction.

When preparing to dismantle or install devices:
Ground your body (for example, by touching a grounded object) before touching sensitive devices.

Ensure that you wear a grounding strap on your wrist when handling such devices. These straps must in turn be attached to an uncoated, non-conductive metal part of the system.

Use only tools and devices that are free of static electricity.

When transporting devices:
Devices must only be touched or held by the edges. Never touch any pins or conductors on the device.

When dismantling or installing devices:
Avoid coming into contact with persons who are not grounded. Such contact may compromise your connection with the earth conductor and thus also compromise the device's protection from any static charges you may be carrying.

When storing devices:
Always store devices in ESD-proof ("antistatic") bags. These bags must not be damaged in any way. ESD-proof bags that are crumpled or have holes cannot provide effective protection against electrostatic discharges.

ESD-proof bags must have a sufficient electrical resistance and must not be made of conductive metals if the device has a lithium battery fitted on it.

2.11 Return of Electrical and Electronic Equipment

ATTENTION!

WEEE Directive on Waste Electrical and Electronic Equipment 2012/19/EU
(WEEE Waste Electrical and Electronic Equipment)

Waste Separation
Product Category: According to the device types listed in Annex I of the WEEE Directive, this product is classified as "IT and Telecommunications Equipment".

This product satisfies the labeling requirements of the WEEE Directive. The product symbol on the left indicates that this electronic product must not be disposed of in domestic waste.

Return and Collection Systems
When disposing of your old equipment, please use the national return or collection systems available to you. Alternatively, you may contact Meinberg, who will provide further assistance.

The return of electronic waste may not be accepted if the device is soiled or contaminated in such a way that it potentially presents a risk to human health or safety.

Return of Used Batteries
The EU Battery Directive prohibits the disposal of batteries marked with the WEEE trashcan symbol above in household waste.

3 Before you start

3.1 Text and Syntax Conventions

This chapter briefly describes the text and syntax conventions used in this manual.

Web Interface: example "Menu Network"
Submenu "Network → Network Interfaces"
Items in Submenu "Network → Network Interfaces → IPv4"

The menu navigation is logically separated by an right arrow ()→.

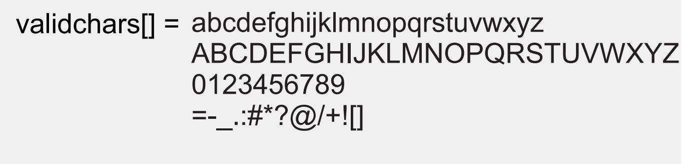
Directory names / Paths Example: Lantime configuration file
The directory names and paths are displayed in italics.

Code and CLI Commands

```
- cmd/www-upload.htm

#Program code and CLI commands are displayed in a grey box with monospace
font.
```

User passwords:
The following characters are currently allowed for user passwords and shared secret:

Allowed character set for both:



```
validchars[] = abcdefghijklmnopqrstuvwxyz
               ABCDEFGHIJKLMNOPQRSTUVWXYZ
               0123456789
               =-_.:#*?@/+![]
```

3.2 Required Tools

	LANTIME IMS SERIES						
	LANTIME M1000	LANTIME M1000S	LANTIME M2000S	LANTIME M3000	LANTIME M3000S	LANTIME M4000	LANTIME M500
Mounting Rackears	TORX T20	TORX T20	TORX T20	TORX T20	TORX T20	TORX T20	x
Mounting DIN rail	x	x	x	x	x	x	Phillips PH1 x 80
Replacing IMS modules	TORX T8	TORX T8	TORX T8	TORX T8	TORX T8	TORX T8	TORX T8
FAN Installation	TORX T8	TORX T8	TORX T8	TORX T8	x	TORX T8 Flat head Screwdriver	x

	LANTIME SERIES						
	LANTIME M100	LANTIME M200	LANTIME M300	LANTIME M400	LANTIME M600	LANTIME M900	SyncFire
Mounting Rackears	x	TORX T20	TORX T20	x	TORX T20	TORX T20	x
Mounting DIN rail	Phillips PH1 x 80	x	x	Phillips PH1 x 80	x	x	x
Replacing Modules	x	x	x	x	x	TORX T8	TORX T10

Figure: Required tools from left to right - INBUS 2,5mm, Phillips PH1 x 80, Flat head Screwdriver, TORX T20, TORX T8

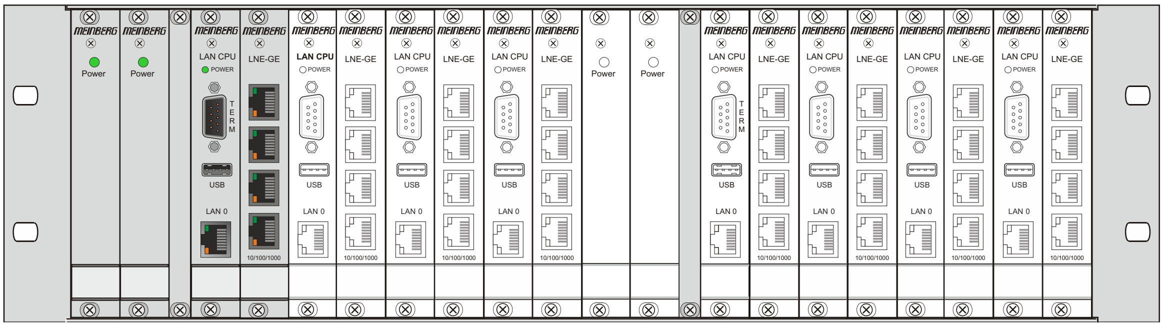
3.3 Abbreviation List

AFNOR	Association Francaise de Normalisation time codes
AC	Alternating Current
ASCII	American Standard Code for Information Interchange
BMC	Best Master Clock
BNC	Bayonet Neil Councilman connector
Bps	Bytes per second
bps	Bits per second
CAT5	Standard Network Cable
CET	Central European Time
CLI	Command Line Interface
DB9	Connector do type D-subminiature
DC	Direct Current
DCF77	Is a longwave time signal. DCF77 stands for D=Deutschland (Germany), C=long wave signal, F=Frankfurt, 77=frequency: 77.5 kHz.
DCFMARK	Single pulse with a programmable date and time
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSCP	Differentiated Services Code Points
DST	Daylight Saving Time
E1	European digital transmission signal at 2.048 MHz used in telecommunication networks.
E2E	End-to-end
ETH	Ethernet
FTP	File Transfer Protocol
FW	Firmware
GE / GbE	Gigabit Ethernet
GLONASS	GLObal NAvigation Satellite System from Russian Aerospace Defense Forces
GND	Ground (Connector)
GNSS	Global Navigation Satellite System (GPS, GLONASS, Galileo, Beidou)
GOAL	GPS Optical Antenna Link
GPS	Global Positioning System (USA)
GSM	Global System for Mobile Communications
HMI	Human-Machine Interface
HP	Horizontal Pitch - is a unit measure the horizontal width of rack mounted electronic equipment
HPS	High Performance Synchronization PTP/NTP/SyncE GBit module
HSR	High-availability Seamless Redundancy
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute of Electric and Electronic Engineers
IEEE 1588	Protocol for high-precision synchronization in nanosecond range (PTP)
IP	Internet Protocol
IP 20	Protection Class 20
IRIG	Inter-range instrumentation group time codes
LCD	Liquid Crystal Display
LDAP(S)	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
LINUX	Unix-like multi-user computer operating system
LIU	Line Interface Unit- an module for generation E1/T1 Signals, both MBit/s (framed) and Clock (unframed)
LNE	Local Network Extention, additional Ethernet Ports
MAC	Media Access Control
MD5	Message-Digest cryptographic hash function
MESZ	Middle European Summer Time
MEZ	Middle European Time
MIB	Management Information Base
MRS	Multi Reference Source
MSF	Time signal transmitter in Anthorn, UK
NIST	National Institute of Standards and Technology
NMEA	Communication standard from National Marine Electronics Association
NTP	Network Time Protocol
NTPD	NTP Deamon
OSV	Original Shipped Version (Firmware)
OUT	Output
P2P	Peer-to-Peer
PLC	Programmable Logic Controller
PLL	Phase Locked Loop
PPM	Pulse per Minute
PRP	Parallel Redundancy Protocol
PPS	Pulse per Second
PPH	Pulse per Hour
PTB	Physical - Technical Institute Braunschweig / Germany
PTP	Precision Time Protocol
RAM	Random Access Memory
RF	Frequency of radio waves, from 3kHz to 300GHz
RG58	Standard coaxial cable used to connect an antenna and a receiver
RJ45	Ethernet Connector with 8 conductors
RMC	Remote Monitoring Control
RoHS	Restriction of Hazardous Substances
RPS	Redundant Power Supply
RS232/485	Serial port levels
RSC	Redundant Switch Control unit
RX	Receiving Data
SBC	Single Board Computer
SDU	Signal Distribution Unit

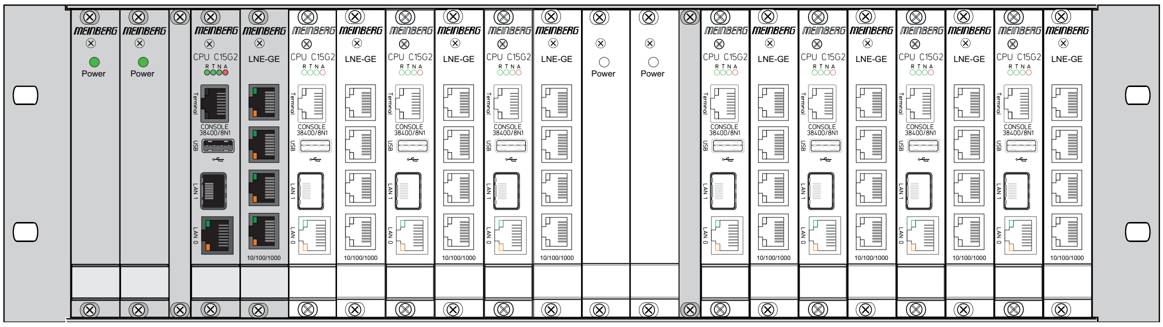
SHA-1	Secure Hash Algorithm 1
SMB	Subminiature coaxial connector
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SMTP	Simple Mail Transfer Protocol
SPS	Standard Positioning System
SSH	Secure SHell network protocol
SSU	Synchronization Supply Unit, specific clock used in telecommunication networks
SSM	Sync Status Messages, clock quality parameters in telecommunication networks.
ST	Bayonet-lock connector
Stratum	Value defines the NTP hierarchy
SYSLOG	Standard for computer data logging
TACACS	Terminal Access Controller Access Control System
TCG	Time Code Generator
TCR	Time Code Receiver for IRIG A/B, AFNOR or IEEE1344 codes
T1	North American telecommunication signal at 1.544 MHz frequency
TCP	Transmission Control Protocol
TTL	Transistor-to-Transistor Logic
TX	Data Transmission
U	Unit - is a unit measure the vertical height of rack mounted electronic equipment.
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UNIX	Multitasking, multi-user computer operating system
UTC	Universal Time Coordinate
VLAN	Virtual Local Area Network
WWVB	Time signal radio station Fort Collins, Colorado (USA)

4 The Modular System LCES-NTP

LCES-NTP is a set of equipment composed of up to eight LAN-CPU, LNE network expansion boards together with two or four power supply units - depending on system configuration (see chapter power supply). All components are installed in a metal 19" modular chassis and ready to operate. The interfaces provided by LCES are accessible via connectors in the front and rear panel of the chassis.



LCES in subrack with LAN CPU C05F1 - Geode^{TM} LX800



LCES in subrack with LAN CPU C15G2 - Intel® Atom^{TM} Processor E Series

5 Technical specifications 3U Chassis

Housing	Chassis 19" / 3U
Housing material	Aluminium

Temperature range

Operation	0 ... 50 °C (32 ... 122 °F)
Storage	-20 ... 70 °C (-4 ... 158 °F)

Relative humidity

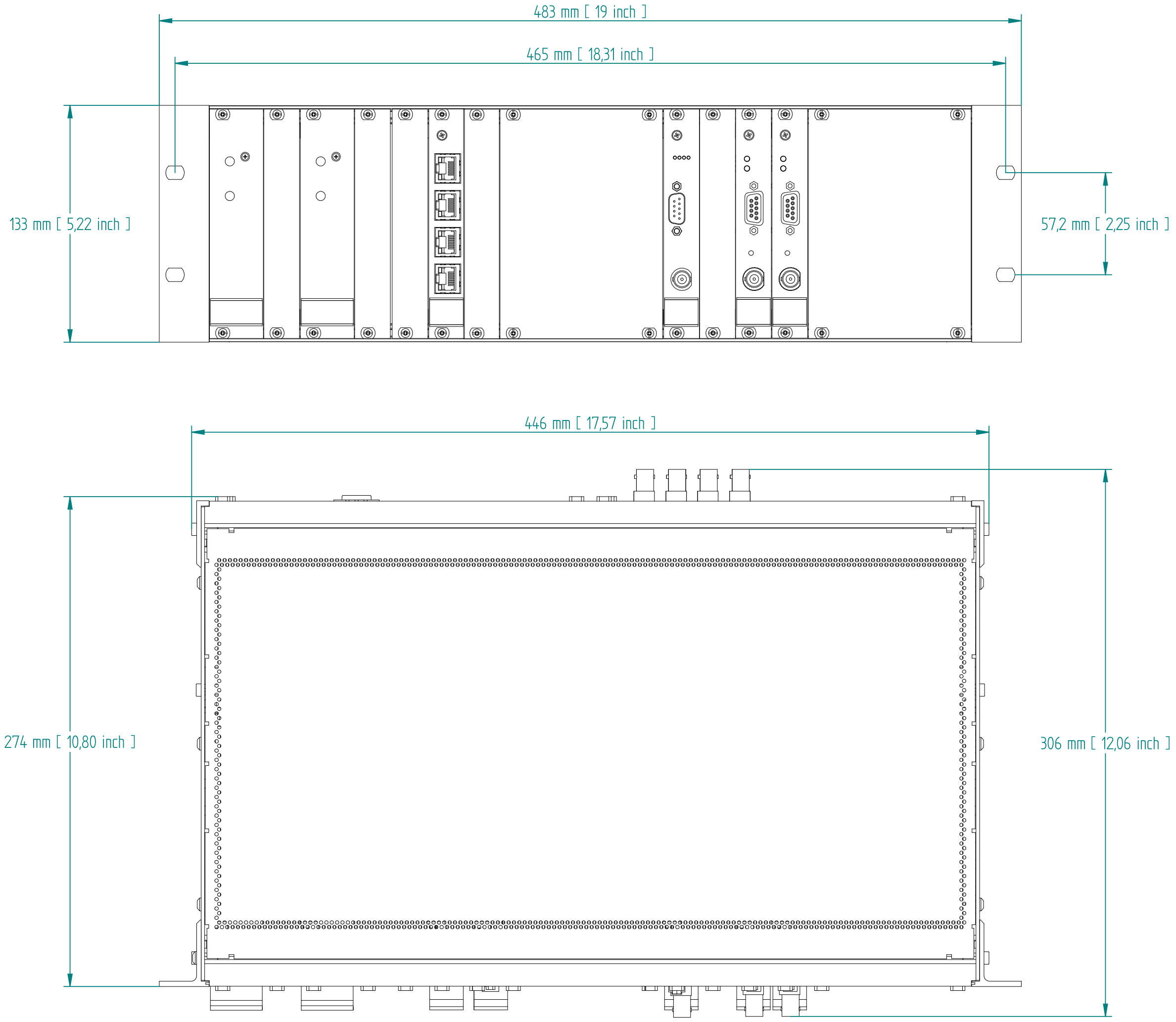
Operation	85 % max. (non-condensing)

Operation height

Operation	2000 m / 6562 ft (above sea level)

Acoustics	0 dB (A)
IP protection class	IP20

Housing dimensions



6 Network Time Protocol (NTP)

NTP is a common method for the synchronization of hardware clocks in local and global networks. The basic concept, version 1 [Mills88], was published in 1988 as RFC (Request For Comments). Experiences acquired from its practical use on the Internet was followed by version 2 [Mills89]. The NTP software package is an implementation of the actual version 3 [Mills90], based on the specification RFC-1305 from 1990 (directory doc/NOTES). Permission to use, copy, modify and distribute this software for any purpose and without fee is hereby granted (read File COPYRIGHT).

NTP operates in a way that is basically different from that of most other timing protocols. NTP does not synchronize all connected clocks; instead it forms a hierarchy of timeservers and clients. Each level in this hierarchy is called a stratum, and Stratum 1 is the highest level. Timeservers at this level synchronize themselves by means of a reference time source such as a radio controlled clock, satelliet receiver or modem time distribution. Stratum 1 Servers distribute their time to several clients in the network which are called Stratum 2.

Highly precise synchronization is feasible because of the several time references. Every computer synchronizes itself with up to three valued time sources. NTP enables the comparison of the hardware times and the adjustment of the internal clock. A time precision of 128 ms, and often better than 1 ms, is possible.

6.1 NTP Clients

The NTP software package was tested on different UNIX systems. Almost all UNIX-like systems come with a pre-installed NTP client software. In order to use the LANTIME as an NTP server, it is required to add its IP address to the client configuration. NTP client software are available for most other operating systems like Microsoft Windows or MAC OS.

The following WEB site is recommended to get the latest version of NTP:
http://www.ntp.org

You can find more information on our web page at: https://www.meinbergglobal.com/english/sw/ntp.htm

7 Security User Guide / Security Advisories

This Chapter describes the configuration of a LANTIME series operating system (LTOS) in terms of security features. It is divided in the following sections: general overview, securing the management, securing the time services and additional information about event log delivery. Finally, some advisories for the update process of a LANTIME are given.

The general knowledge about public key infrastructures, RSA, symmetric keys and the protocols SSL, SSH, NTP and SNMP is assumed.

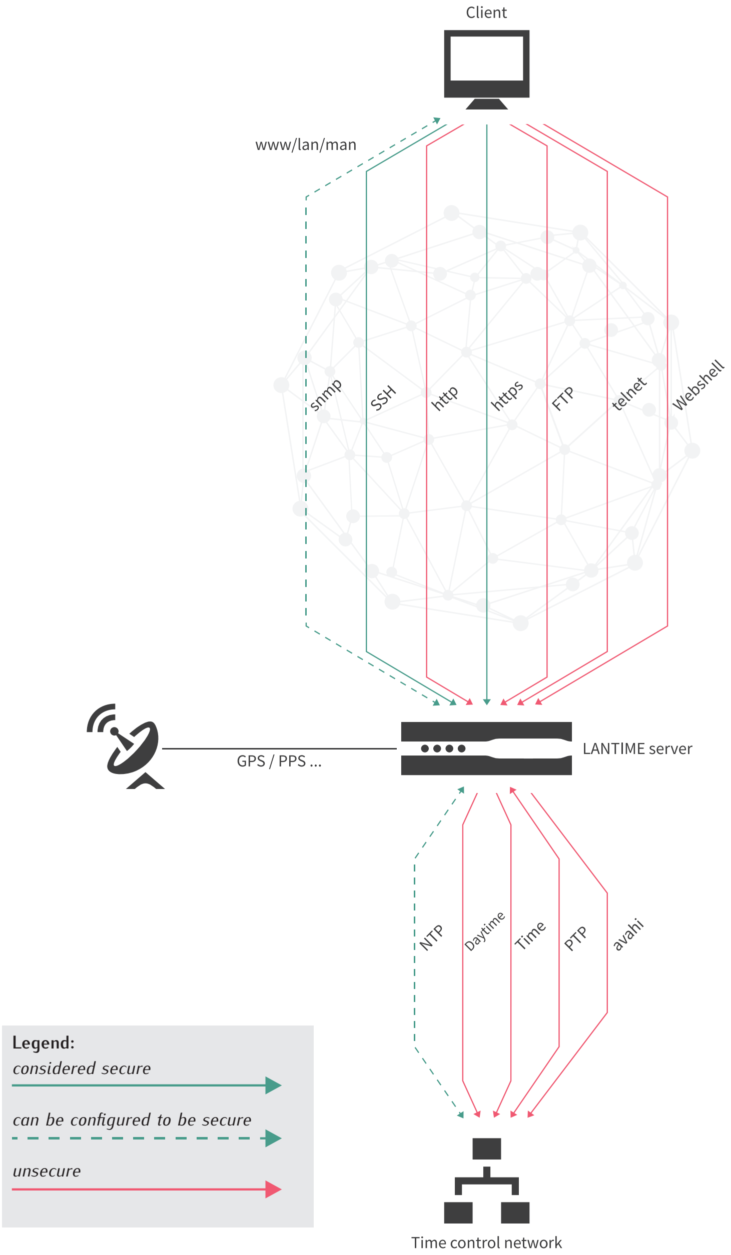


Figure 7.1: LANTIME Services

7.1 General Informations

Before starting with the configuration, take a look at Figure 7.1 to identify the possible services that can be configured to be secure.

In general, a secure management of the LANTIME is possible with SSH, HTTPS and SNMP. If the configuration via SNMP is desired, the usage of version 3 is the only way to get a secure connection to manage the system. It is a good practice to deactivate all services that are not in use, to minimize the attack surface. So if possible, only enable one of the services (SNMP has not the full configuration support, but you can activate the other services over SNMP)!

The delivery of secured time information is only available for NTP. Please note, that the NTP protocol only supports integrity and authenticity but no confidentiality. PTP does not currently support IT security functions. These are only planned for the next protocol standard. For this reason, you must still use NTP to ensure secure time synchronization.

Another important advisory is to use the newest browsers and service clients to support the selection of the best security algorithms for server and client communication. A timely installation of updates can also close known vulnerabilities and minimize the risk of a successful attack.

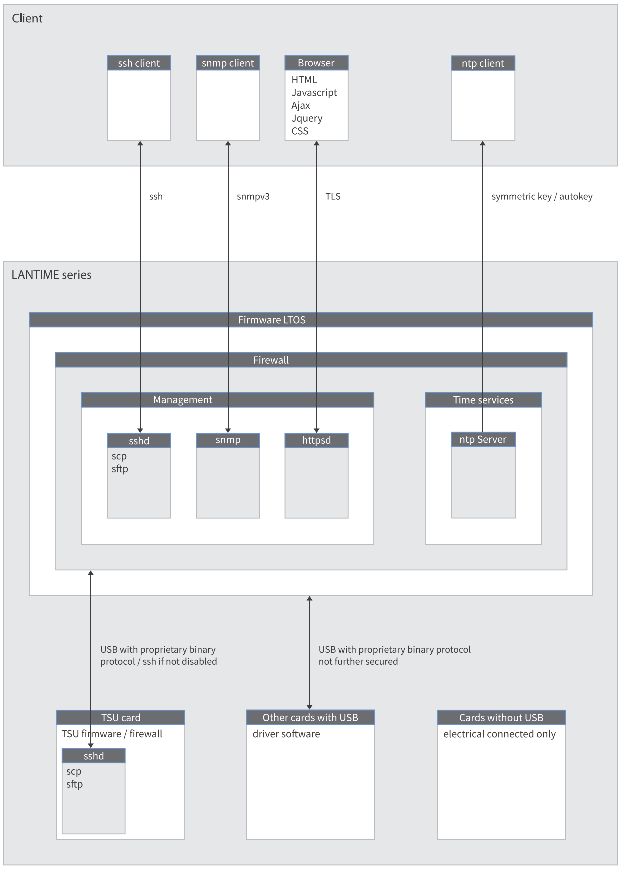
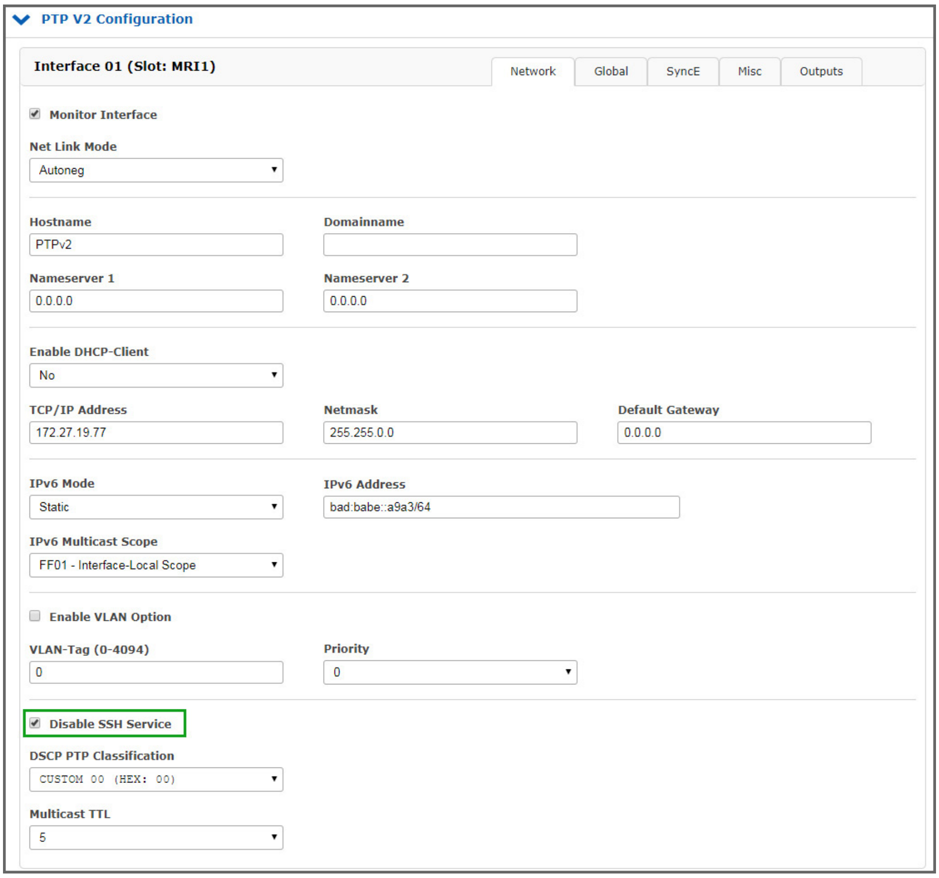


Figure 7.2: The secure protocols in detail

The current firmware version LTOS V7 of Meinberg's TSU boards no longer offers the ability to establish an SSH connection via network. Access is only allowed via the CPU module of the LANTIME. It is still possible to completely disable the SSH service of a TSU card as shown in Figure 7.3.



PTP V2 Configuration

Interface 01 (Slot: MRI1)

☑ Monitor Interface

Net Link Mode: Autoneg

Hostname: PTPv2
Domainname:

Nameserver 1: 0.0.0.0
Nameserver 2: 0.0.0.0

Enable DHCP-Client: No

TCP/IP Address: 172.27.19.77
Netmask: 255.255.0.0
Default Gateway: 0.0.0.0

IPv6 Mode: Static
IPv6 Address: bad:babe::a9a3/64

IPv6 Multicast Scope: FF01 - Interface-Local Scope

☐ Enable VLAN Option

VLAN-Tag (0-4094): 0
Priority: 0

☑ Disable SSH Service

DSCP PTP Classification: CUSTOM 00 (HEX: 00)

Multicast TTL: 5

Figure 7.3: Disable SSH on TSU

Services	Confidentiality	Integ.	Avail.	Auth.	Account.
https	x	x	0	x	(x)
ssh	x	x	0	x	(x)
ntp	–	x	0	x	(x)

Table: Security targets

The table shows the security goals of the protocols in short. The accountability is given through a detailed syslog of the actions performed by every user or process. However, the log files can be changed later by root or super users. For this reason, the system cannot guarantee the non-repudiation.

The most, possible availability of the services is realized through current updates and IP banning. For more protection, implement web application firewalls and traditional firewalls in the network, that are able to identify and prevent DOS/DDOS attacks.

With all changes to the configuration keep in mind, that they are lost after a reboot or could be discarded by other admins or super users , if they are not saved in the startup configuration.

7.2 Securing Management

The most secure way to configure a LANTIME is to connect the client directly to the LANTIME, until only secure channels are established. This guide uses the web interface over ssl as example.

After connecting a reference clock and the following start procedure of a LANTIME, an IP address can be configured via the front panel (see chapter "LTOS Management and Monitoring → Via Web GUI"). Now it is possible to connect to the web interface using the configured ip address. Use the initial credentials to login.

User: *root*
Password: *timeserver*

After you connected successfully, the first thing to do is to check, if it exists a new firmware version (see section Firmware/Software Update for update instructions). After the update is performed, generate or inject a ssl certificate. This example uses a new one. Figure 7.4 shows the button to start the generation.

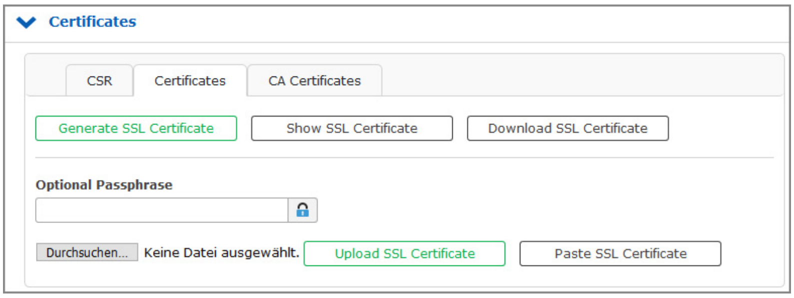
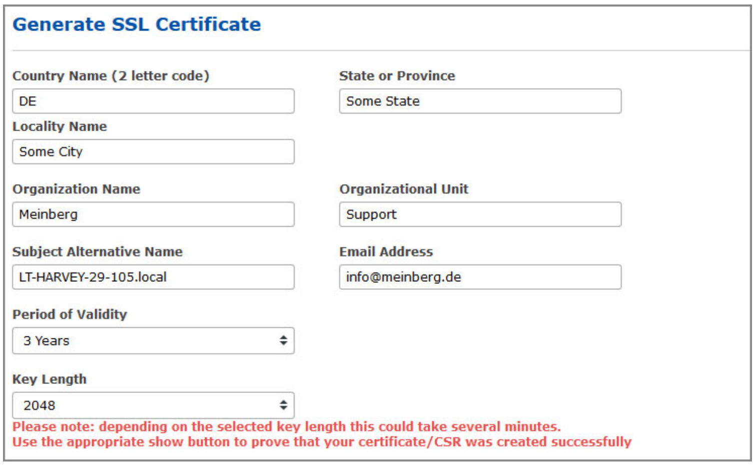


Figure 7.4: Generate SSL certificate step 1

On the next step you have to enter the information needed for the certificate (see also chapter "LTOS Management and Monitoring → Via Web Gui → Security"). Figure 7.5 shows the form. As key length, use 2048 or higher. Shorter durations of the period of validity are better than longer. In this example we select three years as a good trade of short duration and an acceptable management cost.

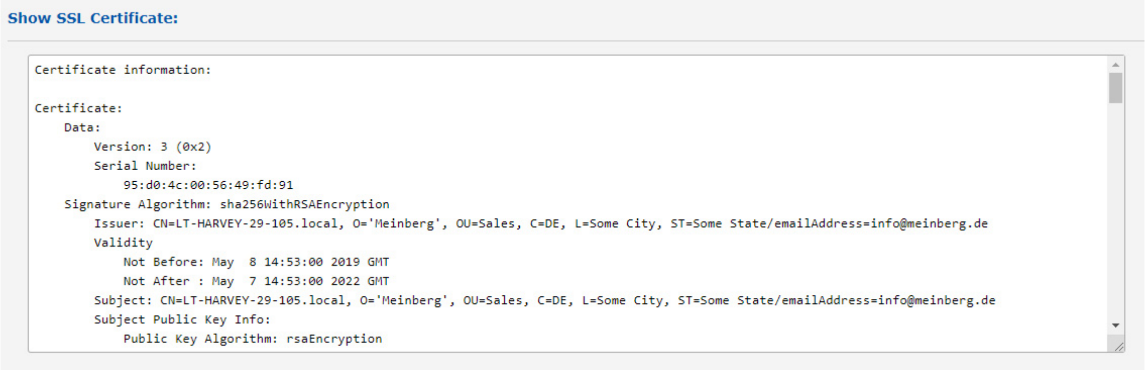


Generate SSL Certificate

Country Name (2 letter code): DE
State or Province: Some State
Locality Name: Some City
Organization Name: Meinberg
Organizational Unit: Support
Subject Alternative Name: LT-HARVEY-29-105.local
Email Address: info@meinberg.de
Period of Validity: 3 Years
Key Length: 2048

Please note: depending on the selected key length this could take several minutes.
Use the appropriate show button to prove that your certificate/CSR was created successfully

Figure 7.5: Generate SSL certificate step 2

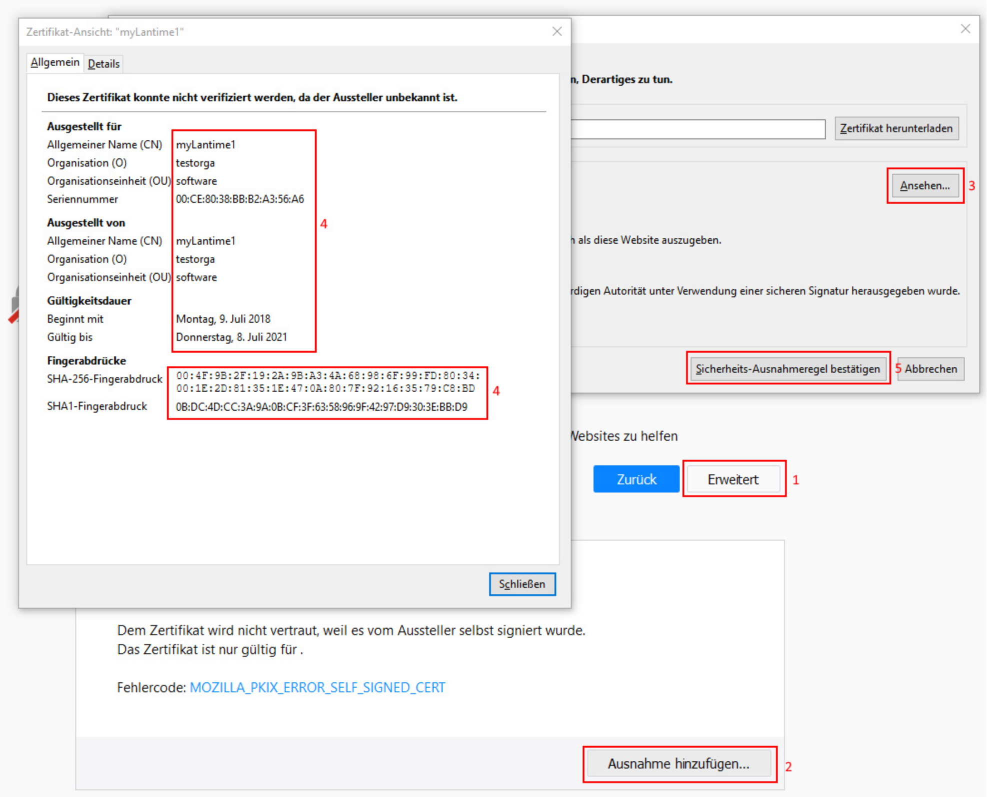


Show SSL Certificate:

```
Certificate information:

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            95:d0:4c:00:56:49:fd:91
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=LT-HARVEY-29-105.local, O='Meinberg', OU=Sales, C=DE, L=Some City, ST=Some State/emailAddress=info@meinberg.de
        Validity
            Not Before: May  8 14:53:00 2019 GMT
            Not After : May  7 14:53:00 2022 GMT
        Subject: CN=LT-HARVEY-29-105.local, O='Meinberg', OU=Sales, C=DE, L=Some City, ST=Some State/emailAddress=info@meinberg.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

Figure 7.6: |Show generated SSL certificate

You can view the generated certificate with the "Show SSL Certificate" button. Use it to compare it with the certificate provided by the browser on your next https connection to the LANTIME. Both should be identical! The import process is illustrated in Figure 7.7. The numbers in the figure describe the sequence of actions to perform. Number four represents the comparison with the previously downloaded certificate of the LANTIME. If both certificates are identical, you can go ahead with step five to confirm the confidence of the LANTIME certificate. Modern browser configurations will show you that the connection is not safe when you use a self signed certificate. Because of this behaviour, we recommend the implementation of a public key infrastructure to avoid the warning. Also make sure that you use a Subject Alternative Name (SAN), as modern browsers also check for this. For this purpose, you can generate a certificate request, download it, sign it and upload the signed certificate again via the web front end on Figure 7.4.



Zertifikat-Ansicht: "myLantime1"

Dieses Zertifikat konnte nicht verifiziert werden, da der Aussteller unbekannt ist.

Ausgestellt für

Allgemeiner Name (CN)	myLantime1
Organisation (O)	testorga
Organisationseinheit (OU)	software
Seriennummer	00:CE:80:38:BB:B2:A3:56:A6

Ausgestellt von

Allgemeiner Name (CN)	myLantime1
Organisation (O)	testorga
Organisationseinheit (OU)	software

Gültigkeitsdauer

Beginnt mit	Montag, 9. Juli 2018
Gültig bis	Donnerstag, 8. Juli 2021

Fingerabdrücke

SHA-256-Fingerabdruck	00:4F:9B:2F:19:2A:9B:A3:4A:68:98:6F:99:FD:80:34: 00:1E:2D:81:35:1E:47:0A:80:7F:92:16:35:79:C8:BD
SHA1-Fingerabdruck	0B:DC:4D:CC:3A:9A:0B:CF:3F:63:58:96:9F:42:97:D9:30:3E:BB:D9

n, Derartiges zu tun.

h als diese Website auszugeben.

rdigen Autorität unter Verwendung einer sicheren Signatur herausgegeben wurde.

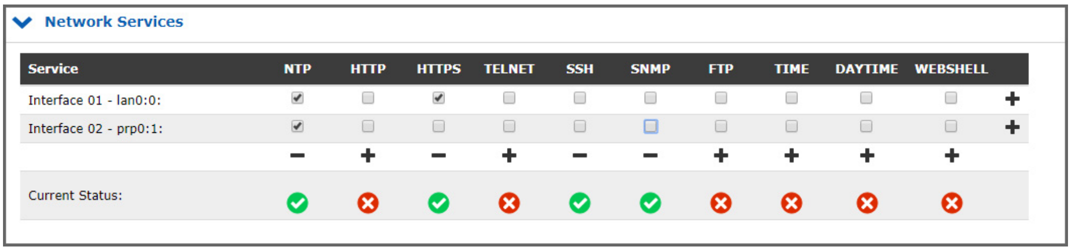
Websites zu helfen

Dem Zertifikat wird nicht vertraut, weil es vom Aussteller selbst signiert wurde.
Das Zertifikat ist nur gültig für .

Fehlercode: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

Figure 7.7: Import process of the new SSL certificate in the browser

If the connection over https is possible, you can deactivate all other unused services like on Figure 7.8. Additionally, in this example only one network interface provides the https web interface. Thus, scenarios like a dedicated configuration network are possible, too.

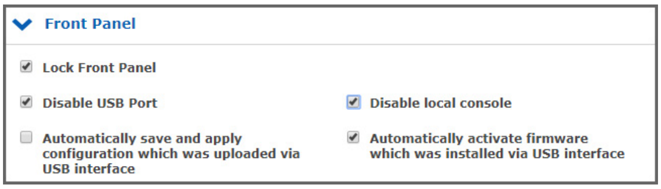


Network Services

Service	NTP	HTTP	HTTPS	TELNET	SSH	SNMP	FTP	TIME	DAYTIME	WEBSHELL	
Interface 01 - lan0:0:	☑	□	☑	□	□	□	□	□	□	□	+
Interface 02 - prp0:1:	☑	□	□	□	□	□	□	□	□	□	+
	−	+	−	+	−	−	+	+	+	+	
Current Status:	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	

Figure 7.8: Deactivating services

For the next step, one other super user than root is needed. Go to section 7.3 to create one. After creation of the new super user, log in with its credentials and disable the root login under "Security → Login/Access → Disable Root Login". Deactivate the front panel, USB port and local console under "Security → Front Panel" if desired. In addition, you can set the remote access control to white listed IP addresses that are allowed to connect to the web interface (Hint: The Remote Access Control does not take effect for SSH connections). Figure 7.9 shows the menus.



Front Panel

☑ Lock Front Panel

☑ Disable USB Port

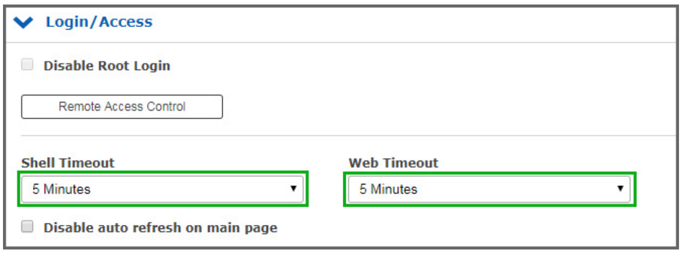
☑ Disable local console

□ Automatically save and apply configuration which was uploaded via USB interface

☑ Automatically activate firmware which was installed via USB interface

Figure 7.9: Deactivation of root and front panel

The timeout for web sessions is configured on the "Security" tab under "Login / Access" which is displayed in Figure 7.10. Shorter durations minimize the security risk.



Login/Access

□ Disable Root Login

Shell Timeout: 5 Minutes

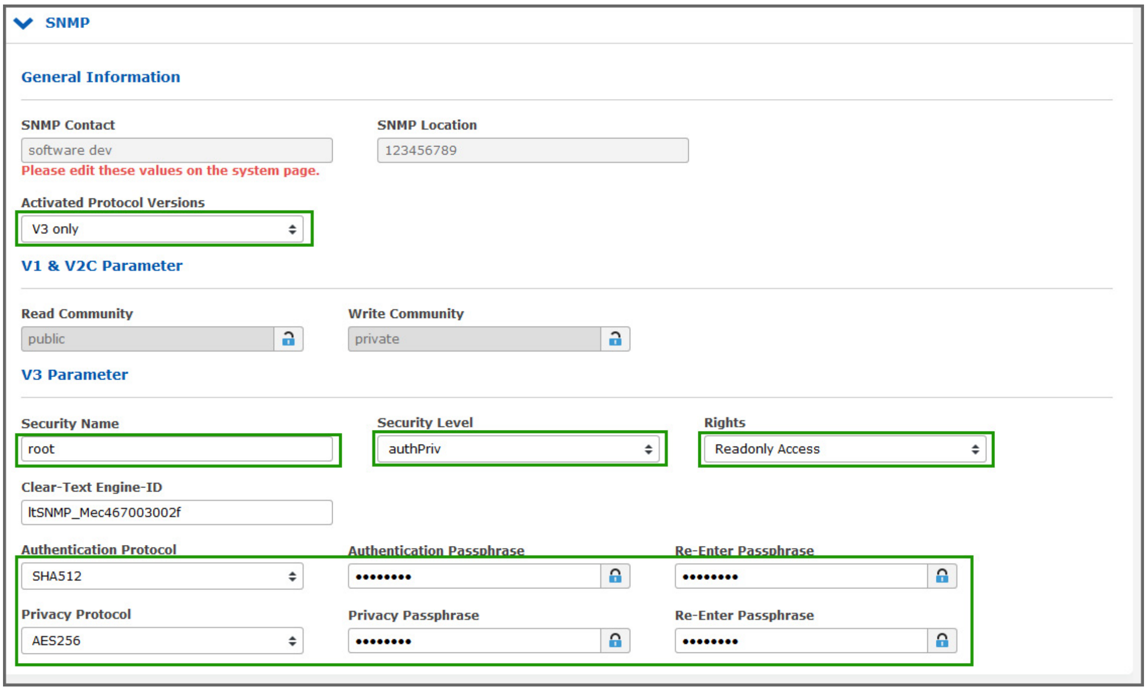
Web Timeout: 5 Minutes

□ Disable auto refresh on main page

Figure 7.10: Set timeout of web interface

From now on, the LANTIME is well configured to be managed secure. Keep in mind to check if the IP configuration and remote access control work in the productive network environment.

Optionally, you can configure SNMP to manage the LANTIME. The security options can be found under "Security → SNMP". Figure 7.11 shows the menu. To establish a secure connection via SNMP you have to use version 3 and the **authPriv** mode. The additional parameters of version 3 are the user name (security name), the access rights, the authentication and privacy protocol/algorithms. Use SHA512 and AES256 as algorithms. As usual, longer passwords are preferred. Start the SNMP service on "Network → Network Services" tab afterwards.



SNMP

General Information

SNMP Contact: software dev

Please edit these values on the system page.

SNMP Location: 123456789

Activated Protocol Versions: V3 only

V1 & V2C Parameter

Read Community: public

Write Community: private

V3 Parameter

Security Name: root

Security Level: authPriv

Rights: Readonly Access

Clear-Text Engine-ID: ltSNMP_Mec467003002f

Authentication Protocol: SHA512

Authentication Passphrase: ••••••••

Re-Enter Passphrase: ••••••••

Privacy Protocol: AES256

Privacy Passphrase: ••••••••

Re-Enter Passphrase: ••••••••

Figure 7.11: SNMP options

7.3 User Management/Administration

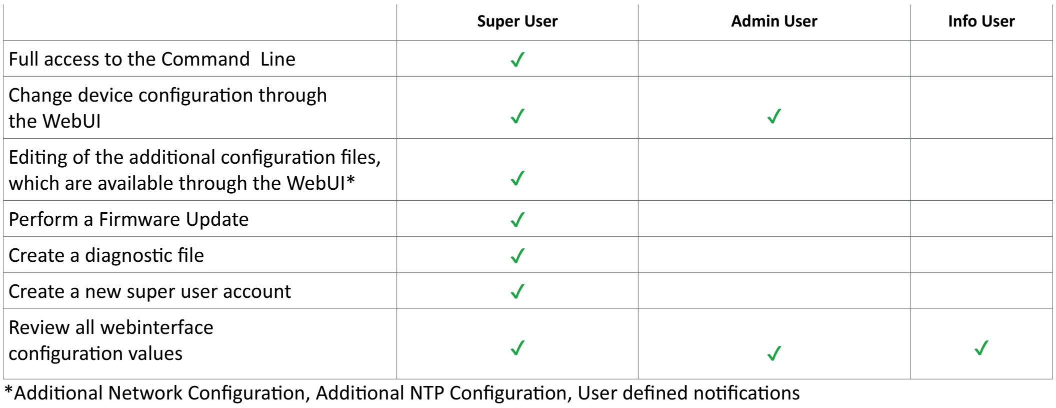
This section describes the administration of user and authentication management. Therefore, it is divided in LANTIME origin and external user authentication. The LANTIME OS supports the two external authentication servers, Radius and TACACS+. You can also see "LTOS Management and Monitoring → Via Web GUI → System → External Authentification" for further information.

7.3.1 LANTIME User Management

The LANTIME delivers a build in user configuration. The options are located under "System → User Management".

There are three different user groups: Super-User, Admin-User and Info-User. Super-Users are allowed to do everything, bash access included. Admin-Users are allowed to do everything that is on the web interface, but no operations that would grant super user rights. Info-Users are just allowed to see all non security relevant informations in the web interface.

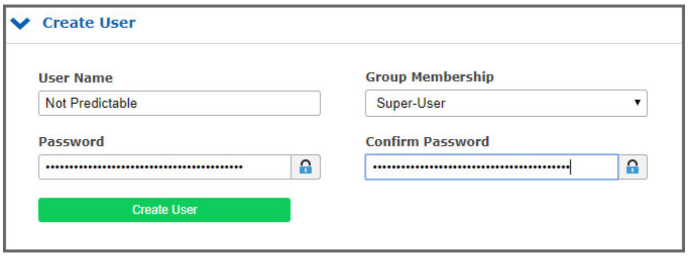
The table below illustrates the user-rights of each access level in detail.



	Super User	Admin User	Info User
Full access to the Command Line	✓		
Change device configuration through the WebUI	✓	✓	
Editing of the additional configuration files, which are available through the WebUI*	✓		
Perform a Firmware Update	✓		
Create a diagnostic file	✓		
Create a new super user account	✓		
Review all webinterface configuration values	✓	✓	✓

*Additional Network Configuration, Additional NTP Configuration, User defined notifications

To create a User, use the form that is shown on Figure 7.12. Super-Users can create all user types. The Admin-User can create other Admin-Users and Info-Users. Enter a name, a password and the group of the user, then press the button **Create User**. If successful, the new user is displayed in the User List, right under the create user form. Choose the user names and passwords in a way that they are not predictable.



Create User

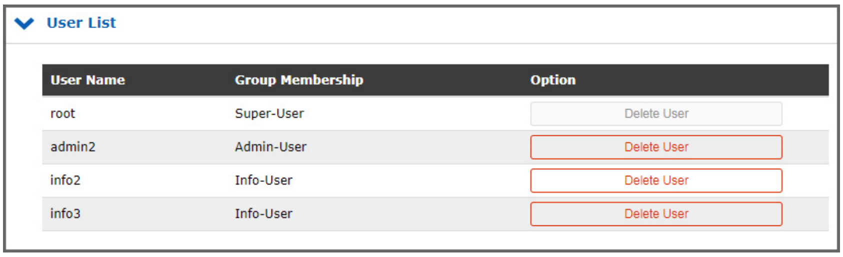
User Name: Not Predictable

Group Membership: Super-User

Password: •••

Confirm Password: •••

Figure 7.12: Create new Super User

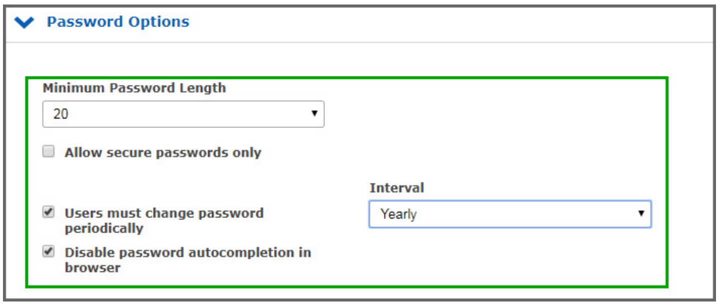


User List

User Name	Group Membership	Option
root	Super-User	Delete User
admin2	Admin-User	Delete User
info2	Info-User	Delete User
info3	Info-User	Delete User

Figure 7.13: User List

For passwords, there are some additional options that are depicted in Figure 7.14. Choose a long password length and a periodical change interval. In addition, you can use the "Allow secure passwords only" checkbox to force a password that contains many different character sets.



Password Options

Minimum Password Length: 20

□ Allow secure passwords only

☑ Users must change password periodically

Interval: Yearly

☑ Disable password autocompletion in browser

Figure 7.14: Password Options

7.3.2 External User Authentication: LDAP(S), Radius and TACACS+

This chapter describes the possible external authentication methods provided by the LANTIME firmware.

LDAP (Lightweight Directory Access Protocol)
LDAP is based on the client-server model and is used for so-called directory services. LDAP describes the communication between the LDAP client and the directory server. Object-related data, such as personal data or computer configurations, can be read from such a directory.

RADIUS (Remote Authentication Dial-In User Service)
A RADIUS server is a central authentication server used by services to authenticate clients on a physical or virtual network (VPN). The RADIUS server handles the authentication for the service, i.e. checking the user name and password.

TACACS (Terminal Access Controller Access-Control-System)
TACACS is a communication protocol for authentication, which is standardized and widely used by the IETF. TACACS servers provide a central authentication instance for users. In typical Cisco network environments (e.g. routers and switches), TACACS+ is used for central user management.

7.3.2.1 Order of Authentication Procedures

The order of authentication is as follows once all authentication methods (LDAP, RADIUS, TACACS+ and LOCAL) have been activated and configured

1. LDAP
2. RADIUS
3. TACACS+
4. local authentication

So if the same user names/password phrases are used in different systems, it is possible that the access rights do not work out as desired. In addition, this can quickly lead to intransparent log messages. So you should always pay attention to the order and consistent user data/rights in the services.

7.3.2.2 LDAP and LDAPS

The LANTIME supports the connection to an LDAP server via LDAP and LDAPS. Meinberg recommends setting up secure communication via LDAPS. For this purpose a central trust center (RootCA) must be made known to the LANTIME.

A certificate of a certification authority can be uploaded via the web interface menu "Security →" Certificates → CA Certificates". The section CA Certificates describes the options for uploading root CA certificates. If the LDAP server uses a certificate signed/issued by a global certificate authority, this step is omitted. The list of trusted global certificate authorities is updated with each LANTIME update.

The configuration of an LDAP(S) connection is described in chapter "Web Interface → User Management → External Authentication → 10.1.6.7 (LDAP Setup)".

7.3.2.3 External Authentication via LDAP

External authentication via LDAP can be configured in the web interface under "System → User Management → User Administration → External Authentication → LDAP / LDAPS". The LANTIME firmware supports anonymous as well as user related logon. For a Microsoft Active Directory logon, a user name (LDAP user or binddn) and a password phrase (LDAP password or bindpw) must be specified. The search strategy (Search Scope) for AD entries can be changed via base (baseObject), one (singleLevel) and sub (wholeSubtree). The corresponding search path in AD can be specified via the field "Search Base". An example for a path would be *"CN=Users,DC=test,DC=mbg,DC=en"*.

To map the AD information to the local settings, "Filter" and "Mappings" must be created. In AD, the attributes that contain the information needed for a LTOS user can be freely selected. A filter is specified to limit the result set of the LDAP response to the required attributes. The mapping is needed to map attributes of the LDAP directory service that differ from RFC2307 to the correct attributes specified in the RFC that are used by the LDAP service on the LANTIME. For example, the user ID for the passwd mapping is mapped from the freely selected attribute "sAMAccountName" to the attribute "uid" provided for this purpose in RFC2307 by the following mapping: *"passwd uid sAMAccountName"*.

The minimum information to be provided is:

- The User-ID (the login name)
- The User ID number (a number that is not or could not be assigned by a local user)
- The User group number (see below for group membership)
- The user home directory (new folder under /home/)

The only value that cannot be freely assigned in the directory server is the group membership in LTOS. The following values can be stored e.g. in the "gidNumber" attribute:

- The group Super-User has the group ID = 0
- The group Admin-User has the group ID = 4
- The group Info-User has the group ID = 100

The connection to the LDAP server can be specified under the menu item "Global" as soon as a new LDAP server has been added via the button "Add LDAP Server". You can choose between "ldap" and "ldaps" and the URI of the LDAP server must be specified.

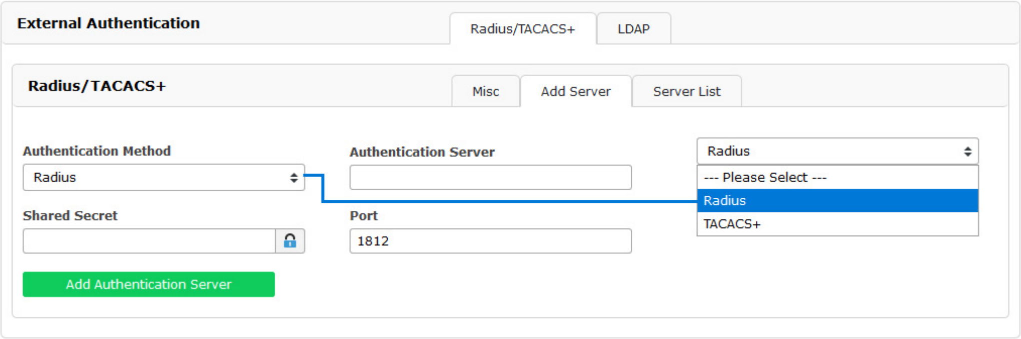
Hint
For a LDAPS connection, the URI must match the URI (in the Common Name or the Subject Alternative Names) of the LDAP server certificate, otherwise the verification fails.

The mode controls whether a configured LDAP server is queried. If the port differs from the defaults (389, 636), another can be selected using the "Alternative Port" field. LDAP servers can be removed via the "Misc" tab. If everything is set, the settings must be transferred to the current configuration by clicking the button "**Save**". After the function test the current configuration can be saved as start configuration.

For the current firmware version 7.02.003, error messages of the ldap service can be viewed via the system messages (CLI or WEB). Authentication errors are written to the */var/log/auth.log* file.

7.3.2.4 Radius and TACACS Connection

In addition to the users managed by LANTIME itself, a Radius or TACACS connection can be used to authenticate users. This configuration is also located in the User Administration under Add External Authentication Server. Look at Figure 7.15 for the input options. You have to enable External Authentication first. Afterwards, choose radius or TACACS+ from the drop down menu and insert the hostname, the previously exchanged key and the correct port. From now on, you are able to login with the external authentication mechanism. At first the system checks the external server for the user. If no user exists with that credentials, the system checks the local users. It is described in "LTOS Management and Monitoring → Via Web GUI → External Authentication Options" how to configure the external authentication server.


External Authentication

Radius/TACACS+

Authentication Method: Radius

Authentication Server:

Shared Secret:

Port: 1812

Figure 7.15: Webinterface Menu "System → User Management → External Authentification"

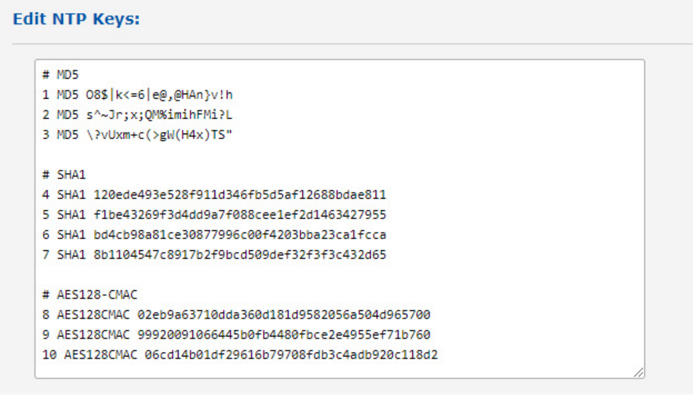
7.4 Securing Time Service NTP

The time service NTP provides an authenticated and integrity secured packet transmission. Currently, NTP autokey is considered to be not as secure as the symmetric key procedure. Therefore, this guide will use the symmetric key configuration. The chapter "LTOS Management and Monitoring → Via Web GUI → NTP Symmetric Keys" describes all configuration options in detail.

To configure a connection, the system needs a key. Either use newly generated or add existing keys in the key file over the button Edit NTP Keys under "NTP → NTP Symmetric Keys". If you automatically generate the keys by the system, MD5 and SHA1 keys will exist in the key file. However, for the highest security currently available, AES128-CMAC keys have to be used. These cannot be generated automatically yet.

How to create AES128-CMAC keys will be explained in chapter "Configuration → Web Interface → NTP → NTP Symmetric Keys".

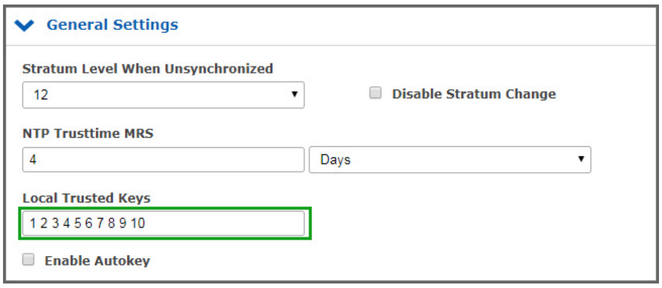
Figure 7.16 shows example keys. The key IDs have to be added to the trusted keys on "General Settings" menu point of NTP tab (see Figure 7.17). On "NTP Restrictions" menu you can deactivate mode 6 and 7 packet support. Optionally, activate access restriction here to grant access only to known IP addresses. The symmetric keys are used for every connection type, i.e. server to client, external NTP server, broadcasting, multicasting and manycasting.



Edit NTP Keys:

```
# MD5
1 MD5 O8$|k<=6|e@,@HAn}v!h
2 MD5 s^~Jr;x;QM%imihFMi?L
3 MD5 \?vUxm+c(>gW(H4x)TS"

# SHA1
4 SHA1 120ede493e528f911d346fb5d5af12688bdae811
5 SHA1 f1be43269f3d4dd9a7f088cee1ef2d1463427955
6 SHA1 bd4cb98a81ce30877996c00f4203bba23ca1fcca
7 SHA1 8b1104547c8917b2f9bcd509def32f3f3c432d65

# AES128-CMAC
8 AES128CMAC 02eb9a63710dda360d181d9582056a504d965700
9 AES128CMAC 99920091066445b0fb4480fbce2e4955ef71b760
10 AES128CMAC 06cd14b01df29616b79708fdb3c4adb920c118d2
```

Figure 7.16: Symmetric NTP Keys



General Settings

Stratum Level When Unsynchronized: 12

□ Disable Stratum Change

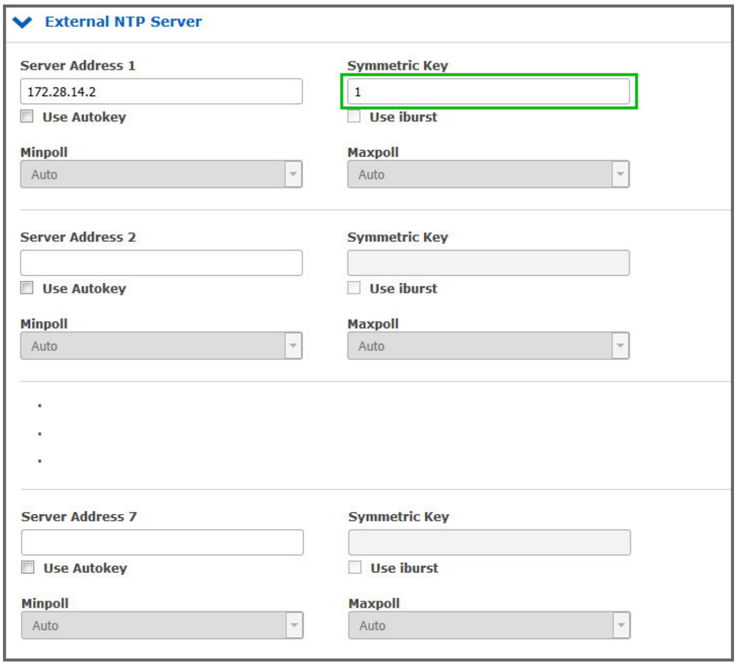
NTP Trusttime MRS: 4 Days

Local Trusted Keys: 1 2 3 4 5 6 7 8 9 10

□ Enable Autokey

Figure 7.17: Trusted key IDs

The insertion points for the right key IDs are marked on Figure 7.18, 7.19 and 7.20. The configuration file of a client is shown in Figure 7.21. It contains the path to the key file, the trusted key IDs and the server IP which uses the key with ID 1 in this example.



External NTP Server

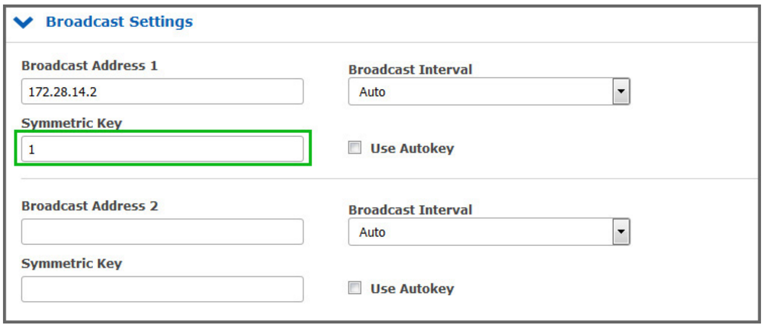
Server Address 1: 172.28.14.2
Symmetric Key: 1
□ Use Autokey
□ Use iburst
Minpoll: Auto
Maxpoll: Auto

Server Address 2:
Symmetric Key:
□ Use Autokey
□ Use iburst
Minpoll: Auto
Maxpoll: Auto

.
.
.

Server Address 7:
Symmetric Key:
□ Use Autokey
□ Use iburst
Minpoll: Auto
Maxpoll: Auto

Figure 7.18: External server configuration

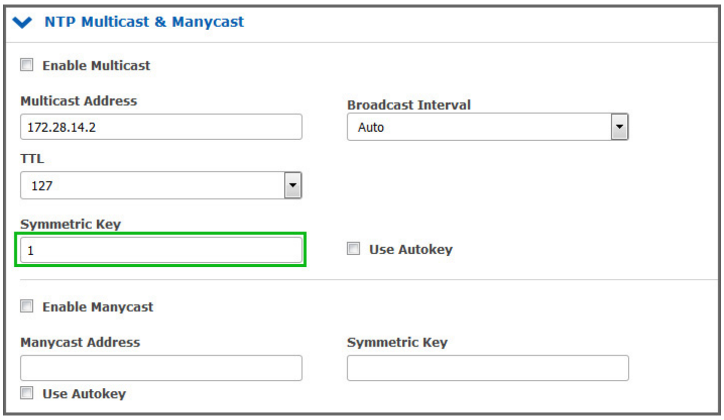


Broadcast Settings

Broadcast Address 1: 172.28.14.2
Broadcast Interval: Auto
Symmetric Key: 1
□ Use Autokey

Broadcast Address 2:
Broadcast Interval: Auto
Symmetric Key:
□ Use Autokey

Figure 7.19: Broadcast configuration



NTP Multicast & Manycast

□ Enable Multicast

Multicast Address: 172.28.14.2

Broadcast Interval: Auto

TTL: 127

Symmetric Key: 1

□ Use Autokey

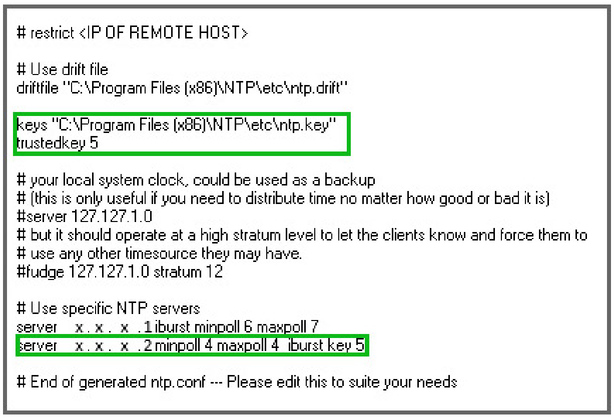
□ Enable Manycast

Manycast Address:

Symmetric Key:

□ Use Autokey

Figure 7.20: Multi and many cast configuration



```
# restrict <IP OF REMOTE HOST>

# Use drift file
driftfile "C:\Program Files (x86)\NTP\etc\ntp.drift"

keys "C:\Program Files (x86)\NTP\etc\ntp.key"
trustedkey 5

# your local system clock, could be used as a backup
# (this is only useful if you need to distribute time no matter how good or bad it is)
#server 127.127.1.0
# but it should operate at a high stratum level to let the clients know and force them to
# use any other timesource they may have.
#fudge 127.127.1.0 stratum 12

# Use specific NTP servers
server    x . x .  x  . 1 iburst minpoll 6 maxpoll 7
server    x . x .  x  . 2 minpoll 4 maxpoll 4  iburst key 5

# End of generated ntp.conf --- Please edit this to suite your needs
```

Figure 7.21: NTP client configuration

7.5 Event Log Delivery

The LANTIME offers many transport channels for event log information and a fine grained notification selection for each of these channels. Currently no event transport channel can be secured with the exception of SNMPv3. It is a good practice to collect event log informations on a central server to correlate and check them for anomalies. Be aware of potential security related information leakage due to the lack of encryption for services other than SNMPv3.

The chapter "LTOS Management and Monitoring → Via Web GUI → Notification" describes the configuration options for the transport channels. If you use SNMP v3 with selected **authPriv** security level, SNMP traps are also sent securely. Configure the SNMP authPriv setting as described in "Security → SNMP" in chapter 7.2.

7.6 Update and Backup LANTIME Firmware

Download the latest LTOS on https://www.meinbergglobal.com/english/sw/firmware.htm. The downloaded LTOS file has to be uploaded via the LANTIME web interface under "System → Firmware/Software Update" like on Figure 7.22. The LTOS V7 firmware is equipped with a digital signature, which is checked during the "Preflight Checks" test directly after upload. If this test detects a faulty signature, a warning is displayed. If this happens, download the new firmware from the Meinberg web site again and repeat the process. In case of repeated warnings please contact the Meinberg support.

In the next step, you have to confirm the update and activate the new firmware like in Figure 7.23. The update was successful if Figure 7.24 is displayed.

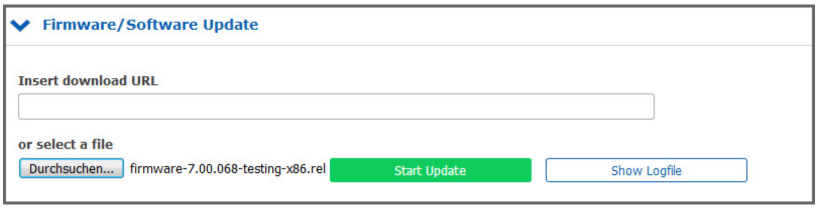
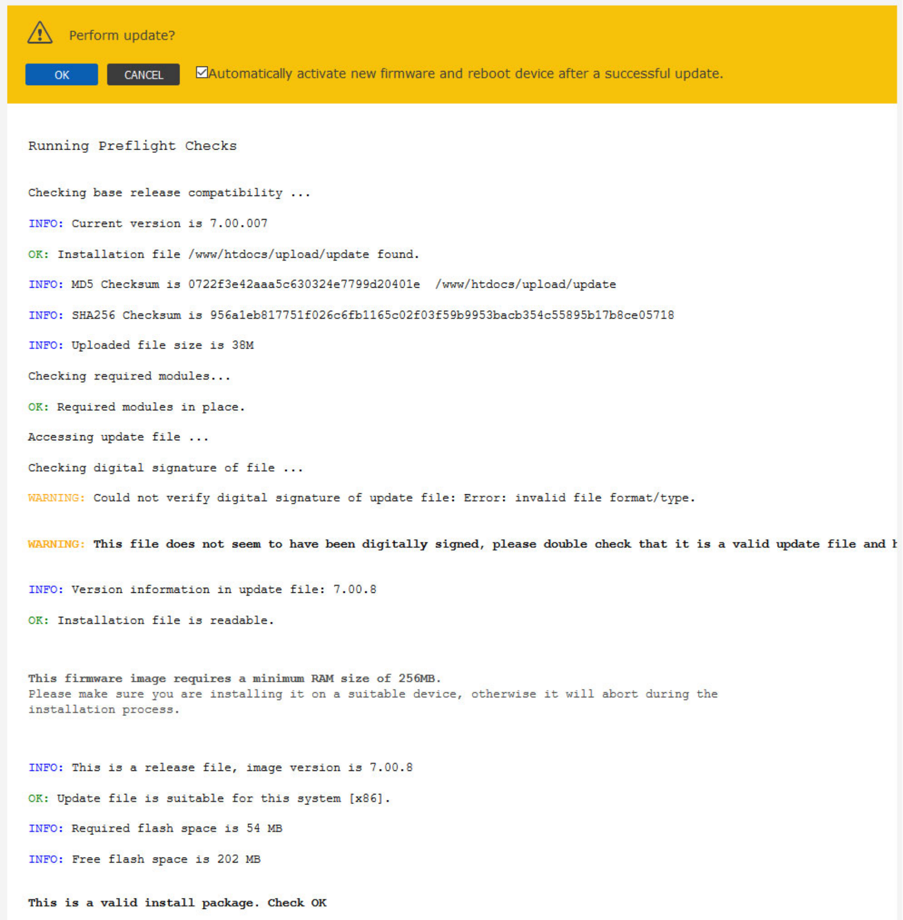


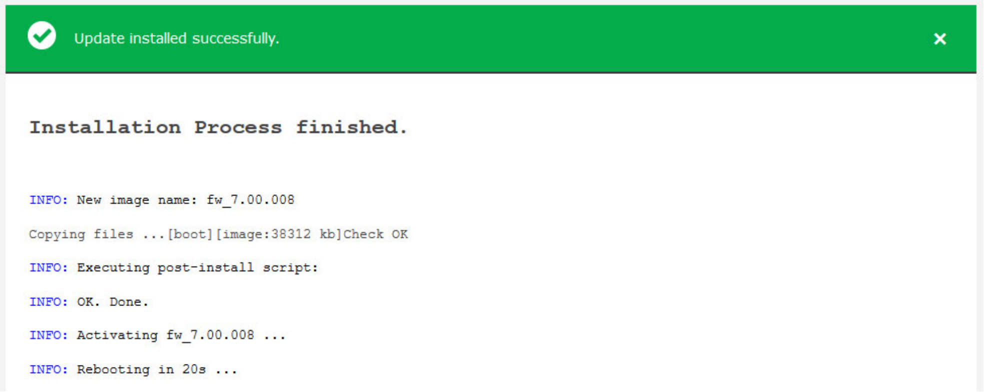
Figure 7.22: Upload firmware



☑Automatically activate new firmware and reboot device after a successful update.

```
Running Preflight Checks

Checking base release compatibility ...

INFO: Current version is 7.00.007

OK: Installation file /www/htdocs/upload/update found.

INFO: MD5 Checksum is 0722f3e42aaa5c630324e7799d20401e  /www/htdocs/upload/update

INFO: SHA256 Checksum is 956a1eb817751f026c6fb1165c02f03f59b9953bacb354c55895b17b8ce05718

INFO: Uploaded file size is 38M

Checking required modules...

OK: Required modules in place.

Accessing update file ...

Checking digital signature of file ...

WARNING: Could not verify digital signature of update file: Error: invalid file format/type.

WARNING: This file does not seem to have been digitally signed, please double check that it is a valid update file and b

INFO: Version information in update file: 7.00.8

OK: Installation file is readable.


This firmware image requires a minimum RAM size of 256MB.
Please make sure you are installing it on a suitable device, otherwise it will abort during the
installation process.


INFO: This is a release file, image version is 7.00.8

OK: Update file is suitable for this system [x86].

INFO: Required flash space is 54 MB

INFO: Free flash space is 202 MB

This is a valid install package. Check OK
```

Figure 7.23: Update process of the firmware



Update installed successfully.

Installation Process finished.

```
INFO: New image name: fw_7.00.008
Copying files ...[boot][image:38312 kb]Check OK
INFO: Executing post-install script:
INFO: OK. Done.
INFO: Activating fw_7.00.008 ...
INFO: Rebooting in 20s ...
```

Figure 7.24: Successful firmware update

The configuration settings of the LANTIME will be preserved during a firmware update, except the configuration files of the web server and the SSH service. These files will be overwritten during an update to be able to deliver current cryptographic methods with an update. If, contrary to our recommendation, the automatic update is not desired, a separate customer-specific configuration file can be stored for these services.

SSH configuration:
The configuration file /etc/ssh/ssh.cfg defines which configuration file the SSH service should use. In factory configuration the file contains the following entry:

```
[SSHD]
CONFIGFILE=/etc/standard/sshd_config
```

If the file */etc/standard/sshd_config* is defined as an SSH configuration file, this file is updated during a firmware update. If the file */etc/ssh/sshd_config* is entered, an own configuration can be created in this file, which is not replaced during an update.

Web server configuration:
The configuration file */etc/webUI/webUI_custom.cfg* defines which configuration file the web server should use. In the factory configuration the file contains the following entry:

```
[CUSTOM CONFIGURATION]
CUSTOM_CONFIG_PATH=
```

If no file is defined as web server configuration file, the factory configuration file, which is updated during a firmware update, is used. If an arbitrary file is entered under */mnt/flash/data/*, an own configuration can be created in this file, which is not replaced during an update. Files that are stored under */mnt/flash/data/* are not part of a configuration, but they are stored reboot-secure (persistent).

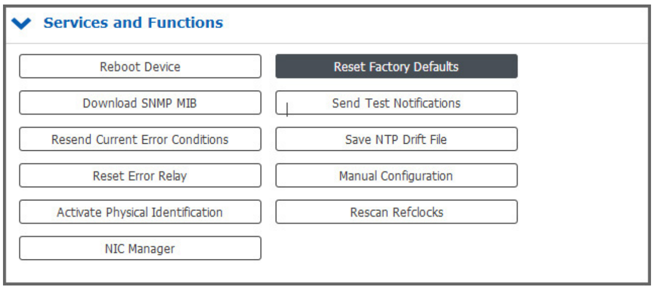


Figure 7.25: Reset factory defaults

To restore automatic configuration updates to the SSH service and the Web server, you can restore the factory paths in these two files.

Restoring the factory defaults via the web interface, as shown in 7.25, resets all custom configuration settings in the current startup configuration except the network settings. In detail, this means that your certificates, credentials, SNMP, NTP and SSH keys, among others, will be lost. Configurations previously saved under a different name are retained even in the event of a factory reset. If desired, these configurations must also be deleted via the web interface.

After the reset via the web interface, all certificates are exchanged to the factory defaults. The SSH key is randomly regenerated at startup after reset.

A backup of the LANTIME firmware, if downloaded or saved on flash of the LANTIME, is in clear text form. For this reason make sure, that no unauthorized person has access to it. The same takes effect for a diagnostic file.

8 LANTIME Basic Configuration Wizard

After the boot-phase of the device, you have to establish a serial connection with the LAN-CPU. Via the terminal connection it is possible to configure parameters with a command line interface. Use a NULL-Modem cable or a CAB-CONSOLE-RJ45 cable to connect your PC or Laptop. You can use for example the standard Hyperterminal program, shipped with your Windows operating system. Configure your terminal program with 38400 Baud, 8 Databits, no parity and 1 Stopbit. The terminal emulation has to be set to VT100. After connecting the LANTIME the login message appears (press RETURN for initial connection):

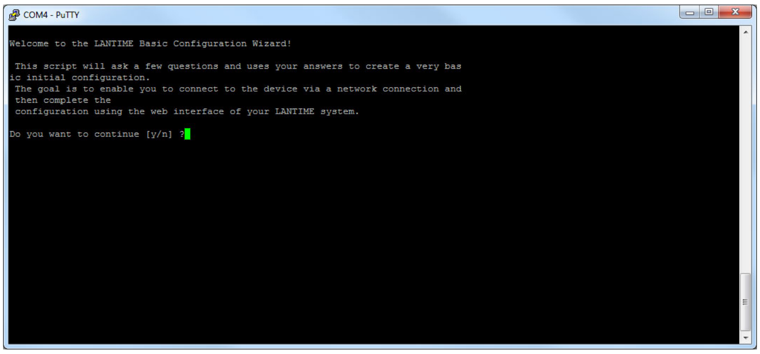
After the connection is successfully established use your login credentials in the welcome screen to enter a console.

```
Welcome to Meinberg LANTIME
login: _
```

Default settings are:
Login: **root**
Password: **timeserver**
(It may be the case to press a RETURN button again).

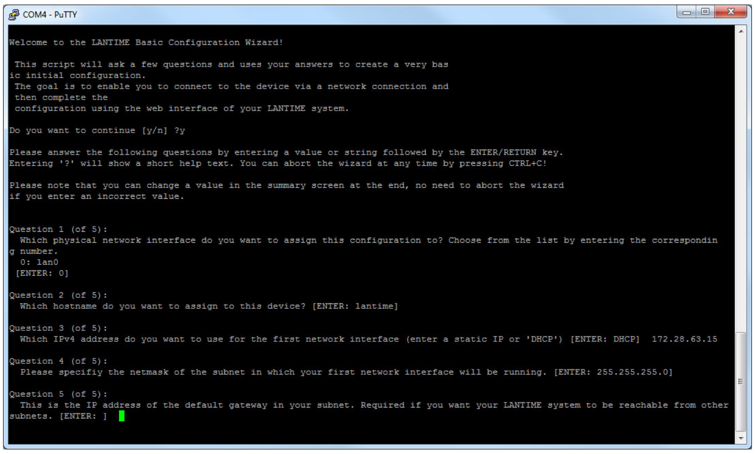
After successful registration change the current path to */wizard/*. Start now the LANTIME Basic Configuration Wizard with “startwizard”.

The following Wizard Welcome screen is now displayed:



```
Welcome to the LANTIME Basic Configuration Wizard!

 This script will ask a few questions and uses your answers to create a very bas
ic initial configuration.
 The goal is to enable you to connect to the device via a network connection and
 then complete the
 configuration using the web interface of your LANTIME system.

Do you want to continue [y/n] ?
```

Confirm with "y" to start the configuration for all the following settings.



```
Welcome to the LANTIME Basic Configuration Wizard!

 This script will ask a few questions and uses your answers to create a very bas
ic initial configuration.
 The goal is to enable you to connect to the device via a network connection and
 then complete the
 configuration using the web interface of your LANTIME system.

Do you want to continue [y/n] ?y

Please answer the following questions by entering a value or string followed by the ENTER/RETURN key.
Entering '?' will show a short help text. You can abort the wizard at any time by pressing CTRL+C!

Please note that you can change a value in the summary screen at the end, no need to abort the wizard
if you enter an incorrect value.


Question 1 (of 5):
  Which physical network interface do you want to assign this configuration to? Choose from the list by entering the correspondin
g number.
  0: lan0
 [ENTER: 0]

Question 2 (of 5):
  Which hostname do you want to assign to this device? [ENTER: lantime]

Question 3 (of 5):
  Which IPv4 address do you want to use for the first network interface (enter a static IP or 'DHCP') [ENTER: DHCP]  172.28.63.15

Question 4 (of 5):
  Please specifiy the netmask of the subnet in which your first network interface will be running. [ENTER: 255.255.255.0]

Question 5 (of 5):
  This is the IP address of the default gateway in your subnet. Required if you want your LANTIME system to be reachable from other
subnets. [ENTER: ]
```

At the end please confirm your configuration.

9 Introduction: Configuration LANTIME

There are several ways to configure the LANTIME parameters:

TELNET
SSH
HTTP Interface
Secure HTTP Interface (HTTPS)
Terminal in front panel (38400/8N1/VT100)
SNMP Management

In order to be able to configure the time server via the web interface or a telnet/SSH connection, an IP address has to be assigned via the front panel keys and LC/VF display (for automatic assignment possibilities please refer to: DHCP IPv4 or AUTOCONF IPv6). Once the IPv4 address, net mask and IPv4 GATEWAY have been set up or the network interface has been automatically configured with DHCP/Autoconf, further configuration changes can be done via a network connection:

Note: If the system doesn't has a display feature (e.g. LANTIME M100), goto chapter LANTIME Setup Wizard in this manual.

To set up a TELNET connection the following commands are entered:
telnet 198.168.10.10 // LANTIME IP
Default User: root
Default Password: timeserver

To set up a SSH connection the following commands are entered:
ssh root@198.168.10.10 // LANTIME IP
Default Password: timeserver

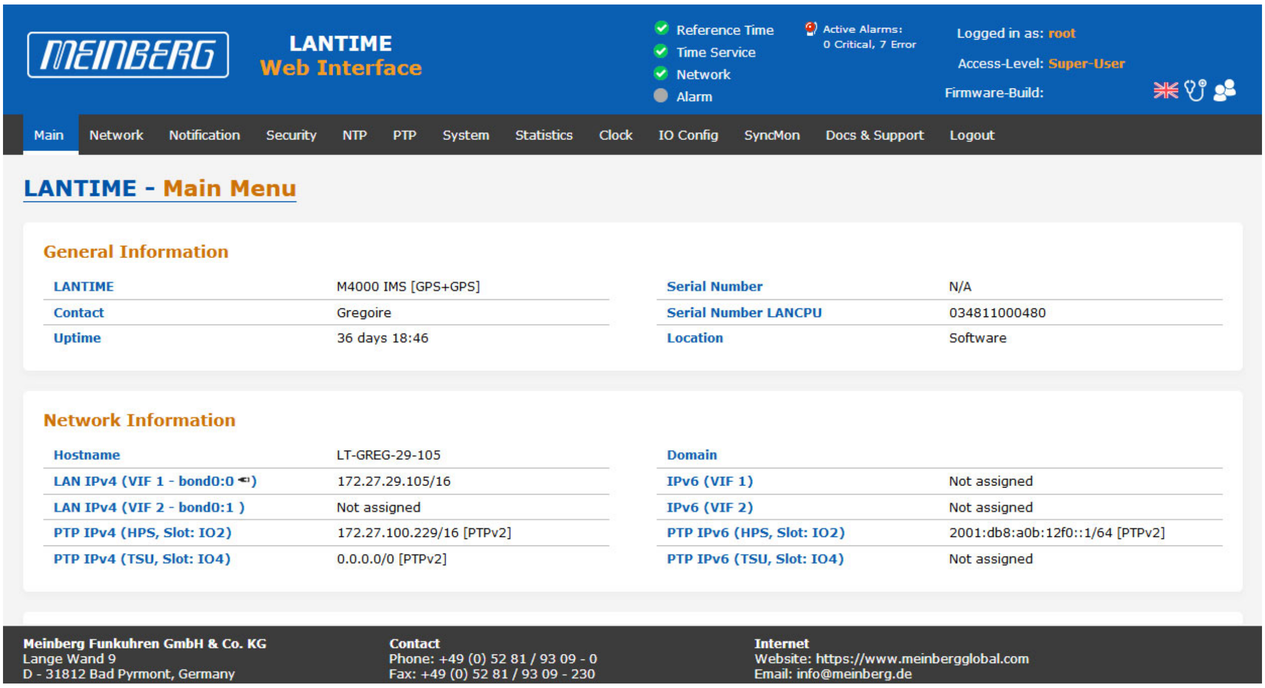
To set up a HTTP connection the following address is to enter in a web browser:
http://198.168.10.10 // LANTIME IP
Default User: root
Default Password: timeserver

To set up a Secure HTTP (HTTPS) connection the following address is entered in a web browser:
https://198.168.10.10 // LANTIME IP
Default User: root
Default Password: timeserver

10 LTOS7 Management and Monitoring

10.1 Via Web GUI

10.1.1 Main Menu



LANTIME - Main Menu

General Information

LANTIME	M4000 IMS [GPS+GPS]	Serial Number	N/A
Contact	Gregoire	Serial Number LANCPU	034811000480
Uptime	36 days 18:46	Location	Software

Network Information

Hostname	LT-GREG-29-105	Domain	
LAN IPv4 (VIF 1 - bond0:0 ◂)	172.27.29.105/16	IPv6 (VIF 1)	Not assigned
LAN IPv4 (VIF 2 - bond0:1)	Not assigned	IPv6 (VIF 2)	Not assigned
PTP IPv4 (HPS, Slot: IO2)	172.27.100.229/16 [PTPv2]	PTP IPv6 (HPS, Slot: IO2)	2001:db8:a0b:12f0::1/64 [PTPv2]
PTP IPv4 (TSU, Slot: IO4)	0.0.0.0/0 [PTPv2]	PTP IPv6 (TSU, Slot: IO4)	Not assigned

Meinberg Funkuhren GmbH & Co. KG
Lange Wand 9
D - 31812 Bad Pyrmont, Germany

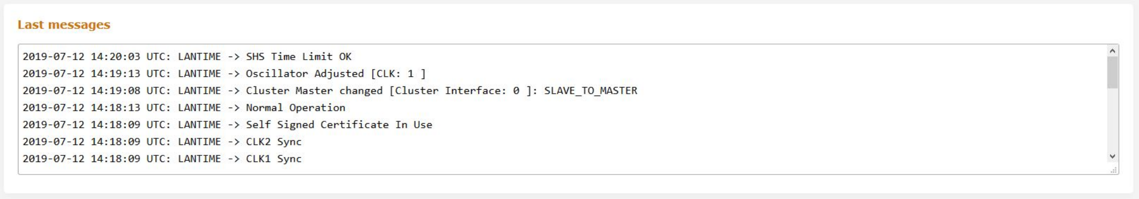
Contact
Phone: +49 (0) 52 81 / 93 09 - 0
Fax: +49 (0) 52 81 / 93 09 - 230

Internet
Website: https://www.meinbergglobal.com
Email: info@meinberg.de

This chapter provides you with configuration options and status information of your LANTIME system accesssed via Web GUI. The main page contatins an overview of the most important configuration and status parameters for the system.

- Information about LANTIME model and software
- Network information
- Receiver status
- NTP status
- PTP status (option)
- Last messages
- Statistics (NTP/MRS Performance, NTP Access ...)
- Extended Statistics (MRS - external reference input signals)
- Documentation (Manuals), support information

The field in the lower section shows the last messages of the system with a timestamp added. The newest messages are on top of the list. This is the content of the file /var/log/lantime_messages, which is created after every start of the system (and is lost after a power off or reboot).



Last messages

```
2019-07-12 14:20:03 UTC: LANTIME -> SHS Time Limit OK
2019-07-12 14:19:13 UTC: LANTIME -> Oscillator Adjusted [CLK: 1 ]
2019-07-12 14:19:08 UTC: LANTIME -> Cluster Master changed [Cluster Interface: 0 ]: SLAVE_TO_MASTER
2019-07-12 14:18:13 UTC: LANTIME -> Normal Operation
2019-07-12 14:18:09 UTC: LANTIME -> Self Signed Certificate In Use
2019-07-12 14:18:09 UTC: LANTIME -> CLK2 Sync
2019-07-12 14:18:09 UTC: LANTIME -> CLK1 Sync
```

By using the navigation on top of the page you can reach a number of configuration menus, which are described in the following chapters.

10.1.1.1 Introduction

To start a http or a secured https session with the Web Interface running on the CPU of your LANTIME system, you need to open your internet browser and type in the IP address of the interface you are using for this connection. Per default configuration https protocol is enabled at each network interface. Http requests are automatically redirected to https.

If you wish to use only one dedicated network interface for management and monitoring and the rest for other services you can find the corresponding configuration options in the Chapter "LTOS Configuration → Via Web → Network" in the submenu Network Services.

If the connection with the LANTIME is established correctly you will be prompted to enter login data to start the web session. Per default the entering user-name/password are: root/timeserver. For security reasons you are advised to change the default credentials after the first login. The corresponding user administration settings can be found in the Chapter "LTOS6 Configuration → Via Web → System" in the submenu User Management.

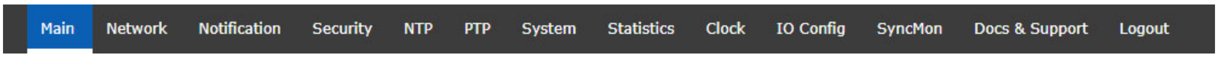
After entering the correct password, the main menu page of the web interface of a LANTIME system shows up.

The main page contains an overview of the most important configuration and status parameters of the system, including:

- general information (model name, serial number, uptime since last reboot)
- assigned network and PTP interfaces (both in IPv4 or IPv6 configuration)
- receiver status information (sync or not, for GNSS receivers some additional satellite data)
- SHS (Secure Hybrid System) status in redundant receiver configuration, which provides a plausibility mode where the incoming times of both time signals are continuously compared against each other. For more information about the SHS mode and the corresponding settings you can find in Chapter "LTOS6 Configuration → Web GUI → Security → SHS Configuration".

10.1.1.2 How to navigate through the Web Interface

By using the navigation on top of the page you can reach a number of configuration menus, which are described in the following chapters.



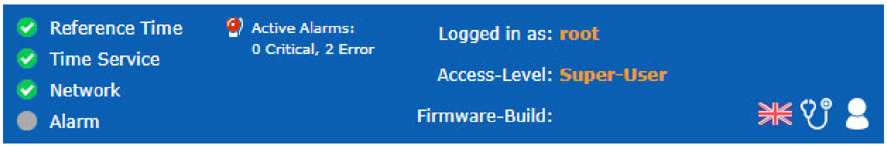
Scrolling down the main page you will find a section containing last log messages generated during the LANTIME operation. The messages in this field are limited to the last 50 and are chronologically ordered. The messages are stored in the file /var/log/lantime_messages, which is created after every start of the system (and is lost after a power off or reboot).To view all log messages in the log file you would have to use the CLI (Command Line Interface). For your reference, a list of available CLI commands for LANTIME management and monitoring is provided in the Command Line Reference.

10.1.1.3 Web Interface - Notifications and Alarms

At the top of the main page in the right corner you can find an image of the status LED lamps which are physically located at the front site of a LANTIME system, in models with an integrated front panel unit. When the system is in operation and everything runs as expected, the upper three status LEDs are turned to green and the Alarm indicator is switched off. If you experience after the powering up the system and after the startup has been completed that one or more LEDs are switched on red, please proceed to the Chapter on Troubleshooting and Alarming.

Please note: startup of the system can take a several minutes, depending on the hardware configuration of your system.

Next to the status LEDs you will see displayed all active alarms currently present on a LANTIME with critical and error severity levels. With a mouse click over the alarms you will reach a table of notification events with red marked indicators at the events which triggered the alarms.



✓ Reference Time
✓ Time Service
✓ Network
● Alarm

Active Alarms:
0 Critical, 2 Error

Logged in as: root

Access-Level: Super-User

Firmware-Build:

For further information how to eliminate a cause of each individual alarm, proceed to the Chapter on Troubleshooting and Alarming.

Next to the alarm area in the main page there is a field with informational data about your login status and information to which access-level group you belong as a current user. There are three types of users: Super-User, Admin-User and Info-User. The exact definitions of the three different user types and their access-level rights you can find in Chapter "LTOS6 → Web GUI → System-> User Management".

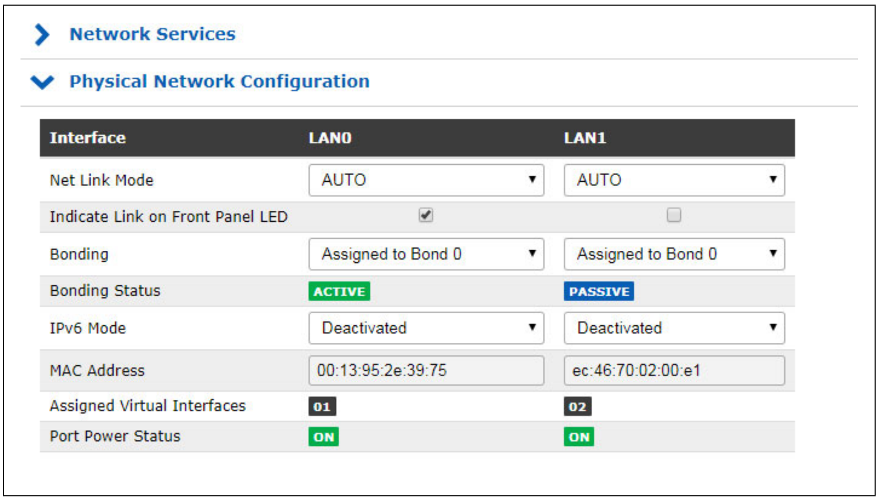
At the top right corner of the main page you can see a few icons. The displayed flag indicates the language pack which is currently activated for the web interface display. For the moment you can choose between English and German languages packs.

Next to the language flag, there is an icon showing a doctor's stethoscope linked with a diagnostic file of the system, which includes all the necessary data for diagnostic and troubleshooting of the device. By clicking this icon a current diagnostic file will immediately start to download for you to save it to your local computer for a further use. The downloading can take up to 60 seconds, depending on the file size, which can be several MB. In the diagnostic file all the data about the system configuration and log messages are stored. The diagnostic file can be also an important tool for the Meinberg support team if you need some help with the configuration or you experience issues which you can not solve on your own. More about the diag file see Chapter "LTOS6 Configuration → via Web GUI → System → Download Diagnostic File".

The web interface is divided into several dialogue menus, where some of the dialogues (e.g. PTP; IO Config and SyncMon) depend on the hardware components which are integrated in the LANTIME system and only appear in systems with a corresponding configuration. The rest of the dialogues are common to all LANTIME and IMS systems.

You can move between the dialogues by clicking each individual name tag at the top of the menu line. When you click on the Logout tag, your Web session with the LANTIME device will be terminated immediately.

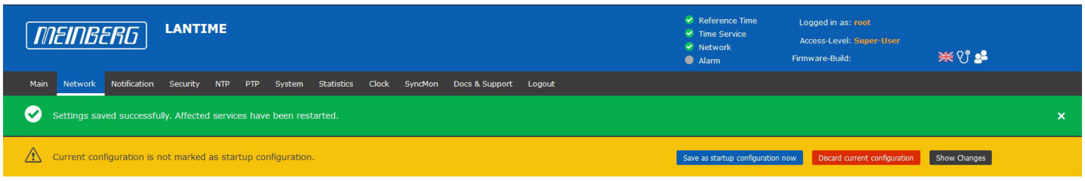
The two dialogues "Main" and "SyncMon" deliver you the status information about the LANTIME system after the last reboot. The rest of the dialogues provide configurations of features for the LANTIME operation and services. The dialogues with feature configurations are presented in a tree structure, where each submenu can be extended into a subtree by clicking at the "+" sign at the beginning of the submenu row. When you open the dialogue, the "+" will turn in "-" and when you click the "-" icon the currently open dialogue will close. You can have a few dialogues open at the same time in the currently selected menu (see the example on the next page).



Interface	LAN0	LAN1
Net Link Mode	AUTO	AUTO
Indicate Link on Front Panel LED	☑	☐
Bonding	Assigned to Bond 0	Assigned to Bond 0
Bonding Status	ACTIVE	PASSIVE
IPv6 Mode	Deactivated	Deactivated
MAC Address	00:13:95:2e:39:75	ec:46:70:02:00:e1
Assigned Virtual Interfaces	01	02
Port Power Status	ON	ON

Figure: A tree structure of each menu. Opening a subtree by clicking a "+" and closing by "-" at the beginning of the submenu name

Generally, in any configuration menu you are located, when you fill in or edit one or more feature fields at the end you need to confirm the setting by clicking the "Save Settings" button at the bottom of the page. By doing so and if the setting has been carried out successfully, you will receive a dialogue in the Main Menu with a confirmation message written on a green field. At the same time when a new configuration has been applied a log message will appear in the list of last messages in the Main Menu saying: "Device Configuration Changed".



Logged in as: root

Access-Level: Super-User

Firmware-Build:

Settings saved successfully. Affected services have been restarted.

Current configuration is not marked as startup configuration.

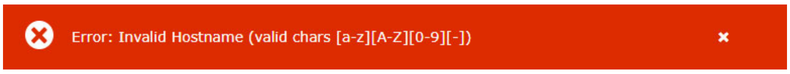
Figure: Settings saved successfully. Affected services have been restarted

A Saving startup configuration dialogue. Options for saving, discarding the current configuration and showing changes between the startup configuration and the current one.

Apart of the configuration message you will receive also an attention notice displayed on a yellow bar, saying: "Current configuration is not yet marked as a startup configuration". This means that you need to confirm the new configuration first by clicking on a "Save as startup configuration now" button if you want to keep it as a startup configuration by the next startup of the system. By clicking this button you will receive another confirmation message saying: "Activate current configuration really as startup configuration?" which you confirm by clicking the "OK" button. The new configuration has now become the startup configuration on your LANTIME system.

On the other hand, if you want to return to the last saved startup configuration then you select "Discard current configuration" button when the message on a yellow bar appears.

Each entry you fill in in the provided dialogues is checked for plausibility for that particular field. If you for example used wrong characters (e.g. letters in the IP Address configuration or any special characters which are not allowed) or you provided an invalid network configuration then you will receive a message displayed on a red bar saying a type of error and at which feature entry it occurred. The false entry will not be accepted by the system, neither the rest of any new settings you may have configured by that time, therefore you will have to redo the configuration steps again. See an example of a warning message if an error by entering a feature occurs.



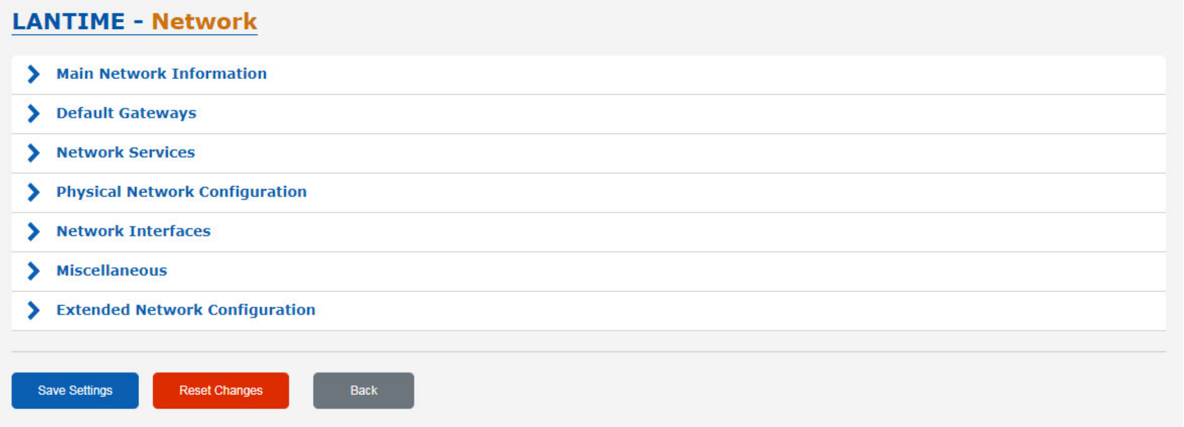
Error: Invalid Hostname (valid chars [a-z][A-Z][0-9][-])

Figure: A display of a warning message with a type of error and indication to which feature it belongs

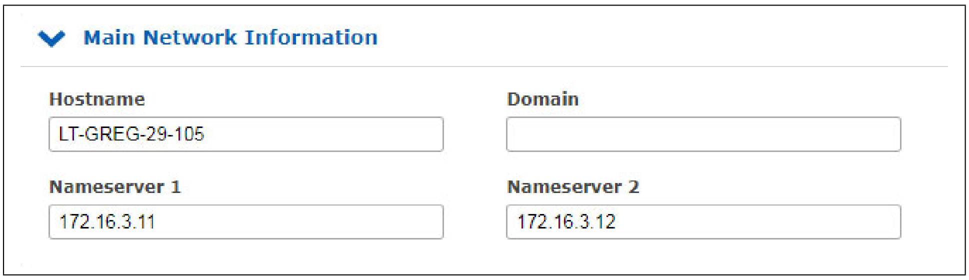
Allowed signs and special characters which you can use to fill in dialogue boxes you can find in the chapter "Before you Start → Text and Syntax Conventions".

For configuration of the system features now proceed to the dedicated menu which is described in a corresponding chapter.

10.1.2 Network



10.1.2.1 Main Network Information



Hostname: LT-GREG-29-105

Domain:

Nameserver 1: 172.16.3.11

Nameserver 2: 172.16.3.12

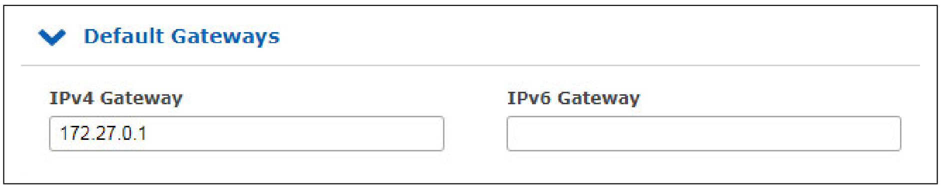
Hostname
The hostname of the LANTIME is a unique name of a computer in a network. Each IP address configured on the LANTIME is assigned to this hostname.

Domain
This field is used to configure the network domain name. A network domain name is a text-based label easier to memorize than the numerical addresses used in the Internet protocol (e.g. meinberg.de).

Nameserver1
IP Address of the primary DNS Server in the network. The DNS server is used to resolve IP addresses as well as hostnames in a network.

Nameserver2
An alternate nameserver can be defined here.

10.1.2.2 Default Gateways



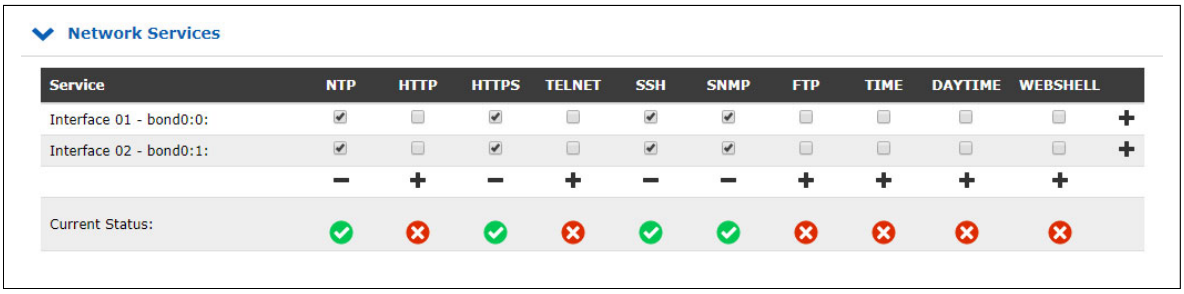
Default Gateways

IPv4 Gateway	IPv6 Gateway
172.27.0.1	

In this menu you can configure default gateways to be used for IPv4 and IPv6. For a default gateway, a "default" entry is created in the main routing table of a LANTIME. If the LANTIME does not have a direct route or a routing rule to a destination IP, it will always attempt to reach the destination via the default gateway.

IPv4 Gateway	Configuration of the default IPv4 gateway.
IPv6 Gateway	Configuration of the default IPv6 gateway.

10.1.2.3 Network Services



Network Services

Service	NTP	HTTP	HTTPS	TELNET	SSH	SNMP	FTP	TIME	DAYTIME	WEBSHELL	
Interface 01 - bond0:0:	☑	□	☑	□	☑	☑	□	□	□	□	+
Interface 02 - bond0:1:	☑	□	☑	□	☑	☑	□	□	□	□	+
	−	+	−	+	−	−	+	+	+	+	
Current Status:	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	

In this submenu you can enable or disable various services for the existing virtual network interfaces. The +/- buttons can be used to select or deselect entire rows or columns in the matrix.

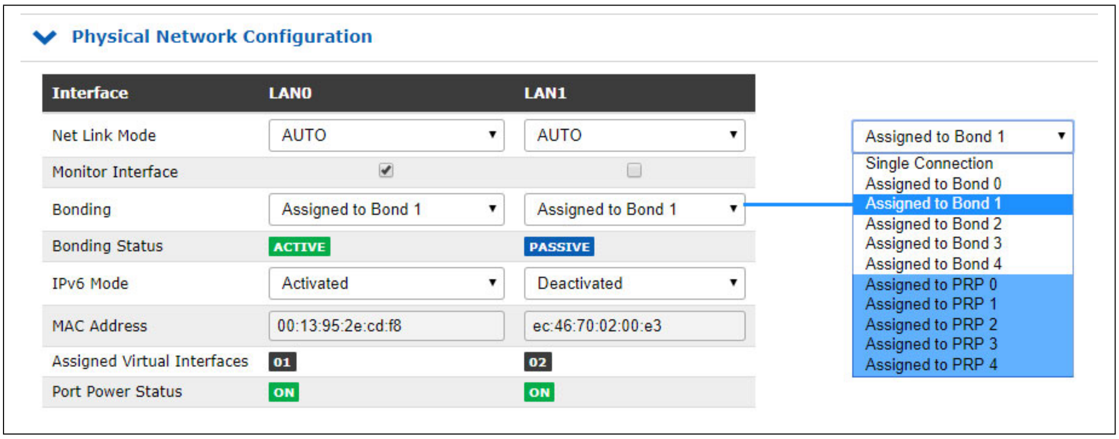
The following service states are possible:

- A service has been activated for at least one virtual interface and is active.
- Service has not been activated for any virtual interface and is therefore stopped.

The following services are supported by the LANTIME:

NTP:	Network Time Protocol, UDP Port 123
HTTP:	Hyper Transfer Protocol, TCP Port 80
HTTPS:	Hyper Transfer Protocol Secure, TCP Port 443
TELNET:	Teletype Network, TCP Port 23
SSH:	Secure Shell, TCP Port 22
SNMP:	Simple Network Management Protocol, UDP Port 161 / 162 (Traps)
FTP:	File Transfer Protocol, TCP Port 20
TIME:	Time Protocol, TCP/UDP Port 37
DAYTIME:	UDP Port 13
FPC:	Emulates the FrontPanel of a LANTIME and maps it in a browser.
WEBSHELL:	Login to a command line interface of a Lantime via a webbrowser. WEBSHELL works on port 4200. Input in the web browser: [IP/HOSTNAME]: 4200

10.1.2.4 Physical Network Configuration



Physical Network Configuration

Interface	LAN0	LAN1
Net Link Mode	AUTO	AUTO
Monitor Interface	☑	□
Bonding	Assigned to Bond 1	Assigned to Bond 1
Bonding Status	ACTIVE	PASSIVE
IPv6 Mode	Activated	Deactivated
MAC Address	00:13:95:2e:cd:f8	ec:46:70:02:00:e3
Assigned Virtual Interfaces	01	02
Port Power Status	ON	ON

Net Link Mode
Allows you to configure the network connection mode of the interface. You can choose among supported link modes of the respective physical interface.

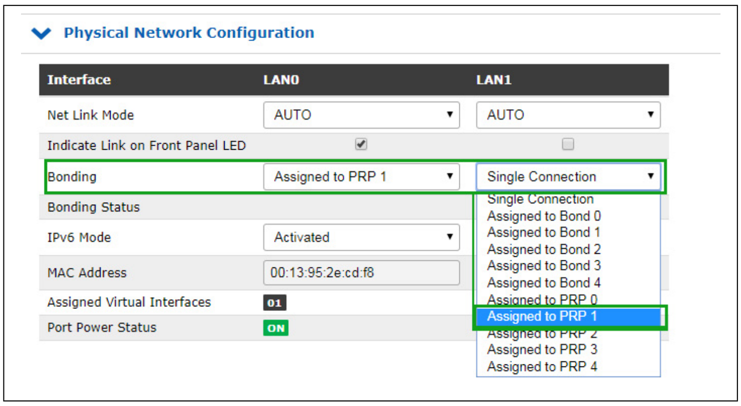
The default value AUTO (Autonegotiation) can remain unchanged under normal circumstances. Autonegotiation refers to a method which allows two interconnected Ethernet devices to independently negotiate the maximum possible transmission speed and the duplex method and to configure them accordingly.

Monitor Interface
As soon as one of the selected network ports has no link, this status will be indicated by a red "Network" LED on the front panel and the "Network Link Down" event will be reported. If a network link is available on all selected ports, the "Network" LED on the front panel will light up green.

Bonding
Here, 2 or more physical network ports can be grouped into a bond (group). The LANTIME supports the bonding modes "Active - Backup" and "LACP". The mode to be used can be selected in the submenu "Network → Miscellaneous → Bonding-Mode". For more information about how the two modes work, see the "Miscellaneous" submenu.

PRP

PRP stands for Parallel Redundancy Protocol and is defined in the standard IEC 62439-3 since 2010. PRP is Layer-2 based and has been developed for computer networks which are in need of a reliable solution regarding high availability and operational functionality. A LANTIME with two or more interfaces, running firmware 6.22.001 or higher, has the ability to act as a DAN ("Dual Attached Node" - a device which is connected to both redundant networks).



Physical Network Configuration

Interface	LAN0	LAN1
Net Link Mode	AUTO	AUTO
Indicate Link on Front Panel LED	☑	□
Bonding	Assigned to PRP 1	Single Connection
Bonding Status		
IPv6 Mode	Activated	
MAC Address	00:13:95:2e:cd:f8	
Assigned Virtual Interfaces	01	
Port Power Status	ON	

As of LANTIME firmware version 7.0, PRP can also be conveniently set via the web interface menu "Network → Physical Network Configuration". Select the same PRP group for at least two interfaces in the drop-down menu "Bonding".

IPv6 Mode

Activation or deactivation of the IPv6 protocol.

MAC Address

Media Access Control, shows the MAC address of the given physical interface.

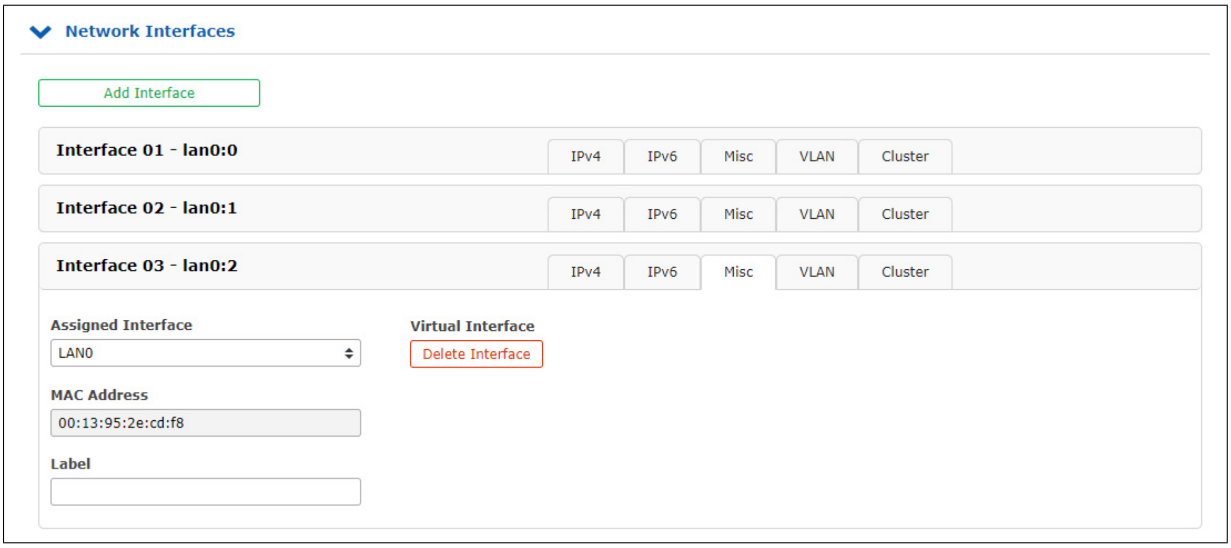
Assigned Virtual Interfaces

Indicates which virtual interfaces are assigned to the given physical interface.

Port Power Status

This feature is available in IMS systems, where several physical interfaces can be available. The port power status is an indicator if a particular physical interface is powered on or off.

10.1.2.5 Network Interfaces



Interface 01 - lan0:0

Interface 02 - lan0:1

Interface 03 - lan0:2

Assigned Interface: LAN0

Virtual Interface

MAC Address: 00:13:95:2e:cd:f8

Label:

In this menu the virtual interfaces of the LANTIME are managed. Up to 99 virtual interfaces can be assigned to the available physical ports. The name of the virtual interface consists of a consecutive number of a physical interface and the number of a virtual interface (starting with zero).

The example above shows a configuration in which a total of three virtual interfaces are assigned to the physical interface **LAN0**, namely **lan0:0**, **lan0:1** and **lan0:2**.

In the case of an active bond, the physical interface is replaced by the name of the bonding group, for example **bond0:0**.

Add interface
With this button a new virtual interface can be created. The new interface is assigned by default to the physical port lan0 and is added at the end of the row of the existing virtual interfaces. The assignment can be changed in the "Miscellaneous" tab.

Submenu IPv4:
In this submenu the IPv4 parameters can be configured or the current configuration given by the DHCP server can be displayed.

TCP/IP address: IPv4-Address of the given interface.

Netmask: Configuration of the subnetmask for the given interface.
Gateway: Configuration of an interface-specific gateway. This setting must be made only if the IP of the interface is NOT in the same subnet as the default gateway and the cross-network traffic in the subnet should be enabled via the gateway.

Enable DHCP-Client: With this setting a DHCP client can be activated for the automatic assignment of the network configuration by a DHCP server.

Submenu IPv6:
In this menu the IPv6 parameters can be configured or the configuration given by a DHCP server can be displayed.

TCP/IP address: Ipv6-Address of the given interface
Enable DHCP-Client: With this setting a DHCPv6 client can be activated for the automatic assignment of the network configuration by a DHCPv6 server.

Submenu Misc:

Assigned Interface: Determines which physical network is associated with the currently selected virtual interface.

"Virtual Interface"
Delete Button: Deletes the currently selected virtual interface.

MAC Address: Displays the MAC address of the assigned physical network port

Label: Individual text-description of the interface (alias).

Submenu VLAN:
Enable VLAN Option: Activation of the tagged VLAN function for the selected virtual interface.

VLAN-Tag (0-4094): VLAN tags from 0-4094 can be entered here. The selected tag is inserted into the data area of an Ethernet packet.

Priority: PCP (Priority Code Point). Sets the priority of an Ethernet frame. Priorities can be set between a low priority, value 1 and a high priority, value 7.

The Priority value 0 corresponds to the Best Effort.

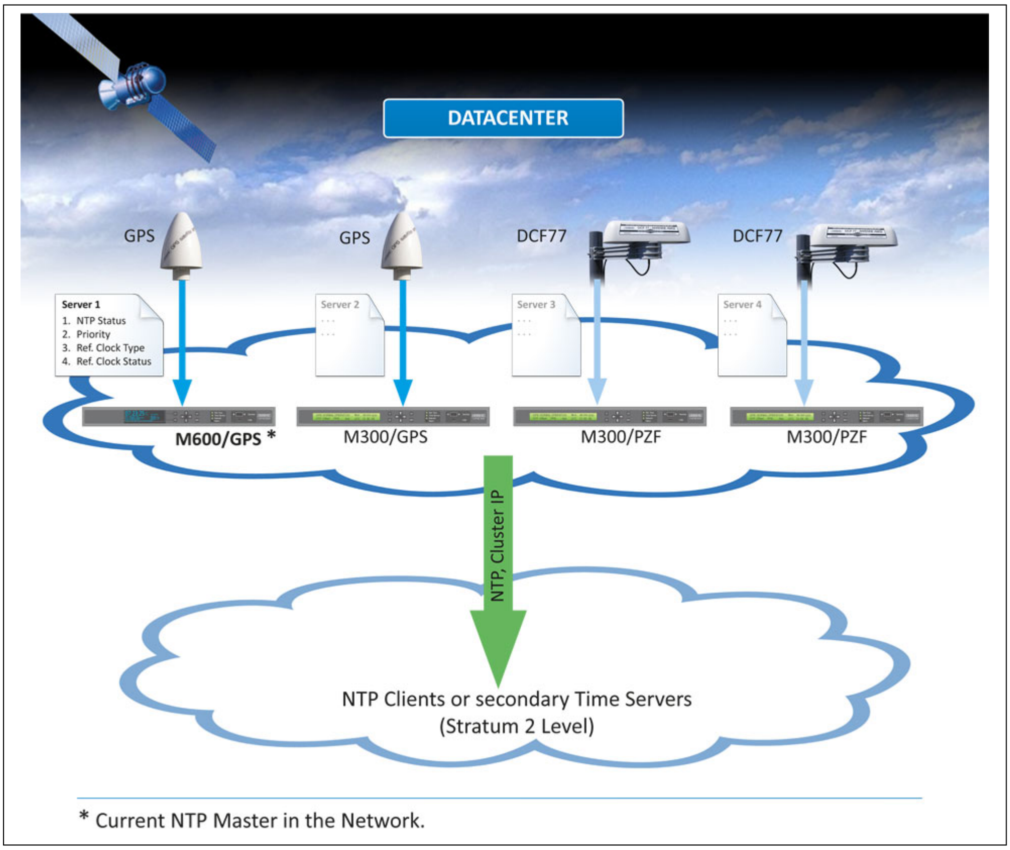
Submenu Cluster:

The Cluster mode is a method for providing redundant time synchronization by groupping (clustering) multiple LANTIME NTP servers. Within this group, the participating NTP servers continuously exchange status and quality information with each other. The status information is compared among each other and by a special algorithm a decision is made, which of the NTP servers should act as a current MASTER in the network. The rest of the group acts as SLAVE and stays passive as a backup. If the current master loses its synchronization source or any other failure occurs, another NTP server from the cluster takes over the master role. The current master responds to requests from NTP clients via a common cluster IP. Even if the master is replaced by another NTP server, this IP does not change.

The configuration of a NTP cluster is useful if at the side of NTP clients only one IP address for an external NTP server can be configured and redundancy is still required.

The current master is selected according to the following parameters in this order:

1. NTP status (sync, not sync);
2. Priority (configurable by the user, the lowest value has the highest priority, default = 0);
3. Ref-Clock Type - GNSS receivers such as GPS have the highest rating;
4. Ref-Clock Status (sync, not sync).



10.1.2.6 Cluster Configuration

Enable Cluster Option: The cluster function can be activated via this selection box.

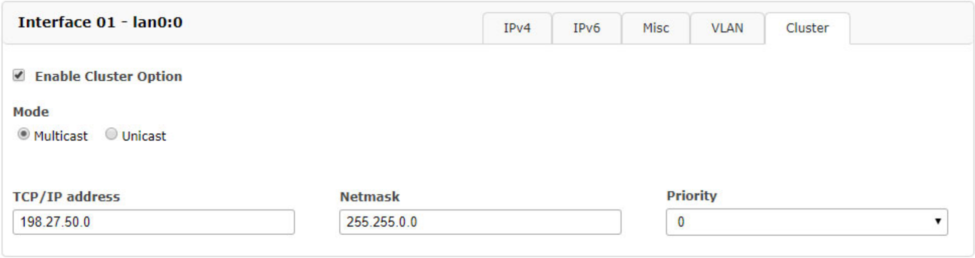
Mode: The cluster members can share their status information either via multicast or unicast messages. For multicast, a cluster multicast address 239.192.0.1 is used by default. This setting can be changed in the menu "Network → Miscellaneous". In addition, the network port which is used for the cluster communication can be changed there. By default, port 7000 is used for the cluster messages.

TCP/IP Address: IP address of the NTP cluster interface. The same cluster IP needs to be configured on all cluster members. It is recommended to configure a cluster IP in the same subnet as the corresponding virtual interface.

Netmask: Netmask Configuration for the cluster interface.

Priority: The priority set here is taken into account when the MASTER is determined by the cluster algorithm. The lowest value has the highest priority.

Example configuration for a multicast cluster:



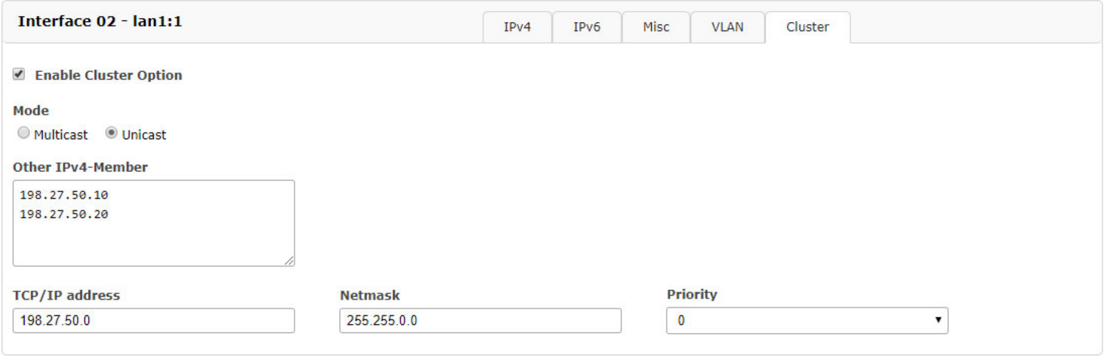
Interface 01 - lan0:0

☑ Enable Cluster Option

Mode
● Multicast ○ Unicast

TCP/IP address: 198.27.50.0
Netmask: 255.255.0.0
Priority: 0

Example configuration for an unicast cluster:



Interface 02 - lan1:1

☑ Enable Cluster Option

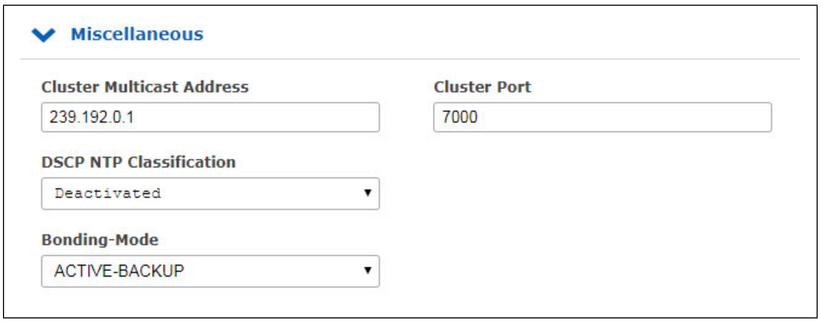
Mode
○ Multicast ● Unicast

Other IPv4-Member
```
198.27.50.10
198.27.50.20
```

TCP/IP address: 198.27.50.0
Netmask: 255.255.0.0
Priority: 0

In the Unicast cluster, the IP addresses of the cluster members must be entered in the "Other IPv4 Member" field.

10.1.2.7 Miscellaneous



Miscellaneous

Cluster Multicast Address: 239.192.0.1

Cluster Port: 7000

DSCP NTP Classification: Deactivated

Bonding-Mode: ACTIVE-BACKUP

Cluster Multicast Address:
Configuration of the cluster multicast address. Via this address, LANTIME cluster members exchange their status messages if Multicast mode is selected.

Cluster Port:
Configuration of a free network port for the cluster communication. Per default this port is set to 7000.

DSCP NTP Classification:
DSCP = Differential Service Code Point. DSCP is generally a method for prioritizing the traffic via IP. On the LANTIME, this setting allows the NTP packets to be assigned to a certain traffic class. The information about the traffic class is inserted into a header of a IPv4 packet. Routers can evaluate this information and handle the NTP packets as prioritized.

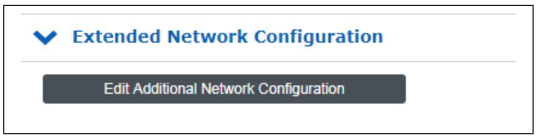
Bonding-Mode:
In the menu “Network → Physical Network Configuration", two or more physical network ports can be grouped into a bond (group). The Bonding Mode is used to configure either the “ACTIVE BACKUP” or the "LACP" mode (Link Aggregation Control Protocol), which are supported on the LANTIME.

ACTIVE-BACKUP:
One physical interface in the bonding group acts as an "active slave". All network traffic of a LANTIME Bond runs through this interface. The other physical interfaces in the bonding group are passive. In case the current active interface loses the network connection, the passive interface seamlessly takes over. Even the MAC address of the network port remains unchanged.

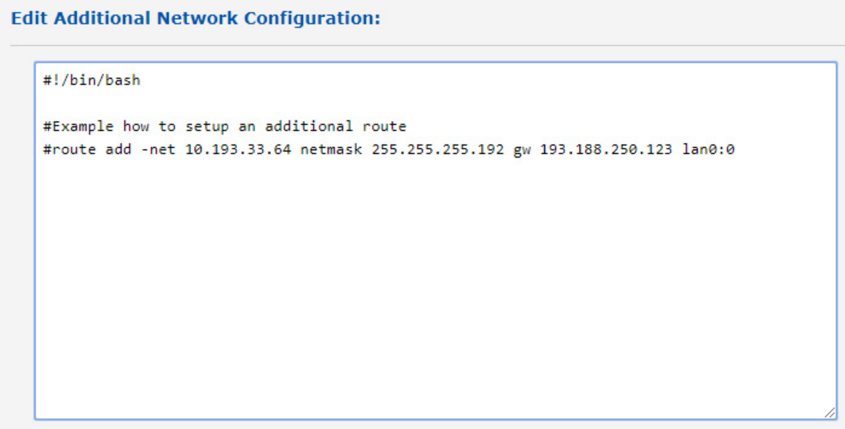
LACP: LACP (802.3ad) allows a combination of multiple physical connections to a logical one. This results in a load sharing and, in addition, increases the safety in case of a failure compared to "Active Backup". It is important that other connected network devices also support LACP and the network ports are configured accordingly.

10.1.2.8 Extended Network Configuration

The Extended Network Configuration are not enabled for security reasons. This function can be subsequently enabled / controlled via an SSH connection in */etc/mbg/msc.cfg* with the "DISABLE SCRIPT" parameter.

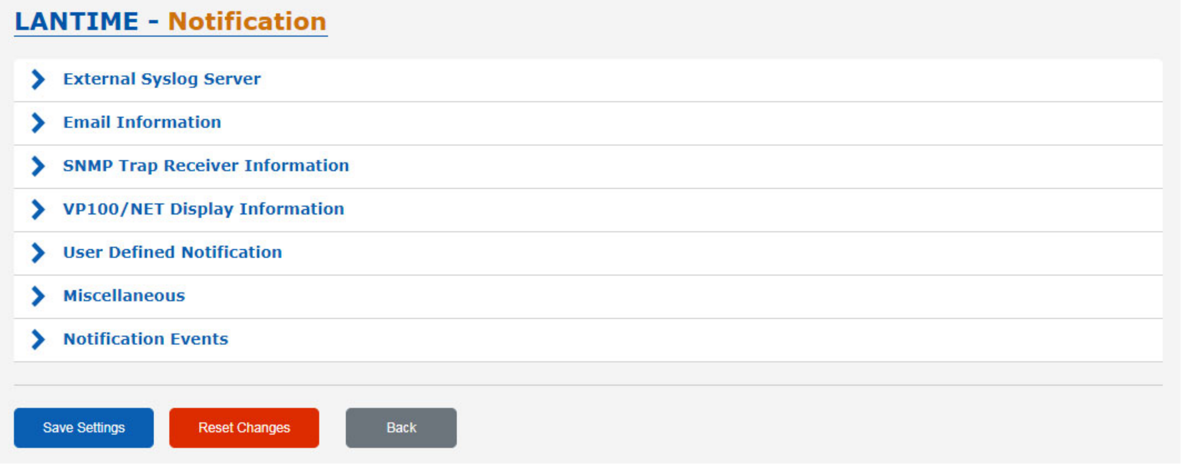

Extended Network Configuration
Edit Additional Network Configuration

In the Extended Network Configuration, a bash script can be edited, which is executed automatically each time the LANTIME is rebooted or a network-related configuration changes.


Edit Additional Network Configuration:

```
#!/bin/bash

#Example how to setup an additional route
#route add -net 10.193.33.64 netmask 255.255.255.192 gw 193.188.250.123 lan0:0
```

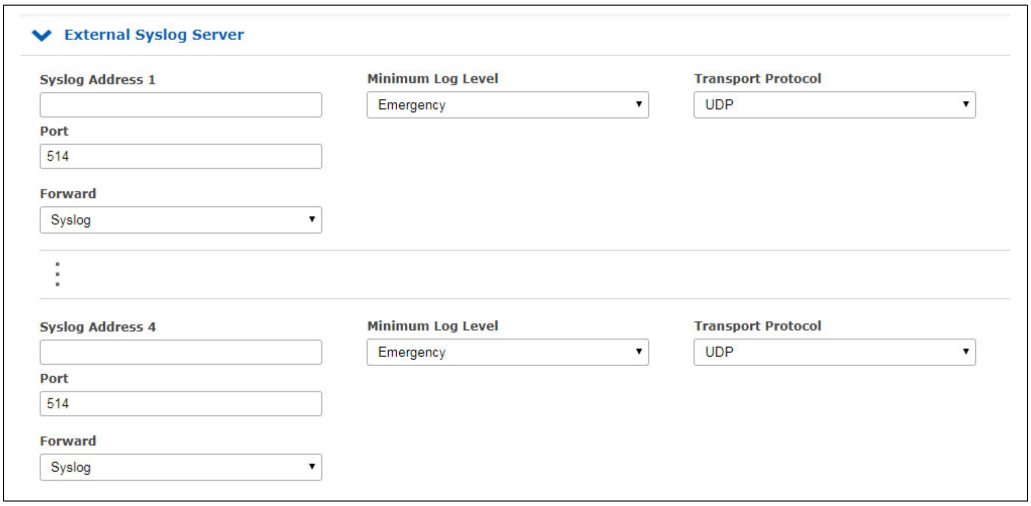
10.1.3 Notification



LANTIME - Notification

10.1.3.1 External Syslog Server

All information which is written into SYSLOG (/var/log/messages) on the LANTIME, can also be forwarded to a remote server.



External Syslog Server

Syslog Address 1:

Minimum Log Level: Emergency

Transport Protocol: UDP

Port: 514

Forward: Syslog

⋮

Syslog Address 4:

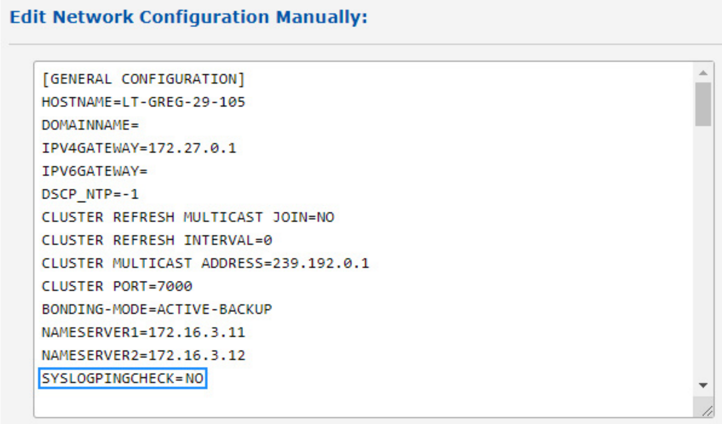
Minimum Log Level: Emergency

Transport Protocol: UDP

Port: 514

Forward: Syslog

Syslog-Address(es):
You can enter up to 4 external Syslog Servers via the webinterface. As standard, the reachability of the Syslog Server is checked via Ping/ICMP. If the registered Syslog Server cannot be reached, it will not be entered into the Syslog configuration file /etc/syslog-ng/syslog-ng.conf. In case IMCP is not allowed in the network, due to firewall regulations, you can switch off the pingcheck via the manual network configuration. To proceed navigate as described down below:



Edit Network Configuration Manually:

```
[GENERAL CONFIGURATION]
HOSTNAME=LT-GREG-29-105
DOMAINNAME=
IPV4GATEWAY=172.27.0.1
IPV6GATEWAY=
DSCP_NTP=-1
CLUSTER REFRESH MULTICAST JOIN=NO
CLUSTER REFRESH INTERVAL=0
CLUSTER MULTICAST ADDRESS=239.192.0.1
CLUSTER PORT=7000
BONDING-MODE=ACTIVE-BACKUP
NAMESERVER1=172.16.3.11
NAMESERVER2=172.16.3.12
SYSLOGPINGCHECK=NO
```

"System Page → Services and Functions → Manual Configuration → Network Configuration": Enter the value "NO" for the Parameter "SYSLOGPINGCHECK" and save the new settings.

Minimum Log Level:
Log Level Configuration

Transport-Protocol:
Transport - Protocol Configuration:
UDP - connectionless transmission
TCP - connection oriented

Port:
Configuration of the network port which is to be used. As default, IANA has registered port 514 for syslog messages.

Forward:

Syslog
Everything that is logged internally to the /var/log/messages file is also sent to the configured syslog server (of course considering the configured log level).

Format:
```
Mar 22 15:35:56 su-rims1-1 PAM-tacplus[3431]: user not authenticated by
TACACS+
```

Notification/Text
Only the events that are listed in the event list under "Notification → Notification Events" are sent to the syslog server.

Format:
```
DAEMON.INFO: Mar 22 14:39:55 su-rims1-1 ext_syslog_cfg_text: Device
Configuration Changed
```

Notification/Splunk
Same as before, only the format differs:

Format:

```
Mar 22 14:41:46 su-rims1-1 ext_syslog_cfg_splunk:  msg_nr=20,
msg_name=Device Configuration Changed, msg_txt=, add_txt=
```

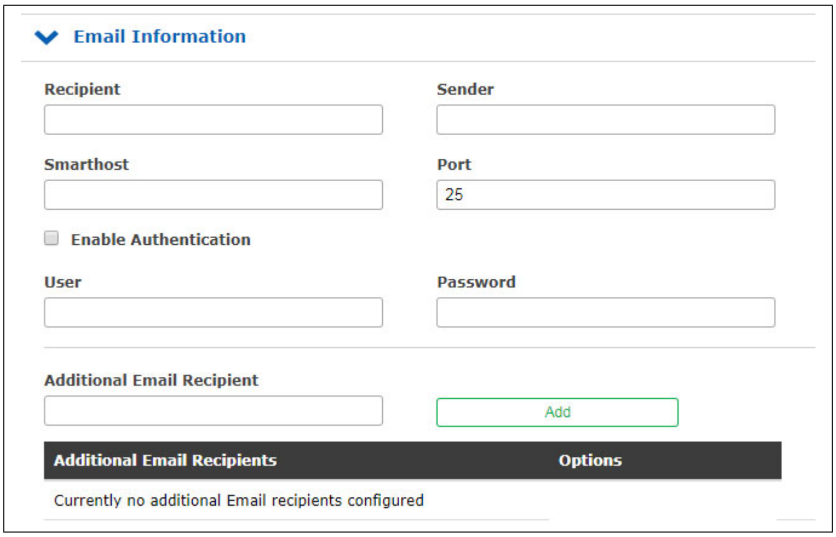
Notification/JSON
Same as before, only the format differs:

Format:

```
Mar 22 14:43:57 su-rims1-1 ext_syslog_cfg_json:  { "msg_nr":  "20",
"msg_name":  "Device Configuration Changed", "msg_txt":  "", "add_txt":  ""
}
```

10.1.3.2 Email Information

The LANTIME is able to inform about certain system events via e-mail. In the menu "Email Information" you can make the necessary settings. In the submenu "Notifications" you can select the system events, for which the LANTIME has to send out a notification e-mail.



Email Information

Recipient

Sender

Smarthost

Port

25

□ Enable Authentication

User

Password

Additional Email Recipient

Additional Email Recipients	Options
Currently no additional Email recipients configured	

Recipient: E-mail of the desired recipient.

Sender: Address of the sender.

Smarthost: To send the e-mails you require a smarthost (relay-server).
Please enter the server address here.

Port: Network port configuration. Default setting is 25, because the
SMTP (Simple Mail Transfer Protocol) uses TCP Port 25 as standard.

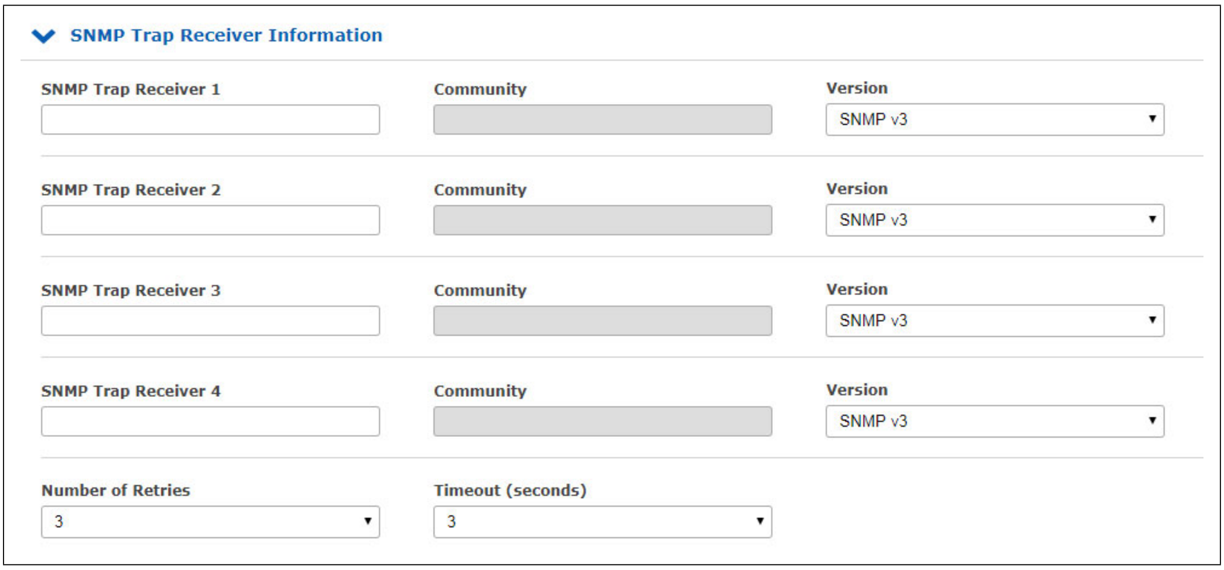
Activate Authentication: (Checkbox) Many mail servers require a valid authentication.
Please check mark the box to activate it.

Username/ Password: Please enter a valid access for the e-mail server.

Additional E-mail Recipients: Configuration of additional e-mail recipients.

10.1.3.3 SNMP Trap Receiver

The LANTIME is able to inform about certain system events with the help of SNMP traps. In the menu "SNMP Trap Receiver" you can configure up to 4 trap receiver. In the submenu "Notifications" you can select the system events, for which the LANTIME has to send an SNMP Trap.



SNMP Trap Receiver Information

SNMP Trap Receiver 1	Community	Version: SNMP v3
SNMP Trap Receiver 2	Community	Version: SNMP v3
SNMP Trap Receiver 3	Community	Version: SNMP v3
SNMP Trap Receiver 4	Community	Version: SNMP v3
Number of Retries: 3	Timeout (seconds): 3	

SNMP Trap Receiver: IP address or hostname of the SNMP trap receiver.

Community: SNMP Read Community of the Trap Receiver.

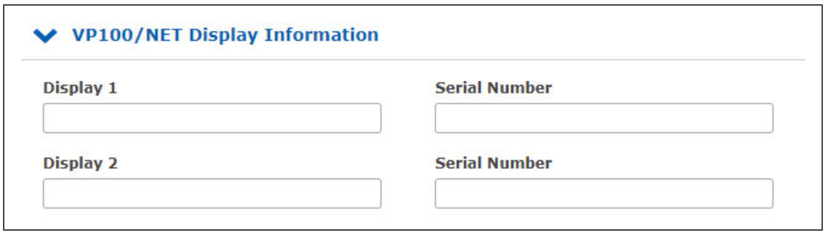
Version: SNMP version to use.

Number of Retries: Specifies the value a lantimes retries to send a Trap.

Timeout: Connection timeout value.

10.1.3.4 VP100/NET Display Information

The Meinberg VP100 / 20NET network display is used to display the time and date. This display has an integrated network card and a SNTP client. The time is taken from any NTP time server via the NTP protocol and thus the internal clock is adjusted. This display can also display any characters as scrolling text. All LANTIME alarm messages can be displayed as text messages on the display. In the submenu "Notifications", you can select the system events which are to be sent to the display by the LANTIME. A message appears three times in succession as a scrolling text on the display.



VP100/NET Display Information

Display 1

Serial Number

Display 2

Serial Number

Display: IP Addres of the network display.

Serial number: You have to enter the correct serial number of the display here.
The serial number is displayed after pressing the red SET button four times.

10.1.3.5 Overview for all Events

Event	Severity Levels (according to X.733)	Description
Normal Operation	Info	Indicates normal operation of the LANTIME
NTP Not Sync	Error	NTP Service is not sync -> NTP Messages
NTP Sync	Info	NTP service is successfully synchronized
NTP Stopped	Critical	NTP service stopped -> NTP Messages
NTP Offset Limit exceeded	Error	Maximum NTP offset value has been exceeded -> Sync Monitoring
NTP Offset Limit OK	Info	Maximum NTP offset not exceeded -> Sync Monitoring
System Reboot	Action	The system has restarted
CLK[NR] Not Responding	Critical	Receiver module is not responding -> Ref. Clock Messages
CLK[NR] Not Sync	Error	Receiver module is not sync -> Ref. Clock Messages
CLK[NR] Sync	Info	Receiver module is synchronous to its time source
Antenna Faulty	Error	No antenna or sufficient signal was detected -> Ref. Clock Messages
Antenna Reconnect	Info	Antenna / signal was detected by the LANTIME
Antenna Short Circuit	Error	Short circuit at the antenna connection -> Ref. Clock Messages
Device Configuration Changed	Action	Software configuration of the LANTIME has been changed

Table: All Notification Events

Event	Severity Levels (according to X.733)	Description
Leap Second Announced	Info	A leapsecond was announced
SHS Time Limit OK	Info	The set SHS time limit value has not been exceeded
SHS Time Limit Warning	Warning	The set threshold for an SHS warning has been exceeded
SHS Time Limit Error	Critical	The set threshold for an SHS error has been exceeded -> SHS Configuration
Power Supply Failure	Critical	Error detected on a power supply -> Safety during Operation
Power Supply OK	Info	Power supply ready for operation
Power Consumption Overload	Critical	Overload of the power supply unit(s). There are not enough power supply units in use -> Redundant Power Supply
Power Consumption OK	Info	The power supplies used provide sufficient power for the system
Power Redundancy not guaranteed	Warning	In case of failure of a power supply unit, trouble-free operation is no longer guaranteed -> Redundant Power Supply
Power Redundancy activated	Info	Normal operation is ensured even after the failure of a power supply unit
Sync Monitor	Action	Sync Monitor limits were exceeded
Sync Monitor Alert	Error	SyncMon malfunction - monitored network node is unreachable -> Error Logs
Sync Monitor OK	Info	No malfunction detected in Sync Monitor

Table: All Notification Events

Event	Severity Levels (according to X.733)	Description
MRS Source: Limit Exceed	Error	Set MRS limits have been exceeded -> Ref. Clock Messages
MRS Source: No Signal	Warning	A configured MRS time source is no longer available -> Ref. Clock Messages
MRS Source: Signal Detected	Info	A configured MRS time source is available
MRS Source: Selected Signal Changed	Action	The active MRS source has changed
MRS Source: Invalid Signal	Warning	A configured MRS source provides an invalid signal
MRS Source: Signal OK	Info	The configured MRS source provides a valid signal
Network Link Down	Error	No network connection on one of the LAN ports -> Network Messages
Network Link Up	Info	Network connection detected on the LAN port
PTP Link Down	Error	No network connection on the PTP network port
PTP Link Up	Info	Network connection detected on the PTP network port
PTP State Changed	Info	The current PTP status has changed
PTP Error	Error	A PTP error has been detected -> ??
Low System Resources	Warning	Low system resources detected
Sufficient System Resources	Info	System resources restored

Table: All Notification Events

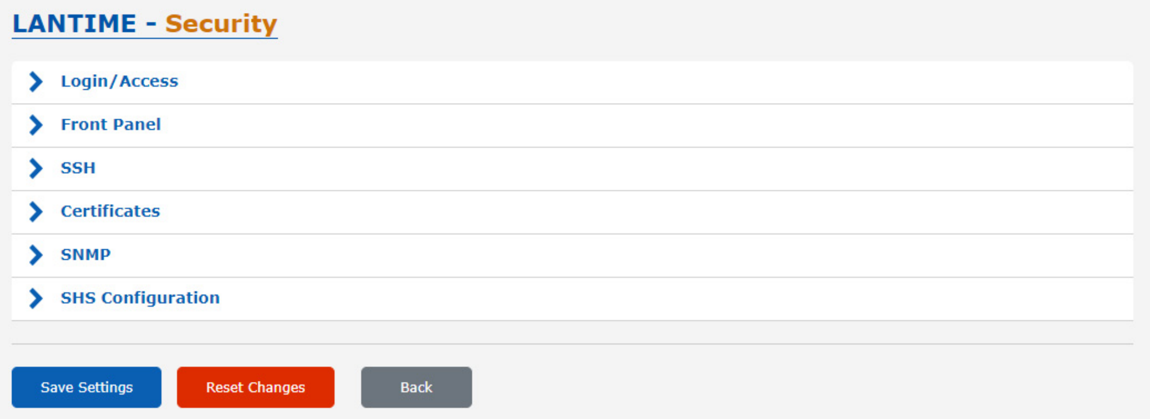
Event	Severity Levels (according to X.733)	Description
Fan Failure	Critical	An error has been detected on a fan -> Miscellaneous Messages
Fan OK	Info	No mistakes on installed fans
Certificate Expired	Error	HTTPS certificate has expired -> Certificates
HTTPS Certificate Expiration Warning (expiration in 90, 60 or 30 days)	Warning	HTTPS certificate expire in 90, 60 or 30 days -> Certificates
Self Signed HTTPS Certificate In Use	Warning	The certificate used is self-signed and does not come from an official certification authority -> Certificates
Oscillator Adjusted	Info	Internal oscillator runs stably and is completely adjusted
Oscillator Not Adjusted	Warning	Internal oscillator is not adjusted -> Ref. Clock Messages
Cluster Master Changed	Info	The master of a LANTIME NTP cluster has changed -> ??
Cluster Falseticker detected	Warning	An NTP falseticker was detected in the cluster compound
Cluster Falseticker cleared	Info	Previously detected cluster falseticker is back in order
IMS Error	Error	An error has been detected on an IMS module -> Miscellaneous Messages
IMS OK	Info	IMS module is error-free
Trusted Source OK	Info	The source selected as trusted is in the configured offset range -> ??
Trusted Source Error	Error	Offset limit violation of trusted source used -> ??

Table: All Notification Events

Event	**Severity Levels (according to X.733)**	**Description**
Sync-E Input Quality Level Changed	Info	The quality factor of the SyncE reference has changed -> ??
Port Error	Error	E.g. short circuit at the input of an IMS-VSI reference card
Port Ok	Info	Signal at the port is OK (the card must support the port event - e.g. IMS-VSI).
Faillock: user banned	Action	Failed login - user is temporarily locked

Table: All Notification Events

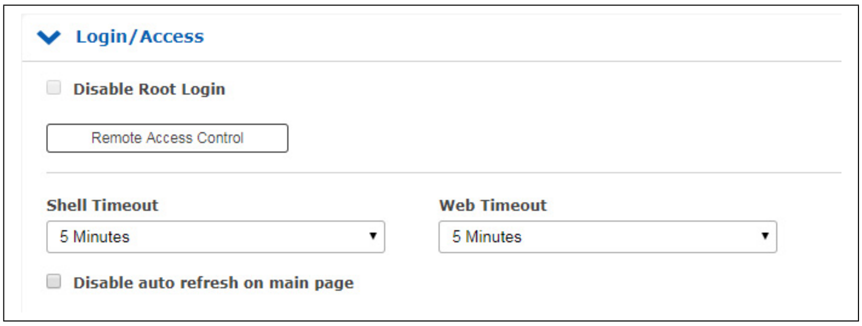
10.1.4 Security



This page allows to configure access restrictions and snmp. It also provides the functionality to handle SSH keys and the HTTPS certificate.

If unsure of required values please contact the network security administrator and provide these parameters.

Login/Access
The "Login" menu allows you to set general security settings for the login behavior of the LANTIME.



□ Disable Root Login

Shell Timeout: 5 Minutes

Web Timeout: 5 Minutes

□ Disable auto refresh on main page

Disable Root Login:
This function can only be activated by an admin user or by a super user. If this function is active, the "root" user can no longer log on to the LANTIME.

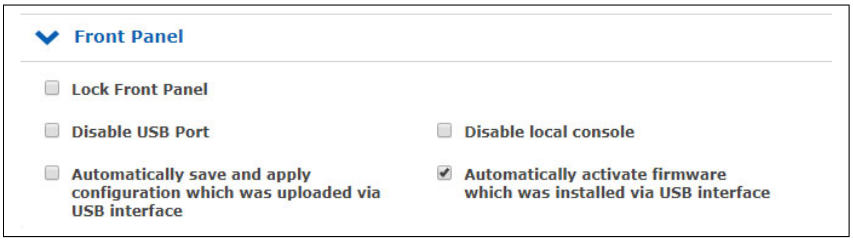
Remote Access Control:
In this configuration file, you can configure an access control for the LANTIME web interface based on the IP protocol. In this file, you can enter the IP addresses to be allowed to access the Web interface. After the first entry, access to all other clients is automatically blocked. Individual client IPs or entire subnets can be configured.

Shell Timeout:
Defines a timeout in seconds. After expiration of this period without any user interaction, the current session on the command line will be terminated for the logged-in user.

Web Timeout:
The parameter Web Timeout defines how many minutes of inactivity can pass before a user is automatically logged out of the Web interface.

Disable auto refresh on main page:
Prevents automatic reloading of the web interface in 60 seconds, as long as a user is in the main LANTIME web interface.

Front Panel:
Contains general security settings for the front panel of the LANTIME.



Front Panel

□ Lock Front Panel

□ Disable USB Port

□ Disable local console

□ Automatically save and apply configuration which was uploaded via USB interface

☑ Automatically activate firmware which was installed via USB interface

Lock Front Panel:
When the function is activated, the front panel of a LANTIME is disabled.

Disable USB Port:
After activating the feature, the USB port of a LANTIME at the front panel is deactivated and connected USB sticks can not be detected.

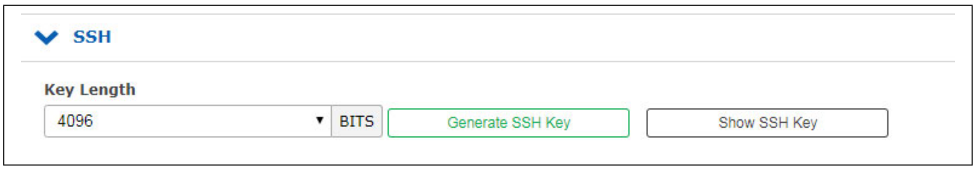
Checkbox "Automatically save and apply configuration which was uploaded via USB interface"
You can install a previously saved configuration on your LANTIME via the USB stick menu, if you have activated this check box, the uploaded configuration will be taken over directly as the start configuration.

Checkbox "Automatically activate firmware which was installed via USB interface"
By activating this checkbox, a firmware version loaded via the USB menu on the LANTIME will be directly taken over as active firmware.

Also see ??.

10.1.4.1 SSH - Secure Shell

Via "Secure Shell Login" (SSH) it is possible to establish a secured connection to the LANTIME. All data is encrypted during the transmission over Ethernet. To use this service, SSH must be enabled on each interface in the network settings (read also the configuration chapter 10.1.2.3 "Web GUI → Network → Network Services").

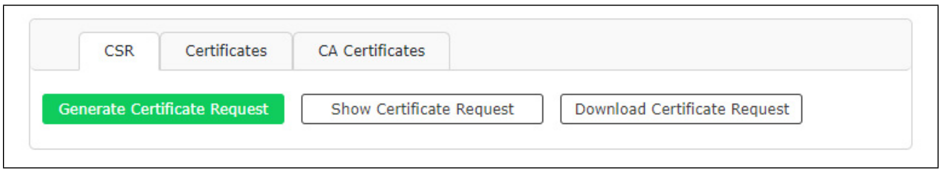


Key Length (Bits):
Determines the key length for a new key to be generated.

Generate SSH Key:
Generates a key pair, consisting of a public and private key, in configurable length.

Show SSH Key:
You can use this button to display the public SSH keys of a LANTIME.

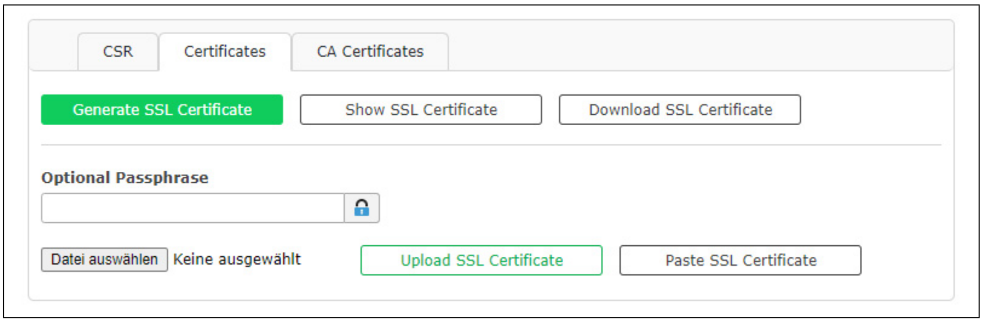
10.1.4.2 Certificates



HTTPS is a standard for encrypted transmission of data between web browser and web server. It relies on X.509 certificates and asymmetric crypto procedures. The timeserver uses these certificates to authenticate itself to a client (web browser). The first time a web browser connects to the HTTPS web server of your LANTIME, you are asked to accept the certificate of the web server.

To make sure that you are talking to your known timeserver, check the certificate and accept it, if it matches the one stored on the LANTIME. All further connections are comparing the certificate with this one, which is saved in your web browser configuration. Afterwards you are prompted to verify the certificate only when it is changed.

Note: Per default there is a self-signed certificate installed on the LANTIME which is not signed by a Certificate Authority (CA). Therefore some web browsers will state that the connection is not secure. If you want to install a certificate which was signed by a trusted Certificate Authority the "Upload SSL Certificate" button can be used. More details on this in the following instructions.



Generate SSL Certificate:
Allows to create a new self-signed SSL certificate.

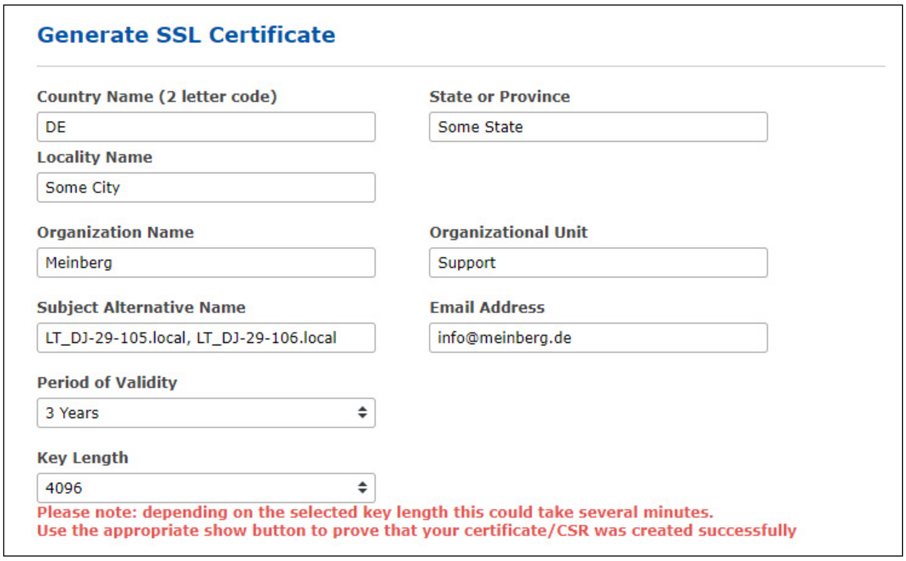
Show SSL Certificate:
Review the currently installed SSL certificate.

Download SSL Certificate:
Allows to download the currently installed SSL certificate.

Optional Passphrase
If your private key uploaded with the certificate is protected with a passphrase, you must enter the "passphrase" here. Otherwise the webserver cannot start automatically because it cannot decrypt the uploaded private key.

Upload SSL Certificate:
Allows to upload a certificate which was signed by a trusted Certificate Authority. This certificate must be in PEM file format.

Generate Certificate Request:
This feature allows you to create a Certificate Signing Request (CSR) that can be sent to a Certificate Authority to request a signed certificate. This function creates a certificate and a private key on the LANTIME. The location for the CSR is *"/mnt/flash/data/https.req"*, the matching key is stored at *"/mnt/flash/data/https.req.pk"*.



Generate SSL Certificate

Country Name (2 letter code): DE	State or Province: Some State
Locality Name: Some City	
Organization Name: Meinberg	Organizational Unit: Support
Subject Alternative Name: LT_DJ-29-105.local, LT_DJ-29-106.local	Email Address: info@meinberg.de
Period of Validity: 3 Years	
Key Length: 4096	

Please note: depending on the selected key length this could take several minutes.
Use the appropriate show button to prove that your certificate/CSR was created successfully

Subject Alternative Name

In the "Subject Alternative Name" field, you can specify additional host names (sites, IP addresses, common names, etc.) to be protected by a single SSL certificate, such as a multi-domain certificate. Multiple SANs must be entered as one comma-separated list.

Hint:
If you has generated the certificate submitted to the certification authority, via the function "Generate Certificate Request", the appropriate key for this certificate is already stored under *"/mnt/flash/data/https.req.pk"*. After uploading the signed certificate, this previously generated private key will be used.

If the submitted and signed certificate was not generated on the LANTIME, then the PEM file must contain the private key and the certificate itself.

The content of the private key starts with
"——BEGIN RSA PRIVATE KEY——"
and ends with
"——END RSA PRIVATE KEY——"

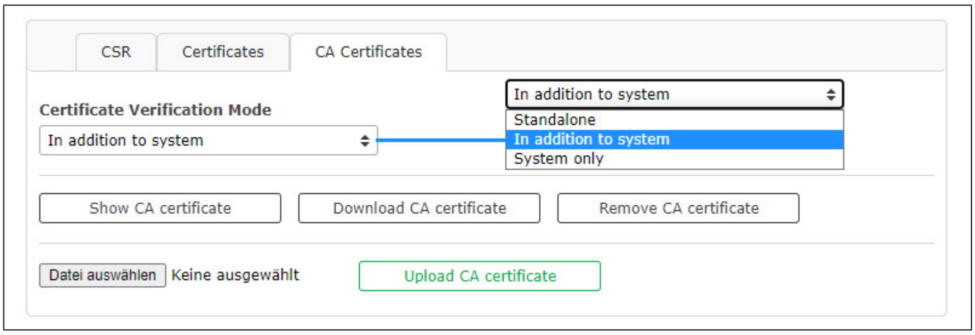
the certificate itself starts with
"——BEGIN CERTIFICATE——"
and ends with
"——END CERTIFICATE——".

This example is an excerpt from a PEM file:

```
---BEGIN RSA PRIVATE KEY---
MIICXQIBAAKBgQC6FkGxyJ6+Bqxzfp3bNtEYyiRIAbQAIsHblYPG7aQk+8XbIXWB
...
aiLbmu7N3TEdWVDgro8kMuQC/Ugkttx7TdJJbqJoVsF5
---END RSA PRIVATE KEY---
---BEGIN CERTIFICATE---
MIIEJTCCA46gAwIBAgIJANF4dlCI2saDMA0GCSqGSIb3DQEBBQUAMIG+MQswCQYD
...
ekZ970dAaPca
---END CERTIFICATE---
```

10.1.4.3 CA Certificates

The functions in the menu "Security → certificates → CA certificates" can be used to add an own, non-public root certification authority to the LANTIME. This allows programs and services which establish a TLS connection, e.g. the LDAP service, to uniquely identify the requested server, even though no (mostly paid) certificate of a public certification authority is used.



Certificate Verification Mode: In addition to system

Datei auswählen Keine ausgewählt

The Certificate Verification Mode can be selected as follows:

Standalone: The LANTIME uses only the uploaded own root certificate to verify connections.

In addition to system: The LANTIME uses the uploaded own root certificate and the system known public certification authority certificates.

System only: The LANTIME uses the system known public certification authority certificates.

10.1.4.4 Uploading signed Multi-Level / chained Certificates

The following steps require SSH access to your time server.

In addition to SSL certificates, multi-level/chained certificates are also supported. The certificate chain is stored in a separate file (*"/etc/https_ca.pem"*), which, like the web server certificate with the private key, must be in PEM format. The certificate-chain file contains the certificates, each of which is enclosed by the BEGIN and END CERTIFICATE lines as shown above.

The multi-level / chained certificates can only be imported via the command line or a file transfer. After these certificates have been saved, the web server must be restarted with the command "**restart https**" to apply the changes. By executing the command "**saveconfig**" the settings are saved permanently.

Alternatively, the yellow banner appears in the web interface, which signals a changed configuration. By clicking on "**Save as startup configuration now**" the changes can also be applied persistently.

Adding the intermediate certificates via the *"/etc/https_ca.pem"* has no influence on the automatic update process for later firmware updates. Thus new/restricted "cipher suites" are automatically adopted.

10.1.4.5 SNMP

The Simple Network Management Protocol (SNMP) is used in network management systems to monitor status of devices. SNMP works by querying "Objects". An object is simply something that we can gather information about a network device. The so called management information base (MIB) is a file which contains all objects that can be managed through SNMP.

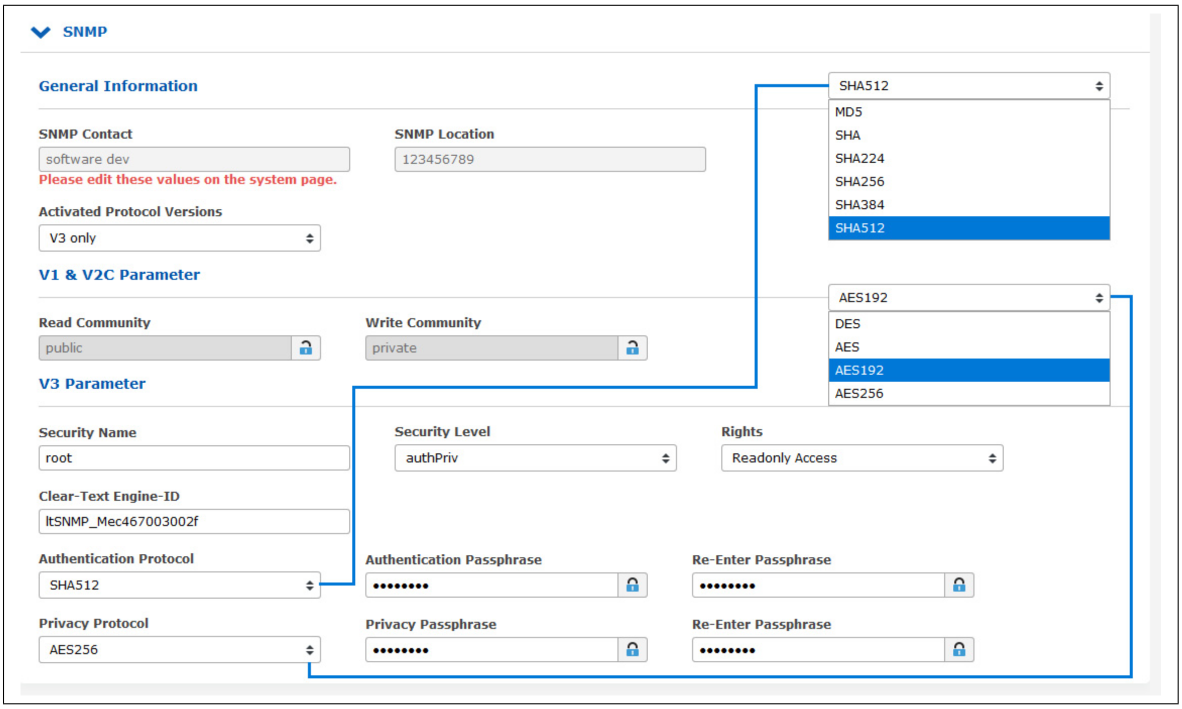
The Meinberg SNMP MIB Files can be downloaded on the "System" page → Services and Functions → Download SNMP MIB". The files named "MBG-SNM P-ROOT-MIB.mib" and "MBG-LANTIME-NG-MIB.mib" need to be used to monitor a LANTIME system.

(see also configuration chapter "Web GUI → System → Services and Functions")

By default the SNMP service is not activated on a LANTIME system. The service can be activated on each interface at the "Network page → Network Services".

(see also configuration chapter "Web GUI → Network → Network Services")

The different SNMP configuration parameters are described below:



SNMP

General Information

SNMP Contact: software dev

SNMP Location: 123456789

Please edit these values on the system page.

Activated Protocol Versions: V3 only

V1 & V2C Parameter

Read Community: public

Write Community: private

V3 Parameter

Security Name: root

Security Level: authPriv

Rights: Readonly Access

Clear-Text Engine-ID: ltSNMP_Mec467003002f

Authentication Protocol: SHA512

Authentication Passphrase: ••••••••

Re-Enter Passphrase: ••••••••

Privacy Protocol: AES256

Privacy Passphrase: ••••••••

Re-Enter Passphrase: ••••••••

Activated Protocol Versions:
Configuration of the SNMP protocol version. The following options can be selected: "V1/V2 only", "V3 only", "V1/V2/V3".

V1/V2 Parameter

Read Community:
The read community is only used for SNMP versions V1 and V2. It is like a user id or password that allows access to the LANTIME SNMP objects. The SNMP Monitoring system sends the read community string along with all SNMP requests. If the community string is correct, the LANTIME responds with the requested information. If the community string is incorrect, the LANTIME simply discards the request and does not respond.

Write Community:
The write community is only used for SNMP versions V1 and V2. It is like a user id or password that allows access to the LANTIME SNMP objects. The SNMP Monitoring system sends the write community string along with all SNMP-SET commands. If the community string is correct, the SNMP-SET command is executed. If the community string is incorrect, the SNMP-SET command is not executed.

V3 Parameter

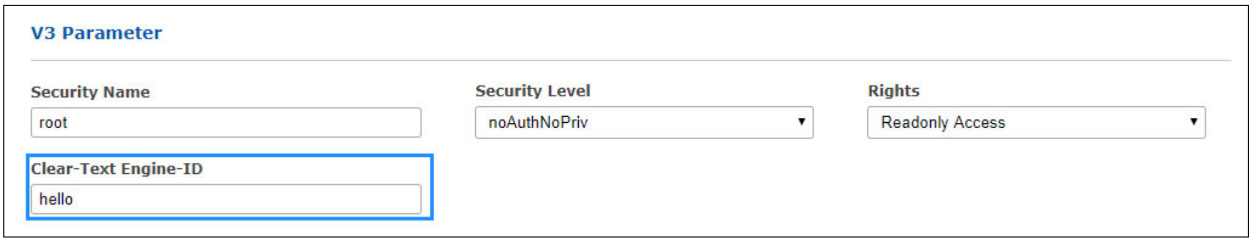
Security Name:
SNMP V3 User name

Security Level:
Messages can be sent unauthenticated, authenticated, or authenticated and encrypted by setting the Security Level to use:

noAuthnoPriv – unauthenticated and unencrypted
authNoPriv – authenticated and unencrypted
authPriv – authenticated and encrypted

Engine ID:
Within an administrative domain, a SNMP V3 Engine ID is an unique identifier of an SNMP engine. A string with a maximum of 27 characters can be entered here. The string is used to generate the hex engineID by using the text format scheme described in RFC3411. If for example the string "hello" is configured as engineID, the generated hex engineID would be 800015dd0468656c6c6f

- 15dd is the hexadecimal representation of the Meinberg enterprise ID 5597
- 04 is an indicator that the text format scheme is used to generate the engine ID
- 68656c6c6f is the hexadecimal representation of the string "hello"



V3 Parameter

Security Name: root

Security Level: noAuthNoPriv

Rights: Readonly Access

Clear-Text Engine-ID: hello

Rights:
Configuration of the access level (Read access or Read/Write access).

Authentication Protocol:
The protocols used for Authentication are MD5 and SHA (Secure Hash Algorithm):

- MD5
- SHA
- SHA224
- SHA256
- SHA384
- SHA512

Authentication-Passphrase:
User passphrase that must be at least 8 characters in length.

Privacy Protocol:
The protocols used for Encryption are DES (Data Encryption Standard) and AES (Advanced Encryption Standard):

- DES
- AES
- AES192
- AES256

Privacy Passphrase:
A passphrase which is used when encrypting packets. It must be at least 8 characters in length.

10.1.4.6 SHS Configuration

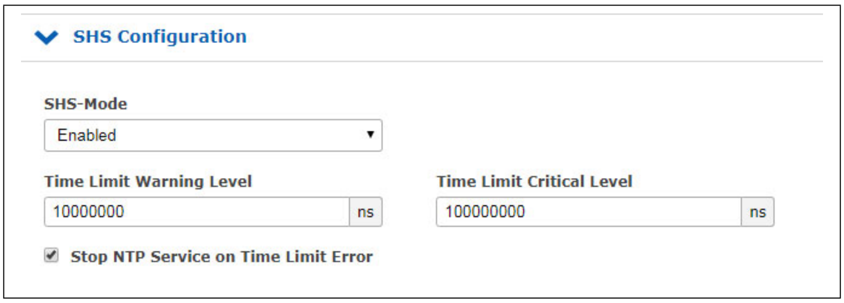
SHS is the abbreviation for Secure Hybrid System and is available on LANTIME systems with two reference clocks. When the SHS mode is enabled only the currently active clock is used for passing the timing signal on to the NTP service, the other clock is indicated as “no select” and used only for measuring and comparing a time difference between both receivers.

In this respect SHS is different from a redundant mode. In redundant mode a switching unit switches between one or the other clock, depending on its availability and sync status and the active clock passes the timing signal on the NTP service.

SHS mode takes care for a secure operation and it steps into action when a time difference between both receivers exceeds a configurable time limit.

When this happens the alarms will be trigged and send out via configured notification channels (e.g SNMP trap, email, syslog message). Besides, the NTP should be stopped in this case too to support the secure operation of the timing service, therefore you have to select “Stop NTP Service on Time Limit Error” at this step.

On the other hand, in IMS Systems with two reference clocks the timing signal coming from the clocks is continuously measured with a RSC card (Redundant Switch Control unit) and compared against each other. The measurements are forwarded to the SHS mode if this is enabled. Similar as in LANTIME systems with SHS, the alarms can be triggered when a difference of the two signals exceeds the configured time limit settings and the NTP service should be configured to stop.



SHS Configuration

SHS-Mode: Enabled

Time Limit Warning Level: 10000000 ns

Time Limit Critical Level: 100000000 ns

☑ Stop NTP Service on Time Limit Error

SHS-Mode
The SHS mode can be selectively enabled or disabled via this selection box. If the SHS mode is disabled, no time comparison takes place and the times of both receivers are transferred directly to the NTP service. The NTP service then decides autonomously which time is used for synchronization (redundant mode).

Time Limit Warning Level
If the calculated time difference between the two reference clocks exceeds the configured value, the LANTIME generates a "SHS Time Limit Warning" alarm. This alarm can be sent via e-mail or SNMP Trap, if it is configured correspondingly in the Notification settings.

(see also configuration chapter "Web GUI → Notification → Email Information")

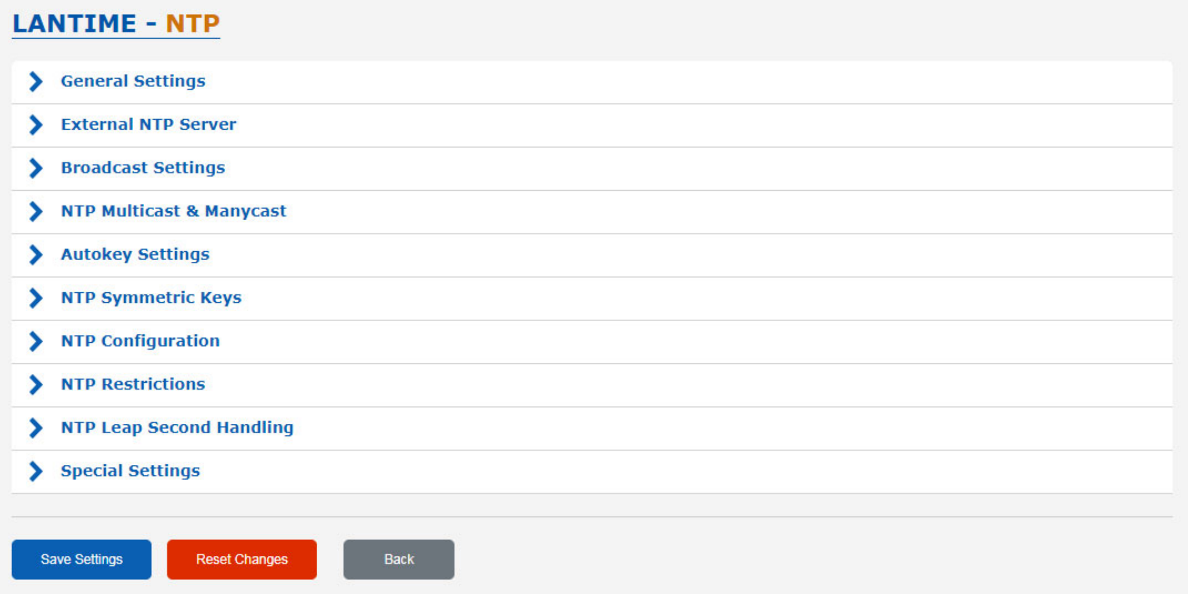
In LANTIME IMS systems with a built-in RSC, the parameter is configured in nanoseconds. For systems without an RSC in milliseconds.

Time Limit Error Level (ms)
If the calculated time difference between the two reference clocks exceeds the configured value, the LANTIME generates a "SHS Time Limit Warning" alarm. This alarm can be sent via e-mail or SNMP Trap, if it is configured correspondingly in the Notification settings.

In LANTIME IMS systems with a built-in RSC, the parameter is configured in nanoseconds. For systems without an RSC in milliseconds.

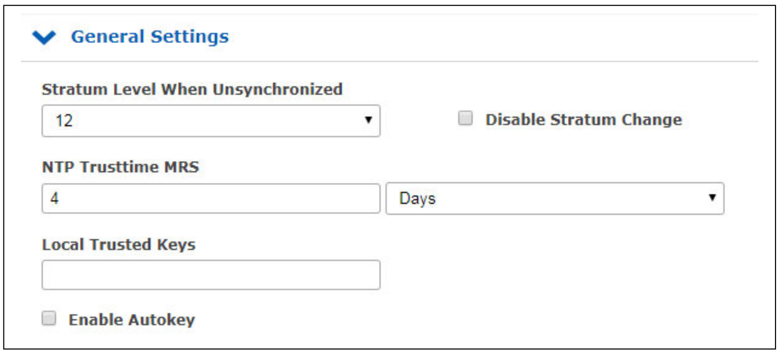
Stop NTP Service on Time Limit Error
Here you can decide if the NTP service is to be terminated at the Critical "TimeLimitError". In this case, requesting NTP clients would no longer receive a response from the time server.

10.1.5 NTP



The NTP configuration page is used to set up the additional NTP parameters needed for a more specific configuration of the NTP subsystem.

10.1.5.1 General Settings



Stratum Level When Unsynchronized: 12

□ Disable Stratum Change

NTP Trusttime MRS: 4 Days

Local Trusted Keys:

□ Enable Autokey

Stratum Level when Unsynchronized
The stratum value for NTP refers to a distance away from a reference source and not the accuracy. For example, a time server with an internal reference such as GPS or DCF77, internally has a Stratum 0 and is considered from an external network as Stratum 1. The setting "Stratum Level when Unsynchronized" is used to configure the stratum value, by which the server presents itself in the network, when a reference time source is not available. This value does not take an effect until the configured NTP Trustime for the internal reference clock has expired and no further time sources such as external NTP servers are available.

Disable Stratum Changes
By activating this operation mode, the server always presents itself (even if asynchronous) as a Stratum 1 server in the network. The "Stratum Level When Unsynchronized" setting will become ineffective.

Examples:

a) A LANTIME, which is synchronized by its internal reference clock such as GPS or DCF77, acts as a Stratum 1 NTP server. If the "Disable Stratum Change" function is activated, the NTP server will act as Stratum 1 server, if the reference clock goes asynchronous and no other time sources are available.

b) A LANTIME, which is only synchronized by an external NTP server with Stratum 3, acts in a network as Stratum 4 NTP server. If the "Disable Stratum Change" function is activated, the NTP server will still act as Stratum 4 NTP server, even if the connection to the external NTP server is lost.

c) If NTP of the LANTIME with activated "Disable Stratum Change" function, changes from its internal reference clock to an external NTP server with Stratum 2, the Stratum of the LANTIME will change from 1 to 3.

NTP Trustime

This setting defines for how long NTP should "trust" the internal reference clock of a server after this has become asynchronous. The status of an asynchronous reference clock is also called "free running". The accuracy of a "free running" reference clock depends on the type of the integrated oscillator. The trust time should therefore be set dependent on the accuracy of the "free running" reference clock.

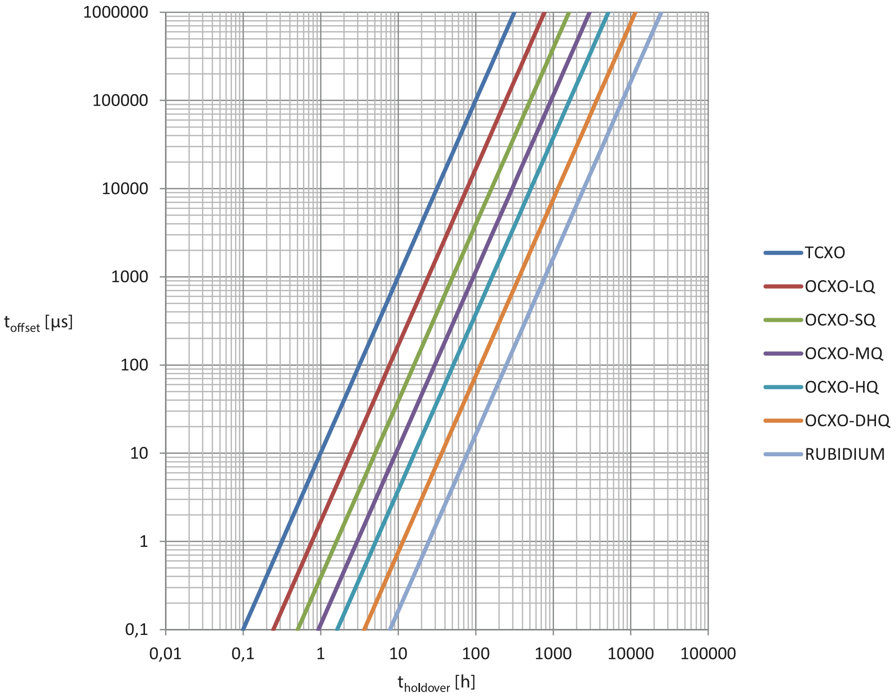


Figure: relation between holdover time (x) and offset (y) by using of built-in Meinberg oscillators

How do I configure the correct Trusttime in my application environment?
As an example, we now assume that our receiver has a built-in TCXO oscillator. The Trusttime should run out from an offset of 1ms. The graphic shows that this offset is reached after 10 hours of holdover time. Therefore a Trusttime of 10 hours should be configured.

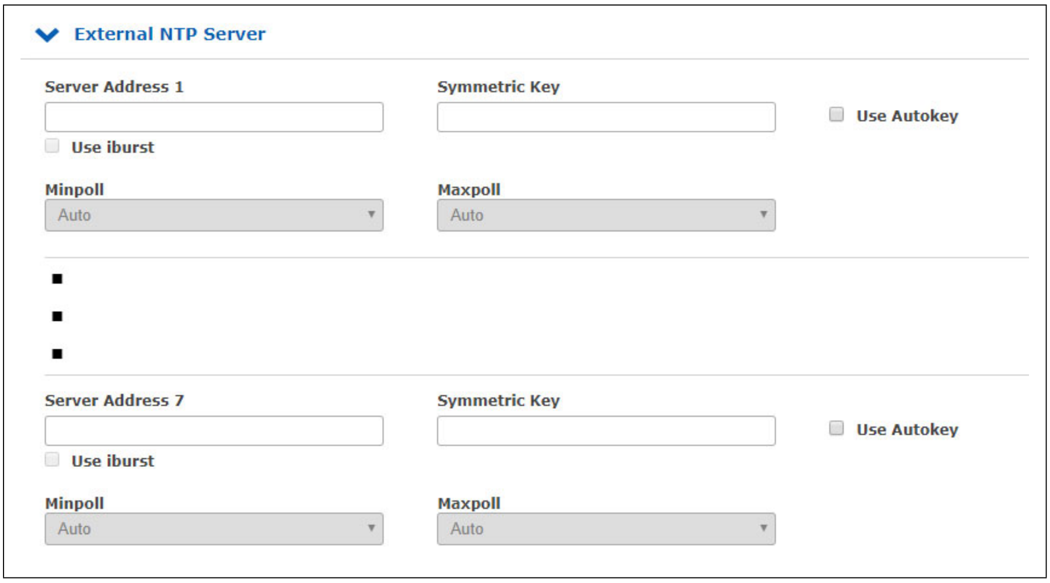
Procedure: First you should find out which oscillator is used. Go to the web interface menu "Monitoring and Management → Clock → ?? → Oscillator Type". Then you can define an offset, from which the NTP should lose its stratum or the trust time.

A list of oscillators available for Meinberg reference clocks:
https://www.meinbergglobal.com/english/specs/gpsopt.htm

Local Trusted Keys
In this field, you can enter the IDs of the symmetric keys which shall be used for the authentication. If you have more than one key, the IDs need to be entered with a space to separate them from one another. You can configure the symmetric keys in the submenu "NTP Symmetric Keys" on the NTP page. See "NTP Symmetric Keys" sub chapter for more information.

10.1.5.2 External NTP Server

Via the configuration page you can enter up to 7 external NTP server as backup for the internal reference clock.



External NTP Server

Server Address 1 | Symmetric Key | □ Use Autokey

□ Use iburst

Minpoll: Auto | Maxpoll: Auto

■

■

■

Server Address 7 | Symmetric Key | □ Use Autokey

□ Use iburst

Minpoll: Auto | Maxpoll: Auto

Server Address:
IP or Hostname of an external Server.

Symmetric Keys:
In this optional field, you can enter the ID of a symmetric key, which is to be used for authentication with the external server.

The following must be considered, to make the authentication work:

a) The NTP key file of the server must contain the ID. You can edit the key file in the submenu "NTP → NTP Symmetric Keys" on the NTP page.

b) Additionally you must enter the ID into the field "Local Trusted Keys" under "NTP → General Settings".

c) The same key with the same ID must be configured on the external server.

Minpoll and Maxpoll (not supported on devices which support the MRS feature):
With these settings, you can set the minimum and maximum polling interval (query cycle) for a given external server. NTP starts with the minimum polling interval and changes step by step to the maximum of the polling interval.

Use Iburst (not supported on devices which support the MRS feature):
The iburst activation accelerates the initial synchronization with an external server.

Particularity LANTIME/MRS:
All external NTP servers will be added to the NTP configuration file /etc/ntp.conf as "noselect". This has the effect that all servers are requested by the NTPD for statistic purposes, but the servers are never selected by the NTPD as synchronization peer. The LANTIME MRS logic then selects the best server among all servers. The selection algorithm for the best external NTP server is separated in the following steps:

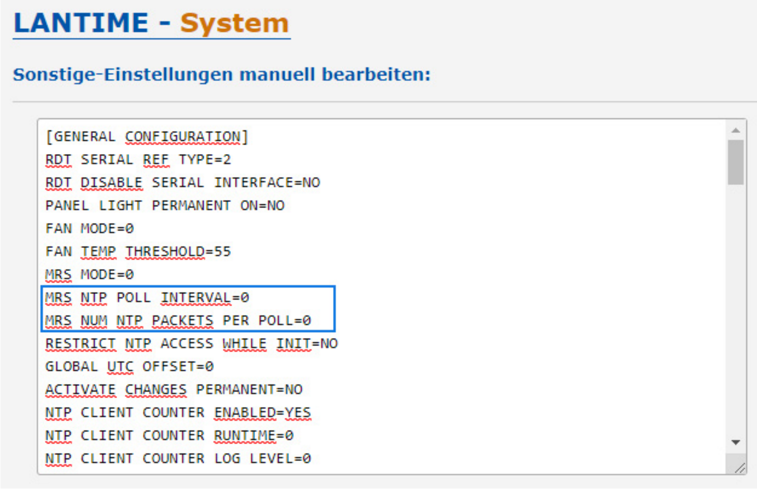
- select which server is accepted
- create groups of different offsets
- select the biggest group
- check for outliers and remove them from that group
- use the median as best-server
- check if last_best_external_NTP_server can be used - to reduce clock hopping

The best server can be checked in the Web Interface under "Statistics → NTP Status" and under "Clock → Status & Configuration → MRS Status". The determined offset is then used to discipline the internal oscillator in case no other reference source with a higher priority is available.

Due to this particularity, the configuration possibilities for external NTP server are different. The parameters Minpoll, Maxpoll and Iburst cannot be configured on a LANTIME/MRS.

For a LANTIME/MRS you can adjust the default polling interval of 32 seconds via the manual configuration of the server. To proceed follow this menu navigation:

Web Interface - "System Page → Services and Functions → Manual Configuration → Standard Configuration → Miscellaneous Configuration"



LANTIME - System

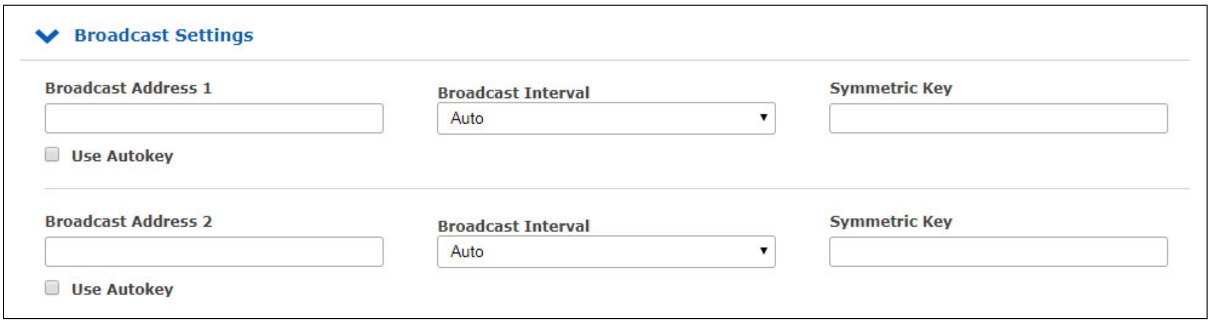
Sonstige-Einstellungen manuell bearbeiten:

```
[GENERAL CONFIGURATION]
RDT SERIAL REF TYPE=2
RDT DISABLE SERIAL INTERFACE=NO
PANEL LIGHT PERMANENT ON=NO
FAN MODE=0
FAN TEMP THRESHOLD=55
MRS MODE=0
MRS NTP POLL INTERVAL=0
MRS NUM NTP PACKETS PER POLL=0
RESTRICT NTP ACCESS WHILE INIT=NO
GLOBAL UTC OFFSET=0
ACTIVATE CHANGES PERMANENT=NO
NTP CLIENT COUNTER ENABLED=YES
NTP CLIENT COUNTER RUNTIME=0
NTP CLIENT COUNTER LOG LEVEL=0
```

You can use the parameter "MRS NTP POLL INTERVAL" to adjust the polling interval of the external server. As per default this value is set to 0, which means that external are queried every 32 seconds. Values can be set between 1 and 10 and are used as a power of 2. For example if this value is set to 6, this is equal to $2_6 =$ 64 seconds for a polling interval.

Use the parameter „MRS NUM NTP PACKETS PER POLL" to set the number of NTP queries sent per polling interval. Per default this value is set to 0, which means that 4 packets are sent in a given polling interval. Set a value between 1 and 8, which corresponds to the actual number of packets.

10.1.5.3 Broadcast Settings



Broadcast Settings

Broadcast Address 1:

Broadcast Interval: Auto

Symmetric Key:

□ Use Autokey

Broadcast Address 2:

Broadcast Interval: Auto

Symmetric Key:

□ Use Autokey

If the NTP time should be distributed in Broadcast mode in a local network, you can enter a valid broadcast address into this menu. Please note: starting with NTP4 version, the broadcast mode must always be used with authentication.

Broadcast Address:
A valid broadcast address of a local network, to which the LANTIME is connected must be entered here.

Broadcast Interval:
The interval at which the server sends the NTP packets to the configured broadcast address.

Symmetric Keys:
In this field you can enter the ID of a symmetric key, which is to be used for authentication with the NTP clients.

The following must be respected, to make the authentication work:

a) The NTP key file of the server must contain the ID. You can edit the key file in the submenu "NTP → NTP Symmetric Keys" on the NTP page.

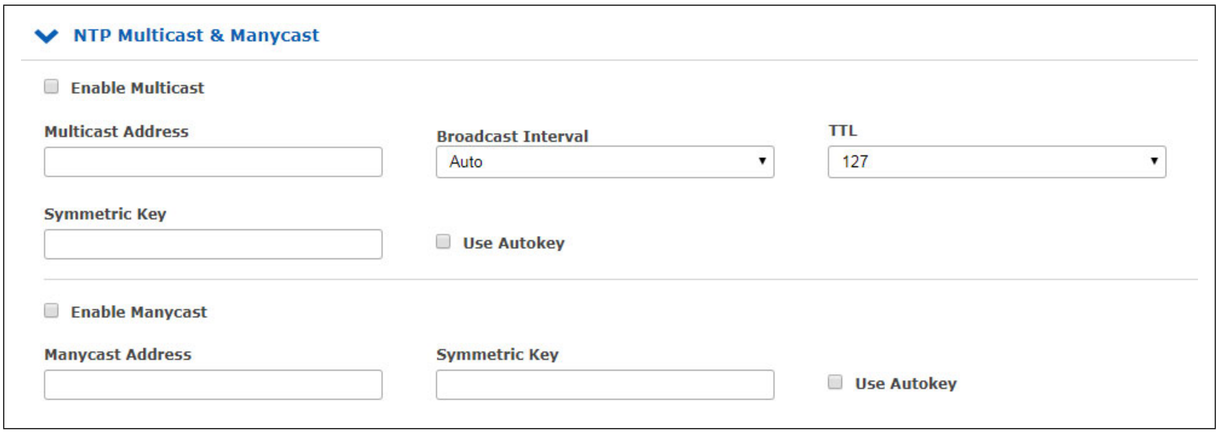
b) Additionally you must enter the ID into the field "Trustable Keys" under "NTP → General Settings".

c) The same key with the same ID must be configured on the NTP client.

The following is an excerpt from the NTP configuration of a client, which is configured as a broadcast client with authentication:

```
keys /etc/ntp.key # Path to the NTP Key File
trustedkey 1 # The Key ID, which is used for the authentication
broadcastclient # This client works as a broadcast client
```

10.1.5.4 NTP Multicast and Manycast



NTP Multicast & Manycast

□ Enable Multicast

Multicast Address

Broadcast Interval: Auto

TTL: 127

Symmetric Key

□ Use Autokey

□ Enable Manycast

Manycast Address

Symmetric Key

□ Use Autokey

10.1.5.5 NTP Multicast

NTP Multicast offers the possibility to distribute the time by multicast in the network. The Internet Assigned Numbers Authority (IANA) has exclusively allocated the multicast IP address 224.0.1.1 for NTP. Therefore, it is recommended to use this address as a multicast address. However, also other addresses of the multicast address space can be set.

The multicast address space is as follows:

```
Ipv4:  224.0.0.0 -> 239.255.255.255
Ipv6:  Every FF00::/8 Address
```

Multicast Address: A correct multicast address must be entered here.

Broadcast Interval: The interval at which the server sends the NTP packets to the configured broadcast address.

TTL: The configured TimeToLive (TTL) value determines how many hops NTP packets can pass in the network. Each network hop reduces this value by 1. When the value reaches zero, the network packet is dropped.

Symmetric Keys: For NTP Multicast, an authentication is recommended, but not mandatory. However, if the authentication is configured on the server side, it is also necessary to do so on the client side.

In the field "Symmetric Keys" you can therefore enter the ID of a symmetric key, which is to be used for authentication with the NTP clients.

The following must be respected, to make the authentication work:

a) The NTP key file of the server must contain the ID. You can edit the key file in the submenu "NTP → NTP Symmetric Keys" on the NTP page.

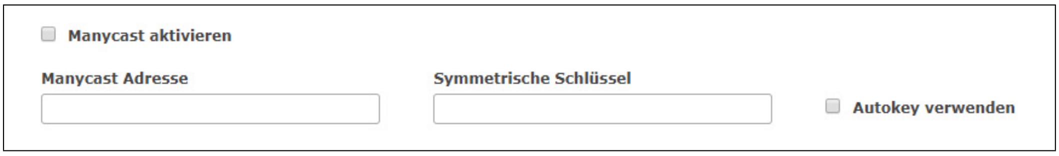
b) Additionally you must enter the ID into the field "Trustable Keys" under "NTP → General Settings".

c) The same key with the same ID must be configured on the NTP client.

The following is an excerpt from the NTP configuration of a client, which is configured as a multicast client with authentication:

```
keys /etc/ntp.key                # Path to the NPT Key file
trustedkey 1                     # The Key ID, which is used for the authentication
multicastclient 224.0.1.1 key 1  # The Client listens on the Multicast Address 224.0.1.1 and
                                 # uses the key with ID 1 for authentication
```

10.1.5.6 NTP Manycast



□ Manycast aktivieren

Manycast Adresse:

Symmetrische Schlüssel:

□ Autokey verwenden

NTP Manycast describes the possibility that one or more NTP servers are behind a multicast address. However, contrary to the multicast method, the servers do not send NTP packets periodically to this mutlicast IP. The Manycast feature is much more a method to automatically reconfigure the NTP service of a requesting client. The NTP service of the client selects up to 3 servers automatically, which seem to be "best" for him. The NTP service then reconfigures itself independently, and establishes a unicast communication with these servers. As with multicasting, it is recommended to use authentication methods.

Enable Manycast: It activates the Manycast-Feature

Manycast Address: Address field for entering the manycast address (mutlicast address space)

The Multicast Address Range is as follows:

```
Ipv4:  224.0.0.0 -> 239.255.255.255
Ipv6:  Every FF00::/8 Address
```

Symmetric Keys: For NTP Manycast, a key method for authentication is recommended, but not mandatory. However, if the authentication method is configured on the server side, it is necessary to do so on the client side.

In the field "Symmetric Keys" you can therefore enter the ID of a symmetric key, which is to be used for authentication with the NTP clients.

The following must be respected, to make the authentication work:

a) The NTP key file of the server must contain the ID. You can edit the key file in the submenu "NTP → NTP Symmetric Keys" on the NTP page.

b) Additionally you must enter the ID into the field "Trustable Keys" under "NTP → General Settings".

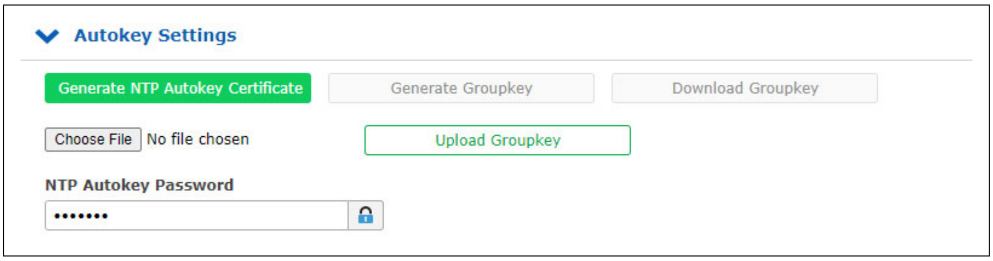
c) The same key with the same ID must be configured on the NTP client.

The following is an excerpt from the NTP configuration of a client, which is configured as a multicast client with authentication:

```
keys /etc/ntp.key               # Path to the NPT Key file
trustedkey 1                    # The Key ID, which is used for the authentication
manycastclient 224.0.1.2 key 1  # The Client listens on the Multicast Address 224.0.1.2 and
                                # uses the key with ID 1 for authentication
```

10.1.5.7 NTP Autokey Settings

NTP Version 4 supports symmetric keys and additionally provides the so-called AUTOKEY feature. The authentic of received time at the NTP clients is sufficiently ensured by the symmetric key technique. In order to achieve a higher security, e.g. against so-called replay attacks, it is important to change the used crypto keys from time to time.



In networks with a lot of clients, this can lead to a logistic problem, because the server key has to be changed on every single client. To help the administrator to reduce this work (or even eliminate it completely), the NTP developers invented the AUTOKEY feature, which works with a combination of group keys and public keys. All NTP clients are able to verify the authentic of the time they received from the NTP servers of their own AUTOKEY group by using this AUTOKEY technique.

The AUTOKEY features works by creating so-called secure groups, in which NTP servers and clients are combined. There are three different kinds of members in such a group:

a) Trusted Host
One or more trusted NTP servers. In order to become a "trusted" server, a NTP server must own a self-signed certificate marked as "trusted". It is good practice to operate the trusted hosts of a secure group at the lowest stratum level (of this group).

b) Host
One or more NTP servers, which do not own a "trusted" certificate, but only a self-signed certificate without this "trusted" mark.

c) Client
One or more NTP client systems, which in contrast to the above mentioned servers do not provide accurate time to other systems in the secure group. They only receive time.

All members of this group (trusted hosts, hosts and clients) have to have the same group key. This group key is generated by a so-called trusted authority (TA) and has to be deployed manually to all members of the group by secure means (e.g. with the UNIX SCP command). The role of a TA can be fulfilled by one of the trusted hosts of the group, but an external TA can be used, too.

The used public keys can be periodically re-created (there are menu functions for this available in the web interface and also in the CLI setup program, see "Generate NTP Autokey Certificate" in section "NTP Autokey Settings" of the "Security Management" page) and then distributed automatically to all members of the secure group. The group key remains unchanged, therefore the manual update process for crypto keys for the secure group is eliminated.
A LANTIME can be a trusted authority / trusted host combination and also a "non-trusted" host in such a secure group.

To configure the LANTIME as a TA / trusted host, enable the AUTOKEY feature and initialise the group key via the HTTPS web interface ("Generate groupkey") or CLI setup program. In order to create such a group key, a crypto password has to be used in order to encrypt / decrypt the certificate. This crypto password is shared between all group members and can be entered in the web interface and CLI setup program, too. After generating the group key, you have to distribute it to all members of your secure group (and setup these systems to use AUTOKEY, too). In the ntp.conf file of all group members you have to add the following lines (or change them, if they are already included):

```
crypto pw cryptosecret
keysdir /etc/ntp/
```

In the above example “cryptosecret“ is the crypto password, that has been used to create the group key and the public key. Please note that the crypto password is included as a plain text password in the ntp.conf, therefore this file should not be world-readable (only root should have read access to it).

On the clients, the server entries must be altered to enable the AUTOKEY feature for the connections to the NTP servers of the group. This looks like:

```
server time.meinberg.de autokey version 4
server time2.meinberg.de
```

You find the server time.meinberg.de which is using the AUTOKEY feature, while time2.meinberg.de is used without any authentic checks.

If you want to setup the LANTIME server as a trusted host, but need to use a different trusted authority, please create your own group key with this TA and include it with the web interface of your LANTIME (on page “Security Management” see section “NTP autokey” , function “Upload groupkey”).

If you want to setup the LANTIME as a “non-trusted” NTP server, you have to upload the group key of your secure group (“Security Management” / “NTP autokey” / “Upload groupkey”) and create your own, self-signed certificate (without marking it as “trusted”). Because every certificate which is creating by using the web interface and/or CLI setup is marked “trusted”, you have to execute the tool “ntp-keygen” manually on your LANTIME by using shell access (via SSH).

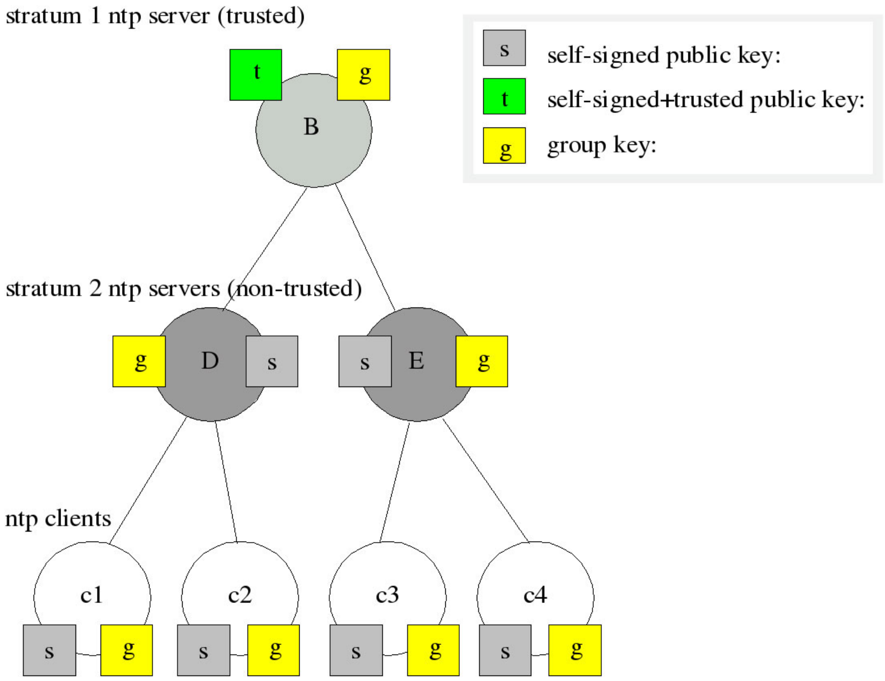
```
LantimeGpsV4:/etc/ntp # ntp-keygen -q cryptosecret
```

Here, too, “cryptosecret“ is the crypto password used in the ntp.conf entry. Then you have to copy the new ntpkeys to the flash disk with:

```
cp /etc/ntp/ntpkey_*   /mnt/flash/config/ntp/uploaded_groupkeys
```

A detailed description about ntp-keygen can be found on the NTP website (http://www.ntp.org).

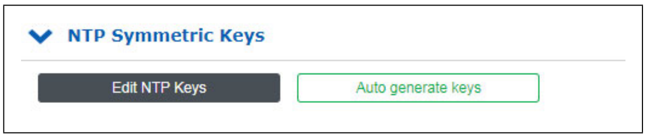
Example:
This autokey group is formed by one Stratum-1-server (B), two Stratum-2-servers (D and E) and a number of clients (in the diagram there are 4 clients shown, c1 – c4). B is the trusted host, he holds the group key and a self-signed certificate marked as "trusted".


stratum 1 ntp server (trusted)
t
g
B
s
self-signed public key:
t
self-signed+trusted public key:
g
group key:
stratum 2 ntp servers (non-trusted)
g
D
s
s
E
g
ntp clients
c1
c2
c3
c4
s
g
s
g
s
g
s
g

D and E are NTP servers, which are "non-trusted" hosts of the group, they hold the group key and a self-signed certificate which lacks the "trusted" mark. The clients also hold the group key and a self-signed certificate. In order to distribute new public keys to the whole group, the administrator only has to generate a new "t" key, which will be distributed automatically to the two hosts D and E. Because these two servers can now present a unbroken chain of certificates to a trusted host, they can be considered "trusted" by the clients as well.

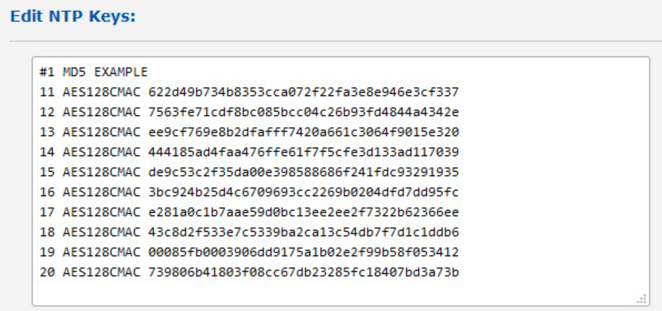
More about the technical background and detailed processes of the AUTOKEY technique can be found at the official NTP website (http://www.ntp.org).

10.1.5.8 NTP Symmetric Keys



Since NTP version 3, NTP has been providing an authentication method using symmetric keys. The "NTP Edit Key" button can be used to edit the NTP key file of the server. Upon delivery of the server, the file contains a sample key. The "Automatically Generate Keys" button allows MD5 keys and SHA1 keys to be generated automatically.

Using AES128-CMAC Keys
To use an AES128-CMAC key, the key suggestions (actually these are only random values or a random "40-character hex digit string") can be created as usual. Then the generated SHA1 keys can be modified – in this case SHA1 is replaced by AES128CMAC.



```
#1 MD5 EXAMPLE
11 AES128CMAC 622d49b734b8353cca072f22fa3e8e946e3cf337
12 AES128CMAC 7563fe71cdf8bc085bcc04c26b93fd4844a4342e
13 AES128CMAC ee9cf769e8b2dfafff7420a661c3064f9015e320
14 AES128CMAC 444185ad4faa476ffe61f7f5cfe3d133ad117039
15 AES128CMAC de9c53c2f35da00e398588686f241fdc93291935
16 AES128CMAC 3bc924b25d4c6709693cc2269b0204dfd7dd95fc
17 AES128CMAC e281a0c1b7aae59d0bc13ee2ee2f7322b62366ee
18 AES128CMAC 43c8d2f533e7c5339ba2ca13c54db7f7d1c1ddb6
19 AES128CMAC 00085fb0003906dd9175a1b02e2f99b58f053412
20 AES128CMAC 739806b41803f08cc67db23285fc18407bd3a73b
```

Figure: Menu "NTP → NTP Symmetric Keys → Edit NTP Keys"

Attention:
If symmetric keys are already in use, the contents of this file must be cached before a new block is automatically generated. The contents of the "old" file must then be re-inserted into the field **Edit NTP Keys** together with the "new" AES128-CMAC keys.

The following is an representative excerpt from an NTP key file:

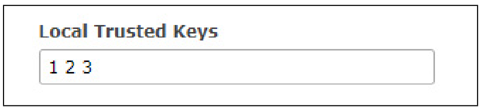
```
1    M            f294fa0                                     # MD5 key
2    MD5          BtdW/<gj2*2M;!'~qAIN                        # MD5 key
3    SHA1         094c533b614d9e4bcb6e18a97a7b0e4d459025bd    # SHA1 key
4    AES128CMAC   02eb9a63710dda360d181d9582056a504d965700    # AES128-CMAC key
```

The first column contains a unique key ID (value range 1 – 65535). The second column contains the key type ("M" or "MD5" for an MD5 key, "SHA1" for a SHA1 key or AES128CMAC for a AES128-CMAC key). The third column contains the key string, which may be between 1 and 40 characters long.

How do I set up authentication between a LANTIME and my NTP clients?

1. Add the keys which are to be used to the key file of the server as shown in the excerpt of an NTP key file.

2. Enter the IDs of these keys into the "Trusted Keys" field under "NTP → General Settings", for example:



Local Trusted Keys

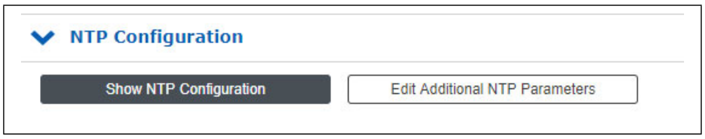
1 2 3

3. The following is a sample excerpt from the NTP configuration of a Linux client which uses the key with the ID 2 for authentication with the server 192.168.100.1 and the key with the ID 3 for authentication with the server 192.168.100.2:

```
keys /etc/ntp.keys # path to keys file
trustedkey 2 3 # IDs of keys to be trusted

server 192.168.100.1 iburst minpoll 6 maxpoll 6 key 2
server 192.168.100.2 iburst minpoll 6 maxpoll 6 key 3
```

In this case, the key file of the client must contain the keys with the IDs 2 and 3, which must be identical to the keys of the server.

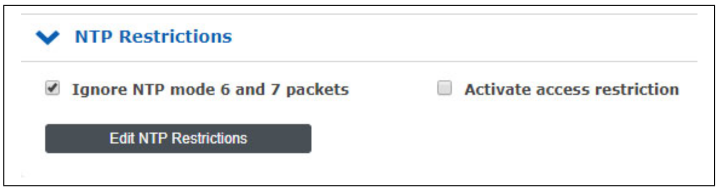
10.1.5.9 NTP Configuration



The current NTP configuration file is displayed via the "Show current NTP configuration" button. This file is automatically generated by the system at every restart or change of the NTP configuration and cannot be edited directly.

If additional settings are required for NTP (Authentication, Restriction ...), which are not covered with the existing settings on the NTP page, an additional configuration file must be used. This file can be edited and managed using the "Edit Additional NTP Parameters" button. Every time the 'ntp.conf' is created this additional file is automatically attached to it.

10.1.5.10 NTP Restrictions



☑ Ignore NTP mode 6 and 7 packets
☐ Activate access restriction

The "NTP Restrictions" page can be used to restrict NTP access to specific IP addresses.

For example, to allow access for all addresses from the subnet 192.168.100.x, enter 192.168.100.0 under IP Address and 255.255.255.0 under Netmask. Access can also be allowed for individual IP addresses.

In order to enable the restricted access, the "Activate Access Restriction" option must be activated here. Client IP addresses, which are not covered in the allowed IP address ranges, will no more receive NTP responses from the LANTIME.

Ignore NTP Mode 6 and 7 Packets
This setting cause that internal information, like Access statistics, cannot be queried by other NTP able devices in the network, via the NTP service of the server. The setting does not have any effect on the time synchronization between NTP clients and the server.

Activate access restriction
By activating this setting the following lines will be written into the NTP configuration of the Server:

```
restrict default noserve
restrict -6 default noserve
restrict 127.0.0.1
restrict -6 ::1
```

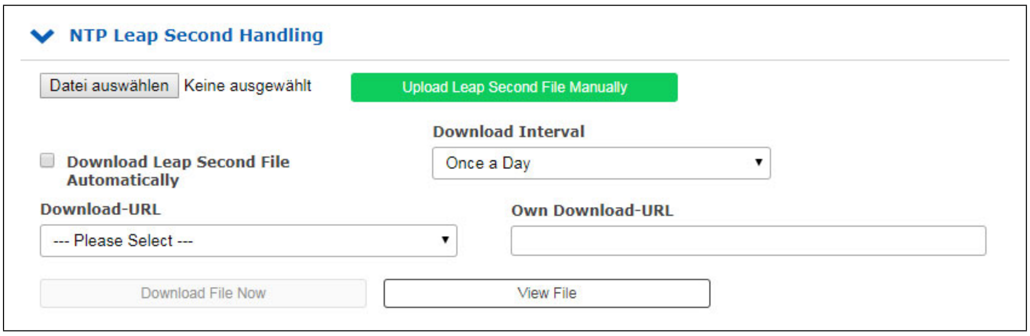
These settings cause that the server no longer responds to NTP requests. In the submenu "Configure NTP Restrictions" you can configure a “white list” of client IP addresses or even entire subnets whose requests are allowed to be answered by the server.

10.1.5.11 NTP Leap Second Handling

The time base for mostly all the world's local time zones is called Coordinated Universal Time, UTC, which is derived from a several atomic clocks which are distributed in different countries all over the world. The rotation of the earth is not constant and varies over time, while the mean earth rotation speed is decreasing slowly. This is the reason why so called leap seconds are inserted into the UTC time scale, which compensate the UTC time with the real earth rotation. A leap second is always inserted at 23:59:59 (UTC), either on 31.12. or 30.06. (Other dates are theoretically possible, but practically have not been used yet).

Some protocols or methods for transferring the time information, e.g. GPS, NTP, PTP, DCF77 and IRIG can pre-announce leap seconds to give a receiver the opportunity to prepare for a leap second in advance. The GPS satellite system distributes the leap second announcement six months before the leap second event. Meinberg LANTIMEs with GPS receivers receive this announcement automatically via the GPS signal. In the log file of the LANTIME, the entry "Leap Second Announced" is generated when the date of the leap second is received.

Other synchronization methods do not offer this announcement possibility, which can lead to a one second time jump. Therefore, it is necessary to keep the NTP leap second file up-to-date on these systems, so that a leap second is correctly inserted at the midnight (UTC).


NTP Leap Second Handling

Datei auswählen Keine ausgewählt

Upload Leap Second File Manually

Download Interval: Once a Day

□ Download Leap Second File Automatically

Download-URL: --- Please Select ---

Own Download-URL:

Download File Now

View File

In the menu "NTP Leap Second Handling", you can view the currently stored leap second file, you can manually upload the file or configure an automatic download from the following source pages:

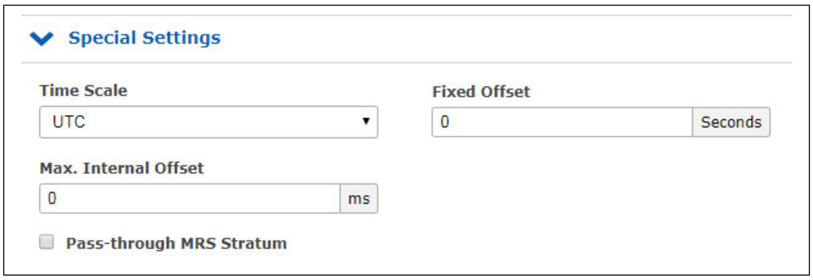
Available Download Sources for Leap Second Files:

1. NIST Leap Second File:
   ftp://time.nist.gov/pub/ (directory listing)
   ftp://time.nist.gov/pub/leap-seconds.list (current leap second file)

2. IERS (Earth Rotation and reference systems Service) Leap Second File:
   https://hpiers.obspm.fr/iers/bul/bulc/ntp/ (directory listing)
   https://hpiers.obspm.fr/iers/bul/bulc/ntp/leap-seconds.list (current leapseconds file)

3. Meinberg Leap Second File (Copy of the IERS Leap Second File):
   https://www.meinberg.de/download/ntp/leap-seconds.list
   https://www.meinberg.de/download/ntp/leap_second

10.1.5.12 Special Settings



Special Settings

Time Scale: UTC

Fixed Offset: 0 Seconds

Max. Internal Offset: 0 ms

□ Pass-through MRS Stratum

Time Scale
This setting configures the time zone of the NTP. The default setting is "UTC", since NTP is based on UTC by default and standard NTP clients expect UTC time.

The setting "LOCAL TIME" should only be selected, if the time server is used to synchronize specific clients that require local time. If you select "LOCAL TIME" here, the exact time zone must be configured in the menu "System → Display".

Attention: The use of "LOCAL TIME" is a violation of the NTP standard and causes standard NTP clients to accept faulty time and to make a time jump accordingly.

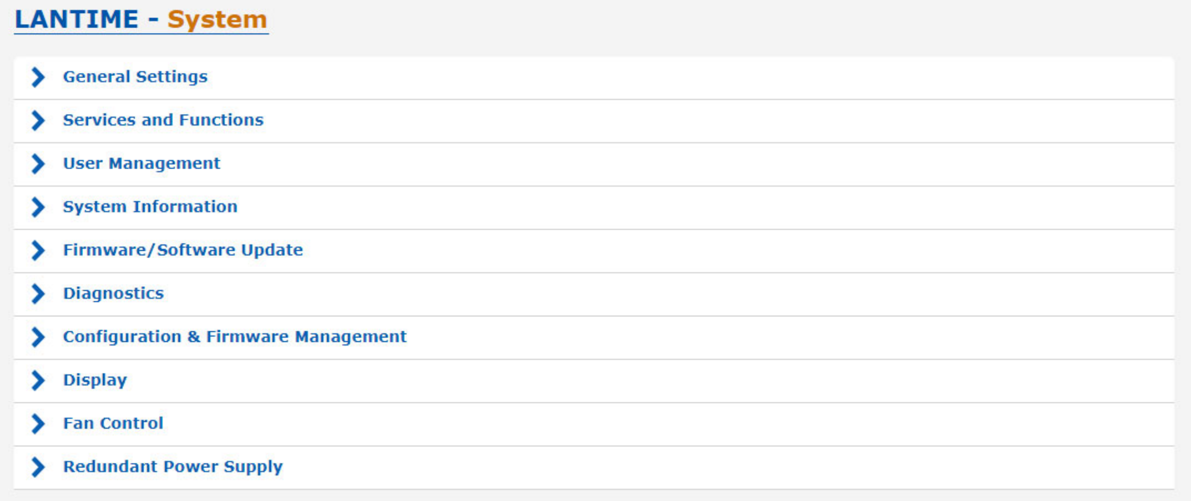
Fixed Offset (s)
This value is used to manipulate the output time of the NTP service. The configured value in seconds is added to the current time and provides a possibility to spoof the NTP time if wanted.

Attention: The use of a "Fixed Offset" is a violation of the NTP standard and causes standard NTP clients to accept faulty time and to make a time jump accordingly.

Max. Internal Offset (s)
This value in milliseconds specifies a minimum accuracy the NTP service must reach, before the server starts to serve time to the clients. E.g. entering a value of 1ms means that the service will wait until the internal clock has reached 1ms accuracy or better.

Pass-through MRS Stratum
This feature only comes into effect if you synchronize a LANTIME with MRS feature primarily via NTP. If "Pass-through MRS Stratum" is not activated, the LANTIME presents itself as Stratum 1 server in the network. If "Pass-through MRS Stratum" is active, the stratum of the external NTP server is considered. For example, if the external server is a Stratum 1 server, the MRS LANTIME would appear as Stratum 2 server in the network.

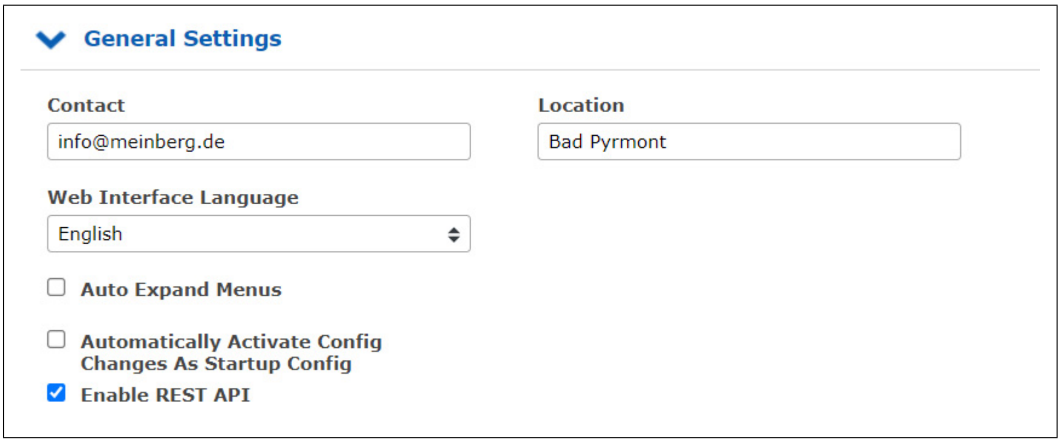
10.1.6 System



LANTIME - System

- General Settings
- Services and Functions
- User Management
- System Information
- Firmware/Software Update
- Diagnostics
- Configuration & Firmware Management
- Display
- Fan Control
- Redundant Power Supply

10.1.6.1 General Settings



General Settings

Contact: info@meinberg.de

Location: Bad Pyrmont

Web Interface Language: English

□ Auto Expand Menus

□ Automatically Activate Config Changes As Startup Config

☑ Enable REST API

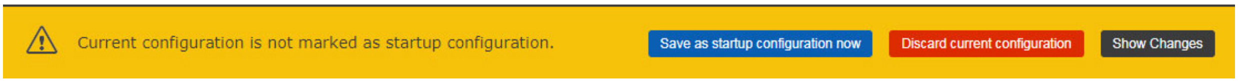
Contact:
An input field for storing the contact information. The information is also displayed on the main page of the web interface and can be queried via SNMP.

Location:
An input field for storing the device location. The information is also displayed on the main page of the web interface and can be queried via SNMP.

Web Interface Language:
Language setting of the web interface.

Auto Expand Menus:
If this feature is enabled all sub-menus will be expanded in each configuration dialogue.

Automatically Activate Config Changes As Startup Config:
If this option is enabled, each configuration change is immediately added to the startup configuration of the LANTIME (the startup configuration is the configuration that is used when the LANTIME is booted). If the option is not activated, the following note is displayed in the header of the Web interface after each configuration change.



Current configuration is not marked as startup configuration.

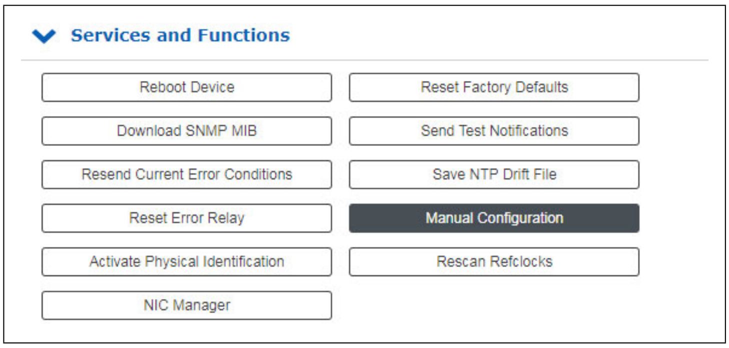
Save as startup configuration now
Discard current configuration
Show Changes

Each configuration change can then be saved as start configuration by confirming with "Save as startup configuration now" button.

REST API Support

In the 7.04 release, a REST API interface is offered for the first time to retrieve status information and make configuration adjustments from external management systems over a secure HTTPS connection. The available objects are stored in a JSON-based syntax as a tree structure. The REST API can be enabled and disabled as a service by configuration. An explanation of all available objects is included in an integrated online help in the firmware and can be accessed via the Web UI: https://YOUR-LANTIME-IP-ADRESS/clihelp/

10.1.6.2 Services and Functions



Reboot Device:

Initiates a restart of the LANTIME operating system. The built-in reference clock and output signals generated by the clock remain unaffected.

Download SNMP MIB:

Download the Meinberg SNMP MIB files. The archive file contains all Meinberg SNMP MIB files. To monitor a LANTIME time server with a V7 firmware via SNMP, only the MBG-SNMP-ROOT-MIB.mib and MBG-LANTIME-NG-MIB.mib files from the archive file are required.

Resend Current Error Conditions:

The button can be used to send the user the LANTIME error logs via e-mail or SNMP Trap. In order to use this function, the error events must be activated on the "Notification" page under "Notification Events" for the desired channel (eg e-mail or SNMP). An e-mail receiver or SNMP trap receiver must also be configured.

Reset Error Relay:

With this button the error relay can be set to an error-free position.

Activate Physical Identification:

This function can be used to find a LANTIME device. After the button is activated, the LANTIME starts to beep once per second and the alarm LED at the front panel flashes red. The function is terminated by pressing the "F2" button on the front panel.

Reset Factory Defaults:

Resets the LANTIME to factory defaults. (Attention: The network settings are retained during the reset via the web interface. If the network settings need to be reset as well, the reset must be initiated via the front panel.) During the reset, LANTIME restarts. After restarting the LANTIME can be reconfigured with the default user "root" and password "timeserver".

Send Test Notifications:
Sending a test notification to the configured e-mail recipients and / or SNMP trap receivers.

Save NTP Drift File:
The NTP service determines the offsets of the system clock at runtime and stores them in the so-called NTP drift file. This file is used by the NTP service to automatically adjust the system clock, even if no time source is currently available at short notice.

The "Save NTP Drift File" function saves the current NTP drift file /etc/ntp.drift on the internal Compact Flash card at /mnt/flash/data/ntp.drift. When the LANTIME is restarted, the value from the stored drift file can be read out by the NTP service, which accelerates the initial time adjusting process.

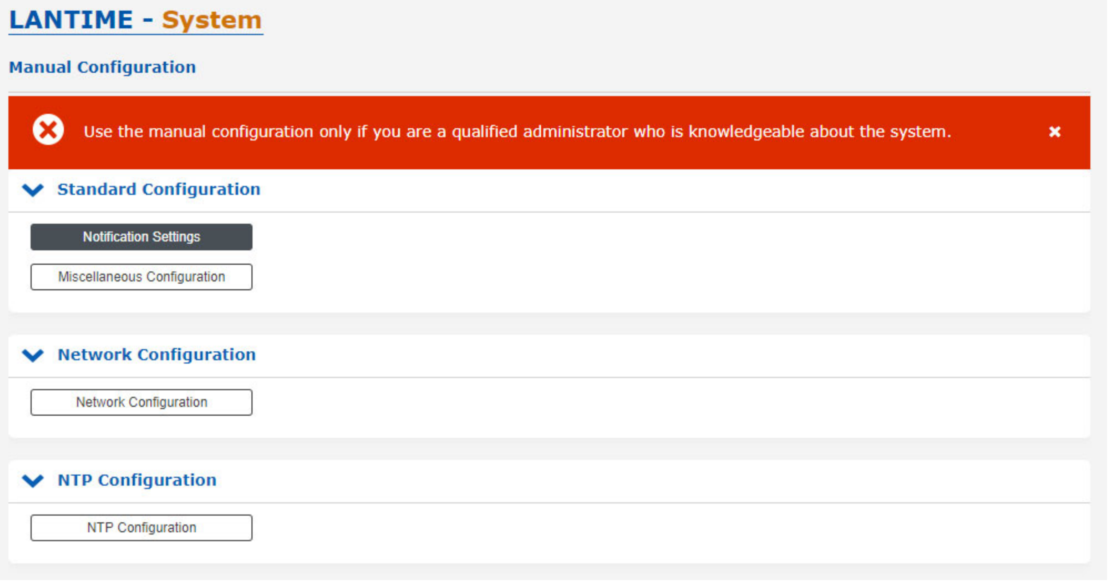
Manual Configuration:
The "Manual Configuration" button allows a direct access to the configuration files of the LANTIME. This feature should only be used by experienced administrators.

NIC Manager
The NIC Manager checks the system for physical network interfaces. This applies to the additional interfaces that can be added to the system via LNE modules. After the installation and initialization of an LNE card, the function must be executed so that the file "etc/mbg/net.cfg" is rewritten. The network port status can then be displayed on the start page of the web interface.

The NIC Manager function should also be executed after removing or replacing an LNE. The system uses the MAC addresses of the individual network ports to check whether they exist, whether their position (slot) in the system has changed or whether new interfaces exist.

Rescan Refclocks
This function must be executed if a second clock is subsequently installed in IMS systems in order to obtain a redundant receiver configuration. After start-up, the system remembers the serial connection of the reference clock used. If, for example, an M3000- or M1000 system with built-in RSC a second clock will be installed during operation (hot-plug), the "Rescan Refclocks" button must be pressed to register the new clock so that the serial connection of the second clock will be saved on the system.

10.1.6.3 Manual Configuration



LANTIME - System

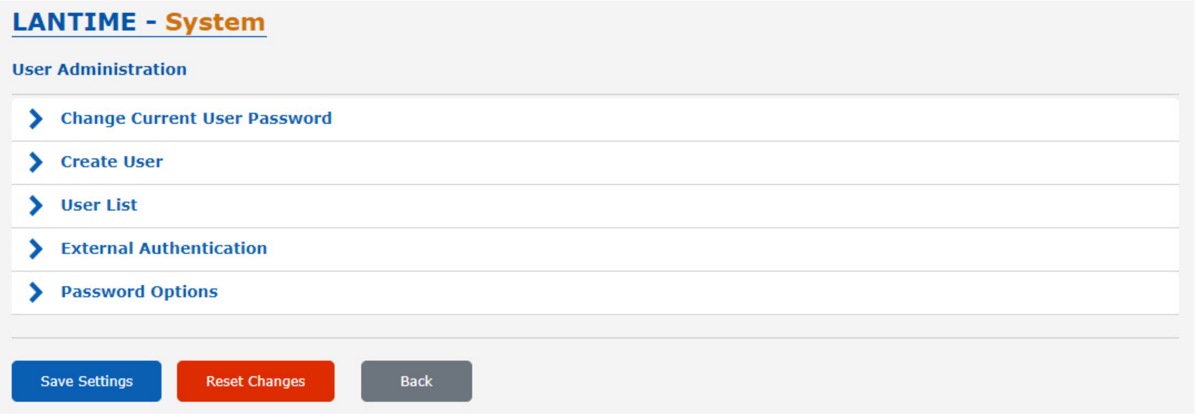
Manual Configuration

Use the manual configuration only if you are a qualified administrator who is knowledgeable about the system.

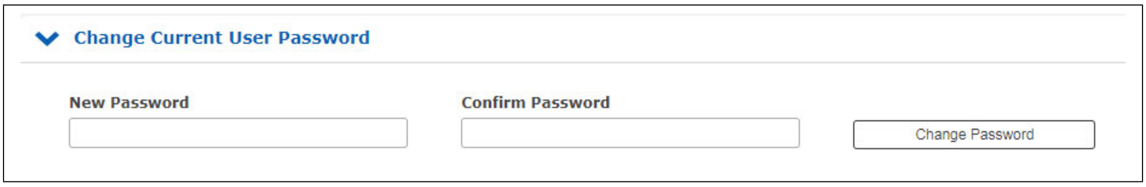
- Notification Settings
- Miscellaneous Configuration
- Network Configuration
- NTP Configuration
- NTP Broadcast Configuration

With "Manual configuration" you are able to change the main configuration by editing the configuration file by hand. After editing, press the “Save file” button to preserve your changes, afterwards you are asked if your changes should be activated by reloading the configuration (this results in reloading several subsystems like NTPD, HTTPD etc.).

10.1.6.4 User Management



Change Current User Password
Here you can change the password of the currently authenticated user.



Create User
It is possible to create multiple user accounts on a LANTIME system, each account can be assigned one of three access levels: the Super-User level has full read-write access to the configuration of the LANTIME system, it can modify all parameters and has full shell access to the system when logging in via Telnet, SSH or serial console port. Administrator level accounts can only modify parameters via the WEB interface but does not have shell access. The access level "Info" can only review status and configuration options but is not allowed to modify any parameters or configuration files.

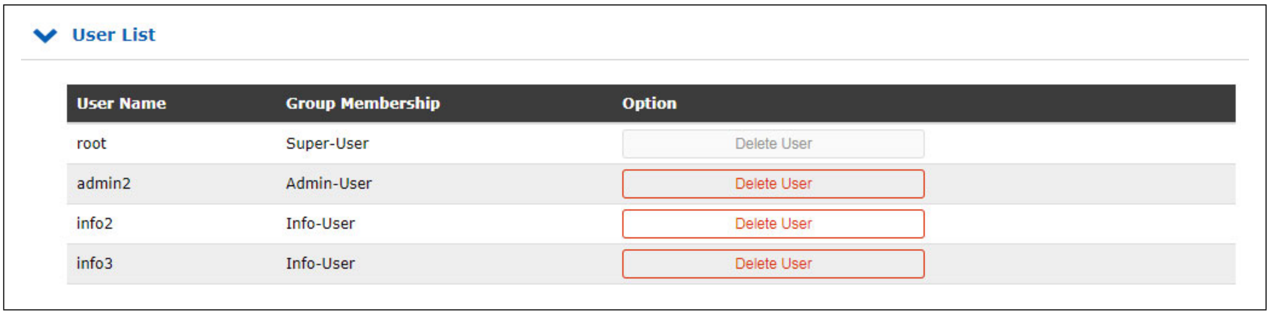
The table below illustrates the user-rights of each access level in detail.

	Super User	Admin User	Info User
Full access to the Command Line	✓		
Change device configuration through the WebUI	✓	✓	
Editing of the additional configuration files, which are available through the WebUI*	✓		
Perform a Firmware Update	✓		
Create a diagnostic file	✓		
Create a new super user account	✓		
Review all webinterface configuration values	✓	✓	✓

*Additional Network Configuration, Additional NTP Configuration, User defined notifications

User List

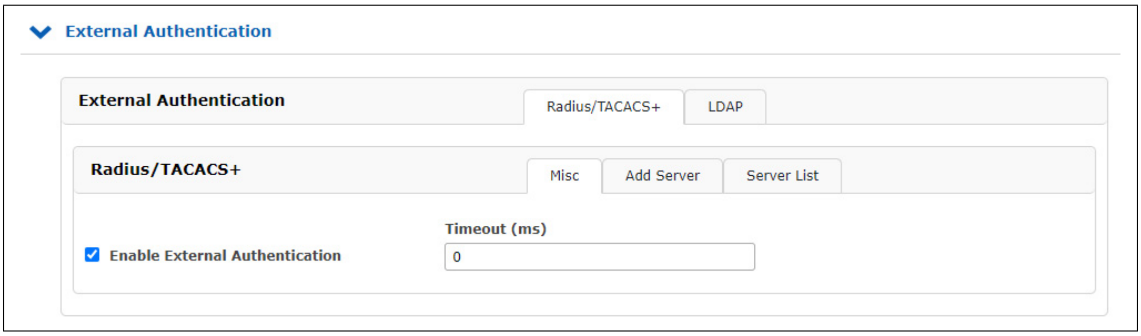
This submenu gives you an overview of all configured LANTIME users. By clicking "Delete User" a single user can be deleted.



User List

User Name	Group Membership	Option
root	Super-User	Delete User
admin2	Admin-User	Delete User
info2	Info-User	Delete User
info3	Info-User	Delete User

10.1.6.5 External Authentication Options



☑ Enable External Authentication

Timeout (ms): 0

The LANTIME supports Radius and TACACS as external authentication methods.

Enable External Authentication:
Through this checkbox you can either enable or disable the external authentication feature of the LANTIME.

Timeout (ms):
Period of time how long to wait for an "access accept" packet from an authentication server.

You can choose between several Authentification Methods:
1. LDAP
2. RADIUS
3. TACACS+

10.1.6.6 LDAP / LDAPS

Lightweight Directory Access Protocol
LDAP is based on the client-server model and is used for so-called directory services. LDAP describes the communication between the LDAP client and the directory server. Object-related data, such as personal data or computer configurations, can be read from such a directory.

10.1.6.7 LDAP Setup

Example LDAP setup in connection with the Microsoft Active Directory (AD)

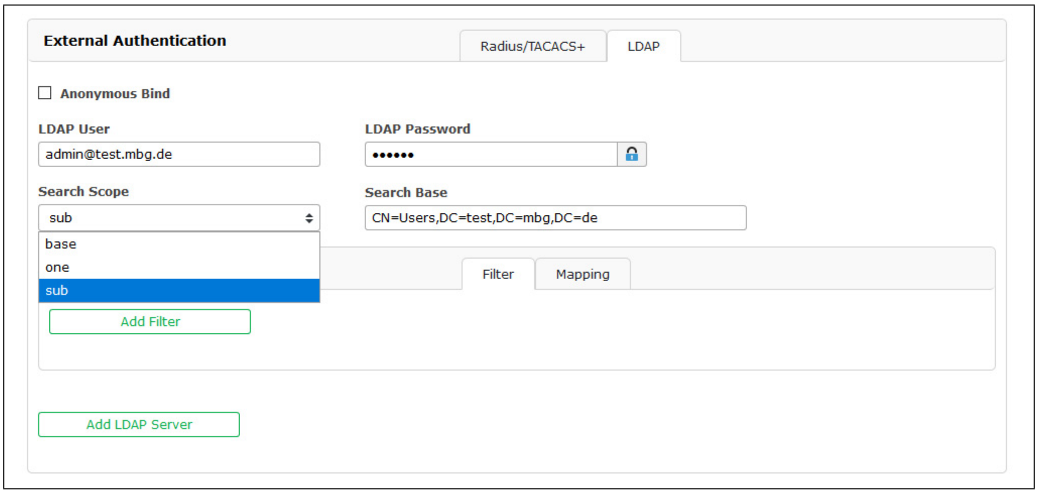
This chapter describes an example for setting up an LDAP connection with the Microsoft Active Directory with non-standard attributes of an admin user. Please note that this is an example only and may not be directly applicable to your directory structure. Please contact your directory service administrator to identify any discrepancies and make any necessary adjustments.

The ADSI editor of the Microsoft Active Directory is used to adjust the following attributes of an LDAP user:

- gidNumber = 4
- sAMAccountName = ldap-ad
- uidNumber = 10020
- unixHomeDirectory = /home/ldap-ad
- loginShell = /bin/false

The name of the user (ldap-ad) the uidNumber and the "HomeDirectory" name are freely selectable. These are only example values. Also the attributes (e.g. sAMAccountName) can be freely chosen by the mapping. It is only important that a mapping of the attribute selected in the directory service is defined by the attribute provided for this purpose in the RFC ("shadow uid sAMAccountName" for this example).

After specifying "LDAP User", "LDAP Password", "Search Scope" and "Search Base", the filters and mappings can be defined. The LDAP user/binddn is required to read information from the AD, and is not normally a user to log into this machine afterwards.



☐ Anonymous Bind

LDAP User: admin@test.mbg.de

LDAP Password: ••••••

Search Scope: sub

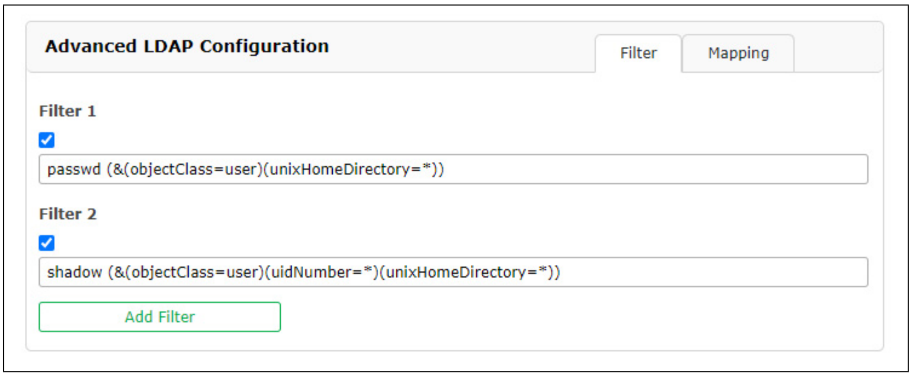
Search Base: CN=Users,DC=test,DC=mbg,DC=de

Figure: Web interface menu "System → User Administration → External Authentication → LDAP"

In the sample domain test.mbg.de the "Search Base" "CN=Users,DC=test,DC=mbg" was selected and the "Search-Scope" was set to "sub".

The following filters and mappings must be added to this sample configuration via the web frontend of LTOS.

Filter:
- passwd (&(objectClass=user)(unixHomeDirectory=*))
- shadow (&(objectClass=user)(uidNumber=*)(unixHomeDirectory=*))



Filter 1

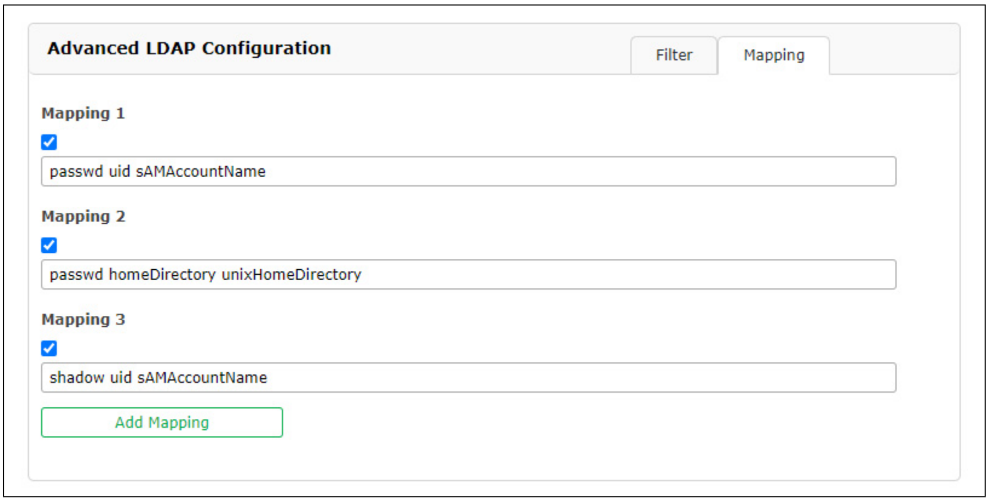
☑ passwd (&(objectClass=user)(unixHomeDirectory=*))

Filter 2

☑ shadow (&(objectClass=user)(uidNumber=*)(unixHomeDirectory=*))

Figure: LDAP sub menu "Advanced LDAP Configuration → Filter"

Mappings:
- passwd uid sAMAccountName
- passwd homeDirectory unixHomeDirectory
- shadow uid sAMAccountName



Mapping 1

☑ passwd uid sAMAccountName

Mapping 2

☑ passwd homeDirectory unixHomeDirectory

Mapping 3

☑ shadow uid sAMAccountName

Figure: LDAP sub menu "Advanced LDAP Configuration → Mapping"

The gidNumber can sometimes conflict with group membership on other systems. Ask your directory service administrator for possible avoidance strategies.

After the URI of the LDAP server is assigned, the settings can be saved. If LDAP is selected as the protocol, the configured LDAP users can log in via the web frontend (and the CLI if a loginShell has been assigned for the super user). If LDAPS is selected as protocol, the rootca certificate that uniquely identifies the LDAP server (see CA Certificates) must be added beforehand.

10.1.6.8 RADIUS

Radius stands for Remote Authentication Dial In User Service and provides centralized authentication for LANTIME devices. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport protocol.

The LANTIME RADIUS authentication requires that each account that should be able to login to the LANTIME has a Vendor Specific Attribute (VSA) called MBG-Management-Privilege-Level configured. This VSA has to be added to the RADIUS configuration of an external authentication server. Here some additional Information on the attribute:

```
Name = MBG-Management-Privilege-Level
Datatype = Integer
Vendor-Code = 5597
Vendor assigned attribute number = 1
Value range = 100, 200, 300
```

In addition you need to assign a value of 100 (Super User), 200 (Admin User) or 300 (Info User) for this attribute for each RADIUS user, which should be able to login to the LANTIME.

10.1.6.9 TACACS

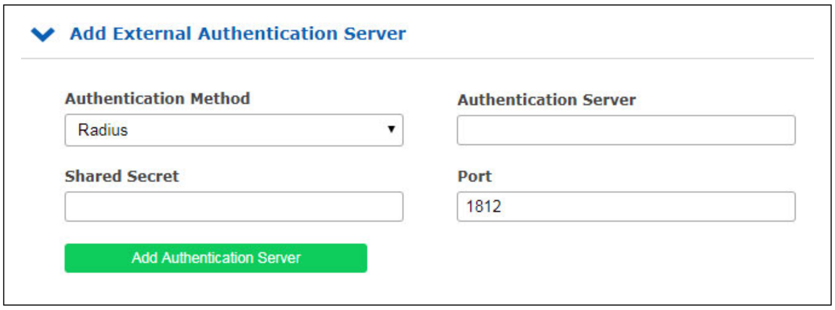
Terminal Access Controller Acc-Control System is a remote authentication protocol that gives the LANTIME the possibility to communicate with a TACACS authentication server.

The LANTIME TACACS authentication requires that each account that should be able to login to the LANTIME has configured an attribute called "priv-lvl". This attribute needs to be configured on the TACACS Server.

For a Super-User account the attribute has to be "100", for an Admin account "200" and for an Info User account "300". In the following an example of a tac_plus server configuration file:

```
# This is the shared secret that clients have to use to access Tacacs+
key = meinberg

# User Groups

group = lantime_super_user {
        service = lantime_mgmt {
                priv-lvl = 100
                }
}

group = lantime_admin_user {
        service = lantime_mgmt {
                priv-lvl = 200
                }
}

group = lantime_info_user {
        service = lantime_mgmt {
                priv-lvl = 300
                }
}

# User

# LANTIME Super User
user = tacacs_su {
        member = lantime_super_user
        pap = cleartext „tacacs_su“ # User Password
}

# LANTIME Admin User
user = tacacs_au {
        member = lantime_admin_user
        pap = cleartext „tacacs_au“ # User Password
}

# LANTIME Info User
user = tacacs_iu {
        member = lantime_info_user
        pap = cleartext „tacacs_iu“ # User Password
}
```

Add External Authentication Server



Add External Authentication Server

Authentication Method: Radius

Authentication Server:

Shared Secret:

Port: 1812

Through this form you can add an external authentication server to the LANTIME configuration. The external authentication has to be enabled first in the "External Authentication Options" menu.

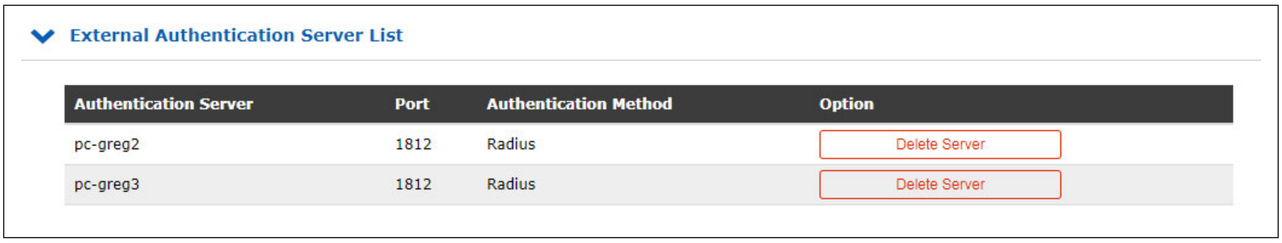
Authentication Method:
Configuration of the authentication method to use, either Radius or TACACS+. More detailed information on both methods can be found in the upper part of this chapter..

Authentication Server:
The IP or Host of the selected Authentication Server (IPv4 and IPv6 are supported).

Shared Secret:
A shared secret is used for a basic authentication between a LANTIME and the authentication server. The shared secret of the external authentication server has to be entered in this field. A list of allowed signs which can be used for the shared secret you can find in the chapter "Before you Start → Text and Syntax Conventions")

Port:
Depending on the authentication method, the default port is already configured here. If needed, the port can be changed.

External Authentication Server List

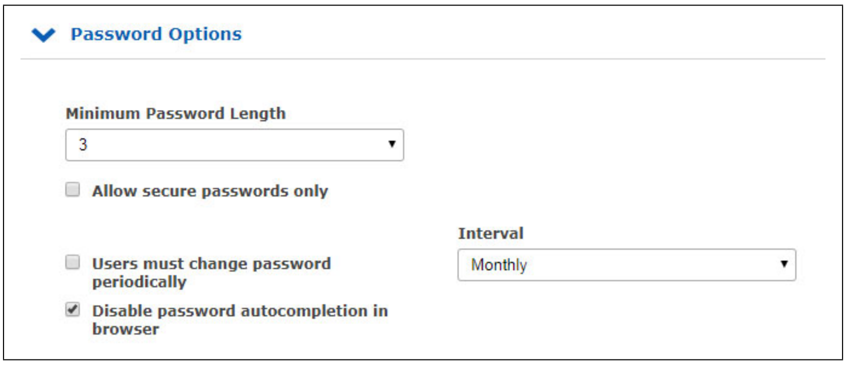


External Authentication Server List

Authentication Server	Port	Authentication Method	Option
pc-greg2	1812	Radius	Delete Server
pc-greg3	1812	Radius	Delete Server

This table gives you a quick overview of the configured authentication servers. Each server can be removed by either a Super- or Admin-User by clicking the "Delete Server" button.

10.1.6.10 Password Options



Password Options

Minimum Password Length: 3

□ Allow secure passwords only

□ Users must change password periodically

Interval: Monthly

☑ Disable password autocompletion in browser

This sub menu provides some general password settings.

Minimum Password Length:
This parameter sets the minimum number of characters of a password before it is accepted by the system as a valid password. This value is used when creating a new user as well as when you change a current user password. Former created passwords are not affected. The maximum length of a password is 64 characters.

Allow secure passwords only:
If this option is activated, only secure passwords will be allowed. A secure password needs at least:

- one lower character [a-z]
- one upper character [A-Z]
- one digit [0-9]
- one special character

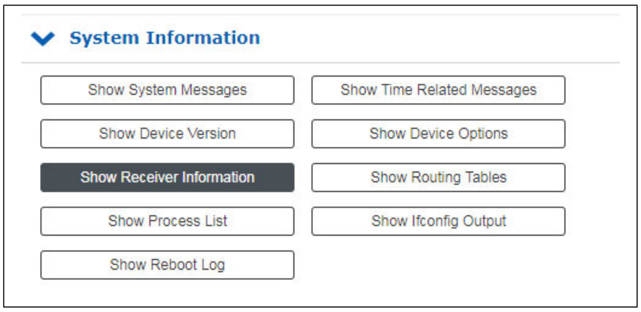
A list of allowed signs which can be used as special characters you can find in the chapter "Before you Start → Text and Syntax Conventions")

Users must change password periodically:
Users will be forced to change passwords at regular intervals. If a password is expired the user can not log in to the unit before changing his current password. Possible intervals:

- Monthly
- Quarterly
- Half-Yearly
- Yearly

Disable password autocompletion in browser:
After this feature is enabled, your browser will not autocomplete the credentials of a LANTIME.

10.1.6.11 System Information



The "System Information" menu offers the possibility to view important log files and setups of the LANTIME.

Show System Messages: Displaying the LANTIME SYSLOG file stored in /var/log/messages

Show Device Version: Displaying the additional device information (model, firmware, serial number, built-in hardware components, etc.)

Show Receiver Information: Displaying the additional status information on the built-in reference clock.

Show Process List: Displaying of all currently running processes.

Show Reboot Log: Displaying the reboot logs stored in /mnt/flash/data/reboot.log. The log file contains information about past system reboots.

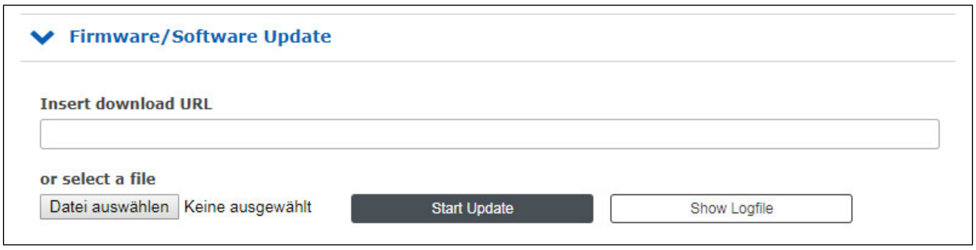
Show Time Related Messages: Displaying the file /var/log/lantime_messages.

Show Device Options: Displaying additional system parameters.

Show Routing Tables: Displaying the network routing table.

Show Ifconfig Output: Displaying information for all network interfaces (output of the command "ifconfig -a")

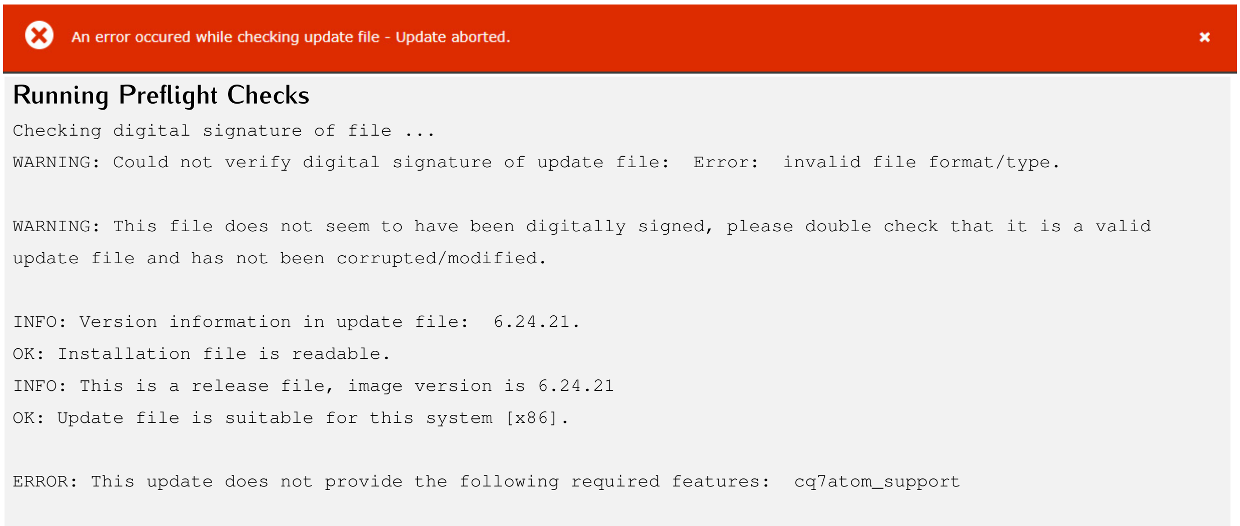
10.1.6.12 Firmware/Software Update



If you need to update the software of your LANTIME, you need a specific update file. You can download the latest LANTIME firmware version from our website: https://www.meinbergglobal.com/english/sw/firmware.htm

The update file can be uploaded to the LANTIME by first choosing the file on your local computer with the "Browse" button and then press "Start Update". Afterwards you are prompted to confirm the start of the update process.

Errors may be detected during installation, such as an unusable update package or a missing signature of the update file. For security reasons, some information is displayed during installation. The following is an excerpt of possible warning or info messages:



An error occured while checking update file - Update aborted.

Running Preflight Checks

```
Checking digital signature of file ...
WARNING: Could not verify digital signature of update file:  Error:  invalid file format/type.

WARNING: This file does not seem to have been digitally signed, please double check that it is a valid
update file and has not been corrupted/modified.

INFO: Version information in update file:  6.24.21.
OK: Installation file is readable.
INFO: This is a release file, image version is 6.24.21
OK: Update file is suitable for this system [x86].

ERROR: This update does not provide the following required features:  cq7atom_support
```

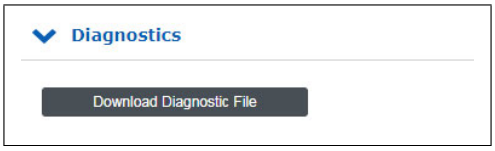
This example shows the attempt to install an update package that does not support the CPU's Q7 processor.

LANTIME - Updates for reference clocks and HPS modules.
Please note that "Refclock Updates" and "HPS100 Firmware Updates" are only feasible on systems running with a LANTIME firmware LTOS > 6.24.013.

On this page you can find the latest firmware update packages:
https://www.meinbergglobal.com/english/sw/refclock-updates.htm

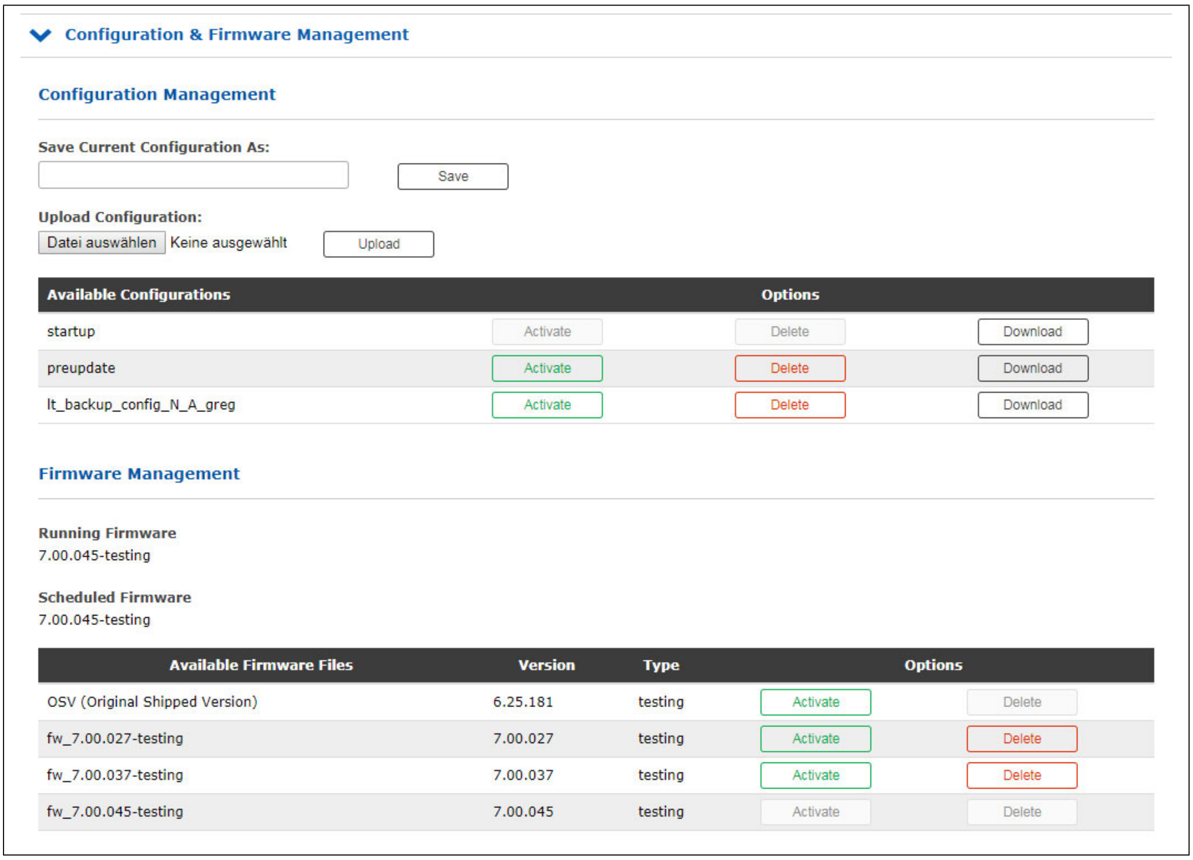
Note: After a successful module update no new firmware version will be displayed in the firmware management. Refclock and HPS100 updates are active immediately after reboot.

10.1.6.13 Download Diagnostic File



A diagnostic file which includes all status data of a LANTIME system logged since the last reboot can be downloaded from all LANTIME servers. The file format of the diagnostic file is a tgz-archive. The archive contains all the important configuration and logfiles. In most support cases it is the first action to ask the user to download the diagnostic file, because it is very helpful to identify the current state of the LANTIME and to find possible errors.

10.1.6.14 Configuration and Firmware Management



Configuration & Firmware Management

Configuration Management

Save Current Configuration As:

Upload Configuration:

Available Configurations	Options		
startup	Activate	Delete	Download
preupdate	Activate	Delete	Download
lt_backup_config_N_A_greg	Activate	Delete	Download

Firmware Management

Running Firmware
7.00.045-testing

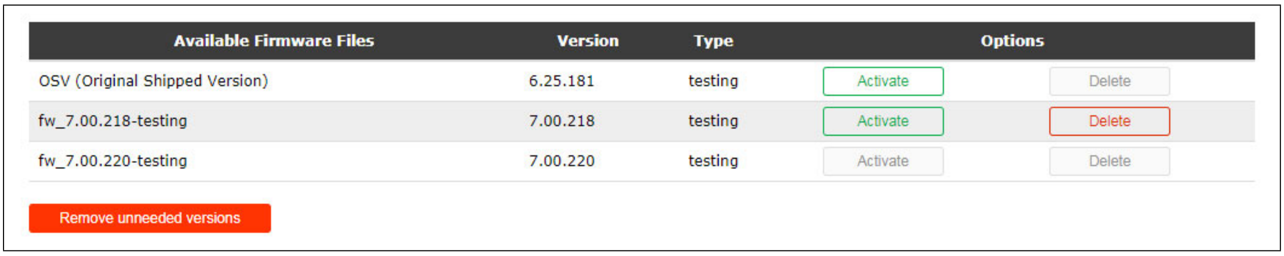
Scheduled Firmware
7.00.045-testing

Available Firmware Files	Version	Type	Options	
OSV (Original Shipped Version)	6.25.181	testing	Activate	Delete
fw_7.00.027-testing	7.00.027	testing	Activate	Delete
fw_7.00.037-testing	7.00.037	testing	Activate	Delete
fw_7.00.045-testing	7.00.045	testing	Activate	Delete

With this menu you can save different configuration files for backup on the flash memory of the LANTIME. By using the "Activate" button a stored configuration can be loaded, the "Delete" button can be used to delete a configuration file and the "Download" button in order to download a file.

Additionally more than one Firmware version can be archived on the LANTIME. If an updated version is not corresponding correctly in the environment, then it is possible to reactivate one of the established versions again on the LANTIME.

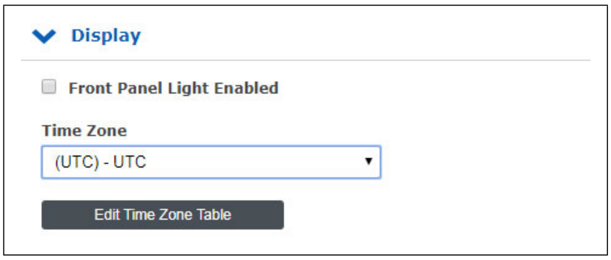
Remove unneeded Versions



Available Firmware Files	Version	Type	Options	
OSV (Original Shipped Version)	6.25.181	testing	Activate	Delete
fw_7.00.218-testing	7.00.218	testing	Activate	Delete
fw_7.00.220-testing	7.00.220	testing	Activate	Delete

With this button all unused firmware versions can be deleted. Only the active firmware and the OSV (Original Shipped Version) remain on the system.

10.1.6.15 Display



Display

☐ Front Panel Light Enabled

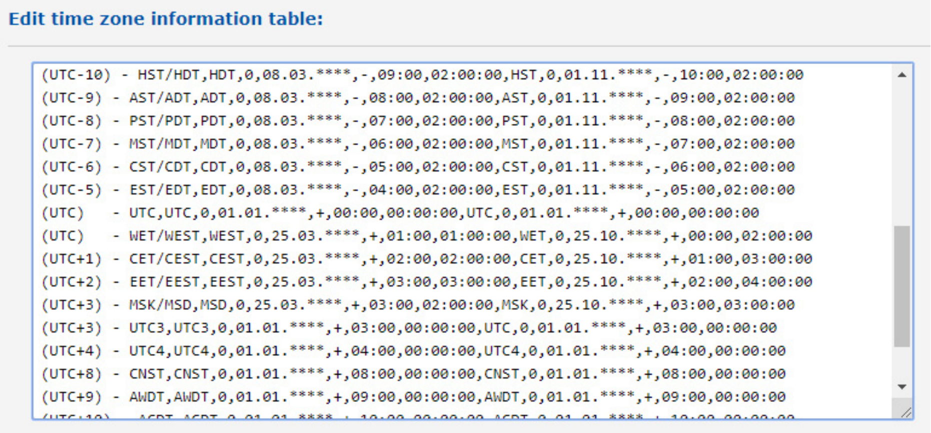
Time Zone: (UTC) - UTC

Front Panel Light Enabled:
Through this checkbox the front panel display light can be switched on permanently.

Time Zone:
Time Zone setting for the front panel display of the LANTIME and the time which is shown in the "Date/Time" section of the Main page in the web interface. Note: This setting does not affect the time which is provided by the LANTIME through NTP, PTP, serial time strings or IRIG.

Exception:
In the case NTP is configured to provide local time instead of UTC you need to configure the exact local time zone here in the display time zone setting. This setting is then used for NTP as well.

Edit Time Zone Table:
The button "Edit Time Zone Table" can be used to add new timezone definitions.



Edit time zone information table:

```
(UTC-10) - HST/HDT,HDT,0,08.03.****,-,09:00,02:00:00,HST,0,01.11.****,-,10:00,02:00:00
(UTC-9) - AST/ADT,ADT,0,08.03.****,-,08:00,02:00:00,AST,0,01.11.****,-,09:00,02:00:00
(UTC-8) - PST/PDT,PDT,0,08.03.****,-,07:00,02:00:00,PST,0,01.11.****,-,08:00,02:00:00
(UTC-7) - MST/MDT,MDT,0,08.03.****,-,06:00,02:00:00,MST,0,01.11.****,-,07:00,02:00:00
(UTC-6) - CST/CDT,CDT,0,08.03.****,-,05:00,02:00:00,CST,0,01.11.****,-,06:00,02:00:00
(UTC-5) - EST/EDT,EDT,0,08.03.****,-,04:00,02:00:00,EST,0,01.11.****,-,05:00,02:00:00
(UTC)   - UTC,UTC,0,01.01.****,+,00:00,00:00:00,UTC,0,01.01.****,+,00:00,00:00:00
(UTC)   - WET/WEST,WEST,0,25.03.****,+,01:00,01:00:00,WET,0,25.10.****,+,00:00,02:00:00
(UTC+1) - CET/CEST,CEST,0,25.03.****,+,02:00,02:00:00,CET,0,25.10.****,+,01:00,03:00:00
(UTC+2) - EET/EEST,EEST,0,25.03.****,+,03:00,03:00:00,EET,0,25.10.****,+,02:00,04:00:00
(UTC+3) - MSK/MSD,MSD,0,25.03.****,+,03:00,02:00:00,MSK,0,25.10.****,+,03:00,03:00:00
(UTC+3) - UTC3,UTC3,0,01.01.****,+,03:00,00:00:00,UTC,0,01.01.****,+,03:00,00:00:00
(UTC+4) - UTC4,UTC4,0,01.01.****,+,04:00,00:00:00,UTC4,0,01.01.****,+,04:00,00:00:00
(UTC+8) - CNST,CNST,0,01.01.****,+,08:00,00:00:00,CNST,0,01.01.****,+,08:00,00:00:00
(UTC+9) - AWDT,AWDT,0,01.01.****,+,09:00,00:00:00,AWDT,0,01.01.****,+,09:00,00:00:00
(UTC+10) - ACDT,ACDT,0,01.01.****,+,10:00,00:00:00,ACDT,0,01.01.****,+,10:00,00:00:00
```

Example:

```
(UTC+1) - CET/CEST,CEST,0,25.03.****,+,02:00,02:00:00,CET,0,25.10.****,+,01:00,03:00:00
```

The string above is the time zone definition for middle Europe. If you require a new time zone setting, this needs to be configured in the same format. The string contains different information, each information is separated by a comma. A detailed description of different string parts shown by an example of the time zone setting for middle Europe is as follows:

1. Field: Display name of the time zone. This name is shown in the list of available time zones → (UTC+1) - CET/CEST

2. Field: Abbreviation of time zone with daylight saving (max 4 letter) → CEST

3. Field: Day of week of changeover to daylight saving time → 0 (Sunday)

4. Field: Date of changeover to daylight saving time (dd.mm.****) →
25.03.**** (Changeover will take place at the first Sunday starting from 25.03.)

5. Field: Sign (+ or -) Add or subtract offset from UTC → +

6. Field: UTC Offset daylight saving (hh:mm) → 02:00

7. Field: Time of changeover → 02:00

8. Field: Abbreviation of standard time zone → CET

9. Field: Day of week of changeover to standard time → 0 (Sunday)

10. Field: Date of changeover to standard time (dd.mm.****) →
25.10.**** (Changeover to standard time will take place at the first Sunday starting from 25.10.)

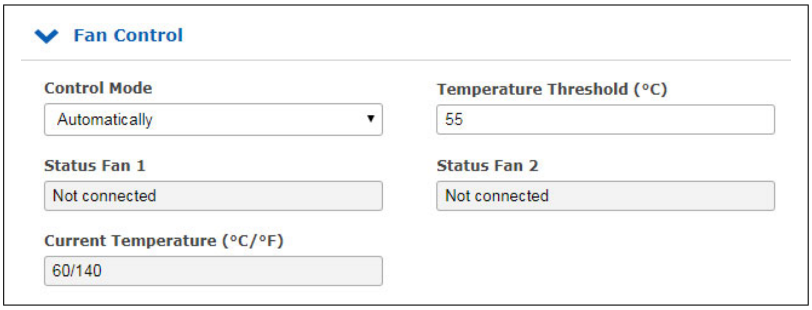
11. Field: Sign (+ or -) Add or subtract offset from UTC → +

12. Field: UTC offset (hh:mm) → 01:00

13. Field: Time of changeover → 03:00

10.1.6.16 Fan Control

These parameters are only available on LANTIME IMS devices with a built-in fan module.



Fan Control

Control Mode: Automatically

Temperature Threshold (°C): 55

Status Fan 1: Not connected

Status Fan 2: Not connected

Current Temperature (°C/°F): 60/140

Control Mode: Setting of the operating mode. The following options are available:

Automatically: With this mode, the fans switch on automatically as soon as the current system temperature exceeds the configured temperature threshold.

On: In this mode the fans run permanently.
Off: In this mode the fans are permanently turned off .

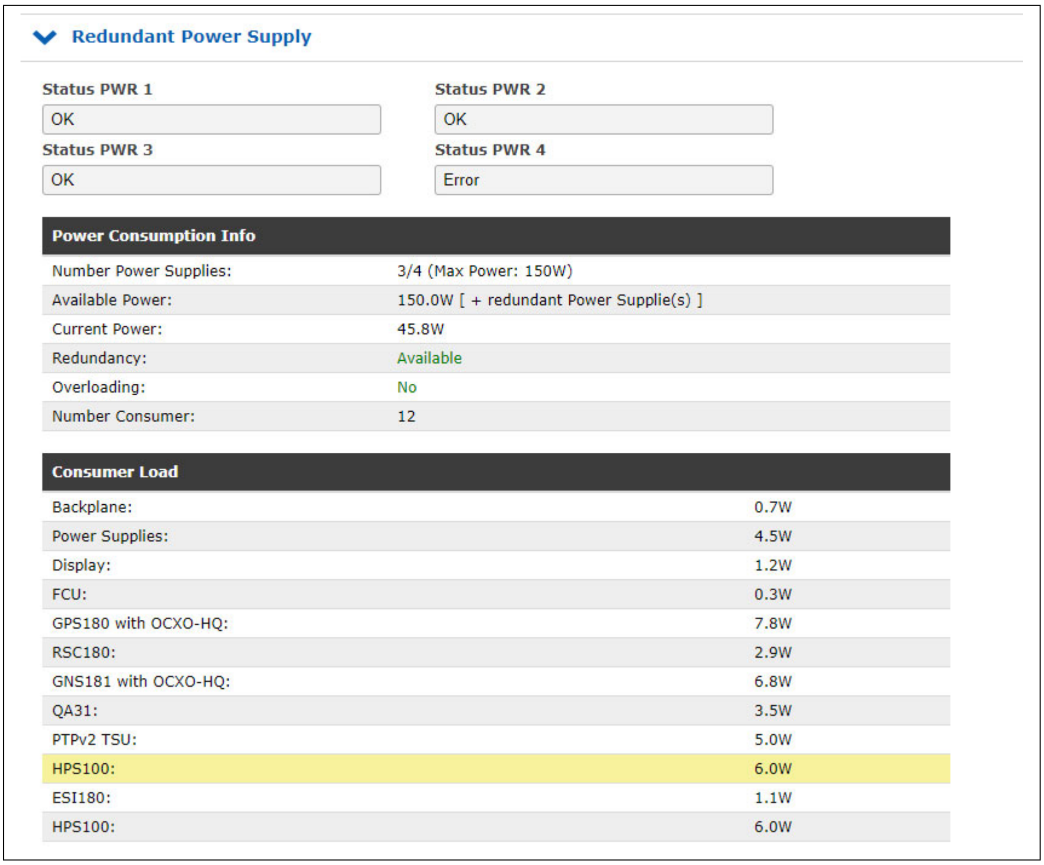
Temperature Threshold (C°): Specification of the system temperature threshold in degrees Celsius. The configured temperature value is taken into account for control of fans when the fan mode "Automatically" is selected.

Status Fan 1: Status display of the 1st fan.
Status Fan 2: Status display of the 2nd fan.

Current Temperature (°/°F): Displaying the current temperature in degrees Celsius and Fahrenheit.

10.1.6.17 Redundant Power Supply

If your LANTIME is an IMS system, all available power supplies and power consumer are displayed and evaluated in this submenu.



Redundant Power Supply

Status PWR 1	Status PWR 2
OK	OK
Status PWR 3	Status PWR 4
OK	Error

Power Consumption Info	
Number Power Supplies:	3/4 (Max Power: 150W)
Available Power:	150.0W [+ redundant Power Supplie(s)]
Current Power:	45.8W
Redundancy:	Available
Overloading:	No
Number Consumer:	12

Consumer Load	
Backplane:	0.7W
Power Supplies:	4.5W
Display:	1.2W
FCU:	0.3W
GPS180 with OCXO-HQ:	7.8W
RSC180:	2.9W
GNS181 with OCXO-HQ:	6.8W
QA31:	3.5W
PTPv2 TSU:	5.0W
HPS100:	6.0W
ESI180:	1.1W
HPS100:	6.0W

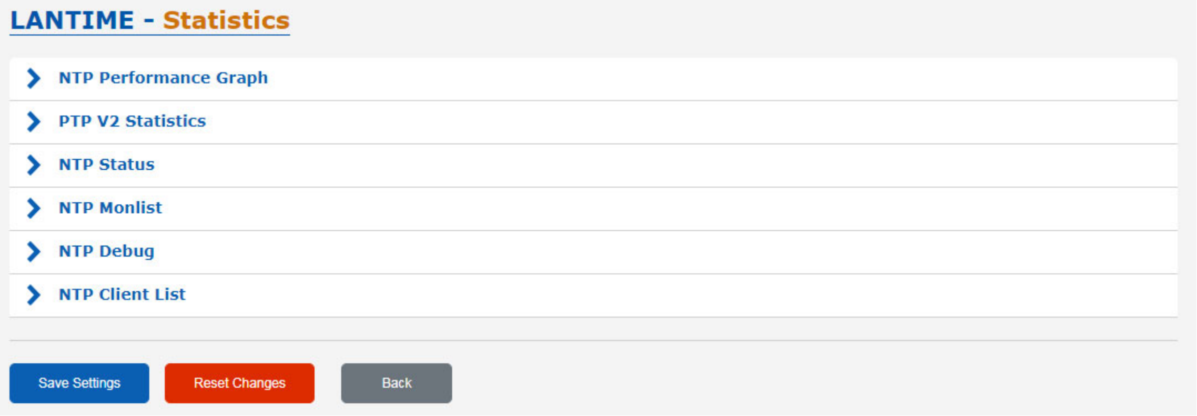
Power Consumption Info
The available power depends on the number of used power supply units. In the example we have three power supply units, each with 50W of power - this results in a total of 150W when all power supply units are in active state.

As long as, as in this example, a value below 50W is displayed in the field "Current Power", only one power supply is sufficient to supply this system. If the value is greater than or equal to 50W, two power supply units are required for supply or three active power supply units are required to ensure redundancy.

The "Redundancy" field is set to "Available" if the "Available Power" minus the "Current Power" is greater than or equal to 50W. The "Overload" field always displays "No" as long as the "Current Power" is less than or equal to "Available Power".

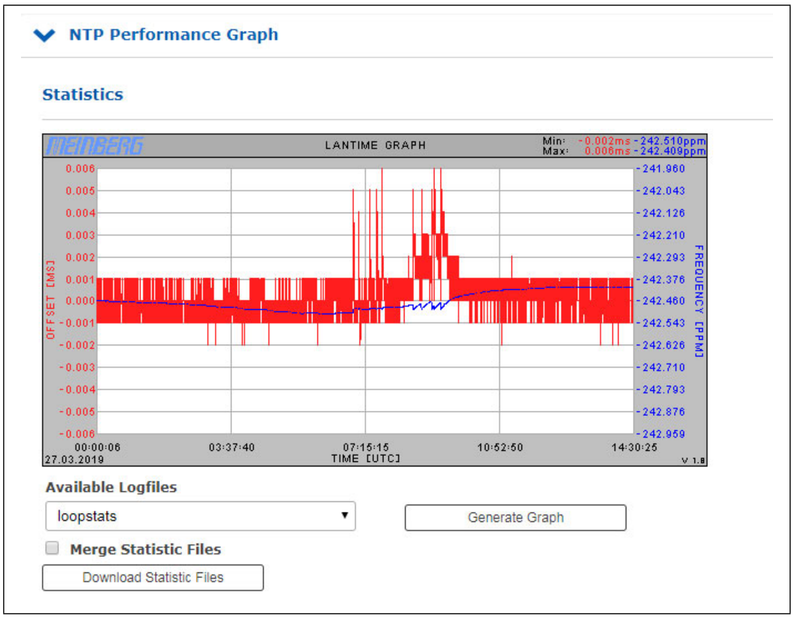
Consumer Load
This table lists all consumers of the system. The backplane, the CPU, the power supplies, the receivers and all other modules used. The sum of all consumers gives the value that is displayed as Current Power.

10.1.7 Statistics



10.1.7.1 NTP Performance Graph

In the submenu NTP performance graph, the NTP statistics (loopstats) are displayed in the form of a graph.



Available Logfiles: loopstats

□ Merge Statistic Files

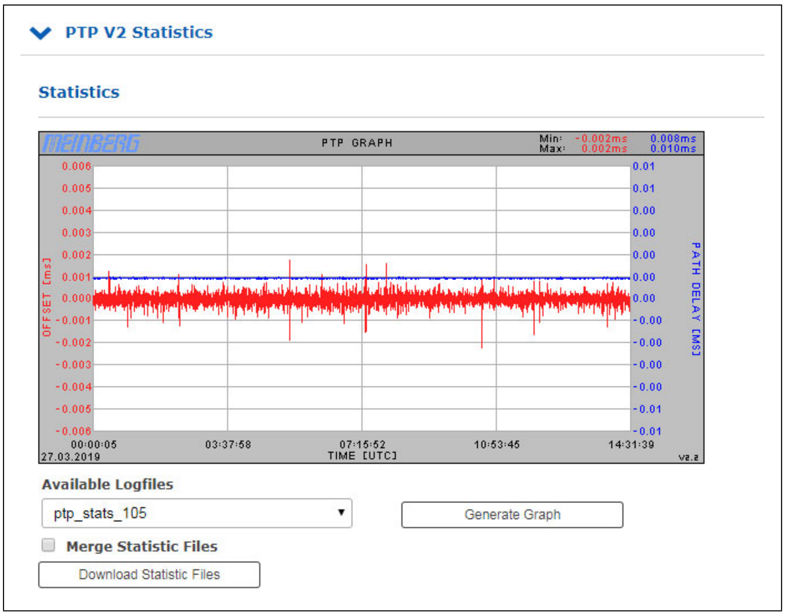
The red lines and the primary Y-axis represent the offset between the system time and the NTP reference time source (in ms). The blue line and the secondary Y-axis, on the other hand, illustrate the frequency adjustment of the oscillator which is built on the CPU by the ntpd (in PPM), to adjust the system time to the reference time source.

The minimum and maximum measured value of the frequency deviation and offsets can be read in the upper right corner.

Available Log Files:
You can select the available log data via the dropdown menu. The ntpd creates a new loopstats file for each day.

Merge Statistic Files:
After activating the checkbox and clicking on "Generate Graph", all available log files are merged and displayed as one graph.

10.1.7.2 PTP V2 Statistics



Available Logfiles: ptp_stats_105 ▾

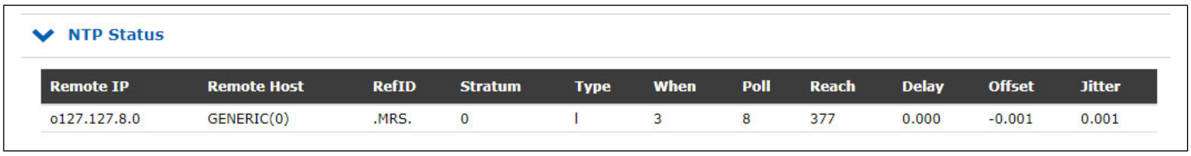
□ Merge Statistic Files

This graphic is only available if the LANTIME is equipped with a PTP module, which is configured as PTP SLAVE.

The red line shows the time offset between the time of the built-in reference clock and the incoming PTP signal (in micro s). The blue line shows the path delay determined by the PTP module.

10.1.7.3 NTP Status

This menu displays the output of the NTP command "ntpq -p". The command lists all reference time sources (peers) that are available to the NTP service. The following example shows the "ntpq -p" output from a LANTIME with a built-in GPS reference clock and 2 configured external NTP time servers:



Remote IP	Remote Host	RefID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
o127.127.8.0	GENERIC(0)	.MRS.	0	l	3	8	377	0.000	-0.001	0.001

Remote IP:
IP address of the NTP peer or 127.127.x.x if it is a hardware time reference, e.g. a radio clock or a GPS receiver.

A legend of codes standing next to each IP address of NTP peers is the following:

'*' This server is selected for synchronization.
'o' The system synchronization is derived from a pulse-per-second (PPS) signal, either indirectly via the PPS reference clock driver or directly via a kernel interface.
'+' The peer is a candidate for synchronization.
'-' The server is not suitable for synchronization.
'x' The server is detected as a falseticker and not suitable for synchronization.
'#' The server is a survivor, but not among the first six servers.
' ' The peer is discarded as unreachable or synchronized to this server (sync loop).

Remote Host:
Resolved DNS name

RefID:
The time reference of the NTP peer.

Stratum:
Stratum value of the NTP peer.

Type:
Type of the NTP Peer:

l:	local reference clock
b:	broadcast or multicast
u:	unicast
s:	symmetric peer
a:	manycast

When:
Value in seconds. Indicates when the NTP peer was last queried.

Poll:
Period in seconds. Specifies the interval at which the NTP peer is queried.

Reach:
Octal value. Indicates the status of the last 8 queries. The value "377" means that the last 8 queries were successful.

Delay:
Value in ms. Displays the runtime of the NTP packet.

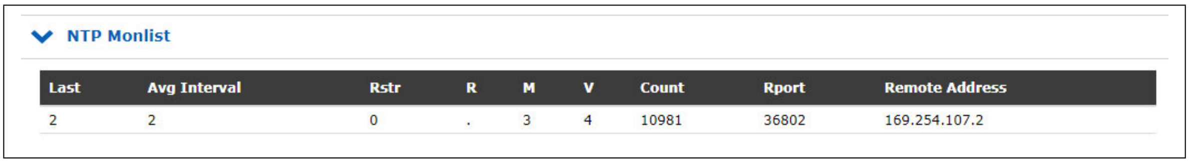
Offset:
The NTP software compares its own system time at regular intervals with its reference time sources. This process is called "polling". After each polling operation, the packet trip time is determined, calculated, and the current time difference ("offset") is calculated and displayed in milliseconds.

Jitter:
The packet trip time changes more or less depending on the characteristics of the network during the "polling" of external NTP sources at each time comparison, and the calculated time offset also varies. For this reason, the results of successive time comparisons are filtered by calculating weighted mean values for packet run time and time offset. The deviations of the individual values from these mean values are referred to as "jitter", and the higher the jitter value, the less accurate is the calculated time offset. On the other hand, a steadily increasing mean time offset indicates that the system time drifts away from the reference time. The value is displayed in milliseconds.

10.1.7.4 NTP Monlist

The submenu "NTP Monlist" lists all NTP clients which have queried the LANTIME time via NTP. The list is created and displayed using the NTP Query Tool. The following ntpq command is issued: ntpq -c mrulist

More information about the NTP Query Tool can be found in the NTP documentation at
http://doc.ntp.org/current-stable/ntpq.html



Last	Avg Interval	Rstr	R	M	V	Count	Rport	Remote Address
2	2	0	.	3	4	10981	36802	169.254.107.2

Last:
Time in seconds. Specifies when the client requested the time from the LANTIME.

Avg Interval:
Interval: Average time in seconds between two NTP requests.

Rstr:
Shows if there are active Restrict Flags for this remote IP.

R:
Indicates whether the "Rate Control" is active or not.

M:
NTP package identification
0 → reserved
1 → symmetric active
2 → symmetric passive
3 → client
4 → server
5 → broadcast
6 → NTP control message
7 → reserved

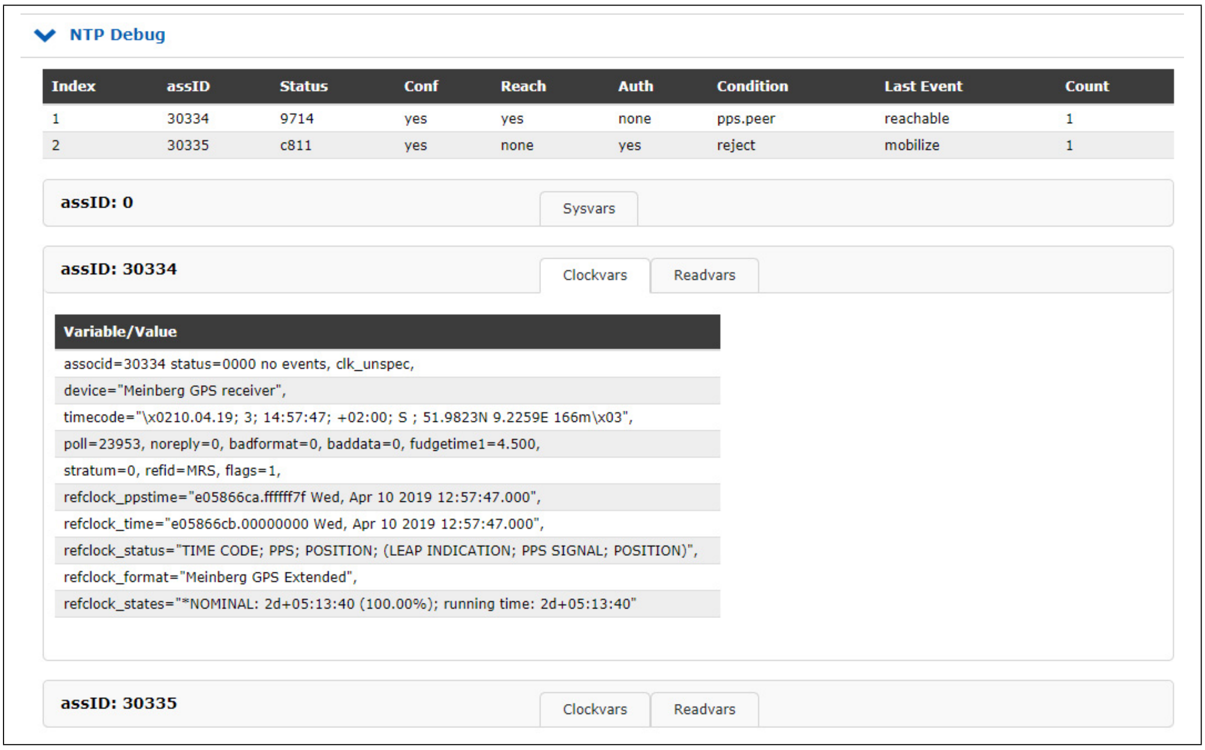
V:
NTP Version

Count:
Number of packets received from the remote address

Rport:
"Source Port" of the last received packet

Remote Address:
IP Address of the requesting device

10.1.7.5 NTP Debug



Index	assID	Status	Conf	Reach	Auth	Condition	Last Event	Count
1	30334	9714	yes	yes	none	pps.peer	reachable	1
2	30335	c811	yes	none	yes	reject	mobilize	1

Variable/Value
associd=30334 status=0000 no events, clk_unspec,
device="Meinberg GPS receiver",
timecode="\x0210.04.19; 3; 14:57:47; +02:00; S ; 51.9823N 9.2259E 166m\x03",
poll=23953, noreply=0, badformat=0, baddata=0, fudgetime1=4.500,
stratum=0, refid=MRS, flags=1,
refclock_ppstime="e05866ca.ffffff7f Wed, Apr 10 2019 12:57:47.000",
refclock_time="e05866cb.00000000 Wed, Apr 10 2019 12:57:47.000",
refclock_status="TIME CODE; PPS; POSITION; (LEAP INDICATION; PPS SIGNAL; POSITION)",
refclock_format="Meinberg GPS Extended",
refclock_states="*NOMINAL: 2d+05:13:40 (100.00%); running time: 2d+05:13:40"

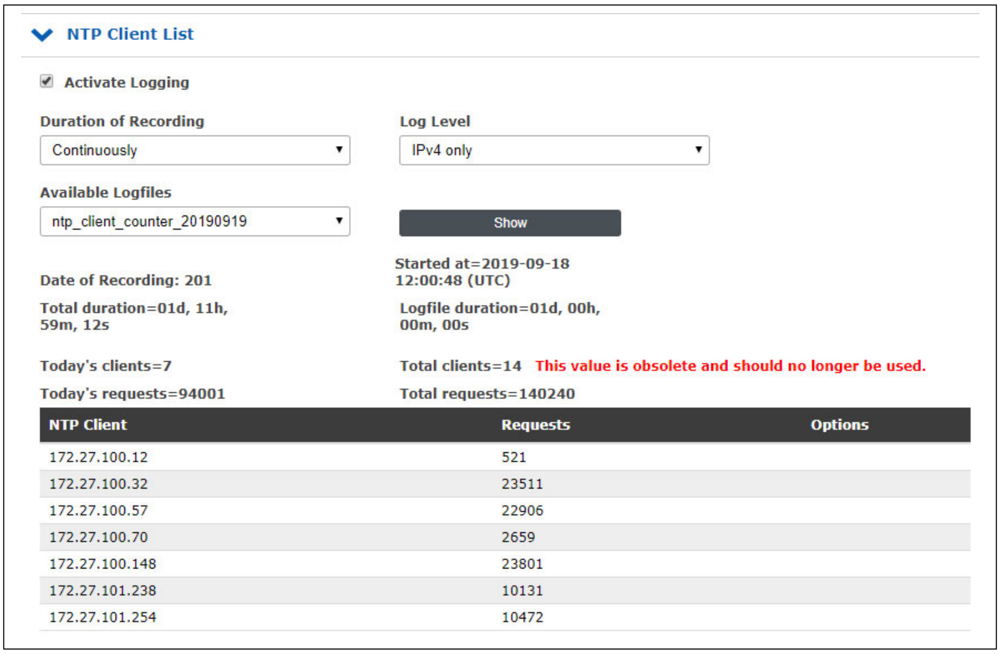
The NTP Debug submenu displays NTP debug information queried by the LANTIME using the NTP Query Tool (ntpq). The "ntpq" is executed with the following parameters:

- "clockvar"
- "associations"
- "readvar"

More information about the query tool can be found in the NTP documentation at
http://doc.ntp.org/current-stable/ntpq.html

10.1.7.6 NTP Client List

In addition to the native NTP logging functions, the LANTIME offers the possibility to maintain a list of all NTP clients. The function is switched off by default, and can be activated if desired.



NTP Client List

☑ Activate Logging

Duration of Recording: Continuously

Log Level: IPv4 only

Available Logfiles: ntp_client_counter_20190919

Show

Date of Recording: 201

Started at=2019-09-18 12:00:48 (UTC)

Total duration=01d, 11h, 59m, 12s

Logfile duration=01d, 00h, 00m, 00s

Today's clients=7

Total clients=14 This value is obsolete and should no longer be used.

Today's requests=94001

Total requests=140240

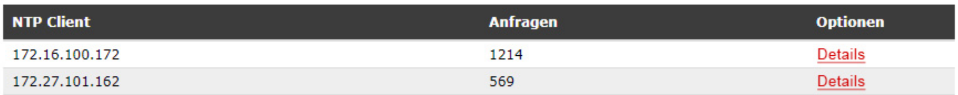
NTP Client	Requests	Options
172.27.100.12	521	
172.27.100.32	23511	
172.27.100.57	22906	
172.27.100.70	2659	
172.27.100.148	23801	
172.27.101.238	10131	
172.27.101.254	10472	

Activate Logging:
Activates the feature on the LANTIME.

Duration of Recording:
The duration for which the LANTIME maintains the client list. When configuring continuous recording, old daily statistics are automatically cleared after a few days in order to save space.

Log Level:
Determines which version of the IP protocol is taken into account. Available are IPv4, IPv6 or both versions in combination.

Available Log Files:
If the client logging is activated, log files for display are provided at this point. Select the desired daily statistics from the selection box and use the "Show" button to display the statistics. You will then receive a list of clients as well as other statistics.

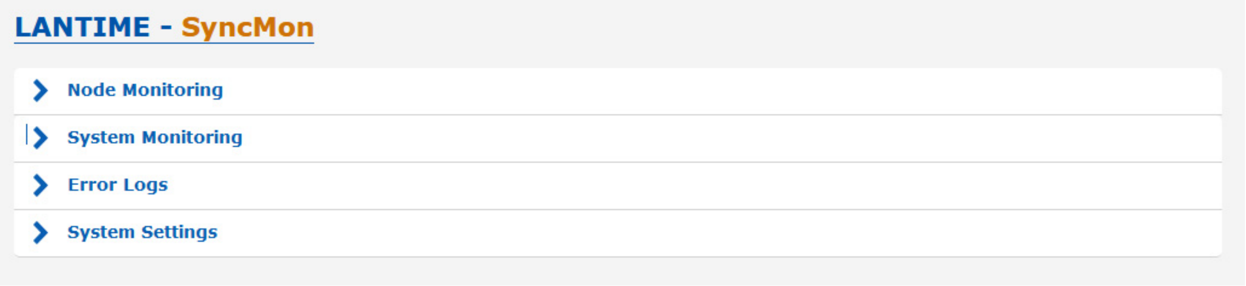


NTP Client	Anfragen	Optionen
172.16.100.172	1214	Details
172.27.101.162	569	Details

A click on Details will now also show you detailed information about the received NTP packets of a particular client.

- Columns 0-23 indicate the hour of the day.
- The 3 additional lines provide information on whether the received NTP packet had mode 3, 4, or another. Modus 3, 4 oder einen anderen hatte.
- Modus 3 → Client
- Modus 4 → Server

10.1.8 Sync Monitoring


LANTIME - SyncMon

Node Monitoring

System Monitoring

Error Logs

System Settings

Figure: Sync Monitor dialog in the LANTIME Web GUI.

10.1.8.1 Sync Monitoring Introduction

The Sync Monitoring feature is used for measuring, monitoring and reporting of network nodes' accuracy against a UTC traceable source (eg. GPS, multi-GNSS or national timing service, e.g. NPL). The Sync Monitoring node can monitor nodes synchronized by network protocols PTP (IEEE 1588v2) or NTP (RFC1305).

PTP nodes need to support the Meinberg TLV approach or standard PTPv2 Management messages, otherwise they cannot be monitored. NTP nodes can only be monitored if they are configured to respond to NTP client requests (Note: A NTP client that is using the Windows Time Service W32Time does not respond to NTP client requests per default configuration. W32Time needs to configured to act as client and server at the same time. Otherwise the node cannot be monitored via SyncMon).

However, also all configured MRS, FDM, PIO and ESI inputs (like PPS and Freq inputs) can be monitored if an ESI (Extension Signal Input) card is available. The Sync Monitor feature is now available on Meinberg IMS Systems with firmware version 7.00 or later and for PTP monitoring with integrated HPS-100 PTP card with a minimum 1024 client performance license.

The Sync Monitor can run either as a node independent from a master clock. In this case a Sync Monitor node can be located basically anywhere in the network; but most probably as close as possible to the slaves to be able to measure their actual accuracy. At the same time you can monitor also the performance of a GM and measure the potential network asymmetry which is present in the link between a GM and the Sync Monitoring Node.

It is possible to configure up to 1000 nodes for monitoring in the Sync Monitoring interface running on a standard LANTIME or IMS System. You can specify monitoring and logging intervals for each individual node separately. Besides, an offset limit can be configured for each node which triggers an alarm notification (via SNMP, email or a user defined channel) if the limit for this particular node is exceeded. For NTP nodes you can define also a stratum limit, which can also trigger an alarming when the defined limit is exceeded.

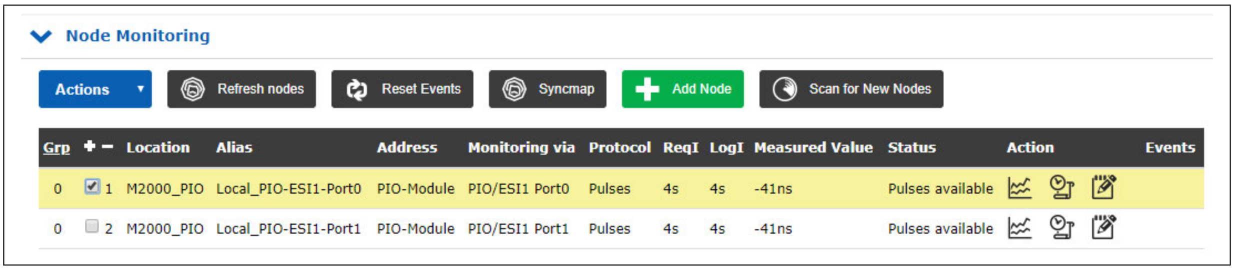
Moreover, for each node it is possible to download all the monitoring data and its log files which can be used to generate a report or for further statistical analysis. Data of each monitored node can be sent online via SYSLOG protocol with different formats or activate an "rsync" service to copy measured data to external data server. Online Data of each node can be read via WEB service like *"curl"* or *"wget"* in JSON format to use current data in other management systems.

A JSON file for each node is available under: */www/htdocs/syncmon/[alias].json* where [alias] is a placeholder for the Node-Alias.

10.1.8.2 Sync Monitor first steps

When SyncMon is started for the first time, there is no monitoring activated. To activate monitoring at least one node has to be added. Press the button "**Add Node**" to add a new monitoring node.

10.1.8.3 Sync Monitor Status and Configuration via WEB Interface



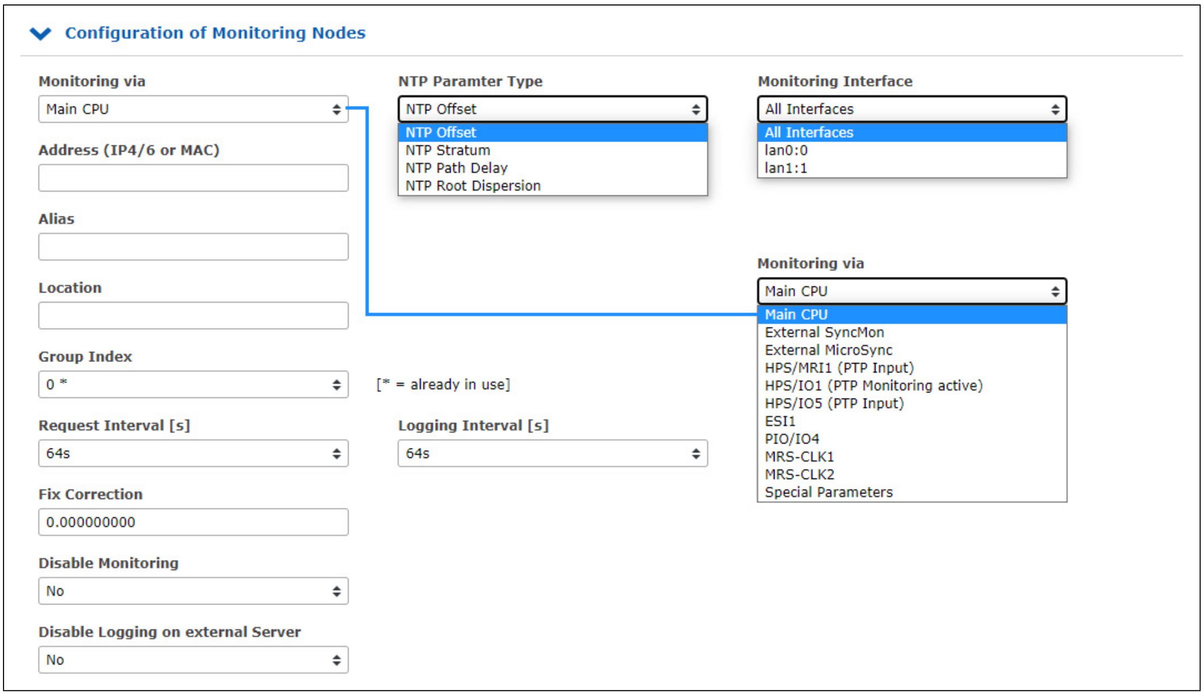
Grp	+ −	Location	Alias	Address	Monitoring via	Protocol	ReqI	LogI	Measured Value	Status	Action	Events
0	☑ 1	M2000_PIO	Local_PIO-ESI1-Port0	PIO-Module	PIO/ESI1 Port0	Pulses	4s	4s	-41ns	Pulses available		
0	□ 2	M2000_PIO	Local_PIO-ESI1-Port1	PIO-Module	PIO/ESI1 Port1	Pulses	4s	4s	-41ns	Pulses available		

Figure: Sync Monitor user interface on LANTIME systems with a FW 7.00 or later.

The "Node Monitoring" will show the current status and configuration of all monitored nodes. A monitoring node can be either a device in the network like NTP servers or PTP devices or an Lantime specific input module for e.g. Pulses or frequencies. Each line in the table represent a monitored node or a group of nodes. The table can be displayed in flat or group mode. In flat mode only nodes will be displayed in a line. To structure the table the group mode can be selected by clicking the "**Grp**" button in the first column – all nodes with the same number are grouped and can be opened separately.

The status on the WEB interface will be updated automatically every 10s. In the Sync Monitor Status and Configuration dialogue you can add new members for measuring their accuracy and monitoring their sync performance. By selecting a "**+ Add Node**" button you will proceed to an enter configuration dialog in order to add a new node for monitoring.

"Refresh Nodes" Button:
This can be used to get an overview of the current values just at that moment even if the request interval is higher. All configured nodes will be refreshed. A new measurement will be done and status in table of nodes will be updated. The refreshed value will be added to the list of measured values to calculate the median value. No measurement will be done on all HPS cards using PTP.



Configuration of Monitoring Nodes

Monitoring via: Main CPU

Address (IP4/6 or MAC):

Alias:

Location:

Group Index: 0 * [* = already in use]

Request Interval [s]: 64s

Logging Interval [s]: 64s

Fix Correction: 0.000000000

Disable Monitoring: No

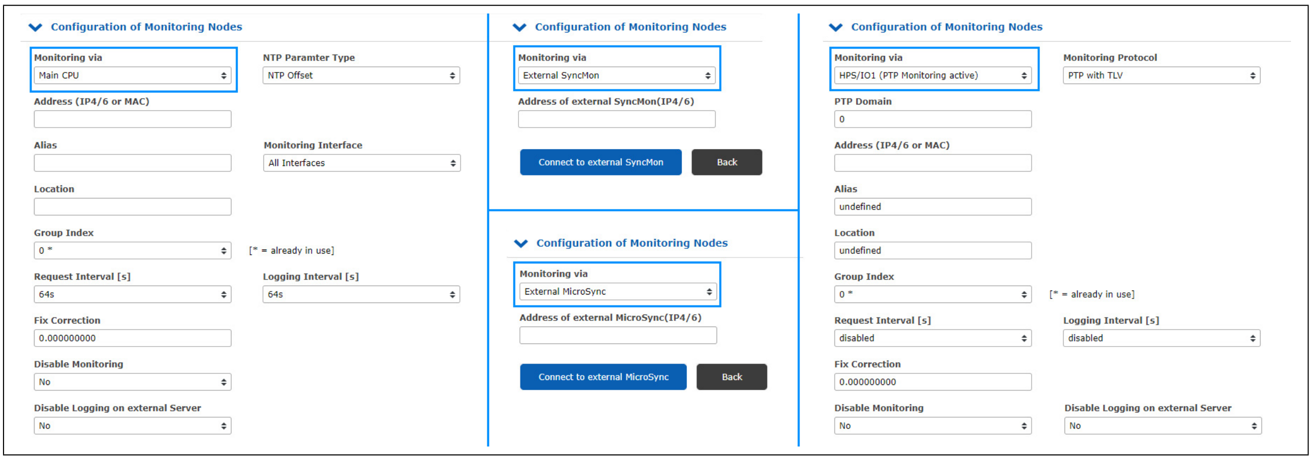
Disable Logging on external Server: No

NTP Paramter Type: NTP Offset

Monitoring Interface: All Interfaces

Figure: Add Node configuration dialog.

The features in the "Add Node" configuration dialog depend on the input selection of the first parameter "Monitoring via" and offer different input masks with different options:



Configuration of Monitoring Nodes

Monitoring via: Main CPU

NTP Paramter Type: NTP Offset

Address (IP4/6 or MAC):

Alias:

Monitoring Interface: All Interfaces

Location:

Group Index: 0 * [* = already in use]

Request Interval [s]: 64s

Logging Interval [s]: 64s

Fix Correction: 0.000000000

Disable Monitoring: No

Disable Logging on external Server: No

Configuration of Monitoring Nodes

Monitoring via: External SyncMon

Address of external SyncMon(IP4/6):

Configuration of Monitoring Nodes

Monitoring via: External MicroSync

Address of external MicroSync(IP4/6):

Configuration of Monitoring Nodes

Monitoring via: HPS/IO1 (PTP Monitoring active)

Monitoring Protocol: PTP with TLV

PTP Domain: 0

Address (IP4/6 or MAC):

Alias: undefined

Location: undefined

Group Index: 0 * [* = already in use]

Request Interval [s]: disabled

Logging Interval [s]: disabled

Fix Correction: 0.000000000

Disable Monitoring: No

Disable Logging on external Server: No

Monitoring via:
Select a monitoring instance from the drop down list. The drop down list appears differently in different HW configurations. The following options are available:

Main CPU: This monitoring instance is always available and is not dependent on HW configuration of the LANTIME system. It can monitor native NTP nodes only, which are responding to NTP client requests (Note: A NTP client that is using the Windows Time Service W32Time does not respond to NTP client requests per default configuration. W32Time needs to configured to act as client and server at the same time. Otherwise the node cannot be monitored via SyncMon). All assigned interfaces can be monitored at the same time or you can select a particular interface from a list if available.

The selection box "NTP Parameter Type" can be used to select whether the "NTP Offset", "NTP Stratum", "NTP Path Delay" or "NTP Root Dispersion" should be saved.

If several network interfaces are available, a specific interface or all interfaces can be selected via the "Monitoring Interface" selection box.

External SyncMon: This monitoring instance can monitor nodes and sensors of other Lantime devices with activated SyncMon. When selecting the external SyncMon with IP address a list of available nodes from that external SyncMon will be downloaded. Configuration and data will be transferred via WEB service (curl).

External Microsync: This can be used to monitor MRS references from external MicroSync devices. When selecting the external MicroSync with IP address, a list of available references is downloaded from this external MicroSync. Configuration and data are transferred via the WEB service (Curl).

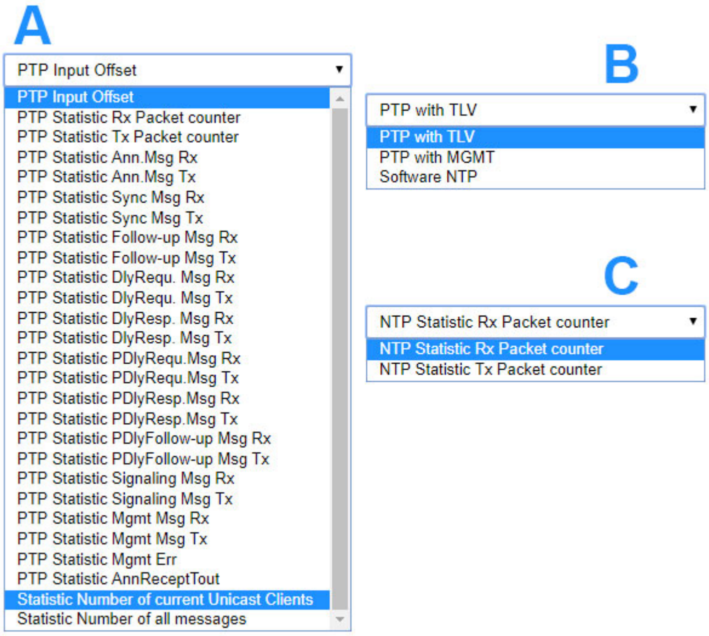
HPS: HPS100 cards can be used for monitoring PTP or NTP on its own network port.

If HPS is configured (see Lantime PTP configuration) as PTP slave then the HPS card will behave like a standard PTP Slave with all its options like Profiles and network specific configurations - but only one PTP Master can be monitored at the same time with the HPS card.

If HPS is configured (see Lantime PTP configuration) as monitoring device (this is only possible if HPS has a 1024 clients license at minimum) then multiple PTP nodes can be monitored with the network port of the HPS card. Then that monitoring instance can monitor PTP nodes, supporting protocols PTP with TLV (proprietary for a Meinberg Sync Node), PTP with MGMT (defined in the IEEE 1588v2 standard) and NTP with software time stamping.

The special protocol "PTP with TLV" is like a reverse PTP: a PTP delay request packet with a special TLV will be send to the PTP device and this will answer with a sync packet and a delay response packet – this method allow measuring the offset from the internal reference to the PTP device even if the PTP device is in Master, Slave or Passive mode.

Statistic Types:


A
PTP Input Offset
PTP Input Offset
PTP Statistic Rx Packet counter
PTP Statistic Tx Packet counter
PTP Statistic Ann.Msg Rx
PTP Statistic Ann.Msg Tx
PTP Statistic Sync Msg Rx
PTP Statistic Sync Msg Tx
PTP Statistic Follow-up Msg Rx
PTP Statistic Follow-up Msg Tx
PTP Statistic DlyRequ. Msg Rx
PTP Statistic DlyRequ. Msg Tx
PTP Statistic DlyResp. Msg Rx
PTP Statistic DlyResp. Msg Tx
PTP Statistic PDlyRequ.Msg Rx
PTP Statistic PDlyRequ.Msg Tx
PTP Statistic PDlyResp.Msg Rx
PTP Statistic PDlyResp.Msg Tx
PTP Statistic PDlyFollow-up Msg Rx
PTP Statistic PDlyFollow-up Msg Tx
PTP Statistic Signaling Msg Rx
PTP Statistic Signaling Msg Tx
PTP Statistic Mgmt Msg Rx
PTP Statistic Mgmt Msg Tx
PTP Statistic Mgmt Err
PTP Statistic AnnReceptTout
Statistic Number of current Unicast Clients
Statistic Number of all messages
B
PTP with TLV
PTP with TLV
PTP with MGMT
Software NTP
C
NTP Statistic Rx Packet counter
NTP Statistic Rx Packet counter
NTP Statistic Tx Packet counter

HPS cards in PTP or NTP mode support packet statistics which can be monitored individualy:

A: HPS in PTPv2 Operating Mode.
B: HPS in Monitoring Mode.
C: HPS in NTP Mode.

ESI: This monitoring instance can monitor PPS and Freq nodes with Extension Signal Input (ESI) card. From a drop down list you can select which particular signal you wish to monitor. Options available are: PPS0, Freq In0, Freq In1, BITS In2.

MRS-CLK: This monitoring instance can monitor all activated MRS input signals for each MRS-reference clock. From a dropdown list you can select which signal you want to monitor. Options available are: GNSS/ GPS, NTP, PTP, PPS, IRIG, 10MHz, E1, 2048kHz, - (depending on HW options (see "Clock" tab in the Web interface).

PIO: This monitoring instance can monitor PPS and Freq nodes with Programmable Input Output (PIO) card. From a drop down list you can select which particular signal you wish to monitor. This depends on the configuration of the PIO card. Options available are: PPS0, PPS1, PPS2, PPS3, Freq In0, Freq In1, Freq In2, Freq In3.

FDM: This monitoring instance can monitor 50/60Hz power line networks nodes with Frequency Deviation Monitor (FDM) card. From a drop down list you can select which particular signal you wish to monitor. Options available are: time deviation or frequency deviation.

Special Parameters:

This monitoring instance can monitor various parameters if they are enabled:

Process Memory:
This can be used to monitor the memory usage of system processes. For this purpose, the name of the process must be specified and the values are displayed in **%**.

ID of selected HPS card:
This option is only offered if a HPS card is active in the system as PTP slave. If several HPS cards are present in the system as PTP slave, then the best card is selected via the internal PTP BMCA (Best Master Clock Algorithm) and used as MRS/PTP reference. With this parameter the selected ID of the card can be monitored.

ID of selected NTP server:
This option is only offered if external NTP servers have been configured in the system.
If several external NTP servers are configured, then the best external NTP server is selected via a special NTP selection procedure and used as MRS/NTP reference. With this parameter the selected ID of the external NTP servers can be monitored.

Address (IP4/6 or MAC):
IPv4 or IPv6 or MAC address of a node you want to monitor over the network. Host names are not allowed.

Alias:
Alias name for a monitoring node to find it easily in the complete table overview. The alias name which is configured by the user will define the name of the directory on flash disc ('Base Path for logfiles for history of days') of each node. The alias name has to be unique and one word without blanks with a maximum length of 63 characters (blanks will be converted to '_' automatically). It is possible to monitor the same node (e.g. the same IP-address) with different alias names – this may be useful if you want to monitor the same node from different monitoring modules (e.g. different HPS100 IMS cards with separate network paths).

Location:
Enter a physical location of a monitoring node for you to recognize this node easily in the complete table. The location name has to be one word without blanks with a maximum length of 63 characters (blanks will be converted to '_' automatically).

Group Index:
You can group monitored nodes within a logical group by assigning them the same index, (e.g. nodes with the same group index may be of the same kind (NTP, PTP, PPS), or at the same location, etc.). Nodes with the same group index will be sorted automatically in the table. The table can be displayed in flat or group mode. In flat mode only nodes will be displayed in a line. To structure the table the group mode can be selected by pressing the "Grp" button on top of the first column – then all nodes with the same group number will be gathered to one line and can be opened separately.

Request Interval (s):
Interval in seconds by which a monitoring node sends monitoring requests to the slaves / clients. The min request interval is 1s, the max is 3600s. A default interval is 64s. If the Request Interval is disabled (0) then no requests will be sent to the nodes and no data will be logged.

Logging Interval (s):
Interval in seconds by which the measured offset and stratum are written to a logfile. If the log-interval is disabled then no data will be stored to the logfile. If the request interval has been activated and the log-interval has been disabled then the nodes will be monitored and limits and notifications will be checked but no data will be stored. If the Request Interval is lower than the Logging Interval then the mean value of the measured offsets at request interval will be logged and the Minimum and Maximum values in the log-interval will be stored additionally.

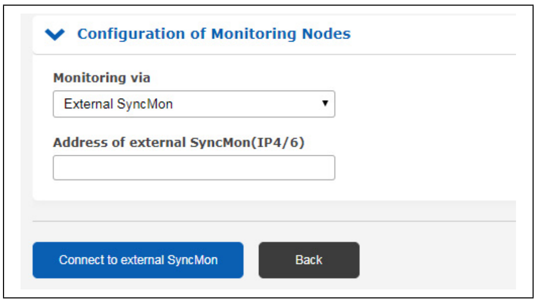
Fix Offset [s]:
A certain offset is known for some network nodes (e.g. network asymmetry). This value serves as a correction value and can be entered here. The "Fix Offset" is always added to the "Measured Value". An entered fixed offset is displayed in the overview with a * in the "Measured Value" column.

Disable Monitoring:
Monitoring can be disabled for each node. If Node has been disabled then no monitoring Data will be send to the Node and no data will be saved.

Disable Logging on external Server:
The measured or logged data can be send via SYSLOG or RSYNC protocol to an external server. This can be disabled for each node (see System settings for external Server Configuration).

10.1.8.4 External SyncMon

"External SyncMon" is a special monitoring instance that can monitor nodes and sensors of other LANTIME devices with activated SyncMon. When selecting the external SyncMon with IP address a list of available nodes from that external SyncMon will be downloaded. Configuration and data will be transferred via WEB service (curl).



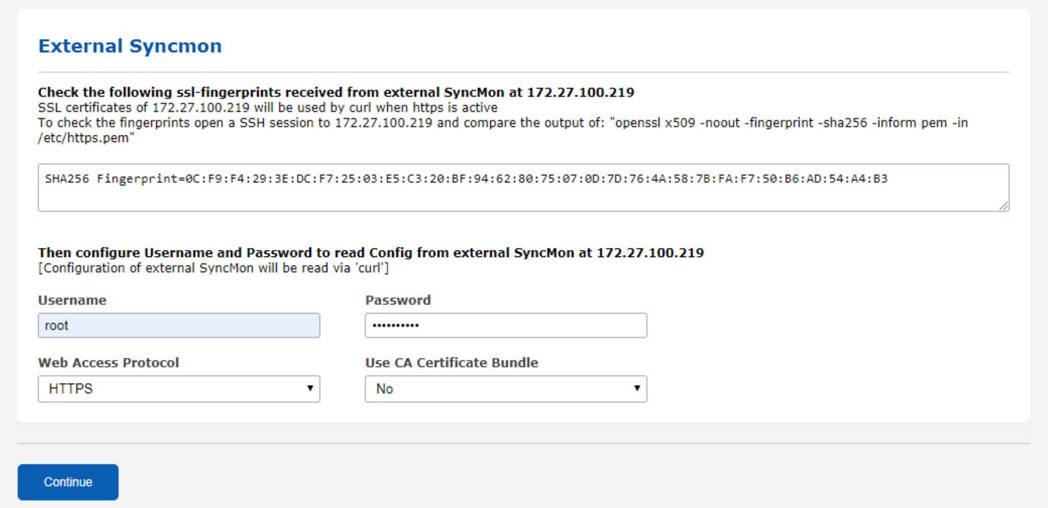
Configuration of Monitoring Nodes

Monitoring via

External SyncMon

Address of external SyncMon(IP4/6)

Press "**Connect to external SyncMon**" will try to connect to the external SyncMon and show the SSL-Fingerprint of that server. Check the following ssl-fingerprints received from external SyncMon. The SSL certificates will be used by curl when https is active. To check the fingerprints open a SSH session on the external SyncMon and compare the output of: "openssl x509 -noout -fingerprint -sha256 -inform pem -in /etc/https.pem". This is to make sure that this is the correct device.



External Syncmon

Check the following ssl-fingerprints received from external SyncMon at 172.27.100.219
SSL certificates of 172.27.100.219 will be used by curl when https is active
To check the fingerprints open a SSH session to 172.27.100.219 and compare the output of: "openssl x509 -noout -fingerprint -sha256 -inform pem -in /etc/https.pem"

```
SHA256 Fingerprint=0C:F9:F4:29:3E:DC:F7:25:03:E5:C3:20:BF:94:62:80:75:07:0D:7D:76:4A:58:7B:FA:F7:50:B6:AD:54:A4:B3
```

Then configure Username and Password to read Config from external SyncMon at 172.27.100.219
[Configuration of external SyncMon will be read via 'curl']

Username: root

Password: ••••••••••

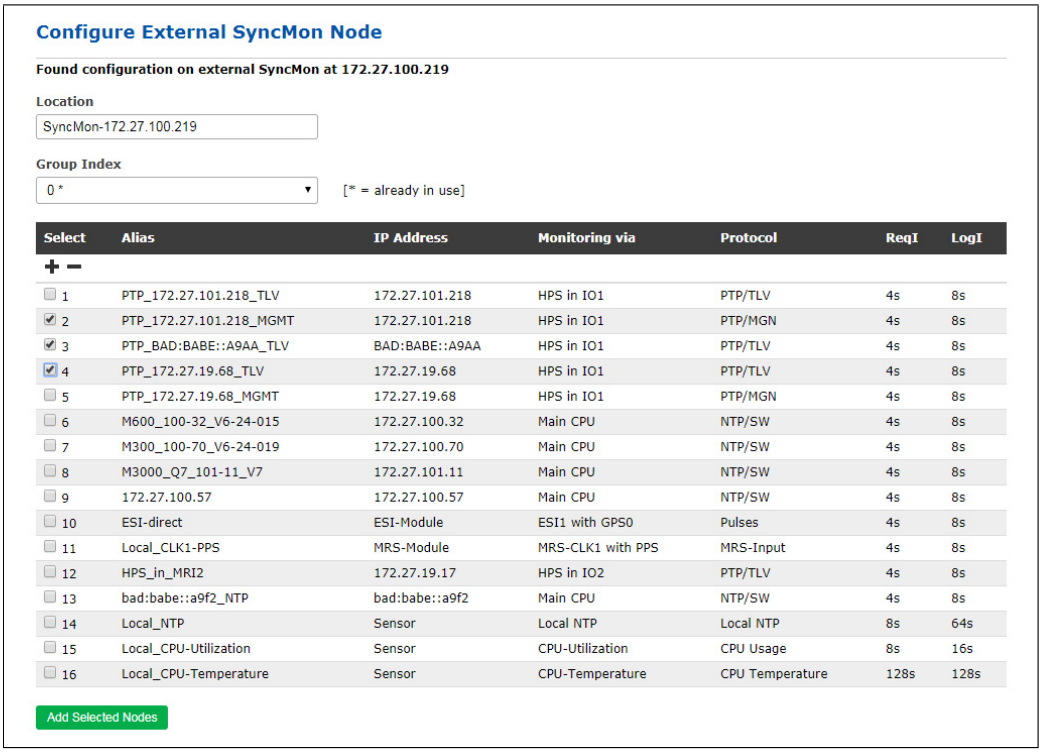
Web Access Protocol: HTTPS

Use CA Certificate Bundle: No

Then enter username and password to read Config from external SyncMon – the current configuration of external SyncMon will be read via *'curl'*. Also you have to configure the WEB access protocol (HTTP or HTTPS) and if you want to use a CA Certificate Bundle to get configuration and measured data from the external SyncMon.

Be aware that if you use HTTPS that all data has to be encrypted and decrypted which costs a lot of CPU-UTILIZATION for each data requesting from the external SyncMon.

Be aware if you want to use HTTP access protocol then you have to activate HTTP network service on the internal and external Lantime. The same is with the HTTPS protocol.



Configure External SyncMon Node

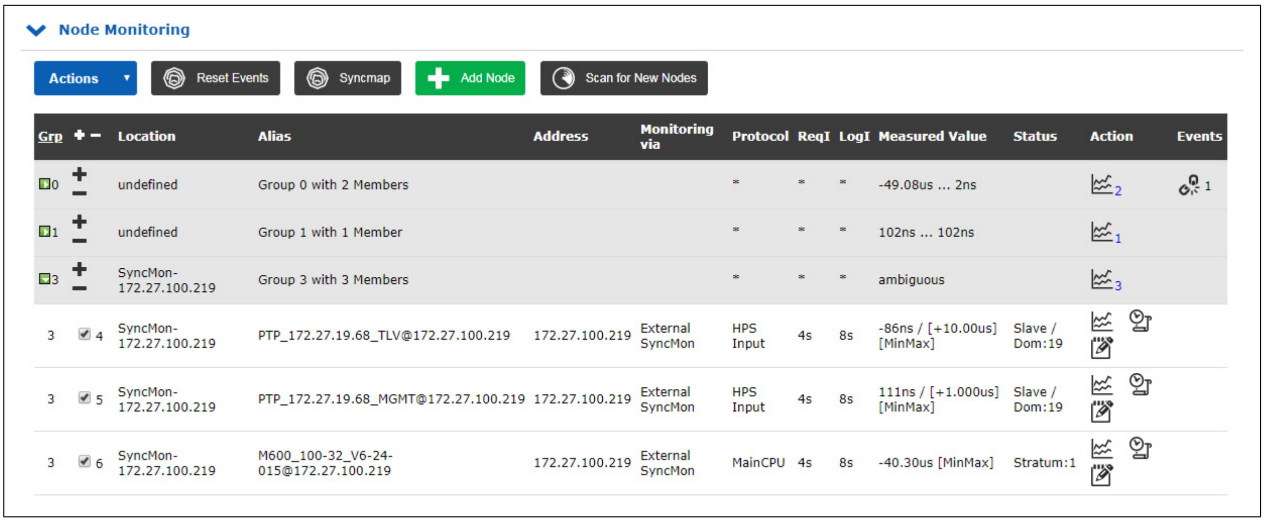
Found configuration on external SyncMon at 172.27.100.219

Location: SyncMon-172.27.100.219

Group Index: 0 * [* = already in use]

Select	Alias	IP Address	Monitoring via	Protocol	ReqI	LogI
☐ 1	PTP_172.27.101.218_TLV	172.27.101.218	HPS in IO1	PTP/TLV	4s	8s
☑ 2	PTP_172.27.101.218_MGMT	172.27.101.218	HPS in IO1	PTP/MGN	4s	8s
☑ 3	PTP_BAD:BABE::A9AA_TLV	BAD:BABE::A9AA	HPS in IO1	PTP/TLV	4s	8s
☑ 4	PTP_172.27.19.68_TLV	172.27.19.68	HPS in IO1	PTP/TLV	4s	8s
☐ 5	PTP_172.27.19.68_MGMT	172.27.19.68	HPS in IO1	PTP/MGN	4s	8s
☐ 6	M600_100-32_V6-24-015	172.27.100.32	Main CPU	NTP/SW	4s	8s
☐ 7	M300_100-70_V6-24-019	172.27.100.70	Main CPU	NTP/SW	4s	8s
☐ 8	M3000_Q7_101-11_V7	172.27.101.11	Main CPU	NTP/SW	4s	8s
☐ 9	172.27.100.57	172.27.100.57	Main CPU	NTP/SW	4s	8s
☐ 10	ESI-direct	ESI-Module	ESI1 with GPS0	Pulses	4s	8s
☐ 11	Local_CLK1-PPS	MRS-Module	MRS-CLK1 with PPS	MRS-Input	4s	8s
☐ 12	HPS_in_MRI2	172.27.19.17	HPS in IO2	PTP/TLV	4s	8s
☐ 13	bad:babe::a9f2_NTP	bad:babe::a9f2	Main CPU	NTP/SW	4s	8s
☐ 14	Local_NTP	Sensor	Local NTP	Local NTP	8s	64s
☐ 15	Local_CPU-Utilization	Sensor	CPU-Utilization	CPU Usage	8s	16s
☐ 16	Local_CPU-Temperature	Sensor	CPU-Temperature	CPU Temperature	128s	128s

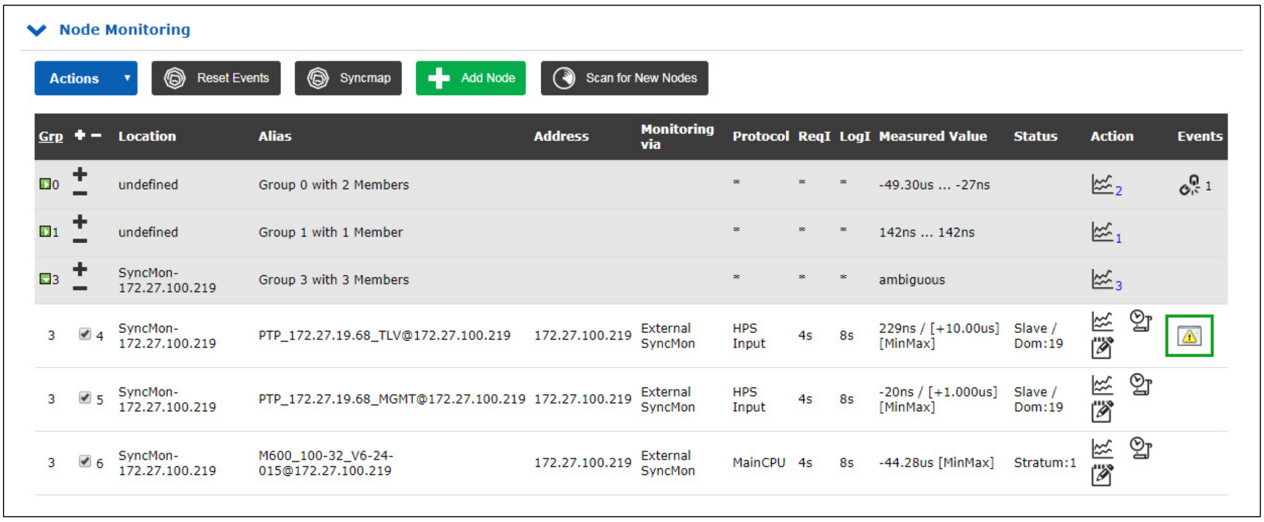
Getting the current configuration from the external SyncMon you have to choose the nodes which you want to monitor of that Lantime. Only nodes will be offered which are not disabled and not disabled for external logging. The parameters for request and log interval will be take over from the external configuration. Location and the Group index can be configured for all selected nodes. The default Location will be "SyncMon-" plus the IP address. The Alias names for the external SyncMon nodes will be the original Alias-name plus "@IP-address". It is recommend to use a non used Group Id for all nodes of an external SyncMon.



Node Monitoring

Grp	+ −	Location	Alias	Address	Monitoring via	Protocol	ReqI	LogI	Measured Value	Status	Action	Events
0	+ −	undefined	Group 0 with 2 Members			*	*	*	-49.08us ... 2ns		2	1
1	+ −	undefined	Group 1 with 1 Member			*	*	*	102ns ... 102ns		1	
3	+ −	SyncMon-172.27.100.219	Group 3 with 3 Members			*	*	*	ambiguous		3	
3	☑ 4	SyncMon-172.27.100.219	PTP_172.27.19.68_TLV@172.27.100.219	172.27.100.219	External SyncMon	HPS Input	4s	8s	-86ns / [+10.00us] [MinMax]	Slave / Dom:19		
3	☑ 5	SyncMon-172.27.100.219	PTP_172.27.19.68_MGMT@172.27.100.219	172.27.100.219	External SyncMon	HPS Input	4s	8s	111ns / [+1.000us] [MinMax]	Slave / Dom:19		
3	☑ 6	SyncMon-172.27.100.219	M600_100-32_V6-24-015@172.27.100.219	172.27.100.219	External SyncMon	MainCPU	4s	8s	-40.30us [MinMax]	Stratum:1		

If changes will be done on that nodes of external SyncMon configuration which will be monitored then a warning sign will be displayed in the main table in the **Event** column for that node. Then you have to change parameters manually for that node.

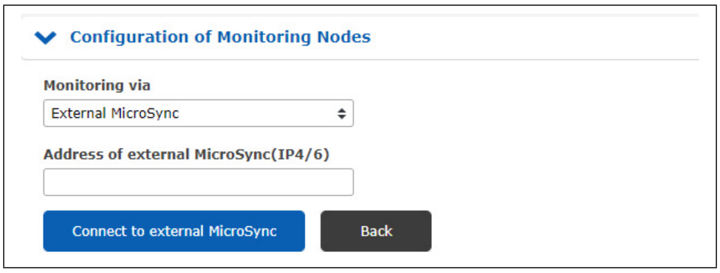


Grp	+ −	Location	Alias	Address	Monitoring via	Protocol	ReqI	LogI	Measured Value	Status	Action	Events
0	+ −	undefined	Group 0 with 2 Members			*	*	*	-49.30us ... -27ns		2	1
1	+ −	undefined	Group 1 with 1 Member			*	*	*	142ns ... 142ns		1	
3	+ −	SyncMon-172.27.100.219	Group 3 with 3 Members			*	*	*	ambiguous		3	
3	☑ 4	SyncMon-172.27.100.219	PTP_172.27.19.68_TLV@172.27.100.219	172.27.100.219	External SyncMon	HPS Input	4s	8s	229ns / [+10.00us] [MinMax]	Slave / Dom:19		⚠
3	☑ 5	SyncMon-172.27.100.219	PTP_172.27.19.68_MGMT@172.27.100.219	172.27.100.219	External SyncMon	HPS Input	4s	8s	-20ns / [+1.000us] [MinMax]	Slave / Dom:19		
3	☑ 6	SyncMon-172.27.100.219	M600_100-32_V6-24-015@172.27.100.219	172.27.100.219	External SyncMon	MainCPU	4s	8s	-44.28us [MinMax]	Stratum:1		

10.1.8.5 External MicroSync

External MicroSync is a special monitoring instance that can monitor MRS references from external MicroSync devices. When selecting the external MicroSync with IP address, a list of available MRS references is downloaded from this external MicroSync.

Configuration and data are transferred via the WEB service (Curl).



Configuration of Monitoring Nodes

Monitoring via: External MicroSync

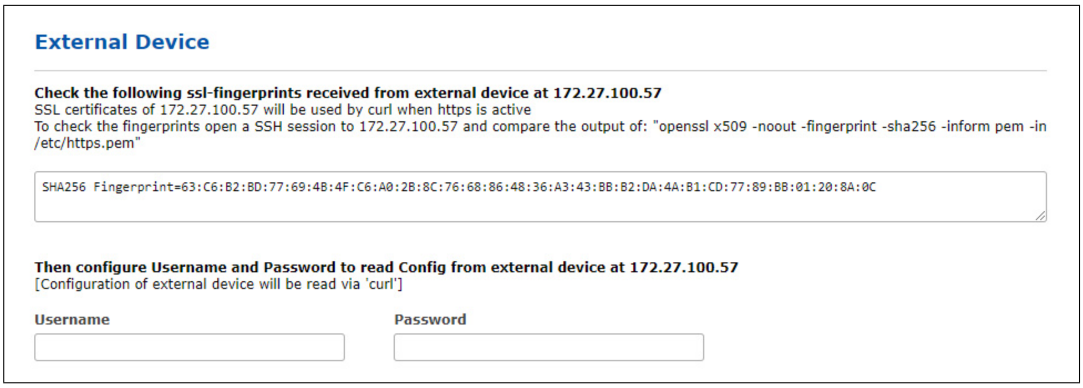
Address of external MicroSync(IP4/6):

Press "Connect to external MicroSync", this will make the system try to connect to the external MicroSync and display the SSL fingerprint of this server. Check the following SSL fingerprints received from external SyncMon. The SSL certificates are used by curl. To verify the fingerprints, open an SSH session on the external MicroSync and compare the output of:

```
openssl x509 -noout -fingerprint -sha256 -inform pem -in /etc/https.pem
```

This ensures that it is the correct device.

Then enter username and password of the MicroSync system to read the configuration from the external MicroSync - the current configuration of the external MicroSync is read via 'curl'. Note that when using HTTPS, all data must be encrypted and decrypted, which causes a lot of CPU usage for each data request to the external MicroSync system.



External Device

Check the following ssl-fingerprints received from external device at 172.27.100.57
SSL certificates of 172.27.100.57 will be used by curl when https is active
To check the fingerprints open a SSH session to 172.27.100.57 and compare the output of: "openssl x509 -noout -fingerprint -sha256 -inform pem -in /etc/https.pem"

```
SHA256 Fingerprint=63:C6:B2:BD:77:69:4B:4F:C6:A0:2B:8C:76:68:86:48:36:A3:43:BB:B2:DA:4A:B1:CD:77:89:BB:01:20:8A:0C
```

Then configure Username and Password to read Config from external device at 172.27.100.57
[Configuration of external device will be read via 'curl']

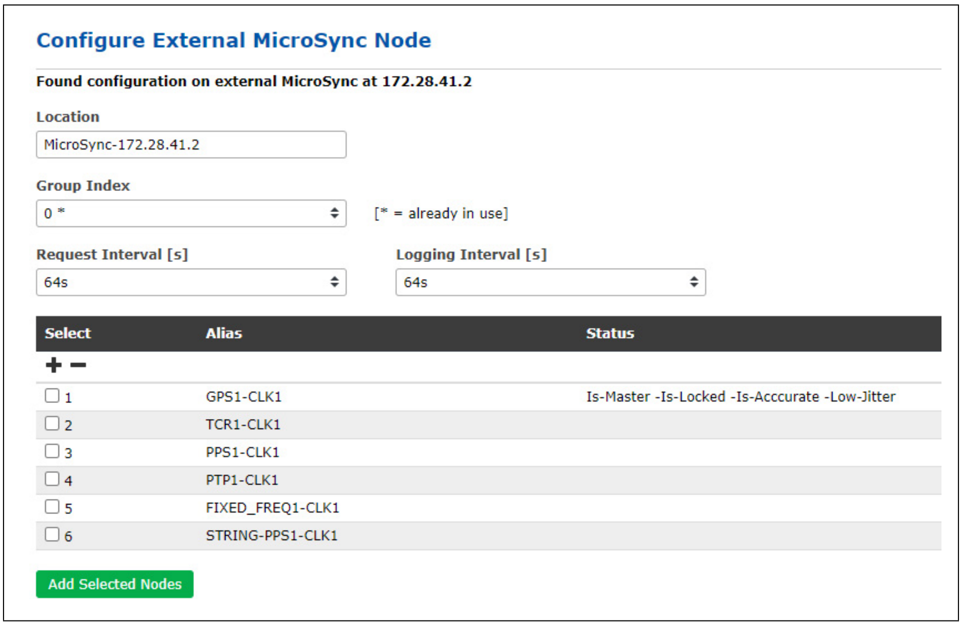
Username:

Password:

To get the current configuration from the external MicroSync you have to select the MRS references you want to monitor from this LANTIME. The parameters for request and log interval are set the same for all of them.

The location and group index can be configured for all selected MRS references. The default location is *MicroSync-** plus the IP address by default.

The alias names for the external MicroSync MRS references are the original alias name plus *@IP address*. It is recommended to use an unused group ID for all MRS references of an external MicroSync.



Configure External MicroSync Node

Found configuration on external MicroSync at 172.28.41.2

Location: MicroSync-172.28.41.2

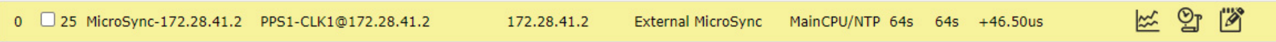
Group Index: 0 * [* = already in use]

Request Interval [s]: 64s

Logging Interval [s]: 64s

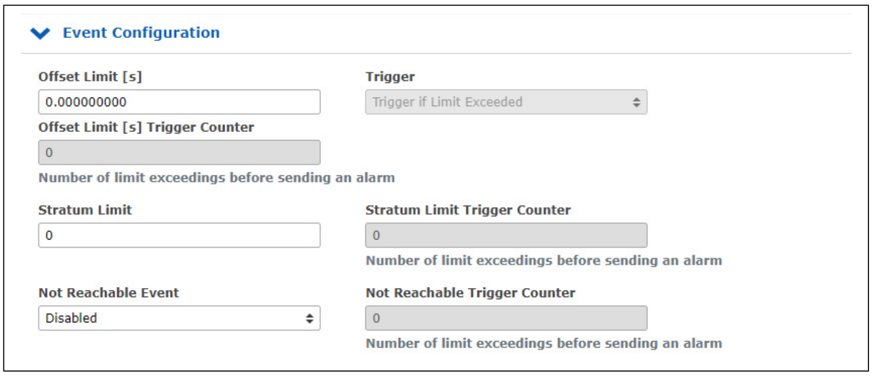
Select	Alias	Status
+ −		
☐ 1	GPS1-CLK1	Is-Master -Is-Locked -Is-Acccurate -Low-Jitter
☐ 2	TCR1-CLK1	
☐ 3	PPS1-CLK1	
☐ 4	PTP1-CLK1	
☐ 5	FIXED_FREQ1-CLK1	
☐ 6	STRING-PPS1-CLK1	

When changes are made to the nodes of the external MicroSync configuration that are to be monitored, a warning sign is displayed in the Events column for this node in the main table. Then you have to change the parameters for this node manually.



0	☐ 25	MicroSync-172.28.41.2	PPS1-CLK1@172.28.41.2	172.28.41.2	External MicroSync	MainCPU/NTP	64s	64s	+46.50us

10.1.8.6 Event Configuration



Event Configuration

Offset Limit [s]: 0.000000000

Trigger: Trigger if Limit Exceeded

Offset Limit [s] Trigger Counter: 0

Number of limit exceedings before sending an alarm

Stratum Limit: 0

Stratum Limit Trigger Counter: 0

Number of limit exceedings before sending an alarm

Not Reachable Event: Disabled

Not Reachable Trigger Counter: 0

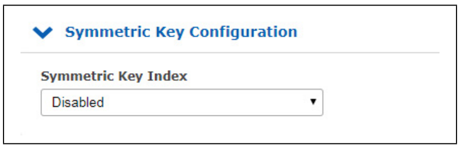
Number of limit exceedings before sending an alarm

Offset Limit (s):
Offset threshold value in seconds. The measured offset between a node and the reference will be compared to the configured threshold. If the calculated difference is higher than the configured offset limit the LANTIME will generate an alarm "Sync Monitor" (which can be sent as a notification eMail, SNMP trap or to an external syslog server). With the "Trigger" option can be choose the direction “Trigger if Limit Exceeded” or "Trigger if Below Limit". With the option "Offset Limit [s] Trigger Counter" the Event will be triggered once after number of limit exceeded in a row.

Stratum Limit:
Threshold value for a NTP stratum level. If the stratum level of a monitored client is higher than the configured stratum limit, it will generate an alarm (sent by eMail, SNMP trap or to an external syslog server). With the option “Stratum Limit Trigger Counter” the Event will be triggered once after number of limit exceeded in a row.

Not Reachable Event:
If configured Node is not reachable for monitoring then LANTIME will generate an alarm "Sync Monitor" (which can be sent as a notification eMail, SNMP trap or to an external syslog server). With this option this can be enabled or disabled. With the option "Not Reachable Limit Trigger Counter" the Event will be triggered once after number of not reachable exceeded in a row.

10.1.8.7 Symmertric Key Configuration

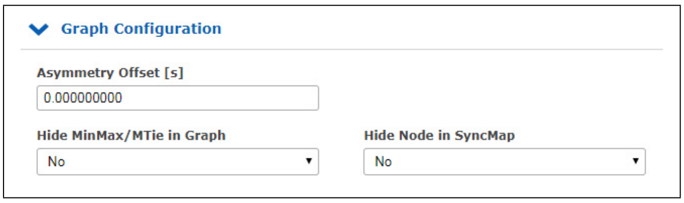


Symmetric Key Index: Disabled

Symmetric Key Index:
If you want to use symmetric key authentication for SyncMon then select a key index from the list of already applied keys. If the keys are not yet defined, proceed to the NTP dialog in the "Web GUI → NTP → Symmetric Keys" and generate a new key file, which should be stored and activated on the monitored node as well. For more information about Symmetric Key Generation please proceed to LTOS7 Configuration "Web GUI → NTP → NTP Symmetric Keys".

10.1.8.8 Graph Configuration

Asymmetry Offset for Graphic:
If a constant asymmetry of the measured nodes is known then you can set this value for the graphical output – the logged values will not be modified - the asymmetry offset is like a fix offset for graphic monitoring only.



Asymmetry Offset [s]: 0.000000000

Hide MinMax/MTie in Graph: No

Hide Node in SyncMap: No

Hide Min/Max/MTie filled curves in Graphic:
If the request-interval is lower than the log-interval additional values for Min and Max will be stored in the logfiles. These Min/Max values will be displayed as a filled curve in a gray color behind the logged offset curve. This feature can be disabled.

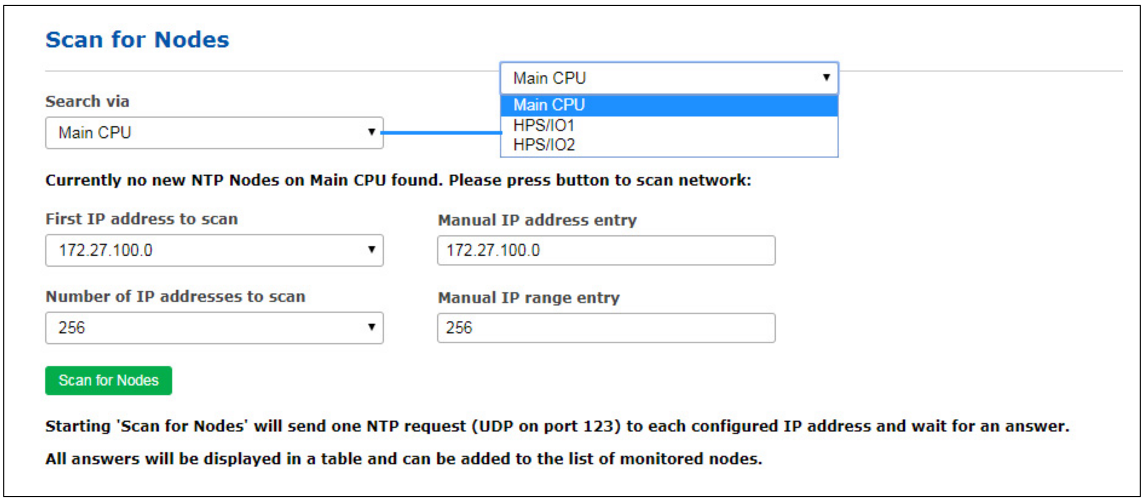
Hide this Node in SyncMap:
You can disable a specific node in the SyncMap.

When you are finished with configuration of a new monitored node, save the current configuration by clicking the "Save Member" button. By clicking the "Remove Member" button you will remove the currently selected node from the complete list of all monitored nodes. All sampled data for the particular node will be lost if you did not back-up the saved data prior its removal.

By clicking the "**Remove Existing Data**" button all data for only this specific node will be erased.

10.1.8.9 Scan for New Nodes

Scan for new Nodes is an automatic search for NTP and PTP nodes within your network. Scan for PTP nodes will be supported by HPS card only with 1024 clients license and monitoring activated.



Scan for Nodes

Search via: Main CPU

Currently no new NTP Nodes on Main CPU found. Please press button to scan network:

First IP address to scan: 172.27.100.0

Manual IP address entry: 172.27.100.0

Number of IP addresses to scan: 256

Manual IP range entry: 256

Starting 'Scan for Nodes' will send one NTP request (UDP on port 123) to each configured IP address and wait for an answer.

All answers will be displayed in a table and can be added to the list of monitored nodes.

Figure: Scan for new Nodes dialog. Only newly found nodes will appear in this temporary table. Select nodes which you wish to add in the overall monitoring node table.

Search via:
First select an instance from a drop-down list to use for searching of new nodes. Possible options are "Main CPU" and "HPS" card. With the Main CPU you can search for NTP nodes only. Scan for PTP nodes will be supported by HPS card only with 1024 clients license and monitoring activated.

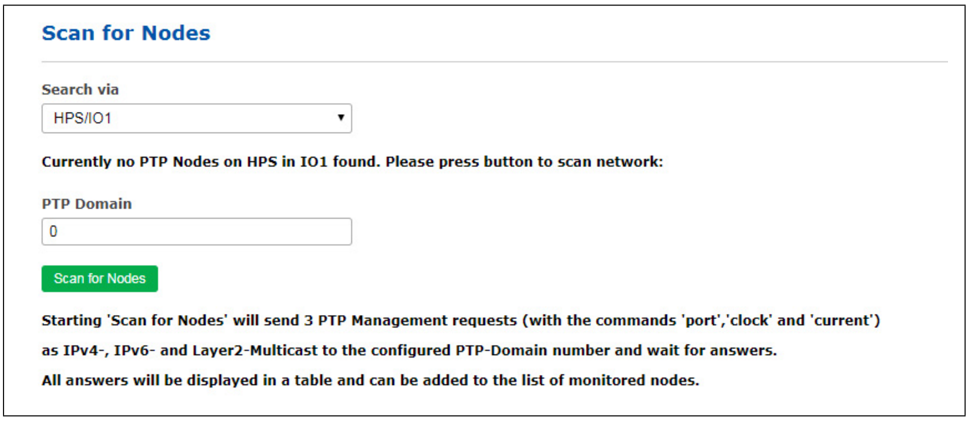
First IP address to scan:
Set the starting IP Address where the search will start with the automatic NTP scan. In the drop-down list you will find all sub net ranges of each network interface. With "Manual IP address entry" an other start point can be defined.

Number of IP Address to scan:
This parameter will set a number of IP-addresses which will be scanned. To each IP address from the IP-Range a separate NTP packet request will be sent. If a NTP client answers to this request and its IP address has not yet been configured then this node will appear in the table. With "Manual IP range entry" an other size of the range can be defined.

Scan for NTP Nodes via Main CPU:
Starting "**Scan for Nodes**" will send one NTP request (UDP on port 123) to each configured IP address (IP address range) and wait for an answer.

All answers will be displayed in a table and can be added to the list of monitored nodes. With select-boxes new nodes can be added automatically to the list of the monitored nodes. The parameters for Location, Group Index, Request Interval, Logging Interval, Offset Limit and Stratum Limit can be defined at the next step, before adding them in the table with other monitored nodes.

Search via HPS:
If a HPS card in monitoring mode (supported by HPS card only with 1024 clients license and monitoring activated) is selected then the "PTP Domain" has to be set up.



Scan for Nodes

Search via
HPS/IO1 ▾

Currently no PTP Nodes on HPS in IO1 found. Please press button to scan network:

PTP Domain
0

Starting 'Scan for Nodes' will send 3 PTP Management requests (with the commands 'port','clock' and 'current')

as IPv4-, IPv6- and Layer2-Multicast to the configured PTP-Domain number and wait for answers.

All answers will be displayed in a table and can be added to the list of monitored nodes.

Figure: To scan the network for PTP nodes a HPS card with activated monitoring has to be selected first in the Search for Nodes drop-down list.

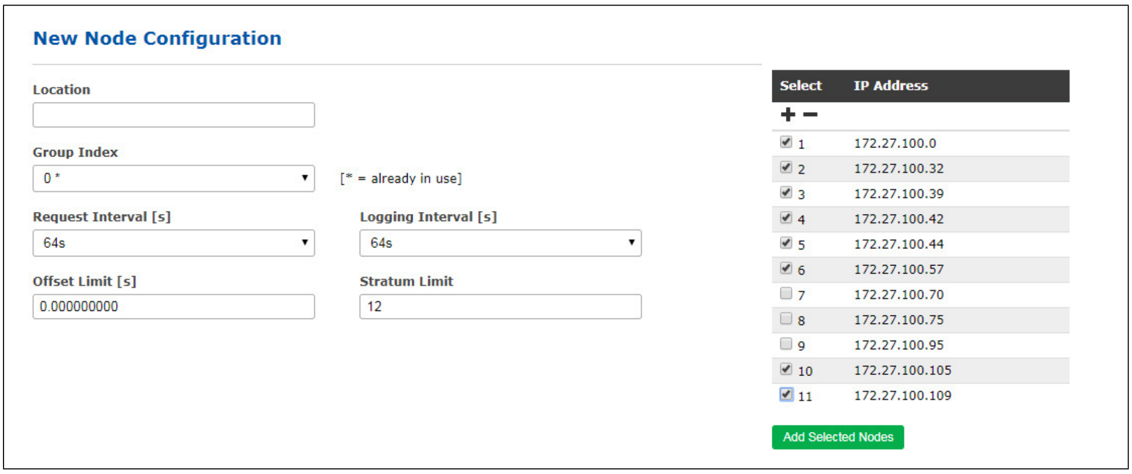
PTP Domain:
The network connected to that HPS card will be scanned in the domain, which was defined here by user. The following mappings as defined in IEEE 1588-2008 will be scanned:

- UDP/IPv4/Ethernet,
- UDP/IPv6/Ethernet,
- Ethernet (IEEE 802.3, layer 2).

When starting the scan first a PTP Management message will be sent in broadcast mode to get the "port state" of each PTP node - this will be done with IPv4, IPv6 and Layer2.

All PTP nodes which answer to this request will ask for the "current status" and "clock status" with management messages that follow. The result will be displayed as a list of all available PTP nodes. Each new PTP Node will be entered in an overview table of the available nodes.

Only new nodes which have not yet been configured will be shown in the table. For each node the PTP-UUID, MAC-Address, IP-Address, Vendor name, Feature (if a node supports PTP with extended TLV for monitoring or PTP management messages only), Domain number, Status (the current PTP status like Slave, Master, Listening . . .), Offset and Delay (current measured values from PTP management message) will be automatically displayed in the table. With select-boxes new nodes can be added automatically to the list of the monitored nodes. The parameters for Location, Group Index, Request Interval, Logging Interval, Offset Limit and Stratum Limit can be defined in the next step before adding the selected nodes.



New Node Configuration

Location

Group Index
0 * ▾ [* = already in use]

Request Interval [s]
64s ▾

Logging Interval [s]
64s ▾

Offset Limit [s]
0.000000000

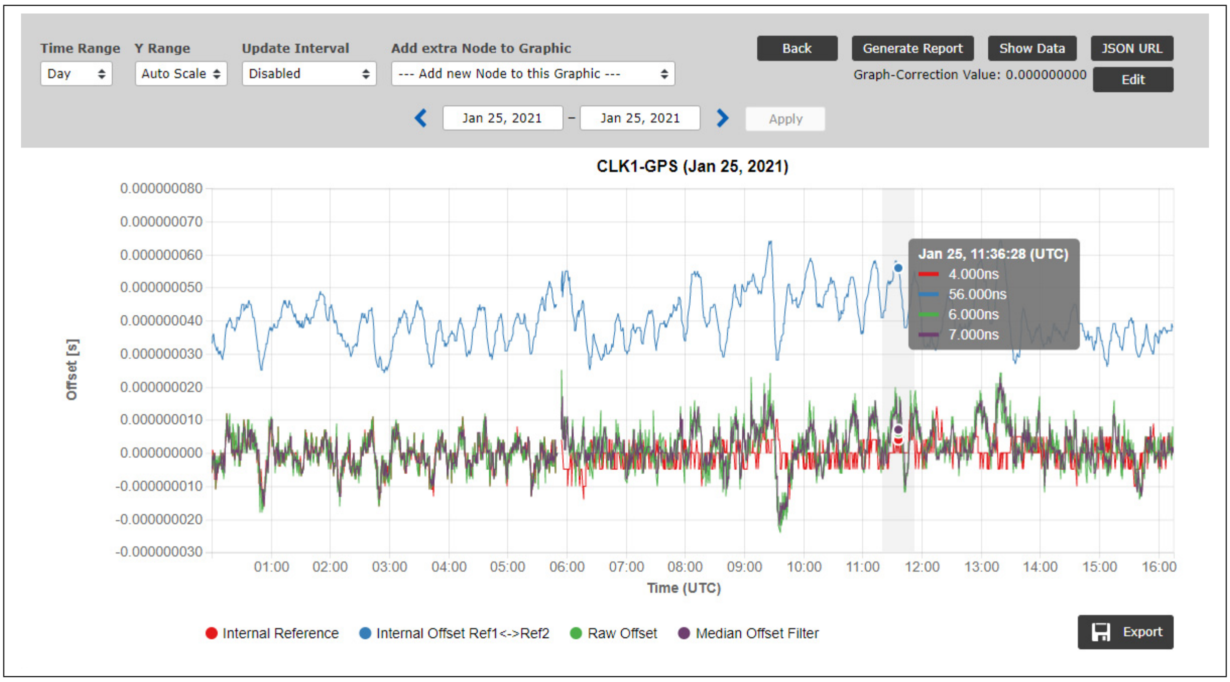
Stratum Limit
12

Select	IP Address
+ −	
☑ 1	172.27.100.0
☑ 2	172.27.100.32
☑ 3	172.27.100.39
☑ 4	172.27.100.42
☑ 5	172.27.100.44
☑ 6	172.27.100.57
☐ 7	172.27.100.70
☐ 8	172.27.100.75
☐ 9	172.27.100.95
☑ 10	172.27.100.105
☑ 11	172.27.100.109

The monitoring engine will start to send PTP/NTP requests in the configured intervals to each node from the list and measure the time received in the responses with its own time (which is traceable to UTC, GNSS sync for example). The current offset and status information can be checked in the status overview table in the Node Monitoring menu.

In the status overview table of monitored nodes, next to the status information you will find 3 action buttons: Graph, Error Logs and Edit.

By selecting the Graph button a Graphical Diagram for the selected node will show up. At this page you find several features for different representation options.



Time Range: Day

Y Range: Auto Scale

Update Interval: Disabled

Add extra Node to Graphic: --- Add new Node to this Graphic ---

Graph-Correction Value: 0.000000000

Jan 25, 2021 – Jan 25, 2021

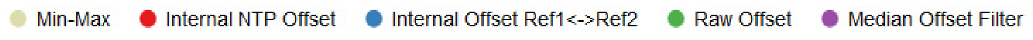
Jan 25, 11:36:28 (UTC)
- Internal Reference: 4.000ns
- Internal Offset Ref1<->Ref2: 56.000ns
- Raw Offset: 6.000ns
- Median Offset Filter: 7.000ns

Figure: Graphical diagram of offset values for each node, selectable for different time ranges (day, week, month or manual selection). With given buttons at the "Select Time Range" you can select either past or future intervals for the graphical representation.

Offsets are collected for each NTP/PTP or other monitored node and can be depicted as graphical representation for selectable time intervals in the web UI of the SyncMon node.

The monitored data are continuously saved on the Sync node "Base Path for logfiles for current day" and will be saved automatically to the Flash Card ('Base Path for logfiles for history of days') at change of a day at 0:00 UTC. Data are available at any time for further statistic processing.

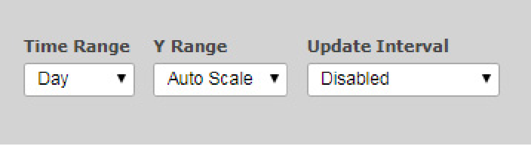
At the bottom of the graph an overview will show which color will represent which data. In this case the red line represents the internal NTP Offset, which is the reference for the monitored NTP node. The green line is the offset between a Sync node reference time and the measured time of a monitored device.



By positioning the cursor to one item in the bottom line then only that graph will be displayed and all other graphs will be shown in light color. When clicking to one item in the bottom line then this graph will be hided.

For PTP and PPS signals, the sync node reference is an internal reference time from the receiver (e.g. multi GNSS (GPS, GLONASS, Galileo, Beidou), external UTC time service, IRIG TC, long wave time reference: eg. PZF, MSF, WWVB . . .). The sync node reference is depicted as a red line and if a second reference is available then the blue line represents the offset between the two referenc clocks. For multi GNSS reference clock in normal operation you will see something in the lower nano second range with 5ns resolution.

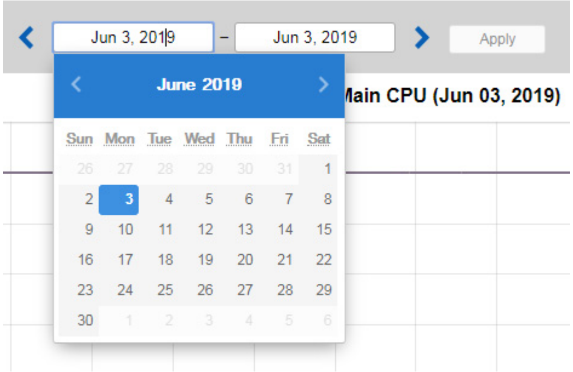
For NTP monitored signal the Sync node is synchronized the internal NTP that is in sync by an internal reference clock (multi GNSS or IRIG TC, long wave ...). In this case the red line in the graph represents the internal NTP system time.


Time Range: Day

Y Range: Auto Scale

Update Interval: Disabled

Time Range:
There are different time ranges to choose from. By day, week, month and custom. When selecting the custom time range click on "**Apply**" to display the graph with the selected time range. For other options it is also possible to go back to see data in the past.



Y Range:
Different options available: auto-scale, or fixed Y ranges in decade intervals: 100ns,1us, 10us, 100us, 1ms, 10ms and 100ms.

Update Interval:
Automatically update of the current graph can be activated from 1s up to 1 hour.

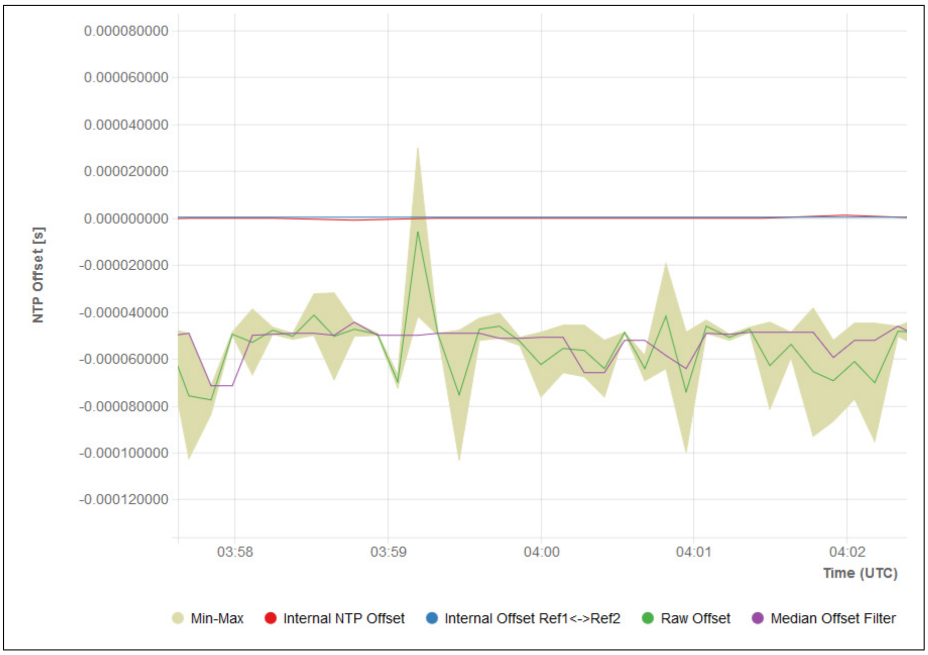
For NTP nodes it is possible to view a graph either as raw data or with applied Median Filter or a graph of the internal reference only (the red line).

For PTP nodes, selected graph modes are **Reported offset from a PTP node** (data obtained from a PTP node by a standard MGMT protocol).

Measured offset to a PTP node (offset of a PTP slave measured against the internal reference). The measurements are available only for PTP nodes which support monitoring PTP protocol with TLVs. The monitored node can be in Slave, Master or Passive mode. Along with the measured values obtained by reverse PTP, also reported value curve is available and MTIE filled curve if MIN and MAX value measurement is supported on the monitored node.

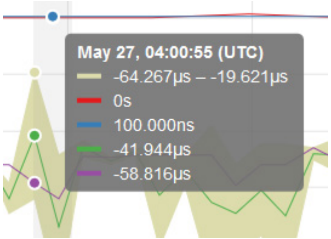
For PPS nodes monitored via an ESI or PIO input card at the Sync node, you will have the graph modes available: raw data, data with applied Median Filter and Internal Reference only (a PPS from an internal reference clock.)

If the request-interval is less than the log-interval then additional Min-Max values for that log-interval will be stored in the data files. These Min-Max values will be added automatically as a filled curve in the graphical diagram and the mean value will be shown as red line in that filled Min/Max curve.



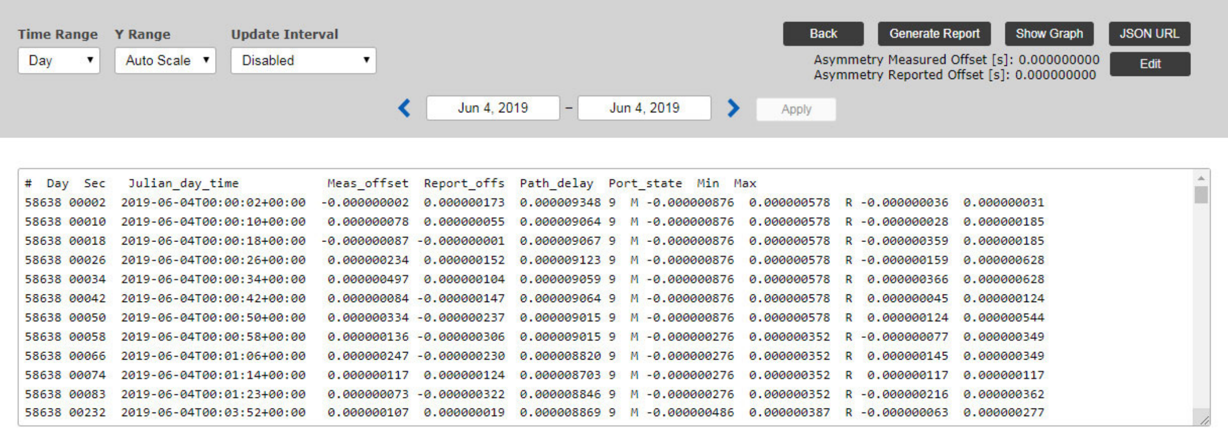
Zoom X/Y-Range:
To zoom in and out the Y-Range position the mouse cursor on the Y-axis and scroll with the mouse wheel to zoom in and out. When pressing the mouse button once on the Y-axis this will be reset to the selected Y-Range. When pressing the mouse button and moving the mouse up and down the Y-axis will be moved up and down.

To zoom in and out the X-Range (time line) position the mouse cursor in the graph and scroll with the mouse wheel to zoom in and out. When pressing the mouse button and moving the mouse left and right the graph will be moved left and right. By moving the mouse over the graph an info view will show all values of all graphs.



Show Data:

With the Button "**Show Data**" you can swap the graphic to a table view of the current displayed values. The first line will show the description of each column. With the "**Show Graph**" button you can go back to the graphical view. If zoomed in then data will be shown of the zoomed time range only.



Asymmetry Measured Offset [s]: 0.000000000
Asymmetry Reported Offset [s]: 0.000000000

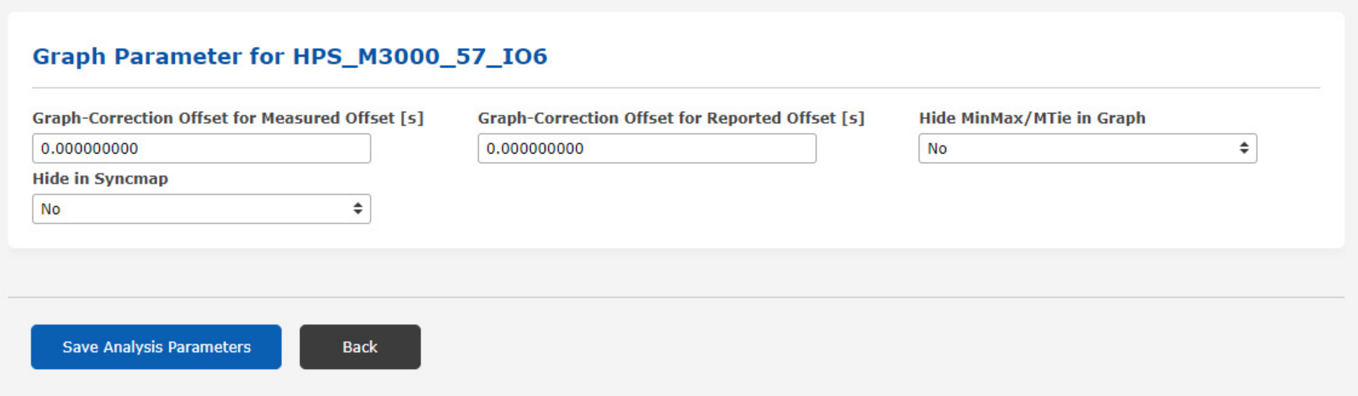
```
#  Day   Sec    Julian_day_time            Meas_offset  Report_offs  Path_delay  Port_state  Min   Max
58638 00002  2019-06-04T00:00:02+00:00  -0.000000002  0.000000173  0.000009348 9  M -0.000000876  0.000000578  R -0.000000036  0.000000031
58638 00010  2019-06-04T00:00:10+00:00   0.000000078  0.000000055  0.000009064 9  M -0.000000876  0.000000578  R -0.000000028  0.000000185
58638 00018  2019-06-04T00:00:18+00:00  -0.000000087 -0.000000001  0.000009067 9  M -0.000000876  0.000000578  R -0.000000359  0.000000185
58638 00026  2019-06-04T00:00:26+00:00   0.000000234  0.000000152  0.000009123 9  M -0.000000876  0.000000578  R -0.000000159  0.000000628
58638 00034  2019-06-04T00:00:34+00:00   0.000000497  0.000000104  0.000009059 9  M -0.000000876  0.000000578  R  0.000000366  0.000000628
58638 00042  2019-06-04T00:00:42+00:00   0.000000084 -0.000000147  0.000009064 9  M -0.000000876  0.000000578  R  0.000000045  0.000000124
58638 00050  2019-06-04T00:00:50+00:00   0.000000334 -0.000000237  0.000009015 9  M -0.000000876  0.000000578  R  0.000000124  0.000000544
58638 00058  2019-06-04T00:00:58+00:00   0.000000136 -0.000000306  0.000009015 9  M -0.000000276  0.000000352  R -0.000000077  0.000000349
58638 00066  2019-06-04T00:01:06+00:00   0.000000247 -0.000000230  0.000008820 9  M -0.000000276  0.000000352  R  0.000000145  0.000000349
58638 00074  2019-06-04T00:01:14+00:00   0.000000117  0.000000124  0.000008703 9  M -0.000000276  0.000000352  R  0.000000117  0.000000117
58638 00083  2019-06-04T00:01:23+00:00   0.000000073 -0.000000322  0.000008846 9  M -0.000000276  0.000000352  R -0.000000216  0.000000362
58638 00232  2019-06-04T00:03:52+00:00   0.000000107  0.000000019  0.000008869 9  M -0.000000486  0.000000387  R -0.000000063  0.000000277
```

JSON URL:

With the button "JSON URL" you will get the WEB address to receive the last measured value of the selected node. This can be used to read the current values via WEB access (wget or curl) from an external program. The JSON format is as follows:

```
{
   "SyncMon_Data": {
       "LastLogValues" :  {
       "NodeName"              : "172.27.100.57",
       "OffsetLimit"           :  0.000000000,
       "RawOffset"             : -0.000050076,
       "MedianOffset"          : -0.000048733,
       "PathDelay"             : -0.000002693,
       "Status"                : 1,
       "LastErrorCode"         : 0,
       "LastConfigChange"      : 0,
       "LogTime"               : 1559025024
  }
 }
}
```

Edit Button:
With the "**Edit**" button all graphical parameters can be displayed and configured. The "Graph Correction Value" can be used to adjust the graph with a fixed offset (e.g. to compensate for a known asymmetry in a network or the runtime of a cable length). In contrast to the "Fix Offset", the "Graph-Correction Value" is only applied to the current graph and not to the stored data.



Graph Parameter for HPS_M3000_57_IO6

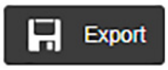
Graph-Correction Offset for Measured Offset [s]: 0.000000000

Graph-Correction Offset for Reported Offset [s]: 0.000000000

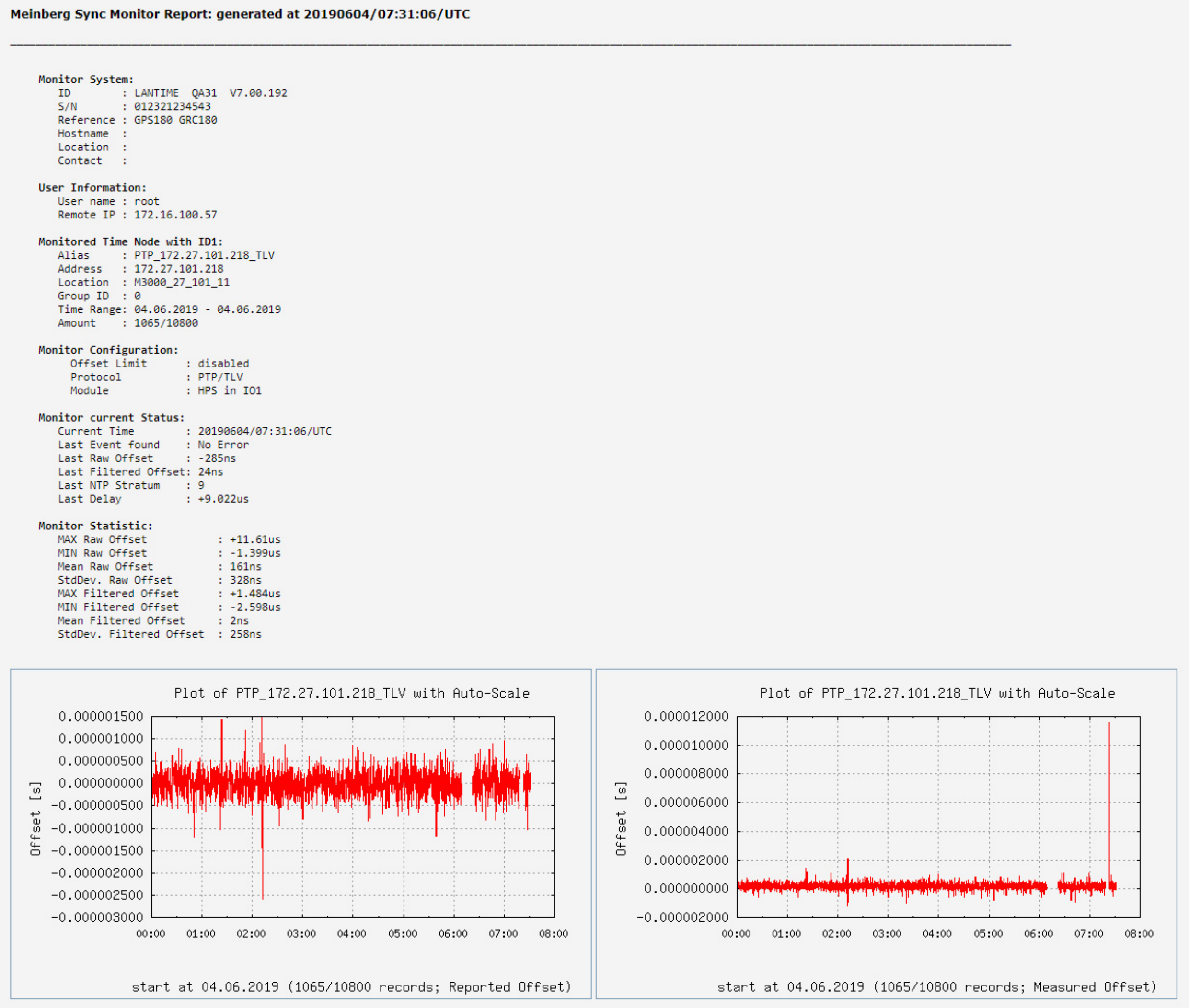
Hide MinMax/MTie in Graph: No

Hide in Syncmap: No

Export Button:
With the "**Export**" button a PNG file of the current graph will be generated. This can be used for printing and saving.



Generate Report Button:
With this selection the current data of the monitored node will be prepared in a form of a report. You can also select a time frame for sampled data from which a report will be generated. The report includes the current status data, monitor configuration, monitoring statistical values over the selected time frame, a graphical diagram and optional a full sync map related to the monitored node.

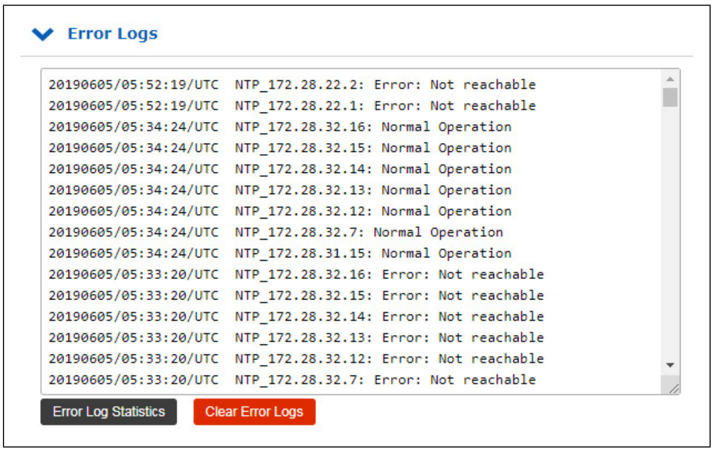


```
Meinberg Sync Monitor Report: generated at 20190604/07:31:06/UTC
_____________________________________________________________________________________________


    Monitor System:
       ID         : LANTIME  QA31  V7.00.192
       S/N        : 012321234543
       Reference : GPS180 GRC180
       Hostname  :
       Location  :
       Contact   :

    User Information:
       User name : root
       Remote IP : 172.16.100.57

    Monitored Time Node with ID1:
       Alias      : PTP_172.27.101.218_TLV
       Address    : 172.27.101.218
       Location   : M3000_27_101_11
       Group ID   : 0
       Time Range: 04.06.2019 - 04.06.2019
       Amount     : 1065/10800

    Monitor Configuration:
         Offset Limit       : disabled
         Protocol           : PTP/TLV
         Module             : HPS in IO1

    Monitor current Status:
       Current Time         : 20190604/07:31:06/UTC
       Last Event found     : No Error
       Last Raw Offset      : -285ns
       Last Filtered Offset: 24ns
       Last NTP Stratum     : 9
       Last Delay           : +9.022us

    Monitor Statistic:
       MAX Raw Offset            : +11.61us
       MIN Raw Offset            : -1.399us
       Mean Raw Offset           : 161ns
       StdDev. Raw Offset        : 328ns
       MAX Filtered Offset       : +1.484us
       MIN Filtered Offset       : -2.598us
       Mean Filtered Offset      : 2ns
       StdDev. Filtered Offset  : 258ns
```

Figure: Generated report for a selected node. The report includes a status information of the selected monitored nodes, monitor configuration, main monitor statistics and graphical diagrams.

"Back" button in Graph view:
When choosing the graphic page the 'Back' button will go back to the main table view and showing the table with all configured nodes. In case of sensors the table of sensors will be opened automatically.

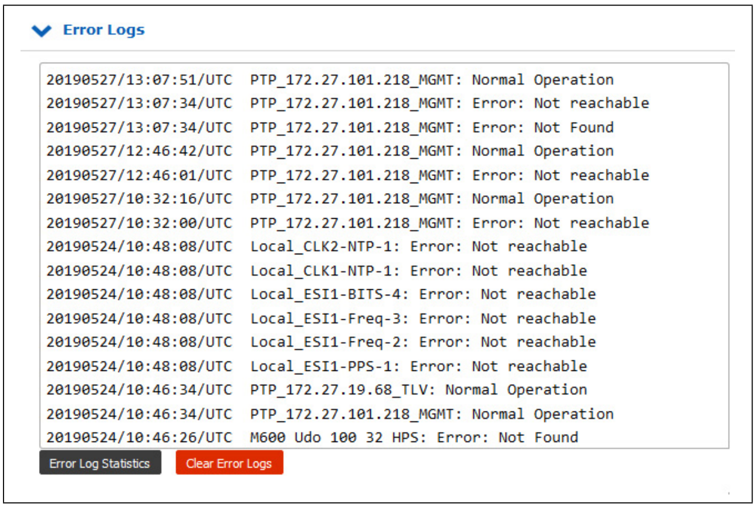
Error Logs:
Back in the main Sync Mon menu, by selecting the Error Logs button you will enter the Error Logs page of the selected monitored node. At this page the log messages are shown since the last system reboot. When the flash memory card gets full, the older logs will be overwritten.



```
20190605/05:52:19/UTC  NTP_172.28.22.2: Error: Not reachable
20190605/05:52:19/UTC  NTP_172.28.22.1: Error: Not reachable
20190605/05:34:24/UTC  NTP_172.28.32.16: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.32.15: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.32.14: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.32.13: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.32.12: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.32.7: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.31.15: Normal Operation
20190605/05:33:20/UTC  NTP_172.28.32.16: Error: Not reachable
20190605/05:33:20/UTC  NTP_172.28.32.15: Error: Not reachable
20190605/05:33:20/UTC  NTP_172.28.32.14: Error: Not reachable
20190605/05:33:20/UTC  NTP_172.28.32.13: Error: Not reachable
20190605/05:33:20/UTC  NTP_172.28.32.12: Error: Not reachable
20190605/05:33:20/UTC  NTP_172.28.32.7: Error: Not reachable
```

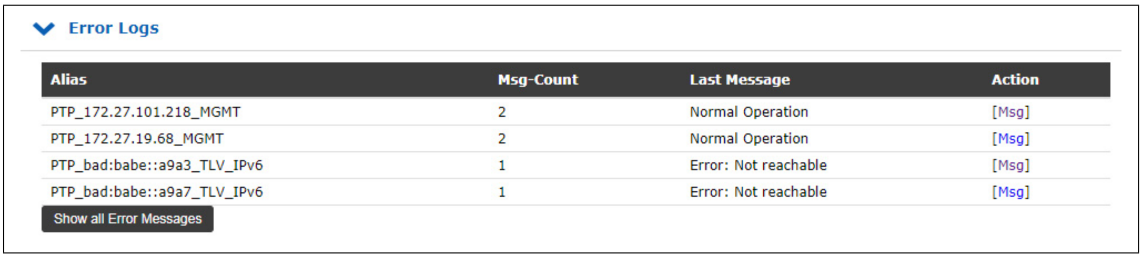
Figure: Error Log Messages for a selected monitored node.

At the bottom of the page there is a button "**Show Global Error Logs**" by which you can switch to view all Error Messages coming from all monitored nodes.



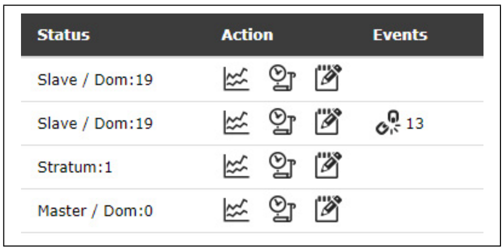
```
20190527/13:07:51/UTC  PTP_172.27.101.218_MGMT: Normal Operation
20190527/13:07:34/UTC  PTP_172.27.101.218_MGMT: Error: Not reachable
20190527/13:07:34/UTC  PTP_172.27.101.218_MGMT: Error: Not Found
20190527/12:46:42/UTC  PTP_172.27.101.218_MGMT: Normal Operation
20190527/12:46:01/UTC  PTP_172.27.101.218_MGMT: Error: Not reachable
20190527/10:32:16/UTC  PTP_172.27.101.218_MGMT: Normal Operation
20190527/10:32:00/UTC  PTP_172.27.101.218_MGMT: Error: Not reachable
20190524/10:48:08/UTC  Local_CLK2-NTP-1: Error: Not reachable
20190524/10:48:08/UTC  Local_CLK1-NTP-1: Error: Not reachable
20190524/10:48:08/UTC  Local_ESI1-BITS-4: Error: Not reachable
20190524/10:48:08/UTC  Local_ESI1-Freq-3: Error: Not reachable
20190524/10:48:08/UTC  Local_ESI1-Freq-2: Error: Not reachable
20190524/10:48:08/UTC  Local_ESI1-PPS-1: Error: Not reachable
20190524/10:46:34/UTC  PTP_172.27.19.68_TLV: Normal Operation
20190524/10:46:34/UTC  PTP_172.27.101.218_MGMT: Normal Operation
20190524/10:46:26/UTC  M600 Udo 100 32 HPS: Error: Not Found
```

With "**Clear Error Logs**" all log entries will be removed. With "**Error Log Statistics**" an overview of logs of all nodes will be displayed.



Alias	Msg-Count	Last Message	Action
PTP_172.27.101.218_MGMT	2	Normal Operation	[Msg]
PTP_172.27.19.68_MGMT	2	Normal Operation	[Msg]
PTP_bad:babe::a9a3_TLV_IPv6	1	Error: Not reachable	[Msg]
PTP_bad:babe::a9a7_TLV_IPv6	1	Error: Not reachable	[Msg]

10.1.8.10 Events



Status	Action	Events
Slave / Dom:19		
Slave / Dom:19		13
Stratum:1		
Master / Dom:0		

In the general overview table the last column Events is dedicated to different alarms, which are defined for monitored nodes:

- Offset limit exceeded
- not reachable
- Stratum limit exceeded
- monitoring not active

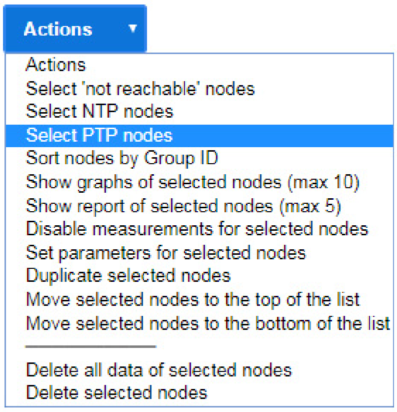
In case of "Offset Limit exceeded" and "not reachable" an icon with the count of events will be shown in the table of monitored nodes in the Events column. These events will be updated automatically every 10s. With the "**Reset Events**" button which can be found above the overview table you can reset the current counter for the events. These events are shown also in the SyncMap.

10.1.8.11 Actions for selected Nodes

In the firmware version 7.00 and following you are able to apply given actions at the same time to a number of selected nodes from the table. First select the nodes which you wish to manage, either by clicking individually a check box at the beginning of each node or by clicking on a "+" sign in the top row of the table if you wish to select all nodes together.

To deselect a node which has been selected, either click again into its check box and it will be deselected or click the "-" icon in the top row and you will deselect all nodes at the same time.

If you click the button "**Actions for selected nodes**" you will find actions which you can apply over the nodes.


Actions ▾
Actions
Select 'not reachable' nodes
Select NTP nodes
Select PTP nodes
Sort nodes by Group ID
Show graphs of selected nodes (max 10)
Show report of selected nodes (max 5)
Disable measurements for selected nodes
Set parameters for selected nodes
Duplicate selected nodes
Move selected nodes to the top of the list
Move selected nodes to the bottom of the list
Delete all data of selected nodes
Delete selected nodes

Select all "not reachable" nodes:
Selection of all nodes, whose offset status shows "not reachable".

Select all NTP nodes:
Selection of all nodes, which are monitored via NTP.

Select all PTP nodes:
Selection of all nodes, which are monitored via PTP, either MGMT or with TLV messages.

Sort nodes by Group ID:
The full list of nodes will be sorted by Group ID

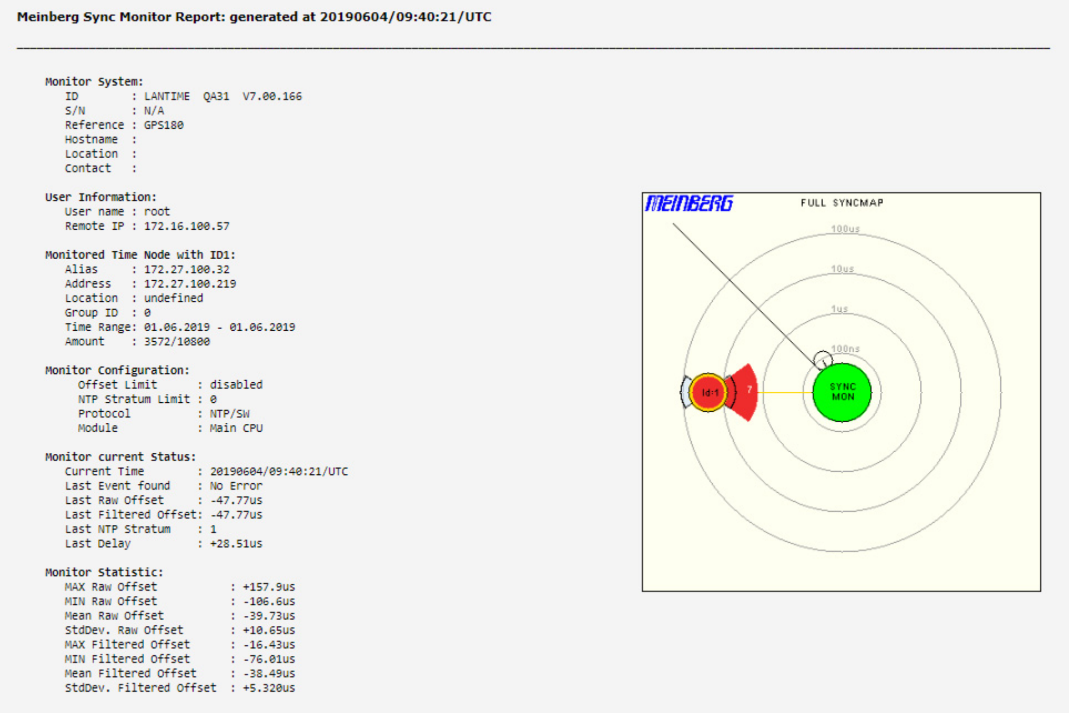
Show overview of the current day:
If none of nodes has been primarily selected than graphical diagrams of the current day will be shown in a thumbnail form for all nodes in the table. Along with the graphical diagrams also the status information and statistics over the current day measurements will be displayed.

Show overview of the time range:
If none of nodes has been primarily selected than graphical diagrams of the selected time range will be shown in a thumbnail form for all nodes in the table. Along with the graphical diagrams also the status information and statistics over the selected time range measurements will be displayed.

Show a Graphical Diagram for selected nodes (max 10):
If you select up to ten nodes in the table, they can be displayed in the same graphical diagram. First, you have to select a time frame in which the graphical diagram will be displayed.

Create a Report for selected nodes (max 5):
If you select up to five nodes in the table, the current data of the selected nodes will be prepared in a form of a report. First, you have to select a time frame for which the report will be generated. The report includes the current status data, monitor configuration, monitoring statistical values over the selected time frame and a graphical diagram which shows the offset trend.

Besides, the report also provides a light version of a sync map, which includes only the selected nodes from the table. In the sync map each individual node is highlighted and the rest are depicted in the background to get a comparison of how the given node is performing in relation to other nodes considered in the report.



Meinberg Sync Monitor Report: generated at 20190604/09:40:21/UTC

```
    Monitor System:
       ID        : LANTIME  QA31  V7.00.166
       S/N       : N/A
       Reference : GPS180
       Hostname  :
       Location  :
       Contact   :

    User Information:
       User name : root
       Remote IP : 172.16.100.57

    Monitored Time Node with ID1:
       Alias     : 172.27.100.32
       Address   : 172.27.100.219
       Location  : undefined
       Group ID  : 0
       Time Range: 01.06.2019 - 01.06.2019
       Amount    : 3572/10800

    Monitor Configuration:
         Offset Limit      : disabled
         NTP Stratum Limit : 0
         Protocol          : NTP/SW
         Module            : Main CPU

    Monitor current Status:
       Current Time        : 20190604/09:40:21/UTC
       Last Event found    : No Error
       Last Raw Offset     : -47.77us
       Last Filtered Offset: -47.77us
       Last NTP Stratum    : 1
       Last Delay          : +28.51us

    Monitor Statistic:
       MAX Raw Offset           : +157.9us
       MIN Raw Offset           : -106.6us
       Mean Raw Offset          : -39.73us
       StdDev. Raw Offset       : +10.65us
       MAX Filtered Offset      : -16.43us
       MIN Filtered Offset      : -76.01us
       Mean Filtered Offset     : -38.49us
       StdDev. Filtered Offset  : +5.320us
```

Figure: Generated report for selected nodes in the table. The report includes a status information of the selected monitored nodes, monitor configuration, main monitor statistics and graphical diagrams.

Disable measurements for selected nodes:
The nodes for which you disable measurements will get a status "Disabled". The measurements will no longer be requested and logged for this node. The latest measured offset will be shown in the Offset column. To start measurements again, select a node and choose "**Enable measurements for selected nodes**".

Set parameter for selected nodes:
For the selected nodes you can set or edit a list of monitoring parameters at the same time. When you select this feature the configuration dialog will show up where you can re-configure any of the parameters. The new configuration will be applied to all the nodes you have selected for this action after you confirm with the "**Apply to Nodes**" button.

Duplicate selected nodes:
The nodes which you have selected will be copied and pasted below their origin nodes. Afterwards you can edit their parameters.

Move selected nodes to the top of the list:
The selected nodes will be moved to the top of the list.

Move selected nodes to the bottom of the list:
The selected nodes will be moved to the bottom of the list.

Delete all data of selected nodes:
The logged measurement data of the selected nodes will be permanently deleted from the internal flash.

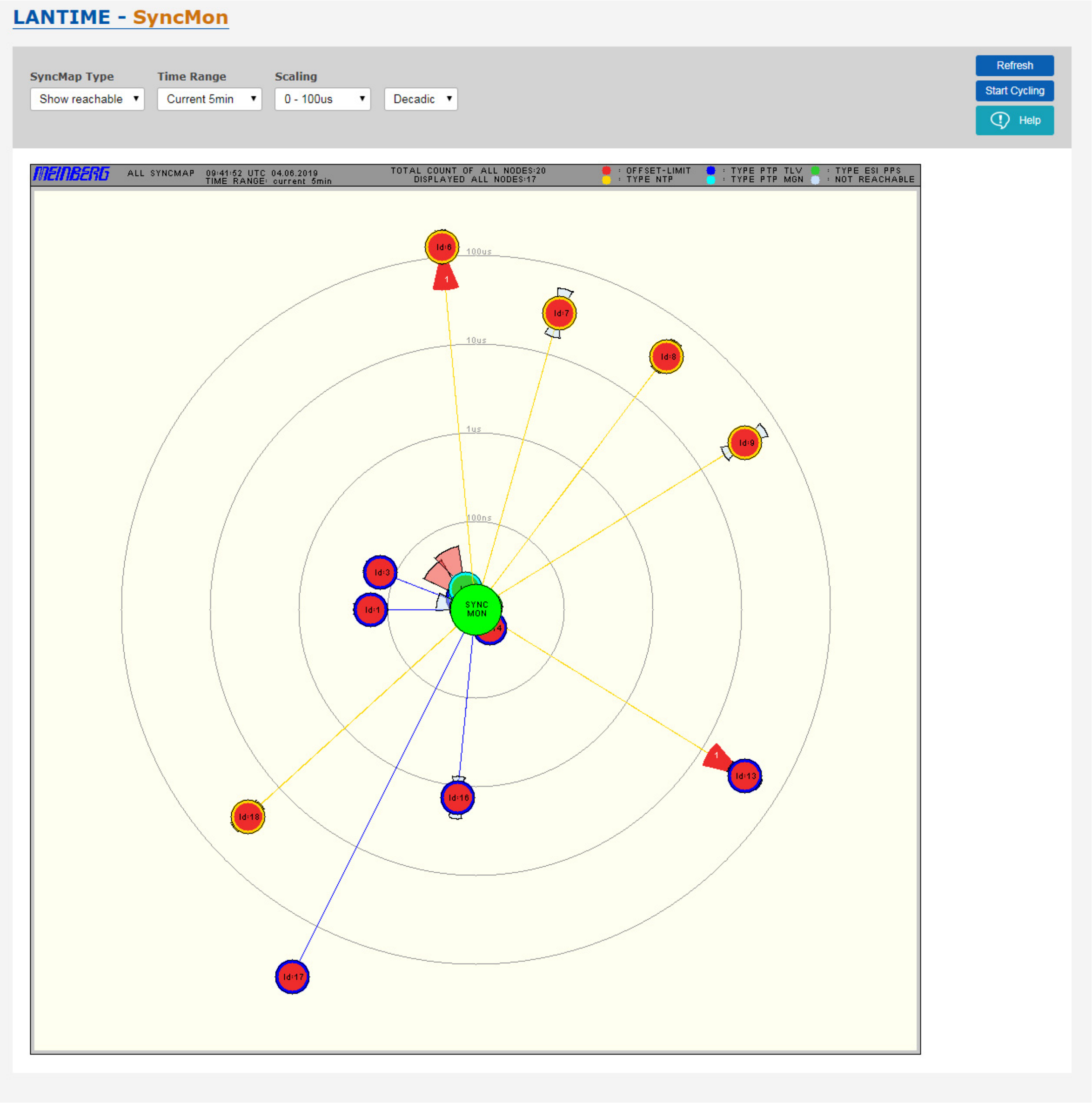
Delete selected nodes:
The selected nodes will be permanently deleted from the list of nodes. The logged measurements up to this point will be preserved.

10.1.8.12 Meinberg Sync Map

The Meinberg SyncMap is a graphical representation of monitored nodes in a network visualized as a polar diagram. The idea of the SyncMap is to give a quick overview of the synchronization status of all monitored devices in a complex network structure.

The monitored devices are called nodes. Nodes have to support one of the following signals: NTP (RFC1305), PTP (IEEE 1588v2) or PPS connected to ESI (Extension Signal Input) IMS card.

The goal is to visualize an absolute offset of monitored nodes in terms of predefined offset limits. The data can be shown according to the current offset status or over a selectable time range (e.g. one day). It is also possible to animate the dynamic behavior of the monitored nodes of the last 60min, where SyncMaps are generated automatically every minute. This mode is called SyncMap Cyclic Mode.



LANTIME - SyncMon

SyncMap Type: Show reachable
Time Range: Current 5min
Scaling: 0 - 100us
Decadic

ALL SYNCMAP 09:41:52 UTC 04.06.2019
TIME RANGE: current 5min
TOTAL COUNT OF ALL NODES:20
DISPLAYED ALL NODES:17

🟥 : OFFSET-LIMIT
🟨 : TYPE NTP
🟦 : TYPE PTP TLV
● : TYPE PTP MGN
🟩 : TYPE ESI PPS
○ : NOT REACHABLE

Figure: The SyncMap as a graphical representation of the monitored nodes in a network visualized as a polar diagram. It can display nodes which support: NTP, PTP (IEEE 1588v2) or PPS signals.

Each monitored node will be represented as a circle with different statistical information.

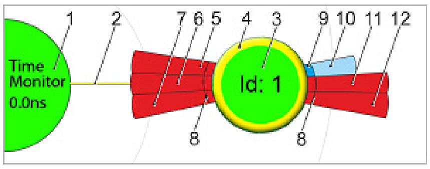


Figure: A node representation in the SyncMap. The meaning of different color codes and parts which belong to a node are explained in the text.

The Time Monitor reference with its reference clock stands in the middle, labeled as the "Time Monitor" [1]. It provides a timing reference by a controlled oscillator (synchronized by GPS, GLN, PZF, Galileo, Beidou or an external clock supply). The Time Monitor node in the center [1] is shown in green color when the reference clock is synchronous. In addition the current offset between the controlled oscillator and the reference time source is shown as a value [1].

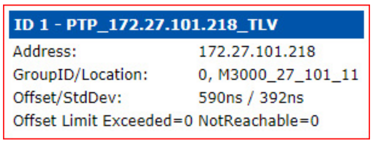
Around the center four concentric circles representing the scaling of the polar diagram are drawn. All nodes [3] are connected concentrically by a line [2] from the central node. The distance from the center to the nodes represents the absolute average time offset between the Time Monitor and each individual node. The average value is calculated over the selected "Time Range". Each node is shown as a circle with a color inside [3] that corresponds the status and an outer ring [4],that corresponds its type.

Status:	green	= Offset $<$ Limit
	red	= Offset $\geq$ Limit or outside the maximum scaling
Type:	yellow	= NTP
	dark blue	= PTP with TLV
	light blue	= PTP with Management Msgs
	green	= ESI PPS
	grey	= not available

Additionally, the statistical values: the standard deviation [8] is represented as circle segments. These values represent the temporal jitter of the measured values around the mean value. When the circle segment color is red, then the deviation is dependent on the scaling and it exceeds the half of range of the decade → example: if the middle deviation is in the range 1μs - 10μs and the largest found maximum >5μs, then the individual segment is drawn red, otherwise blue [10].

If one of the events occur "Offset Limit Exceeded" or "not reachable" then the circle segment will become dark red and a white value which represents the count of each event. The circle slide near the center [5,7] represent the Events “not reachable” and the outer circle slide [6,7] represent the Events "Offset Limit Exceeded".

While sliding with the mouse over a node in the SyncMap without clicking a corresponding info window with the name and some statistical values will be shown:

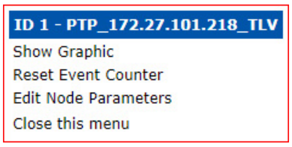


ID 1 - PTP_172.27.101.218_TLV

Address:	172.27.101.218
GroupID/Location:	0, M3000_27_101_11
Offset/StdDev:	590ns / 392ns

Offset Limit Exceeded=0 NotReachable=0

By selecting a specific node in the SyncMap with a left mouse click the following menu will be opened:



ID 1 - PTP_172.27.101.218_TLV

Show Graphic

Reset Event Counter

Edit Node Parameters

Close this menu

"Show Graphic" will open the corresponding graphical diagram.

Example of a full SyncMap

The following picture shows a SyncMap of a network with 250 monitored NTP nodes running on a Sync Fire. This is a real measurement of our Test-Network for burn in tests in the Lantime production. The red signed nodes are DCF77 receivers with no compensation of the distance between a transmitter site and a receiver.

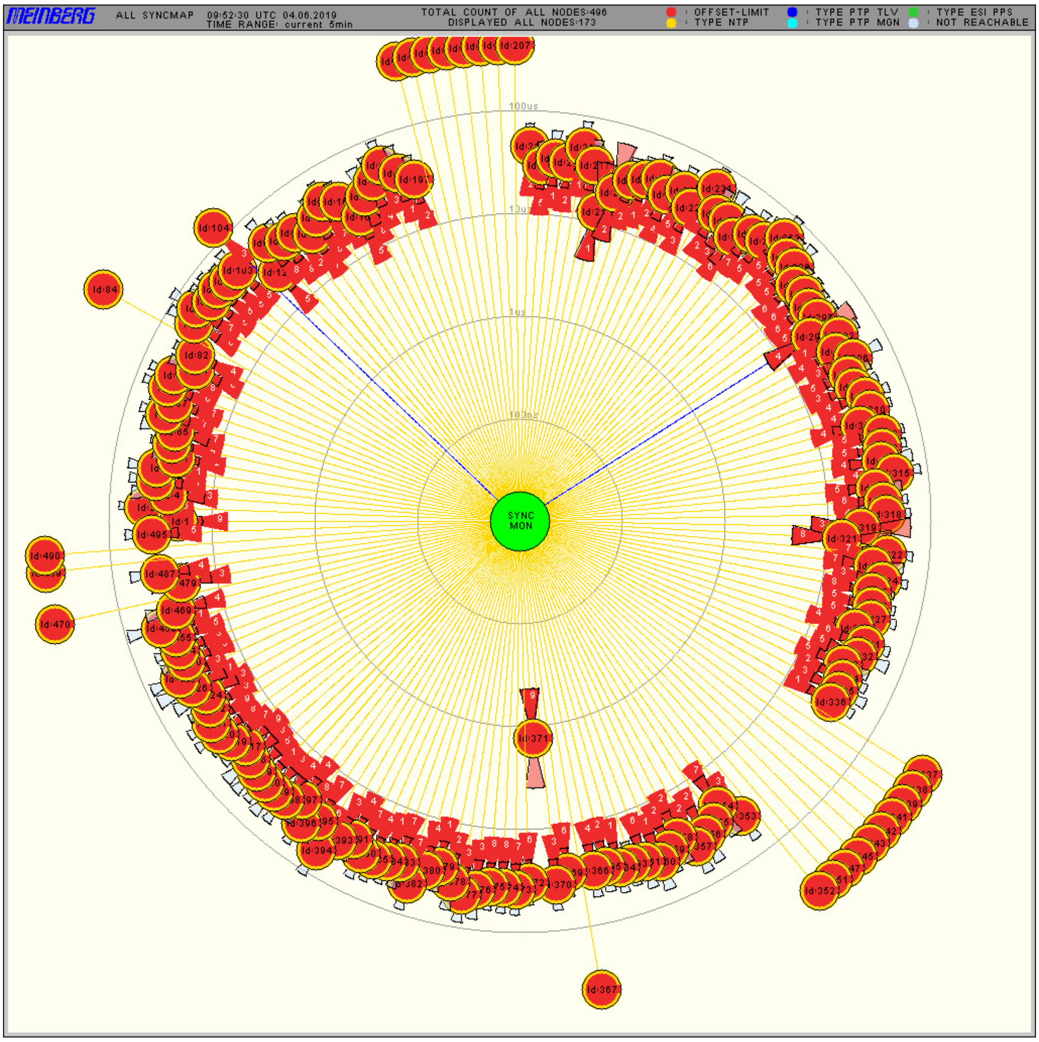


Figure: An example of a Sync map with 250 nodes.

Sync Map Type:

- Show reachable: currently reachable nodes are shown in the Sync Map.
- Show all Nodes: all nodes configured in the monitoring list are shown in the Sync Map, even unreachable ones.
- Show NTP only: only nodes which are monitored via NTP protocol are shown in the Sync Map. They will appear encircled with a yellow ring.
- Show PTP only: only nodes which are monitored via PTP protocol will be shown in the Sync Map. Nodes will appear with a dark blue ring if the PTP with TLV protocol is used for monitoring or with a light blue ring if the PTP protocol with Management Messages is used.

Time Range: the Sync Map can be generated using the monitoring data sampled in the past 30 min, past 5 min, in the past 24 hrs or within a manually selected time range. Also the statistical values are calculated using the data in the selected time interval respectively.

Scaling: possible scaling options: decade steps or linear for different time accuracy ranges. For PTP nodes it may be suitable to use scaling in lower microsecond range, whereas for NTP you can select ranges in a few 100microseconds or millisecond range.

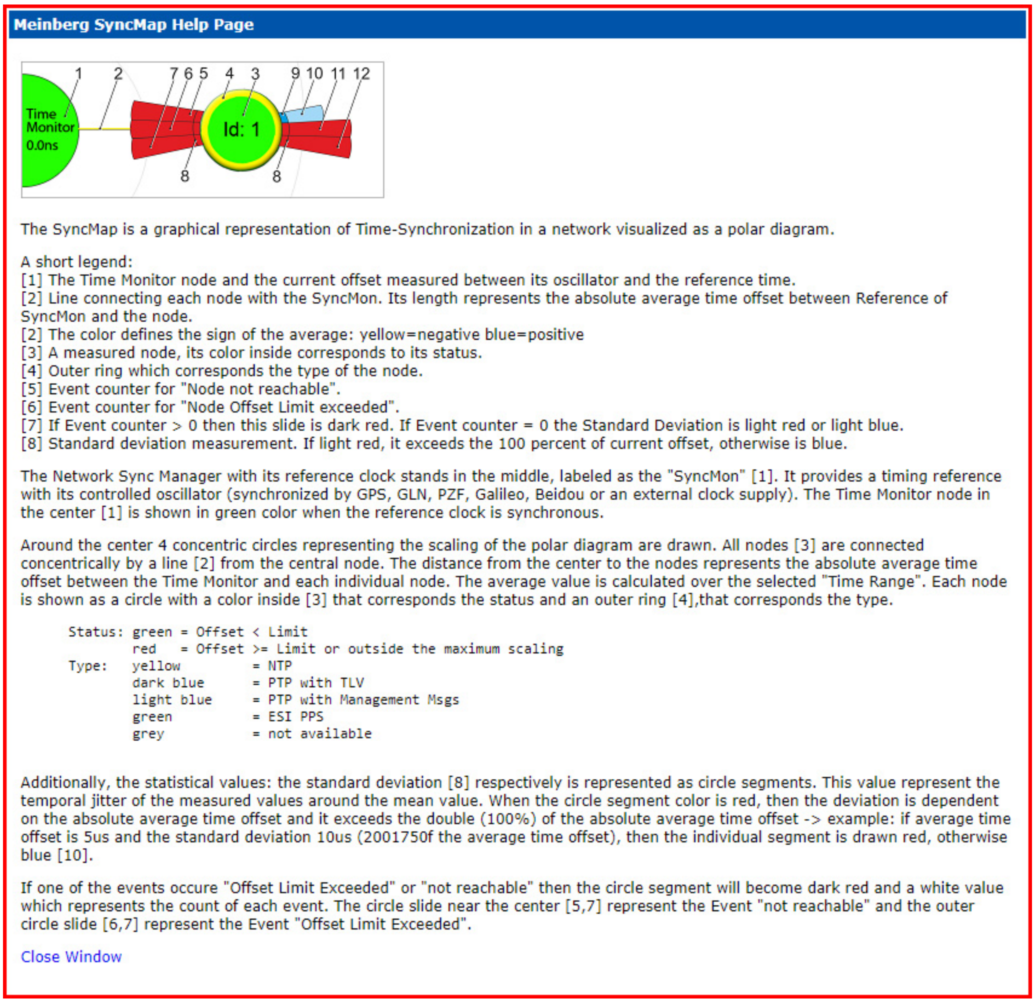
Refresh Button: Immediately refreshes the Sync Map based on the currently available statistics of each single node. A new SyncMap with the selected time range will be generated- it is like a reload of this WEB page with the latest measurements.

Start Cyclic: will activate the SyncMap animation mode. In this mode every minute a new SyncMap with the latest measurements will be generated. The last 60 SyncMaps will be then displayed as an animation. A new sequence will start with a blank SyncMap. The statistics time range will be set by default to 5min.

The number of PNGs stored in RAM is set to 1000 in auto refresh mode if a Q7 CPU or a Syncfire is in use.

Help Button: will show the online help page for a SyncMap feature.

10.1.8.13 Sync Map - Help Window



Meinberg SyncMap Help Page

The SyncMap is a graphical representation of Time-Synchronization in a network visualized as a polar diagram.

A short legend:
[1] The Time Monitor node and the current offset measured between its oscillator and the reference time.
[2] Line connecting each node with the SyncMon. Its length represents the absolute average time offset between Reference of SyncMon and the node.
[2] The color defines the sign of the average: yellow=negative blue=positive
[3] A measured node, its color inside corresponds to its status.
[4] Outer ring which corresponds the type of the node.
[5] Event counter for "Node not reachable".
[6] Event counter for "Node Offset Limit exceeded".
[7] If Event counter > 0 then this slide is dark red. If Event counter = 0 the Standard Deviation is light red or light blue.
[8] Standard deviation measurement. If light red, it exceeds the 100 percent of current offset, otherwise is blue.

The Network Sync Manager with its reference clock stands in the middle, labeled as the "SyncMon" [1]. It provides a timing reference with its controlled oscillator (synchronized by GPS, GLN, PZF, Galileo, Beidou or an external clock supply). The Time Monitor node in the center [1] is shown in green color when the reference clock is synchronous.

Around the center 4 concentric circles representing the scaling of the polar diagram are drawn. All nodes [3] are connected concentrically by a line [2] from the central node. The distance from the center to the nodes represents the absolute average time offset between the Time Monitor and each individual node. The average value is calculated over the selected "Time Range". Each node is shown as a circle with a color inside [3] that corresponds the status and an outer ring [4],that corresponds the type.

```
      Status: green = Offset < Limit
              red   = Offset >= Limit or outside the maximum scaling
      Type:   yellow         = NTP
              dark blue      = PTP with TLV
              light blue     = PTP with Management Msgs
              green          = ESI PPS
              grey           = not available
```

Additionally, the statistical values: the standard deviation [8] respectively is represented as circle segments. This value represent the temporal jitter of the measured values around the mean value. When the circle segment color is red, then the deviation is dependent on the absolute average time offset and it exceeds the double (100%) of the absolute average time offset -> example: if average time offset is 5us and the standard deviation 10us (2001750f the average time offset), then the individual segment is drawn red, otherwise blue [10].

If one of the events occure "Offset Limit Exceeded" or "not reachable" then the circle segment will become dark red and a white value which represents the count of each event. The circle slide near the center [5,7] represent the Event "not reachable" and the outer circle slide [6,7] represent the Event "Offset Limit Exceeded".

Close Window

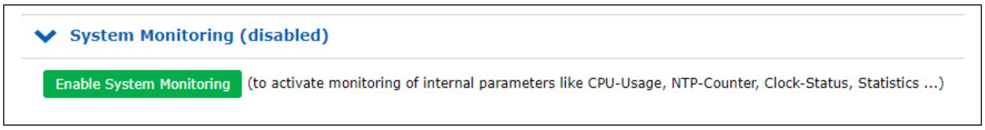
A short legend:

1 The Time Monitor node and the current offset measured between its oscillator and the reference time.
2 Line connecting each node with the SyncMon. Its length represents the absolute average time offset between Reference of SyncMon and the node.
The color defines the sign of the average: yellow=negative blue=positive
3 A measured node, its color inside corresponds to its status.
4 Outer ring which corresponds the type of the node.
5 Event counter for "Node not reachable".
6 Event counter for "Node Offset Limit exceeded".
7 If Event counter > 0 then this slide is dark red. If Event counter = 0 the Standard Deviation is light red or light blue.
8 Standard deviation measurement. If light red, it exceeds the 100 percent of current offset, otherwise is blue.

10.1.8.14 System Monitoring

System Monitoring monitors internal signals in the LANTIME system that do not belong to the monitored nodes (e.g. CPU utilization, local NTP, ESI inputs, MRS references and reference clock parameters). The number and type of internal signals depends on the integrated hardware components in a LANTIME system.

The System Monitoring is an optional function and disabled by default. It can be activated in the "Sync-Mon → System Settings" menu in the System Parameters dialog or directly via the "System Monitoring" tab:



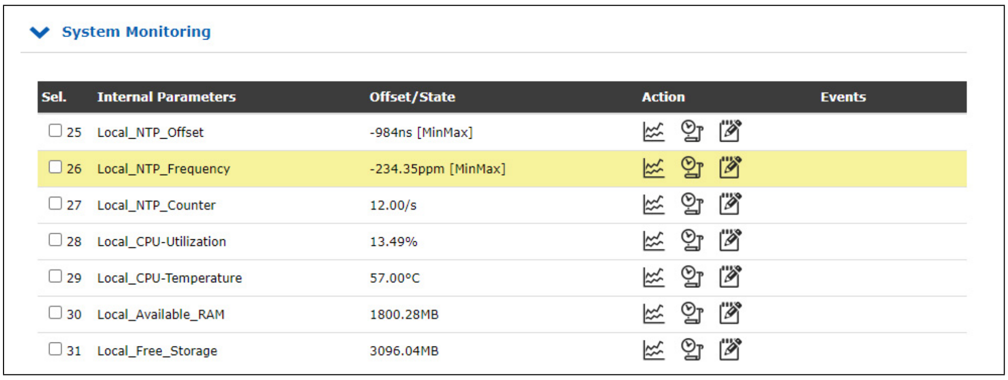
(to activate monitoring of internal parameters like CPU-Usage, NTP-Counter, Clock-Status, Statistics ...)

If the System Monitoring is enabled, then all signals will be measured and logged automatically in the same way like Node Monitoring, namely System Monitoring page will be visible.

The number of MRS references (CLK1-GPS-0, CLK1-NTP-1, CLK1-PTP-2 ...) depends on the activated source priorities for each reference clock - this can be configured via "MRS Settings" in the web interface menu "Clock" for each reference clock used.

Each node from the "System Monitoring" can be selected and displayed in a graph together with nodes from the "Node Monitoring".

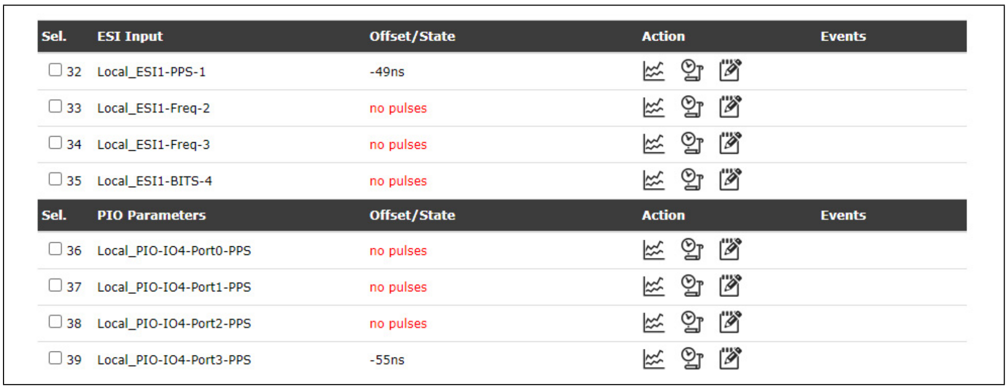
List of possible Sensors in SyncMon:



System Monitoring

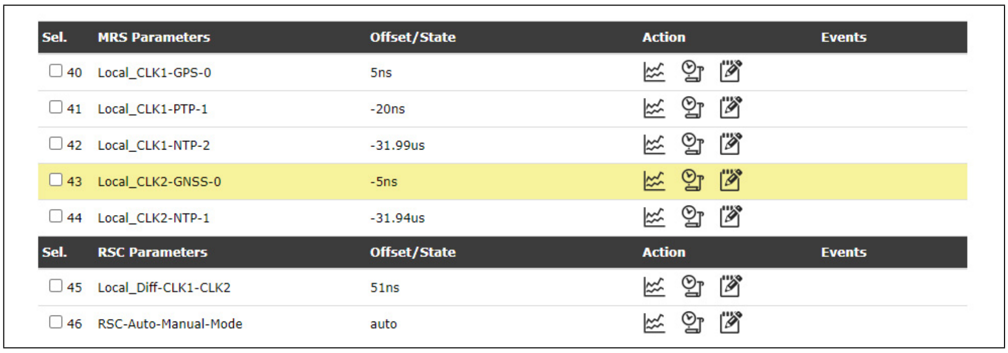
Sel.	Internal Parameters	Offset/State	Action	Events
□ 25	Local_NTP_Offset	-984ns [MinMax]	📈 🔔 📝	
□ 26	Local_NTP_Frequency	-234.35ppm [MinMax]	📈 🔔 📝	
□ 27	Local_NTP_Counter	12.00/s	📈 🔔 📝	
□ 28	Local_CPU-Utilization	13.49%	📈 🔔 📝	
□ 29	Local_CPU-Temperature	57.00°C	📈 🔔 📝	
□ 30	Local_Available_RAM	1800.28MB	📈 🔔 📝	
□ 31	Local_Free_Storage	3096.04MB	📈 🔔 📝	

Internal parameters:	NTP offset NTP frequency NTP Counter Local_CPU-Utilization Local_CPU-Temperature System Free RAM Memory Status System Flash Storage Status



Sel.	ESI Input	Offset/State	Action	Events
□ 32	Local_ESI1-PPS-1	-49ns	📈 🔔 📝	
□ 33	Local_ESI1-Freq-2	no pulses	📈 🔔 📝	
□ 34	Local_ESI1-Freq-3	no pulses	📈 🔔 📝	
□ 35	Local_ESI1-BITS-4	no pulses	📈 🔔 📝	
Sel.	**PIO Parameters**	**Offset/State**	**Action**	**Events**
□ 36	Local_PIO-IO4-Port0-PPS	no pulses	📈 🔔 📝	
□ 37	Local_PIO-IO4-Port1-PPS	no pulses	📈 🔔 📝	
□ 38	Local_PIO-IO4-Port2-PPS	no pulses	📈 🔔 📝	
□ 39	Local_PIO-IO4-Port3-PPS	-55ns	📈 🔔 📝	

ESI input:	ESI PPS in ESI Freq in ESI BITS in
PIO Parameters:	PIO PPS in



Sel.	MRS Parameters	Offset/State	Action	Events
□ 40	Local_CLK1-GPS-0	5ns	📈 ⚙ 📝	
□ 41	Local_CLK1-PTP-1	-20ns	📈 ⚙ 📝	
□ 42	Local_CLK1-NTP-2	-31.99us	📈 ⚙ 📝	
□ 43	Local_CLK2-GNSS-0	-5ns	📈 ⚙ 📝	
□ 44	Local_CLK2-NTP-1	-31.94us	📈 ⚙ 📝	
Sel.	**RSC Parameters**	**Offset/State**	**Action**	**Events**
□ 45	Local_Diff-CLK1-CLK2	51ns	📈 ⚙ 📝	
□ 46	RSC-Auto-Manual-Mode	auto	📈 ⚙ 📝	

MRS reference inputs:

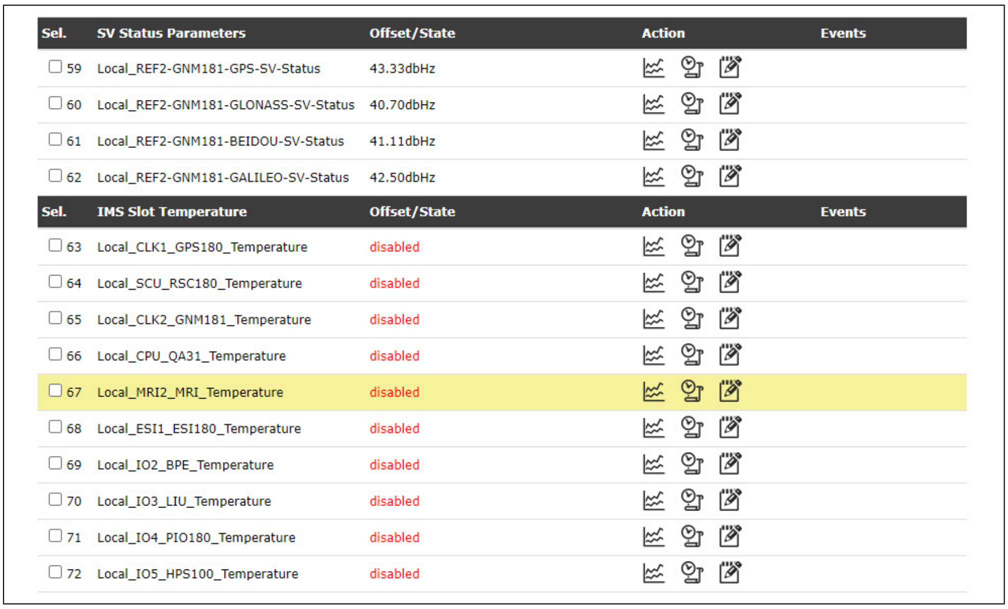
Standard GPS
10 MHz input frequency
1 PPS input signal
combined 10 MHz plus PPS
IRIG input
Network Time Protocol (NTP)
Precision Time Protocol (PTP/IEEE1588)
fixed frequency
1 PPS in addition to time string
variable input signal via GPIO
DCF77 PZF providing much more accuracy than a standard LWR
long wave receiver. e.g. DCF77 AM, WWVB, MSF, JJY
GNSS receiver

RSC parameters:

Local_Diff-CLK1-CLK2
RSC-Auto-Manual-Mode

For each refclock:

- Refclock-State
- MRS-SubState
- Refclock-Usage
- Refclock-DCF-Field
- Refclock-DCF-Correlation
- Refclock-Sat-in-view
- Refclock-good-Sat
- Position change

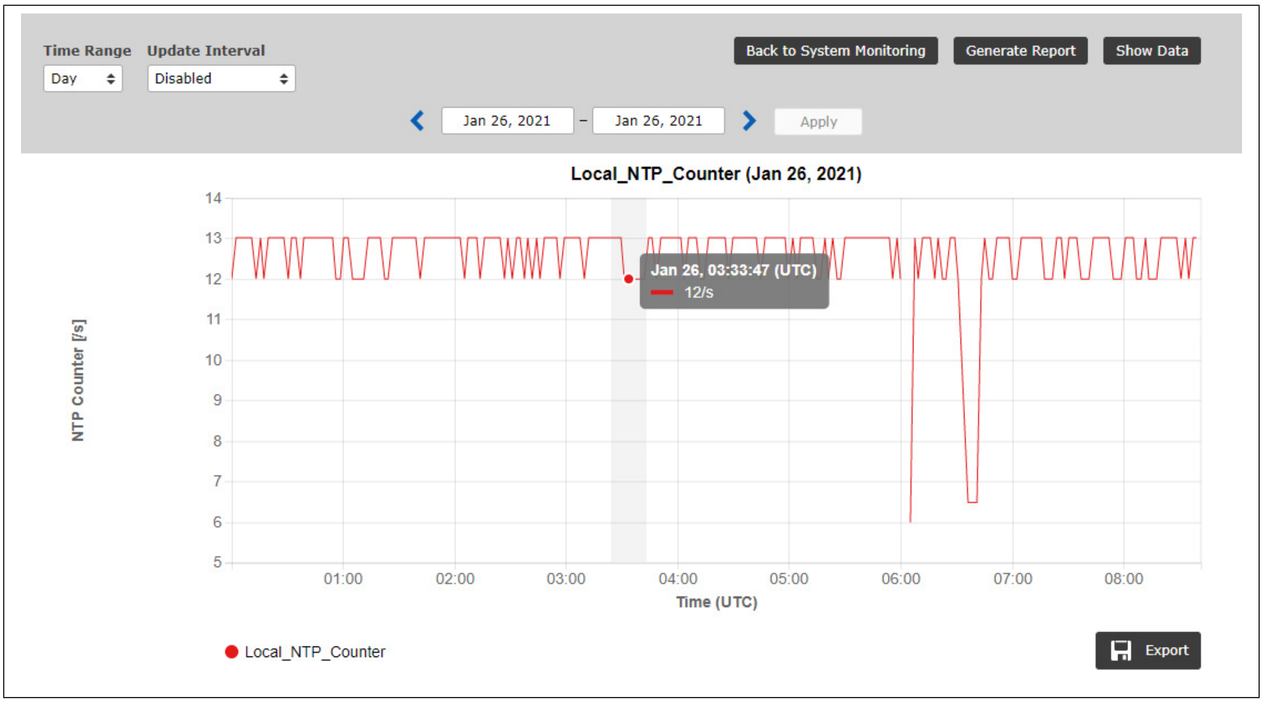


Sel.	SV Status Parameters	Offset/State	Action	Events
☐ 59	Local_REF2-GNM181-GPS-SV-Status	43.33dbHz	📈 🕑 📝	
☐ 60	Local_REF2-GNM181-GLONASS-SV-Status	40.70dbHz	📈 🕑 📝	
☐ 61	Local_REF2-GNM181-BEIDOU-SV-Status	41.11dbHz	📈 🕑 📝	
☐ 62	Local_REF2-GNM181-GALILEO-SV-Status	42.50dbHz	📈 🕑 📝	
Sel.	**IMS Slot Temperature**	**Offset/State**	**Action**	**Events**
☐ 63	Local_CLK1_GPS180_Temperature	disabled	📈 🕑 📝	
☐ 64	Local_SCU_RSC180_Temperature	disabled	📈 🕑 📝	
☐ 65	Local_CLK2_GNM181_Temperature	disabled	📈 🕑 📝	
☐ 66	Local_CPU_QA31_Temperature	disabled	📈 🕑 📝	
☐ 67	Local_MRI2_MRI_Temperature	disabled	📈 🕑 📝	
☐ 68	Local_ESI1_ESI180_Temperature	disabled	📈 🕑 📝	
☐ 69	Local_IO2_BPE_Temperature	disabled	📈 🕑 📝	
☐ 70	Local_IO3_LIU_Temperature	disabled	📈 🕑 📝	
☐ 71	Local_IO4_PIO180_Temperature	disabled	📈 🕑 📝	
☐ 72	Local_IO5_HPS100_Temperature	disabled	📈 🕑 📝	

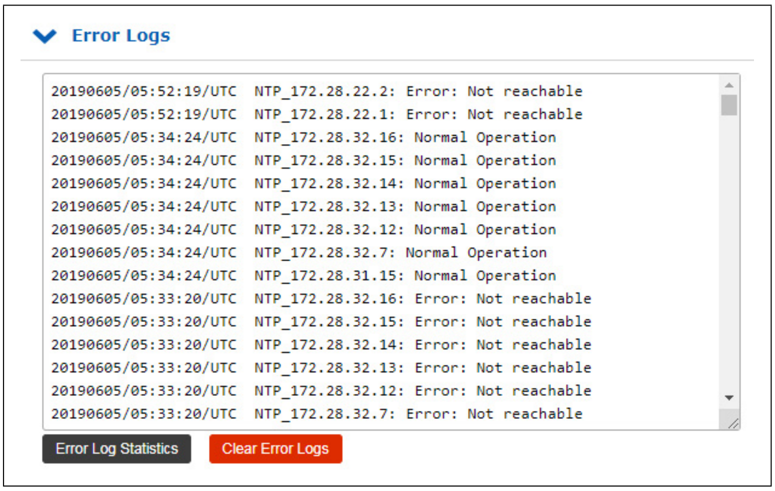
SV status parameters:	- GPS-SV-Status - GLONASS-SV-Status - BEIDOU-SV-Status - GALILEO-SV-Status
IMS slot temperature:	CLK, SCU, CPU, MRI, ESI, IO

10.1.8.15 Local NTP Counter

The LANTIME automatically counts all incoming network packets on UDP port 123 of all available network interfaces. This statistic is displayed graphically in the table "System Monitoring" under **Local_NTP_Counter**. The red line shows a value of the received NTP packets within a selected time period.



10.1.8.16 Error Logs

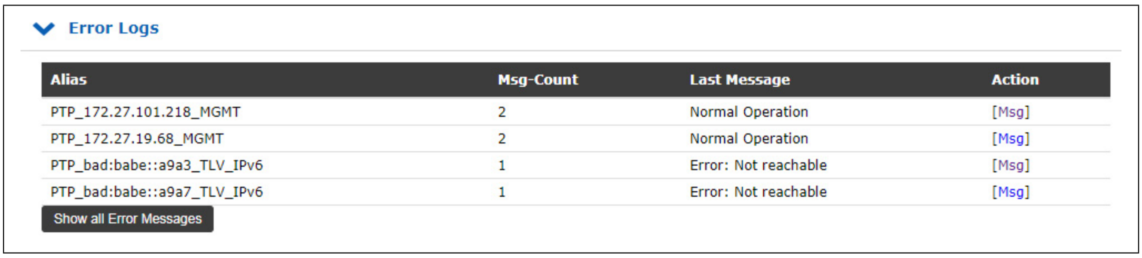


```
20190605/05:52:19/UTC  NTP_172.28.22.2: Error: Not reachable
20190605/05:52:19/UTC  NTP_172.28.22.1: Error: Not reachable
20190605/05:34:24/UTC  NTP_172.28.32.16: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.32.15: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.32.14: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.32.13: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.32.12: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.32.7: Normal Operation
20190605/05:34:24/UTC  NTP_172.28.31.15: Normal Operation
20190605/05:33:20/UTC  NTP_172.28.32.16: Error: Not reachable
20190605/05:33:20/UTC  NTP_172.28.32.15: Error: Not reachable
20190605/05:33:20/UTC  NTP_172.28.32.14: Error: Not reachable
20190605/05:33:20/UTC  NTP_172.28.32.13: Error: Not reachable
20190605/05:33:20/UTC  NTP_172.28.32.12: Error: Not reachable
20190605/05:33:20/UTC  NTP_172.28.32.7: Error: Not reachable
```

Figure: Log Messages from all monitored nodes.

Global Error Log gives the option to track all error events.

Error Log Statistics: categorization of error logs for each specific node.
Clear Error Logs: deletes the list of logged errors.

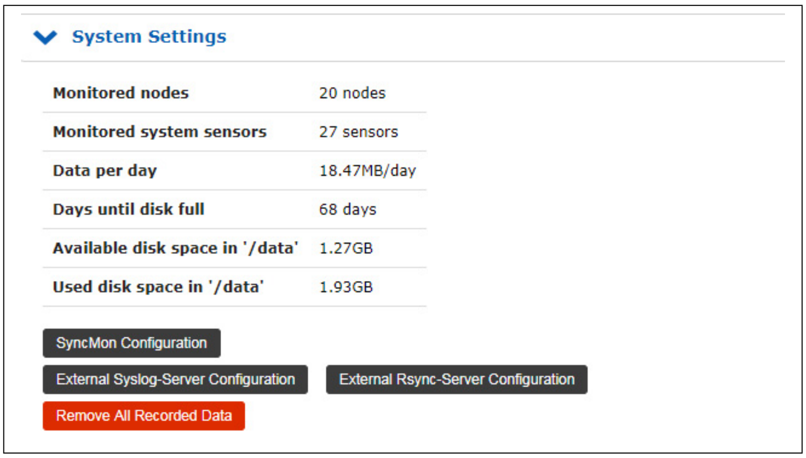


Alias	Msg-Count	Last Message	Action
PTP_172.27.101.218_MGMT	2	Normal Operation	[Msg]
PTP_172.27.19.68_MGMT	2	Normal Operation	[Msg]
PTP_bad:babe::a9a3_TLV_IPv6	1	Error: Not reachable	[Msg]
PTP_bad:babe::a9a7_TLV_IPv6	1	Error: Not reachable	[Msg]

Figure: Error Log Statistics.

10.1.8.17 System Settings

The menu for "System Settings" will show the current available space on the flash disc and will calculate the count of days which can be stored depending on the count of monitored nodes and the log-interval.



System Settings

Monitored nodes	20 nodes
Monitored system sensors	27 sensors
Data per day	18.47MB/day
Days until disk full	68 days
Available disk space in '/data'	1.27GB
Used disk space in '/data'	1.93GB

SyncMon Configuration
External Syslog-Server Configuration
External Rsync-Server Configuration
Remove All Recorded Data

Figure: Memory card status, available space left and logfiles archiving options.

There is an indicator implemented which informs about the available flash space "Available Space on Flash" and the number of days left for monitoring of the current sync node setup. The current data will be stored on the flash card.

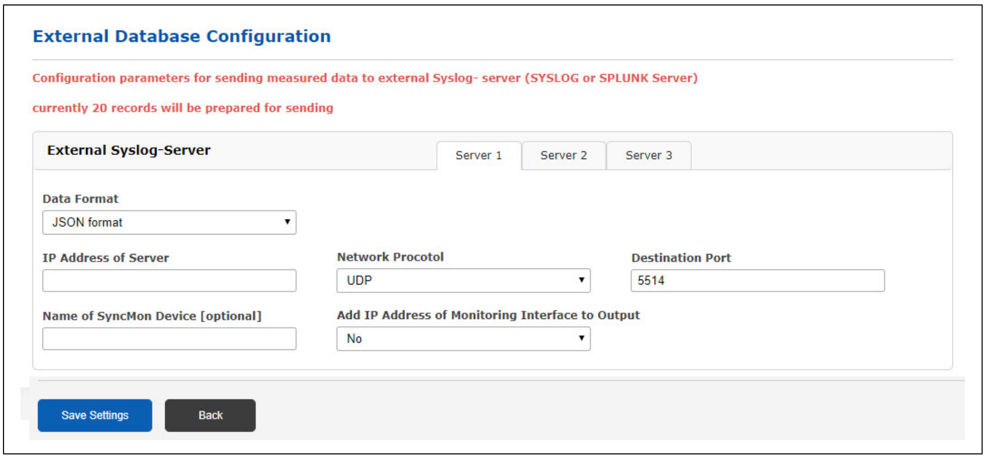
With the button "Remove All Recorded Data" all files on the flash storage belonging to SyncMon will be removed without a backup.

10.1.8.18 Send Monitoring Data to external SYSLOG Server as a Backup

In SyncMon Menu in the Web Interface menu "System Settings → External Syslog-Server Configuration" you can configure up to 3 external Servers, where the measured data is sent at each log interval via the SYSLOG protocol. On the external server has to run a service like a standard Syslog-Server.

In order to backup the monitoring data and store them for later analytical processing, you can enable automatic sending of the data via SYSLOG protocol to up to 3 external database servers. In this case every node measurement processed in a log-interval will be sent to a specified server.

In the following dialog you can configure the target servers where you want to store your data.



External Database Configuration

Configuration parameters for sending measured data to external Syslog- server (SYSLOG or SPLUNK Server)

currently 20 records will be prepared for sending

External Syslog-Server

Data Format: JSON format

IP Address of Server:

Network Procotol: UDP

Destination Port: 5514

Name of SyncMon Device [optional]:

Add IP Address of Monitoring Interface to Output: No

Figure: Configuration options for external database servers where the monitoring data can be stored.

For each of these external servers the following parameters can be set:

- network protocol: UDP or TCP
- a port number (default is 514 for standard SYSLOG)
- a device name
- optionally the IP Address of the network port used for the measurement can be activated
- configuration of the output format:
  - Meinberg Standard Format
  - Key-Value-Pairs (SPLUNK friendly)
  - JSON Format

As Network Protocol options you can choose between the UDP or TCP/IP protocols, running as per default on a port:514.

Name of this SyncMon device: you can monitor your network by different Sync Monitoring devices. You can give them unique names to recognize it easily in the database server, where the data come from.

The Meinberg Standard Format corresponds to the SyncMon data format stored in a file system on a LANTIME. This will be later used for the SyncMon Manager. The SyncMon Manager is currently in development and will be able to visualize the data stored on an external server and generate reports.

An excerpt of the SyncMon format “Meinberg Standard Format” sending via Syslog protocol:

```
SyncMon 172.27.100.32 M3000_100_57_NTP_LAN0 58154 34813 2018-02-05T09:40:13+00:00
0.000000494 0.000041453 0.000073266 1 R -0.000011100 0.000041453
```

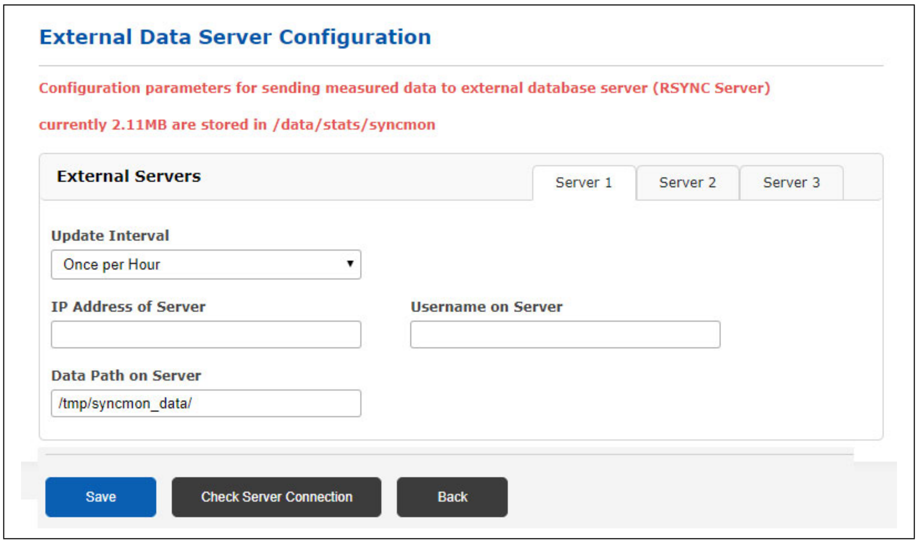
For more Details about SyncMon formats see chapter "Appendix → SyncMon Formats".

10.1.8.19 Copy Monitoring Data to external Server via RSYNC as a Backup

In SyncMon Menu in the Web Interface menu "System Settings → External Rsync-Server Configuration" you can configure up to 3 external Servers, where the measured data is copied every hour or once at 00:00 UTC via the RSYNC protocol. On the external server has to run a service like a standard RSYNC-Server.

In the following dialog you can configure the target servers where you want to store your data.

RSYNC-Server



External Data Server Configuration

Configuration parameters for sending measured data to external database server (RSYNC Server)

currently 2.11MB are stored in /data/stats/syncmon

External Servers

Update Interval: Once per Hour

IP Address of Server:

Username on Server:

Data Path on Server: /tmp/syncmon_data/

Figure: External RSYNC server configuration

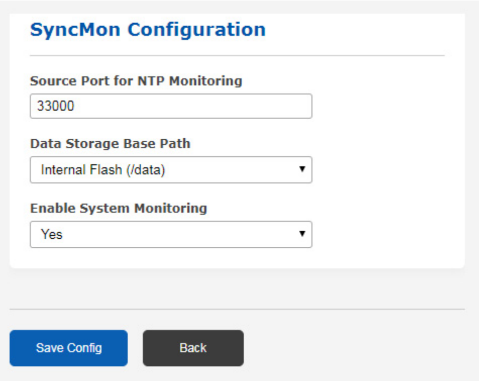
To automatically send data hourly or once a day via **'rsync'**, you must prepare the ssh key for the external RSYNC server:

- Registration via SSH on LANTIME
- Check if identities are available in */root/.ssh/id_rsa.pub*.
- If not, create an identity with **'ssh-keygen -t rsa'**.
- Save this identity for permanent use with: **'saveconfig @'**.
- Copy the identity of the LANTIME to the external RSYNC server with: **'ssh-copy-id ip-adresse-of-RSYNC-server'**.

10.1.8.20 SyncMon Configuration

With the "SyncMon Configuration" button some system configuration parameters can be set:

- Source Port of outgoing NTP packets: default is 33000.
- Base Path for logfiles for history of days. The default path is the internal compact flash with /data. e.g. this could be changed to /mnt/usb-storage if an USB-Memorystick is used.
- Enable Monitoring of System internal parameters.



SyncMon Configuration

Source Port for NTP Monitoring
33000

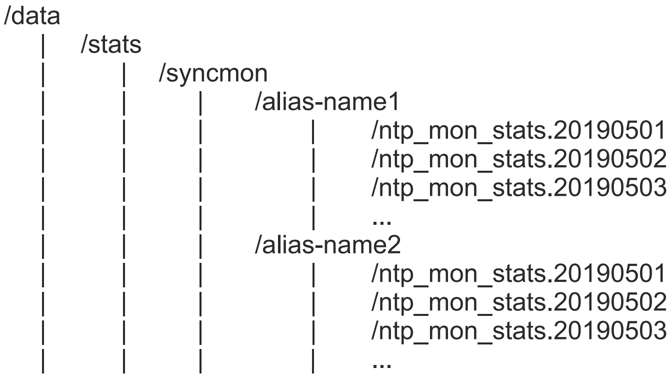
Data Storage Base Path
Internal Flash (/data)

Enable System Monitoring
Yes

Figure: System Parameters settings within the SyncMon feature. Here you can set the current path where the data is stored. Be aware when the flash card is full, the oldest data will be overwritten.

Enable System Monitoring: the monitoring of internal signals like CPU-Utilization, local NTP, ESI inputs, MRS-References and Refclock parameters, depending on integrated hardware of the system will be activated. By default the monitoring of the system is disabled.

The measured data of the monitored nodes will be stored in separate directories on a flash disc. The base path of the stored data files can be configured by the user, therefore it is also possible to use an external flash disc (e.g. USB stick). The data will be stored separately for each day and each monitored node.



```
/data
  |    /stats
  |      |    /syncmon
  |      |      |    /alias-name1
  |      |      |          |    /ntp_mon_stats.20190501
  |      |      |          |    /ntp_mon_stats.20190502
  |      |      |          |    /ntp_mon_stats.20190503
  |      |      |          |    ...
  |      |      |    /alias-name2
  |      |      |          |    /ntp_mon_stats.20190501
  |      |      |          |    /ntp_mon_stats.20190502
  |      |      |          |    /ntp_mon_stats.20190503
  |      |      |          |    ...
```

Figure: Example for default path structure of history of days data files on the flash card.

The data file format:

1. MJD: Modified Julian Date - is the continuous count of days since the beginning of the Julian Period (started at 1858 Nov 17 - 0:00)
2. time past midnight in seconds
3. time stamp (ISO from MJD and time past midnight)
4. measured clock offset raw (If the request interval is less than the Logging interval then the mean value of the measured offsets at request interval will be stored)
5. in case of NTP: clock offset median (Median of the 5 last measured offsets at request-int
   in case of PTP: reported offset
6. path delay in seconds
7. NTP stratum or PTP state
8. 'R' (optional indicator for min/max values of raw data: if the request interval is less than the log-interval then automatically the Min and Max values of the raw data will be stored in the next 2 lines
9. see 8. (optional)
10. see 8. (optional)
11. 'M' (optional indicator for min/max values of MTie (Maximum Time interval error) values from PTP nodes which supports this option: if the PTP node support MTie feature with extended TLVs then the Min and Max values will be stored in the next 2 lines.
12. see 11. (optional)
13. see 11. (optional)

Samples of Monitoring Data stored in the history of days files:

Example for NTP data files:

```
# Day Sec Modified_Julian_day_time Raw_offset Median_offs Path_delay Stratum
58043 21705 2017-10-17T06:01:45+00:00 -0.000000129 -0.000000053 0.000007667 1
```

Example for NTP data files with request interval less than log interval:

```
# Day Sec Modified_Julian_day_time Raw_offset Median_offs Path_delay St Min Max
58043 21705 2017-10-17T06:01:45+00:00 -0.00000129 -0.000000053 0.000007667 1 R -0.01 0.01
```

Example for PTP data files:

```
# Day Sec Modified_Julian_day_time Raw_offset Report_offs Path_delay Portstate
58043 21705 2017-10-17T06:01:45+00:00 -0.000000129 -0.000000053 0.000007667 9
```

Example for PTP data files supporting Mtie feature:

```
# Day Sec Modified_Julian_day_time Raw_offset Median_offs Path_delay St Min Max
58043 21705 2017-10-17T06:01:45+00:00 -0.00000129 -0.000000053 0.000007667 9 M -0.01 0.01
```

10.1.8.21 System Utilization

With the latest SyncMon version it is possible to configure up to 1000 nodes to monitor. The request and logging interval can be set to 1s. Be aware that system CPU will be heavily used in case of high counts of nodes and low request and log-intervals. This could decrease the NTP server performance as well.

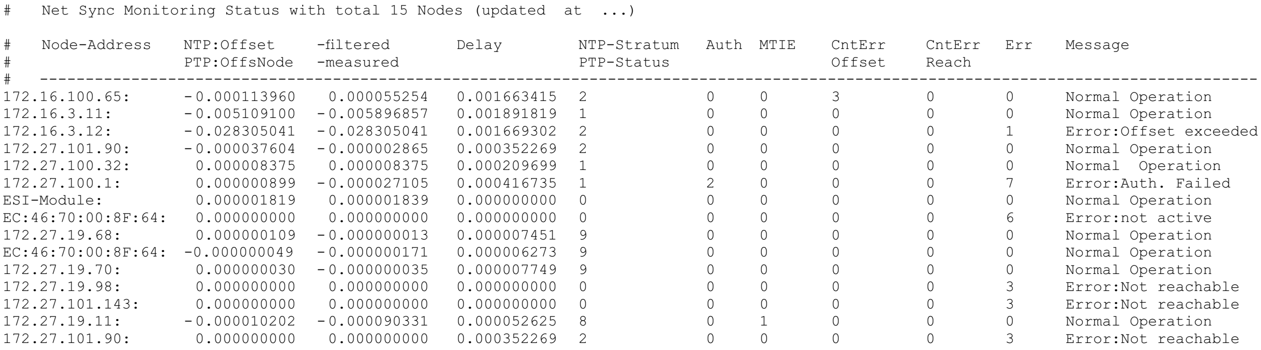
Examples:

- 10 monitoring nodes with log-interval = 1s will store 70MBytes (69194kBytes) per day – the default size of the flash used for SyncMon logging is about 400MB – so 5 days can be stored on internal flash disk.
- 100 monitoring nodes with log-interval = 1s will store 700MB per day – then data logging will stop if the flash is full – the log rotating for SyncMon will be started at 00:00 UTC and will erase data files older than 2 days. The CPU utilization will increase about 10%.
- 100 monitoring nodes with request interval = 1s and log-interval = 64s will store about 12MBytes per day – so about 40 days can be stored on internal flash disk. The CPU utilization will increase about 7%.
- 900 monitoring nodes with request interval = 1s and log-interval = 64s will store about 100MBytes per day – so about 4 days can be stored on internal flash disk. The CPU utilization will increase about 45%
  - this is critical for the NTP server performance of the device.

The size of a data file per day depends on the logging interval and has a size of about 110kB if log-interval is 64s.

10.1.8.22 Sync Monitor Status files via CLI

The current status of the monitored nodes as displayed in the Web-GUI is stored in an ASCII file /var/lo /sync-mon_node_status, updated after every full scan of the configured nodes and can be accessed over CLI.



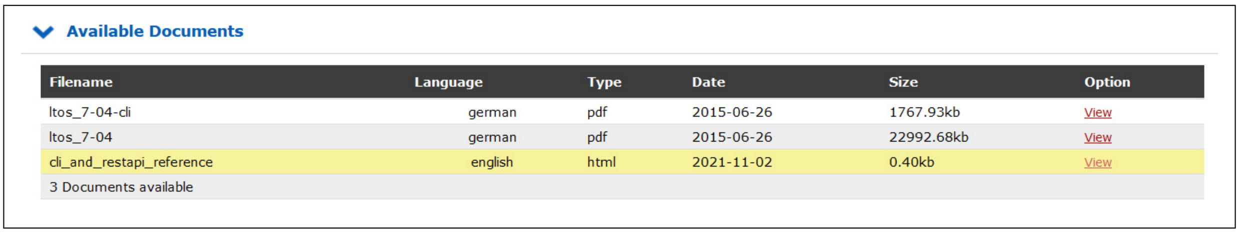
```
#   Net Sync Monitoring Status with total 15 Nodes (updated  at  ...)

#   Node-Address     NTP:Offset    -filtered     Delay         NTP-Stratum   Auth  MTIE   CntErr    CntErr  Err    Message
#                    PTP:OffsNode  -measured                   PTP-Status                  Offset    Reach
#   -------------------------------------------------------------------------------------------------------------------------------
172.16.100.65:      -0.000113960   0.000055254  0.001663415  2             0     0      3         0       0      Normal Operation
172.16.3.11:        -0.005109100  -0.005896857  0.001891819  1             0     0      0         0       0      Normal Operation
172.16.3.12:        -0.028305041  -0.028305041  0.001669302  2             0     0      0         0       1      Error:Offset exceeded
172.27.101.90:      -0.000037604  -0.000002865  0.000352269  2             0     0      0         0       0      Normal Operation
172.27.100.32:       0.000008375   0.000008375  0.000209699  1             0     0      0         0       0      Normal  Operation
172.27.100.1:        0.000000899  -0.000027105  0.000416735  1             2     0      0         0       7      Error:Auth. Failed
ESI-Module:          0.000001819   0.000001839  0.000000000  0             0     0      0         0       0      Normal Operation
EC:46:70:00:8F:64:   0.000000000   0.000000000  0.000000000  0             0     0      0         0       6      Error:not active
172.27.19.68:        0.000000109  -0.000000013  0.000007451  9             0     0      0         0       0      Normal Operation
EC:46:70:00:8F:64:  -0.000000049  -0.000000171  0.000006273  9             0     0      0         0       0      Normal Operation
172.27.19.70:        0.000000030  -0.000000035  0.000007749  9             0     0      0         0       0      Normal Operation
172.27.19.98:        0.000000000   0.000000000  0.000000000  0             0     0      0         0       3      Error:Not reachable
172.27.101.143:      0.000000000   0.000000000  0.000000000  0             0     0      0         0       3      Error:Not reachable
172.27.19.11:       -0.000010202  -0.000090331  0.000052625  8             0     1      0         0       0      Normal Operation
172.27.101.90:       0.000000000   0.000000000  0.000352269  2             0     0      0         0       3      Error:Not reachable
```

Figure: The status information table accessed over a CLI.

Configuration via CLI
The configuration file can be edited with a text editor directly in the command line (CLI) of the system or can be replaced by an external prepared file. Further information can be found in the LANTIME CLI reference.

10.1.9 Documentation and Support

This page provides easy access to some documents stored on your LANTIME, in particular the manuals. The list shows the filename, language, file type, date, and size of the documents/notes.



Available Documents

Filename	Language	Type	Date	Size	Option
ltos_7-04-cli	german	pdf	2015-06-26	1767.93kb	View
ltos_7-04	german	pdf	2015-06-26	22992.68kb	View
cli_and_restapi_reference	english	html	2021-11-02	0.40kb	View
3 Documents available					

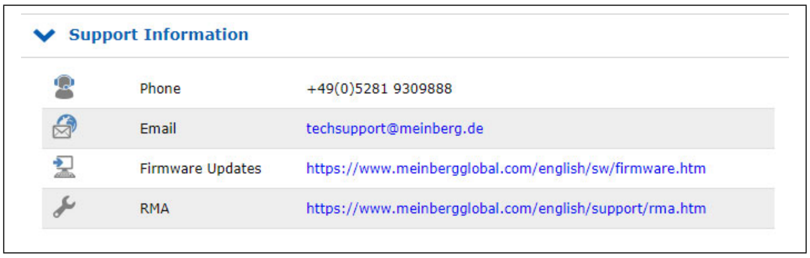
LT_CLI Help
A link to the LT_CLI online help is also provided. This online help is available on all IMS LANTIME devices and on all SyncFire systems with system RAM of at least $\geq$ 512 MB, and can be opened via the link.

For users who do not have such a system, we have made this online help feature accessible from our public web server: http://demo.meinberg.de/lt_cli/.

This CLI help can also also be downloaded as a ZIP archive:
http://demo.meinberg.de/lt_cli/firmware-7.04.008-x86-clihelp.zip.

Once downloaded, the file should be unzipped to your own file system, either in your network environment or on your local PC. Once this is done, the help can be accessed like a normal web page.

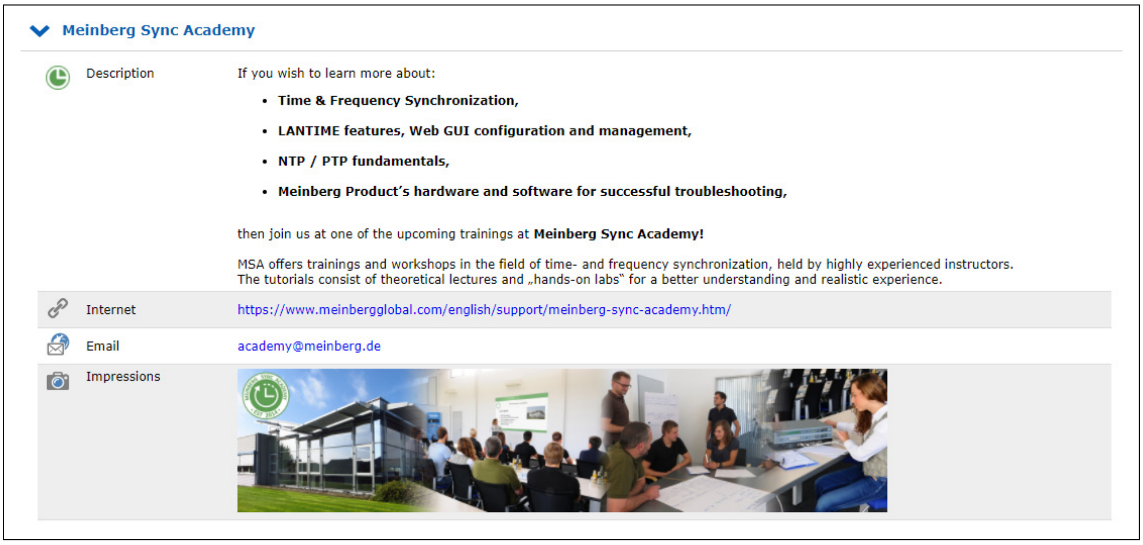
The Support Information chapter provides all necessary information on how to contact Meinberg Technical Support, and also includes a link to Meinberg's firmware update page.



Support Information

Phone	+49(0)5281 9309888
Email	techsupport@meinberg.de
Firmware Updates	https://www.meinbergglobal.com/english/sw/firmware.htm
RMA	https://www.meinbergglobal.com/english/support/rma.htm

The "Docs & Support" tab also provides some important weblinks and contains information about the Meinberg Sync Academy - MSA.



Meinberg Sync Academy

Description	If you wish to learn more about: • **Time & Frequency Synchronization,** • **LANTIME features, Web GUI configuration and management,** • **NTP / PTP fundamentals,** • **Meinberg Product's hardware and software for successful troubleshooting,** then join us at one of the upcoming trainings at **Meinberg Sync Academy!** MSA offers trainings and workshops in the field of time- and frequency synchronization, held by highly experienced instructors. The tutorials consist of theoretical lectures and „hands-on labs" for a better understanding and realistic experience.
Internet	https://www.meinbergglobal.com/english/support/meinberg-sync-academy.htm/
Email	academy@meinberg.de
Impressions	

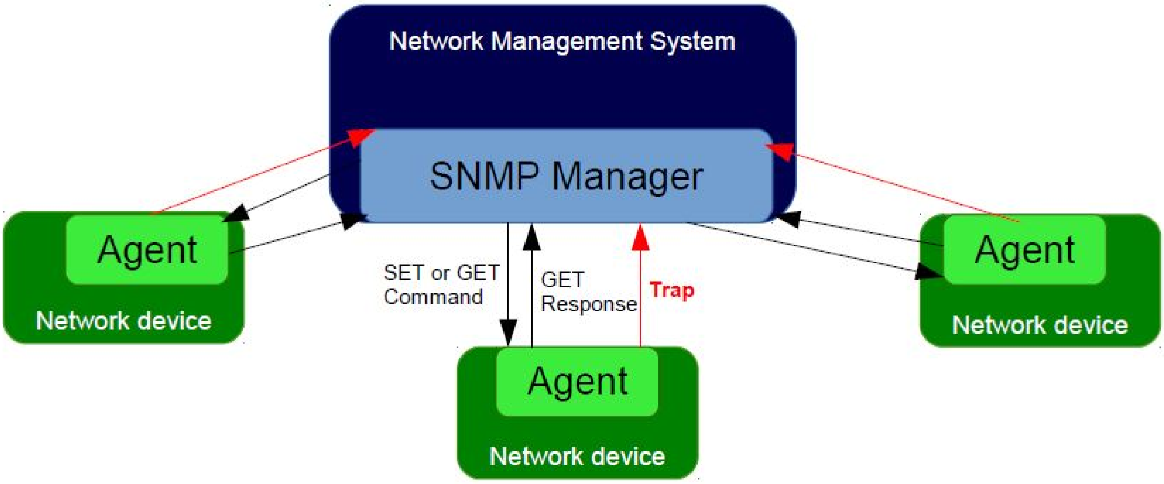
The Meinberg Sync Academy develops and offers training courses in the field of time and frequency synchronization, covering topics such as NTP, IEEE 1588 PTP, and many more. This part of the LANTIME "Docs & Support" tab provides some basic information about the Sync Academy, along with some links to helpful information at: https://www.meinbergglobal.com/english/support/meinberg-sync-academy.htm

10.2 Via SNMP

10.2.1 The Simple Network Managment Protocol

Most network connected devices support a number of management options including the Simple Network Management Protocol, or SNMP. SNMP is a network protocol which allows a single network management system to monitor a large number of devices on the network.

The way it works is each network element has an Agent which communicates with the Manager via SNMP. Each Agent has a corresponding Management Information Base, or MIB. The MIBs organize data elements in a tree structure. It is written in a standard, highly structured language so that the MIBs from all of the devices on the network can be compiled into the same Manager.



MIB elements are called Object Identifiers or OIDs. They consist of configuration variables, status variables, tree structure labels and notifications. The OIDs can be read or changed using SNMP SET and GET commands. There are also recursive commands which allow the Manager to ask for all of the OIDs in a branch (subtree), or even the whole tree. This process is referred to as “walking the MIB”. Event Notifications, commonly referred to as traps, are a special type of OID. A trap can be configured so that when the status of the device changes a message is immediately sent from the Agent to the Manager.

10.2.2 MIB Objects of a LANTIME

An LTOS operating systems running on Meinberg LANTIME servers supports all SNMP versions (v1,v2c and v3) with a full functionality. The LANTIME propriatery OIDs are structured into subtrees, which define a particular system component or a mode of operation. The main subtree with OIDs referring to the LANTIME status of different modes is called LantimeNGStatus, NG standing for New Generation of LANTIME features in the LANTIME firmware. The LantimeNGStatus consists of eight subtrees, where Refclock, NTP, PTP, SystemHardware, Cluster and Misc are the most important to monitor.

10.2.2.1 Refclock subtree

Here is a short list of OIDs from the NGStatus subtree with corresponding descriptions:

mbgLtNgRefclockState
This OID describes a current state of a LANTIME refclock (hardware clock module) referring to GNSS
or any other time source signal in MRS (Multi Reference Source) model.

Status	Description
0:	*refclock is not available:* See the possible troubleshooting: 1. Refclock module cannot be accessed. 2. Check if it is damaged and replace it if necessary.
1:	*synchronized:* The reflock of your system is correctly synchronized to the selected time source (GPS or MRS). In an MRS system, a refclock can be synchronized to a reference time source from the priority list. See an example in the next figure. The MRS system above synchronizes first to GPS, but if the GPS signal is unavailable, the refclock switches to the next time source from the priority list (PTP in our case). The switch happens only after a trust time of the unavailable time source (GPS signal) has run out. This is to prevent hopping from one time source to another in short time periods. If GPS becomes available again, the refclock switches back to GPS, without waiting for the PTP trust time in this case, since GPS itself a higher precision than PTP.
2:	*not synchronized:* Obviously the refclock is not synchronized to its time source. Here is the possible troubleshooting: A) Check if the GPS antenna is connected and reference time received. More about how to mount and position Meinberg GPS antenna correctly learn here. B) If GPS is the current time source, check number of satellites in view. There should be at least four to provide sync information. C) Start “warm boot” to refresh current satellite position. This is useful especially if the physical position of your LANTIME has been displaced by more than 100 km from its previous location and therefore obsolete satellite data are still stored in the system. D) Start "cold boot" to update a satellite almanac. E) If nothing from above helps, the GPS clock module needs to be changed.

```
It is recommended configuring your network management software to check
this status regularly, if possible every 60 s.
```

mbgLtNgRefclockLeapSecondDate
This OID conveys information about the next Leap Second Date. If the upcoming Leap Second Date has not been announced yet, the OID holds information about the previous leap second event.

Here is short summary of the leap seconds. There are two different timescales we usually talk about in the sync environment: GPS, which stands for Global Positioning System time and UTC (Universal Time Co-ordinated), formerly known as GMT (Greenwich Mean Time). They differ from each other by number of leap seconds introduced since beginning of GPS time on 6-Jan-1980. In the moment of writing the UTC is 16 seconds behind the GPS time, which is due to the uneven rotation of the Earth.

```
Since the introduction of a new leap second influences the time in the
whole system being synchronized, we suggest to check this status regularly,
e.g.  1/hour.
```

Next in a row of OIDs are those referring to NTP status. They can be found in the “mbgLtNgNtp” subtree.

10.2.2.2 NTP subtree

Here is a short list of OIDs from the NGStatus subtree with corresponding descriptions:

mbgLtNgNtpCurrentState
This is one of the most important OID in this subtree to check regularly. It informs about the NTP service of your LANTIME. There are three states possible:

Status	Description
0:	*not available:* See the possible troubleshooting: A) Check if NTP service is actually enabled at a given LAN interface. To check it, log in to a webinterface. Factory default credentials: root/timeserver. Go to menus: "Network → Network Services" and activate the service of the corresponding interface. See Figure 3 for details. B) Check if it is damaged and replace it if necessary.
1:	*not synchronized:* In case of "not synchronized" the NTP service is not yet synchronized to a reference clock. Possible causes for this state are as follows: A) NTP daemon is still in its initialization phase for which it needs approx. 3-5 min. Therefore wait a while and see if the status changes. B) If a refclock is not sync, the same is indicated in the NTP status. In such case NTP daemon is switched to synchronize to its local clock and its stratum value changes to 12. Please check the possible troubleshooting for a refclock status as described above.
2.	*synchronized:* The NTP service is in normal operation. The LANTIME is now working properly.

```
It is recommended to check NTP status regularly,
but not more than every 64 s.
```

10.2.2.3 Hardware subtree

mbgLtNgSysPsStatus
If a LANTIME has a redundant power supply (RPS) unit, it is important to check the status of both RPS modules regularly. This PowerSupplyStatus OID can be found in the System Hardware subtree. The following states are available:

Status	Description
0:	*notAvailable:* The queried power supply unit is not recognized by a system. Check to see if it is damaged, and replace it if necessary.
1:	*down:* The power supply unit of interest is not in service. Check to see if it is damaged, and replace it if necessary.
2:	*up:* The queried power supply module is in operation.

```
It is recommended to check this OID every 60 s.
```

10.2.2.4 Misc subtree

mbgLtNgEthPortLinkState
In the mbgLtNgMisc subtree one can find an EthPortLinkState OID which identifies the status of each physical Ethernet port of a LANTIME. Available values:

Status	Description
0:	*notAvailable:* The queried port is down, check the link LED. If faulty, replace the network card.
1:	*up:* The port of interest is in normal operation.

```
It is recommended to check this OID every 60 s.
```

10.2.2.5 PTP subtree

If your LANTIME has IEEE 1588 PTPv2 functionality, the corresponding PTP OIDs can be found in the "mbgLtNgPtp" subtree. These are the most important OIDs to monitor:

mbgLtNgPtpPortState
The following PTP Port States are possible:

Status	Description
0:	*uninitialized:* The port is booting up, the software daemon has not yet started, the IP address is not yet assigned.
1:	*initializing:* In this state the port initializes its data sets, hardware, and communication facilities.
2:	*faulty:* Not defined in a LANTIME.
3:	*disabled:* PTP service has been disabled on this port, either by user configuration or because the module is in a standby mode.
4:	*listening:* The port is waiting for the announceReceiptTimeout to expire or to receive an Announce message from a master.
5:	*preMaster:* A short transitional state while the port is becoming a master.
6:	*master:* The port is a current master.
7:	*passive:* The port is in passive mode, meaning there is another master clock active in the PTP domain. The port can enter master state when it wins the BMCA due to a failure/service degradation of the current master.
8:	*uncalibrated:* One or more master ports have been detected in the domain.
9:	*slave:* The port has successfully subscribed to a master and receives all expected messages. It also successfully measured the path delay using delay request messages.

```
It is recommended to monitor the PtpPortState OID every 3 s
```

10.2.3 SNMP Traps

SNMP Trap Name:	mbgLtNgTrapNTPNotSync
OID:	.1.3.6.1.4.1.5597.30.3.0.1
Severity:	Warning or critical
Short explanation:	the trap is sent when NTP is not synchronized
Reference to other chapters:	Troubleshooting and Alarming → NTP Messages → NTP Not Sync
Cleared By:	mbgLtNgTrapNTPSync

SNMP Trap Name:	mbgLtNgTrapNTPStopped
OID:	.1.3.6.1.4.1.5597.30.3.0.2
Severity:	Critical
Short explanation:	trap to be sent when NTP is stopped
Reference to other chapters:	Troubleshooting and Alarming → NTP Messages → NTP Stopped
Cleared By:	MbgLtNgTrapNTPSync or mbgLtNgTrapNTPNotSync

SNMP Trap Name:	mbgLtNgTrapServerBoot
OID:	.1.3.6.1.4.1.5597.30.3.0.3
Severity:	Info
Short explanation:	trap to be sent when time server has finished boot sequence
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapReceiverNotResponding
OID:	.1.3.6.1.4.1.5597.30.3.0.4
Severity:	Critical
Short explanation:	trap to be sent when receiver is not responding
Reference to other chapters:	Troubleshooting and Alarming → Reference Clock → CLK Not Rsponding
Cleared By:	MbgLtNgTrapReceiverNotSync or mbgLtNgTrapReceiverSync

SNMP Trap Name:	mbgLtNgTrapReceiverNotSync
OID:	.1.3.6.1.4.1.5597.30.3.0.5
Severity:	Error
Short explanation:	trap to be sent when receiver is not synchronised
Reference to other chapters:	Troubleshooting and Alarming → Reference Clock → CLK Not Sync
Cleared By:	mbgLtNgTrapReceiverSync

SNMP Trap Name:	mbgLtNgTrapAntennaFaulty
OID:	.1.3.6.1.4.1.5597.30.3.0.6
Severity:	Critical
Short explanation:	trap to be sent when connection to antenna is broken
Reference to other chapters:	Troubleshooting and Alarming → Reference Clock → Antenna Faulty
Cleared By:	mbgLtNgTrapAntennaReconnect

SNMP Trap Name:	mbgLtNgTrapAntennaReconnect
OID:	.1.3.6.1.4.1.5597.30.3.0.7
Severity:	Clearing event
Short explanation:	trap to be sent when antenna has been reconnected
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapConfigChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.8
Severity:	Info
Short explanation:	trap to be sent when timeserver reloaded its configuration
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapLeapSecondAnnounced
OID:	.1.3.6.1.4.1.5597.30.3.0.9
Severity:	Info Warning
Short explanation:	trap to be sent when a leap second has been announced
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → Leap Second Announced LTOS 6 Managm./Mon. → NTP → Leap Second Handling
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitError
OID:	.1.3.6.1.4.1.5597.30.3.0.10
Severity:	Critical
Short explanation:	trap to be sent when SHS timelimit exceeded
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → SHS Time Limit Warning LTOS 6 Managm./Mon. → Web GUI → Introduction LTOS 6 Managm./Mon. → Web GUI → Security → SHS Mode LTOS 6 Managm./Mon. → Web GUI → Security → SHS Time Limit
Cleared By:	mbgLtNgTrapSHSTimeLimitOk

SNMP Trap Name:	mbgLtNgTrapSecondaryRecNotSync
OID:	.1.3.6.1.4.1.5597.30.3.0.11
Severity:	Warning
Short explanation:	trap to be sent when secondary receiver is not synchronised
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → CLK Not Sync
Cleared By:	mbgLtNgTrapSecondaryRecSync

SNMP Trap Name:	mbgLtNgTrapPowerSupplyFailure
OID:	.1.3.6.1.4.1.5597.30.3.0.12
Severity:	Critical
Short explanation:	trap to be sent when one of the redundant power supplies fails
Reference to other chapters:	Important Safety Information → Security during Installation Important Safety Information → Safety during Operation
Cleared By:	mbgLtNgTrapPowerSupplyUp

SNMP Trap Name:	mbgLtNgTrapAntennaShortCircuit
OID:	.1.3.6.1.4.1.5597.30.3.0.13
Severity:	Critical
Short explanation:	trap to be sent when a connected antenna fails due to a short circuit
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → Antenna Short Circuit
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapReceiverSync
OID:	.1.3.6.1.4.1.5597.30.3.0.14
Severity:	Clearing event
Short explanation:	trap to be sent when receiver is synchronised
Reference to other chapters:	Antenna and Receiver Information → Reference Time Sources
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapNTPClientAlarm
OID:	.1.3.6.1.4.1.5597.30.3.0.15
Severity:	Error
Short explanation:	trap to be sent when an NTP Client Monitoring alarm occurs, e.g. when a monitored client is not reachable
Reference to other chapters:	check the network configuration in LTOS 6 Managm./Mon. → Network
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapPowerSupplyUp
OID:	.1.3.6.1.4.1.5597.30.3.0.16
Severity:	Info
Short explanation:	trap to be sent when a power supply returned to a healthy state
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapNetworkDown
OID:	.1.3.6.1.4.1.5597.30.3.0.17
Severity:	Critical
Short explanation:	trap to be sent when a monitored network port is down
Reference to other chapters:	Troubleshooting and Alarming → Network → Network Link Down
Cleared By:	mbgLtNgTrapNetworkUp

SNMP Trap Name:	mbgLtNgTrapNetworkUp
OID:	.1.3.6.1.4.1.5597.30.3.0.18
Severity:	Clearing event
Short explanation:	trap to be sent when a monitored network port is up
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapSecondaryRecNotRespp
OID:	.1.3.6.1.4.1.5597.30.3.0.19
Severity:	Warning or critical
Short explanation:	trap to be sent when secondary receiver is not responding
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → CLK Not Responding
Cleared By:	mbgLtNgTrapSecondaryRecSync

SNMP Trap Name:	mbgLtNgTrapMrsLimitExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.30
Severity:	Warning
Short explanation:	trap to be sent when a reference offset exceeds the configured limit
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → Clock → MRS Settings Troubleshooting and Alarming → Ref. Clock → MRS Limit Exceed
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapMrsRefDisconnect
OID:	.1.3.6.1.4.1.5597.30.3.0.31
Severity:	Critical
Short explanation:	trap to be sent when a reference signal has been lost
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → MRS Reference Disconnected
Cleared By:	mbgLtNgTrapMrsRefReconnect

SNMP Trap Name:	mbgLtNgTrapMrsRefReconnect
OID:	.1.3.6.1.4.1.5597.30.3.0.32
Severity:	Clearing event
Short explanation:	trap to be sent when a reference signal recovered
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapFdmError
OID:	.1.3.6.1.4.1.5597.30.3.0.33
Severity:	Critical
Short explanation:	trap to be sent when the Fdm module generates an alarm
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → FDM → FDM Configuration
Cleared By:	mbgLtNgTrapFDMOk

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitWarning
OID:	.1.3.6.1.4.1.5597.30.3.0.34
Severity:	Warning Critical
Short explanation:	trap to be sent when SHS warning limit exceeded
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → Introduction LTOS 6 Managm./Mon. → Web GUI → Security → SHS Configuration LTOS 6 Managm./Mon. → Web GUI → Security → SHS Mode Troubleshooting and Alarming → Ref. Clock → SHS Time Limit Warning
Cleared By:	mbgLtNgTrapSHSTimeLimitOk

SNMP Trap Name:	mbgLtNgTrapSecondaryRecSync
OID:	.1.3.6.1.4.1.5597.30.3.0.35
Severity:	Clearing event
Short explanation:	trap to be sent when secondary receiver is synchronised
Reference to other chapters:	Antenna and Receiver Information → Reference Time Sources
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapNTPSync
OID:	.1.3.6.1.4.1.5597.30.3.0.36
Severity:	Clearing event
Short explanation:	trap to be sent when NTP is synchronised
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapPtpPortDisconnected
OID:	.1.3.6.1.4.1.5597.30.3.0.37
Severity:	Warning or critical
Short explanation:	trap to be sent when PTP network port got disconnected
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → PTP → PTP Global Status
Cleared By:	mbgLtNgTrapPtpPortConnected

SNMP Trap Name:	mbgLtNgTrapPtpPortConnected
OID:	.1.3.6.1.4.1.5597.30.3.0.38
Severity:	Clearing event
Short explanation:	trap to be sent when PTP network port got connected
Reference to other chapters:	no further Information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapPtpStateChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.39
Severity:	Info Warning
Short explanation:	trap to be sent when PTP state changed (e.g. from 'passive' to 'master')
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → PTP → PTP Global Status
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapPtpError
OID:	.1.3.6.1.4.1.5597.30.3.0.40
Severity:	Warning Critical
Short explanation:	trap to be sent when PTP raised an error
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → PTP → PTP Global Status
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapLowSystemResources
OID:	.1.3.6.1.4.1.5597.30.3.0.41
Severity:	Clearing event
Short explanation:	trap to be sent when system is running on low resources
Reference to other chapters:	no further information
Cleared By:	mbgLtNgTrapSufficientSystemResources

SNMP Trap Name:	mbgLtNgTrapFanDown
OID:	.1.3.6.1.4.1.5597.30.3.0.45
Severity:	Critical
Short explanation:	trap to be sent when fan goes down
Reference to other chapters:	Troubleshooting and Alarming → Miscellaneous → Fan Failure
Cleared By:	mbgLtNgTrapFanUp

SNMP Trap Name:	mbgLtNgTrapFanUp
OID:	.1.3.6.1.4.1.5597.30.3.0.46
Severity:	Clearing event
Short explanation:	trap to be sent when fan comes up
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapCertificateExpired
OID:	.1.3.6.1.4.1.5597.30.3.0.47
Severity:	Info or warning
Short explanation:	trap to be sent when HTTPS certificate expires or will expire
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → Security → HTTPS Certificate
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapSufficientSystemResources
OID:	.1.3.6.1.4.1.5597.30.3.0.48
Severity:	Clearing event
Short explanation:	trap to be sent when system has regained sufficient resources
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapOscillatorWarmedUp
OID:	.1.3.6.1.4.1.5597.30.3.0.49
Severity:	Clearing event
Short explanation:	trap to be sent when oscillator is warmed up
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapOscillatorNotWarmedUp
OID:	.1.3.6.1.4.1.5597.30.3.0.50
Severity:	Info
Short explanation:	trap to be sent when oscillator is not warmed up
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → Oscillator not Adjusted
Cleared By:	mbgLtNgTrapOscillatorWarmedUp

SNMP Trap Name:	mbgLtNgTrapMrsRefChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.51
Severity:	Info Warning
Short explanation:	trap to be sent when MRS reference source changed
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapClusterMasterChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.52
Severity:	Warning
Short explanation:	trap to be sent when cluster mode is active and cluster changed
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → Network → Network Interf. - Cluster
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapClusterFalsetickerDetected
OID:	.1.3.6.1.4.1.5597.30.3.0.53
Severity:	Warning
Short explanation:	trap to be sent when cluster mode is active and a cluster member is dectected as falseticker
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → Network → Network Interf. - Cluster
Cleared By:	mbgLtNgTrapClusterFalsetickerCleared

SNMP Trap Name:	mbgLtNgTrapClusterFalsetickerCleared
OID:	.1.3.6.1.4.1.5597.30.3.0.54
Severity:	Clearing event
Short explanation:	trap to be sent when cluster mode is active and a cluster member is no longer a falseticker
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitOk
OID:	.1.3.6.1.4.1.5597.30.3.0.55
Severity:	Info
Short explanation:	trap to be sent when SHS timelimit error has been acknowledged or time difference drops below warning limit
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → Introduction
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapIMSError
OID:	.1.3.6.1.4.1.5597.30.3.0.56
Severity:	Critical
Short explanation:	trap to be sent when an IMS module is not responsive anymore has got temperature issues, etc.
Reference to other chapters:	Troubleshooting and Alarming → Miscellaneous → IMS Error
Cleared By:	mbgLtNgTrapIMSOk

SNMP Trap Name:	mbgLtNgTrapIMSOk
OID:	.1.3.6.1.4.1.5597.30.3.0.57
Severity:	Clearing event
Short explanation:	trap to be sent when an IMS module returns to healthy state
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapFDMOk
OID:	.1.3.6.1.4.1.5597.30.3.0.58
Severity:	Clearing event
Short explanation:	trap to be sent when an FDM module returns to healthy state
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → FDM → FDM Configuration
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapNTPOffsetLimitExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.59
Severity:	Error
Short explanation:	trap to be sent when monitoring an NTP client and its offset limit is exceeded
Reference to other chapters:	Troubleshooting and Alarming → NTP → NTP Offset Limit Exceeded
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapNTPOffsetLimitOk
OID:	.1.3.6.1.4.1.5597.30.3.0.60
Severity:	Info
Short explanation:	trap to be sent when monitoring an NTP client and its offset limit is back again in a valid range
Reference to other chapters:	no further information
Cleared By:	mbgLtNgTrapNTPOffsetLimitExceeded

SNMP Trap Name:	mbgLtNgTrapXheRubError
OID:	.1.3.6.1.4.1.5597.30.3.0.61
Severity:	Info
Short explanation:	trap to be sent when external rubidium announces OK
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapXheRubError
OID:	.1.3.6.1.4.1.5597.30.3.0.62
Severity:	Error
Short explanation:	trap to be sent when external rubidium announces error
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapPowerConsumptionExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.63
Severity:	Warning
Short explanation:	trap to be sent when device consumes too much power
Reference to other chapters:	no further information
Cleared By:	mbgLtNgTrapPowerConsumptionOk

SNMP Trap Name:	mbgLtNgTrapPowerConsumptionOk
OID:	.1.3.6.1.4.1.5597.30.3.0.64
Severity:	Info
Short explanation:	trap to be sent when device has got enough power
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapPowerRedundancyNotAvail
OID:	.1.3.6.1.4.1.5597.30.3.0.65
Severity:	Warning
Short explanation:	trap to be sent when there currently is no power supply backup avail
Reference to other chapters:	no further information
Cleared By:	mbgLtNgTrapPowerRedundancyAvail

SNMP Trap Name:	mbgLtNgTrapPowerRedundancyAvail
OID:	.1.3.6.1.4.1.5597.30.3.0.66
Severity:	Info
Short explanation:	trap to be sent when there is at least one power supply as backup
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapTrustedSourceError
OID:	.1.3.6.1.4.1.5597.30.3.0.67
Severity:	Warning
Short explanation:	trap to be sent when a MRS source's time deviation exceeds a configured limit
Reference to other chapters:	no further information
Cleared By:	mbgLtNgTrapTrustedSourceOk

SNMP Trap Name:	mbgLtNgTrapTrustedSourceOk
OID:	.1.3.6.1.4.1.5597.30.3.0.68
Severity:	Clearing Event
Short explanation:	trap to be sent when a MRS source's time deviation returns to its configured bounds
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapNormalOperation
OID:	.1.3.6.1.4.1.5597.30.3.0.77
Severity:	Clearing event
Short explanation:	trap to be sent when the system returned to a healthy state
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapHeartbeat
OID:	.1.3.6.1.4.1.5597.30.3.0.88
Severity:	Info
Short explanation:	trap to be sent periodically to indicate that time server is still alive
Reference to other chapters:	LTOS 6 Managm./Mon. → Notifications → Miscellaneous - Enable Heartbeat
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapTestNotification
OID:	.1.3.6.1.4.1.5597.30.3.0.99
Severity:	Info
Short explanation:	trap to be sent when a test notification has been requested
Reference to other chapters:	no further information
Cleared By:	-

11 Troubleshooting and Alarming

11.1 NTP Messages

Error and System message / Explanation	Troubleshooting / Additional information
NTP Not Sync / The NTP service of a LANTIME is not sync.	• For LANTIMEs with built-in reference clock, please check the status of the clock on the main page. If the reference clock is not synchronized, please refer to the troubleshooting information for "CLK Not Sync". • For LANTIMEs, which are to be synchronized by external NTP servers, make sure that the external NTP servers are reachable. • For MRS devices, check whether MRS reference time sources are configured in the Web interface (→ Clock → MRS settings) and corresponding signals are available (→ Clock → MRS status). • Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.
NTP Stopped / The NTP service stopped	• Info: After every configuration change relevant to the NTP, the NTP service is stopped and restarted. In this case, a message 'NTP Stopped' is written into the system log of the LANTIME. • Contact the Meinberg TechSupport and provide a LANTIME diagnostic file, if 'NTP Stopped' is permanently displayed as NTP status in the front panel or in the web interface.
NTP Offset Limit Exceeded / LANTIME generates this message if the internal time offset between LANTIME system time and the reference clock is higher than the configured threshold value.	• Check the configured threshold value in the Web Interface: "NTP → Special Settings → Max. Internal Offset (ms.)“ • Note: After restarting the LANTIME it takes several minutes, depending on the reference time source, until the internal offset is < ±1 ms. • Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

11.2 Ref. Clock Messages

Error and System message / Explanation

Troubleshooting / Additional information

CLK Not Responding /
The LANTIME can no longer communicate with its internal reference clock.

- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file.

CLK Not Sync /
Performance and system ressources
issue of the NTP

LANTIME with GNSS reference clock (GPS/GLN/GNS):

- Check the antenna position:
- If the GPS reference clock is connected to a GPS antenna distributor GPSAV4 (https://www.meinbergglobal.com/english/products/gps-antenna-distributor.htm), make sure that the "Clock 1" port of the GPSAV4 is attached , since the GPSAV4 and the antenna are supplied by power via this port.

LANTIME with a longwave receiver (DCF77-PZF/WWVB/MSF/JJY):

- Check the antenna position

LANTIME with TCR reference clock (IRIG):

- Check whether the timecode input port at the back of the LANTIME is correctly connected to an IRIG source. In the Web interface, check whether the correct IRIG input code has been configured (Clock → IRIG Settings → Input Timecode). The input timecode is the IRIG code provided to the LANTIME by the IRIG source.
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

Antenna Faulty /
GNSS reference clock (GPS/GLN/GNS):
The antenna has not been detected.

- Check the connections between the antenna and a LANTIME.
- Check the output voltage at the LANTIME antenna connector.
- To do this, disconnect the antenna cable from the LANTIME antenna port. The following voltage value should
- be measured between the inner and outer conductor:
  - GPS Receiver → 15-18 V DC
  - GLN Receiver → 5V DC
  - GNS Receiver → 5V DC
- If the voltage is 0V DC, please contact the Meinberg TechSupport:
- If the measured voltage at the antenna port of the LANTIME is correct, reconnect the antenna cable and
- check the voltage at the other end of the antenna cable.
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

Longwave receiver (DCF77-PZF/WWVB/MSF/JJY):
Either the antenna or any other input signal has not been detected.

- Check the connections between the antenna and a LANTIME.
- Check the status of the received antenna signal in the main page of the web interface. The displayed field strength value should be > 40. If this is not the case, please check how the antenna is positioned.
- Check the output voltage at the LANTIME antenna connector.
- To do this, disconnect the antenna cable from the LANTIME antenna port. The following voltage value should be measured between the inner and outer conductor: Long Wave Receiver → 5 V DC
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

Antenna Short Circuit / Short circuit at the antenna connection.	• Disconnect the antenna cable from the LANTIME antenna connector. • Perform a powercycle of the device • If the LANTIME does not show the error message after the start-up, connect the antenna again. Otherwise contact the Meinberg TechSupport and provide a LANTIME diagnostic file.
GPS Warm Boot / In warm boot mode, the GPS reference clock performs the position determination. To complete this process successfully, at least 4 satellites should be received. After successful position determination, the position will be stored in the battery-buffered memory of the clock. Thus the position determination does not to be carried out again after a restart.	• If the LANTIME can not complete the GPS warm boot process, check the number of "good satellites" that can be viewed in the web interface: "Clock → GPS (GNSS Clock → Receiver Information → Number of good satellites". • If the number of good satellites is permanently below 4 and the LANTIME can not complete the position determination, then refer to the troubleshooting case for "CLK Not Sync". • Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.
GPS Cold Boot / In GPS Cold Boot mode, the GPS reference clock tries to download the GPS almanac, which contains the satellite track data for all satellites. To complete this process, at least 1 satellite should be received. The process takes at least 12 minutes. After the cold boot is completed, the clock automatically switches to the GPS warm boot to determine the position. The GPS almanac is stored in the battery-buffered memory of the clock.	• If the LANTIME can not complete the GPS Cold Boot operation after more than 30 minutes, check the number of "good satellites" in the web interface: "Clock → GPS (GNSS Clock → Receiver Information → Number of good satellites". • If the number of good satellites is 0, then refer to the troubleshooting case for "CLK Not Sync". • Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

SHS Time Limit Warning /
LANTIME systems with two built-in reference clocks send out this message as soon as the time difference between both clocks exceeded the pre-configured "Time Limit Warning Level" setting.

- Check the current time difference between the two reference clocks in the main menu of the web interface.
- Check your SHS configuration under "Security → SHS Configuration". Are the configured thresholds possibly too strict?
- Check the status of both reference clocks in the main menu of the web interface. If one of the two clocks is not synchronized, please refer to the troubleshooting case for "CLK Not Sync".
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

Oscillator not Adjusted /
The internal oscillator is not (yet) fully disciplined. As soon as this process is finished, the LANTIME sends out a log message "Oscillator Adjusted". The time needed for an oscillator to be disciplined depends on the quality of the incoming signal, the aging and environmental influences on the oscillator.

- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

Leap Second Announced /
LANTIMEs with a GNSS reference clock (GPS / GLN / GNS) or long wave receiver (DCF77-PZF / WWVB / MSF / JJY) send out the "Leap Second Announced" notification message as soon as they have received the announcement by the reference signal. The GPS satellites announce the upcoming leapsecond usually about half a year in advance. Long wave transmitters usually send the announcement 1 hour in advance.

- This is only an info notification, therefore no further action is required.

XMR Limit Exceed /
LANTIME generates this message when the measured time offset of an MRS time source has exceeded the configured threshold value.

- Check the current MRS time source status in the Web Interface under "Clock → GNSS Clock → MRS Status".
- Check the MRS configuration in the Web Interface under "Clock → GNSS Clock → MRS Settings". Are the configured threshold values (check the "Limit" column) configured possibly too strict?
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

XMR Reference Disconnected /
LANTIME generates this message if the configured MRS time source is no longer available.

- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

11.3 Network Messages

Error and System message / Explanation

Troubleshooting / Additional information

Network Link Down /
There was no link detected at one of the LANTIME's network interface.

- Check which ports are physically connected and the link should be available.
- Check for compatible network settings on switch and LANTIME.
- Check the settings for link monitoring via the Web Interface: "Network → Physical Network Configuration → Indicate Link on Front Panel LED".
  - The LANTIME monitors a link status for the ports where the "Indicate Link on Front Panel LED" option is activated.
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

11.4 Miscellaneous Messages

Error and System message / Explanation

Troubleshooting / Additional information

Fan Failure /
The LANTIME has detected a fault on a fan module, or a fan module has been removed during system operation.

- If the fan module has not been intentionally removed, contact the Meinberg TechSupport and provide a LANTIME diagnostic file.

IMS Error /
Either the LANTIME has detected an error on an IMS module or an IMS module has been plugged out of the LANTIME IMS system during the operation.

Troubleshooting / Additional information

- If the IMS module has not been intentionally removed, contact the Meinberg TechSupport and provide a LANTIME diagnostic file.

CPU No Response (This error message can only appear on a display) /
The display does not receive any information from the installed LANTIME CPU unit.

Troubleshooting / Additional information

- Check whether the LANTIME is still available over the network (try to ping, SSH, HTTP / HTTPS)
- Does a power cycle solve this problem?
- If the LANTIME is still accessible via HTTP / HTTPS, please download a diagnostic file via the web interface and send it to the Meinberg TechSupport. If no connection to the LANTIME is possible, contact the Meinberg TechSupport with the serial number of your LANTIME.

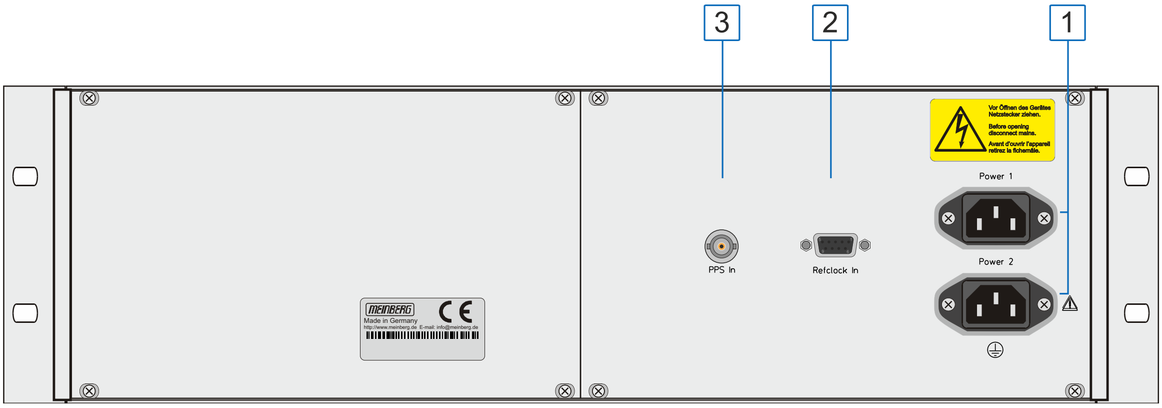
Certificate Expired /
LANTIME generates this warning 60 days, 30 days, and 15 days before the end period of the installed SSL certificate for HTTPS service.

Troubleshooting / Additional information

- Check the validity of the installed SSL certificate via the Web Interface: "Security → HTTPS Certificate → Show SSL Certificate".
- Upload a new SSL certificate using the LANTIME Web Interface in the Security Page dialogue.: "Security → HTTPS Certificate → Upload SSL Certificate".
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

Low System Resource / LANTIME generates this warning: directory "/var" < 1MB free directory "/var" > 90% usage RAM Mem free < 6MB	**Troubleshooting / Additional information** • Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance for solving the problem.

12 Attachment: Technical Information


3
2
1
Vor Öffnen des Gerätes Netzstecker ziehen.
Before opening disconnect mains.
Avant d'ouvrir l'appareil retirez la fichemâle.
Power 1
Power 2
PPS In
Refclock In
MEINBERG
Made in Germany
http://www.meinberg.de E-mail: info@meinberg.de

ENGLISH

1. Power supply connector
2. Refclock Input, DSUB-9 conncetor
3. PPS Input, BNC female

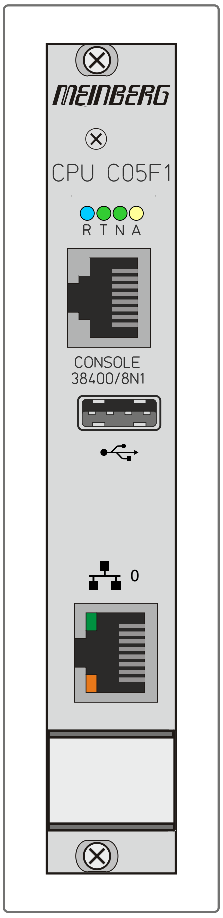
DEUTSCH

1. Spannungsversorgung
2. Refclock Eingang, DSUB-9 Anschluss
3. PPS Eingang, BNC Buchse

12.1 LAN-CPU Time Server Module

The LAN-CPU module is a complete single-board computer with LINUX operating system and pre-installed NTP server. The board can be integrated into various GNSS, DCF77, WWVB, MSF or IRIG systems from Meinberg to expand them to a NTP Stratum 1 server.

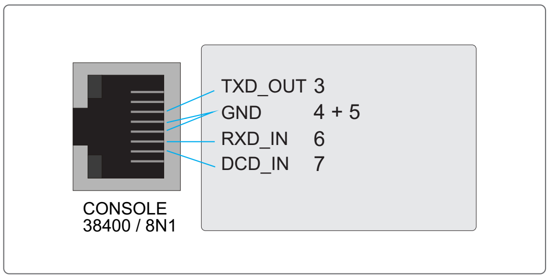
The system allows various management and configuration methods which can be activated/deactivated individually for security reasons: Web interface (HTTP/HTTPS), text-based setup program (TELNET/SSH) and SNMP. Firmware updates can be easily carried out via the Web interface.



Technical specifications LAN-CPU

CPU Module Type:	C05F1
Processor:	Geode^{TM} LX800 with 500 MHz
Main Memory:	256 MB
Cache Memory:	16 KB 2nd Level Cache
Flash Disk:	1 GB
Signal:	100BASE-T
Data transmission rate:	10/100 Mbit/s
Connection type:	8P8C (RJ45)
Cable:	Copper twisted pair, e.g. CAT 5.0
Duplex Modes:	Half/Full/Autonegotiaton

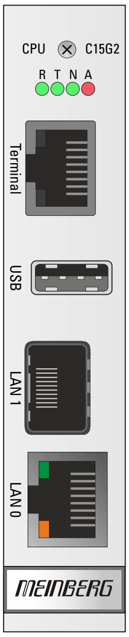
To connect a serial terminal (according to the device model), use the RJ45 connector of the LAN-CPU. Via the serial terminal connection it is possible to configure parameters with a command line interface. You have to use a CAB-CONSOLE-RJ45 cable to establish a connection to your PC or Laptop computer. You can use e.g. the standard Hyperterminal program shipped with your Windows operating system. Configure your terminal program with 38400 Baud, 8 Databits, no parity and 1 Stopbit. The terminal emulation have to set to VT100. After connecting to the timeserver there will be displayed the login message (press RETURN for first connection:



Default User: *root*; Password: *timeserver*

12.2 Technical Specifications - IMS CPU-C15G2

As the central management and control element, the CPU module in an LANTIME system is responsible for management, configuration and alarm notifications. It additionally provides NTP and SNTP services on its network interface. The CPU-C15G2 is equipped with two integrated network interfaces, additional network ports can be added by installing LNE modules.



Processor:	Intel® Atom^{TM} Processor E Series (2 Cores, 1.33GHz, TDP 3W)
Main Memory:	onboard 2 GB
Cache Memory:	1MB 2nd Level Cache
Flash Disk:	4 GB
Network Connector:	1 x 10/100/1000 Base-T with RJ45-Jack 1 x 1000Base-T with SFP-Jack
Serial Interface:	RJ45 connector console: 38400 / 8N1, connection via CAB-CONSOLE cable
USB Port:	install firmware upgrades backup and restore configuration files copy security keys lock / unlock front keys
Operating System:	GNU/Linux 4.x
State LEDs:	**LAN 0 Interface** LED - Connect, Activity and Speed of the network connection LAN-CPU R - Reference Time T - Time Service N - Network A - Alarm

Supported Protocols:

Network Time Protocol (NTP):	NTP v2 (RFC 1119), NTP v3 (RFC 1305), NTP v4 (RFC 5905) SNTP v3 (RFC 1769), SNTP v4 (RFC 4330)
OSI Layer 2 (Data Link Layer):	PRP (IEC 62439-3)
OSI Layer 3 (Network Layer):	IPv4, IPv6
OSI Layer 4 (Transport Layer):	TCP, UDP, TIME (RFC 868), DAYTIME (RFC 867), SYSLOG
OSI Layer 7 (Application Layer):	HTTP / HTTPS (RC 2616), DHCP, FTP, NTPv3 / NTPv4, SNTP, RADIUS, TACACS, FTP, SSH (incl. SFTP, SCP) - SSH v1.3 / SSH v1.5 / SSH v2 (OpenSSH), SNMPv1 (RFC 1157) / SNMPv2c (RFC 1901-1908) / SNMP v3 (RFC 3411-3418), Telnet (RFC 854-RFC 861)

Environmental:

Ambient Temperature:	0 ... 50°C / 32 ... 122°F
Humidity:	Max. 85%

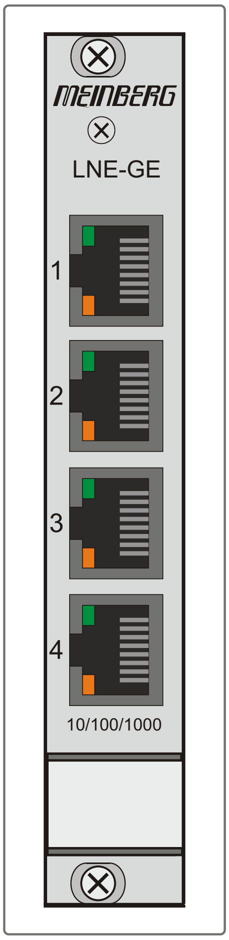
12.3 LNE-GbE: Additional Ethernet Ports

LANTIME Network Expansion LNE, additional network ports for LANTIME Time Server with Gigabit support.

Description

The board LNE-GbE is used to extend the LANTIME NTP server by four additional network connections. Thus the standard functions of the LANTIME are available to further separated (autarkic) networks.

The additional ports can be used to provide time synchronization to separate networks or - by using a feature called "bonding" - to configure redundant network connections (note: the involved active network components like switches have to support this).



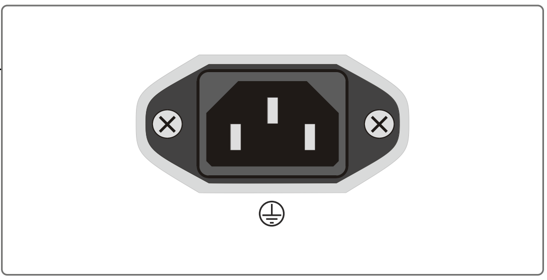
Output signal	1000BASE-T
Data transmission rate:	10/100/1000 Mbit/s
Connector Type:	8P8C (RJ45)
Cable:	Copper twisted pair, e.g. CAT 5.0

There are 7 modes available:
- Autosensing
- 10 Mbit/Half Duplex
- 100 Mbit/Half-Duplex
- 1000 Mbit/Half-Duplex (Gigabit Support)
- 10MBit/Full-Duplex
- 100 Mbit/Full-Duplex
- 1000 Mbit/Full-Duplex (Gigabit Support)

Configuration can be done via display menu or web interface.

12.4 Power Connector

Connector Type: IEC320 AC inlet



Input Parameter

Nominal Voltage Range:	U_N	=	100-240 V∼
	U_N	=	100-200 V ⎓
Maximum Voltage Range:	U_{max}	=	90-265 V∼
	U_{max}	=	90-250 V ⎓
Nominal Current:	I_N	=	0.50 A
Nominal Frequency Range:	f_N	=	50-60 Hz
Maximum Frequency Range:	f_{max}	=	47-63 Hz

Output Parameter

Maximum Power:	P_{max}	=	50 W
Max. Wärmeabgabe:	E_{therm}	=	180.00 kJ/h (170.61 BTU/h)

WARNING!
This equipment is operated at a hazardous voltage.

Danger of death from electric shock!

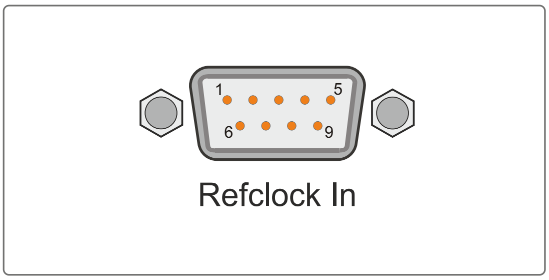
- This device must be connected by qualified personnel (electricians) only.
- Never handle exposed terminals or plugs while the power is on.
- All connectors must provide protection against contact with live parts in the form of a suitable plug body!

- Note: Always ensure that wiring is safe!

- Important: The device must be grounded by means of a connection with a correctly installed protective earth conductor (PE).

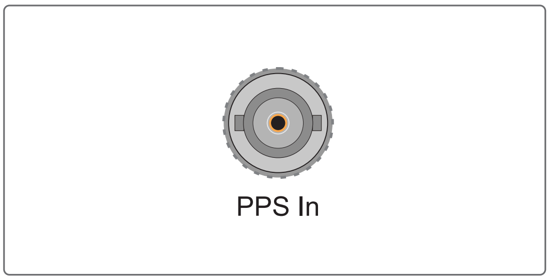
12.5 Refclock In

Signal:	Reference, RS-232
Connection type:	D-SUB male 9pol.
Cable:	shielded data line
Assignment:	
Pin 1:	PPS (optional)
Pin 2:	RxD
Pin 5:	GND



12.6 PPS In

Cable:	shielded coaxial line
pulse length:	$>= 5\mu$s, active high
Connector:	BNC female



13 Appendix

13.1 Time Telegrams

13.1.1 Format of the Meinberg Standard Time String

The Meinberg Standard Time String is a sequence of 32 ASCII characters starting with the STX (start-of-text) character and ending with the ETX (end-of-text) character. The format is:

<STX>D:***dd.mm.yy;T:w;U:hh.mm.ss;uvxy***<ETX>

The letters printed in italics are replaced by ASCII numbers whereas the other
characters are part of the time string. The groups of characters as defined below:

<STX> Start-Of-Text, ASCII Code 02h
sending with one bit accuracy at change of second

dd.mm.yy the current date:
dd day of month (01..31)
mm month (01..12)
yy year of
the century (00..99)

w the day of
the week (1..7, 1 = Monday)

hh.mm.ss the current time:
hh hours (00..23)
mm minutes (00..59)
ss seconds (00..59, or 60 while leap second)

uv clock status characters (depending on clock type):

u: ‘#’ GPS: clock is running free (without exact synchr.)
PZF: time frame not synchronized
DCF77: clock has not synchronized after reset
‘ ‘ (space, 20h)
GPS: clock is synchronous (base accuracy is reached)
PZF: time frame is synchronized
DCF77: clock has synchronized after reset

v: ‘*’ GPS: receiver has not checked its position
PZF/DCF77: clock currently runs on XTAL
‘ ‘ (space, 20h)
GPS: receiver has determined its position
PZF/DCF77: clock is syncronized with transmitter

x time zone indicator:
‘U’ UTC Universal Time Coordinated, formerly GMT
‘ ‘ CET European Standard Time, daylight saving disabled
‘S’ (CEST) European Summertime, daylight saving enabled

y anouncement of discontinuity of time, enabled during last hour before discontinuity comes in effect:
‘!’ announcement of start or end of daylight saving time
‘A’ announcement of leap second insertion
‘ ‘ (space, 20h) nothing announced

<ETX> End-Of-Text, ASCII Code 03h

13.1.2 Format of the Meinberg GPS Time String

The Meinberg Standard Time String is a sequence of 36 ASCII characters starting with the STX (start-of-text) character and ending with the ETX (end-of-text) character. Contrary to the Meinberg Standard Telegram the Meinberg GPS Timestring carries no local timezone or UTC but the direct GPS time without conversion into UTC. The format is:

<STX>D:*tt.mm.jj;T:w;U:hh.mm.ss;uvGy;lll*<ETX>

The letters printed in *italics* are replaced by ASCII numbers whereas the other characters are
part of the time string. The groups of characters as defined below:

<STX> Start-Of-Text (ASCII code 02h)

tt.mm.jj the current date:
tt day of month (01..31)
mm month (01..12)
jj year of
the century (00..99)

w the day of the week (1..7, 1 = monday)

hh.mm.ss the current time:
hh hours (00..23)
mm minutes (00..59)
ss seconds (00..59, or 60 while leap second)

uv clock status characters:
u: '#' clock is running free (without exact synchr.)
' ' (space, 20h)
clock is synchronous (base accuracy is reached)

v: '*' receiver has not checked its position
' ' (space, 20h)
receiver has determined its position

G time zone indicator 'GPS-Time'

y anouncement of discontinuity of time, enabled during last hour
before discontinuity comes in effect:
'A' announcement of leap second insertion
' ' (space, 20h) nothing announced

lll number of leap seconds between UTC and GPS-Time
(UTC = GPS-Time + number of leap seconds)

<ETX> End-Of-Text, (ASCII Code 03h)

13.1.3 Format of the Meinberg Capture String

The Meinberg Capture String is a sequence of 31 ASCII characters terminated by a CR/LF (Carriage Return/-Line Feed) combination. The format is:

CH*x_tt.mm.jj_hh:mm:ss.fffffff* <CR><LF>

The letters printed in italics are replaced by ASCII numbers whereas the other characters
are part of the time string. The groups of characters as defined below:

x 0 or 1 corresponding on the number of the capture input
_ ASCII space 20h

dd.mm.yy the capture date:

dd	day of month	(01..31)
mm	month	(01..12)
yy	year of the century	(00..99)

hh:mm:ss.fffffff the capture time:

hh	hours	(00..23)
mm	minutes	(00..59)
ss	seconds	(00..59, or 60 while leap second)
fffffff	fractions of second, 7 digits	

<CR> Carriage Return, ASCII Code 0Dh

<LF> Line Feed, ASCII Code 0Ah

13.1.4 Format of the SAT Time String

The SAT Time String is a sequence of 29 ASCII characters starting with the STX (start-of-text) character and ending with the ETX (end-of-text) character. The format is:

<STX>***dd.mm.yy/w/hh:mm:ssxxxxuv***<ETX>

The letters printed in italics are replaced by ASCII numbers whereas the other characters
are part of the time string. The groups of characters as defined below:

<STX> Start-Of-Text, ASCII Code 02h
sending with one bit accuracy at change of second

dd.mm.yy the current date:

	dd	day of month	(01..31)
	mm	month	(01..12)
	yy	year of the century	(00..99)
	w	the day of the week	(1..7, 1 = Monday)

hh:mm:ss the current time:

	hh	hours	(00..23)
	mm	minutes	(00..59)
	ss	seconds	(00..59, or 60 while leap second)

xxxx time zone indicator:

	'UTC'	Universal Time Coordinated, formerly GMT
	'CET'	European Standard Time, daylight saving disabled
	'CEST'	European Summertime, daylight saving enabled

u clock status characters:

	'#'	clock has not synchronized after reset
	' '	(space, 20h) clock has synchronized after reset

v anouncement of discontinuity of time, enabled during last hour
before discontinuity comes in effect:

	'!'	announcement of start or end of daylight saving time
	' '	(space, 20h) nothing announced

<CR> Carriage Return, ASCII Code 0Dh

<LF> Line Feed, ASCII Code 0Ah

<ETX> End-Of-Text, ASCII Code 03h

13.1.5 Format of the Uni Erlangen String (NTP)

The time string Uni Erlangen (NTP) of a GPS clock is a sequence of 66 ASCII characters starting with the STX (start-of-text) character and ending with the ETX (end-of-text) character. The format is:

<STX>***tt.mm.jj; w; hh:mm:ss; voo:oo; acdfg i;bbb.bbbbn lll.llle hhhhm***<ETX>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<STX> Start-Of-Text, ASCII Code 02h
sending with one bit occuracy at change of second

dd.mm.yy the current date:

dd	day of month	(01..31)
mm	month	(01..12)
yy	year of the century	(00..99)
w	the day of the week	(1..7, 1 = Monday)

hh.mm.ss the current time:

hh	hours	(00..23)
mm	minutes	(00..59)
ss	seconds	(00..59, or 60 while leap second)

v sign of the offset of local timezone related to UTC

oo:oo offset of local timezone related to UTC in hours and minutes

ac clock status characters:

a:	‘#’	clock has not synchronized after reset
	‘ ‘	(space, 20h) clock has synchronized after reset
c:	‘*’	GPS receiver has not checked its position
	‘ ‘	(space, 20h) GPS receiver has determined its position

d time zone indicator:

‘S’	CEST	European Summertime, daylight saving enabled
‘ ‘	CET	European Standard Time, daylight saving disabled

f anouncement of discontinuity of time, enabled during last hour before discontinuity comes in effect:

‘!’	announcement of start or end of daylight saving time
‘ ‘	(space, 20h) nothing announced

g anouncement of discontinuity of time, enabled during last hour before discontinuity comes in effect:

‘A’	announcement of leap second insertion
‘ ‘	(space, 20h) nothing announced

i leap second insertion

‘L’	leap second is actually inserted (active only in 60th sec.)
‘ ‘	(space, 20h) no leap second is inserted

bbb.bbbb latitude of receiver position in degrees
leading signs are replaced by a space character (20h)

n latitude, the following characters are possible:

‘N’	north of equator

'S' south d. equator

lll.llll longitude of receiver position in degrees
leading signs are replaced by a space character (20h)

e longitude, the following characters are possible:
'E' east of Greenwich
'W' west of Greenwich

hhhh altitude above WGS84 ellipsoid in meters
leading signs are replaced by a space character (20h)

<ETX> End-Of-Text, ASCII Code 03h

13.1.6 Format of the NMEA 0183 String (RMC)

The NMEA String is a sequence of 65 ASCII characters starting with the '$GPRMC' character and ending with the characters CR (carriage return) and LF (line-feed). The format is:

$GPRMC,_hhmmss.ss,A,bbbb.bb,n,lllll.ll,e,0.0,0.0,ddmmyy,0.0,a*hh_<CR><LF>

The letters printed in italics are replaced by ASCII numbers or letters where as the
other characters are part of the time string. The groups of characters as defined below:

$ Start character, ASCII Code 24h
sending with one bit accuracy at change of second

hhmmss.ss the current time:

hh	hours	(00..23)
mm	minutes	(00..59)
ss	seconds	(00..59, or 60 while leap second)
ss	seconds	(1/10 ; 1/100)

A Status (A = time data valid, V = time data not valid)

bbbb.bb latitude of receiver position in degrees
leading signs are replaced by a space character (20h)

n latitude, the following characters are possible:

'N'	north of equator
'S'	south d. equator

lllll.ll longitude of receiver position in degrees
leading signs are replaced by a space character (20h)

e longitude, the following characters are possible:

'E'	east of Greenwich
'W'	west of Greenwich

0.0,0.0 Speed over the ground in knots and track angle in degrees,
with a Meinberg GPS clock these values are always 0.0,
in case of a GNS clock the values will be calculated by the
receiver in mobile applications

ddmmyy the current date:

dd	day of month	(01..31)
mm	month	(01..12)
yy	year of the century	(00..99)

a magnetic variation

hh checksum (EXOR over all characters except '$' and '*')

<CR> Carriage Return, ASCII Code 0Dh

<LF> Line Feed, ASCII Code 0Ah

13.1.7 Format of the NMEA 0183 String (GGA)

The NMEA (GGA) String is a sequence of characters starting with the '$GPRMC' character and ending with the characters CR (carriage return) and LF (line-feed). The format is:

$GPGGA,_**hhmmss.ss,bbbb.bbbbb,n,lllll.ll,e,A,vv,hhh.h,aaa.a,M,ggg.g,M,,0*cs**_**<CR><LF>**

The letters printed in italics are replaced by ASCII numbers or letters where as the
other characters are part of the time string. The groups of characters as defined below:

$ Start character, ASCII Code 24h
sending with one bit accuracy at change of second

hhmmss.ss the current time:

hh	hours	(00..23)
mm	minutes	(00..59)
ss	seconds	(00..59, or 60 while leap second)
ss	fractions of seconds	(1/10 ; 1/100)

A Status (A = time data valid)
(V = time data not valid)

bbbb.bbbbb latitude of receiver position in degrees
leading signs are replaced by a space character (20h)

n latitude, the following characters are possible:
'N' north of equator
'S' south d. equator

lllll.lllll longitude of receiver position in degrees
leading signs are replaced by a space character (20h)

e longitude, the following characters are possible:
'E' east of Greenwich
'W' west of Greenwich

A Position fix (1 = yes, 0 = no)

vv Satellites used (0..12)

hhh.h HDOP (Horizontal Dilution of Precision)

aaa.h Mean Sea Level altitude (MSL = altitude of WGS84 - Geoid Separation)

M Units, meters (fixed value)

ggg.g Geoid Separation (altitude of WGS84 - MSL)

M Units, meters (fixed value)

cs checksum (EXOR over all characters except '$' and '*')

<CR> Carriage Return, ASCII Code 0Dh

<LF> Line Feed, ASCII Code 0Ah

13.1.8 Format of the NMEA 0183 String (ZDA)

The NMEA String is a sequence of 38 ASCII characters starting with the **'$GPZDA'** character and ending with the characters **CR** (carriage return) and LF (line-feed). The format is:

$GPZDA,*hhmmss.ss,dd,mm,yyyy,HH,II*cs*<CR><LF>
ZDA - Time and Date: UTC, day, month, year and local timezone.

The letters printed in italics are replaced by ASCII numbers or letters where as the
other characters are part of the time string. The groups of characters as defined below:

$ Start character, ASCII Code 24h
sending with one bit accuracy at change of second

hhmmss.ss the current UTC time:

hh	hours	(00..23)
mm	minutes	(00..59)
ss	seconds	(00..59 or 60 while leap second)

HH,II the local timezone (offset to UTC):

HH	hours	(00..±13)
II	minutes	(00..59)

dd,mm,yy the current date:

dd	day of month	(01..31)
mm	month	(01..12)
yyyy	year	(0000..9999)

cs checksum (EXOR over all characters except '$' and '*')

<CR> Carriage Return, ASCII Code 0Dh

<LF> Line Feed, ASCII Code 0Ah

13.1.9 Format of the ABB SPA Time String

The ABB SPA Time String is a sequence of 32 ASCII characters starting with the characters "**>900WD**" and ending with the **<CR>** (Carriage Return) character. The format is:

>900WD:*yy-mm-tt_hh.mm;ss.fff:cc*<CR>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

yy-mm-tt	the current date:		
	yy	year of the century	(00..99)
	mm	month	(01..12)
	dd	day of month	(01..31)
	_	Space (ASCII code 20h)	
hh.mm;ss.fff	the current time:		
	hh	hours	(00..23)
	mm	minutes	(00..59)
	ss	seconds	(00..59, or 60 while leap second)
	fff	milliseconds	(000..999)
cc	Check sum. EXCLUSIVE-OR result of the previous characters, displayed as a HEX byte (2 ASCII characters 0..9 or A..F)		
<CR>	Carriage Return, ASCII Code 0Dh		

13.1.10 Format of the Computime Time String

The Computime time string is a sequence of 24 ASCII characters starting with the T character and ending with the LF (line feed, ASCII Code 0Ah) character. The format is:

T:***yy:mm:dd:ww:hh:mm:ss***<CR><LF>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

T Start character
sending with one bit accuracy at change of second

yy:mm:dd the current date:

yy	year of the century	(00..99)
mm	month	(01..12)
dd	day of month	(01..31)
ww	the day of the week	(01..07, 01 = monday)

hh:mm:ss the current time:

hh	hours	(00..23)
mm	minutes	(00..59)
ss	seconds	(00..59, or 60 while leap second)

<CR> Carriage Return, ASCII Code 0Dh

<LF> Line Feed, ASCII Code 0Ah

13.1.11 Format of the RACAL standard Time String

The RACAL standard Time String is a sequence of 16 ASCII characters terminated by a X (58h) character and ending with the CR (Carriage Return, ASCII Code 0Dh) character. The format is:

<X><G><U>***yymmddhhmmss***<CR>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<X>	Control character sending with one bit accuracy at change of second		code 58h
<G>	Control character		code 47h
<U>	Control character		code 55h
yymmdd	the current date:		
	yy	year of the century	(00..99)
	mm	month	(01..12)
	dd	day of month	(01..31)
hh:mm:ss	the current time:		
	hh	hours	(00..23)
	mm	minutes	(00..59)
	ss	seconds	(00..59, or 60 while leap second)
<CR>	Carriage Return, ASCII code 0Dh		

13.1.12 Format of the SYSPLEX-1 Time String

The SYSPLEX1 time string is a sequence of 16 ASCII characters starting with the SOH (Start of Header) ASCII controll character and ending with the LF (line feed, ASCII Code 0Ah) character.

Please note:
To receive the Timestring on a selected terminal correctly you have to send a " **C** " (once, without quotation marks).

The format is:

<SOH>ddd:hh:mm:ssq<CR><LF>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<SOH>	Start of Header (ASCII control character) sending with one bit accuracy at change of second		
ddd	day of year		(001..366)
hh:mm:ss	the current time:		
	hh	hours	(00..23)
	mm	minutes	(00..59)
	ss	seconds	(00..59, or 60 while leap second)
	q	Quality indicator	(space) Time Sync (GPS lock) (?) no Time Sync (GPS fail)
<CR>	Carriage-return (ASCII code 0Dh)		
<LF>	Line-Feed (ASCII code 0Ah)		

13.1.13 Format of the ION Time String

The ION time string is a sequence of 16 ASCII characters starting with the SOH (Start of Header) ASCII controll character and ending with the LF (line feed, ASCII Code 0Ah) character. The format is:

<SOH>ddd:hh:mm:ssq<CR><LF>

The letters printed in italics are replaced by ASCII numbers whereas the other
characters are part of the time string. The groups of characters as defined below:

<SOH>	Start of Header (ASCII control character) sending with one bit accuracy at change of second		
ddd	day of year		(001..366)
hh:mm:ss	the current time:		
	hh	hours	(00..23)
	mm	minutes	(00..59)
	ss	seconds	(00..59, or 60 while leap second)
	q	Quality indicator	(space) Time Sync (GPS lock) (?) no Time Sync (GPS fail)
<CR>	Carriage-return (ASCII code 0Dh)		
<LF>	Line-Feed (ASCII code 0Ah)		

13.1.14 Format of the ION Blanked Time String

The ION Blanked time string is a sequence of 16 ASCII characters starting with the SOH (Start of Header) ASCII controll character and ending with the LF (line feed, ASCII Code 0Ah) character. The format is:

<SOH>ddd:hh:mm:ssq<CR><LF>

Attention: Intervall of the String: 2min. 30 seconds every 5 minutes.

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<SOH>	Start of Header (ASCII control character) sending with one bit accuracy at change of second		
ddd	day of year		(001..366)
hh:mm:ss	the current time:		
	hh	hours	(00..23)
	mm	minutes	(00..59)
	ss	seconds	(00..59, or 60 while leap second)
	q	Quality indicator	(space) Time Sync (GPS lock) (?) no Time Sync (GPS fail)
<CR>	Carriage-return (ASCII code 0Dh)		
<LF>	Line-Feed (ASCII code 0Ah)		

13.1.15 Format of the IRIG J Time String

The time code consists of ASCII characters, send in the format 7O1

- 1 start bit
- 7 data bits
- 1 parity bit (odd)
- 1 stop bit

The on-time marker is represented by the leading edge of the start bit. The time code consists of 15 characters, sent once per second at a baud rate of 300 or greater. The format is:

<SOH>*DDD:HH:MM:SS*<CR><LF>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

SOH	ASCII code „Start of Heading“ (0x01h)
DDD	ordinal date, day of year (1 to 366)
HH, MM, SS	time of the start bit given in hour (HH), minute (MM), second (SS)
CR	ASCII code „Carriage Return“ (0x0Dh)
LF	ASCII code „Line Feed“ (0x0Ah)

13.2 SyncMon Formats

SyncMon format for LANTIME firmware usage:

```
SyncMon 172.27.100.32 M3000_100_57_NTP_LAN0_test 58154 34813 2018-02-05T09:
40:  13 + 00:  00 0.000000494 0.000041453 0.000073266 1 R -0.000011100
0.000041453
```

Key-Value-Pairs
The Format with Key-Value-Pairs can be accessed directly from a SPLUNK database server and has the following format:

```
isoTime           =   2018-02-05T09: 40: 13 + 00: 00
syncMonName       =   SyncMon
optInterfaceIp    =   172.27.100.32
utcTime           =   1517823613
node              =   M3000_100_57_NTP_LAN0_test
offset1           =   0.000000494
offset2           =   0.000041453
pathDelay         =   0.000073266
status            =   Stratum: 1 / [10]
offset1Min        =   -0.000011100
offset1Max        =   0.000041453
type              =   NTP / SW / CPU
```

JSON
The JSON format can be processed directly by most databases and has the following format:

```
{
    "IsoTime":          "2018-02-05T09: 40: 13 + 00: 00",
    "syncMonName":      "SyncMon",
    "optInterfaceIp":   "172.27.100.32",
    "utcTime":          1517823613,
    "node":             "M3000_100_57_NTP_LAN0_test",
    "offset1":          0.000000494,
    "offset2":          0.000041453,
    "pathDelay":        0.000073266,
    "status":           "stratum 1 / [10]",
    "offset1Min":       - 0.000011100,
    "offset1Max":       0.000041453,
    "type":             "NTP / SW / CPU"
}
```

13.3 Third party software

The LANTIME network timeserver is running a number of software products created and/or maintained by open source projects. A lot of people contributed to this and we explicitly want to thank everyone involved for her/his great work.

The used open source software comes with its own license which we want to mention below. If one of the licenses for a third party software product is violated, we will as soon as possible apply any changes needed in order to conform with the corresponding license after we acknowledged about that violation.

If a license for one of the software products states that we have to provide you with a copy of the source code or other material, we will gladly send it to you on data media via normal post or by e-mail upon request. Alternatively we can provide you with a link to a download location in the internet, allowing you to download the most actual version. Please note that we have to charge you for any incurred expenses if you choose to receive the source code on data media.

13.3.1 Operating System GNU/Linux

The distribution of the GNU/Linux operating system is covered by the GNU General Public License (GPL), which we included below.

More information about GNU/Linux can be found on the GNU website
www.gnu.org

and on the website of GNU/Linux
www.linux.org

13.3.2 Samba

The Samba software suite is a collection of programs, which implement the Server Message Block (SMB) protocol for UNIX systems. By using Samba your Lantime is capable of sending Windows popup messages and serves request for network time by clients using the NET TIME command.

The distribution of Samba is covered – like GNU/Linux – by the GNU General Public License, see below.

The website of the Samba project (or a mirror) can be reached at
www.samba.org

13.3.3 Network Time Protocol Version 4 (NTP)

The NTP project, lead by David L. Mills, can be reached in the internet at www.ntp.org. There you will find a wealthy collection of documentation and information covering all aspects of the application of NTP for time synchronization purposes. The distribution and usage of the NTP software is allowed, as long as the following notice is included in our documentation:

```
**************************************************************************
*                                                                         *
* Copyright (c) David L. Mills 1992-2004                                  *
*                                                                         *
* Permission to use, copy, modify, and distribute this software           *
* and its documentation for any purpose and 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.                                                               *
*                                                                         *
**************************************************************************
```

13.3.4 lighttpd

For our web based configuration tool (HTTP and HTTPS) we use Lightttpd. Lighttpd is a free web server, with all the essential
functions of a web server. Lighttpd has been developed by the german Software Developer Jan Kneschke.

The use of this software is covered by the following license:

13.3.5 GNU General Public License (GPL)

Version 2, June 1991 - Copyright (C) 1989, 1991

Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software–to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING,
DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

13.4 List of Literature

[**Mills88**] Mills, D. L., "Network Time Protocol (Version 1) - specification and implementation",
DARPA Networking Group Report RFC-1059, University of Delaware, July 1988

[**Mills89**] Mills, D. L., "Network Time Protocol (Version 2) - specification and implementation",
DARPA Networking Group Report RFC-1119, University of Delaware, September 1989

[**Mills90**] Mills, D. L., "Network Time Protocol (Version 3) - specification, implementation and analysis",
Electrical Engineering Department Report 90-6-1, University of Delaware, June 1989

Kardel, Frank, "Gesetzliche Zeit in Rechnernetzen", Funkuhren, Zeitsignale und Normalfrequenzen,
Hrsg. W. Hilberg, Verlag Sprache und Technik, Groß-Bieberau 1993

Kardel, Frank, "Verteilte Zeiten", ix Multiuser-Multitasking-Magazin, Heft 2/93,
Verlag Heinz Heise, Hannover 1993

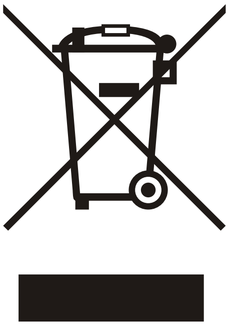
14 RoHS and WEEE

Compliance with EU Directive 2011/65/EU (RoHS)

We hereby declare that this product is compliant with the European Union Directive 2011/65/EU and its delegated directive 2015/863/EU “Restrictions of Hazardous Substances in Electrical and Electronic Equipment”. We ensure that electrical and electronic products sold in the EU do not contain lead, cadmium, mercury, hexavalent chromium, polybrominated biphenyls (PBBs), polybrominated diphenyl ethers (PBDEs), bis(2-ethylhexyl)phthalat (DEHP), benzyl butyl phthalate (BBP), dibutyl phthalate (DBP), or diisobutyl phthalate (DIBP) above the legal limits.

WEEE status of the product

This product is handled as a B2B (Business to Business) category product. To ensure that the product is disposed of in a WEEE-compliant fashion, it must be returned to the manufacturer. Any transportation expenses for returning this product (at end-of-life) must be covered by the end user, while Meinberg will bear the costs for the waste disposal itself.



15 Declaration of Conformity

Konformitätserklärung

Doc ID: LCES/NTP/LNE/RPS/BGT-February 4, 2022

Hersteller	Meinberg Funkuhren GmbH & Co. KG
Manufacturer	Lange Wand 9, D-31812 Bad Pyrmont

erklärt in alleiniger Verantwortung, dass das Produkt,
declares under its sole responsibility, that the product

Produktbezeichnung	**LCES/NTP/LNE/RPS/BGT**
Product Designation	

auf das sich diese Erklärung bezieht, mit den folgenden Normen und Richtlinien übereinstimmt:
to which this declaration relates is in conformity with the following standards and provisions of the directives:

EMV – Richtlinie	DIN EN 61000-6-2:2019
EMC Directive	DIN EN 61000-6-3:2007 + A1:2011
	DIN EN 55032:2015
2014/30/EU	DIN EN 55024:2010 + A1:2015
	DIN EN 61000-3-2:2019
	DIN EN 61000-3-3:2013 + A1:2019
Niederspannungsrichtlinie	DIN EN 62368-1:2014 + A11:2017
Low-voltage Directive	
2014/35/EU	
RoHS – Richtlinie	DIN EN IEC 63000:2018
RoHS Directive	
2011/65/EU + 2015/863/EU	

Bad Pyrmont, February 4, 2022

S. Meinberg

Stephan Meinberg
Production Manager