The Synchronization Experts.

MANUAL

microSync

NTP/PTP Time Source

July 6, 2023

Meinberg Funkuhren GmbH & Co. KG

Table of Contents

1 Copyright and Liability Exclusion

At the time of writing of this document, reasonable effort was made to carefully review links to third-party websites to ensure that they were compliant with the laws of the Federal Republic of Germany and relevant to the subject matter of the document. Meinberg accepts no liability for the content of websites not created or maintained by Meinberg, and does not warrant that the content of such external websites is suitable or correct for any given purpose.

While Meinberg makes every effort to ensure that this document is complete, suitable for purpose, and free of material errors or omissions, and periodically reviews its library of manuals to reflect developments and changing standards, Meinberg does not warrant that this specific document is up-to-date, comprehensive, or free of errors. Updated manuals are provided at **www.meinbergglobal.com**.

You may also write to **techsupport@meinberg.de** to request an updated version at any time or provide feedback on errors or suggested improvements, which we are grateful to receive.

Meinberg reserves the right to make changes of any type to this document at any time as is necessary for the purpose of improving its products and services and ensuring compliance with applicable standards, laws & regulations.

2 The microSync System

2.1 microSync - Brand and Device Type

The registered trademark microSync describes a product family of Meinberg radio clocks for the synchronization of time and frequency signals in networks and directly connected systems such as signal distributors.

The microSync system is offered in two housing variants (HR = 9.5 inch half-rack chassis, RX = 19 inch full-rack chassis) with different input and output options. The system name describes the exact hardware configuration.

The available configurations are optimized for the different application areas.

2.2 Device Manufacturer

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
Internet:	https://www.meinbergglobal.com
E-Mail:	info@meinberg.de

Date:	July 6, 2023
Manual Version:	2.4

2.3 Target Readership

This manual is intended to be used by professionals responsible for installing, setting up, maintaining, troubleshooting, or operating any device within the specified product range.

This manual employs a structure and terminology that assumes that the technicians tasked with installing and setting up the device are familiar with the handling of electronic devices and network components.

2.4 Returning Products

Only Meinberg is authorized to repair any components of your Meinberg system. Should your device experience a malfunction, the customer must contact our Support Service. Do not attempt to repair the device yourself.

To submit a repair order for a Meinberg device, first call Meinberg's Technical Support service to review the shipping options and obtain an RMA (Return Material Authorization) number for shipping.

You can also request an RMA number via our website:
https://www.meinbergglobal.com/english/support/rma.htm.

The device must be packed in the original packaging or other suitable packaging in such a way that it is protected against impact and moisture. Ship the device to the manufacturer's address. The address of origin and RMA number must also be quoted.

What needs to be included in the shipment?
Please return the device, if possible complete with accessories such as the antenna or cables. A complete return can help us significantly to identify the cause of the fault.

3 microSync System Description

3.1 Device Design, Functions and Area of Application

The microSync product family is a range of high-performance synchronization systems available in 9.5-inch (Half-Rack) and 19-inch models.

All microSync models offer a wide range of output signals including 1PPS, 10 MHz, IRIG timecodes, programmable pulses, and fiber optic signals. Furthermore, the Gigabit network ports enable network synchronization of NTP clients and PTP slaves.

The microSync systems have an integrated embedded network processor with the sync-optimized firmware **meinbergOS**. The firmware supports NTP, as well as all common PTP IEEE 1588 profiles and numerous network protocols for management and monitoring tasks.

The variety of outputs and interfaces allows the use of microSync models in several industries and applications. Depending on the system requirements, customers can choose from different variants that are best suited to their needs. The variants are defined via the BNC connectors, which can provide several I/O options. The following variants are currently available:

10 series / 20 series*
With preconfigured outputs such as Programmable Pulse (TTL), Time Code AM (IRIG, AFNOR) and Frequency Synthesizer (0.1 Hz to 10 MHz).

30 series / 40 series*
With preconfigured I/Os such as PPS input (TTL), 10 MHz input (sine/TTL), 10 MHz output (TTL) and 10 MHz sine output.

31 series / 41 series*
With preconfigured I/Os such as PPS input (TTL), 10 MHz input (sine/TTL), Programmable Pulses (TTL).

33 series / 43 series*
With preconfigured I/Os such as PPS input (TTL), 10 MHz input (sine/TTL), 10 MHz output (sine), Programmable Pulses (TTL).

70 series / 80 series*
With preconfigured I/Os such as Blackburst output, Blackburst input, LTC/GPIO, DARS, Word Clock output (TTL), programmable pulses (TTL).

---

* With LE display and rotary function knob. These models are only available in the microSync^{RX} series.

3.2 System Variants microSync

The microSync synchronization system is available in different versions. Two housing variants are available - the space-efficient HR housing (Half Rack, 1HE/9.5 inch built-in housing) and the RX housing variant as 1HE/19 inch built-in rackmount chassis. The RX enclosure offers the option of redundant power with a second power supply unit as an option. The HR enclosure can be mounted in any 19-inch server cabinet using a 19-inch mounting bracket. When using multiple HR chassis, it is possible to install two HR devices next to each other in a 19-inch server rack.

In addition, there are various reference signal options as well as input and output signals optimized for special applications. A detailed list of all options and their order codes can be found in the following overview.

Model Codes
The microSync model code (also order code) has the following structure: **AA112BB(B)/CC##(CC##)**

AA – Chassis Type

HR	Half-Rack (1HE/9,5 inch)
RX	Full-Rack (1HE/19 inch)

11 – Input and Output Options / Interfaces

1xx, 2xx, 3xx, 4xx, 5xx, 6xx, 7xx, 8xx	Status indicators LAN-CPU / Receiver Status indicators PP1 - PP8 COM 0 Timestring - Output PPS + Timestring - Input USB Terminal / USB Host 4x Network interfaces
1xx, 2xx, 3xx, 4xx	DMC X1 / DMC X2 Terminal connector 2x programmable pulse outputs* – fiber optic
52x, 62x	Pulse Per Second input, Frequency input RS-422 - PPS Timestring output, 2048 kHz Frequency output DMC X1 - Terminal connector
2xx, 4xx, 6xx, 8xx	OLED display (microSync^{RX} only)
10x, 20x	Frequency synthesizer output Timecode** AM output (modulated) 2x programmable pulse* outputs (PP 1 and PP 2)
30x, 40x	10 MHz input (Sine or TTL) PPS input (TTL) 10 MHz sine output 10 MHz output (TTL)
31x, 41x	10 MHz input (Sine or TTL) PPS input (TTL) 2x programmable pulse* outputs (PP 1 and PP 2)
32x, 42x	10 MHz input (Sine or TTL) PPS input (TTL) 1x 10 MHz output (TTL) 1x PPS output (TTL)

33x, 43x	10 MHz input (Sine or TTL) PPS input (TTL) 1x 10 MHz sine output 1x PPS output (TTL)

* For a detailed description of the Programmable Pulse Output signals, see chapter Description of Programmable Pulse Outputs .

** An overview of the selectable time code formats can be found in chapter Description of Time Code Formats .

70x, 80x	1x LTC/GPIO (TTL) 2x Programmable pulse outputs (PP 1 and PP 2) 1x DARS output (TTL) 1x Word Clock output (TTL) 1x Blackburst (CVBS signal) output 1x Blackburst (CVBS signal) input 1x PPS input (TTL) 1x Word Clock input (TTL)

2 – Receiver

0	GNS: L1 Multi-GNSS (GPS, GLONASS, Galileo, BeiDou)
1	GPS: Meinberg GPS
2	GNS-UC: Meinberg Multi-GNSS (GPS, Galileo)

BB(B) – Oscillator

SQ	OCXO SQ
MQ	OCXO MQ
HQ	OCXO HQ
DHQ	OCXO DHQ

CC##(CC##) – Power Supply *

	nominal voltage range	max. voltage range
microSyncRX		
AD10	100-240 V ∼, 50-60Hz / 100-200 V ⎓	90-265 V ∼, 47-63 Hz / 90-250 V ⎓
DC20	24-48 V ⎓	20-60 V ⎓

microSyncHR

The available HR models are supplied with two different DC power supplies.
The microSyncHR does not have a power supply identifier at the end of the model code.

Connection type - DMC connector:

nominal voltage range	max. voltage range
24-48 V ⎓	20-60 V ⎓
24 V ⎓	10-36 V ⎓

Connection type - hollow socket/low voltage socket:

Power supply for microSyncHR in broadcast configuration (e.g. HR701SQ)

24 V ⎓	10-36 V ⎓

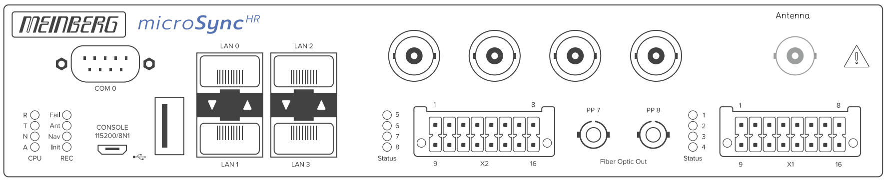
microSync Model Code Samples

HR101HQ	Half rack chassis of I/O-type 10 with Meinberg GPS receiver, OCXO HQ oscillator.
HR701SQ	70 series half-rack enclosure with Meinberg GPS receiver, OCXO SQ oscillator.
RX300DHQ/AD10DC20	Full rack chassis of I/O-type 30 with Multi GNS receiver, OCXO SQ oscillator and redundant power supplies (AD10 and DC20).

3.3 Hardware Specifications

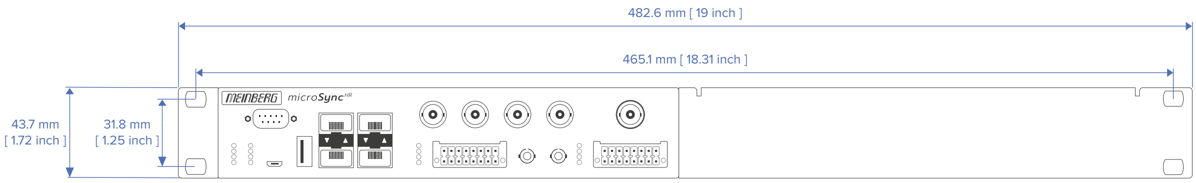
3.3.1 Chassis Specifications

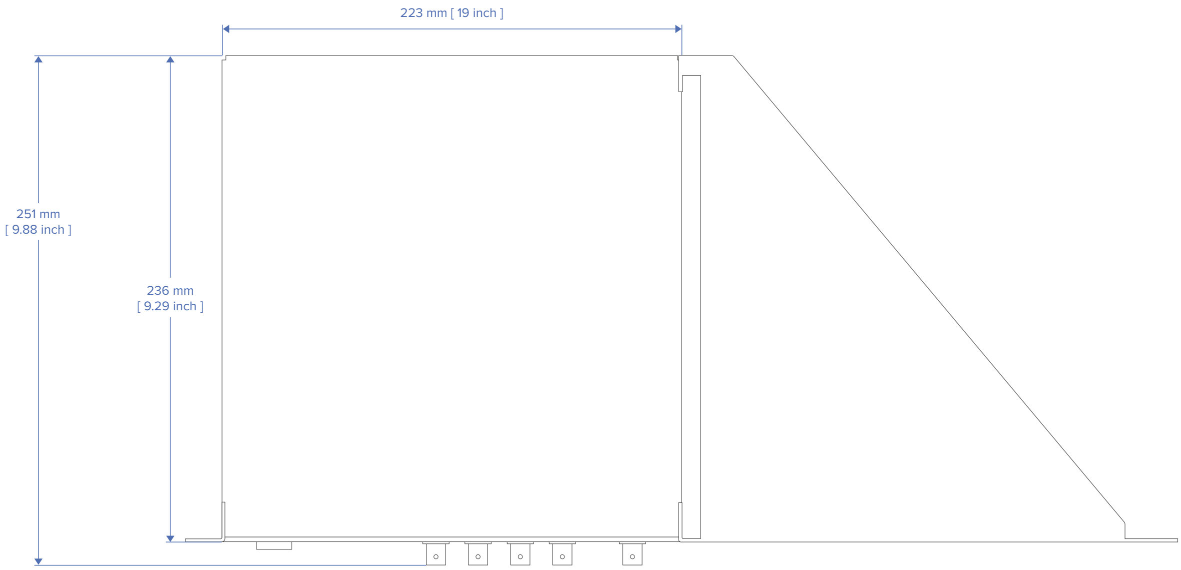
3.3.1.1 HR: Half-Rack Chassis



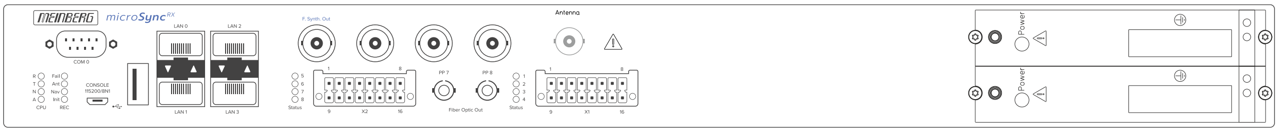
The microSync^{HR} system is a space-saving synchronization solution in a 9.5-inch/1U half rack housing. It is possible to mount two systems side by side in a 19-inch server rack. A special mounting bracket is available in the supplied mounting kit for mounting a single microSync^{HR} device.

Physical Dimensions:



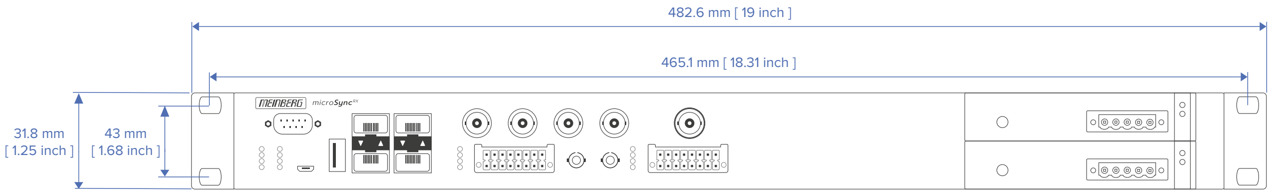


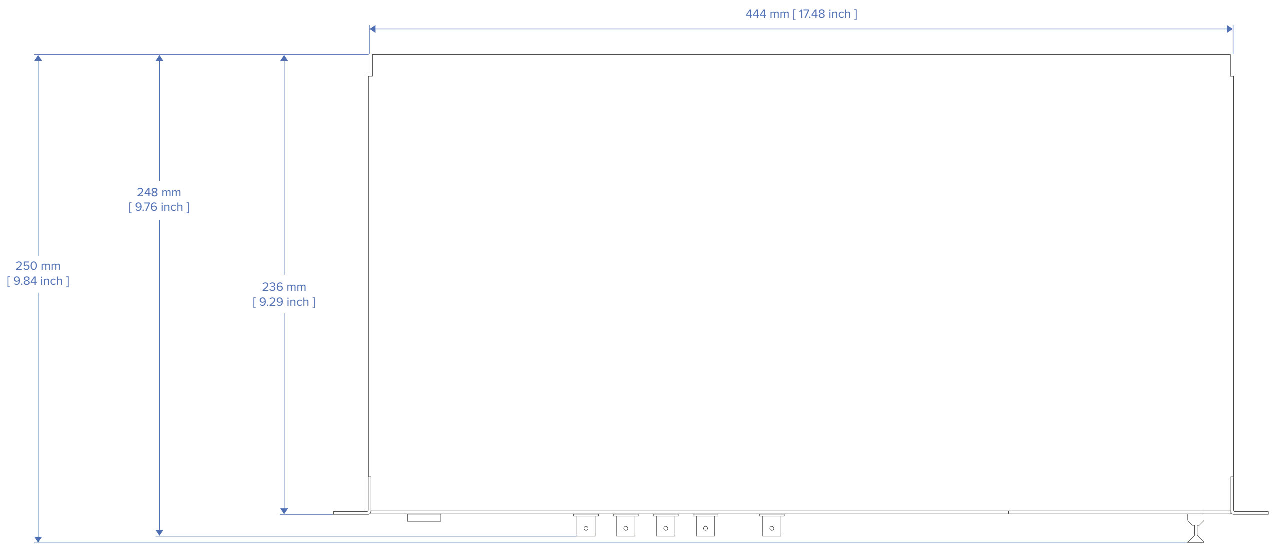
3.3.1.2 RX: 19 Inch Chassis



The microSync^{RX} system from Meinberg is a synchronization solution in a 19-inch/1HE housing, with the option of redundant power supplies with AC/DC or DC voltage.

Physical Dimensions:





3.3.2 Available Power Supplies

microSync^RX

100-240 V AC / 100-200 V DC

Input parameters

Nominal Voltage Range	U_N	100-240 V ∼ 100-200 V ⎓
Max. Voltage Range	U_{max}	90-254 V ∼ 90-240 V ⎓
Nominal Current	I_N	1.0 A ∼ 0.6 A ⎓
Nominal Frequency	f_N	50-60Hz
Max. Frequency Range	f_{max}	47-63Hz

Output parameters

Power Consumption	P_{max}	50 W
Maximum heat emisson	E_{therm}	180.00 kJ/h (170.61 BTU/h)

20-60 V DC

Input parameters

Nominal Voltage Range	U_N	24-48 V ⎓
Max. Voltage Range	U_{max}	20-60 V ⎓
Nominal Current	I_N	2.10 A ⎓

Output parameters

Power Consumption	P_{max}	50 W
Maximum heat emission	E_{therm}	180.00 kJ/h (170.61 BTU/h)

microSync^HR

20-60 V DC

Input parameters

Nominal Voltage	U_N	48 V ⎓
Max. Voltage Range	U_{max}	20-60 V ⎓
Nominal Current	I_N	0.63 A ⎓

Output parameters

Power Consumption	P_{max}	30 W
Maximum heat emission	E_{therm}	108.00 kJ/h (102.37 BTU/h)

microSync^{HR} Broadcast

24 V DC via desktop AC adapter

Input parameters

Input Voltage Range	U_N	24 V ⎓
Max. Voltage Range	U_{max}	10–36 V ⎓
Nominal current	I_N	1.25 A ⎓

Output parameters

Max. Power	P_{max}	30 W
Maximum heat emission	E_{therm}	108.00 kJ/h (102.37 BTU/h)

3.3.3 Available Receiver and Oscillator Options

Receiver Type	Signal Type	Value	Connector
GPS (12 Channel)	IF (Meinberg Antenna)	15 V DC	BNC
GNS-UC GPS, Galileo (72 Channel)	IF (Meinberg Antenna)	15 V DC	BNC
GNSS GPS, GLONASS, Galileo, BeiDou (72 Channel)	L1/E1/B1 band	5 V DC	SMA

Oscillator Options

Type	Holdover Performance (1 Day)	Holdover Performance (1 Year)
OCXO SQ	$\pm$ 220 μsec	$\pm$ 4.7 sec
OCXO MQ	$\pm$ 65 μsec	$\pm$ 1.6 sec
OCXO HQ	$\pm$ 22 μsec	$\pm$ 788 msec
OCXO DHQ	$\pm$ 4.5 μsec	$\pm$ 158 msec

3.3.4 Environment

Operating Temperature Range:	microSync models 1xx, 2xx, 3xx and 4xx –20 to 55 °C (–4 to 131 °F) microSync models 5xx, 6xx, 7xx and 8xx 0 to 50 °C (32 to 122 °F)
Storage Temperature Range	microSync models 1xx, 2xx, 3xx and 4xx –30 to 70 °C (–22 to 158 °F) microSync models 5xx, 6xx, 7xx and 8xx –20 to 70 °C (–4 to 158 °F)
Relative Humidity	5 to 95 % (non-condensing) at 40 °C (104 ° F)
Operating Altitude	up to 4,000 m (13,123 ft) above sea level
Atmospheric Pressure	615 to 1600 hPa

3.4 Type Tests / Compatibilities

3.4.1 Electromagnetic Compatibility - Emission

CISPR 16-1-2 and CISPR 16-2-1	Conducted disturbance voltage measurements
CISPR 16-2-3	Radiated radio disturbance
CISPR 32	Conducted disturbance current measurements
FCC 47 CFR Part 15 section 15.107 (b) [3] RSS-Gen Issue 4 section 8.8 [4]	Conducted emission
FCC 47 CFR Part 15 section 15.109 (b) [3] RSS-Gen Issue 4 section 8.9 [4]	Radiated emission
ETSI EN 303 413	Standard for GNSS receiver

3.4.2 Electromagnetic Compatibility - Immunity (microSync models 1xx, 2xx, 3xx and 4xx)

The tests were performed according to IEC 61000-6-5 and IEC 61850-3 referring to the following standards:

IEC 61000-4-2	Immunity test to electrostatic discharges	±6 kV contact discharge ±8 kV air discharge
IEC 61000-4-3	Immunity test to radiated, radio-frequency, electromagnetic fields	10 V/m
IEC 61000-4-4	Immunity test to electrical fast transients (Burst)	±4 kV, 100 kHz (microSync^{HR}) ±2 kV, 100 kHz (microSync^{RX})
IEC 61000-4-5	Immunity test to surges	up to ±1 kV line to line up to ±2 kV line to earth
IEC 61000-4-6	Immunity test to conducted disturbances, induced by radio-frequency fields	10 V
IEC 61000-4-8	Immunity test to power frequency magnetic fields	100 A/m continuous 1000 A/m at 1 s
IEC 61000-4-11 (microSync^{RX} only)	Immunity tests to voltage dips, short interruptions and voltage variations	ΔU 30% for 1 period ΔU 60% for 50 periods ΔU 100% for 5 periods ΔU 100% for 50 periods
IEC 61000-4-16	Immunity test to conducted, common mode disturbances	30 V continuous 300 V at 1 s
IEC 61000-4-17	Immunity test to ripple on d.c. input power ports	10 % of U_n
IEC 61000-4-18	Immunity test to damped oscillatory waves	±1 kV line to line ±2.5 kV line to earth
IEC 61000-4-29	Immunity test to voltage dips, short interruptions and voltage variations	ΔU 30% for 100 ms ΔU 60% for 100 ms ΔU 100% for 50 ms

3.4.3 Electromagnetic Compatibility - Immunity (microSync models 5xx, 6xx, 7xx and 8xx)

The tests were performed according to IEC 61000-6-5 and IEC 61850-3 referring to the following standards:

IEC 61000-4-2	Immunity test to electrostatic discharges	±4 kV contact discharge ±8 kV air discharge
IEC 61000-4-3	Immunity test to radiated, radio-frequency, electromagnetic fields	10 V/m, 80-1000 MHz, 80% AM (1 kHz) 3 V/m, 1400-2700 MHz, 80% AM (1 kHz)
IEC 61000-4-4	Immunity test to electrical fast transients (Burst)	±2 kV, DC main lines ±1 kV, Signal lines
IEC 61000-4-5	Immunity test to surges	DC main lines: up to ±0.5 kV line to line up to ±0.5 kV line to earth Signal lines: up to ±1 kV line to earth
IEC 61000-4-6	Immunity test to conducted disturbances, induced by radio-frequency fields	10 V, 0.15-80 MHz, 80% AM (1 kHz)
IEC 61000-4-8	Immunity test to power frequency magnetic fields	30 A/m
IEC 61000-4-29	Immunity test to voltage dips, short interruptions and voltage variations	ΔU 30% for 100 ms ΔU 60% for 100 ms ΔU 100% for 50 ms

3.4.4 Safety Tests

IEC 62368-1 Safety Requirements	Overvoltage Category	II
	Protection Class	1
	Degree of Pollution	2
IEC 60529	Protection Rating / IP Code	IP30

3.4.5 Environmental Tests - microSync models 1xx, 2xx, 3xx and 4xx

The tests were performed according to IEC 61850-3 referring to the following standards:

IEC 60068-2-1	Cold	–40 °C (-40 °F), 16 h
IEC 60068-2-2	Dry heat	85 °C (185 °F), 16 h
IEC 60068-2-14	Change of temperature	–20 to 55 °C (-4 to 131 °F), 5 cycles, (1 °C/min)
IEC 60068-2-30	Damp heat, cyclic (12 h + 12 h)	55 °C (131 °F), 97 % RH, 6 cycles
IEC 60068-2-78	Damp heat, steady state	40 °C (104 °F), 93 % RH, 240 h
IEC 60255-21-1	Vibration (sinusoidal) [1] Class 2	10–150 Hz, 1 g_n, 2 sweeps, 3 axes 10–150 Hz, 2 g_n, 40 sweeps, 3 axes
IEC 60255-21-2	Shock [1] Class 2	10 g_n, 11 ms, ±3 shocks, 3 axes 30 g_n, 11 ms, ±3 shocks, 3 axes 20 g_n, 16 ms, ±1000 shocks, 3 axes
IEC 60255-21-3	Seismic [1, 2] Class 2	4-35 Hz, 1 g_n, 1 sweep, hor. axes 4-35 Hz, 2 g_n, 1 sweep, ver. axis

1) *In order to withstand the tests for vibration, shock and seismic, special mounting brackets are optionally available.*

2) *The frequency range deviates from the values required by the standard. In this test, a frequency range of 4-35 Hz instead of 1-35 Hz was used.*

3.4.6 Environmental Tests - microSync models 5xx, 6xx, 7xx and 8xx

The tests were performed according to IEC 61850-3 referring to the following standards:

IEC 60068-2-1	Cold	–5 °C (23 °F), 16 h
IEC 60068-2-2	Dry heat	55 °C (131 °F), 16 h
IEC 60068-2-14	Change of temperature	–5 to 55 °C (23 to 131 °F), 5 cycles, 1 °C (34 °F)/min
IEC 60068-2-30	Damp heat, cyclic (12 h + 12 h)	55 °C (131 °F), 97 % RH, 6 cycles
IEC 60068-2-78	Damp heat, steady state	40 °C (104 °F), 93 % RH, 240 h
IEC 60255-21-1	Vibration (sinusoidal) [1] Class 1	10–150 Hz, 0.5 g_n, 2 sweeps, 3 axes 10–150 Hz, 1 g_n, 40 sweeps, 3 axes
IEC 60255-21-2	Shock [1] Class 1	5 g_n, 11 ms, ±3 shocks, 3 axes 15 g_n, 11 ms, ±3 shocks, 3 axes 10 g_n, 16 ms, ±1000 shocks, 3 axes
IEC 60255-21-3	Seismic [1, 2] Class 1	4-35 Hz, 1_{gn}, 1 sweep, hor. axes 4-35 Hz, 2_{gn}, 1 sweep, ver. axis

1) *In order to withstand the tests for vibration, shock and seismic, special mounting brackets are optionally available.*

2) *The frequency range deviates from the values required by the standard. In this test, a frequency range of 4-35 Hz instead of 1-35 Hz was used.*

3.4.7 Compliance

CB Scheme	√	CSA	√
CE	√	WEEE	√
FCC	√	RoHS	√
UL	√	REACH	√

4 Important Safety Information

4.1 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.

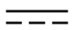
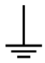
WARNING!
This signal indicates a hazard with a medium risk level . Such a notice refers to a procedure or other action that may result in serious injury or even death if not observed or if improperly performed.

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.

4.2 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.*

4.3 Product Documentation

Extensive documentation for the product is provided on the Meinberg Customer Portal – https://www.meinberg.support. The manuals can also be downloaded from the Meinberg website at https://www.meinbergglobal.com/english/docs/. On our website you can enter your system name into the search box at the top of the page to find the desired manual. If you have any questions or problems, our support team will be pleased to help you.

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.

4.4 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.

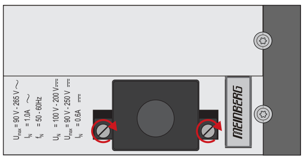
Before the device is connected to the power supply, a grounding conductor must be connected to the earth terminal of the device.

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

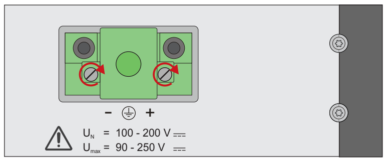
Before operation, check that all cables and lines work properly and are undamaged. Ensure in particular that the cables do not have kinks, that they are not wound too tightly around corners, and that no objects are placed on the cables.

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.

<table>
<tr><th>AC Power Supply</th><th>DC Power Supply</th></tr>
<tr><td>

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.

</td><td>

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.

</td></tr>
</table>

4.5 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 ground connection is provided on the housing, it must be connected to the grounding busbar (earthing busbar) for safety reasons before connecting the power supply. Like this, any possible leakage current on the housing is safely discharged to earth.

The screw, washer and toothed lock washer necessary for mounting the grounding cable are located at the grounding point of the housing. A grounding cable is not included in the contents of delivery.

Note:
Please use a grounding cable with cross-section $\geq$ 1.5 mm^2, as well as a suitable grounding clamp/lug. Always ensure that the connection is properly crimped!

4.6 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 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.

4.7 Safety During Maintenance

WARNING!

When modifying the device in any way, only use components that are approved for use with the system. Failure to comply with this requirement may result in violations of EMC or safety standards and cause the device to malfunction.

When modifying or removing components approved for the system, the force required to remove the components (approx. 60 N) presents a risk of injury to the hands. Information on which components are approved for installation can be obtained from Meinberg Technical Support.

The device must not be opened. Repairs to the device may only be performed by the manufacturer or authorized personnel. Improperly performed repairs expose the user to considerable risk (electric shock, fire hazard).

- Danger from moving parts. Keep away from moving parts.

- Parts of the device may get very hot during operation. Do not touch the surfaces of these! Switch off the device and allow it to cool if necessary before installing or removing any components.

4.8 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.

IMPORTANT!

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

4.9 Safety Information for SFP Modules

This safety information describes how the SFP modules recommended by Meinberg should be handled to ensure safe usage. These SFP modules are hot-pluggable input/output devices (I/O devices) that are connected to a network via a fiber optic or electrical connection. The safety information below must be read and heeded before installing an SFP module in a Meinberg device, before setting up a Meinberg device equipped with SFP modules for use, or before performing maintenance on such a Meinberg device.

CAUTION!

The SFP modules recommended by Meinberg are equipped with a Class 1 laser.

Risk of injury from laser radiation!

- Only use fiber optic SFP modules that are compliant with the definition of a Class 1 laser in accordance with IEC standard 60825-1.
- Fiber optic products that are not compliant with this standard may emit radiation capable of causing eye injuries.
- Never look into an unconnected connector of a fiber optic cable or an unconnected SFP port.
- Unused fiber optic connectors should always be fitted with a suitable protective cap.
- This device may be installed, replaced, and maintained only by trained and qualified personnel.

ATTENTION!

- The safety information and manufacturer specifications relating to the SFP modules used must be heeded.
- The SFP module used must be capable of providing protection against voltage spikes in accordance with IEC 62368-1.
- The SFP module used must be tested and certified in accordance with applicable standards.

4.10 Cleaning and Care

ATTENTION!

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

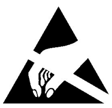
Liquids can cause irreparable damage to the electronics of the device! The ingress of liquids into the device chassis may cause short circuits in the electronic circuitry.

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

4.11 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.

4.12 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.

5 Before you start

5.1 Text and Syntax Conventions

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

Meinberg Device Manager:	Example "Network Settings" menu
Submenu	"Network Settings → Interfaces"
Tab in a submenu	"Monitoring Settings → SNMP → SNMPv3"

Menu navigation is described by the options to be selected being listed in sequence, separated by a right arrow.

Services
Services running on the system are shown in italics.

Example: NTP deamon: *ntpd*

Links to other chapters in the document:
Links to other chapters in the document are displayed in dark blue; e.g., "see chapter Support Information"

Selectable Options and Logical Groups:
Selectable options (such as those in a drop-down menu) are underlined and then briefly described. If several options in a menu are combined into logical groups, these are also underlined and displayed in bold (e.g., PTP status → **Parent Datasets** .

Example:
PTP (IEEE1588) Settings menu → Operation Mode

Multicast Master
...

Terminal

```
# Output via a terminal window is displayed
# in a grey box in a monospace font.
```

5.2 Abbreviation List

ACPI	Advanced Configuration and Power Interface
AFNOR	Association Francaise de Normalisation
AC	Alternating Current
ASCII	American Standard Code for Information Interchange
BMC	Best Master Clock
BNC	Bayonet Neill-Conselman connector
Bps	Bytes per second
bps	Bits per second
CAT5/CAT6/ CAT7	Category 5/6/7 Cable
CEST	Central European Summertime
CET	Central European Time
CLI	Command Line Interface
DB9	D-Subminiature 9-pin
DC	Direct Current
DCF77	A long-wave time signal. D=Deutschland (Germany), C=long wave signal, F=Frankfurt, 77=frequency: 77.5 kHz.
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSCP	Differentiated Services Code Points
DST	Daylight Saving Time
E1	E-carrier protocol
E2E	End-to-end
ETH	Ethernet
FTP	File Transfer Protocol
FW	Firmware
GE / GbE	Gigabit Ethernet
GLONASS	GLObal NAvigation Satellite System
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
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
IP	Internet Protocol
IP20	Ingress Protection Rating 20
IRIG	Inter-Range Instrumentation Group
LCD	Liquid Crystal Display
LED	Light-Emitting Diode
LIU	Line Interface Unit - a module for generating E1/T1 Signals, both MBit/s (framed) and Clock (unframed)
LNE	Local Network Extension
MAC	Media Access Control
MD5	Message-Digest Algorithm 5
MIB	Management Information Base
MRS	Multi Reference Source
MSF	Time signal transmitter in Anthorn, UK
NIST	National Institute of Standards and Technology
NMEA	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	Physikalisch-Technische Bundesanstalt
PTP	Precision Time Protocol
RAM	Random Access Memory
RF	Radio Frequency
RMC	Remote Monitoring Control
RoHS	Restriction of Hazardous Substances Directive
RPS	Redundant Power Supply
RSC	Redundant Switch Control unit
RX	Receiving Data
SBC	Single-Board Computer
SDU	Signal Distribution Unit
SHA-1	Secure Hash Algorithm 1
SMB	Subminiature-B
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
SSM	Sync Status Messages
ST	Straight Tip
SYSLOG	System Log

TACACS	Terminal Access Controller Access Control System
TCG	Time Code Generator
TCR	Time Code Receiver
T1	Transmission System 1
TCP	Transmission Control Protocol
TTL	Transistor-to-Transistor Logic
TX	Data Transmission
U	(Rack) Unit (also RU)
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network
WWVB	Time signal radio station in Fort Collins, Colorado (USA)

5.3 Required Tools

	microSync HR	microSync RX
Haltewinkel Rack-Einbau	Torx T10	Torx T10
Erdungsanschluss	Torx T20	Torx T20
Netzteil	---	Torx T8

Figure: Required tools from left to right:
TORX T20, TORX T10, TORX T8

5.4 Additional Software

Meinberg Device Manager
We provide "Meinberg Device Manager" free of charge as an alternative for setting up, configuring, and monitoring your device. This is a graphical desktop application that you can use to manage and monitor multiple Meinberg devices concurrently over an encrypted network connection.

Meinberg Device Manager offers a number of advanced functions that are currently not available via the Web Interface. The Web Interface will suffice for most standard configuration and monitoring processes, but the use of Meinberg Device Manager is recommended for certain functions such as the following:

- Uploading a SSL certificate
- Forcing a cold or warm boot (for refreshing the almanac data of the receiver)
- Displaying an analysis of satellite reception (with data on visible satellites, C/NO ratios, etc.)

Meinberg Device Manager for Windows supports Windows 7 and later. The application is provided as an installable setup file, and a "Portable Version" is also available if your company's IT security policy prohibits or discourages the installation of applications with system-wide permissions.

Meinberg Device Manager for Linux is provided as a non-distribution-specific *.tar.gz* package that can be simply unpacked in the desired directory and executed from there.

The software can be downloaded free of charge from our website:
https://www.meinbergglobal.com/english/sw/mbg-devman.htm

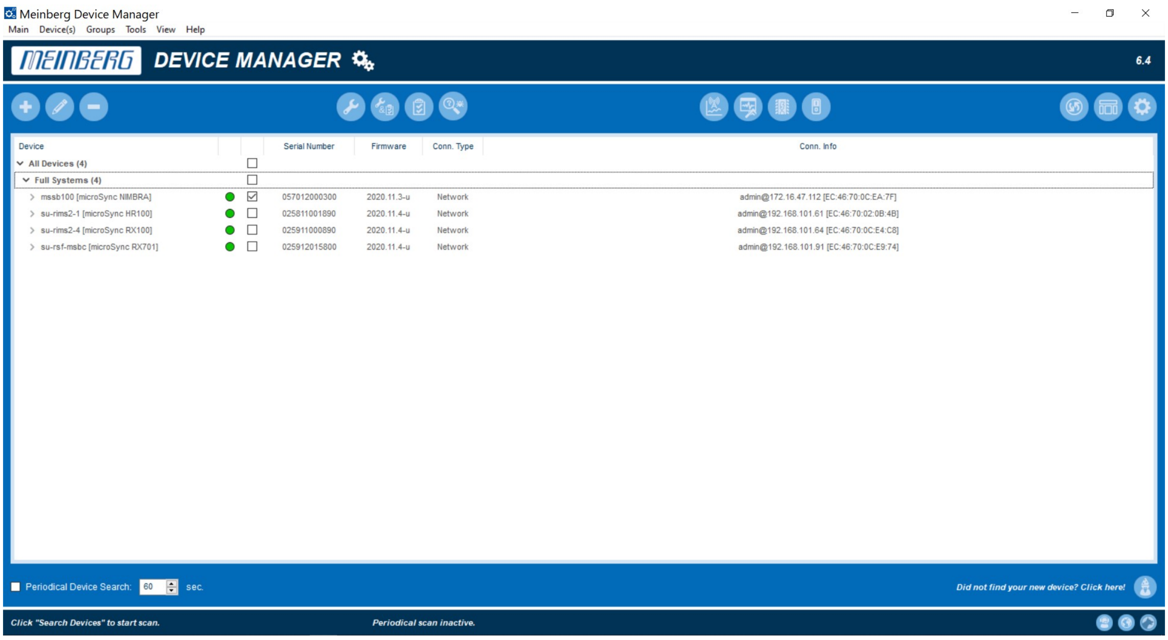


Illustration: Meinberg Device Manager Launch Window

5.5 Preparing Installation

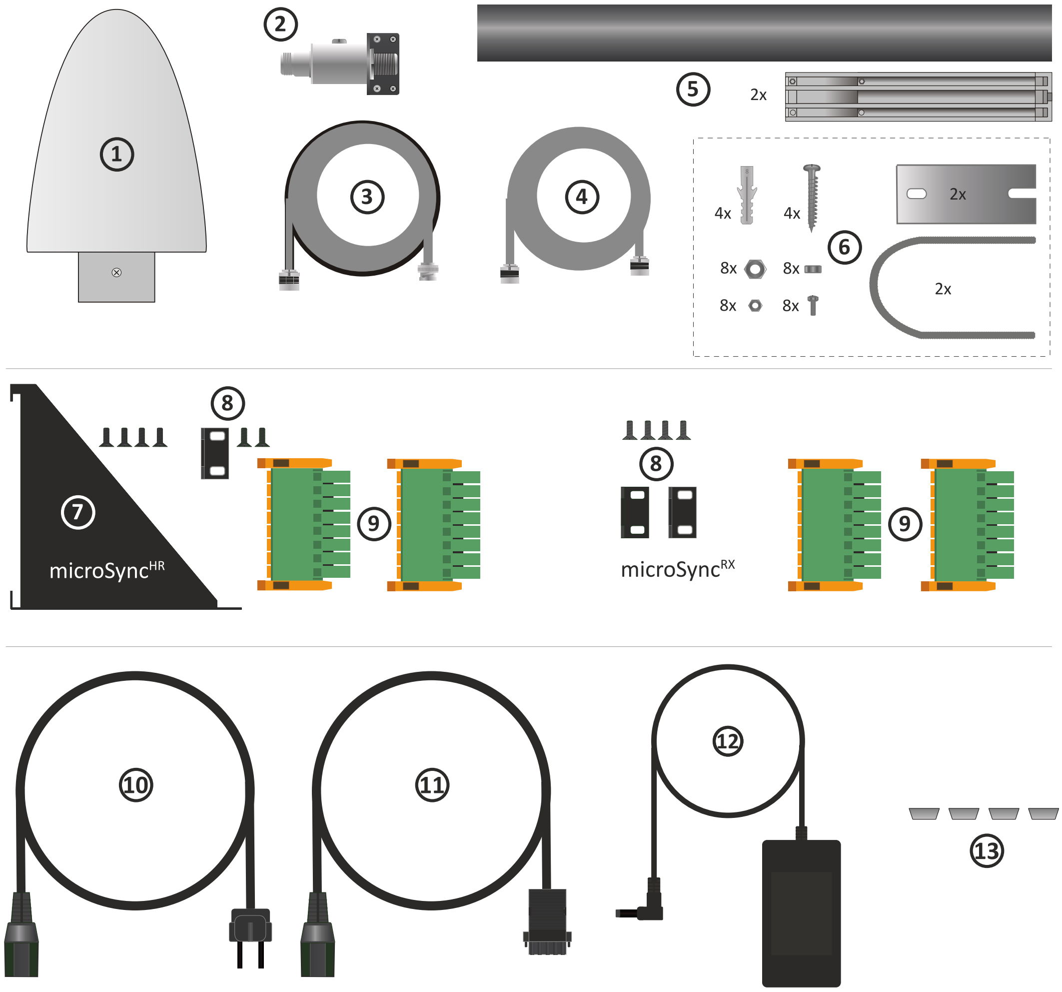
Meinberg microSync systems are designed for installation in 19-inch racks. Rack systems come with all necessary accessories (mounting brackets, screws, adapters for power supply ...). For installations in regions outside of Germany that have other standards (e.g. for power supply connections), please specify exactly which adapters or cables you need to put the device into operation when ordering.

Before unboxing the system, make sure that there is sufficient space in the built-in cabinet to ensure safe ventilation of the system. Avoid dirt and dust during installation.

 It is important that you follow the safety instructions in this manual to avoid damage to the system and personal injury.

5.6 Unboxing the Device

Carefully unpack the system and all accessories and put them aside. Check the scope of delivery with the packing list to ensure that no parts are missing. If any of the listed contents are missing, please contact Meinberg Funkuhren.



Antenna Mounting

1.	GNSS antenna
2.	Overvoltage protection (optional)
3.	Antenna cable
4.	Coaxial cable for overvoltage protection (optional)
5.	Retaining tube and clips (only for Meinberg GPS antenna)
6.	Mounting kit for Meinberg GPS antenna

Rack Mount

7.	Mounting bracket for microSync^{HR} 19-inch extension and mounting screws
8.	Mounting bracket (standard) and fixing screws
9.	Connector for DMC X1/X2 connection
10.	2 m Power cord (for microSync^{HR} 70 series & microSync^{RX})
11.	1 m Adapter cable for 5-pin voltage connection (microSync^{RX} only)
12.	Power supply (Desktop AC adapter) (for microSync^{HR} 70 series)
13.	Protection spacer

Check the system for shipping damage. If the system is damaged or cannot be put into operation, contact

Meinberg Funkuhren immediately. Only the recipient (the person or company receiving the system) can assert a claim against freight forwarder for shipping damage.

Meinberg recommends that you keep the original packaging materials for possible future transport.

Please read the safety instructions and the manual carefully to familiarize yourself with the safe and proper handling of electronic devices.

You can find the product documentation in the Meinberg customer portal: https://meinberg.support

5.7 Disposal of Packaging Materials

The packaging materials we use are fully recyclable:

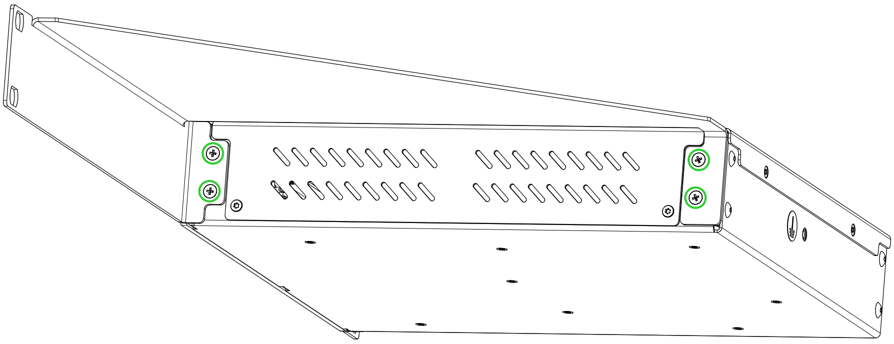
Material	Used for	Disposal
Polystyrene	Support, Cushioning, Protection (Polystyrene Peanuts, Bubble Wrap)	Recycling Depot
PE-LD Low-Density Polyethylene	Packaging of Accessories	Recycling Depot
Cardboard	Packaging for Shipping, Packaging of Accessories	Paper Recycling

6 System Installation

19 inch Rackmount

Mounting brackets and fixing screws are included in the scope of delivery of a half or full rack system. If the system is supplied with an antenna and antenna cable, it is advisable to first mount the antenna in a suitable location (see chapter Antenna Mounting) and lay the antenna cable. The power supply cable and the network cable should also be available at the installation site before the system is installed. Make sure that all necessary adapters for connecting the device are available. Make sure that the voltage is disconnected from the power source during installation.

Rackmount - microSync^{HR}



For the installation of a microSync^{HR} Half-Rack system in a 19-inch server rack, a special mounting bracket is included in the scope of delivery. Use this bracket to mount your system. The bracket is attached to the microSync^{HR} enclosure at the four green dots (see figure) using the supplied Torx screws.

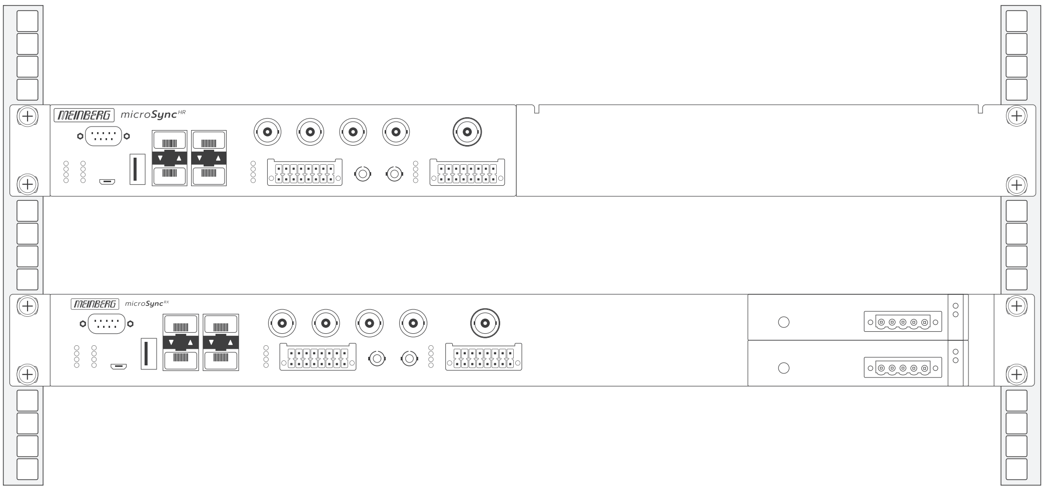


Figure: microSync^{HR} and microSync^{RX} rack mount. The screws for rack mounting are not included in the scope of delivery.

In order to meet the specified shock and vibration requirements,
special mounting brackets are required.

6.1 Connecting the System

Make sure that the system to be connected is connected to your PC or the network via either a serial or a network connection and is on the same physical network.

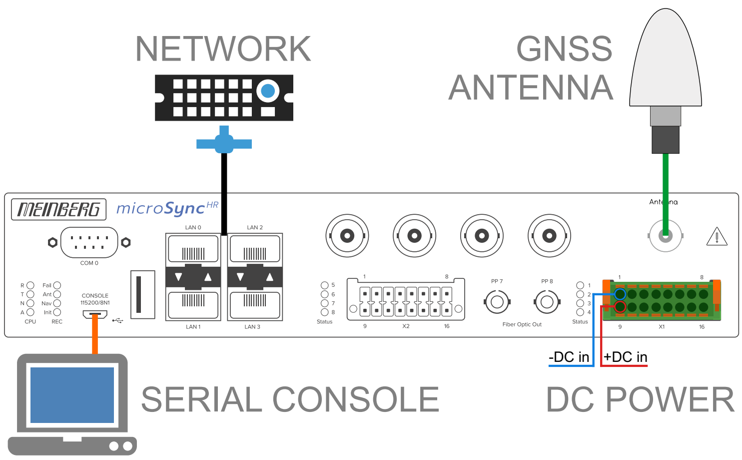


Figure: Connection scheme microSync^{HR} with power supply, network connector, serial connection and antenna link

Hint:
Please make sure that only microSync^{HR} systems receive DC power via the DMC X1 connector. For the microSync^{RX} models the voltage connection (AC/DC or DC) is made directly at the power supply unit.

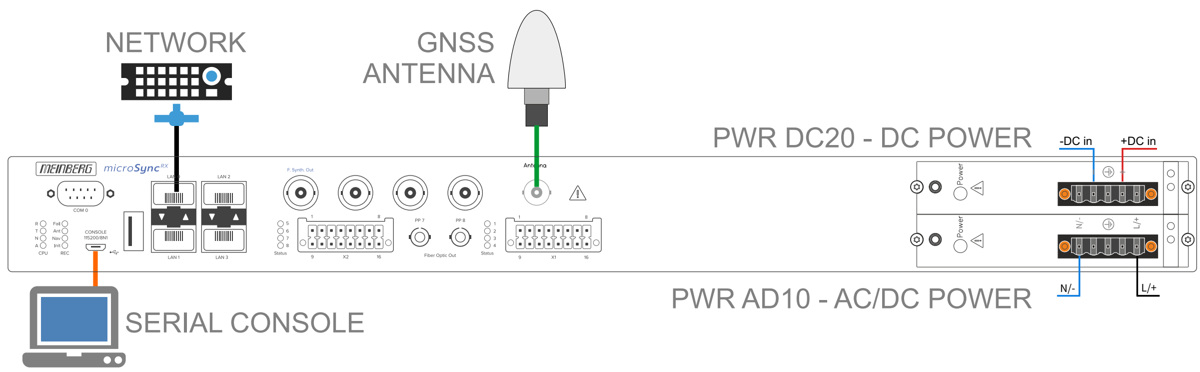


Figure: Connection scheme microSync^{RX} with power supply, network connector, serial connection and antenna link

The following section describes how you can initially put a microSync system into operation with the help of the Meinberg Device Manager Software. You can download the Meinberg Device Manager software for free from our website: https://www.meinbergglobal.com/english/sw/mbg-devman.htm

If you do not wish to install the software on your local PC, you can also download the "Portable Version" of Meinberg Device Manager and launch it directly from a portable USB storage medium.

6.2 Initial Network Configuration

Once the microSync has been successfully initialized, the initial setup process can be performed.

The microSync is shipped with DHCP disabled and a statically configured IP address. This means that a network connection must be manually established to be able to setup the device fully.

There are three ways to perform the basic network configuration of your microSync:

- Configuration via a serial connection, see Chapter 6.2.1.
- Configuration via the Web Interface, see Chapter 6.2.2.
- Configuration via Meinberg Device Manager, see Chapter 6.2.3.

6.2.1 Network Configuration via Serial Connection

The initial network configuration of the microSync can also be performed via a serial USB connection. You can connect the USB port on the PC with the micro-USB port of the microSync using a standard USB cable (Micro-USB Type B to USB-A). Your PC will recognize this connection as a serial connection.

Under Windows, you can identify which COM interface is used to communicate by opening the Device Manager. The information is usually provided under the group "*Ports (COM & LPT)*".

In many commonly used Linux distributions, the output of the terminal command *dmesg* can be used to identify which serial interface is to be used to communicate with the microSync. The relevant entry would look something like this:

```
[77833.359948] usb 1-1.2.1.6.3:  FTDI USB Serial Device converter now
attached to ttyUSB0
```

This reveals, for example, that you should establish a connection via /dev/ttyUSB0.

You can now use a terminal client such as PuTTY to establish a serial connection with the system.

Use the following connection parameters:

Conn. Type: Serial

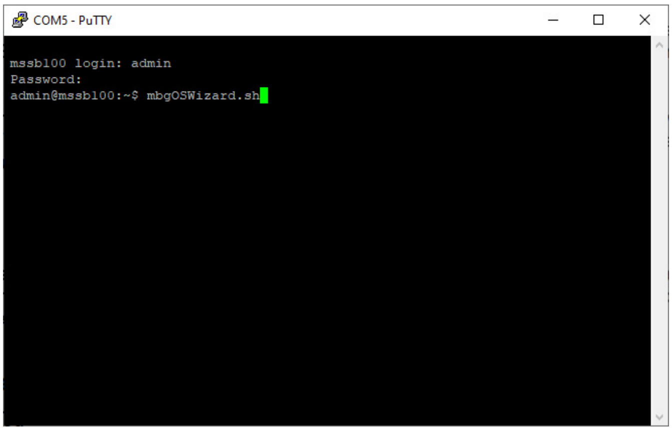
Serial Line: The serial interface identified as above (e.g., *COM13* or */dev/ttyUSB0*)

Speed: 115200

Framing: 8N1

Once the connection has been detected, you will be prompted to enter a username and password. User: *admin* / Password: *timeserver*. Press the Enter key after each entry.

Once a connection has been successfully established, you can use the meinbergOS Wizard to perform the initial network configuration.



First, launch the wizard by entering *mbgOSWizard.sh*; this will prompt you to enter the password (Default: *timeserver*).

You can now select the physical network interface that you wish to use for management purposes. The next step is to enter the IPv4 address that you wish to assign to the selected port. The final step is to enter the subnet mask (e.g., 255.255.255.0). You can then confirm your entries with '*y*'.

The initial network configuration process is now complete and you can close the setup wizard. All further configuration can be performed using the Web Interface or Meinberg Device Manager.

Information:

If the microSync's network configuration has already been previously performed using the Web Interface or Meinberg Device Manager, you will not be able to do this using *mbgOSWizard.sh*.

6.2.2 Network Configuration via Web Interface

The network configuration for the microSync can be performed via the Web Interface. In its factory-shipped state, the microSync has the following network configuration:

Network Port LAN 0

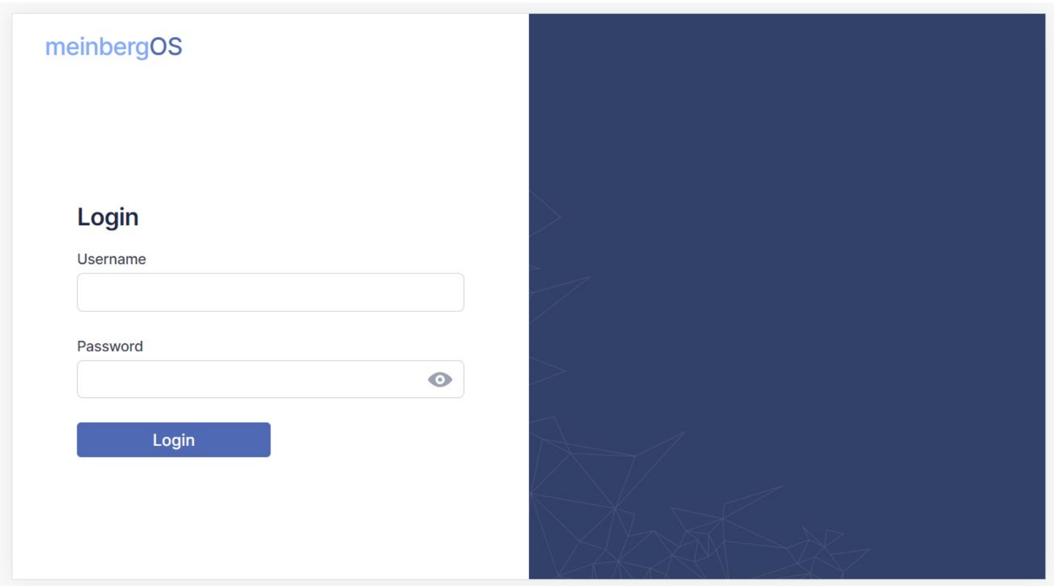
IPv4 Address: *192.168.19.79*

Subnet Mask: *255.255.255.0*

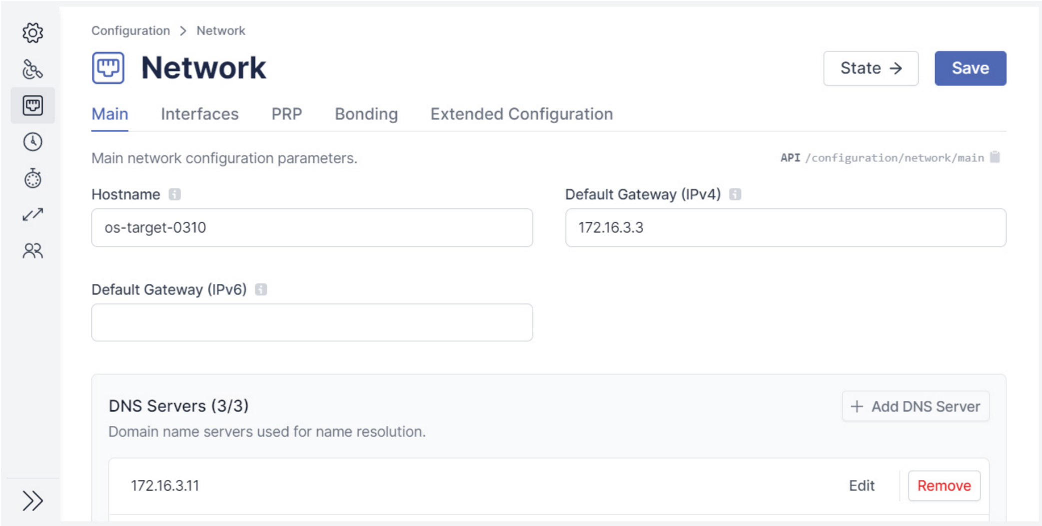
Gateway: Not defined

DHCP: Disabled

The PC from which the Web Interface will be accessed via a browser must be able to establish a network connection with the above address in the appropriate subnet. If the PC's network configuration or the network's topology or addressing prevent a connection from being established with the microSync, the network configuration of the PC will need to be (temporarily) changed and a different physical connection may need to be established (e.g. a direct network connection).



Open a web browser of your choice and open the address *https://192.168.19.79*. This should bring up the login page. Enter "*admin*" as the username and "*timeserver*" as the password.



As soon as the Dashboard appears, click on the "**Configuration**" section in the Header Bar, then select the "**Network**" tile. Be sure in particular to correctly configure the network settings for the intended management interface ("**Interfaces**" tab) to ensure that it is accessible within the subnet.

Once you have performed the configuration, click on "**Save**" to store the changes.

6.2.3 Network Configuration via Meinberg Device Manager

The network configuration for the microSync can be performed using Meinberg Device Manager (see Chapter 5.4, Additional Software).

In its factory-shipped state the microSync has the following network configuration:

Netzwerkport LAN 0

IPv4 Adresse	*192.168.19.79*
Netzmaske:	*255.255.255.0*
Gateway:	Not defined
DHCP:	Disabled

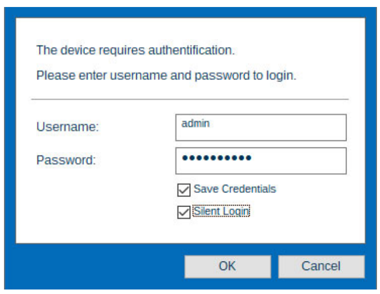
The PC on which Meinberg Device Manager is used must be able to establish a network connection with the above address in the appropriate subnet. If the PC's network configuration or the network's topology or addressing prevent a connection from being established with the microSync, the network configuration of the PC will need to be (temporarily) changed and a different physical connection may need to be established (e.g. a direct network connection).

Information:

Please ensure that any effective firewalls or other security solutions allow network traffic to pass through TCP port *10002*.

Clicking on the button "**Search Devices**" will cause all Meinberg products accessible over the network connection to be detected and then listed.

Select the device with which you wish to establish a connection. With the microSync, you will then be prompted to enter your account details. When setting the device up for the first time, please enter "*admin*" as the username and "*timeserver*" as the password.

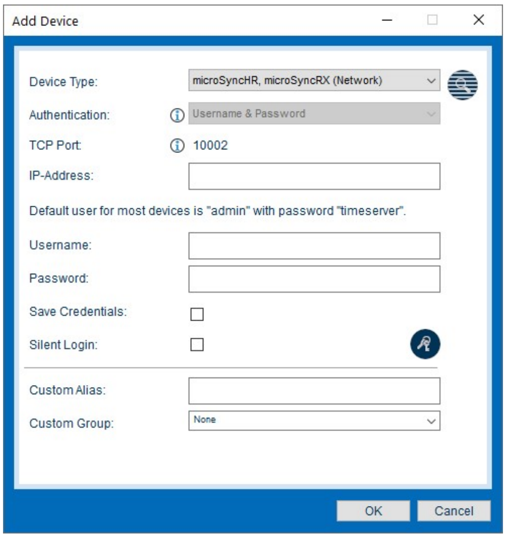


If the inserted microSync cannot be found via the automatic search, the **Add Device** button can be used to set up the connection manually.

Manual Setup

Select the connection type
microSyncHR, microSyncRX (Network).

Then enter the IPv4 address of the microSync (*192.168.19.79*). Enter "*admin*" as the username and "*timeserver*" as the password.



Once the network connection has been established, open the "**Network**" section of the left "**Config**" panel, then make the appropriate adjustments to the network settings. Be sure in particular to correctly configure the network settings for the intended management interface ("**Interfaces**" tab) to ensure that it is accessible within the subnet.

Once you have performed the configuration, click on "**Apply Configuration**" (the check mark) to store the changes.

6.3 Initial Start of Operation

6.3.1 Start of Operation with meinbergOS Web Interface

microSync systems with meinbergOS Version *2022.05.1* or later provide a feature-rich Web Interface that can be used to perform most configuration processes easily and also allows you to monitor your device's status and condition.

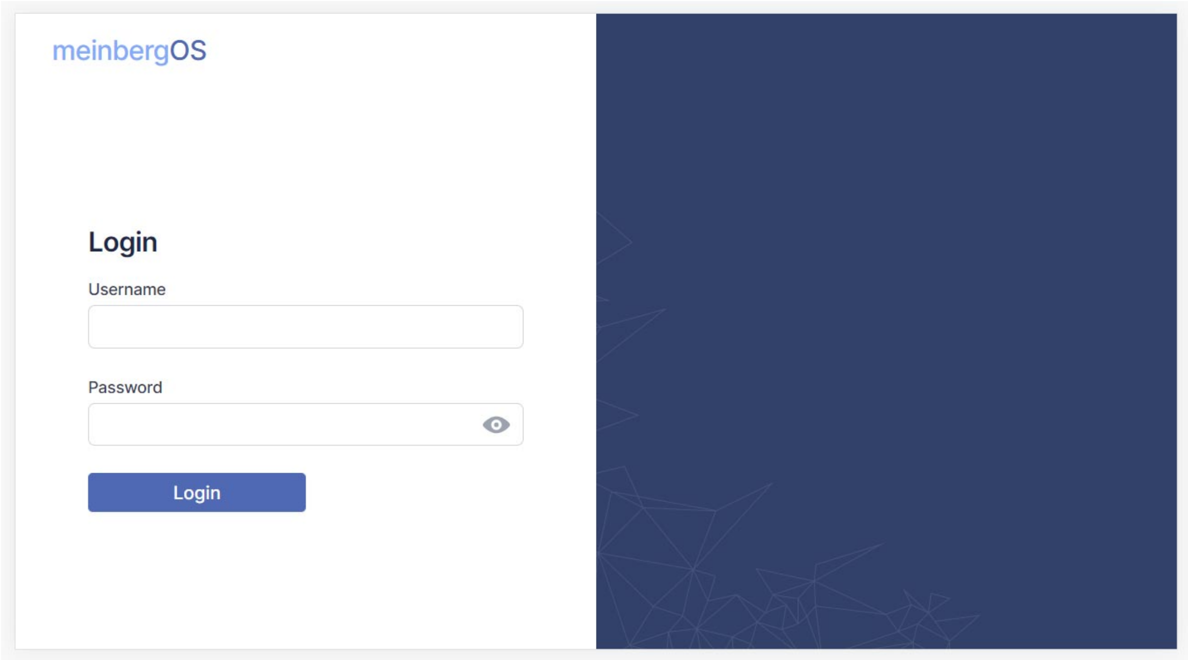


Figure 6.1: Login Page of meinbergOS Web Interface

Once you have entered the IP address of your meinbergOS device into the address bar of your web browser, the login page will appear (Figure 6.1).

The default settings are:

Username:	*admin*
Password:	*timeserver*

Further information about the meinbergOS web interface in the chapter "The meinbergOS Web Interface" to be found in the microSync installation manual:

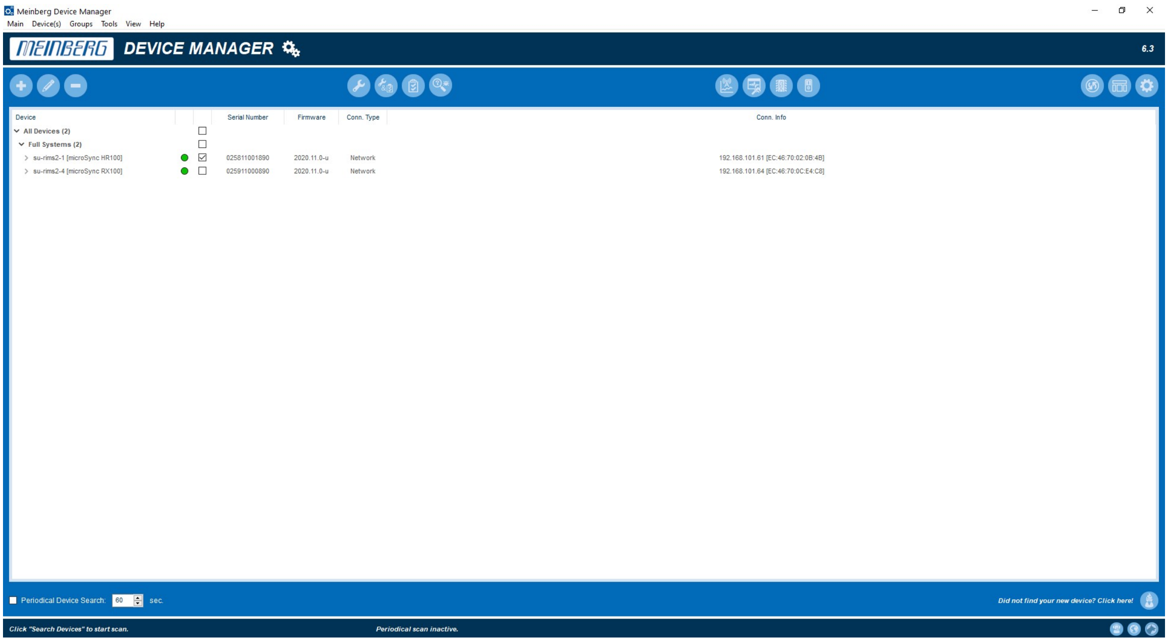
https://www.meinberg.de/download/docs/manuals/english/microsync.pdf

6.3.2 Start of Operation with Meinberg Device Manager Software

First install the Meinberg Device Manager software. After the setup, start the program. If you do not wish to install the software on your local PC, you can also download the "Portable Version" of Meinberg Device Manager and launch it directly from a portable USB storage medium.

The Meinberg Device Manager software is freely available for download from our website: https://www.meinbergglobal.com/eng
devman.htm

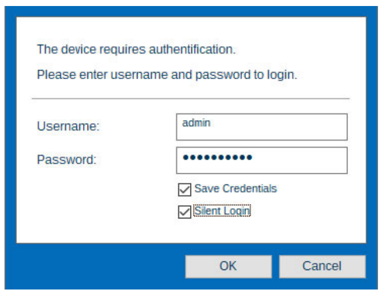
A comprehensive manual of the Meinberg Device Manager software can be downloaded here:
https://www.meinbergglobal.com/download/docs/manuals/english/meinberg-device-manager.pdf



By clicking on the Search Devices button, all available microSync systems that have a serial or a network connection are recognized by the Meinberg Device Manager and will be listed then.

- Found systems are displayed with a green dot.
- Modules that are no longer recognized are displayed with a red dot.
- Modules whose password or password/user name combination is unknown will be marked with a red x.

Use the corresponding checkbox to select the device with which you want to establish a connection. With a microSync system you will then be prompted to enter your connection data. At the initial start please use "**admin**" for user and "**timeserver**" as password.



If the connected system was not found by the automatic search, a connection can be established manually by **Add Device**.

Establishing a Network Connection
Select the connection type *Network*. Then enter the IPv4 address of the system you want to connect to.

Authentication
Select the authentication option. The option Username & Password is only supported on systems with MeinbergOS.

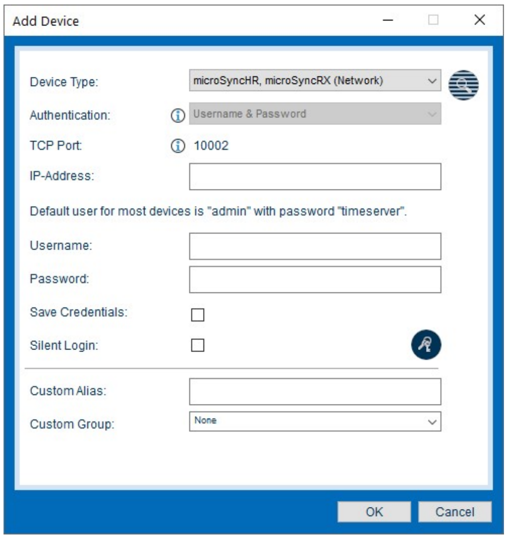
TCP Port
The TCP port is used to communicate with your system. Please make sure that the port is not blocked by your firewall configuration.

Save Credentials
With this checkbox you ensure that the Device Manager has remembered the login for this system. When the program is restarted, the User and Password fields are already filled out.

Silent Login
You have the option that the Meinberg Device Manager does not ask for a user name and password every time you log in.

Custom Alias
Assign a custom alias for better identification of individual systems/modules in Device Manager.

Custom Group
Assign the module/assembly to a previously created group.



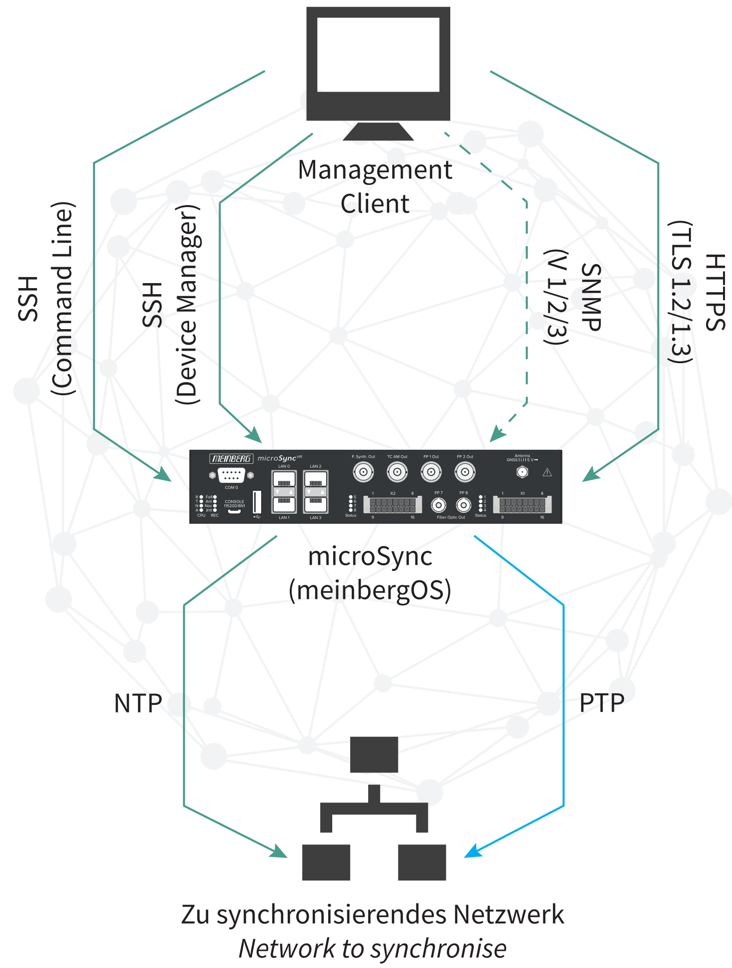
7 Security Guide

This chapter illustrates how to securely configure meinbergOS for the microSync series of products. It contains a general overview of the context in which security should be considered when managing your microSync, as well as sections on securing management interfaces, securing time services, log management, and keeping your microSync up to date with the latest firmware updates.

This Security Guide requires a basic understanding of the concepts and terminology behind public key infrastructures (PKI), RSA encryption, symmetric-key algorithms, and the TLS, SSH, NTP, and SNMP protocols.

7.1 General Overview

Before undertaking any security-related configuration of your microSync, you should first consider the following diagram. It shows the supported network services, and the connections that may be established with or by a microSync as a result.



Generally speaking, any management task can be performed over a secure connection. Ideally, this should be over the Web Interface over a *HTTPS* session, or using the RestAPI. The microSync can also be configured using Meinberg Device Manager via an SSH tunnel. Alternatively, the microSync can also be configured from the command line via an SSH terminal. However, this alternative method does not provide the same range of configuration options as Meinberg Device Manager or the Web Interface. SNMP can only be configured with read-only access. If you wish to use SNMP securely, always ensure that you are using Version 3 of SNMP, as this is the only version that allows adequately secure use of SNMP.

Secure time information can only be sent over NTP. While the NTP protocol offers features for securing the integrity and ensuring the authenticity of time information, the protocol does not support security against interception. However, in the vast majority of NTP use cases, this is not necessary. In exceptional circumstances, VPNs or network architecture segmentation can be used to prevent data interception or achieve compartmentalization. PTP currently does not support any IT security functionality, which is why NTP must be used if you need to secure your time synchronization services over insecure networks.

Meinberg recommends always using the most up-to-date browsers, service clients, and the latest version of Meinberg Device Manager to ensure that the best security algorithms for server/client communication are applied. Timely installation of updates can also help eliminate vulnerabilities and minimize the risk of a successful attack.

Detailed syslog functionality, which logs actions performed by every user or process, ensures that responsibility for system changes can be properly identified. However, log files can be modified by root or admin users after the fact, which is why these log files cannot be guaranteed to be tamper-proof.

Regular updates and a greatly streamlined operating system help to ensure maximum availability for the services. For enhanced protection against DoS/DDoS attacks, web application firewalls and conventional firewalls capable of detecting and foiling such attacks can be implemented in the network. It should be noted that any changes made to the configuration will be lost upon reboot or can be rejected by other admin users if they have not been saved to the start configuration beforehand.

7.2 Securing Management Access

The most secure way of configuring a microSync is to directly connect the client (PC, laptop, etc.) to the microSync until a more secure management channel has been set up. The description of the configuration of the microSync that follows uses the options provided by the Web Interface as an example. However, because the Web Interface does not yet provide all of the available functionality of other methods, it is necessary to use Meinberg Device Manager to perform some settings. If your microSync model features a display, the control panel can be used once the setup process for a microSync has been completed to configure an IP address (see chapter "TODOref"). If your microSync model does not feature a display, you will need to access the system via a browser using the standard IP address 192.168.19.79. This requires that the client be able to access the network 192.168.0.0. Alternatively, it is also possible to establish a serial connection with the device (see chapter "TODOref") for the purpose of modifying the IP address, subnet mask, and gateway for the network interface.

The default login details for the initial login are as follows:
Username: admin
Password: timeserver

Once you have successfully connected, you should first verify that the latest version of the firmware is installed. An update of the firmware is strongly recommended if the latest version is not already installed. The update procedure is described in the meinbergOS manual (chapter "Maintenance → Inventory → Firmware") and also in the Meinberg Device Manager manual (chapter "Firmware Configuration").

Once opening the Web Interface for the first time, your browser may display a security warning, as the certificate is "self-signed". When setting up your microSync for use for the first time via the Web Interface, the certificate must be added as an exception to your browser.

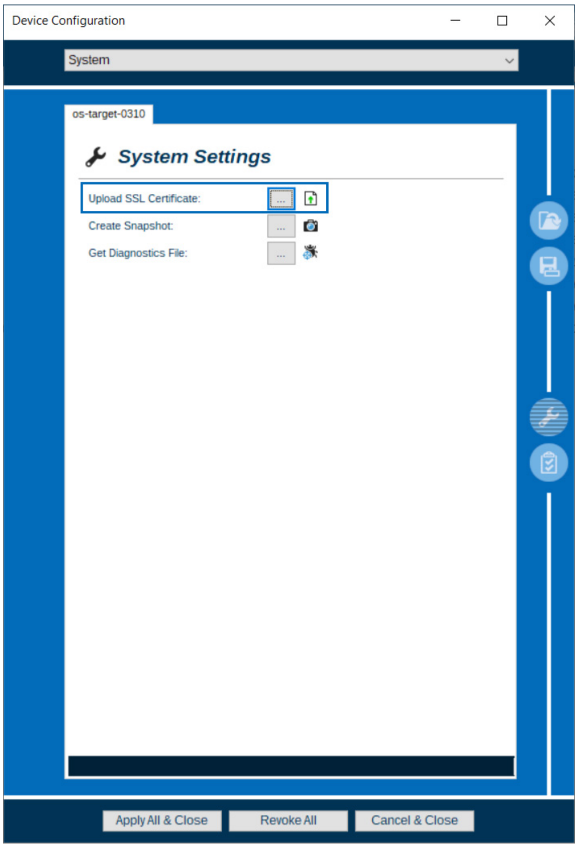


Figure 7.1: Uploading a Certificate using Meinberg Device Manager

Once the system has the latest firmware installed, you will need to provide a valid certificate for the web server or Web Interface. Currently, this needs to be done using Meinberg Device Manager using the "Upload

SSL Certificate" function as shown in Figure 7.1. Please refer to the Meinberg Device Manager manual for further information. The certificate will need to be created on a different device, as the microSync can only generate a certificate with pre-defined values in the event that no certificate exists (when first setting up the device).

To generate a certificate you can use a standard PKI solution or, alternatively, a solution such as the open-source tool OpenSSL. Your microSync will accept the certificate and its key as long as it is provided in the form of an unencrypted X.509 v3 certificate in PEM format. Meinberg recommends using a certificate with a key length of at least 2048 bits and to have the validity period as short as possible. When creating the certificate, you should also ensure that the proper SAN (Subject Alternative Name, usually the name of the device according to the DNS) and key usage extensions ("server authentication") are specified in the certificate.

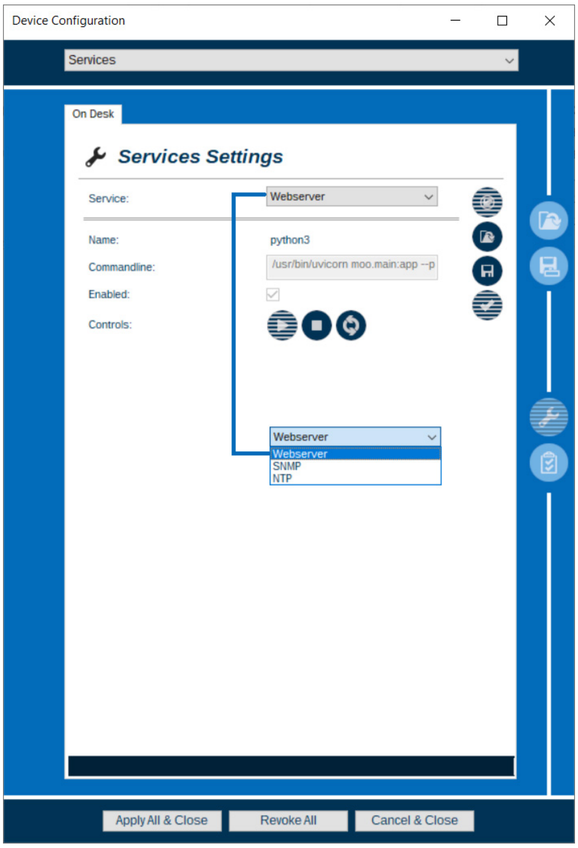


Figure 7.2: Enabling and Disabling the microSync Services

Once the certificate has been installed, a connection should be established via the browser to verify whether the certificate has been renewed. Most browser developers provide guides explaining how to display the certificate currently in use. You can then disable the services that are not required. The services also need to be configured using Meinberg Device manager, as shown in Figure 7.2. The Web Interface, NTP, and SNMP can be stopped and started using the Services menu item. PTP will only be enabeld if an instance is actually created via the PTP menu item. The SSH service cannot be entirely disabled and services are always enabled or disabled for all interfaces (with the exception of PTP).

Only version 3 of the SNMP standard in conjunction with authPriv mode guarantees a fully secured connection. The additional parameters provided by version 3 are the username (security name), access privileges, and the authentication and privacy protocols (or algorithms). SHA512 and AES256 are the most robust algorithms. As is standard, longer passwords are preferred. The configuration can be performed using the "Monitoring" form in Meinberg Device Manager. Figure 7.3 shows what this form contains.

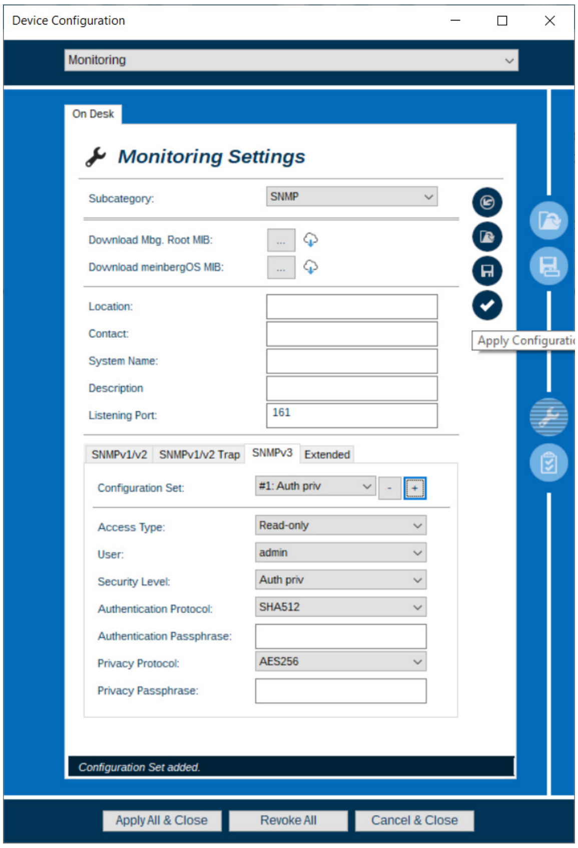


Figure 7.3: Configuring SNMP in Meinberg Device Manager

The next step is to create a new user and set a new password. This is necessary to ensure that the publicly known username/password combination can no longer be used.

The next section describes the user administration configuration options available.

7.3 User Management

meinbergOS provides user configuration options that can be modified to fulfill a given purpose. The options are provided in the Web Interface under "/admin/configuration/users". Each user can be assigned "channels" and "permissions". "Channels" dictate which connections or channels a user can log on to the device, while "permissions" determine which functions can be operated through these channels by that user. These permissions apply to all channels. The available channels are "Web Interface", "Device Manager", "Shell" (command line), and "SNMP". In addition to the normal "permissions", there are another two special permissions—"Allow Multiple Sessions" and "Allow sudo in Shell". The "Allow Multiple Sessions" permission enables a given user to log on to the device from multiple clients at the same time, while the "Allow sudo in Shell" permission enables the user to execute commands with root privileges from the command line.

In order to simplify the configuration of the permissions somewhat, there are three pre-defined user permissions templates: Admin, Info, and Status. These templates can be selected when creating a new user, and the profiles can then be fine-tuned accordingly.

The following should be heeded in particular when assigning permissions to users:

- A user that possesses the "write config Network" permission will be able to acquire root privileges.
- A user that possesses the "write config Users" permission will be able to acquire root privileges.
- A user that possesses the "write config System" permission will be able to acquire root privileges.
- A user that possesses the "write config Firmware" permission will be able to acquire root privileges.
- To create a diagnostic file, the user requires the "write config System" permission as well as Shell channel access.
- To upload a firmware file (via the Web Interface), the user requires the "write config System" and "write config Firmware" permissions.
- To view the system log files, the user requires the "read state System" permission and Shell channel access.
- Write permissions also include read permissions via the RESTful API.

The following table shows which permissions are required for which functions in the Web interface, RESTful API or Meinberg Device Manager.

Effects of permissions on configuration via the Web Interface or RESTful API:
Note: The system of notation used here (e.g., "admin/maintenance/inventory,firmware") refers to the address of the selected menu item as located in the meinbergOS Web Interface – *"https://[MICROSYNC.IP]/admin/maintenance/inventory#firmware"*.

	Read State	**Read Configuration**	**Write Configuration**
Database	No effect	No effect	No effect
Firmware	No effect	/admin/maintenance/ inventory,firmware displayed in WebUI and API	/admin/maintenance/ inventory,firmware modifiable in WebUI and API
IO Ports	/state/IOPorts displayed in WebUI	/configuration/IOPorts displayed in WebUI	No effect
Monitoring	No effect	No effect	No effect
Network	Network displayed in Dashboard, /state/network, and readable in API	Network displayed in Dashboard, /configuration/network, and readable in API	/configuration/network modifiable in WebUI and API
NTP	NTP displayed in Dashboard, /state/ntp, and readable in API	Network displayed in Dashboard, /configuration/ntp, and readable in API	/configuration/ntp modifiable in WebUI and API
Password	Not available	Not available	Own password modifiable
PTP	/state/ptp displayed in WebUI und readable in API	/configuration/ptp displayed in WebUI und readable in API	/configuration/ptp modifiable in WebUI and API
Receiver	No effect	No effect	No effect

Table: Read/Write Permissions

	Read State	Read Configuration	Write Configuration
Sensors	No effect	Not available	Not available
Ref.Sources	/state/references displayed in WebUI and readable in API	/configuration/references displayed in WebUI and readable in API	/configuration/references modifiable in WebUI and API
Serial Ports	No effect	No effect	No effect
Services	No effect	No effect	No effect
System	System displayed in Dashboard and readable in API	System readable in API	"Save as Startup" operable, modifiable in API
Users	/state/users displayed in WebUI and readable in API	/configuration/users displayed in WebUI und readable in API	/configuration/users modifiable in WebUI and API

Table: Read/Write Permissions

Effects of permissions on configuration via Meinberg Device Manager:

	Read State	**Read Configuration**	**Write Configuration**
Database	No effect	Function "Show GNSS Statistics" enabled	No effect
Firmware	Not available	/configuration/firmware displayed	/configuration/firmware modifiable
IO Ports	/state/IOPorts displayed	/configuration/IOPorts displayed	/configuration/IOPorts modifiable
Monitoring	/state/monitoring displayed	/configuration/monitoring displayed	/configuration/monitoring modifiable
Network	/state/network displayed	/configuration/network displayed	/configuration/network modifiable
NTP	/state/NTP displayed	/configuration/NTP displayed	/configuration/NTP modifiable
Password	Not available	Not available	No effect
PTP	No effect	No effect	No effect
Receiver	/state/clock/satellites, /state/clock/clock and /state/clock/overview displayed	/configuration/clock/clock displayed	/configuration/clock/clock modifiable
Ref.Sources	/state/references displayed	/configuration/references displayed	/configuration/references modifiable
Sensors	/state/sensors displayed	Not available	Not available

Table: Read/Write Permissions

	Read State	**Read Configuration**	**Write Configuration**
Serial Ports	Not available	/configuration/clock/ serialports displayed	/configuration/clock/ serialports modifiable
Services	/state/services displayed	/configuration/services displayed	/configuration/services modifiable
System	/state/system and /state/clock/system displayed	/configuration/system, /configuration/clock/ system, and /configuration/clock/ timezone displayed	/configuration/system, /configuration/clock/ system, and /configuration/clock/ timezone modifiable, "Save as Startup" operable
Users	/state/users displayed	/configuration/users displayed	/configuration/users modifiable

Table: Read/Write Permissions

Figure 7.4 shows an example of a configuration form in the Web Interface for a user's permissions. This form can be found at "Admin → Configuration → Users".

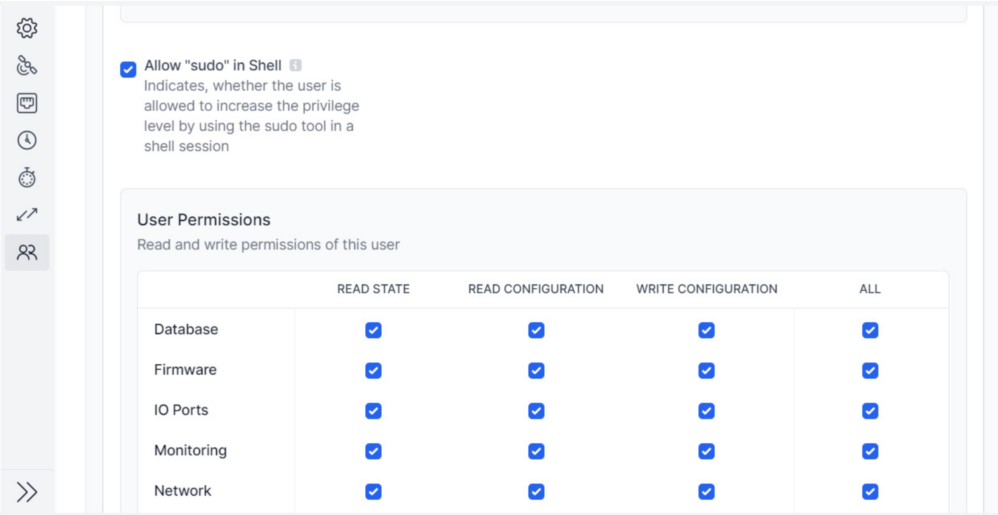


Figure 7.4: Management of a User's Permissions

A microSync in its factory-shipped state has three users: *admin*, *info*, and *status*. Because these usernames/-password combinations are quoted in publicly available documentation, the users will need to be replaced. To this end, a new user must first be created that has all permissions and thus serves as the admin user. To create a new user, the pre-defined admin user must be used to log on to the Web Interface. This is done using the username *admin* and the password *timeserver*.

You can then create a new user under "/admin/configuration/users" using the button shown in Figure 7.5. The "Create New User" page can be see in the image 7.6.

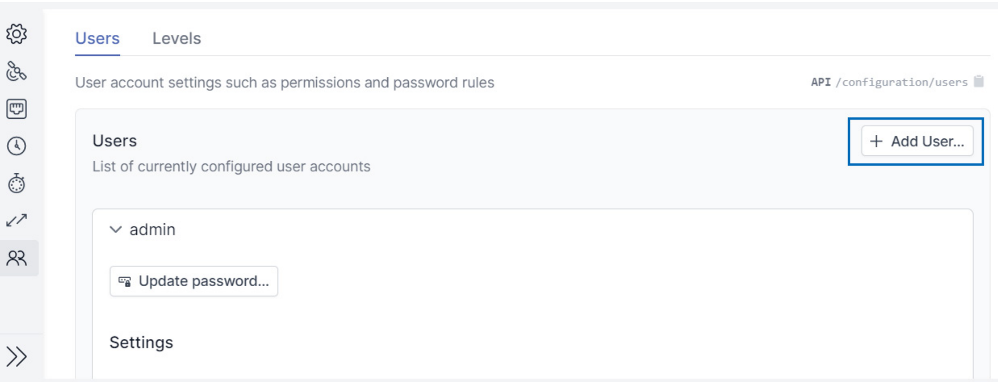


Figure 7.5: Creating a New User

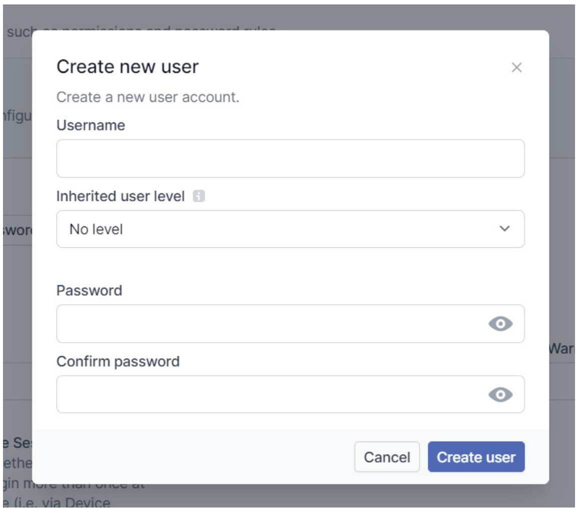


Figure 7.6: New User Page

You can set not only the username and password here, but also the user level to be used as a template for the permissions. The "admin" user level is recommended as the template for the new admin user. Once the page has been completed, the user can be created by pressing the "Create User" button. You can now use the new admin user to log on again. From this new admin account, you can now delete all of the pre-defined users and create additional users with permissions specifically adapted to the tasks to be performed.

7.4 Securing the NTP Time Service

The NTP time service provides several methods for authenticating and ensuring the integrity of packet transmissions. The NTP Autokey method is considered to be insecure, which is why this guide illustrates how to configure the symmetric key method. All of the configuration options are described in detail in the chapter TODOref. The following sections describe the configuration process.

Configuring Symmetric Key Encryption
The system requires a symmetric key to establish a secure connection. The "Symmetric Keys" form is provided in the Web Interface under "Configuration → NTP" for creating keys. The required keys are entered into the "Key" field. The ID and type and can be selected as required. As soon as the checkbox "Trusted" is enabled, a client can authenticate the microSync and ensure the integrity of the packets received when submitting queries.

If you wish to implement the strongest security currently supported, use AES-128 CMAC keys.

Additional keys can be added using the button **Add Symmetric Key**.

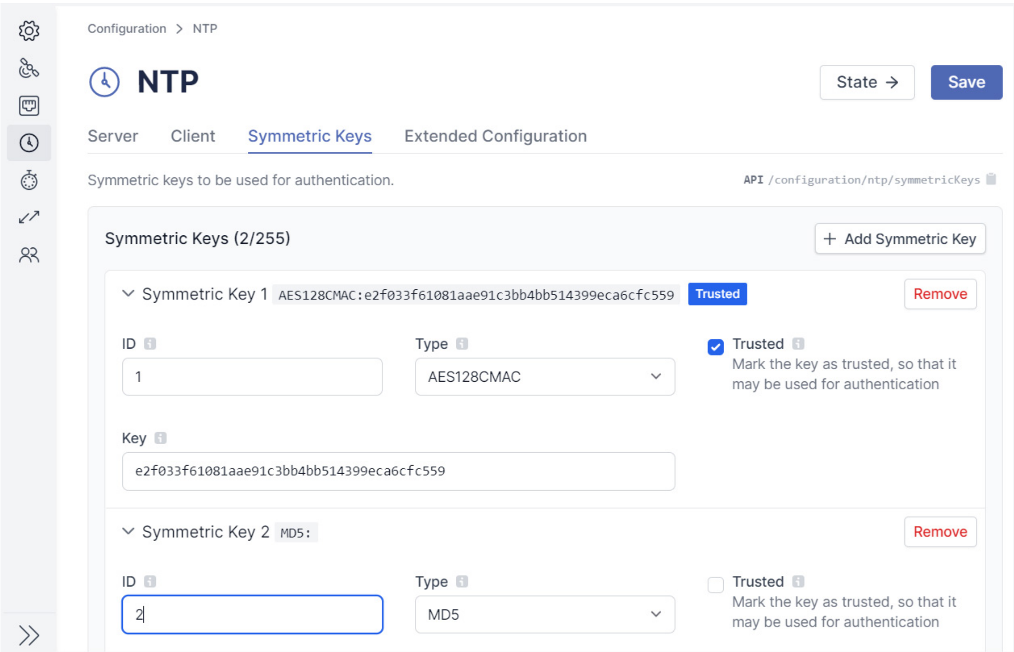


Figure 7.7: Configuring Symmetric Keys

Figure 7.7 shows an example of an AES-128 CMAC NTP key. The "Extended Configuration" form enables additional NTP configuration options to be set that are otherwise not available in the pre-defined parameters. For example, if you wish to reject all unauthenticated queries, you can enter the keyword "notrust" here using an NTP "restrict" statement.

If the microSync is to act as a client and will be synchronized with another NTP server, an external NTP server will need to be specified using the "Client" form. This connection can also be secured using symmetric keys. As soon as a key has been marked as "Trusted" and the checkbox "Authentication Enabled" has been activated as shown in Figure 7.8, you can use "Authentication Key ID" to select a key to be used for authentication.

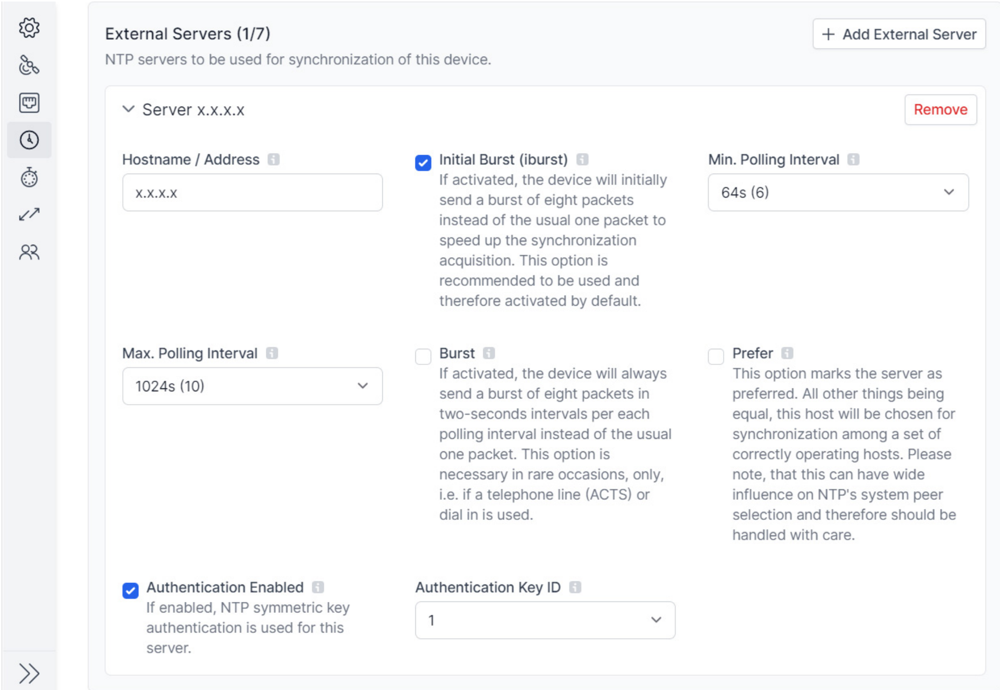


Figure 7.8: External NTP Server Configuration

7.5 Event Logs

The meinbergOS operating system used by your microSync provides two ways of delivering event log/status information to a centralized monitoring server: syslog and SNMP. It is also possible to configure the system to have certain events such as logons or temperature limit overruns sent over SNMP or output to syslog. At present, it is only possible to cryptographically secure SNMPv3 transmissions.

It is good practice to collect event log information on a central server for the purpose of comparison and review for anomalies. When using services other than SNMPv3, however, it is important to note that there is a risk of information being intercepted due to the lack of encryption.

External syslog servers can be configured using Meinberg Device Manager under "Monitoring → Syslog" as shown in Figure 7.9.

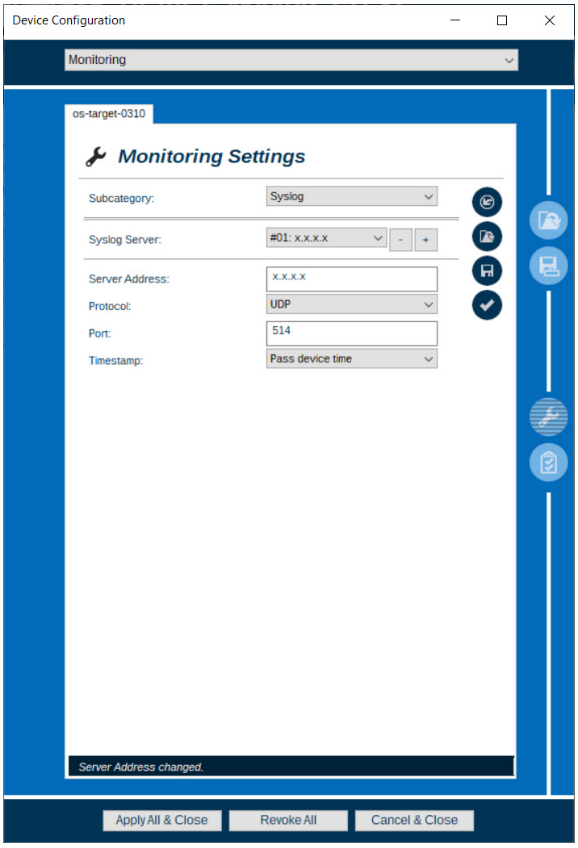


Figure 7.9: Configuring an External syslog Server

Using the settings previously described in Chapter Securing Management Access, SNMPv3 can be configured to be secure. SNMP traps are only possible with Version 2, but SNMPv2 traps cannot be secured to the same level as SNMPv3.

7.6 Updating the Firmware and Backing Up the Configuration

Firmware files can be uploaded to the microSync via the Web Interface using the button **Install New Firmware** on the page "Maintenance → Inventory → Firmware" as shown in Figure 7.10. The update process can then be triggered by selecting a file and clicking on "Install Firmware" in the panel that then appears. Once the button "Activate New Firmware Now" has been pressed, the firmware will be activated and the device will be rebooted, provided that the upload process was completed without any errors.

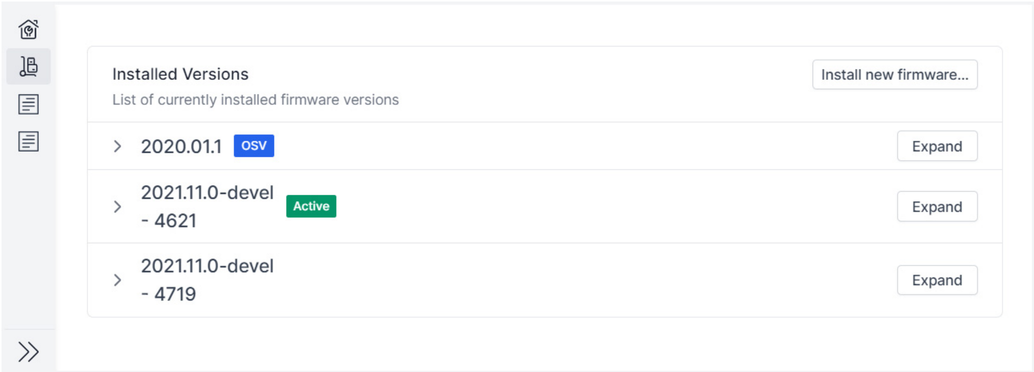


Figure 7.10: Installing a New Firmware Version

The microSync's configuration is preserved with each firmware update. The permitted cryptographic algorithms for *SSH* and *HTTPS* are specified by the firmware version in question.

It is possible to create a backup of the entire configuration via Meinberg Device Manager using the button **Save Multiple Subject Configurations**. In the window that then appears, all of the configuration subjects can be selected and backed up. The button **Load Multiple Subject Configurations** can be used to restore a configuration backup.

The two buttons are marked in Figure 7.11.

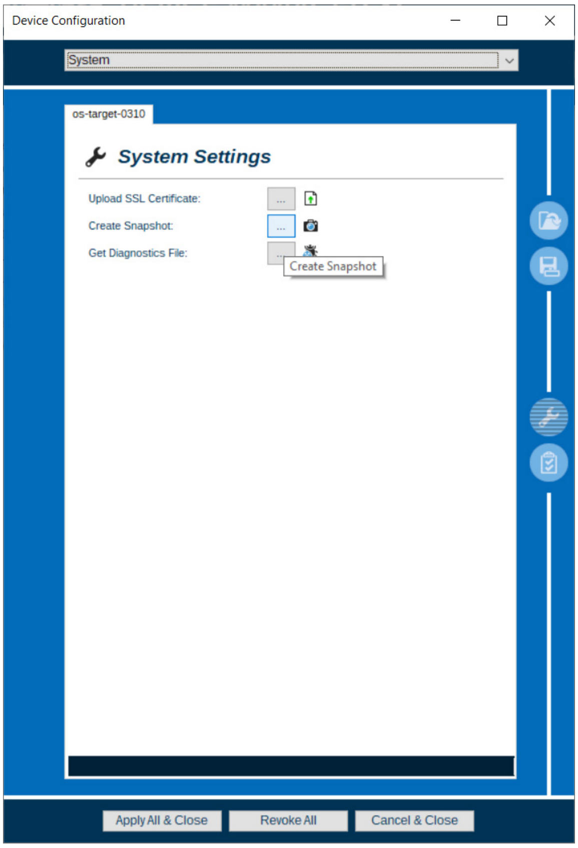


Figure 7.11: Backing Up and Restoring a Configuration

8 The meinbergOS Web Interface

8.1 Introduction: meinbergOS Web Interface

microSync systems with meinbergOS Version *2022.05.1* or later provide a feature-rich Web Interface that can be used to perform most configuration processes easily and also allows you to monitor your device's status and condition.

The meinbergOS Web Interface provides access to your microSync system's most essential configuration functions and also allows you to monitor the status of the system, install new firmware versions, and archive old versions.

For many operations, the Web Interface therefore eliminates the need to install a desktop application or run a portable application from a portable USB storage medium.

The Web Interface will be updated automatically whenever the meinbergOS device firmware is updated.

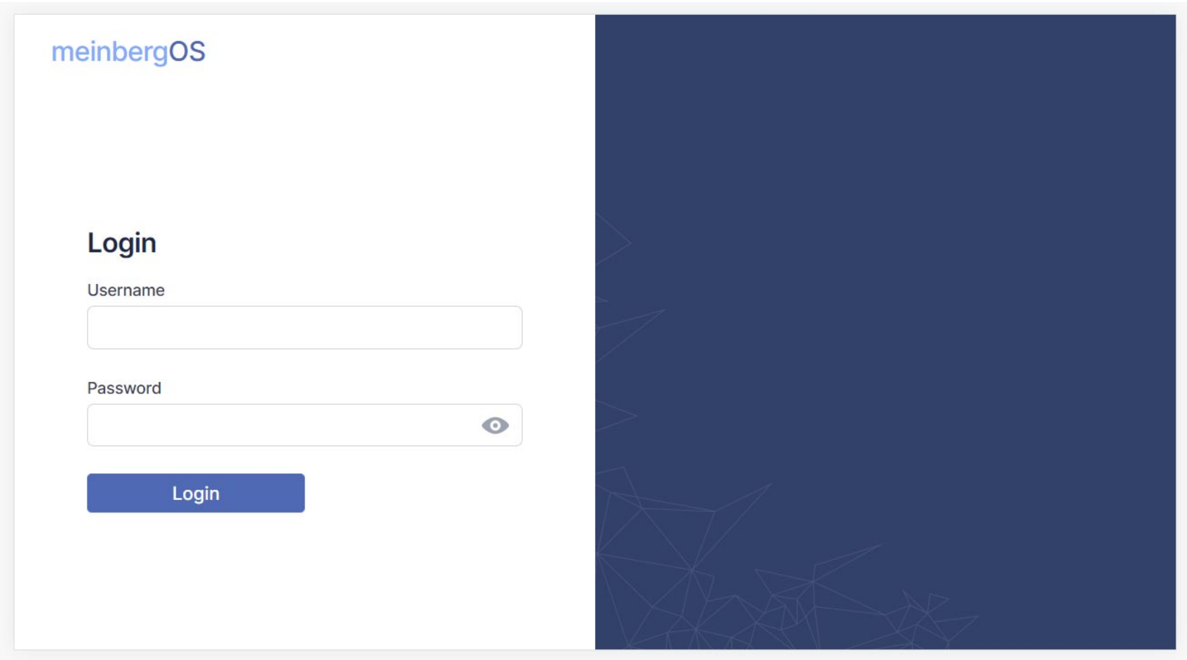


Figure 8.1: Login Page of meinbergOS Web Interface

Once you have entered the IP address of your meinbergOS device into the address bar of your web browser, the login page will appear (Figure 8.1).

The default account details are:

Username: `admin`
Password: `timeserver`

Information:

If your meinbergOS system is not yet configured for your network, please refer to the Technical Reference of your meinbergOS system, specifically the chapter "**Initial Network Configuration**", for further information on how to configure your meinbergOS system accordingly.

Information:

In the interest of optimizing the security of your meinbergOS device, it is recommended to carefully study not only this manual but also the **meinbergOS Security Guide**, which is available from Meinberg if you do not already have it.

8.1.1 Terminology of Navigation Elements in the meinbergOS Web Interface

The following terminology is used to describe the display and navigational elements that are employed in the meinbergOS Web Interface:

The **Web Interface** (always capitalized) denotes the entirety of the meinbergOS configuration and monitoring interface accessible via a conventional web browser.

The **Header Bar** (always capitalized) is the navigation bar at the top of the page in the standard meinbergOS page layout. While in *Light Mode*, it is distinguished by its dark blue background.

The **Sidebar** (always capitalized) is the bar located on the left of the page, containing links to the various subsections of each section.

The **User Menu** (always capitalized) is the menu available by selecting the user name at the right of the Header Bar.

Page refers to any complete page layout in the web browser, including Header Bar, Sidebar, and tabs, as well as the contents of the section. It can also refer to any page that does not conform to the standard meinbergOS Web Interface layout (e.g., login page).

The **Content Area** (always capitalized) is the area in which all content is shown outside of the Header Bar and Sidebar. In *Light Mode* it is distinguished by its white background.

Section refers to the four main sections listed in the Header Bar: **Dashboard**, **Configuration**, **State**, **Maintenance**.

Subsection refers to a subdivision of a section, linked to in the Sidebar and marked by icons on the left.

Tab refers to a subdivision of a subsection, which groups information and options under the horizontally organized headers beneath the heading of each subsection in the Content Area. The active tab is underlined. Tabs can also be accessed via the Sidebar, where they are listed (without icons) beneath the open subsection.

Panel refers to any wide rectangular layout element denoted by a title with information or options below it. Panels may also feature **sub-panels**. Panels and sub-panels may feature a right-facing arrow ">" on the left and/or a button marked **Expand** or **Collapse** on the right, if space could reasonably be saved by hiding the content. In this case, a collapsed sub-panel can be expanded by selecting it to reveal more information or options, and an expanded sub-panel can be collapsed by selecting it again to hide this information and options.

Checkbox refers to any navigational element that can be enabled (denoted by a rounded square with a checkmark) or disabled (denoted by an empty rounded square).

Button refers to any element that is solely clicked on (using a mouse or touchpad) or pressed (on a touch display) to perform a given function.

Tile refers to any rectangular or square element that is part of a grid-like layout (such as that on the Dashboard) and provides a brief overview of the information that can be accessed by selecting it.

Dialog box refers to any prompt that appears inside a page that renders the rest of the page inoperable until closed (for example, a file selection dialog box).

An element is described as **grayed out** if a normally black or colored navigation element is deliberately displayed in a light gray against a white background for the purpose of indicating that it is not modifiable.

8.1.2 Formatting and Structural Principles of this Manual

This manual applies the following formatting and structural conventions in relation to the meinbergOS Web Interface:

Structure

Sections of the meinbergOS Web Interface are described in first-level chapters, specifically **Chapters** 8.3 (Dashboard), **8.4** (Configuration), **8.5** (State), and **8.6** (**Maintenance**).

Subsections of a given section of the meinbergOS Web Interface are described in second-level chapters beneath that section, for example **Chapter** 8.4.2, **Configuration - Network**.

Tabs under a subsection of the meinbergOS Web Interface are described in third-level chapters beneath that subsection, for example, **Chapter** 8.4.2.2, **Configuration - Network - Interfaces**.

Where specific guidance regarding selected processes is warranted, it is provided in a corresponding second, third or fourth-level chapter under the relevant section, subsection, or tab where it is conventionally performed and prefixed with the word "Guide". Example: **Chapter** 8.6.1.4**, Guide: Installing a New Firmware Version**.

Formatting

Names of sections, subsections, and tabs are displayed in **bold text**. The full navigational path to a given tab or subsection is shown in quotation marks, bold, and separated by a right arrow symbol (→). Example: "**Configuration** → **Network** → **Interfaces**".

Field names, and button labels are also displayed in **bold text**. Example: **Install New Firmware**.

Filenames, possible values, and listed options for a configuration or status field are conventionally listed in *italics*. Example: The firmware is provided as an *.ufu* file.

References to other chapters in this manual are shown in dark blue and bold, and if the manual is viewed in a supported PDF reader, can be clicked on to directly jump to that chapter. Example: **Formatting and Structural Principles of this Manual**.

8.1.3 Basic Configuration Principles

meinbergOS operates on the basis of a dual-configuration system: the **Running Configuration** and the **Startup Configuration**.

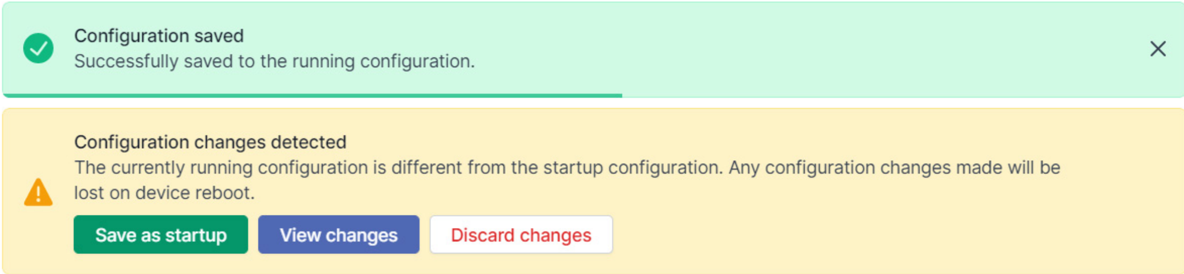


Figure 8.2: meinbergOS Web Interface: Saving Changes to the Running Configuration

The **Running Configuration** is the configuration that is currently active on the meinbergOS device. Whenever a change to the configuration is applied using a "**Save**" button, that change will be confirmed using the green dialog box shown in the screenshot above, which confirms that it has been applied to the Running Configuration.

The **Startup Configuration** is the configuration that is applied as the Running Configuration when the meinbergOS device is (re)booted. If there are differences between the current Running Configuration and the saved Startup Configuration, the yellow dialog box shown in Fig. 8.2 will be displayed. To save the Running Configuration as the Startup Configuration, click on **Save as Startup** and the Startup Configuration will be overwritten with the current Running Configuration.

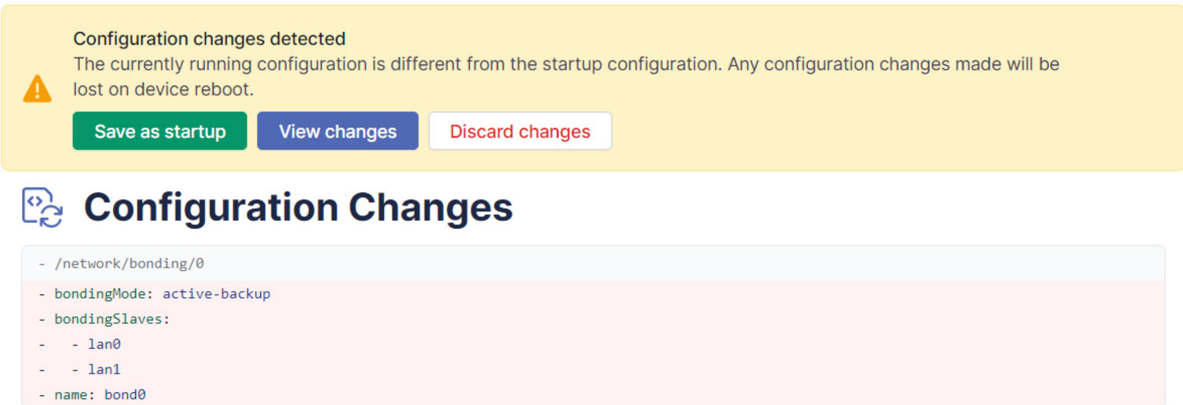


Figure 8.3: meinbergOS Web Interface: Reviewing Changes to the Configuration

If you are unsure which changes have been made to the configuration and wish to review them before adopting them as the Startup Configuration, click on **View Changes** to view the changes that have been made (see Fig. 8.3).

To reject all changes to the configuration and re-apply the Startup Configuration, click on **Discard Changes**.

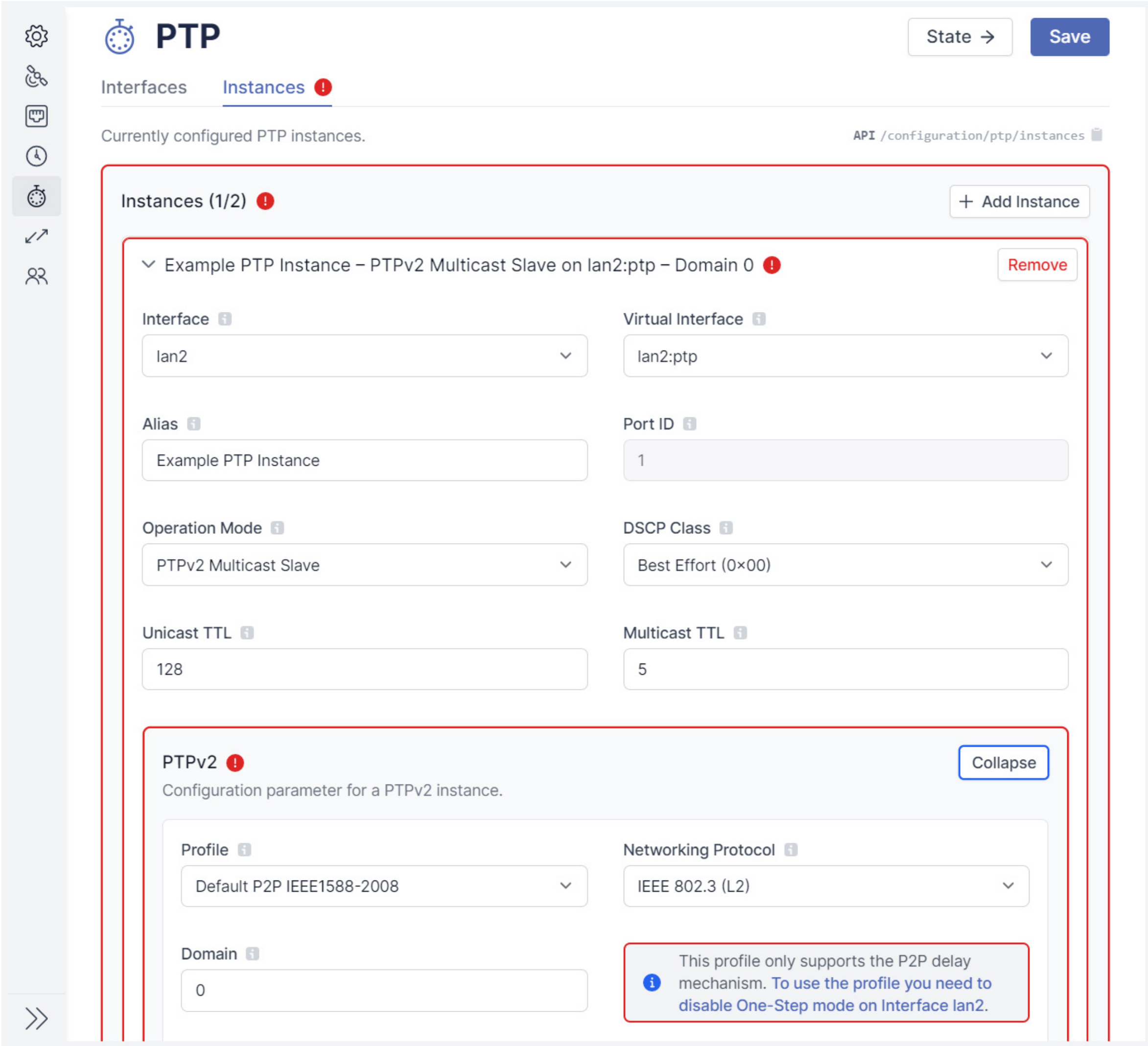


Figure 8.4: meinbergOS Web Interface: Detailed Indication of an Error in Configuration

If a configuration cannot be saved due to an error in an entry or a conflict between two settings, the red dialog box shown in Fig. 8.4 will appear and the source of the conflict or error will be identifiable by a red frame and red alert symbol around the relevant panels and/or fields.

If the source of the conflict or error is located in another subsection, the corresponding tab will show a red alert symbol next to it.

Figure 8.5: meinbergOS Web Interface: Automatic Adjustment of a Parameter

When a parameter is manually adjusted, meinbergOS may automatically adjust another parameter in the same subsection to ensure consistency and avoid configuration conflicts. When this happens, a notification will appear at the bottom of the page with a black background (Fig. 8.5), indicating what exactly has been changed.

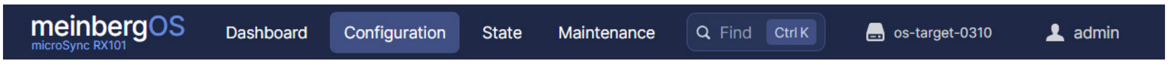


Figure 8.6: meinbergOS Web Interface: Header Bar

8.2 Header Bar

The **Header Bar** (Fig. 8.6) is the primary method of navigation throughout the meinbergOS Web Interface. It can be used to navigate to any of the Web Interface's four main sections, and provides a **Find Anything** tool for locating a certain option in the Web Interface's many sections, subsections, and tabs. It also provides a summary of the configured network interfaces, and a user menu for managing the visual design of the interface and the current user account.

Find Anything

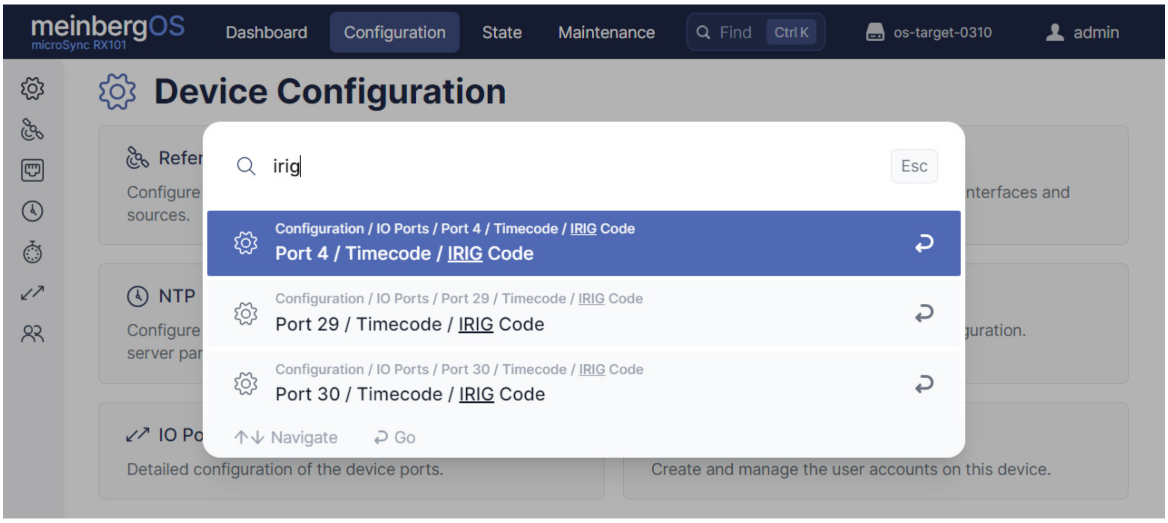


Figure 8.7: meinbergOS Web Interface: Find Anything

The **Find Anything** tool (Fig. 8.7) can be used to quickly find and immediately jump to any option found in any section, subsection, or tab of the Web Interface. As the field suggests, it can also be accessed from a keyboard using the *CTRL+K* shortcut (or *Command+K* if using a browser under MacOS). Enter the search term, then click on the desired entry in the search results dialog box that appears in the middle of the page.

Network Summary

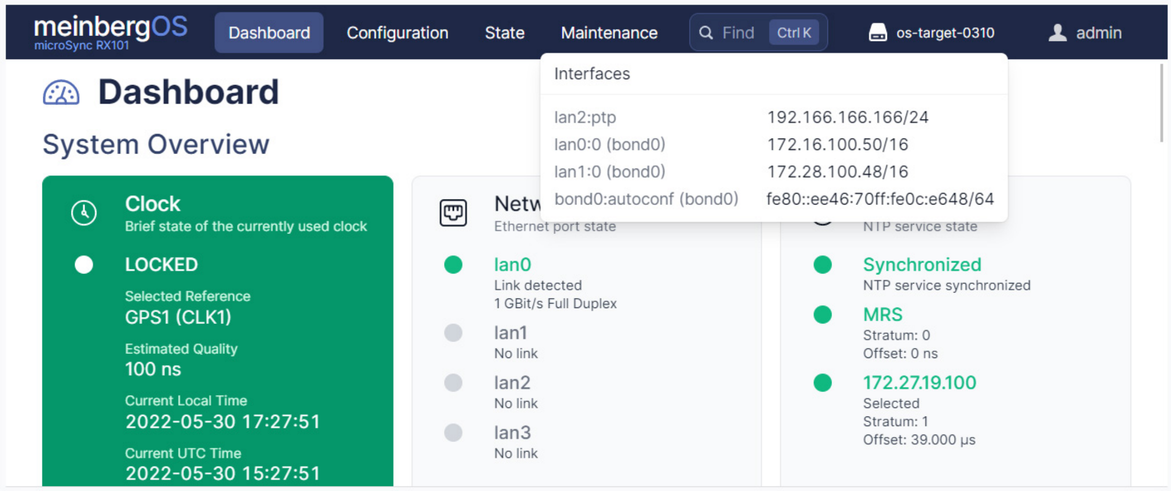


Figure 8.8: meinbergOS Web Interface: Network Summary

The **Network Summary** (Fig. 8.8) displays the current hostname of the meinbergOS device (*os-target-0310* in the example above) and can be selected to display an overview of the currently configured network interfaces.

User Menu

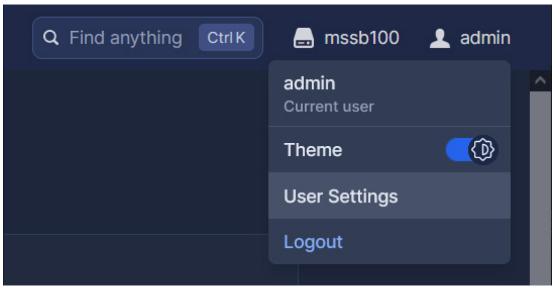


Figure 8.9: meinbergOS Web Interface: User Menu

The **User Menu** (Fig. 8.9) shows the current username. One of its functions is to change the account password (via **User Settings**), which we urgently recommend you do once the system is set up.

The "**Theme**" switch can be used to change the meinbergOS color scheme between *Light Mode* and *Dark Mode*. *Dark Mode* may be easier on the user's eyes when working in poorly lit environments.

8.3 Dashboard

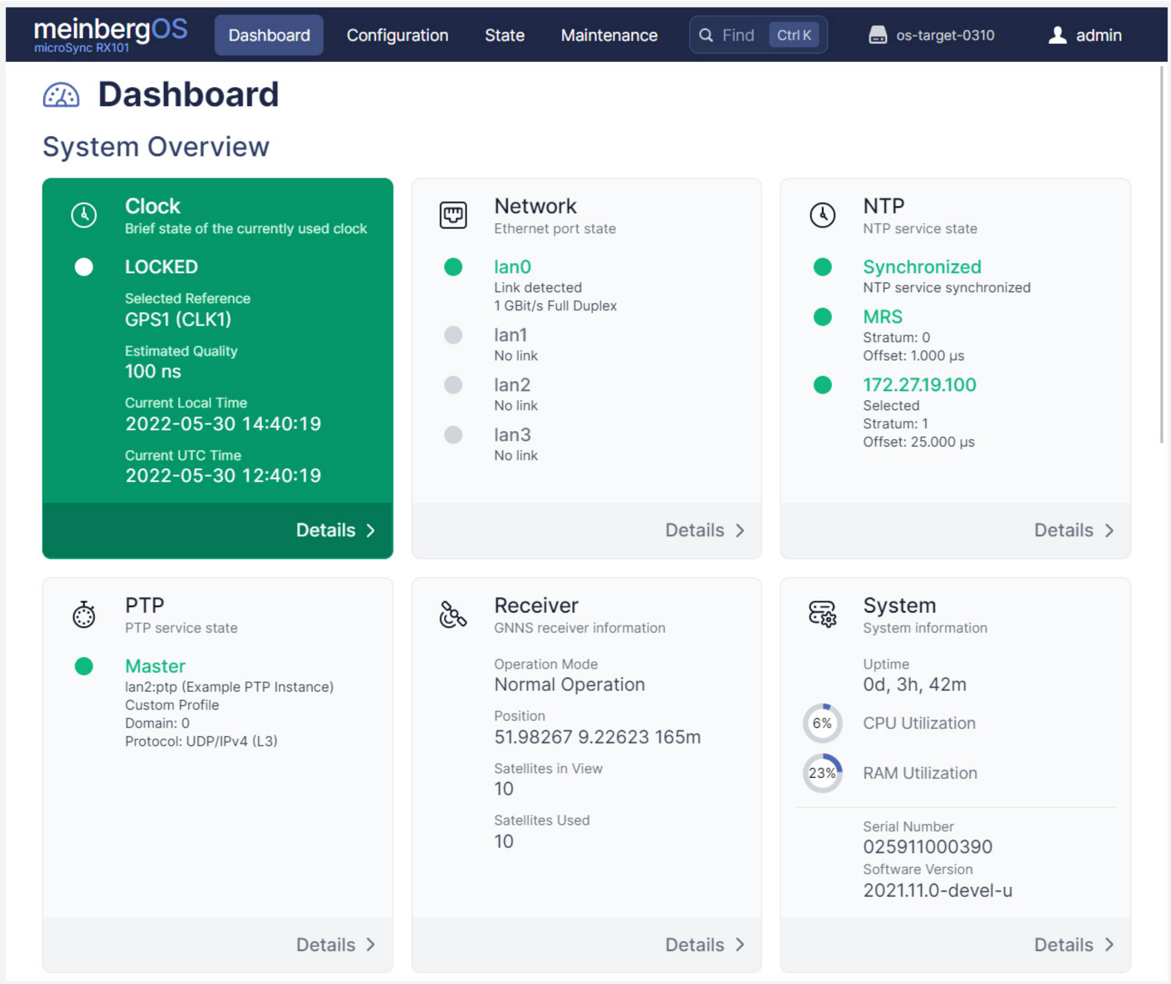


Figure 8.10: meinbergOS Web Interface Dashboard

The **Dashboard** (Figure 8.10) provides an overview of the most important system information, including:

Clock Status: The synchronization status of the receiver currently in use. The color of this tile makes the synchronization status of the meinbergOS device immediately apparent. If it is green, the reference source is locked and synchronized. If it is yellow, the clock is still synchronizing or locking, or is temporarily in Holdover Mode. If it is red, there is a problem with the reference clock that requires attention and the meinbergOS device will operate in free run mode until appropriate action has been taken.

Network: This tile shows a brief overview of the available Ethernet links. A green indicator shows an active and functional link and the link mode is displayed beneath it. Gray denotes the absence of a link.

NTP: This tile briefly indicates the state of the internal NTP service, and if synchronized with external NTP servers, the state of the main NTP server.

PTP: This tile shows the state of the PTP service, indicating the virtual interface, protocol in use, and the current PTP profile.

Receiver: This tile provides information on the meinbergOS device's primary receiver, including its current mode of operation (normal, cold boot, etc.), the current calculated position, the number of satellites in view, and the number of satellites currently in use.

System: This tile provides system information such as the serial number and firmware version.

Below these Dashboard tiles there is also an overview of all active and inactive reference sources, input and output signals, communication interfaces, and configured virtual network interfaces.

8.4 Configuration

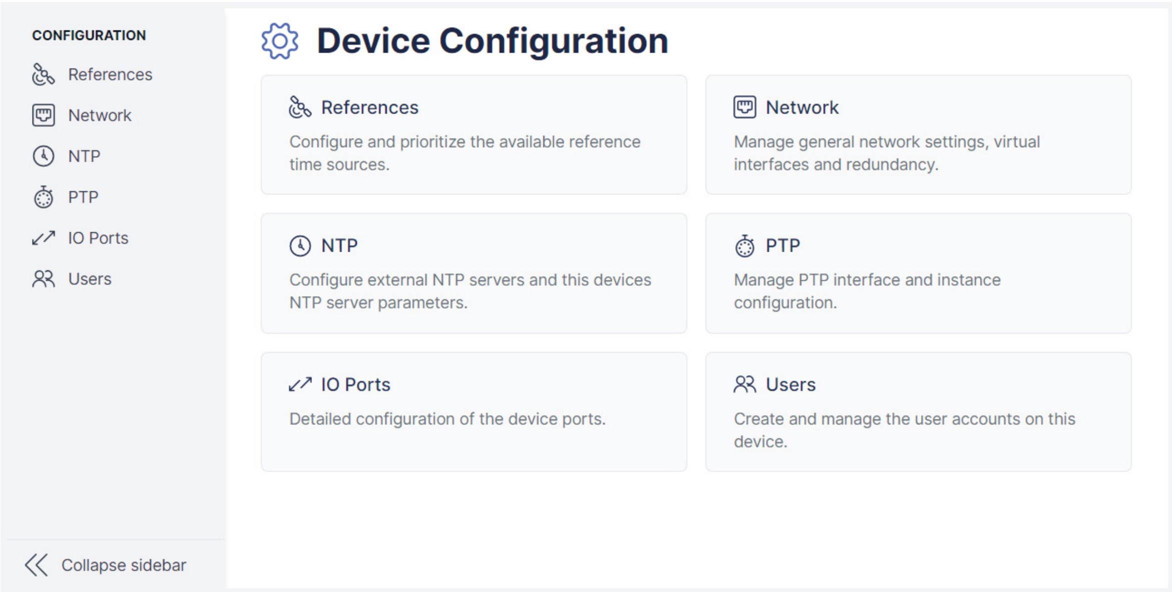


Figure 8.11: meinbergOS Web Interface: "Configuration" Section

The **Configuration** section (Figure 8.11) is where the fundamental system parameters are configured and managed.

References: This is where you can configure the reference sources supported by your system. It also provides options for the prioritization of references, the ability to compensate for propagation delays, and an option to manually define static precision values for each reference.

Network: The network connectivity of your meinbergOS device is configured here. This subsection also provides options for PRP support, network bonding, and configuration of virtual interfaces, as well as the ability to make advanced modifications to your network configuration via the integrated text editor (e.g., for static routing).

NTP: This subsection is used to configure the NTP server functionality of your meinbergOS device as well as external NTP servers. You can also enter symmetric keys here for authenticating NTP packets and enter advanced NTP configuration options using the integrated text editor.

PTP: The PTP subsection contains all options relating to the PTP functionality of your meinbergOS device, in particular the physical interfaces, the operating mode (*Master*/*Slave*), and also PTP multicast and unicast transmission settings.

IO Ports: This subsection provides a visual representation of all physical inputs and outputs to enable you to make suitable port-specific adjustments, to allow you to find the appropriate configuration subsection more easily, and also to obtain information about pin assignments with GPIO connectors.

Users: The **Users** subsection provides options for user and password management, and also allows you to set a user security policy and user permissions.

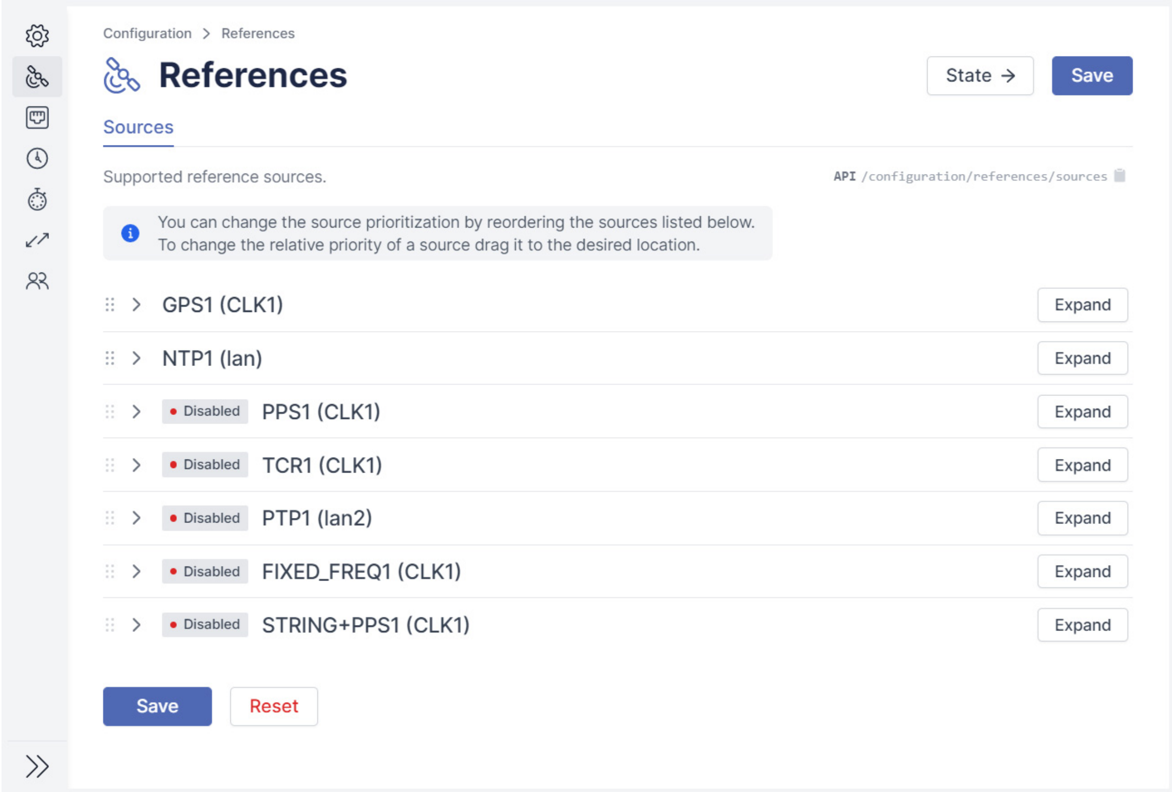


Figure 8.12: meinbergOS Web Interface: "Configuration → References" Tab

8.4.1 Configuration - References

This list in this subsection (Fig. 8.12) allows you to prioritize the handling of input signals; the priorities dictate how clock switching is handled if a master reference ceases to be available. The prioritization of the input signals should be in descending order with respect to the accuracy of the signals.

The reference prioritization can be modified by dragging any reference to another position in the list.

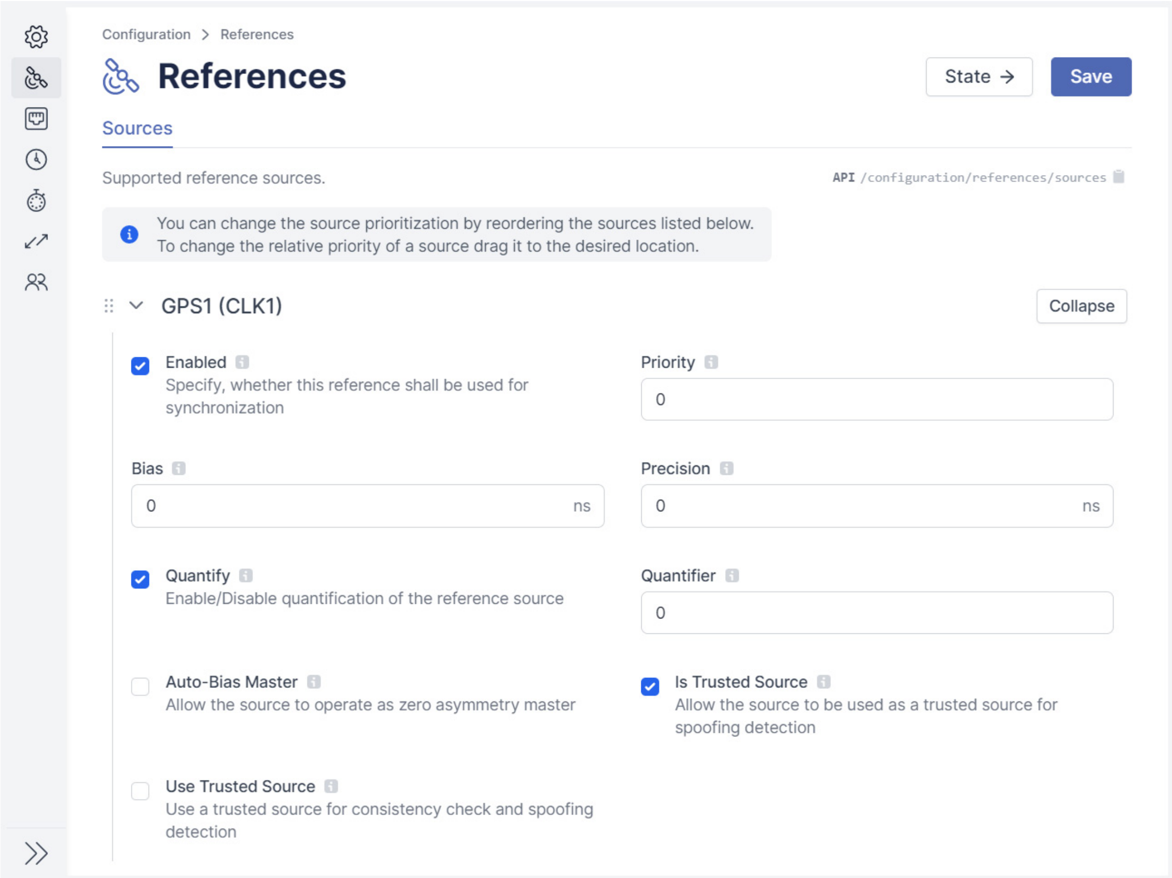


Figure 8.13: meinbergOS Web Interface: Expanded Reference Source

The configuration options for each reference source can be displayed by clicking on the panel or the corresponding **Expand** button (Fig. 8.12). This panel enables the available references of your meinbergOS device to be configured in detail.

An expanded panel can of course be collapsed again by clicking on the panel, or on the corresponding **Collapse** button (Fig. 8.13).

Enabled: Specifies whether this reference should be used for synchronization.

Priority: The priority index of the selected reference, which must be a unique value. The values are automatically renumbered to the lowest available value at the same priority level for ease of management (i.e., if a reference is set to Priority *6* and Priorities *3*, *4*, and *5* are still available, that reference will be renumbered to Priority *3*).

Bias: Used to specify a static delay offset (e.g., to account for path delays).

Precision: This parameter is used to define a manual precision value for this time reference.

When switching between different time sources, this value and the precision class of the oscillator is used to calculate a holdover time, after which the actual switchover is performed.

There is usually little point in switching straight from a more precise reference to a less precise one right after losing synchronization with a precise source.

If the time inaccuracy caused by a drift in the holdover source is less than the fundamental precision of next best available time reference, the most precise time reference will continue to be used.

If, on the other hand, there is a time reference available with a higher priority and better **precision** value, it will be switched to immediately.

If the **precision** value is 0, no holdover period will be calculated and the reference will be switched immediately.

The switching algorithm calculates the appropriateness of switching using the following formula:

*(Precision of the next reference / precision of the current master) * (constant [s])*

The parameter *constant* here is dependent on the quality of the internal oscillator.

Quantify: Enables/disables quantification of the reference source (see **Quantifier** below).

Quantifier: The quantifier can be used to minimize switching operations between redundant clocks.

If a reference with a better priority and the same quantifier value becomes available on the currently unused clock, the system will continue using its current reference clock instead of switching to the other clock. This value is ignored in systems without redundant clocks.

Auto-Bias Master: Allows the source to operate as a zero-asymmetry master. **Auto-Bias Master** can be used to automatically determine static time offsets of other reference sources if the function **Auto-Bias Slave** is activated for those sources.

Auto-Bias Slave: (PTP only) Forces the slave to accept static bias correction from a zero-asymmetry master. If this function is activated, any static time offset of the time source can be compensated by measuring against a source with the **Auto-Bias Slave** function enabled.

Is Trusted Source: Designates the source as a **Trusted Source** for spoofing detection and consistency checks. See **Use Trusted Source** below for further information.

Use Trusted Source: Ensures that only a Trusted Source is used for consistency checking and spoofing detection. The Trusted Source functionality of meinbergOS ensures that only trusted reference sources are used to verify the integrity of a primary reference source's signal.

For example, if GPS is used as the primary reference source and the precision of this source exceeds *100 ns*, selecting **Use Trusted Source** will cross-reference the data with the next highest-priority reference which has **Is Trusted Source** enabled.

Therefore, sources considered to be beyond reproach (e.g., PPS) should be marked as **Is Trusted Source**, while primary sources considered to be "at risk" (e.g., GNSS) should be marked as **Use Trusted Source**.

Information:

The checkbox **Is Trusted Source** must be checked for at least one source for **Use Trusted Source** to have any effect.

Is Time of Day Source: Designates the source as a reference for synchronization of time of day (absolute time). Only appears for sources suitable for use as a time of day reference.

Is Phase Source: Designates the source as a reference for phase synchronization.

Statistics Only: Prevents the source from being automatically selected as a synchronization reference so that it is used only for statistical analysis.

Asymmetry Step Detection: (PTP only) Asymmetry Step Detection is used to detect clock jumps. This function enables automatic bias correction in the event that a clock jump is detected so that the clock refrains from following this clock jump and instead tries to maintain its current phase. For this purpose, the time offset of the source (bias) will be re-measured.

8.4.2 Configuration - Network

In this subsection you can perform all of the main network configuration processes for your meinbergOS device.

Main: These are the main parameters for the general network configuration, notably the hostname, default gateways, and DNS servers.

Interfaces: This is where the physical network interfaces and associated virtual interfaces are managed. It also provides options for Synchronous Ethernet (SyncE) and the **Network** LED on the device itself.

PRP: The Parallel Redundancy Protocol (PRP) settings are used to set which physical network interfaces are connected to two redundant networks for a PRP implementation.

Bonding: The bonding options can be used to select the physical interfaces that you wish to use for link aggregation, and also enable selection of the bonding mode so that you can prioritize bandwidth optimization or interface redundancy as needed.

Extended Configuration: This is where manual network configuration entries are entered for your meinbergOS device (e.g., for static routing).

8.4.2.1 Configuration - Network - Main

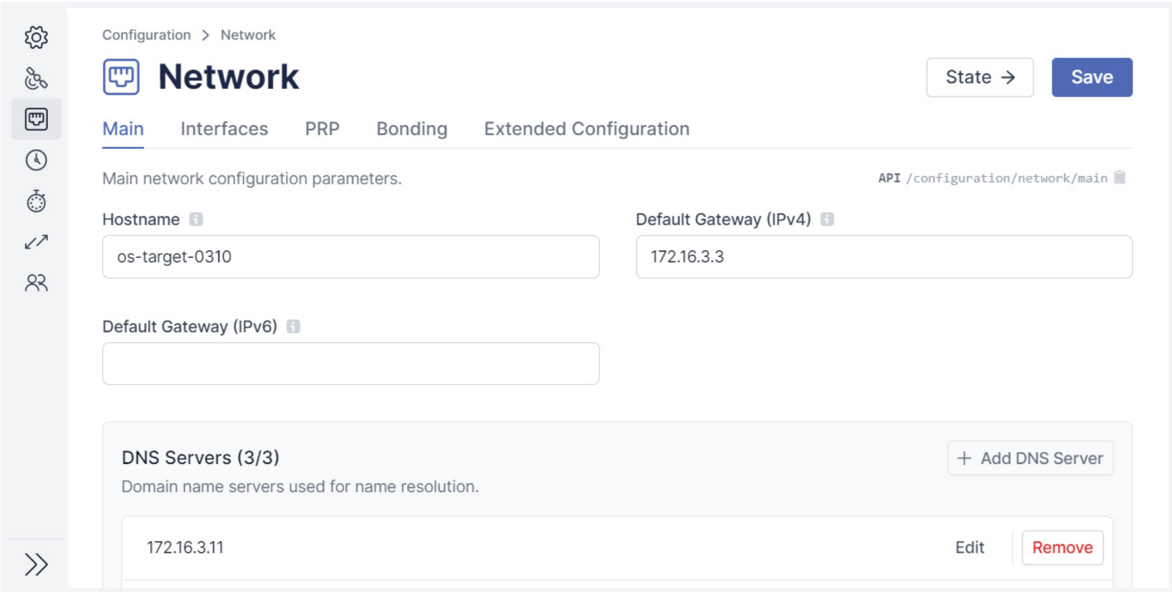


Figure 8.14: meinbergOS Web Interface: "Configuration → Network → Main" Tab

The "**Configuration** → **Network** → **Main**" tab (Fig. 8.14) is used to modify the essential network configuration for your meinbergOS device that enables it to actually reach other devices in the network.

Hostname: The hostname under which the meinbergOS device is advertised and can be found in the network. This can also be a fully qualified domain name (FQDN).

Default Gateway (IPv4): System-wide default gateway for IPv4 addresses. This parameter allows you to configure a system-wide gateway to be used for IPv4.

A gateway only needs to be configured if network traffic needs to be routed between multiple different logical networks (subnets); in other words, if your meinbergOS device needs to communicate with other devices outside of the network it is located in.

The gateway for the subnet must be configured to allow the exchange of data traffic with other networks.

Default Gateway (IPv6): System-wide default gateway for IPv6 addresses. This parameter allows you to configure an interface-specific gateway to be used for IPv6.

This configuration is only necessary if the IP address of the interface is not located in the same subnet as the default gateway.

DNS Servers: The domain name servers to be used for name resolution. Up to three DNS servers can be configured. These servers translate the hostname to an IP address to enable identification of an IP address based on that hostname.

A DNS server must be configured in particular if a hostname is specified elsewhere as the address of a network device, such as an external NTP server.

DNS Search Domain: Domains used to form fully qualified domain names when performing cleartext searches in DNS. You can specify up to three DNS search domains.

8.4.2.2 Configuration - Network - Interfaces

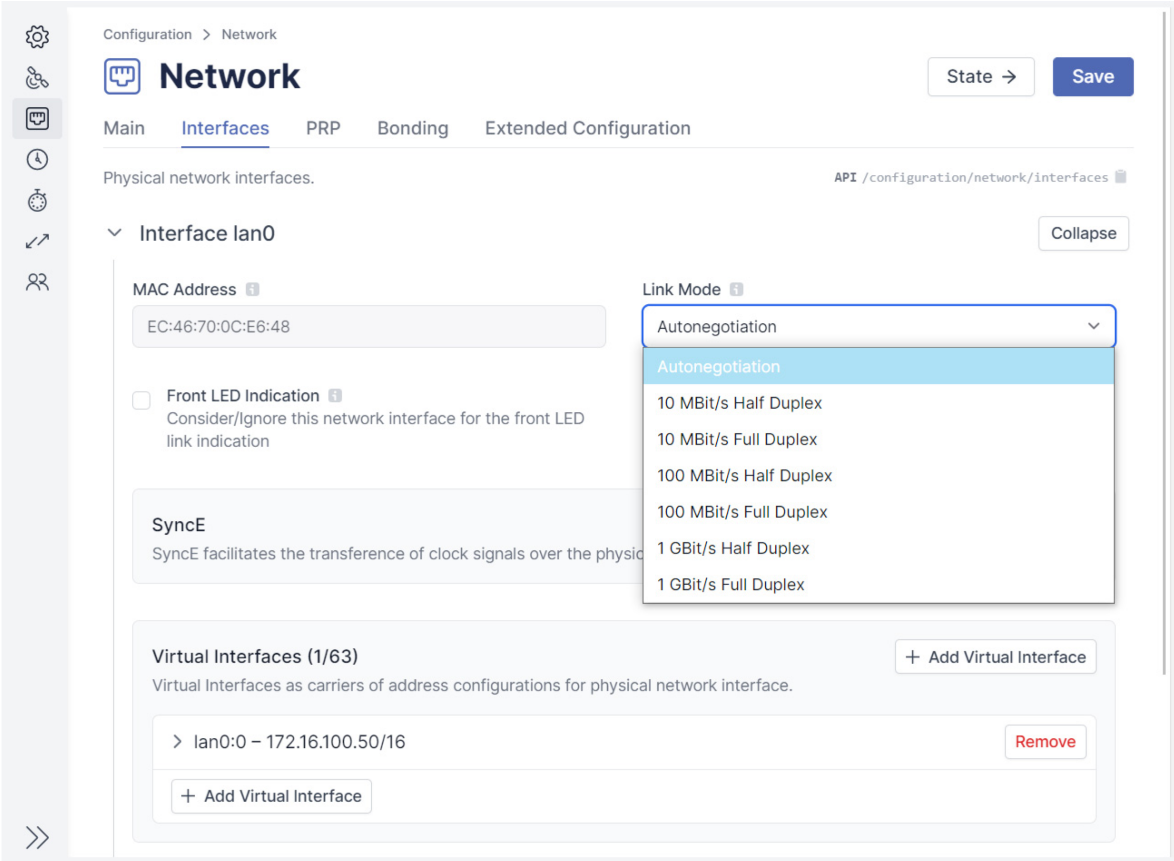


Figure 8.15: meinbergOS Web Interface: "Configuration → Network → Interfaces" Tab

The physical and virtual network interfaces and Synchronous Ethernet functionality are configured in this tab (Fig. 8.15).

Physical Network Interfaces

The available physical network interfaces are listed here and can be selected.

MAC Address: The Media Access Control (MAC) address—the unique identifier for a Network Interface Controller (NIC). This is used as a physical (OSI Layer 2) network address.

Link Mode: Transmission parameters that define the link speed and duplex mode; auto-negotiation enables two linked ports to negotiate the link speed and duplex mode automatically.

You can select one of seven available modes:

- *Autonegotiation* (automatic detection) (**default**)
- *10 Mbit/s Half Duplex* (10BaseT)
- *10 Mbit/s Full-Duplex* (10BaseT)
- *100 Mbit/s Half Duplex* (100BaseT)
- *100 Mbit/s Full Duplex* (100BaseT)
- *1 Gbit/s Half Duplex* (1000BaseT)
- *1 Gbit/s Full Duplex* (1000BaseT)

Front LED Indication: Specifies whether the state of this network interface should be indicated via the LED link indicator on the front of the device or not.

It is possible to have the link status of individual interfaces indicated visually via the LED on the front.

LED Indicator	Network Status	Front LED Status
Not activated	–	Yellow
Enabled for LAN 0 Interface (for example)	Link Up	Green
Enabled for LAN 0 Interface (for example)	Link Down	Red
Enabled for interfaces (such as LAN 0/LAN 1)	LAN 0: Link Up / LAN 1: Link Up	Green
Enabled for interfaces (such as LAN 0/LAN 1)	LAN 0: Link Up / LAN 1: Link Down	Red

SyncE

SyncE enables clock signals to be transmitted over the physical Ethernet layer. SyncE-specific parameters will be displayed once SyncE is enabled.

Information:

For more information regarding the SSM Quality Levels used in SyncE, refer to the appendix "SSM Quality Levels".

Active: Enables/disables SyncE for this network interface.

Quality Level Detection: If this function is enabled, the **Quality Level** is automatically detected based on the clock status. In *Master* mode, it is transmitted within the ESMC (Ethernet Synchronization Message Channel), while in *Slave* mode, it is used as the received level.

SDH Network Option: The selected values for the Quality Levels are dependent on the SDH network options: *Option 1* for SDH and E1-based systems, or *Option 2* for SONET and T1-based systems.

Fixed Input SSM: This is used to set a fixed **Quality Level** for the SyncE input signal.

Fixed Output SSM: This is used to set a fixed **Quality Level** for the SyncE output signal.

Minimum Input SSM: This specifies the minimum **Quality Level** of an input signal for it to be usable as a clock reference.

This is where you can select the lowest SSM **Quality Level** of the incoming signal (e.g., *QL-SSU-B*) that is considered acceptable as an incoming signal. If the clock reports a lower **Quality Level** (e.g., *QL-EEC1/SEC*) than the set minimum SSM **Quality Level**, the system will not use it for synchronization.

Local Priority: This is used to locally prioritize clocks in *Master* mode that have the same **Quality Level** and identical datasets. This can be done, for example, to manually prioritize a certain physical Ethernet port for SyncE even if **Quality Levels** are consistent among multiple sources.

RJ-45 GBit Clock Mode: When using RJ45 GBit copper links, the master and slave need to be defined.

A port can be used as a slave or as a master. SFP ports with fiber-optic connections can synchronize automatically in both directions and therefore do not need to be configured.

Virtual Interfaces

Virtual Interfaces are used to transport address configurations for physical network interfaces; it is possible to have to 63 Virtual Interfaces for each physical network interface.

Interface Label: A unique interface identifier to enable the state to be unambiguously attributed to the configuration addresses. This identifier must begin with the name of the physical interface (e.g., *lan2*) followed by a colon, then a meaningful suffix consisting of one or more letters or numbers (e.g., *lan2:ptp*). The complete virtual interface identifier must thus be at least six characters long. The name is case-sensitive.

DHCP: Dynamic Host Configuration Protocol (DHCP); this is used to have a server dynamically assign IPv4/IPv6 addresses as well as additional network parameters in the network.

If the DHCP option is enabled, the fields for static IP configuration will be disabled, as the address is automatically assigned by the DHCP server. It is still possible to configure a VLAN, however.

IP Address: This is the IPv4 or IPv6 address to be set manually for this virtual interface. If DHCP is enabled, this field will not be displayed, as the address is automatically assigned by the DHCP server.

Netmask / Prefix Bits: The number of prefix bits denoting the subnet address range within which the network address resides. If **DHCP** is enabled, this field will not be displayed, as the subnet address range is managed by the DHCP server.

Gateway: The interface-specific gateway for this virtual interface through which outbound traffic from that interface is routed to addresses outside of the subnet. If left empty, the virtual interface will route this traffic through the **Default Gateway** defined under "**Configuration** → **Network** → **Main**". If DHCP is enabled, this field will not be displayed, as the gateway is specified by the DHCP server.

Information:

The netmask in this case is not specified in decimal dot notation (e.g., *255.255.255.0*), but rather as the number of bits that define the address prefix of the subnet. For example, if your subnet encompasses the addresses *192.168.1.128* to *192.168.1.255* and your netmask in decimal dot notation is thus *255.255.255.128*, the first 25 bits of the subnet address range form the prefix.

VLAN: This checkbox enables VLAN tagging. VLANs ensure that network applications remain isolated from one another, despite being connected to the same physical network, without the need for multiple sets of cables and multiple devices.

VLAN ID: A 12-bit value (*0–4096*) that enables VLAN network traffic to be separated into discrete VLANs so that VLAN packets can be uniquely assigned to their respective VLANs.

VLAN Priority (PCP): A general priority level that relates to the IEEE 802.1p Class of Service (CoS). This can be used to prioritize VLAN packets.

Static Routes

Static routes to specified networks or hosts for this virtual interface. A static route can be defined by clicking on the **Add Static Route** button in the **Static Routes** panel inside the **Virtual Interfaces** panel.

Destination Type: Specifies whether this route points to a network or host address.

Destination Network: If *Network* is selected as the **Destination Type**, this is the network address that this route leads to.

Destination Host: If *Host* is selected as the **Destination Type**, this is the address to which this route leads.

Netmask / Prefix Bits: The number of prefix bits denoting the subnet address range within which the destination network address resides. The netmask is to be specified as the number of prefix bits, not in decimal dot notation. See note above for more information.

Gateway / Router Address: The address of the gateway/router used to route traffic to the specified network or host.

8.4.2.3 Configuration - Network - PRP

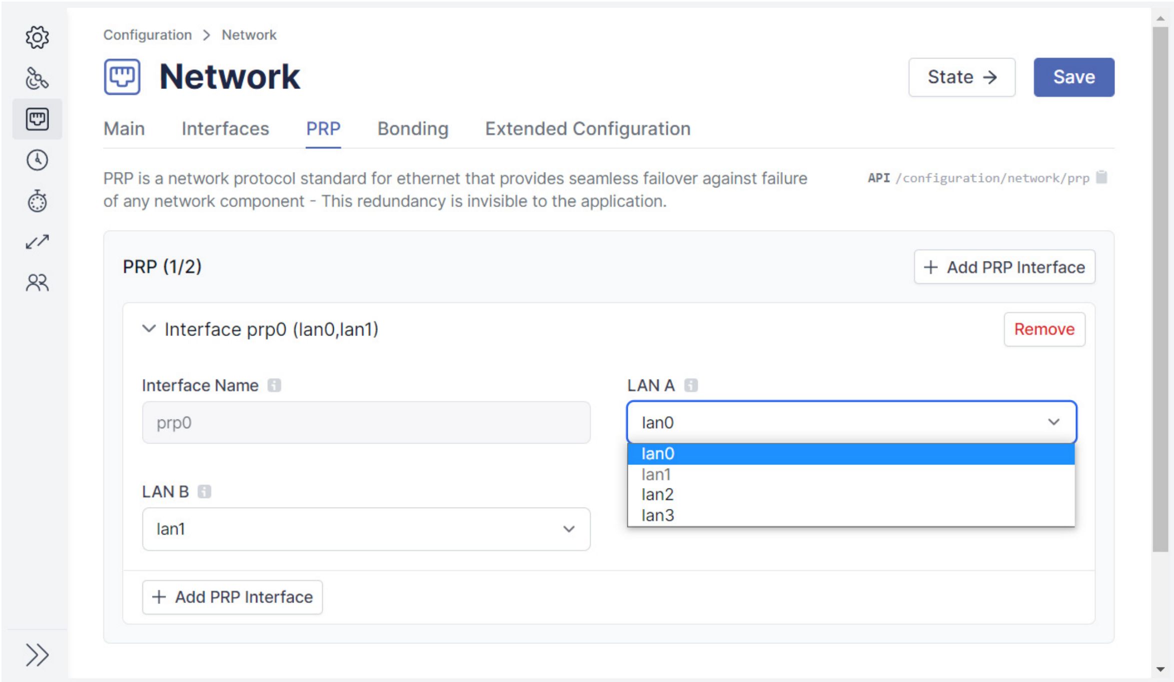


Figure 8.16: meinbergOS Web Interface: "Configuration → Network → PRP" Tab

PRP (Parallel Redundancy Protocol) is a network protocol standard for Ethernet networks that provides seamless failover to a redundant network in the event of the failure of any network component. This redundancy is invisible to applications.

PRP has been defined since 2010 in the standard IEC 62439-3. It is based on Layer 2 and was developed for computer networks that require a reliable solution to ensure high availability and operational capacity. A microSync, for example, is capable of operating as a DAN ("Dual Attached Node"), i.e., as a device that is connected to both redundant networks.

You can ensure network redundancy using the Layer 2 PRP protocol by connecting two separate network interfaces (e.g., *LAN 2* and *LAN 3* on a microSync) to two physically redundant networks, **LAN A** and **LAN B** (Fig. 8.16).

Interface Name: Name of the interface as specified by the Kernel.

It is possible to create one or multiple PRP interfaces; this enables, for example, the use of a microSync as a PRP end device to create one or more PRP networks.

LAN A: The physical interface that is connected to LAN A (lan0 - lan3).

LAN B: The physical interface that is connected to LAN B (lan0 - lan3).

To set up a redundant network with PRP support, the networks **LAN A** and **LAN B** each need to be assigned to their own network ports.

8.4.2.4 Configuration - Network - Bonding

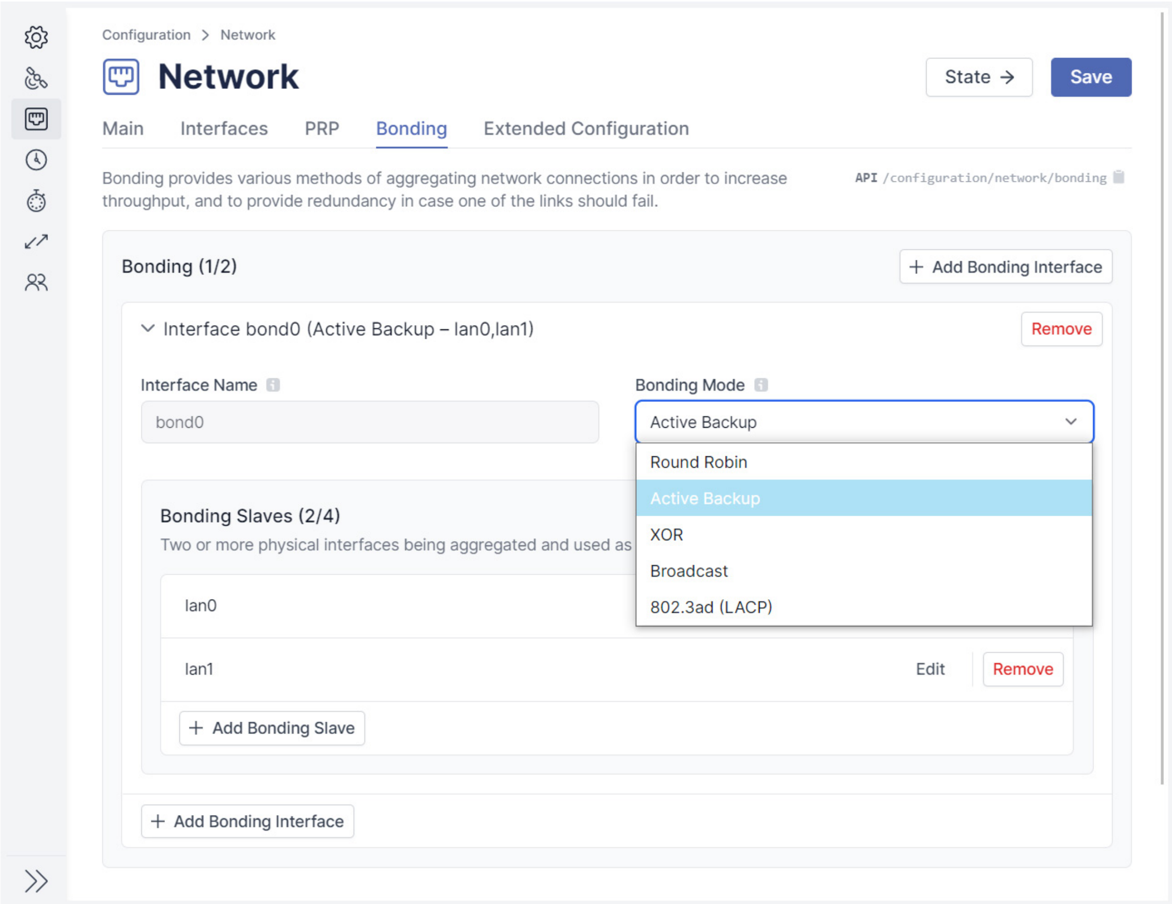


Figure 8.17: meinbergOS Web Interface: "Configuration → Network → Bonding" Tab

The tab "**Network** → **Bonding**" (Fig. 8.17) enables two or physical network connections to be bonded (grouped) into a single, joint interface.

Bonding mode is used to ensure physical interface redundancy or optimize the bandwidth usages of the interfaces. Various bonding modes are provided to suit your application requirements, and these are explained in more detail below.

To add a physical interface to a bonding group, click on "**Add Bonding Slave**" and select the interface in the drop-down menu that appears. Once you have selected the necessary interfaces, click on "**Save**" to save your configuration.

Bonding Modes

Active Backup:
A physical interface in the bonding group acts as an "active slave". All network traffic in a meinbergOS device's bonding group passes through this interface. The other physical interfaces in the bonding group are passive. If the active interface loses its link-up, the bond will switch seamlessly to the passive interface, in which case the MAC address of the network interface will also remain unchanged.

Round Robin:
Packets are transmitted over each slave interface in sequence, starting with the first interface, ending with the last, then beginning from the first again. All interfaces must be connected to the same switch. The switch ports must be trunked.

This mode enables bandwidth optimization and provides fault tolerance.

XOR:
The transmitting interface is determined using an XOR hash of the MAC address of the destination and the MAC address of the source. All interfaces must be connected to the same switch. The switch ports must be trunked.

This mode enables bandwidth optimization and provides fault tolerance.

Broadcast:
All packets are transmitted to all interfaces. All interfaces must be connected to the same switch. The switch ports must be trunked.

This mode only provides fault tolerance and does not enable bandwidth optimization.

802.3ad (LACP):
802.3ad (Link Aggregation Control Protocol, LACP) enables multiple physical connections to be combined into a single, logical connection. This allows for load distribution while also providing better security than *Active Backup*, should an interface fail. Other connected network devices also need to support LACP in this case and the network ports must be configured accordingly.

8.4.2.5 Configuration - Network - Extended Configuration

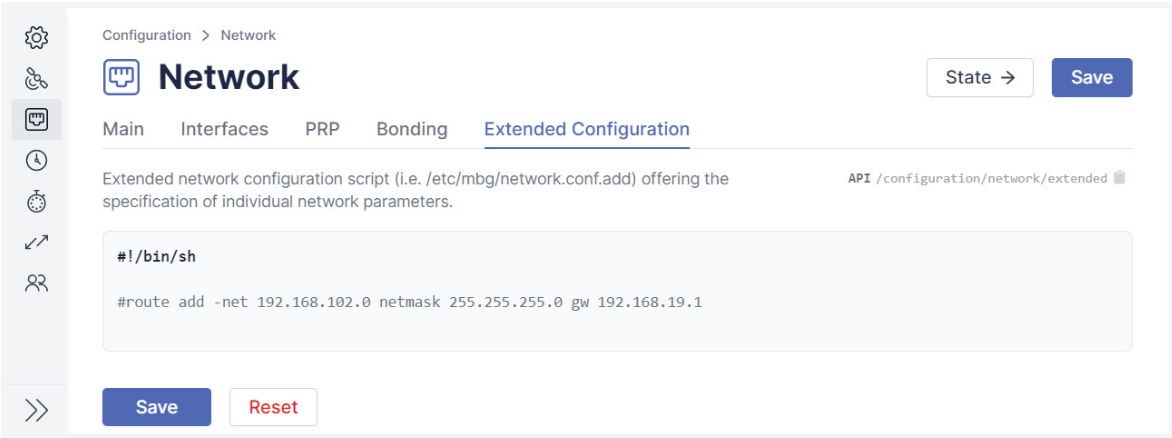


Figure 8.18: meinbergOS Web Interface: "Configuration → Network → Extended Network Configuration" Tab

The **Extended Configuration** tab (Fig. 8.18) is a basic text editor for an Extended Network Configuration Bash script that enables custom network parameters to be specified. This script is saved on the meinbergOS device's storage as */etc/mbg/network.conf.add* and is executed automatically each time the meinbergOS device is (re)booted or a change is made to a network-related configuration.

Important!

This subsection is intended solely for use by qualified system administrators and must be handled with care. Commands entered here will be executed as *root* user with the corresponding comprehensive rights. Improper usage of this input option may cause privileges to be improperly conferred upon other processes or users (privilege escalation), compromising the security of your meinbergOS device.

8.4.3 Configuration - NTP

This subsection provides the means to configure your meinbergOS device's NTP functionality. The type and number of configurable parameters depends on the module or device selected.

Server: This is where the meinbergOS device is configured in relation to how it operates as an NTP server.

Client: This tab provides configuration options for the meinbergOS operating as an NTP client or peer.

Symmetric Keys: Configuration options for NTP server/client authentication using symmetric MD5, SHA-1 and AES-128-CMAC keys are provided here.

Extended Configuration: This tab provides a text editor for entering custom NTP configuration parameters.

8.4.3.1 Configuration - NTP - Server

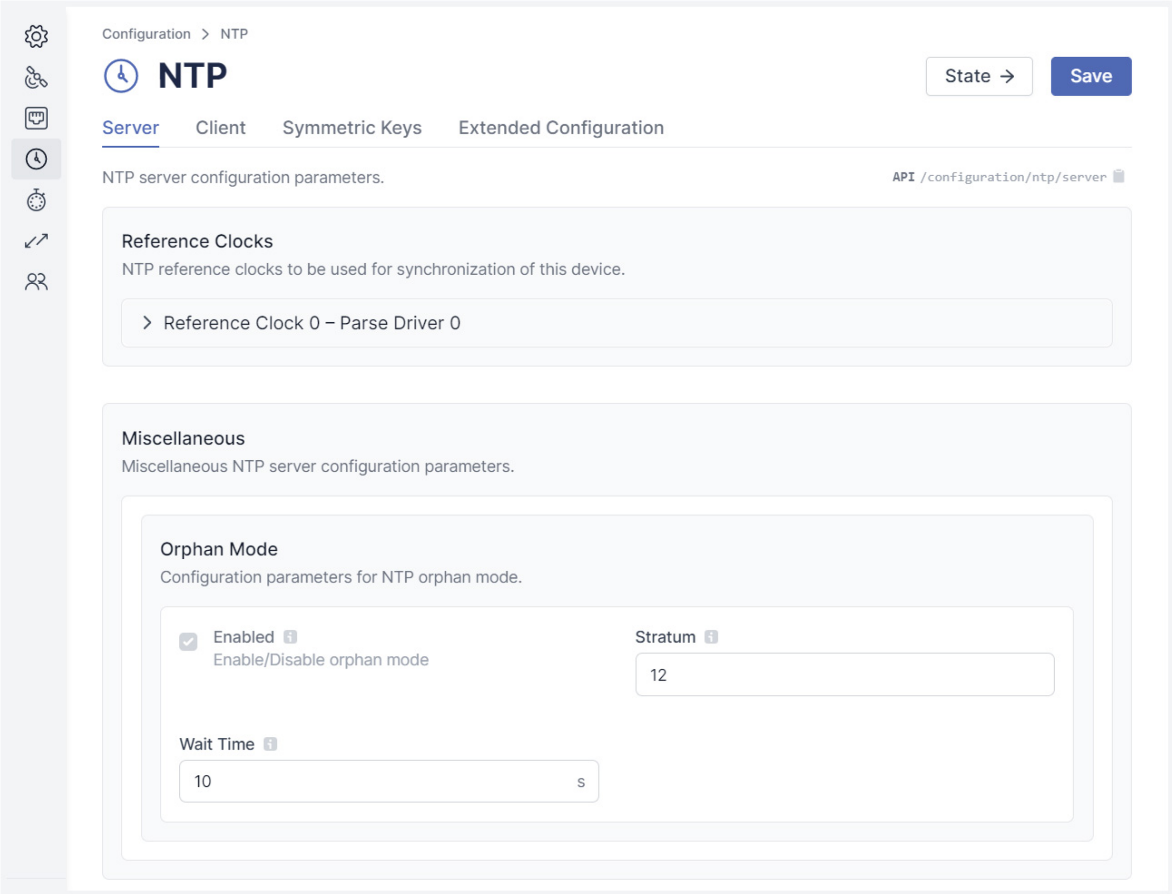


Figure 8.19: meinbergOS Web Interface: "Configuration → NTP → Server" Tab

Information:

These options relate to how your meinbergOS device operates as an NTP server or peer and not to your meinbergOS device as a client.

For the configuration of NTP server/client relationships where your meinbergOS device is the client, please open the subsection "**Configuration** → **NTP** → **Client**" and refer to the guidance provided in the corresponding chapter of this manual.

Information:

Many configuration options for the NTP server in this subsection are grayed out and are thus not editable. This is entirely normal as they relate solely to meinbergOS' internal handling of NTP traffic and there is no reason to adjust these. They are only displayed for reference purposes. This chapter will therefore only address the options that **are** editable.

Reference Clocks

The NTP reference clocks to be used to synchronize this device.

Time 2: Driver-specific **Time 2** for the reference clock (e.g., Trust Time).

For the Parse driver, this value specifies the **Trust Time** (provided that flag1 = 1 in */etc/ntpd.conf*).

The **Trust Time** specifies how long the NTP service will continue to 'trust' a desynchronized receiver to continue providing accurate time based on an oscillator that is in free-run mode. This period starts from the time at which the receiver ceases to be synchronized with its time source.

Trust Time is not supported for the reference clock if any driver other than the PARSE driver is used for the reference clock (e.g., NMEA driver, shared memory driver). There are reference clock drivers that do not support Trust Time, which is why the specified values may be interpreted differently.

Miscellaneous

Miscellaneous NTP server configuration parameters.

Orphan Mode: The configuration parameters for NTP Orphan Mode.

Orphan Mode is a 'fallback' mode that applies, for example, when a GPS receiver ceases to have reception. In this case, some NTP clients would expect the stratum value of this server to switch to a less favorable value while there is no GPS reception available. However, with NTPv4 clients, this is not necessary and may even be counterproductive.

The client recognizes that its time is drifting based on the increasing **root dispersion** value provided by the server's responses, and it can react by 'switching' to another server if one is available.

Stratum: The stratum level to be announced if no reference source is available.

This parameter's value specifies the stratum that NTP will announce in the network if the service has lost synchronization and the Trust Time has expired. Enter a custom value into this field, or leave it at the default value of 12.

The value **Time 2** (see above) should thus only be set for the purpose of adjusting the **Trust Time**.

You can set the stratum value to a less favorable stratum, but in general, this value should not be modified.

Wait Time: Time to wait until stratum demotion when **Orphan Mode** becomes active.

8.4.3.2 Configuration - NTP - Client

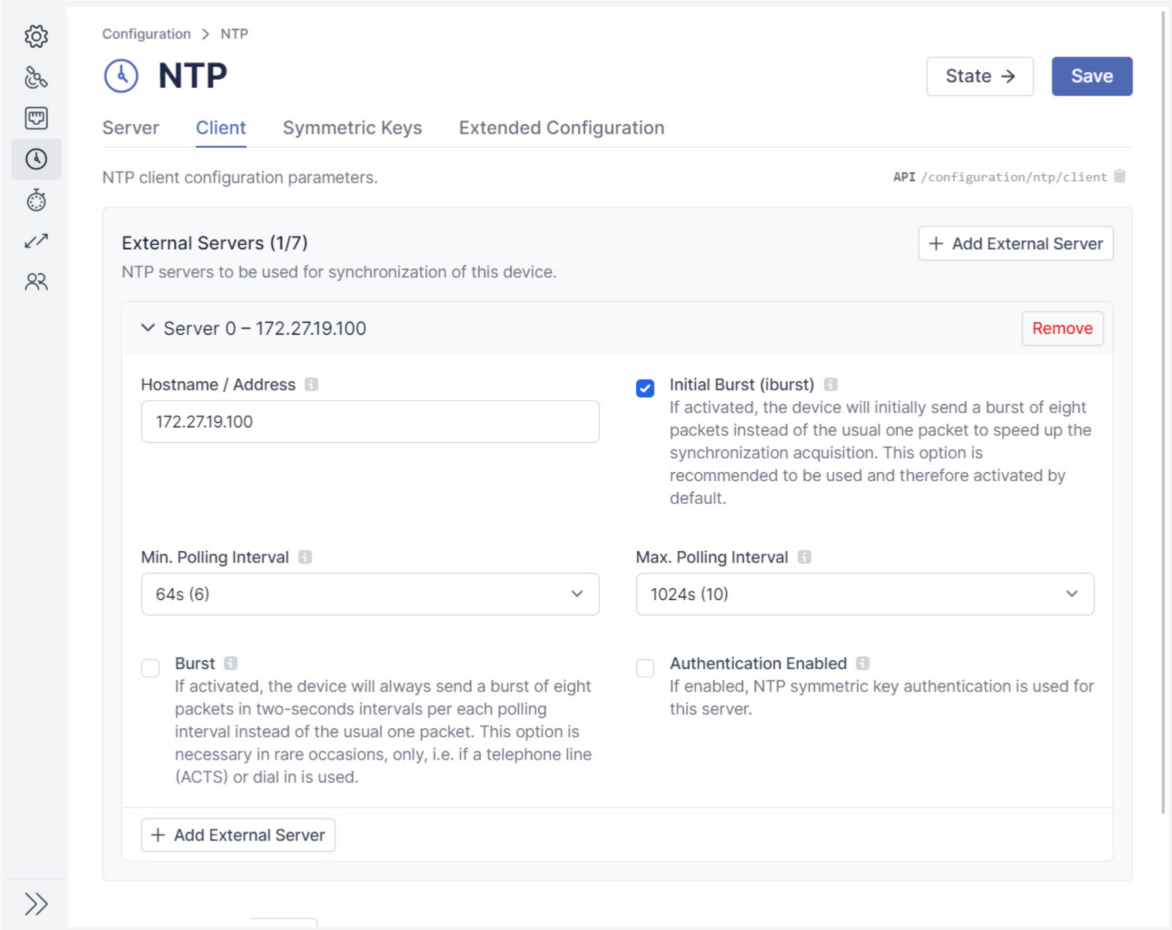


Figure 8.20: meinbergOS Web Interface: "Configuration → NTP → Client" Tab

Information:

These options relate to how your meinbergOS device operates as an NTP client and not to clients connected to your meinbergOS device (in its capacity as a server).

For the configuration of NTP server/client relationships where your meinbergOS device is the server, please open the subsection "**Configuration → NTP → Server**" and refer to the guidance provided in the corresponding chapter "Configuration - NTP - Server" of this manual.

External Servers

NTP servers to be used for synchronization of this device.

Hostname / Address: Hostname or IP address of the server.

Initial Burst (*iburst*): If enabled, the device will initially send a burst of eight packets instead of the usual one packet in order to speed up the synchronization acquisition. Enabling this option is recommended and it is therefore activated by default.

Min. Polling Interval: The minimum polling interval for NTP messages.

Max. Polling Interval: The maximum polling interval for NTP messages.

Burst: If enabled, the device will always send a burst of eight packets at two-second intervals upon each polling interval instead of the usual one packet. This option is only necessary on rare occasions, for example if a telephone line (ACTS) or dial-in is being used.

Authentication Enabled: If enabled, NTP symmetric key authentication will be used for this server.

Authentication Key ID: Only appears if **Authentication Enabled** is checked. This option allows you to select the trusted symmetric key to be used for NTP authentication.

8.4.3.3 Configuration - NTP - Symmetric Keys

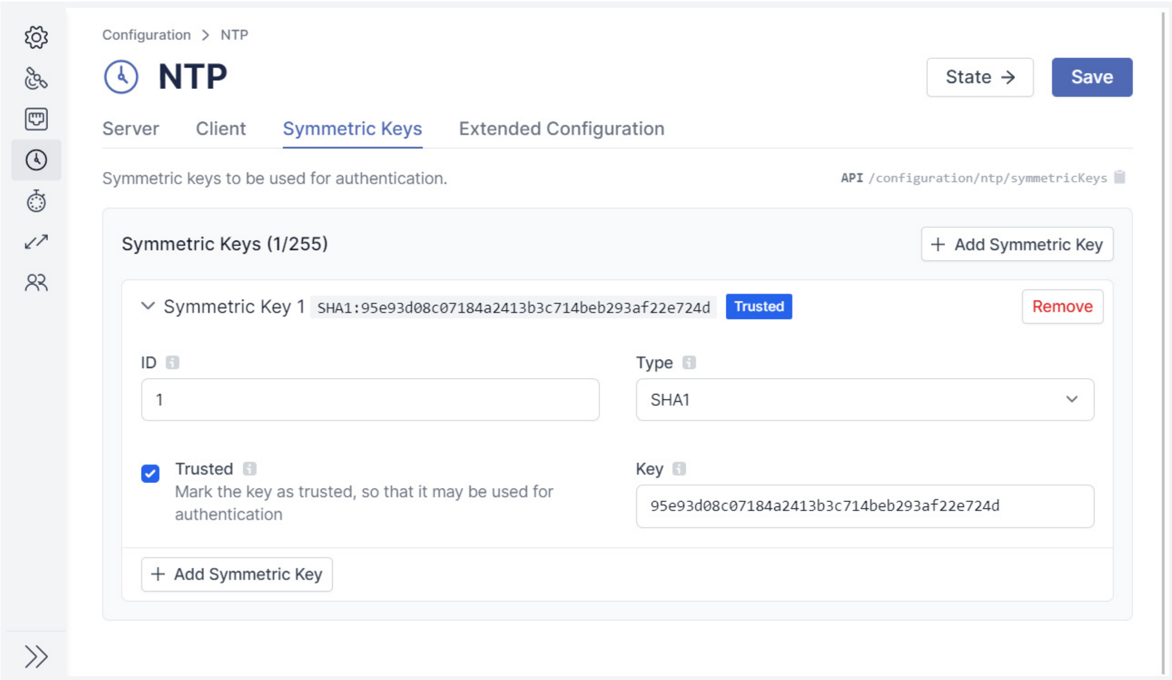


Figure 8.21: meinbergOS Web Interface: "Configuration → NTP → Symmetric Keys" Tab

This tab (Fig. 8.21) can be used to configure symmetric keys to provide authenticated NTP clock synchronization. The keys can be used both for communication with NTP clients and for communication with external servers. The system supports MD5, SHA-1 and AES-128-CMAC keys.

The button **Add Symmetric Key** is used to create a new entry for configuring a symmetric key.

ID: Unique ID of the symmetric key (*1–65535*). A symmetric key can be assigned an ID that will be used later to refer to this key when configuring trusted keys and external servers.

Type: The message-digest or cryptographic algorithm (*MD5*, *SHA-1*, or *AES-128 CMAC*) to be used for this key.

Trusted: This marks the configured symmetric key as **trusted** so that it can be used for authentication. If the device receives an NTP request from a key that is not recognized as **trusted**, the request will be rejected.

Key: The key phrase itself. Keys can consist of a series of up to 20 printable ASCII characters (except '#') or 40 hexadecimal characters (*0–9*, *A–F*).

8.4.3.4 Configuration - NTP - Extended Configuration

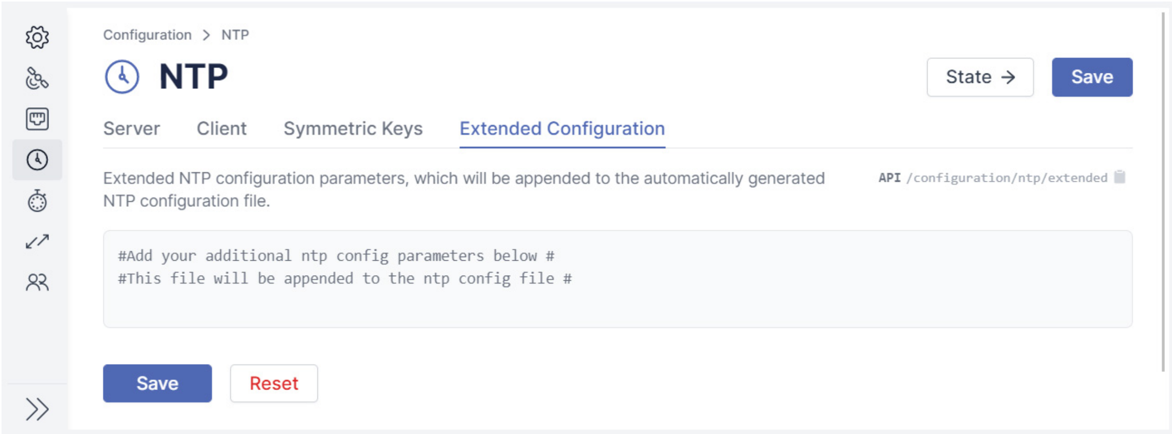


Figure 8.22: meinbergOS Web Interface: "Configuration → NTP → Extended Configuration" Tab

This tab (Fig. 8.22) enables you to add any custom configuration parameters that are not provided in the other configuration subsections. These parameters will be appended to *ntp.conf* after application of the main configuration.

8.4.4 Configuration - PTP

This subsection enables you to configure all of the main PTP parameters for your module or device. The level of configurability will depend on the interface/license.

Interfaces: This tab hosts the PTP-specific configuration options for the virtual network interfaces to be used for PTP applications.

Instances: This tab provides the configuration options for the PTP instances, including industry-specific profile settings.

8.4.4.1 Configuration - PTP - Interfaces

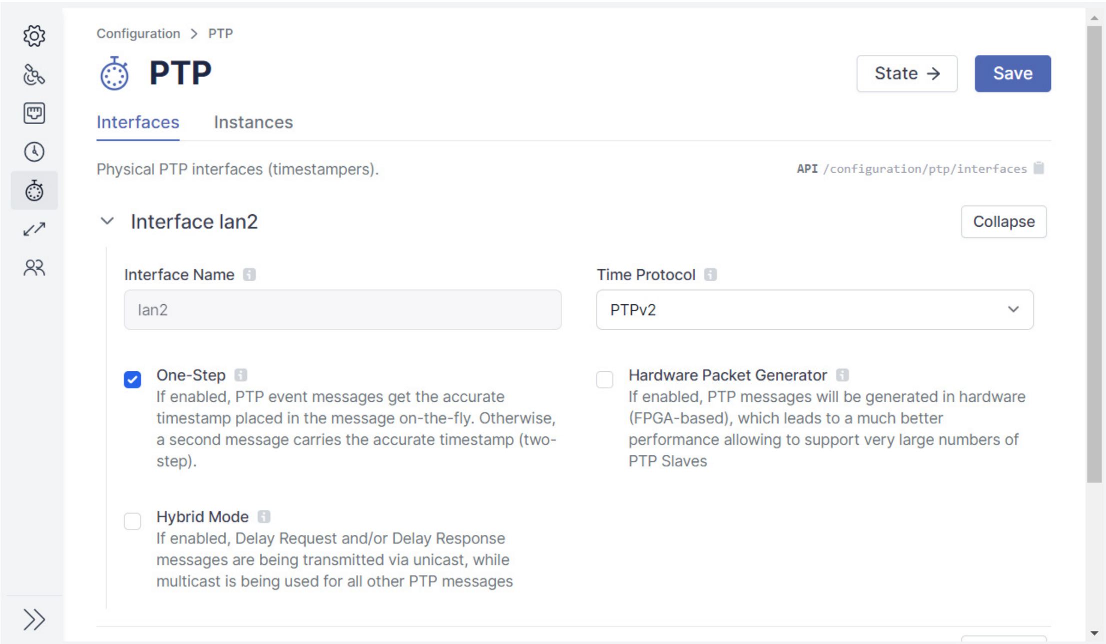


Figure 8.23: meinbergOS Web Interface: "Configuration → PTP → Interfaces" Tab

This tab (Fig. 8.23) is used to configure the PTP-specific parameters for the virtual interfaces used by the PTP instances.

Interface Name: Name of the physical PTP interface.

One-Step: If enabled, PTP event messages will have an accurate timestamp placed directly in the message on the fly. If disabled, the accurate timestamp will be transmitted in a second message (*two-step*).

Hardware Packet: Generator: If enabled, PTP messages will be generated in hardware (FPGA-based). This can vastly improve performance and allow a very large number of slaves to be supported.

Information:

The Hardware Packet Generator is only compatible with one-step PTP and Layer 3 network protocols (UDP/IPv4 and UDP/IPv6). It can therefore not be used with any PTP profile that requires Layer 2 IEEE 802.3 communication.

Hybrid Mode: If enabled, **Delay Request** and/or **Delay Response** messages will be sent in unicast transmissions, while all other PTP messages will be sent as multicast transmissions.

8.4.4.2 Configuration - PTP - Instances

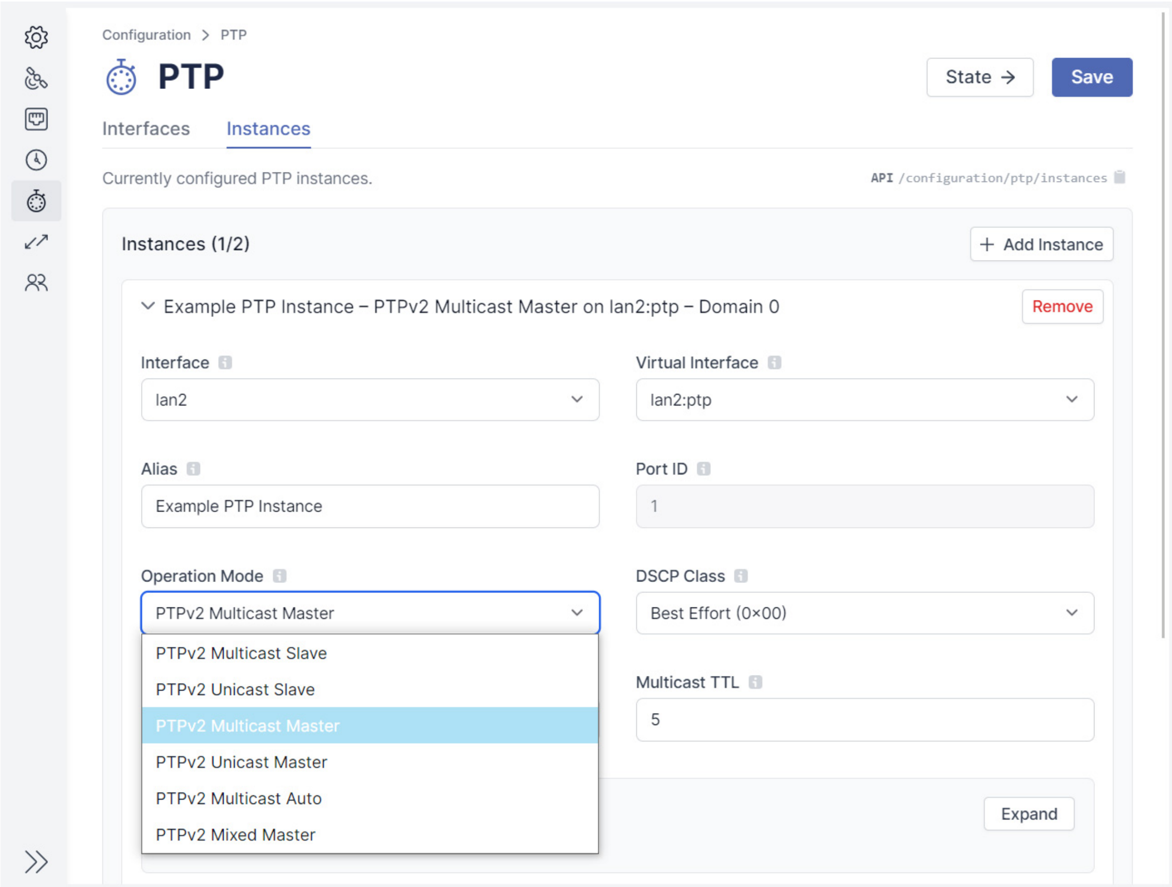


Figure 8.24: meinbergOS Web Interface: "Configuration → PTP → Instances" Tab

This tab (Fig. 8.24) is where the PTP instances are created, assigned to a pre-defined virtual interface, and (re)configured. Specifically, the configuration options listed here relate to the transmission and handling of PTP messages in the network functions. There are also a number of PTPv2-specific options when *PTPv2* is selected.

Interface: The physical PTP interface that this instance is running on.

Virtual Interface: The virtual interface (i.e., IP address) of the selected physical interface to be used by this instance.

Alias: An optional, descriptive name for this instance, purely for informational purposes.

Port ID: The read-only port ID of this instance, as assigned by the management process.

Operation Mode: This is used to select the appropriate operation role that the PTP stack should assume. The available options are dependent on the hardware support of the physical PTP interface.

The possible roles are:
- *Multicast Slave* (*lan2* only)
- *Unicast Slave* (*lan2* only)
- *Multicast Master* (*lan2* and *lan3*)
- *Unicast Master* (*lan2* and *lan3*)
- *Multicast Auto* (*lan2*)
- *Mixed Master* (*lan2* and *lan3*)

Information:

Unicast Slave mode requires the unicast masters to be entered manually in the **PTPv2** panel. See below for further information.

DSCP Class: 6-bit differentiated services code point (DSCP) in the **Differentiated Services** field of the IP header for packet classification purposes.

IPv6 Multicast Scope: The address range to be used for IPv6 multicast frames.

Unicast TTL: **TTL (time-to-live)** value for IPv4 or **hop count** limit for IPv6 unicast packets.

Multicast TTL: **TTL (time-to-live)** value for IPv4 or **hop count** limit for IPv6 multicast packets.

Delay Asymmetry Compensation: Enables/disables compensation for known delay asymmetry.

Asymmetry Compensation Value: If **Delay Asymmetry Compensation** is enabled, this specifies the offset to be applied by the instance to compensate for delay asymmetry in nanoseconds.

Enable Packet Counters: Enables/disables packet counter statistics. This data can be viewed under "**State** → **PTP** → **Instances** → **Packet Counters**". Refer to the chapter "**State - PTP - Instances**" for more information.

Log Level: The log level of the PTP instance. Valid values range from *0* (Error) to *4* (Debug).

Information:

The PTP stack logs are not accessible via the Web Interface or Meinberg Device Manager. The files must be acquired manually by logging into the meinbergOS device through a terminal, be it through SSH or a wired connection to the console interface. The log files are located at */var/log* and have the filename *ptpstack_<virtualinterfacename>.log*.

Temporarily Disabled: Select this option to temporarily disable an instance without removing its configuration.

PTPv2

Additional configuration parameters for PTPv2 instances.

Profile: Enables the selection of a specific PTP profile that sets specific operating parameters for defined PTP performance requirements.

Networking Protocol: The IP addressing protocol used for UDP/IP communication. This can be *UDP/IPv4* or *UDP/IPv6* communication (OSI Layer 3 communication). *IEEE 802.3* Layer 2 communication is also supported, but requires the FPGA-based Hardware Packet Generator to be disabled.

Domain: This is the domain number used for this PTP device. Only devices with the same domain number will communicate with each other in a network; this allows multiple PTP instances to be operated concurrently in isolation from one another within a single network.

Delay Mechanism: The delay measurement mechanism for path delay calculation. This can either be peer-to-peer (*P2P*) or end-to-end (*E2E*). The mechanisms available will depend on the selected profile.

Priority 1 (Master/Auto Mode only): This field is used by the PTP Best Master Clock algorithm for selection of the grandmaster. Conventionally this is set at *128* for devices designed to serve as master clocks and *255* for devices designed to serve exclusively as slaves, but can be fine-tuned if you wish to define priorities among multiple individual master clocks.

Priority 2 (Master/Auto Mode only): This field is also used by the PTP Best Master Clock algorithm for selection of the grandmaster, but is only considered by the algorithm if the **Clock Class**, **Accuracy**, and **Variance** values are essentially identical. This value is generally used to determine which master clocks serve as primary and backup clocks when multiple redundant master clocks are in place.

Announce Receipt Timeout: Establishes how many **Announce** intervals the receiving device will wait until it stops listening for **Announce** messages.

Announce Interval: Specifies the requested average interval between **Announce** messages.

Sync Interval: Specifies the requested average interval between **Sync** messages.

(Peer) Delay Request Interval: Specifies the minimum interval at which **Delay Request** messages should be sent from PTP master to slave or between peers.

Enable PTP Timescale: Specifies whether the standard PTP timescale (TAI) should be used (checkbox enabled) or if an arbitrary timescale should be applied instead (checkbox disabled). This will be grayed out if the selected profile mandates the use of the TAI timescale.

Enable Path Trace TLV (Master/Auto Mode only): If enabled, this option will cause PTP messages to follow a Path Trace TLV.

Enable V1 Hardware Compatibility (Master/Auto Mode only): This should be enabled if using PTP clocks in a network that only support PTPv1. This causes sync messages to be padded with enough bytes to ensure that the messages meet the PTPv1 message size requirement. Enabling this will increase the bandwidth requirement.

Enable Management Messages: Enabling this checkbox will cause PTP Management Messages to be sent and parsed. Disabling it will cause **all** Management Messages to be ignored.

PTPv2 Fixed Quality

If *Master* or *Auto* mode is selected, the **Fixed Quality** parameters can be opened within the **PTPv2** panel to enable the quality parameters to be forced for the Best Master Clock algorithm. These settings do not appear or apply in *Slave* mode.

> **Information:**
>
> It is possible to have only individual quality parameters forced and the remainder calculated automatically. Parameters that are to be left unforced (calculated automatically) should be set (or left at) a value of *0*.

Clock Class (Sync): Specifies which fixed BMC **Clock Class** is to be reported while the meinbergOS device is synchronized with its reference.

Clock Class (Holdover): Specifies which fixed BMC **Clock Class** is to be reported while the meinbergOS device is still (re)synchronizing.

Clock Class (Free Running): Specifies which fixed BMC **Clock Class** is to be reported while the meinbergOS device is in free-run mode (running solely off the oscillator).

Clock Accuracy: Specifies which BMC **Clock Accuracy** is to be reported.

Clock Variance: Specifies which BMC **Clock Variance** is to be reported.

Time Source: Specifies what type of Time Source the clock declares itself to be.

PTPv2 Unicast Masters

Instances operating as a unicast slave require the manual entry of the unicast masters that the slave will use for synchronization. These can be entered in this panel by clicking on **Add Unicast Master**.

Address: Specifies the address of the unicast master. This can be the MAC address or, if using *UDP/IPv4* or *UDP/IPv6*, the IP address.

Clock ID: Specifies the PTP **Clock ID** of the unicast master. If this ID is unknown, you may enter the wildcard ID *ff:ff:ff:ff:ff:ff:ff:ff*.

Port ID: Specifies the **port ID** of the unicast master. If the port is unknown, you may enter the wildcard port *65535*.

Announce Interval: The interval to be requested of the unicast master for **Announce** messages.

Sync Interval: The interval to be requested of the unicast master for **Sync** messages.

Delay Request Interval: The interval to be requested of the unicast master for **Delay Request** messages.

Transmission Duration: Specifies how long in seconds **Announce**, **Sync**, and **Delay Request** messages may be requested for before the subscription must be renewed by the device.

Profile-Specific Parameters

Certain PTPv2 profiles provide additional configurable profile-specific parameters.

<u>**Power IEEE C37.238-2011**</u>

Grandmaster ID: Specifies the ID of the network's grandmaster to be communicated in the profile-specific TLVs.

Network Time Inaccuracy: Specifies a set inaccuracy value relative to the master.

Alternate Time Offset Indicator: Specifies an alterative time offset indicator to be embedded in the profile-specific TLV. Currently only supports UTC.

<u>**Telecom ITU-T G.8275.1**</u>

MAC Address: Specifies the multicast MAC address for PTP frames over Ethernet. Options are *01:80:C2:00:00:0E* (non-forwardable) and *01:1B:19:00:00:00* (forwardable).

<u>**SMPTE ST 2059-2**</u>

System Frame Rate: Specifies the nominal frame rate of the system: *23.98 Hz*, *24 Hz*, *25 Hz*, *29.97 Hz* (also referred to as 29.98 Hz or 29.976 Hz), *50 Hz*, or *59.94 Hz*. This data is embedded in the profile-specific TLVs of the PTP messages.

Drop Frame: If enabled, this option will integrate the drop frame flag to allow drop frames to be accounted for in SMPTE 12M timecode for 29.97 Hz (NTSC) content in 30 Hz systems.

Color Frame: If enabled, this option will integrate the color frame flag for chrominance data.

Next Jam Mode: Specifies the method by which discontinuities between the timecode and timescale caused by drop frames are corrected in the timecode continuity. This can be a *Daily Jam Event* (correction performed at the same time each day), *Single Jam Event* (correction performed once on a given date at a given time) or upon the *Next Discontinuity in Local Time*.

Jam Date: Only applies to single one-off jam events. Specifies the date in the format *YYYY-MM-DD* on which the jam event is to be applied.

Jam Time: Only applies to single one-off or daily jam events. Specifies the time in the format *hh:mm:ss* at which the jam event is to be applied on the specified jam date or each day, as appropriate.

Event Timescale: Specifies the timescale to be applied for the timing of jam events: *Local Time*, *UTC*, *PTP (TAI)*, or *GPS*.

<u>IEEE 802.1AS</u>

Propagation Delay Threshold: Specifies the maximum propagation delay that a PTP instance must observe to be accepted as a usable clock for IEEE 802.1AS infrastructure.

Time Base Indicator: Specifies the master clock time base indicator. This value is incremented every time there is a step change in the time or frequency to indicate a new time base.

<u>Power IEEE C37.238-2017</u>

Grandmaster ID: Specifies the grandmaster of the PTP network as a 16-bit ID (*0–65535*) to be integrated into the TLV of the PTP messages.

8.4.4.3 Guide: Creating a PTP Instance

Because the process of setting a PTP instance on an interface is rather more involved than the configuration of NTP or other signal outputs, this chapter will briefly explain how to create a PTP instance and assign it to a virtual interface.

1. Create a virtual network interface by opening "**Configuration** → **Network** → **Interfaces**", selecting the physical interface that you wish to create a new virtual interface on, and then clicking on **Add Virtual Interface**. Proceed as described in the chapter "**Configuration - Network - Interfaces**". Please ensure that you select an interface that supports PTP.

2. Configure the PTP interface by opening "**Configuration** → **PTP** → **Interfaces**", opening the panel for the corresponding physical interface. Define whether you wish to use *one-step* or *two-step* message transmission (depending on your network configuration), hardware packet generation, and hybrid unicast/multicast transmission for PTP messages. For more information, refer to the chapter "**Configuration - PTP - Interfaces**".

3. Configure the PTP instance by opening "**Configuration** → **PTP** → **Instances**". Select the physical interface, the virtual interface on that physical interface that you have just created, and configure the instance accordingly as described in the chapter "**Configuration - PTP - Instances**".

8.4.5 Configuration - IO Ports

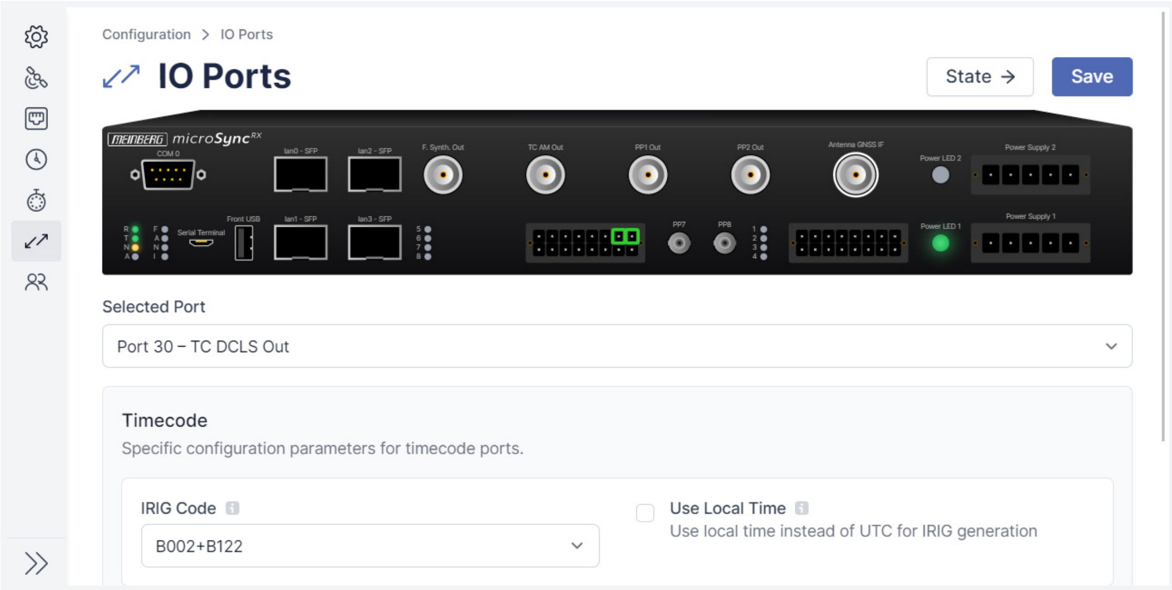


Figure 8.25: meinbergOS Web Interface: "Configuration → IO Ports" Subsection

This subsection (Fig. 8.25) provides an overview of the available interfaces and visual status indicators on the front of your meinbergOS device (e.g., a microSync).

Selecting a interface, plug, or socket will open the corresponding panel or subsection used to configure that connector (if configurable).

The interfaces shown in this subsection will vary depending on the specific meinbergOS device. Therefore, please refer to your meinbergOS device's manual for further information.

8.4.6 Configuration - Users

The "**Configuration** → **Users**" subsection can be used to create new users and to edit or delete existing users. oder gelöscht werden.

Accounts: This tab is where the meinbergOS device's user accounts are managed. It provides functions for creating and deleting accounts as well as assigning or revoking permissions.

Levels: This tab provides the ability to manage templates for the creation of new user accounts.

Important!

The **Users** subsection is only visible to users with the **Read Configuration** permission for **Users** and can only be modified by accounts with the **Write Configuration** permission for **Users**. Accordingly, new accounts can also only be created and existing accounts can only be deleted by accounts with the **Write Configuration** permission for **Users**.

It is therefore essential for at least one accessible account to always have **Write Configuration** permissions for **Users**. If no accounts have **Write Configuration** permissions for **Users**, it will become impossible to create or delete accounts and you may be permanently locked out of certain functions.

8.4.6.1 Configuration - Users - Accounts

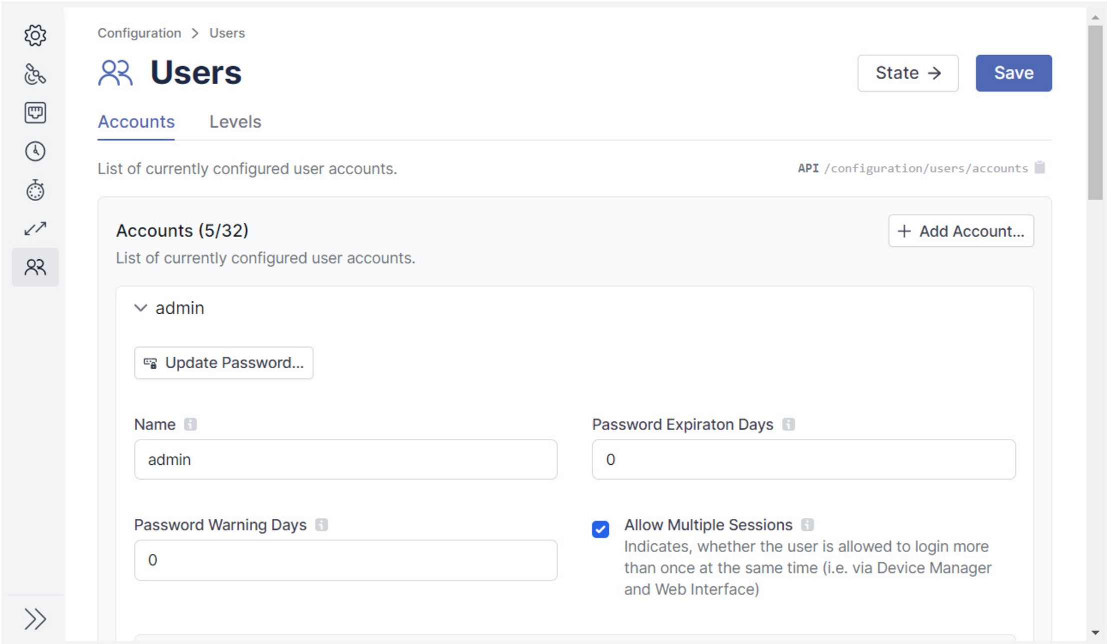


Figure 8.26: meinbergOS Web Interface: "Configuration → Users → Accounts" Tab

Important!

Assigning the **Write Configuration** permission **Users** to any account will enable that account to modify not only their own permissions but also the permission of **every** account on that system. This permission should therefore only ever be assigned to users who are completely trusted.

The following settings can be modified in this tab (Fig. 8.26):

Name: The unique name of the user account.

Password Expiration Days: The number of days after which the password becomes invalid (*0* = Never).

Password Warning Days: The number of days after which the user is to be warned that their account password will be expiring imminently (*0* = Never).

Allow Multiple Sessions: Specifies whether the account can be used to log in more than once at the same time (for example, one via Meinberg Device Manager, another via the Web Interface).

Channels: Specifies the channels via which this account can connect to the device:
- *Web Interface*
- *Device Manager*
- *Shell*
- *SNMP*

An **Admin** account can be used to assign the channels to each account based on the user's specific needs.

Allow "sudo" in Shell: Specifies whether the account is allowed to gain elevated privileges in a shell session by using the **sudo** tool.

Channels

The channels specify which interfaces the user may use to connect and interact with the meinbergOS device.

Web Interface: Allows access to the meinbergOS Web Interface via a web browser.

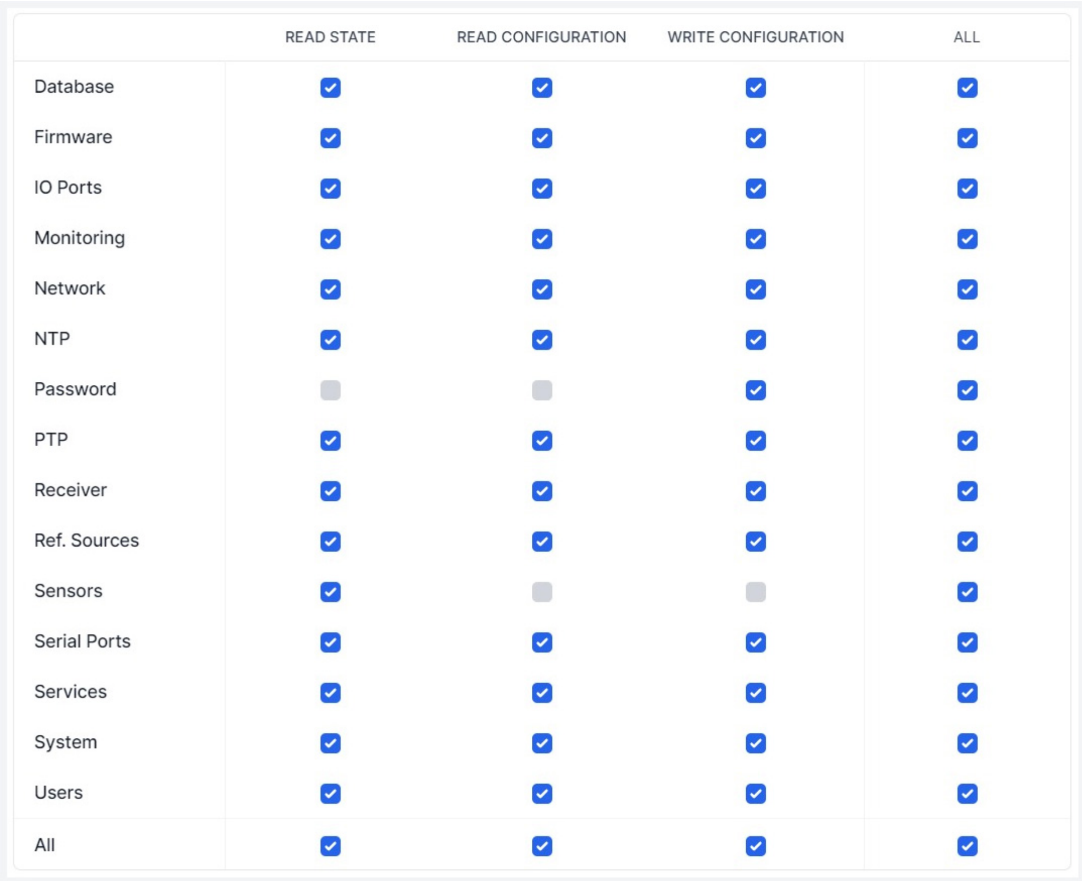
Device Manager: Allows access to the meinbergOS device using Meinberg Device Manager.

Shell: Allows access to the Linux command line interface (CLI) via terminal software. This channel is also required for viewing the system log and kernel log, even through the meinbergOS Web Interface.

SNMP: Allows access to the meinbergOS device's SNMP interface for remote monitoring and control of the meinbergOS device using an SNMP tool.

User Permissions

Specifies the read and write permissions of this user.



	READ STATE	READ CONFIGURATION	WRITE CONFIGURATION	ALL
Database	☑	☑	☑	☑
Firmware	☑	☑	☑	☑
IO Ports	☑	☑	☑	☑
Monitoring	☑	☑	☑	☑
Network	☑	☑	☑	☑
NTP	☑	☑	☑	☑
Password	☐	☐	☑	☑
PTP	☑	☑	☑	☑
Receiver	☑	☑	☑	☑
Ref. Sources	☑	☑	☑	☑
Sensors	☑	☐	☐	☑
Serial Ports	☑	☑	☑	☑
Services	☑	☑	☑	☑
System	☑	☑	☑	☑
Users	☑	☑	☑	☑
All	☑	☑	☑	☑

Figure 8.27: meinbergOS Web Interface: User Permissions

Database:

Read Configuration:
This currently has no function.

Write Configuration:
Allows the user to reset the satellite statistics database. This process is performed using Meinberg Device Manager and is currently not possible in the meinbergOS Web Interface.

Read State:
This currently has no function.

Information:

Access to the satellite statistics database in Meinberg Device Manager also requires access to the **Shell** channel and the **Allow "sudo" in Shell** permission.

Firmware:

Read Configuration:
Provides access to view all meinbergOS firmware information, including information on the currently active firmware build, the clock module firmware, and the installed firmware versions.

Write Configuration:
Allows the user to select one of the installed firmware versions and to install new versions.

IO Ports:

Read Configuration:
Allows the user to view the physical I/O port configuration options and status information from the Configuration section including input/output signal specifications and communication protocols (except Ethernet ports, which are governed by **Network** permissions).

Write Configuration:
Specifies the ability to modify the communication/output settings of the physical I/O ports (except Ethernet ports, which are governed by **Network** permissions).

Read State:
Allows the user to view the same information as with the **Read Configuration** permission, but must be accessed from the **State** section.

Monitoring:

Read Configuration:
Grants the account access to the **Monitoring** configuration tab in Meinberg Device Manager, allowing it to read the SNMP, syslog, and events monitoring configurations through Meinberg Device Manager. This is currently not possible through the meinbergOS Web Interface.

Write Configuration:
Allows the user to modify the settings of the **Monitoring** configuration tab in Meinberg Device Manager, allowing it to modify the SNMP, syslog, and events monitoring configurations through Meinberg Device Manager. This is currently not possible through the meinbergOS Web Interface.

Information:

SNMP, syslog, and events monitoring currently cannot be configured through the meinbergOS Web Interface.

Read State:
Provides access to the **Monitoring** status tab in Meinberg Device Manager. Much of the information contained therein is already provided on the Web Interface Dashboard even without this permission.

NTP:

Read Configuration:
Allows the user to view (but not modify) the configuration options for the NTP service available in the **Configuration** section.

Write Configuration:
Allows the user to modify the configuration options for the NTP service available in the **Configuration** section.

Read State:
Allows the user to open the **NTP** subsection in the **State** section and thus view NTP-related status information.

Network:

Read Configuration:
Allows the user to view (but not modify) the configuration options for network connectivity available in the **Configuration** section.

Write Configuration:
Allows the user to modify the configuration options for network connectivity available in the **Configuration** section.

Read State:
Allows the user to open the **Network** subsection in the **State** section and thus view network-related status information.

PTP:

Read Configuration:
Allows the user to view (but not modify) the configuration options for the PTP service available in the **Configuration** section.

Write Configuration:
Allows the user to modify the configuration options for the PTP service available in the **Configuration** section.

Read State:
Allows the user to open the **PTP** subsection in the **State** section and thus view PTP-related status information.

Password:

Write Configuration:
Specifies whether the user is permitted to modify the account's password.

Receiver:

Read Configuration:
Allows the user to view (but not modify) options related to the internal clock module in Meinberg Device Manager. These options are currently not accessible via the meinbergOS Web Interface.

Write Configuration:
Allows the user to modify options related to the internal clock module in Meinberg Device Manager. This permission does not affect access to configuration options in the meinbergOS Web Interface; some of these options (simulation mode, compensation for cable length) are also available via the **IO Ports** permission.

Read State:
Allows the user to open the **Clock Module** subsection in the **State** section and thus view status information related to the receiver, such as information on its antenna connection and satellite reception.

Information:

It is possible to enable Simulation Mode and compensation for cable length-related signal propagation delays via the **IO Ports** configuration subsection and thus with the **IO Ports** configuration permissions.

Ref. Sources:

Read Configuration:
Allows the user to view (but not modify) the configuration options for the reference sources available in the **Configuration** section.

Write Configuration:
Allows the user to modify the configuration options for the reference sources available in the **Configuration** section.

Read State:
Allows the user to open the **References** subsection in the **State** section and thus view status information related to the reference sources.

Sensors:

Read State:
Provides access to hardware temperature readings viewable in Meinberg Device Manager.

Information:

Temperature sensor information is currently not available in the meinbergOS Web Interface.

Serial Ports:

Read Configuration:
This permission is required to provide the user with read access to the **IO Ports** configuration options in the meinbergOS Web Interface.

Write Configuration:
This permission is required to provide the user with write access to the **IO Ports** configuration options in the meinbergOS Web Interface.

Information:

The **Serial Ports** permissions, which govern access to the time string output from the serial ports, and the **IO Ports** permissions, which govern access to the I/O ports in general, provide access to different options when using Meinberg Device Manager, but these options are combined in a single subsection in the meinbergOS Web Interface. It is therefore necessary to have both **Read Config** and/or both **Write Config** permissions activated if a user is intended to access and/or make changes in the **IO Ports** configuration subsection.

Services:

Read Configuration:
This permission affects access to certain options available in Meinberg Device Manager relating to the control of the SNMP, Web Interface, and NTP services.

Write Configuration:
This permission mostly relates to the ability to modify certain options in Meinberg Device Manager relating to the control of the SNMP, Web Interface, and NTP services. For the purposes of the meinbergOS Web Interface, it is required to restart the NTP service from the **Maintenance** section. Refer to "Maintenance" for more information.

Information:

With the exception of the **Restart NTP** function provided in the **Maintenance** subsection, the functions that the **Services** permissions relate to are currently only accessible from Meinberg Device Manager and are currently not accessible via the meinbergOS Web Interface.

System:

Read Configuration:
This permission does not have any bearing on the functions of the meinbergOS Web Interface. It only affects access to the **System** sections of Meinberg Device Manager, which are used to create system snapshots and upload SSL certificates.

Write Configuration:
This permission relates to the execution of system-wide maintenance operations, specifically rebooting, saving the current configuration as the Startup Configuration, recovering the Startup Configuration by discarding the current configuration, and performing a factory reset. It is also required to download a diagnostics file.

Read State:
This permission relates to the display of the **System** tile on the Dashboard and the **Overview** subsection of the **Maintenance** section, both of which contain hardware-related information such as the serial number. This permission is also required to view the system log and kernel log.

Information:

A user without the **System Write** permission cannot save changes to the Startup Configuration, so any changes made by that user to the configuration will be lost if the system is rebooted or unexpectedly powered down, unless another user with the appropriate permission logs in to save the Startup Configuration.

Users:

Read State/Read Configuration:
Specifies whether the user is permitted to view configuration information for all users on the system.

Write Configuration:
Specifies whether the user is permitted to create new users and modify the configuration of existing users.

8.4.6.2 Configuration - Users - Levels

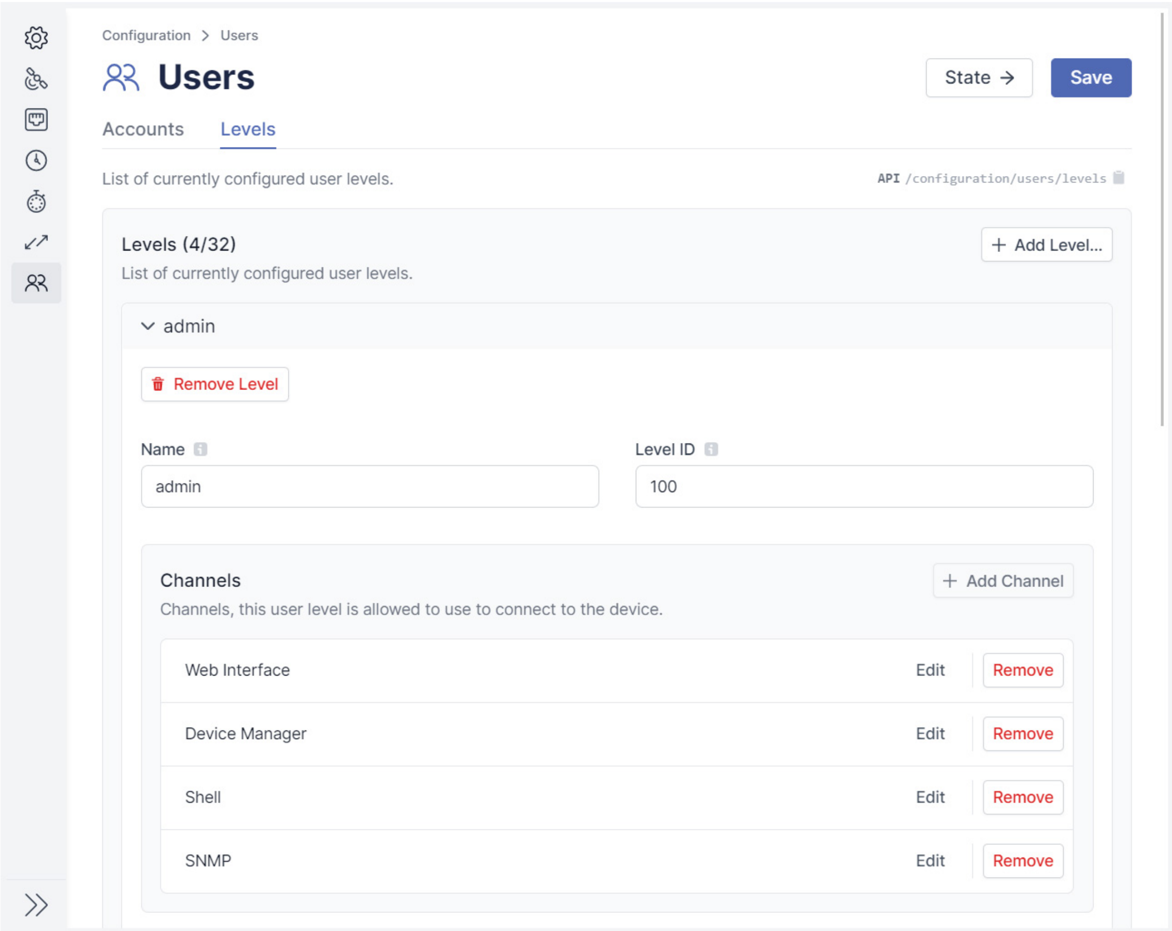


Figure 8.28: meinbergOS Web Interface: "Configuration → Users → Accounts" Tab

The "**Configuration → Users → Levels**" tab (Fig. 8.28) is used to define or modify user levels to enable more efficient creation of user accounts. User levels are essentially customized user profiles that serve as templates for the creation of new user accounts. When a new user account is created, one of these levels can be selected so that the new user account inherits the level's permissions configuration.

Important!

User accounts only inherit a level's defined configuration upon creation of that account. Any changes made to the level template after the fact will not be carried over to existing accounts created using that level. Therefore, please note that this function cannot be used to add or revoke permissions to multiple users concurrently and/or retroactively.

The button **Add Level** can be used to add a new level, while the **Levels** panel shows the list of currently defined levels, each of which can be expanded and collapsed as necessary.

Name: The unique name of the user level.

Level ID: The unique ID (*0–999*) of the user level.

Channels: The channels that this user level is allowed to use to connect to the device.

Channels

The channels specify which interfaces the user may use to connect and interact with the meinbergOS device.

Web Interface: Allows access to the meinbergOS Web Interface via a web browser.

Device Manager: Allows access to the meinbergOS device using Meinberg Device Manager.

Shell: Allows access to the Linux command line interface (CLI) via terminal software. This channel is also required for viewing the system log and kernel log, even through the meinbergOS Web Interface.

SNMP: Allows access to the meinbergOS device's SNMP interface for remote monitoring and control of the meinbergOS device using an SNMP tool.

Important!

Removing Web Interface access from the current user account will cause the account to be immediately logged out, and it will only be possible to regain access either through another account or via a channel that has been enabled for the modified account!

8.5 State

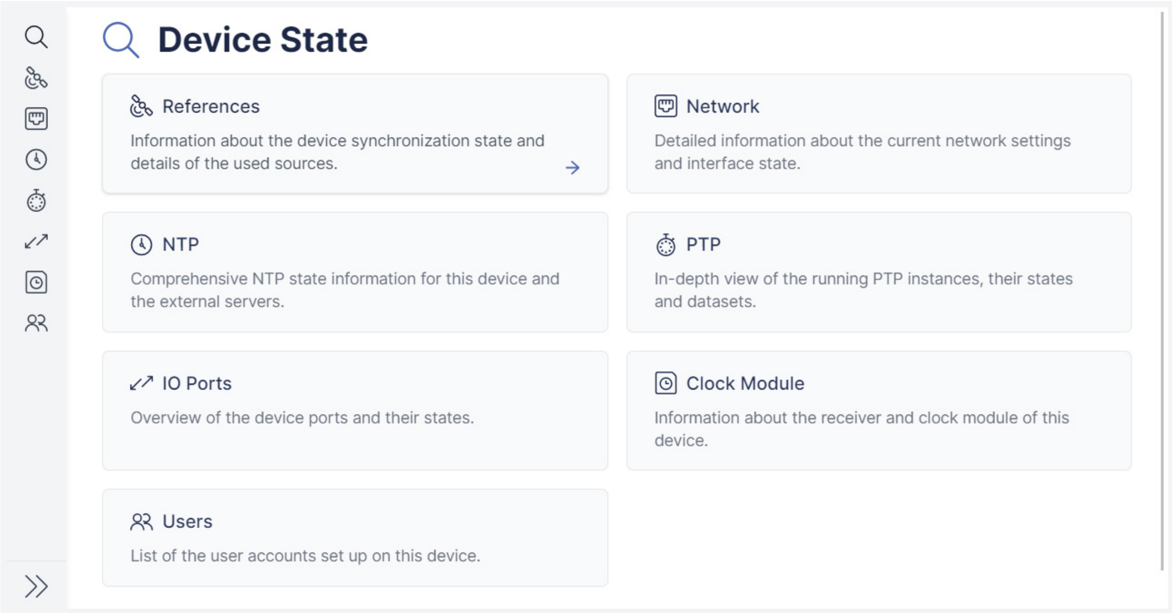


Figure 8.29: meinbergOS Web Interface: "State" Section

The **State** section of the meinbergOS Web Interface (Fig. 8.29) provides you with a wealth of information about the status of your microSync device, including an overview of the various reference sources, network connectivity and redundancy, NTP and PTP functionality, I/O ports, and user access.

Information:

The pages for these subsections are regularly refreshed automatically. If you wish to disable this automatic refresh for a specific page for any reason, you can do so by clicking on the link **Disable auto-refresh** at the top of each page. The auto-refresh will then remain disabled for that page even after it is closed, until it is actively re-enabled for that page.

8.5.1 State - References

The "**State** → **References**" subsection provides general information about the system's reference clocks, including the signal availability and phase lock, accuracy, and jitter status.

Overview: This tab provides a list of all available references, both enabled and disabled, showing their availability, offset, and other states.

Global: This tab provides more detailed information on the current master reference.

Sources: This tab provides more detailed information on all of the available reference sources.

8.5.1.1 State - References - Overview

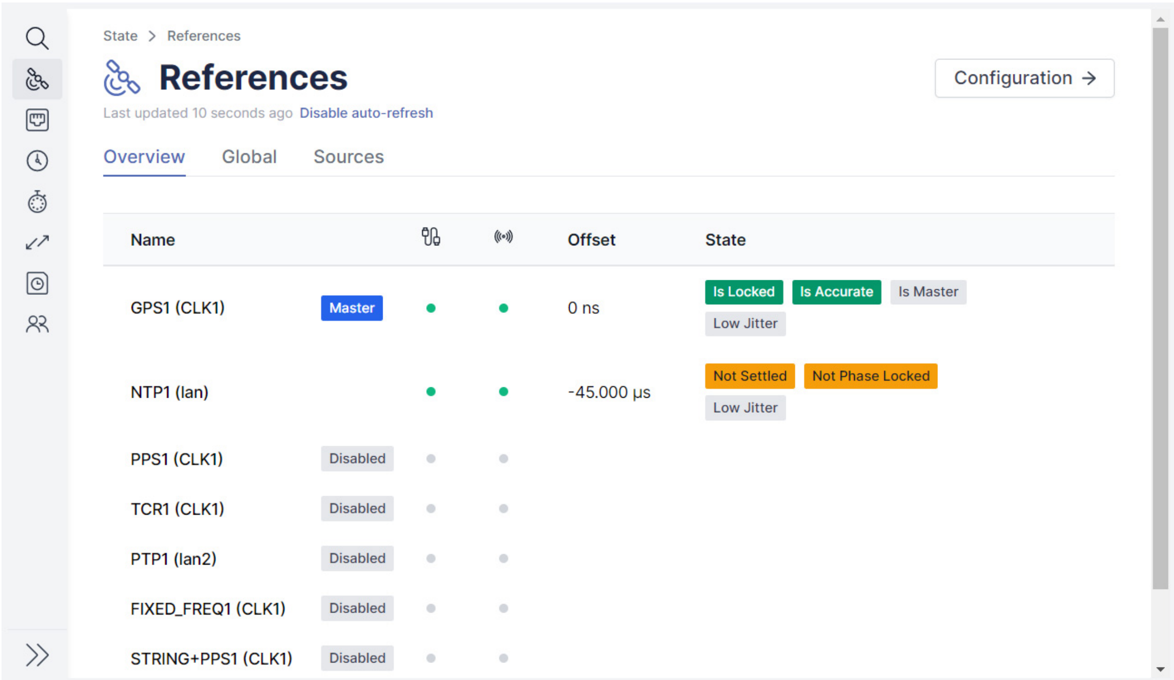


Figure 8.30: meinbergOS Web Interface: "State → References → Overview" Tab

The "**State** → **References** → **Overview**" tab (Fig. 8.30) provides a summary of your clock references and their synchronization status.

Name

The designation of the clock source. The interface connector is shown in parentheses:

CLK1: Signal transmitted through internal reference clock.
(e.g., GPS antenna, PPS, time string)

lan: NTP data communication over any configured Ethernet interface.

lan2: PTP data communication over the input-enabled PTP interface.

Information:

As of Version *2022.05.1*, *lan2* is the only input-enabled PTP interface and is therefore the only interface that can be operated as a PTP slave.

The reference source that is currently being used to adjust the clock is designated by a blue *Master* tag. Clock sources that have a gray *Disabled* tag appended to them have been explicitly disabled in the "**Configuration** → **References**" subsection.

Connection Detected

Green: Indicates that a wired connection is established with the signal source.

Red: Indicates that no wired connection is established to the signal source, or that the connection is faulty (e.g., coaxial cable from time server to antenna may be defective).

Signal Available

Green: Indicates that a viable signal has been detected over the connected cable.

Red: Indicates that no viable signal can be detected over the connected cable.

Offset

Reports the difference between the local system clock and the clock signal.

State

This column may show any number of tags indicating the status of the clock and its signal:

Is Locked: The clock is locked with the external reference signal and is using it to adjust the oscillator.

Is Accurate: The external clock signal is judged to be accurate (i.e., the minimum required accuracy of the oscillator has been reached).

Is Master: This reference source is currently being used to adjust the clock.

Is External: This reference source has been connected externally.

Low Jitter: The system has detected minimal jitter in the external clock signal, so that the accuracy of the reference source is acceptable.

Not Settled: The internal oscillator is not (yet) frequency-locked with the external clock signal.

Not Phase Locked: The internal oscillator is not (yet) phase-locked with the external clock signal.

No Connection: No wired connection with the signal source is detected.

No Signal: A wired connection with the signal source has been detected, but there is no viable signal detected over this cable.

Num. Sources Exceeded: The maximum limit for the number of allowed time sources has been exceeded.

ITU Limit Violated: The input source is of poor stability such that it is not in compliance with a specified ITU-T mask (e.g. PRC or SSU-A).

TRS Limit Violated: The time error limit for the Trusted Reference Source feature has been exceeded.

MTTF Limit Violated: This indicates that the reference exceeds the defined maximum offset ("Maximum Time to Follow") relative to the current reference and will therefore not be used in the event that the system falls back to Holdover Mode.

8.5.1.2 State - References - Global

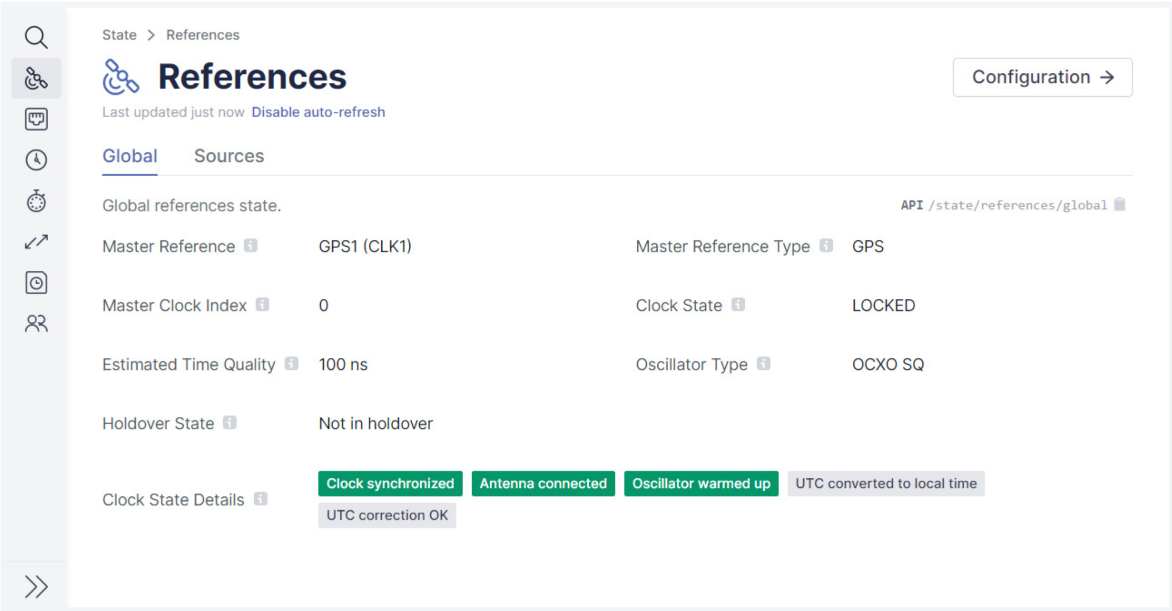


Figure 8.31: meinbergOS Web Interface: "State → References → Global" Tab

The "**State** → **References** → **Global**" tab (Fig. 8.31) provides a summary of your general clock status.

Master Reference: Indicates the source of the external master clock signal. The information in parentheses is the interface through which this clock signal is being passed.

Master Clock Index: The index number of the currently selected master clock. In meinbergOS systems without clock redundancy, this value will always be *0*.

Estimated Time Quality: An estimate of the quality of the system time relative to the external clock source.

Holdover State: Indicates whether the system is in **Holdover Mode**. Holdover Mode is defined as the state where the system is temporarily without an external clock synchronization source, meaning that the system is effectively de-synchronized, but the system is attempting to re-synchronize. In Holdover Mode, the system will attempt to maintain accurate time using the internal oscillator until it can be resynchronized.

Master Reference Type: The type of external signal received by the master clock interface.

Clock State: The synchronization and communication status of the master clock.

Oscillator Type: The type of oscillator installed inside your meinbergOS device (e.g., *OCXO SQ*, *OCXO HQ*).

Clock State Details

This provides detailed information on the status of the master clock.

Time Not Verified: While the clock is synchronized with this reference source, meinbergOS is not using the time from it as the trustworthiness of it is in question.

Clock Synchronized: The clock is synchronized with the reference signal.

Clock Not Synchronized: The clock is not (yet) synchronized with any reference signal; accordingly, the clock time is not deemed to be correct.

Antenna Connected: There is a functioning wired connection between the microSync system and the antenna used to receive the signal.

Antenna Short Circuit: The receiver has detected a short circuit in the antenna connection.

Antenna Disconnected: The antenna has been disconnected from the receiver or is not drawing any power.

Position Not Verified: The GNSS receiver has not (yet) been able to calculate its position.

Oscillator Warmed Up: The oscillator has reached its target frequency and is phase-locked with the reference PPS and 10 MHz signals.

Oscillator Not Warmed Up: The oscillator is not yet aligned with the phase and frequency of its reference signal.

UTC Converted to Local Time: The UTC time obtained from the reference signal is converted to the local time.

UTC Correction OK: The current UTC adjustment parameters (including current leap second data) isdeemed valid.

Daylight Saving Change Announced: A change in Daylight Saving Time has been announced at least one hour before the change is due to come into effect.

Daylight Saving In Effect: The current local time includes the offset for Daylight Saving Time.

Leap Second Announced: A leap second has been announced at least 12 hours before it is due to take effect.

Leap Second is Inserted: The current second is a leap second (second 60 added to a minute).

Leap Second is Negative: The current leap second insertion is negative (second 59 of a minute suppressed).

Invalid Time: The clock time has not yet been initialized since startup.

Synchronized Externally: The clock time has been set by external source.

Holdover Mode: The clock is temporarily running off its internal oscillator as all of the previously used input source signals have been lost.

8.5.1.3 State - References - Sources

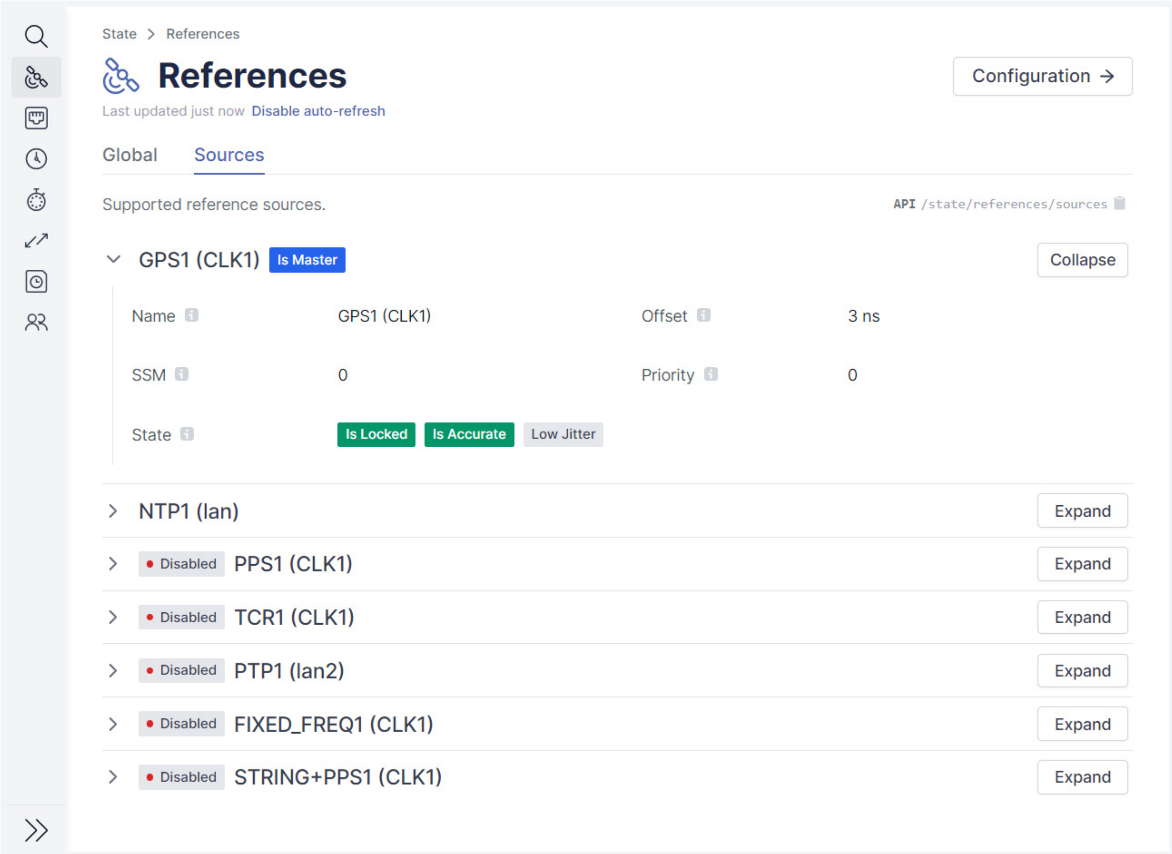


Figure 8.32: meinbergOS Web Interface: "State → References → Sources" Tab

The "**State** → **References** → **Sources**" tab (Fig. 8.32) provides more detailed information on each of the reference sources. Click on the panel of a specific reference to expand it and display the information. Click on the name or arrow again to collapse the panel and hide the information.

Name:	The reference source name and interface through which it is provided.
Offset:	Difference in time between the time source and the main reference.
SSM:	**Synchronization Status Message**. Specifies the quality of the time source and is relevant for SyncE.
Priority:	Priority of the source as defined under "**Configuration** → **References** → **Sources**".
Mean Offset (PPS/PTP/Fixed Freq. only):	The mean offset calculated during the previous statistical polling interval.
Standard Deviation (PPS/PTP/Fixed Freq. only):	The standard deviation of the offset values calculated during the previous statistical polling interval.
Current Record Timestamp: (PPS/PTP/Fixed Freq. only):	The timestamp of the most recent statistical record.
Span: (PPS/PTP/Fixed Freq. only):	The difference between the minimum and maximum offset values recorded during the last statistical interval.
Step Compensated: (PPS/PTP/Fixed Freq. only):	Specifies whether a time jump has been compensated for at the input source.
State:	A series of tags illustrating the status of the source. See chapter "**State - References - Overview**" for more details.
Additional Info:	Provides additional information about the source as supported (such as IP address).

8.5.2 State - Network

The "**State** → **Network**" subsection provides general information about your network connectivity, including PRP network path redundancy and network bonding.

Main: This tab shows the main general network configuration parameters, notably the hostname, default gateways, and DNS servers.

Interfaces: This tab provides information on the physical network interfaces and associated virtual interfaces. It also provides options for Synchronous Ethernet (SyncE) and the **Network** LED on the device itself.

PRP: The **PRP** (Parallel Redundancy Protocol) tab provides information on the physical network interfaces connected for a PRP implementation.

Bonding: The bonding tab shows which physical interfaces are used for link aggregation, and also provides information on the bonding mode used.

8.5.2.1 State - Network - Main

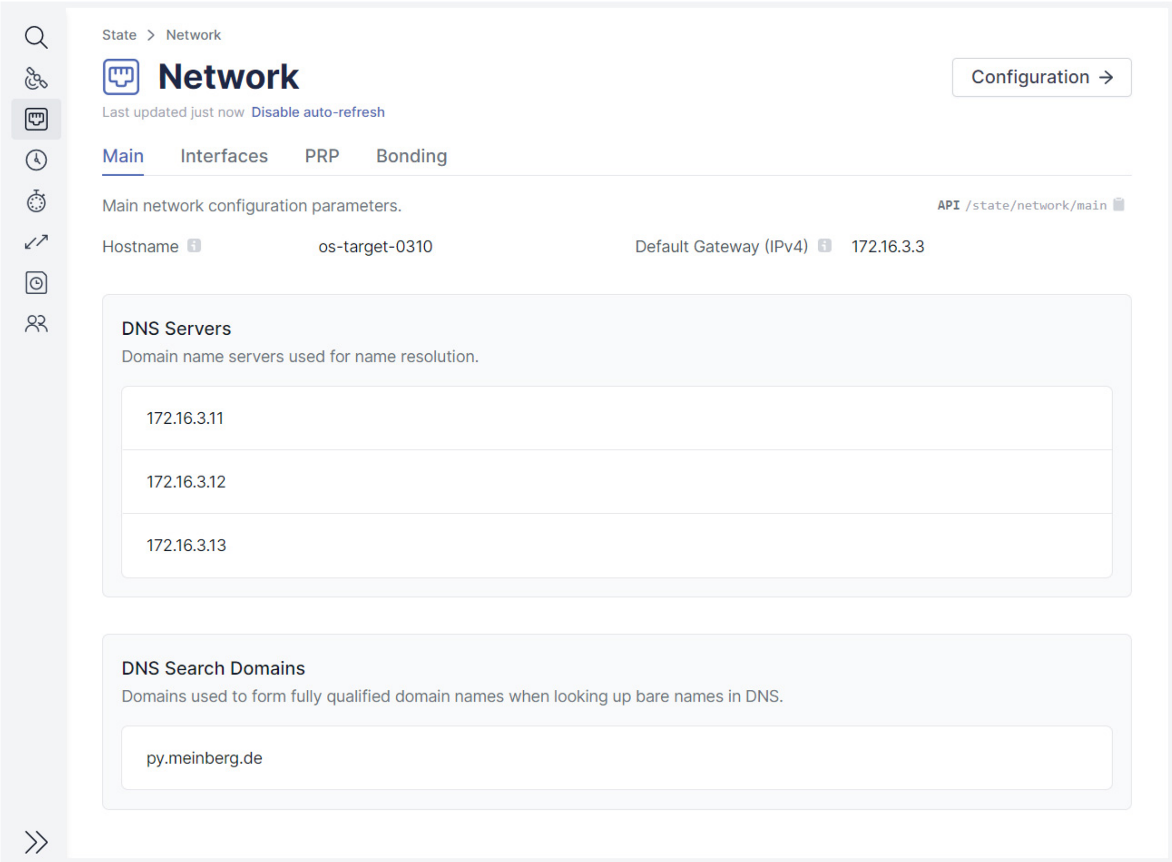


Figure 8.33: meinbergOS Web Interface: "State → Network → Main" Tab

The "**State** → **Network** → **Main**" tab (Fig. 8.33) provides a summary of your primary network configuration.

Hostname: The current hostname of the meinbergOS device, as defined under "**Configuration** → **Network** → **Main**".

Default Gateway (IPv4): The IPv4 address of the default network gateway.

Default Gateway (IPv6): The IPv6 address of the default network gateway, provided that IPv6 is configured. If IPv6 is not configured, this field will show *n/a*.

DNS Servers: Shows the DNS servers used for domain name resolution.

DNS Search Domains: The domains to be appended to bare (unqualified) hostnames for DNS queries.

8.5.2.2 State - Network - Interfaces

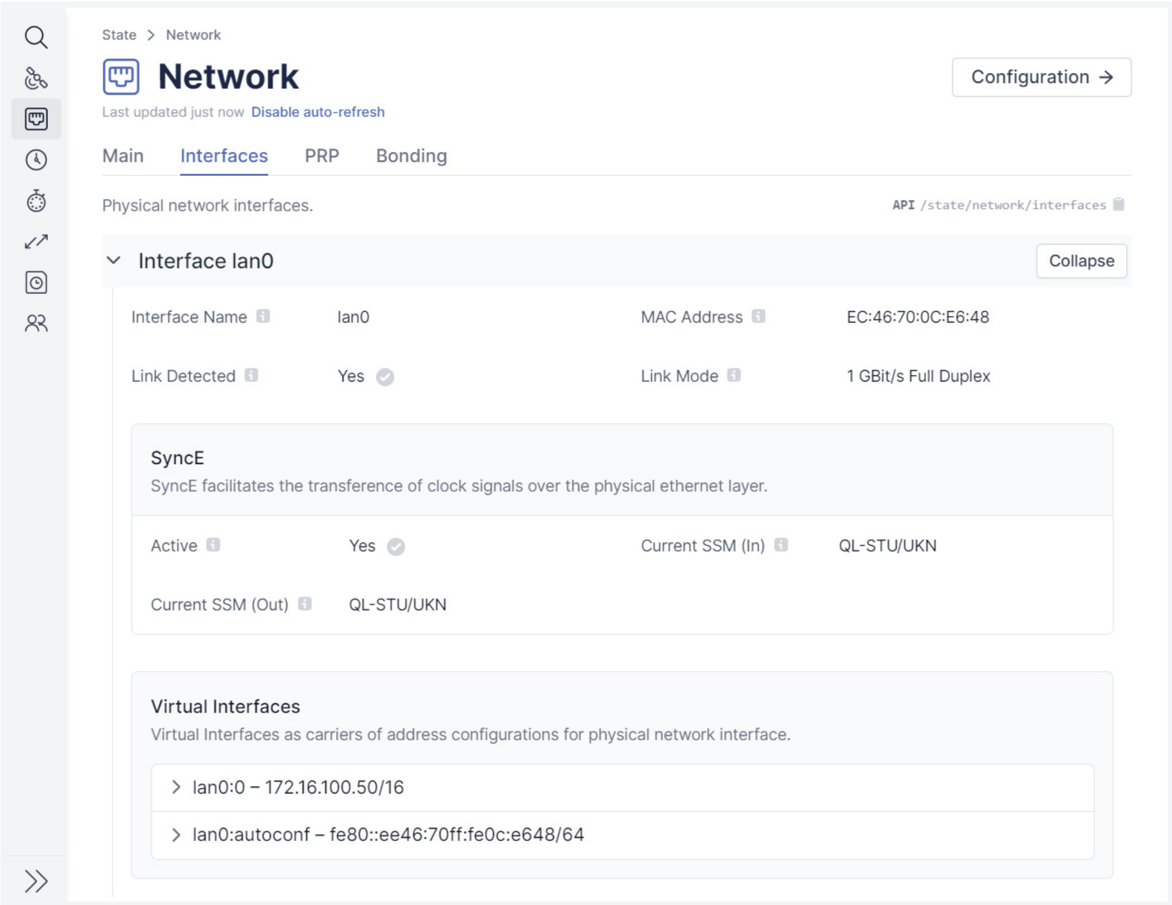


Figure 8.34: meinbergOS Web Interface: "State → Network → Interfaces" Tab

The "**State → Network → Interfaces**" tab (Fig. 8.34) provides details of the status of each individual Ethernet interface in your meinbergOS device. Each interface panel can be opened and closed by selecting it.

Interface Name: The internal system designation for the Ethernet interface.

MAC Address: Indicates the MAC address for the network interface controller (NIC) managing that Ethernet interface. If two Ethernet interfaces are bound to a PRP interface, the MAC address for those two Ethernet interfaces will be identical.

Link Detected: Indicates whether a physical Ethernet connection has been detected ("link-up").

Link Mode: Specifies the link speed and duplex mode of the Ethernet connection. This may have been autonegotiated or manually set under "Configuration".

SyncE: Specifies whether Synchronous Ethernet has been enabled for this Ethernet interface, and if so, the current **Quality Level** in *Master* (output) and *Slave* (input) mode. Refer to "SSM Quality Levels" for further information.

PRP Master: If PRP is enabled for this interface, this indicates the PRP interface that this Ethernet interface is currently bound to. For a functional PRP implementation, two of the Ethernet interfaces listed here must have the same PRP master.

PRP Path: If PRP is enabled for this interface, this specifies which of the two paths in the PRP configuration this Ethernet interface is used for.

Virtual Interfaces: The virtual interfaces configured for this physical interface are displayed in this panel, showing the interface name, DHCP state, set or assigned IP address, and prefix bits for the netmask.

8.5.2.3 State - Network - PRP

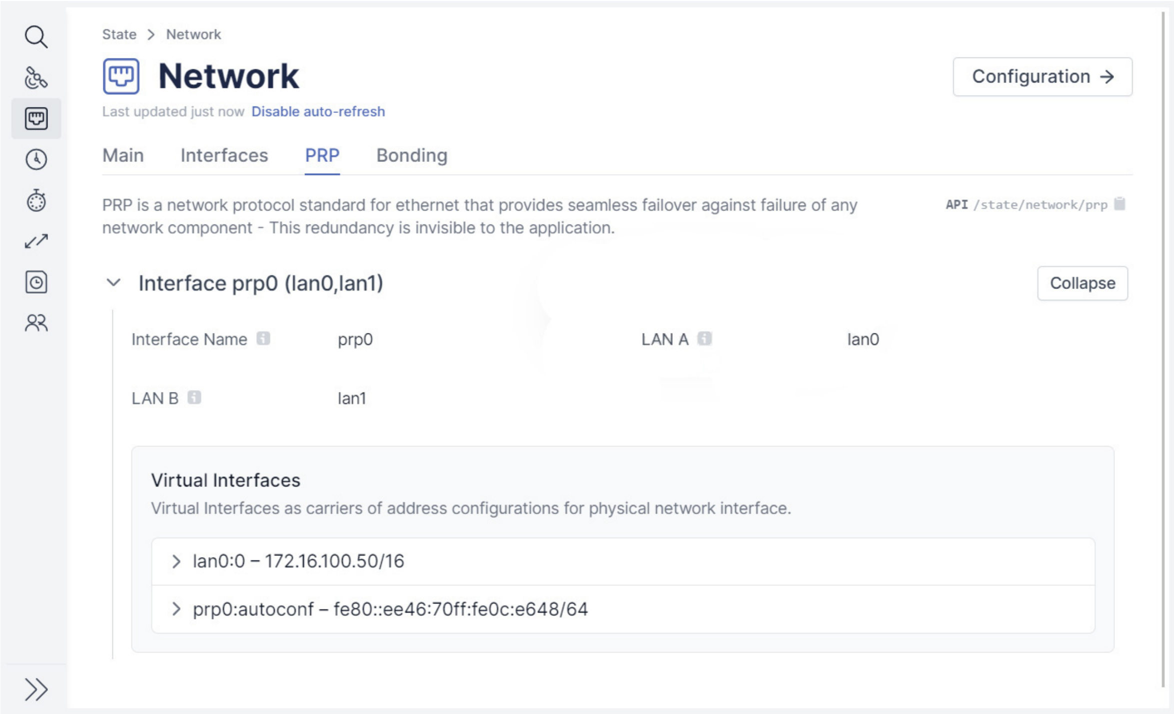


Figure 8.35: meinbergOS Web Interface: "State → Network → PRP" Tab

The "**State → Network → PRP**" tab (Fig. 8.35) provides details for configured PRP interfaces. PRP is a network protocol standard for Ethernet that enables seamless network path failover in the event of failure of any network components.

Interface Name: The internal system designation for the PRP interface.

LAN A: The physical Ethernet interface that serves as the first PRP path, as configured under "**Configuration → Network → PRP**".

LAN B: The physical Ethernet interface that serves as the second PRP path, as configured under "**Configuration → Network → PRP**".

Each PRP interface panel also features a sub-panel showing the virtual interfaces assigned to that PRP interface. Refer to the chapters "**Configuration - Network - Interfaces**" and "**State - Network - Interfaces**" for more information.

8.5.2.4 State - Network - Bonding

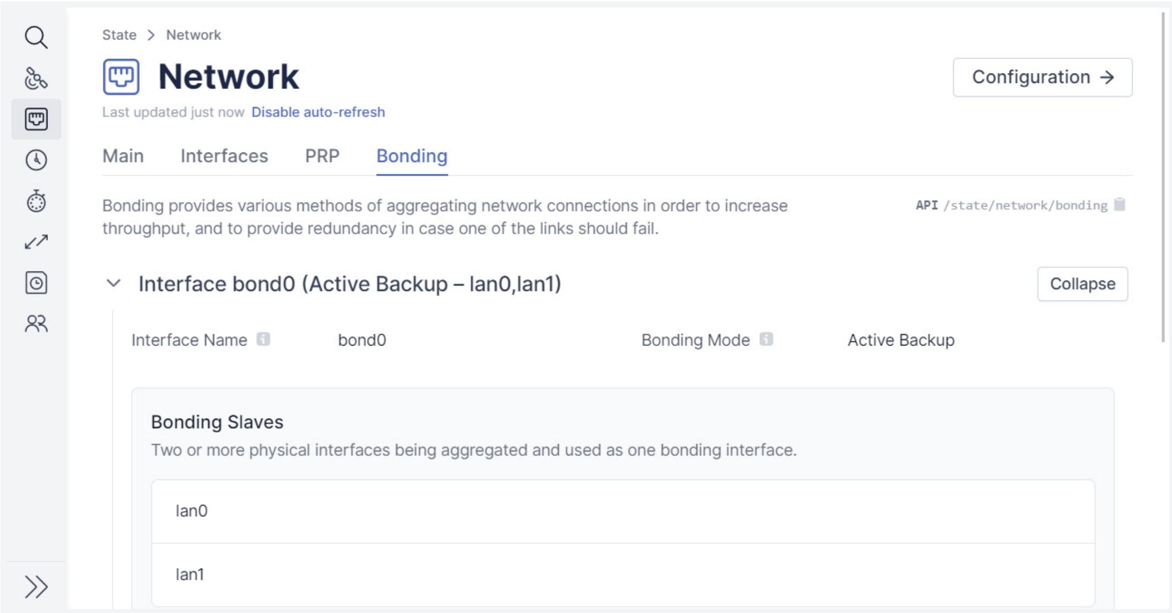


Figure 8.36: meinbergOS Web Interface: "State → Network → Bonding" Tab

The "**State** → **Network** → **Bonding**" tab (Fig. 8.36) provides information on aggregated ('bonded') network connections. Bonded network connections are used to increase throughput and provide redundancy by various means in case one of the links fails.

Interface Name: The internal system designation assigned by the Kernel for the bonding interface.

Bonding Mode: The mode set for the Linux bonding driver (network interface aggregation mode). This is the mode defined under **Configuration**, and may be "*Round Robin*", "*Active Backup*", "*XOR*", "*Broadcast*", or "*802.3ad (LACP)*".

Bonding Slaves: The slave interfaces in the bonding group are listed here.

Virtual Interfaces: The virtual interfaces assigned to this bonding group.

8.5.3 State - NTP

The "**State** → **NTP**" subsection provides general information about the system's NTP functionality, both as a server and as a client.

Main: This tab provides general information about the meinbergOS device's own NTP service.

Server: This tab provides information about the local NTP server as used to serve external clients.

Client: This tab provides information about remote NTP servers serving this meinbergOS device.

8.5.3.1 State - NTP - Main

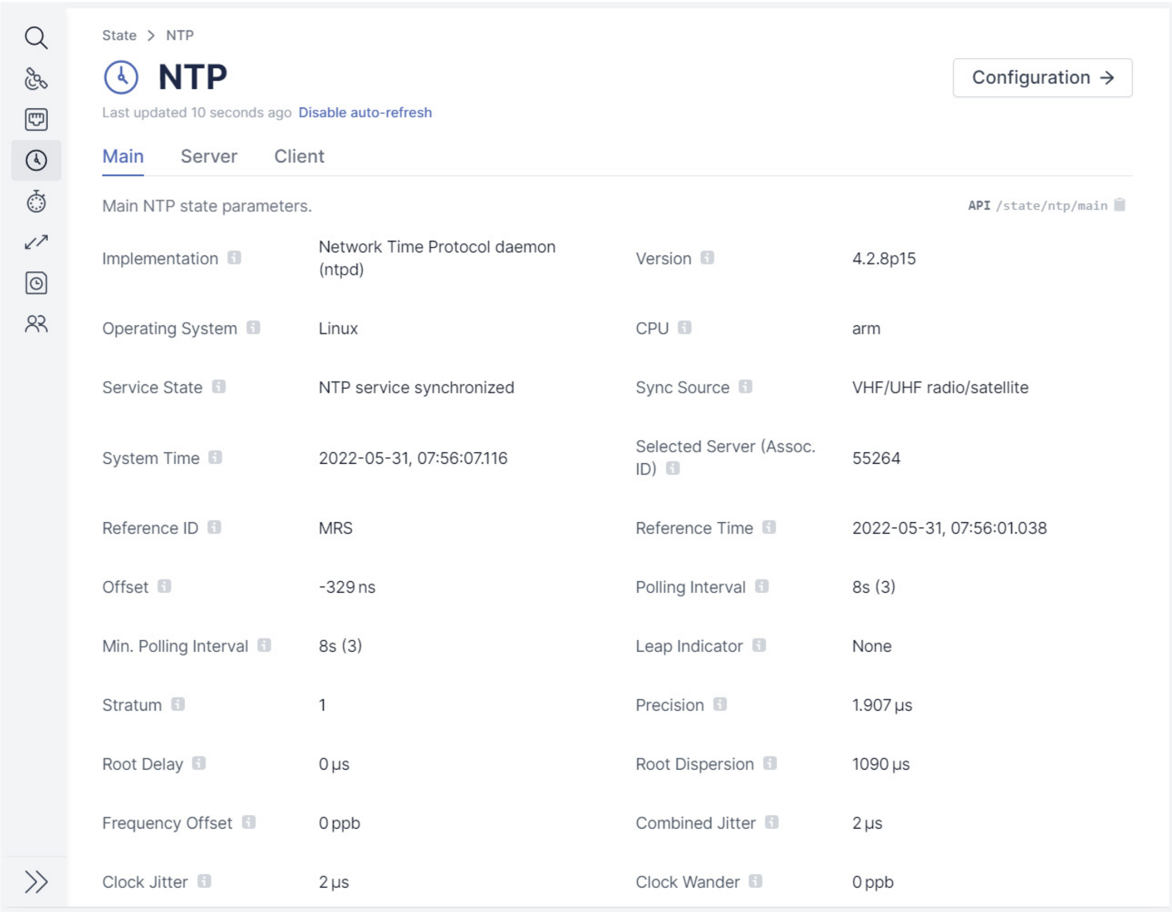


Figure 8.37: meinbergOS Web Interface: "State → NTP → Main" Tab

The "**State → NTP → Main**" tab (Fig. 8.37) provides general information about the meinbergOS device's own NTP service.

Implementation: The NTP implementation being used by the system. This should always read "*Network Time Protocol daemon (ntpd)*".

Version: The version of the NTP implementation of the system. This version number relates to the version numbering system employed by the official NTP Project.

Operating System: The operating system used for your system. This should always read "*Linux*".

CPU: The type of CPU used in the device. For most systems, this will usually be "*arm*".

Service State: The current synchronization status of the NTP service. This can be:

- *NTP service initializing*
- *NTP service synchronized*
- *NTP service not synchronized*
- *NTP service stopped*

Sync Source: The "source" of the signal used to synchronize the system. This will usually read "*VHF/UHF radio/satellite*" due to how the NTP service operates within the meinbergOS device. The actual reference source for the NTP service can be identified under "**State** → **References**". Refer to chapter "**State - References**" for further information.

System Time: The current system time as at the time this page was last loaded.

Selected Server (Assoc. ID): The association ID of the current system peer. This references a relationship (association) between an NTP server and NTP client.

Reference ID: The reference ID of the current NTP system peer. This will usually be "*MRS*", which refers to the internal clock module of meinbergOS devices.

Reference Time: The last time the system time was adjusted.

Offset: The cumulative offset relative to the current system peer.

Polling Interval: The current polling interval for NTP system peers. This is the value currently applied by this system for querying the selected system peer.

Min. Polling Interval: The minimum polling interval for system peers.

Leap Indicator: The latest leap indicator announcement, if provided by the NTP service. The leap indicator may specify if a leap second is to be inserted ("*Insert second*") or removed ("*Delete second*"), or if leap indicators cannot be acquired due to loss of synchronization ("*Alarm*").

Stratum: The current stratum level of the system. A clock that is synchronized directly against a Stratum 0 clock such as a GPS signal is a Stratum 1 clock; therefore, provided that your system has a stable Stratum 0 lock, this value should be *1*.

If the system becomes desynchronized, the NTP service will enter "orphan mode", and the corresponding stratum level defined under "**Configuration** → **NTP** → **Server**" will be displayed here.

Precision: The current accuracy of the system clock.

Root Delay: The total estimated round trip delay (time to transmit messages to current system peer plus time to receive acknowledgement of receipt).

Root Dispersion: The additional dispersion time in communication with the system peer, representing delays caused by other factors such as clock frequency inaccuracy.

Frequency Offset: The current frequency offset relative to the hardware clock. This value is calculated automatically to account for possible drift in the hardware clock.

Combined Jitter: The total combined jitter of the system. This value corresponds to the *ntpq* value *sys_jitter*.

Clock Jitter: The current jitter of the clock. Clock jitter refers to phase deviations in the actual clock waveform edge positions relative to the expected waveform edge positions.

Clock Wander: The frequency wander of the clock. Clock wander refers to long-term frequency variations in the clock, is measured in parts per billion (ppb) and is an indicator of overall system clock stability. It corresponds to the *ntpq* value *clk_wander*.

8.5.3.2 State - NTP - Server

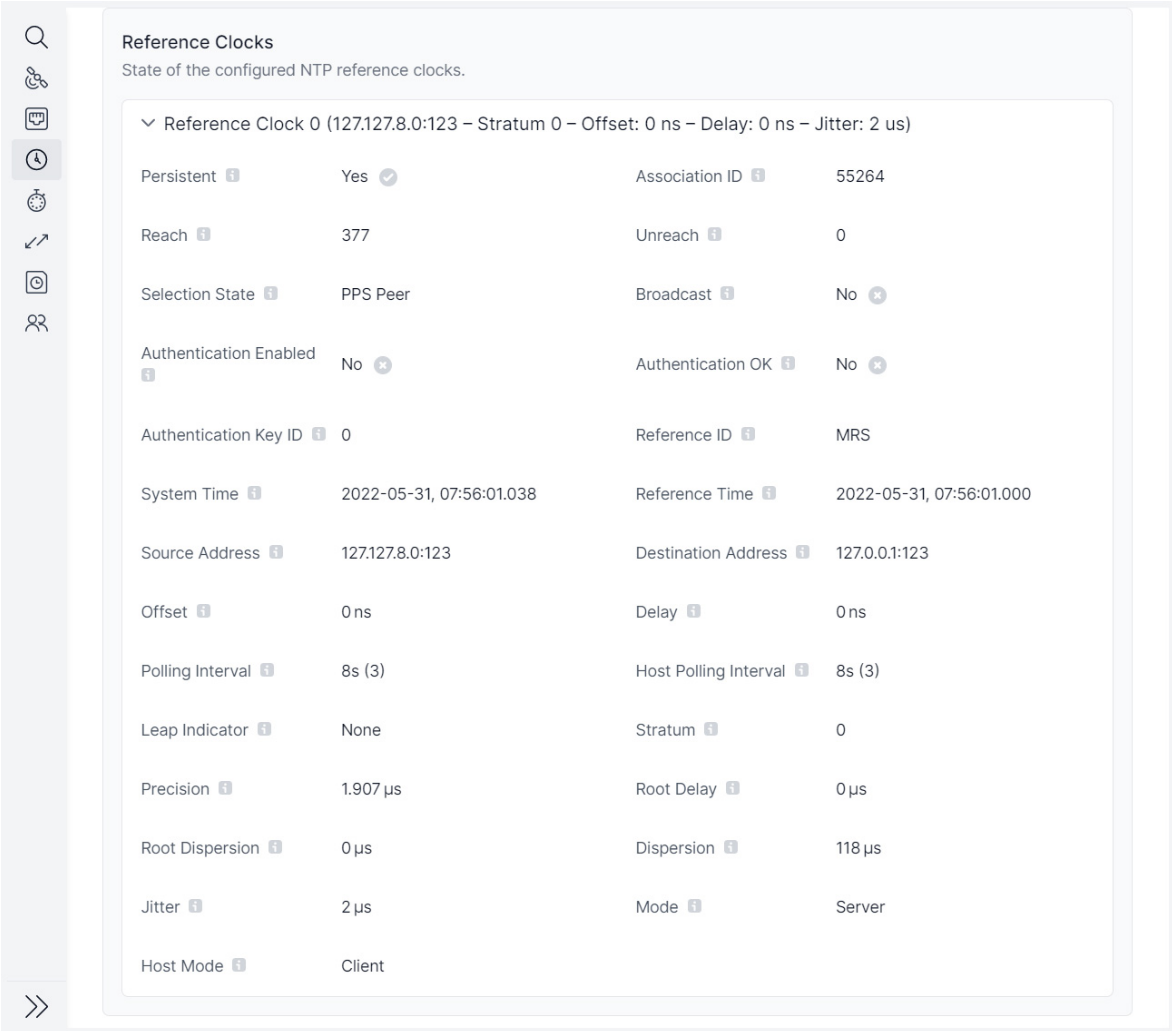


Figure 8.38: meinbergOS Web Interface: "State → NTP → Server" Tab

Information:

This information relates to how your meinbergOS device operates as an NTP server or peer and not to your meinbergOS device as a client.

For information on NTP server/client relationships where your meinbergOS device is the client, please open the subsection "**State → NTP → Client**" and refer to the information provided in the corresponding chapter of this manual.

Reference Clocks

State of the configured NTP reference clocks.

Persistent: If this source is configured as a persistent server (i.e., not accessed as part of a pool server), this entry will show *Yes*.

Association ID: The unique association ID for this source assigned by NTP.

Reach: This is a reachability shift register for the last eight polling intervals, expressed as a three-digit octal value. This octal value can be used to easily derive each individual bit of the 8-bit shift register by converting each digit to its corresponding binary value.

It should always be "*377*" in this case, as the local NTP client is polling the local NTP server. Any other value may be indicative of an internal system error.

Unreach: The total number of unsuccessful polling intervals since last (re)boot or since the last restart of the NTP daemon. This should generally be *0*. Any other value may be indicative of an internal system error.

Selection State: The current peer selection status of the source.

Broadcast: Indicates if the peer association with this source is a broadcast association.

Authentication Enabled: Indicates if authentication is enabled for this source.

Authentication OK: Indicates if authentication was successful for this source.

Authentication Key ID: This is the ID of the symmetric key being used for authentication.

Reference ID: The reference ID of this system as a source.

System Time: The current system time of this source as at the time this page was last loaded.

Reference Time: This shows when the time of this source was last adjusted.

Source Address: IP address and port of the local clock. This will generally read *127.127.8.0:123*, as this is the address of the NTP server as accessible from the NTP server itself and relates to the internal clock of the meinbergOS device.

Destination Address: IP address and port of the local system. This will generally read *127.0.0.1:123*, which is the address of the NTP client residing on the NTP server itself and relates to the internal clock of the meinbergOS device.

Offset: The filter offset between the reference clock and the current system time for this NTP source. This value should be *0* as long as the clock is synchronized.

Delay: The filter path delay between the reference clock and the current system time for this NTP source. This value should be *0* when using the meinbergOS device's internal clock module and the clock frequency is stable.

Polling Interval: The polling interval currently used internally by this source from the perspective of the local NTP server and applied to associations with external NTP clients and peers.

Host Polling Interval: The polling interval currently used internally by this source from the perspective of the local NTP client. This will be identical to the host polling interval, which is the polling interval used internally by this source from the perspective of the local NTP server.

Leap Indicator: The latest leap indicator announcement of this source. The leap indicator may specify if a leap second is to be *inserted* or *removed*, or if leap indicators cannot be acquired due to loss of synchronization ("*Alarm*").

Stratum: The current stratum level of this NTP server in relation to its own NTP client. This will always be a fictitious *0* and has no bearing on the actual stratum of the meinbergOS device in use as an NTP server.

Precision: The current accuracy of this source.

Root Delay: The total estimated round trip delay (time to transmit messages to current system peer of this source, plus time to receive acknowledgement of receipt). This should generally be *0*, as there is no round trip involved in the internal communication.

Root Dispersion: The additional dispersion time in communication with the system peers of this source, representing delays caused by other factors such as clock frequency inaccuracy. This should generally be *0*.

Dispersion: The filter dispersion for this source.

Jitter: The filter jitter for this source.

Mode: The NTP mode for this source. This will always be *Server*.

Host Mode: The NTP mode of the requesting host. This will always be *Client*.

8.5.3.3 State - NTP - Client

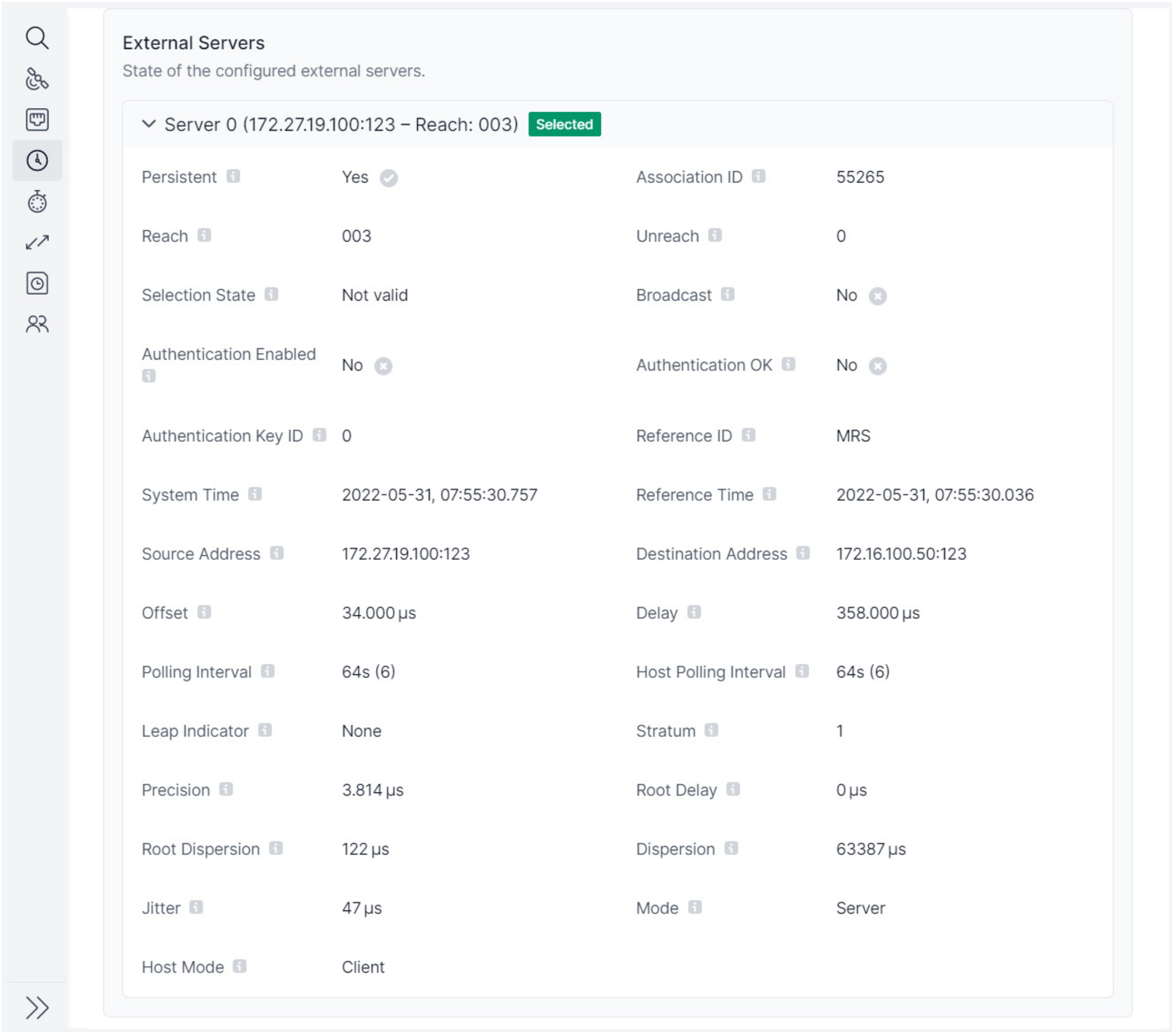


Figure 8.39: meinbergOS Web Interface: "State → NTP → Client" Tab

Information:

This information relates to how your meinbergOS device operates as an NTP client and not to clients that your meinbergOS device may be a server to.

For information on NTP server/client relationships where your meinbergOS device is the **server**, please open the subsection "**State** → **NTP** → **Server**" and refer to the guidance provided in the corresponding chapter of this manual.

External Servers

Shows the state of the external servers configured for the meinbergOS device's NTP client.

Persistent: If this source is configured as a persistent server (i.e., not accessed as part of a pool server), this entry will show *Yes*.

Association ID: The unique association ID for this source assigned by NTP.

Reach: This is a reachability shift register for the last eight polling intervals, expressed as a three-digit octal value. This octal value can be used to easily derive each individual bit of the 8-bit shift register by converting each digit to its corresponding binary value.

For example, a value of "*377*" indicates that all of the last eight polling intervals were successful, because *3 = 11* and *7 = 111*, making *377* equivalent to the binary value *11111111*.

Unreach: The total number of unsuccessful polling intervals since last (re)boot or since the last restart of the NTP daemon.

Selection State: The current peer selection status of the source.

Broadcast: Indicates if the peer association with this source is a broadcast association.

Authentication Enabled: Indicates if authentication is enabled for this source.

Authentication OK: Indicates if authentication was successful for this source.

Authentication Key ID: This is the ID of the symmetric key being used for authentication.

Reference ID: The reference ID of this source.

System Time: The current system time of this source as at the time this page was last loaded.

Reference Time: This shows when the time of this source was last adjusted.

Source Address: The IP address and port of this source (server or peer).

Destination Address: The IP address of this system's NTP client.

Offset: The filter offset for this NTP source.

Delay: The filter delay for this NTP source.

Polling Interval: The polling interval currently used by this peer or server.

Host Polling Interval: The polling interval currently used by the meinbergOS device.

Leap Indicator: The latest leap indicator announcement, if provided by the NTP service. The leap indicator may specify if a leap second is to be inserted ("*Insert second*") or removed ("*Delete second*"), or if leap indicators cannot be acquired due to loss of synchronization ("*Alarm*").

Stratum: The current stratum level of this NTP source. Servers directly synchronized with a Stratum 0 clock will be Stratum *1*. If an NTP server or peer is unable to reach any of its sources, it will generally be Stratum *16*.

Precision: The current accuracy of this source.

Root Delay: The total estimated round trip delay (time to transmit messages to current system peer of this source, plus time to receive acknowledgement of receipt).

Root Dispersion: The additional dispersion time in communication with the system peers of this source, representing delays caused by other factors such as clock frequency inaccuracy.

Dispersion: The filter dispersion for this source.

Jitter: The filter jitter for this source.

Mode: The NTP mode for this server.

Host Mode: The NTP mode for the meinbergOS device in respect of its association with the server or peer.

8.5.4 State - PTP

The "**State** → **PTP**" subsection provides general information about the system's PTP functionality, both as a master and a slave. It also provides two tabs—**Interfaces**, which provides information on the PTP-related states of the PTP-enabled virtual interfaces, and **Instances**, which provides information on the configured PTP instances and comprehensive readouts of the relevant datasets.

The panels at the top of the Content Area provides an overview of the PTP service at each assigned virtual interface. The header shows the name set under "**Configuration** → **PTP** → **Instances**", the virtual interface, and the EUI-64 clock identifier.

Network Interface:	Indicates the link state of the physical network interface.
Domain:	The PTP domain set for this PTP instance.
GM Clock Class:	An 8-bit value (*0–255*) specifying the class of the grandmaster. The **Clock Class** indicates the clock's suitability as a master clock (lower value = more suitable).
GM Clock Accuracy:	The accuracy range of the grandmaster clock relative to UTC.
GM Clock Variance:	A statistical value representing clock jitter and wander between two sync message intervals.
GM Clock Identity:	The EUI-64 identifier of the grandmaster clock.
UTC Offset:	The current UTC offset of this instance.
Offset from Master (Slave only):	Specifies the current offset from the master clock.
Offset from Reference (Slave only):	Specifies the current offset from the internal reference.
Path Delay (Slave only):	Specifies the current mean path delay relative to the current master clock.

Time Properties

These are the time property flags that may be displayed in relation to the current PTP time:

Time is traceable:	This specifies whether the master clock's time can be traced back to a primary reference other than itself.
Frequency is traceable:	This specifies whether the master clock's frequency can be traced back to a primary reference other than itself.
UTC offset is valid:	This specifies whether the master clock's UTC offset (or the instance's own UTC offset if the instance is itself in *Master* Mode) is valid.
Is PTP Timescale:	This specifies whether the master clock is using the PTP timescale (TAI).
Leap 59 announced:	This specifies that a negative leap second has been announced by the instance's reference source.
Leap 61 announced:	This specifies that a positive leap second has been announced by the instance's reference source.

8.5.4.1 State - PTP - Interfaces

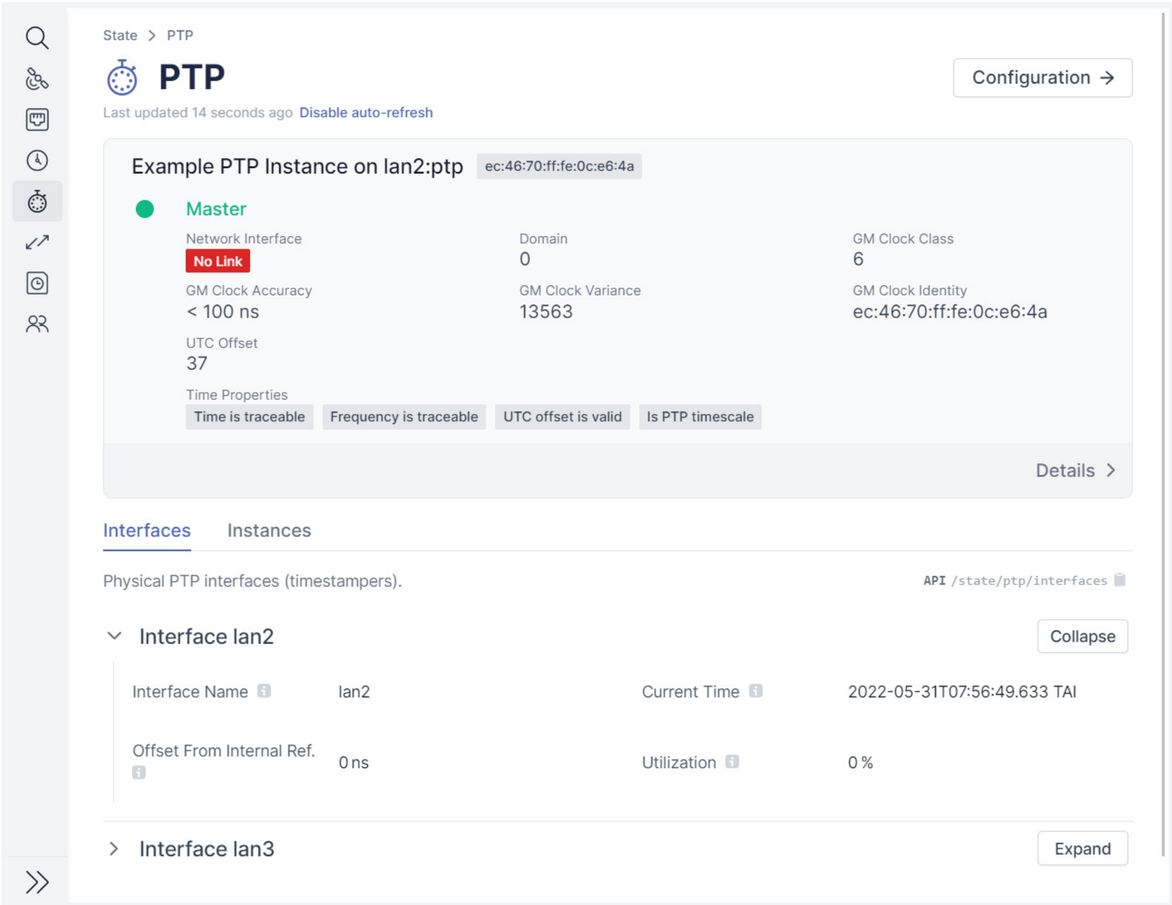


Figure 8.40: meinbergOS Web Interface: "State → PTP → Interfaces" Tab

The tab "**State** → **PTP** → **Interfaces**" (Fig. 8.40) provides information about the physical PTP interfaces (timestampers) supported by your meinbergOS device.

Interface Name: The name of the physical PTP interface of the meinbergOS device.

Current Time: The current time of the timestamper, formatted according to ISO 8601.

Offset From Internal Ref.: Current time offset between the timestamper time and the internal reference time.

Utilization: Current resource utilization (messages per second) of this timestamper in percent.

8.5.4.2 State - PTP - Instances

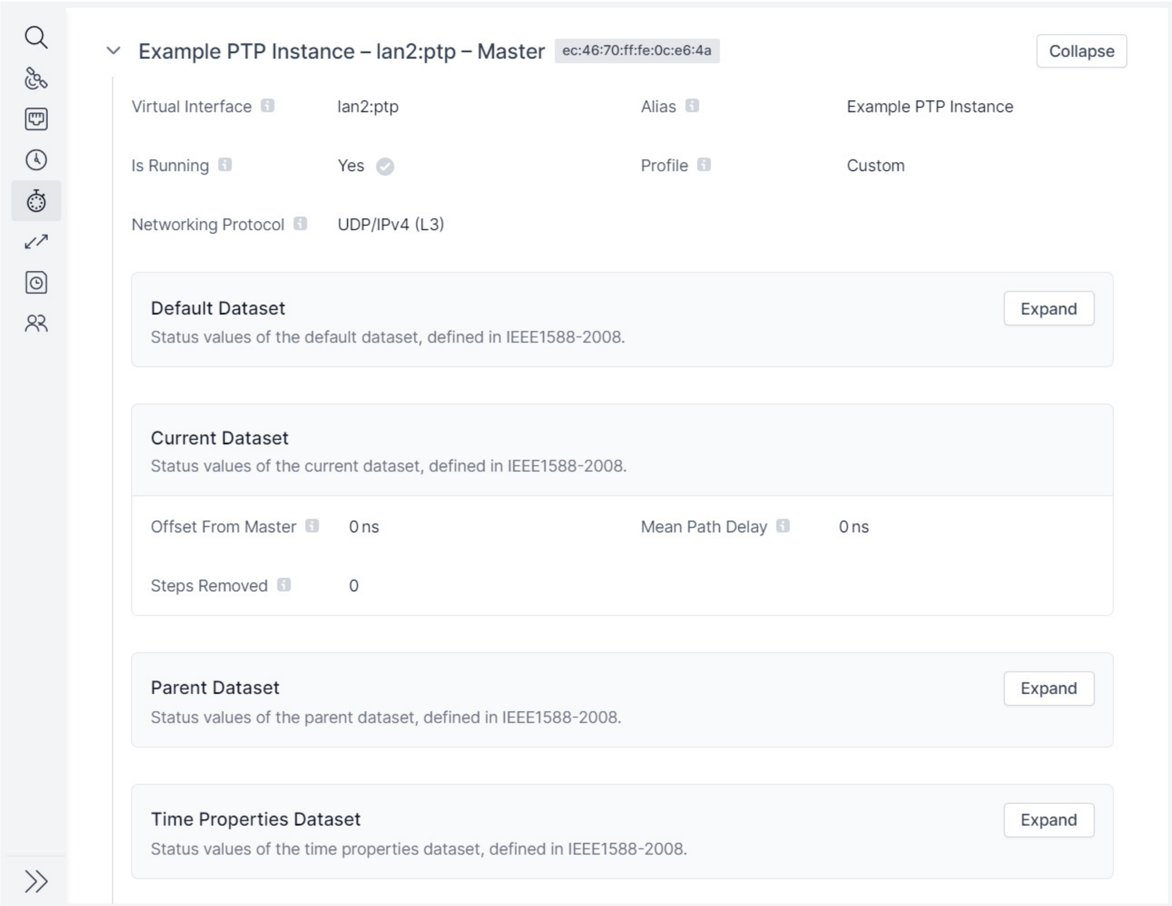


Figure 8.41: meinbergOS Web Interface: "State → PTP → Instances" Tab

The tab "**State** → **PTP** → **Instances**" (Fig. 8.41) provides information about the defined PTP instances.

Virtual Interface: The virtual interface (i.e., IP address) that the instance is using.

Alias: A manually assigned descriptive alias of this instance (if configured).

Is Running: Indicates whether the PTP stack of this instance is currently running.

Profile: The PTP profile that this instance is currently running in.

Networking Protocol: The networking protocol used by this instance. This may be *UDP/IPv4 (L3)*, *UDP/IPv6 (L3)*, or *IEEE 802.3 (L2)*.

Utilization: Current resource utilization (messages per second) in percent.

Default Dataset

These are the status values of the default dataset as defined in IEEE 1588-2008.

Number Ports: The number of PTP ports on the device.

Is Two-Step: Indicates whether the clock is a two-step clock (sync and timestamp are sent in two separate PTP messages). In end-to-end networks this should be *No*, as two-step clocks require predictable latency values with a singularly defined peer-to-peer connection.

Is Slave-Only: Indicates whether the clock is a slave-only clock.

Clock Class: The **Clock Class** attribute as defined by IEEE 1588-2008 or specific PTP profiles. It reflects the current synchronization state of the local clock. A lower class generally means a better master clock.

Clock Accuracy: One of the **Clock Accuracy** classes defined in IEEE 1588 reflecting the current accuracy of the local clock.

These classes are: *< 25 ns, < 100 ns, < 250 ns, < 1 us, < 2.5 us, < 10 us, < 25 us, < 100 us, < 250 us, < 1 ms, < 2.5 ms, < 10 ms, < 25 ms, < 100 ms, < 250 ms, < 1 s, < 10 s, more than 10 s*

Clock Variance: The **Offset-Scaled Log Variance** representing the time stability of the local clock. This value provides a basis of estimating the precision of the timestamping while not synchronized.

Priority 1: The **Priority 1** attribute of the local clock. This value dictates the absolute priority of the clock as a master candidate above any other operational factors.

Priority 2: The **Priority 2** attribute of the local clock. This value determines the priority of the clock as a master candidate, but is generally disregarded if the Best Master Clock can be other determined using **Clock Class**, **Clock Accuracy**, and **Clock Variance**. It is generally applied for backup or redundant master clocks.

Clock ID: The unique ID of the local clock. This is a 64-bit extended unique identifier ("EUI-64") that is normally based on the MAC address of the network device.

Domain Number: The PTP domain number of the local clock. The clock will ignore PTP messages with domain numbers other than this.

Current Dataset

These are the status values of the current dataset as defined in IEEE 1588-2008.

Offset From Master: The current difference between the master time and slave time.

Mean Path Delay: The current mean propagation time for messages between the master and slave.

Steps Removed: The number of hops between the local clock and the PTP grandmaster. If the local clock is connected directly to the grandmaster, this value will be *1*.

Parent Dataset

These are the status values of the parent dataset as defined in IEEE 1588-2008, relating to the parent of the local clock (the master clock most directly connected to the local clock).

Parent Clock ID: The clock ID of the master clock from which the local clock is currently directly receiving PTP messages. This is a 64-bit extended unique identifier ("EUI-64") that is normally based on the MAC address of the network device.

Parent Port ID: The port number of the master clock from which the local clock is currently directly receiving PTP messages.

Is Statistics Valid: Indicates whether the local clock has computed statistically valid estimates of the log variance and phase change rate of the parent clock.

GM Priority 1: The **Priority 1** attribute of the current grandmaster clock. This value dictates the absolute priority of the grandmaster as a master candidate above any other operational factors.

GM Priority 2: The **Priority 2** attribute of the current grandmaster clock. This value determines the priority of the clock as a master candidate, but is generally disregarded if the Best Master Clock can be other determined using **Clock Class**, **Clock Accuracy**, and **Clock Variance**. It is generally only applied for backup or redundant master clocks.

GM Clock Class: The **Clock Class** attribute for the grandmaster clock as defined by IEEE 1588-2008 or specific PTP profiles. It reflects the current synchronization state of the grandmaster clock.

GM Clock Accuracy: One of the **Clock Accuracy** classes defined in IEEE 1588 reflecting the current accuracy of the grandmaster clock.

GM Clock Variance: The **Offset-Scaled Log Variance** representing the time stability of the grandmaster clock. This value provides a basis of estimating the precision of the timestamping while not synchronized.

GM Clock ID: The **Clock ID** of the current grandmaster clock. This is a 64-bit extended unique identifier ("EUI-64") that is normally based on the MAC address of the network device.

Time Properties Dataset

These are the status values of the time properties dataset as defined in IEEE 1588-2008.

Is UTC Offset Valid: Specifies whether the current UTC offset is known to be valid.

Is Leap 61: If this is *Yes*, the last minute of the current UTC day will last 61 seconds (thus adding a leap second).

Is Leap 59: If this is *Yes*, the last minute of the current UTC day will last 59 seconds (thus removing a leap second).

Is PTP Timescale: If this is *Yes*, the timescale applies by the current grandmaster is the PTP timescale (International Atomic Time, TAI).

Is Time Traceable: If this is *Yes*, the timescale and UTC offset can be traced back to a primary reference.

Is Frequency Traceable: If this is *Yes*, the frequency determining the timescale can be traced back to a primary reference.

Time Source: The time source currently used by the grandmaster clock.

Port Dataset

These are the status values of the port dataset as defined in IEEE 1588-2008.

Clock ID: The clock ID of the local port. This is a 64-bit extended unique identifier ("EUI-64") that is normally based on the MAC address of the network device.

Port ID: The local port through which the local clock is currently communicating PTP messages.

Port State: The current state of the protocol engine currently associated with this port.

Announce

Receipt Timeout: The number of message intervals that has to pass without receipt of an **Announce** message before a network path or device is considered to possibly be failed.

Announce Interval: The mean time between individual **Announce** messages.

Sync Interval: The mean time between successive **Sync** messages when transmitted as multicast messages.

Delay Mechanism: The method used to calculate the propagation delay when computing the mean path propagation delay. This can be *P2P* (peer-to-peer) or *E2E* (end-to-end).

Version Number: The PTP version in use on this port.

Unicast Slaves

Unicast slaves connected to this meinbergOS device (serving as the PTP unicast master) are listed here.

Packet Counters

This list provides detailed packet counter statistics for all types of PTP messages, both incoming and outgoing.

Is Enabled:	Specifies if packet counting is enabled for this PTP instance.
Announce Receipt Timeouts:	This counts how many **Announce** receipt timeouts there have been so far.

Receive and Transmit Counters

The packet counters for incoming and outgoing packets respectively are explained below.

Total Messages:	The total number of messages received/sent.
Total Messages Per Second:	The number of messages currently being received/sent per second.
Announce Messages:	The total number of **Announce** messages that have been received/sent.
Announce Messages Per Second:	The number of **Announce** messages currently being received/sent per second.
Sync Messages:	The total number of **Sync** messages that have been received/sent.
Sync Messages Per Second:	The number of **Sync** messages currently being received/sent per second.
Follow Up Messages:	The total number of **Follow-Up** messages that have been received/sent.
Follow Up Messages Per Second:	The number of **Follow-Up** messages currently being received/sent per second.
Delay Request Messages:	The total number of **Delay Request** messages that have been received/sent.
Delay Request Messages Per Second:	The number of **Delay Request** messages currently being received/sent per second.
Delay Response Messages:	The total number of **Delay Response** messages that have been received/sent.
Delay Response Messages Per Second:	The number of **Delay Response** messages currently being received/sent per second.
Peer Delay Request Messages:	The total number of **Peer Delay Request** messages that have been received/sent.

Peer Delay Request Messages Per Second: The number of **Peer Delay Request** messages currently being received/sent per second.

Peer Delay Response Messages: The total number of **Peer Delay Response** messages that have been received/sent.

Peer Delay Response Messages Per Second: The number of **Peer Delay Response** messages currently being received/sent per second.

Peer Delay Response Follow Up Messages: The total number of **Peer Delay Response Follow-Up** messages that have been received/sent.

Peer Delay Response Follow Up Messages Per Second: The number of **Peer Delay Response Follow-Up** messages currently being received/sent per second.

Signaling Messages: The total number of **Signaling** messages that have been received/sent.

Signaling Messages Per Second: The number of **Signaling** messages currently being received/sent per second.

Management Messages: The total number of **Management** messages that have been received/sent.

Management Messages Per Second: The number of **Management** messages currently being received/sent per second.

Management Errors: The total number of **Management** message errors.

8.5.5 State - IO Ports

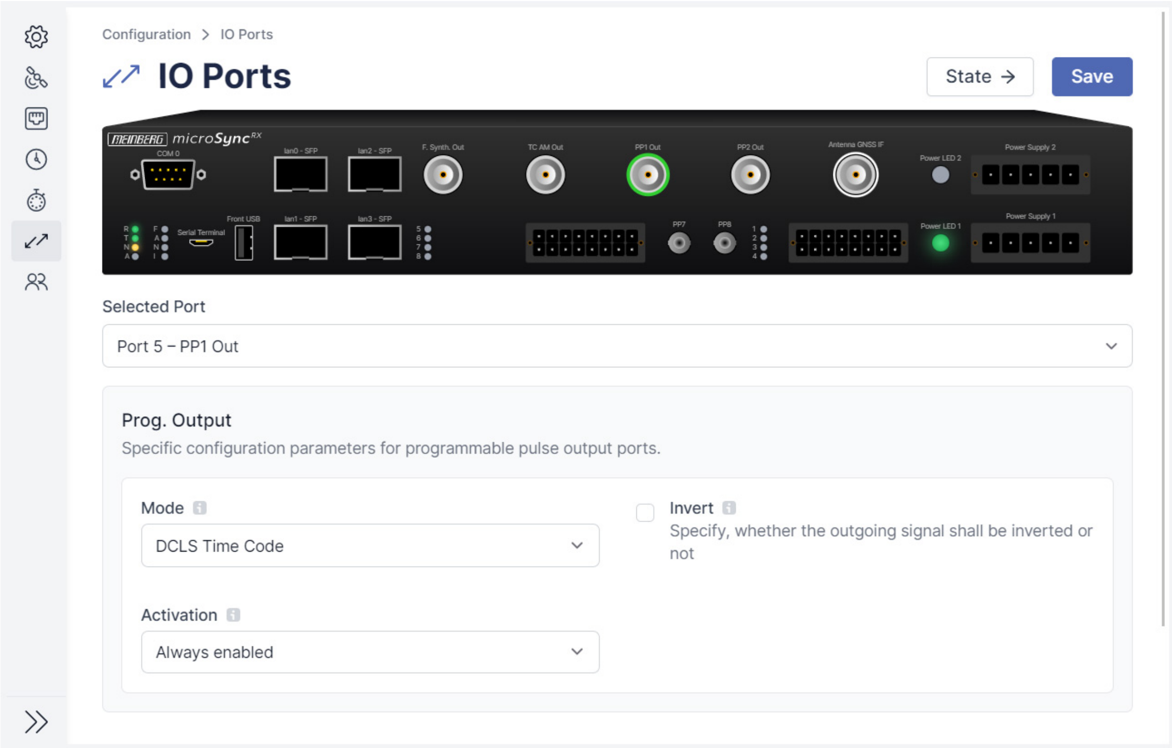


Figure 8.42: meinbergOS Web Interface: "State → IO Ports" Subsection

The "**State → IO Ports**" subsection (Fig. 8.42) provides a graphical representation of your physical meinbergOS device (for example, a microSync). Hovering with the mouse over any indicator or connector (or, in the case of multi-pin connectors, over an individual pin of a connector) will provide a brief explanation of the purpose of that component.

Clicking on a configurable connector or pin will open the corresponding configuration panel for that connector or indicator or provide a link to the relevant **Configuration** or **State** section.

Information:

Configuration options are not available for all I/O ports.

For more information, please refer to the chapter "**Configuration - IO Ports**".

8.5.6 State - Clock Module

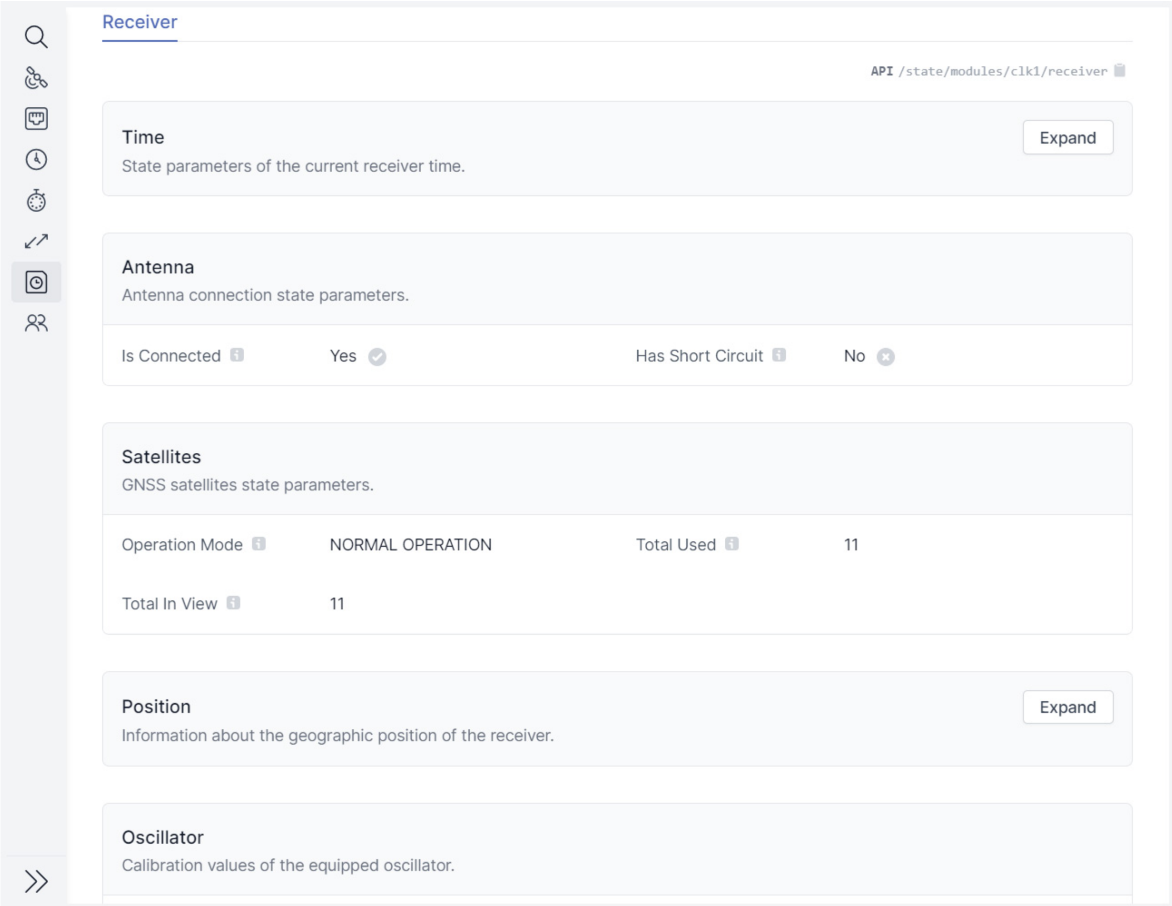


Figure 8.43: meinbergOS Web Interface: "State → Clock Module" Subsection

The **Clock Module** subsection provides information about the receiver integrated into the meinbergOS device.

Time

The **Time** panel provides status information regarding the time provided by the receiver.

Timestamp: The current time provided by the receiver.

UTC Offset: If the receiver is providing local time, this will show the current offset from UTC of the receiver's time.

Is Local Time: Indicates if the time provided by the receiver is the local time (not UTC).

Is Daylight Saving Time: This indicates if Daylight Saving Time is currently active, assuming that the receiver is providing local time. If the receiver is providing UTC time, this will of course show *No*.

Positive Leap Second Announced: This indicates if the upstream time source has provided the receiver with an announcement of an imminent positive leap second (61 seconds in last minute of day).

Negative Leap Second Announced: This indicates if the upstream time source has provided the receiver with an announcement of an imminent negative leap second (59 seconds in last minute of day).

GPS Week Number: This is the current GPS week number; this scale runs from the time the GPS system first entered service.

GPS Week Second: This is the current second in the current GPS week as of the last page refresh.

Antenna

The **Antenna** panel provides information on the connection between the clock module and the antenna.

Is Connected: Indicates if a connection with the antenna has been detected. Specifically, it establishes if a closed DC circuit is established with the antenna via the coaxial cable.

Has Short Circuit: Indicates if the clock module has detected a short circuit in the connection with the antenna (i.e., short from core to outer conductor of the coaxial cable).

Satellites

This **Satellites** panel provides information on the satellites found by the integrated GNSS receiver.

Operation Mode: This indicates the satellite lock status of the receiver. If this shows "*NORMAL OPERATION*", the receiver is locked into at least four satellites and is therefore able to establish its own geographical position. If this shows "*WARM BOOT*", it has not (yet) located enough satellites for geolocation, but is relying on existing almanac data to locate previously detected satellites. If "*COLD BOOT*" is displayed here, the receiver has not located enough satellites and does not have almanac data to refer to, which means that a GPS lock will take much longer to establish.

Total Used: This is the total number of satellites currently in use by the receiver for synchronization.

Total In View: This is the total of number of satellites currently detected by the receiver.

Position

The **Position** panel provides detailed information about detected geographical position of the antenna. The **Brief Information** shows the geographical coordinates in decimal degrees and the altitude above sea level in meters. The **Latitude** and **Longitude** panels can be expanded accordingly to obtain more precise geolocation information.

Oscillator

The **Oscillator** panel provides calibration information on the receiver's internal oscillator, specifically the coarse and fine calibration values of the digital-to-analog converter (DAC).

8.5.7 State - Users

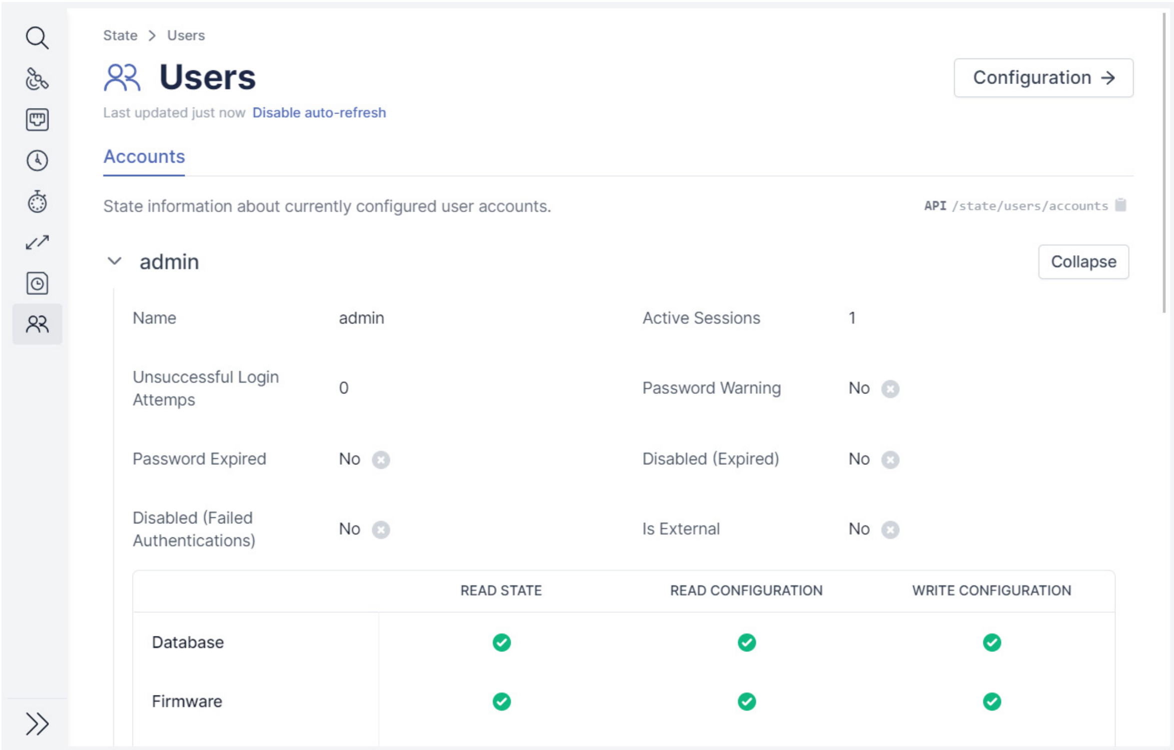


Figure 8.44: meinbergOS Web Interface: "State → Users" Subsection

The "**State** → **Users**" subsection (Fig. 8.44) provides a summary of all users currently configured on the system. Click on the user name or the "**Expand**" or "**Collapse**" buttons to expand or collapse the panel for that user account accordingly.

Name: The name used to log into the meinbergOS device.

Active Sessions: The number of sessions currently using the account as a login. If **Allow Multiple Sessions** is disabled under "**Configuration** → **Users**" this should never be more than *1*.

Unsuccessful Login Attempts: The number of failed attempts to log in using this account.

Password Warning: If *Yes*, a warning of the need to change the password has been issued.

Password Expired: If *Yes*, the password for this account has expired.

Disabled (Expired): This will show *Yes* if the account has been disabled due to the expiry of the password.

Disabled (Failed Authentications): This will show *Yes* if the account has been disabled due to the number of failed login attempts exceeding the defined limit.

Is External: If the meinbergOS device is only able/configured to use local user profile information, this will display *No*. If the meinbergOS device supports and is configured for an external directory service (such as LDAP), this will show *Yes*.

User Permissions

The permissions listed here show the permissions assigned to the user to view and/or modify various aspects of the meinbergOS device's configuration. **Read State** refers to the ability to view the corresponding status information in the **State** section. **Read Configuration** refers to the ability to view the corresponding configuration in the **Configuration** section. **Write Configuration** refers to the ability to view and modify the corresponding configuration subsection in the **Configuration** section.

Please note that to view this user status subsection in the first place, the user must be configured to have **Read State** access to **Users**.

Please refer to the chapter "**Configuration - Users**" for more information.

8.6 Maintenance

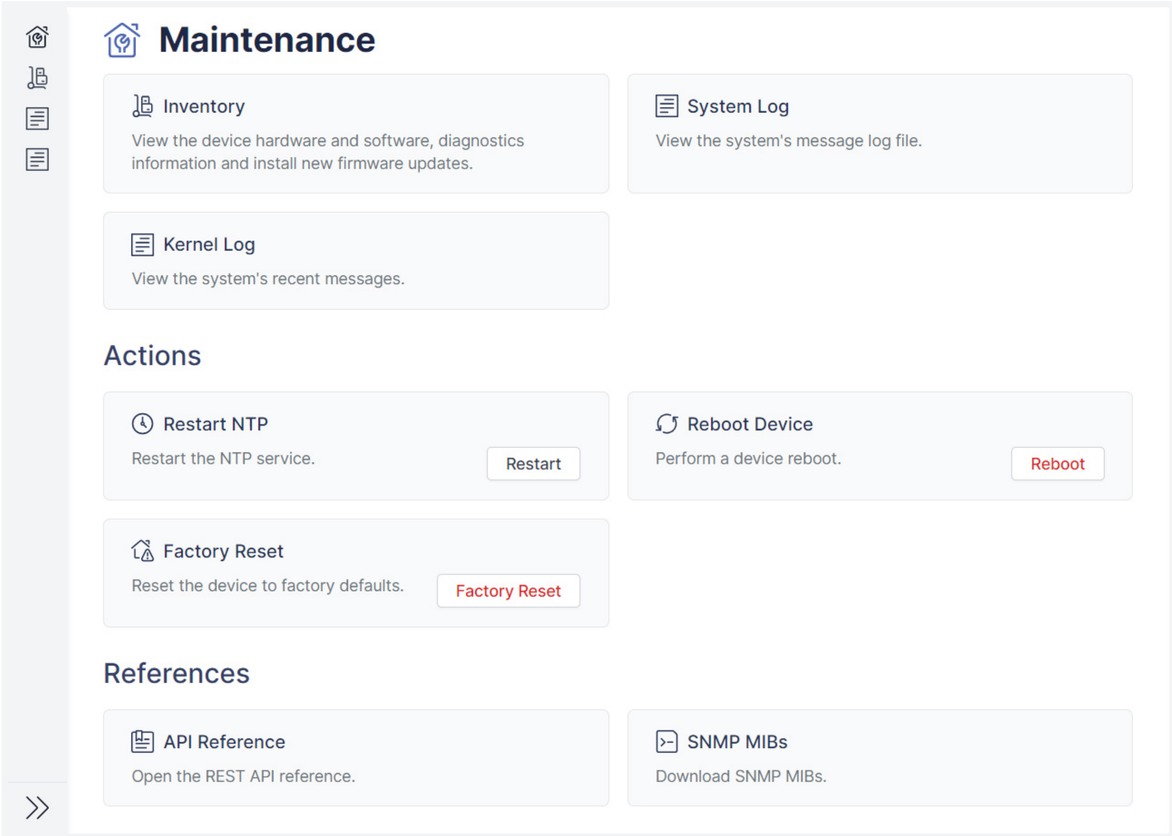


Figure 8.45: meinbergOS Web Interface: "Maintenance" Section

The **Maintenance** section (Fig. 8.45) hosts general system-related monitoring, diagnostic, logging, and management functions that are not directly related to your meinbergOS device's function as a timekeeping or clock management system and are, as the name suggests, purely related to the maintenance and care of your system.

8.6.1 Maintenance - Inventory

The "**Maintenance → Inventory**" subsection provides general information about the hardware of the meinbergOS device, the option to download a diagnostics file for support purposes, and information about the installed firmware, along with the ability to install new firmware versions or re-enable past versions of installed firmware.

8.6.1.1 Maintenance - Inventory - Overview

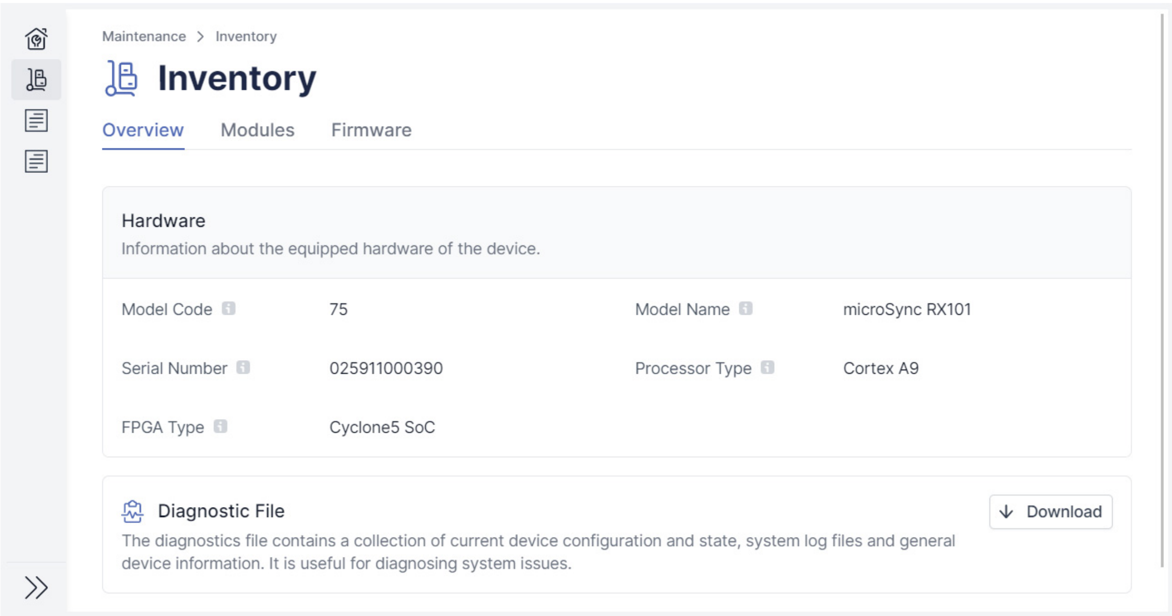


Figure 8.46: meinbergOS Web Interface: "Maintenance → Inventory → Overview" Tab

Hardware

Information about the hardware underlying your meinbergOS device.

Model Code: The specific product identifier for this meinbergOS device. This relates specifically to the **Model Name** below.

Model Name: The brand name of this meinbergOS device under which it is marketed.

Serial Number: The unique serial number of the device. This information is relevant when contacting Meinberg for support or downloads.

Processor Type: The type of central processing unit (CPU) in the device.

FPGA Type: The type of field-programmable gate array (FPGA) in the device.

Diagnostics File

This option allows you to download a diagnostics file containing a collection of files providing up-to-date device configuration and status information, system log files, and general device information that is often useful for diagnosing system issues. The diagnostics file is provided as a *.tar.gz* archive.

When contacting Meinberg Technical Support for assistance with your meinbergOS device, you may be prompted to download and send this archive for further analysis.

8.6.1.2 Maintenance - Inventory - Modules

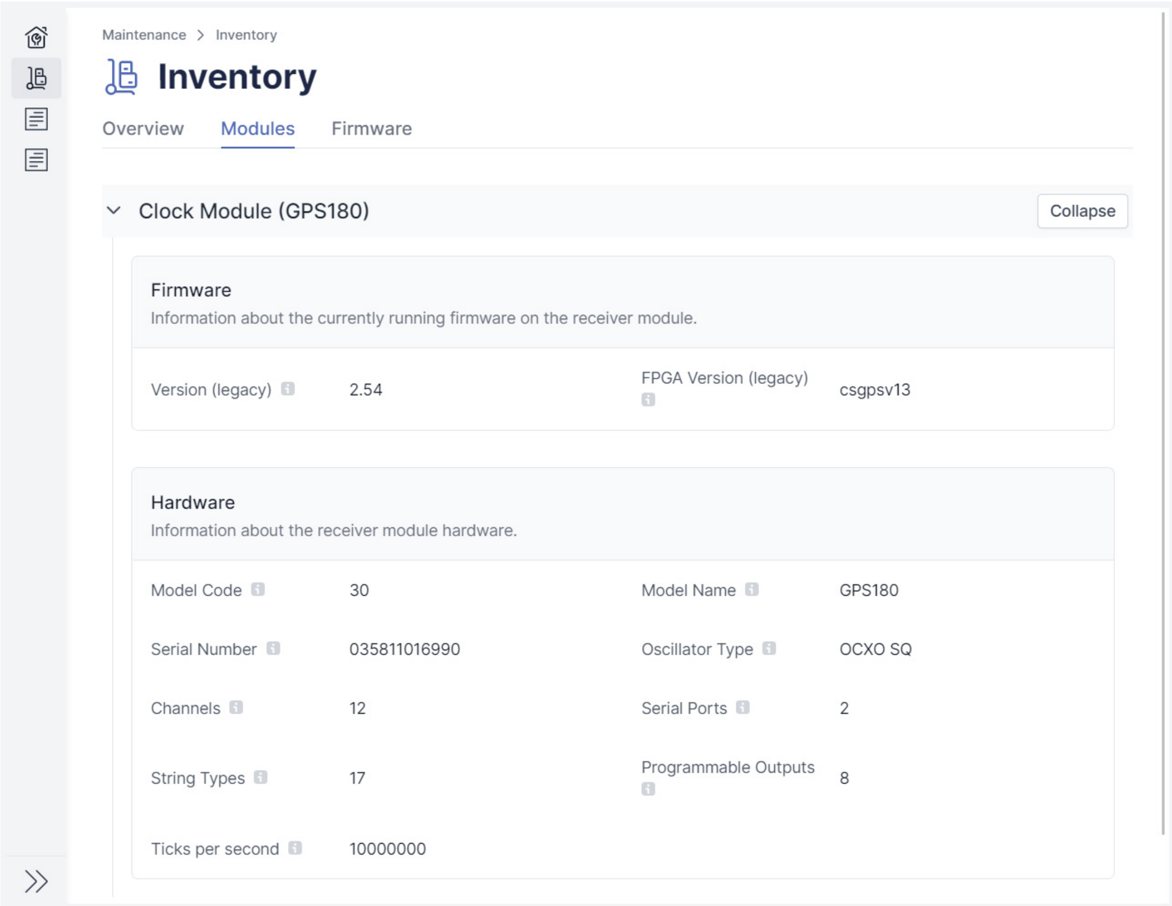


Figure 8.47: meinbergOS Web Interface: "Maintenance → Inventory → Modules" Tab

This tab provides information about the hardware and firmware of the modules integrated into your meinbergOS device, specifically the clock module and any other I/O modules that your device may feature.

Clock Module

Information on the receiver module integrated in the meinbergOS device.

Firmware

Version (Legacy): This is the version number of the clock module firmware.

FPGA Version (Legacy): This is the version number of the integrated FPGA.

Hardware

Model Code: The manufacturer's product model code for the clock module.

Model Name: The product name assigned by the manufacturer for the clock module.

Serial Number: The serial number of the clock module.

Oscillator Type: The type of oscillator integrated into the clock module.

Channels: This value specifies how many satellites the clock module is capable of tracking simultaneously.

Serial Ports: Number of serial interfaces provided by the internal clock module.

String Types: Number of string types supported by the clock module and outputtable through the serial port.

Programmable Outputs: Number of programmable outputs provided by the device.

Ticks per Second: The maximum timing resolution supported by the clock module.

IO Modules

Information on any I/O modules integrated into the meinbergOS device.

Firmware

Version (Legacy): This is the version number of the I/O module firmware.

FPGA Version (Legacy): This is the version number of the integrated FPGA.

Hardware

Model Code: The manufacturer's product model code for the I/O module.

Model Name: The product name assigned by the manufacturer for the I/O module.

String Types: Number of string types supported by the I/O module and outputtable through the serial port.

Ticks per Second: The maximum timing resolution supported by the I/O module.

8.6.1.3 Maintenance - Inventory - Firmware

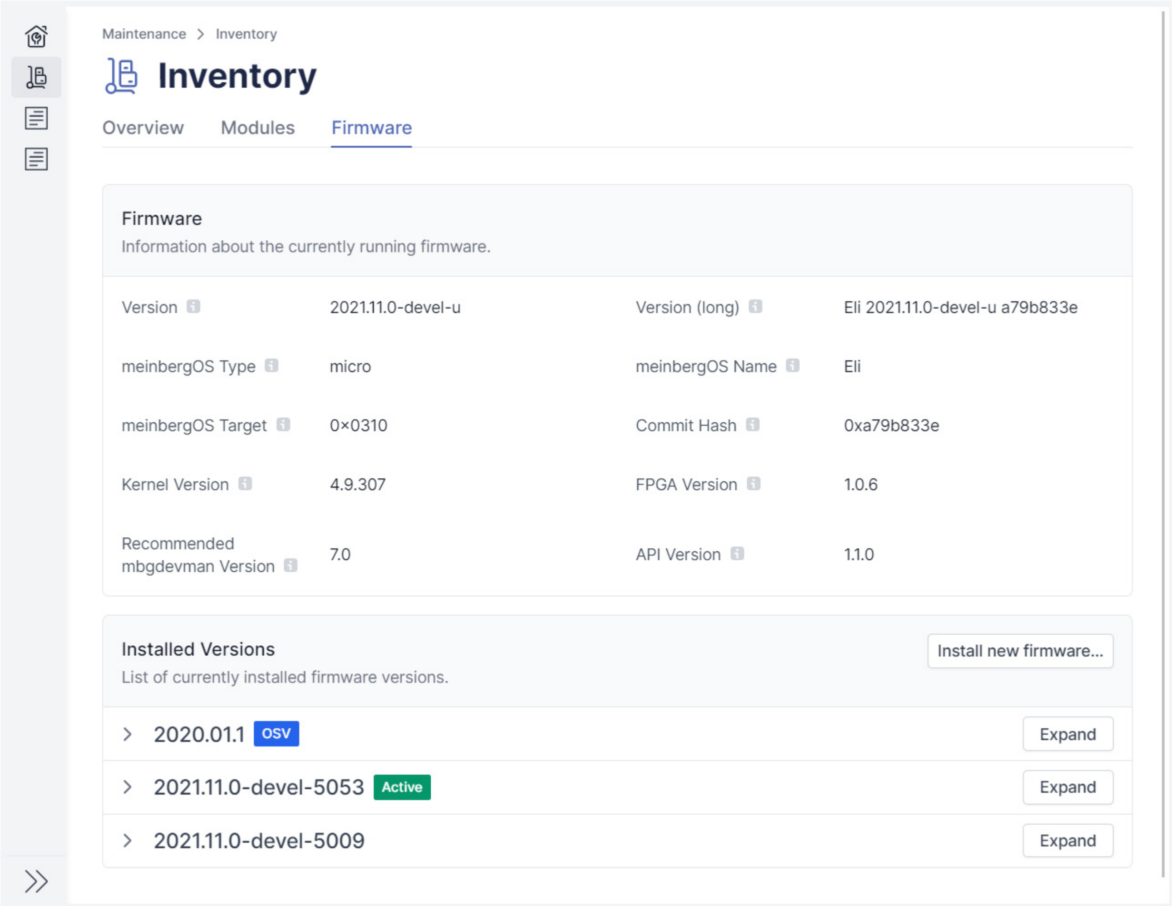


Figure 8.48: meinbergOS Web Interface: "Maintenance → Inventory → Firmware" Tab

This tab (Fig. 8.48) provides information on the currently installed and activated firmware version, as well as any other installed versions that are not active. It also provides the ability to install a new firmware version, to re-activate a previously installed and disabled version, and to remove old versions that are no longer needed.

Firmware

This provides information on the currently activated firmware.

Version: The firmware version number that is currently activated and running.

meinbergOS Type: The type of meinbergOS build that is currently running on this device.

meinbergOS Name: The code name of the meinbergOS main version that is currently activated and running.

Kernel Version: meinbergOS is based on the Linux Kernel, and this is the version of the Linux Kernel currently installed. Please note that the Linux Kernel is updated concurrently with firmware updates; it cannot be updated individually.

FPGA Version: The version of the FPGA firmware currently running.

Recommended mbgdevman Version: The version of Meinberg Device Manager that is recommended for the configuration and monitoring of this device. Meinberg Device Manager is a freely available tool designed to facilitate the management of multiple Meinberg devices in a single network. Please visit **http://www.mbg.link/mbgdevman** for more information.

API Version: The version of the RESTful API used in the currently activated firmware.

Installed Versions

This is the list of currently installed firmware versions. The version that is marked with a green **Active** tag is the firmware version that is currently activated on your meinbergOS device. The version that is marked with a blue **OSV** tag is the firmware version that your meinbergOS device was originally shipped with.

The following information is provided for each firmware version installed:

Version: The version number of this firmware.

Build Number: The Build Number of this firmware version. This is a development-specific value that you may be prompted to provide when contacting Meinberg Technical Support.

Build Date: The date and time of this build of the firmware version.

Is OSV: If this firmware version is the version that the meinbergOS device shipped with, this will show *Yes*. To ensure that your system always has a stable build to fall back to in the event of problems, this version cannot be erased from your system.

Is Active: If this is the currently activated version of meinbergOS, this will show *Yes*.

Is Erasable: If this firmware version can be erased, this will show *Yes*. Any firmware can generally be erased if it is not the OSV and not the currently activated version.

Is Mutable: If individual files within this firmware version (i.e., module firmware updates) can be updated, added, deleted, etc. this will show *Yes*.

Module Updates: This shows which individual module firmware updates are included in this firmware version (e.g., clock receiver), specifically the name of the module and the firmware version.

8.6.1.4 Guide: Installing a New Firmware Version

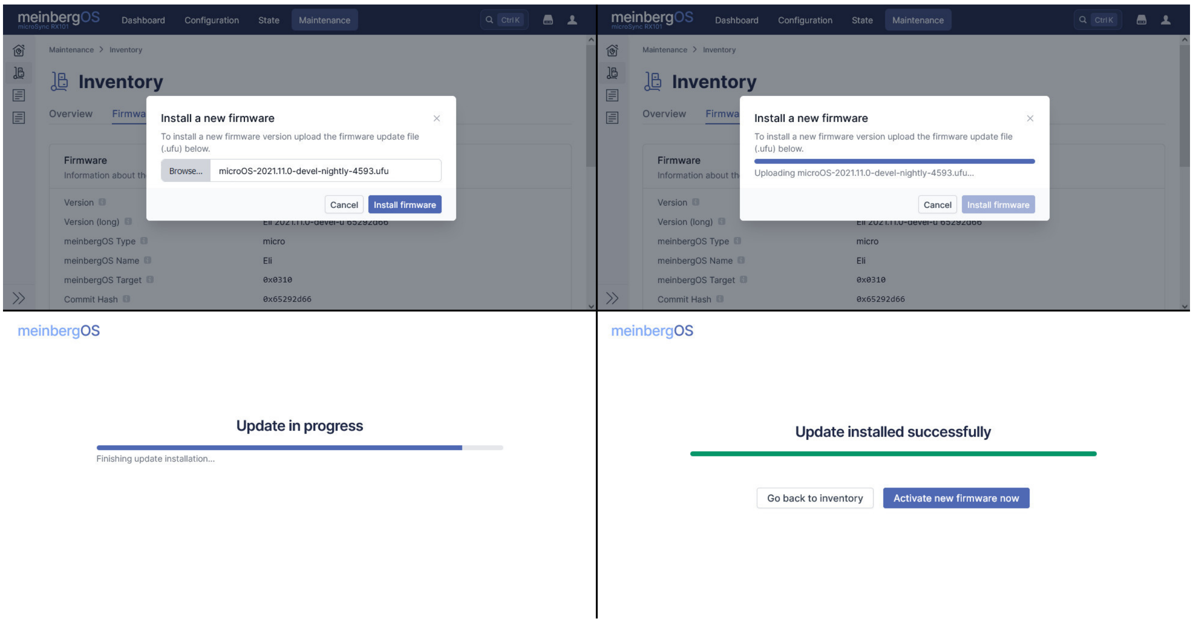


Figure 8.49: meinbergOS Web Interface: Installing a New Firmware Version

Information:

Before activating another version of meinbergOS, remember to save any configuration changes as the Startup Configuration if you wish to keep them; any unsaved changes will be lost.

You may have a maximum of five meinbergOS versions installed at any one time.

Firmware updates are provided by Meinberg for your meinbergOS device in the form of files with a *.ufu* extension. If you wish, you may install a meinbergOS firmware update by clicking on the **Install New Firmware...** button at the top right of the **Installed Versions** panel (Fig. 8.48). You will then be prompted to select the *.ufu* firmware update file; click on **Browse...** in the dialog box that appears (Fig. 8.49, top left) and select the file using the file browser. Confirm that the correct file name appears in the corresponding field, then click on the blue **Install Firmware** button to proceed (Fig. 8.49, top right).

The installation process will take a brief moment (Fig. 8.49, bottom left) . Once completed, you will be informed that the update has been successfully installed and can now select whether you wish to activate this new firmware or return to the Firmware Inventory for now (Fig. 8.49, bottom right).

Please note that it can take a few moments to activate the newly installed firmware because the system needs to be rebooted for this purpose. As soon as the system is available again, your browser should automatically load the login page. If the login page does not appear after two minutes, try and force a reload by refreshing your browser.

8.6.1.5 Guide: Removing a Firmware Version from the Inventory

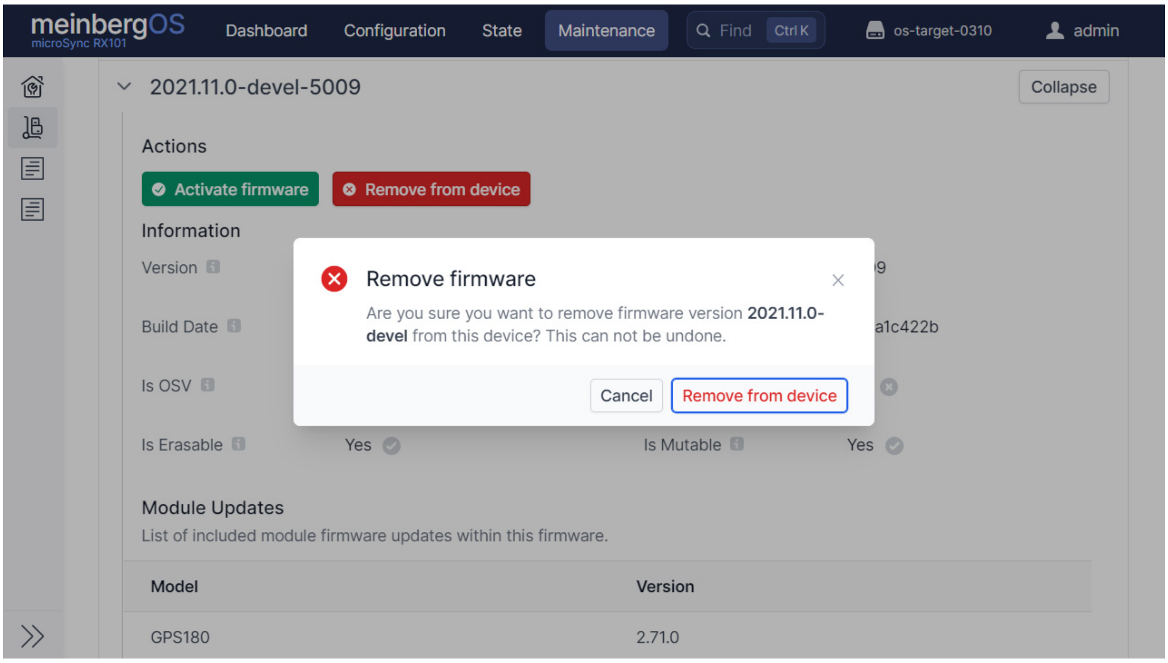


Figure 8.50: meinbergOS Web Interface: Removing a Firmware Version

If you wish to remove an old firmware version from your inventory, you can do so by clicking on the red **Remove from Device** button under the corresponding firmware version in the list. Please note that this process is permanent and cannot be undone; if you do not have the corresponding *.ufu* firmware update file stored elsewhere, you will not be able to recover this version again.

It is not possible to remove the Original Shipped Version (OSV) or the currently active version of the firmware; the **Remove from Device** button will therefore be grayed out for that version of the firmware.

8.6.1.6 Guide: Activating an Installed Firmware Version

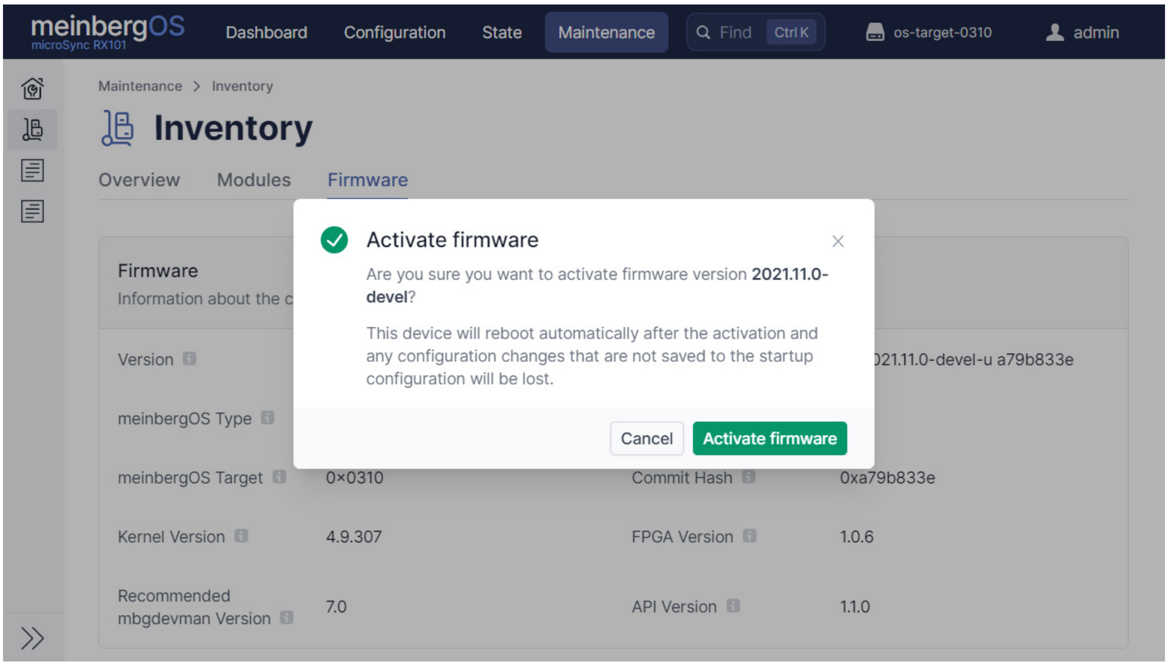


Figure 8.51: meinbergOS Web Interface: Activating a Firmware Version

If you wish to activate a different firmware version that is already installed on your system, you can do so by clicking on the firmware version in the list to open it, then clicking on the green **Activate Firmware** button underneath the relevant firmware version (Fig. 8.51). The system will then advise you that it will need to reboot in order to apply the firmware version and that any configuration changes will be lost if they are not saved as the Startup Configuration.

Information:

Activating an older version of meinbergOS in which newer features are missing will cause the configuration for those features to be lost as soon as a new configuration is saved under that older meinbergOS version.

Important!

Older versions of meinbergOS prior to *2022.05.1* did not feature a Web Interface and were only accessible using Meinberg Device Manager or over SSH/Telnet. Activating a version of meinbergOS older than *2022.05.1* that pre-dates the introduction of the Web Interface will cause you to lose access to the Web Interface. In this case, you will need to reactivate or reinstall a newer version of meinbergOS using Meinberg Device Manager to regain access to the Web Interface.

Visit **https://mbg.link/mbgdevman** for more information.

8.6.2 Maintenance - System Log

Figure 8.52: meinbergOS Web Interface: System Log

The "**Maintenance → System Log**" subsection (Fig. 8.52) provides access to the device's system log, which provides information such as past logins (both successful and failed), file system access, and cryptographic processes. This information can be useful for security and other analyses, and when contacting Meinberg Technical Support, you may be prompted to provide a copy of it.

Information:

The user must have the **Shell** channel permission to be able to read the System Log. Refer to the chapter "Configuration - Users" for further information.

8.6.3 Maintenance - Kernel Log

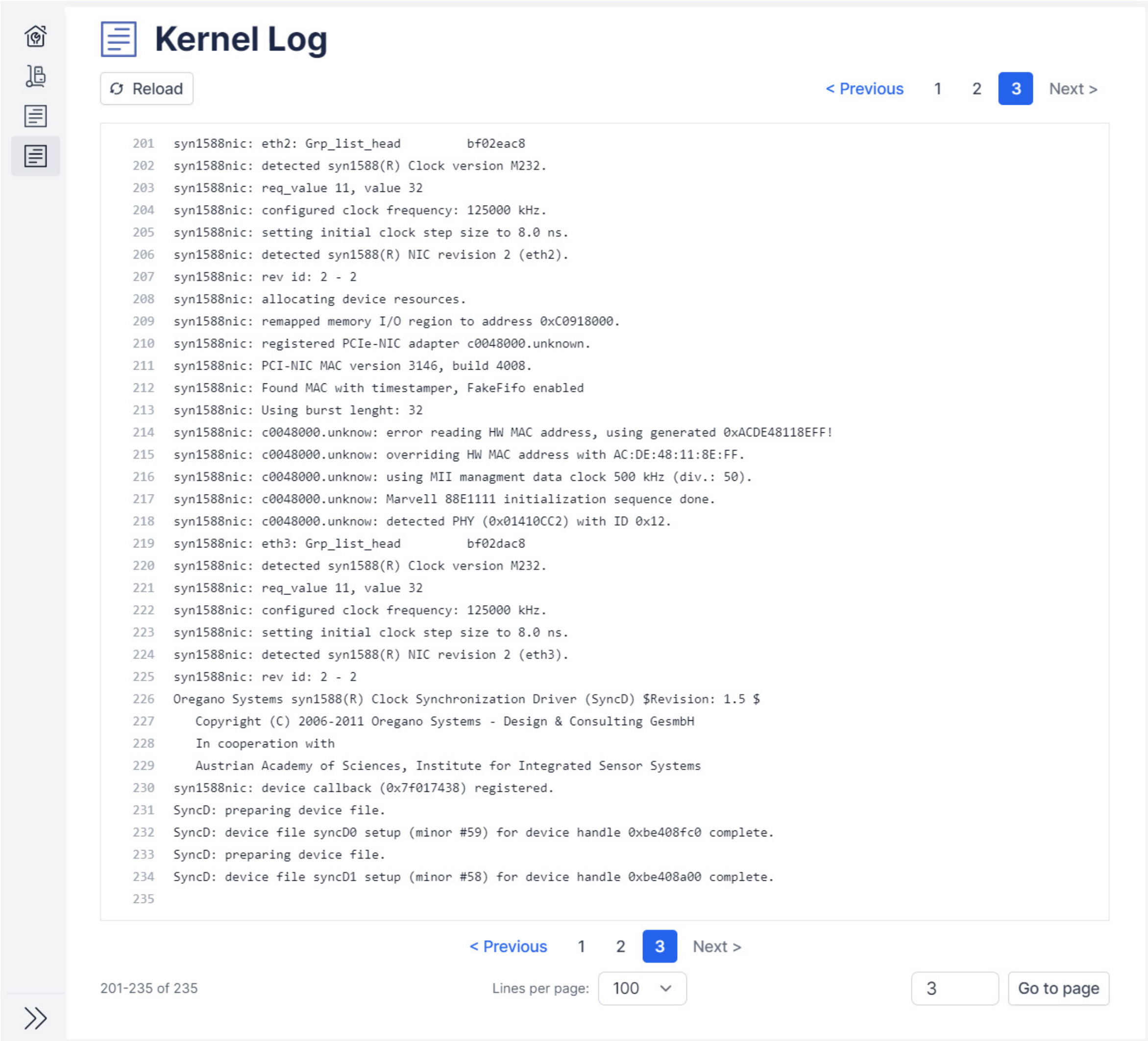


Figure 8.53: meinbergOS Web Interface: Kernel Log

The "**Maintenance** → **Kernel Log**" (Fig. 8.53) subsection provides access to the device's Linux Kernel log, which mainly provides hardware-related information. This information can be useful for system diagnosis, and you may be prompted to provide a copy of it when contacting Meinberg Technical Support.

Information:

The user must have the **Shell** channel permission to be able to read the Kernel Log. Refer to the chapter "Configuration - Users" for further information.

8.6.4 Maintenance - Restart NTP

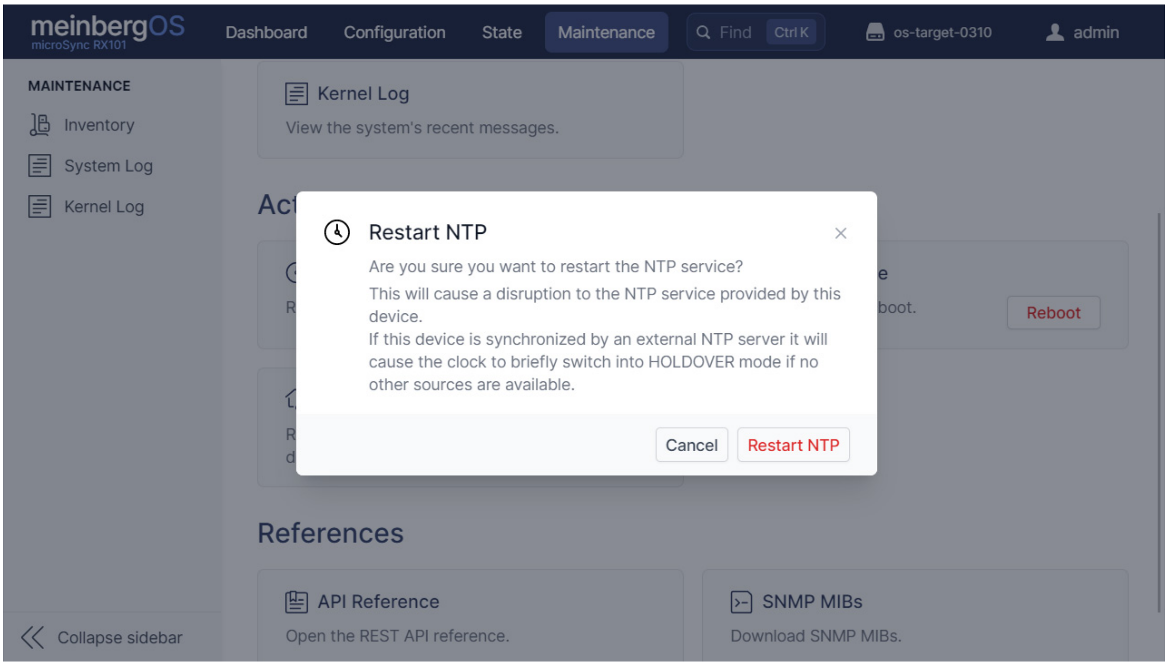


Figure 8.54: meinbergOS-Webinterface: Restart NTP-Service

If the meinbergOS device's NTP service is malfunctioning in any way and you do not wish to disrupt the other timekeeping or clock synchronization functionality, you may restart the internal NTP service individually using this button.

Information:

If the meinbergOS device is exclusively synchronized by an external NTP source, restarting the NTP service will briefly cause the clock module to switch to Holdover Mode until the NTP service is re-established.

8.6.5 Maintenance - Reboot Device

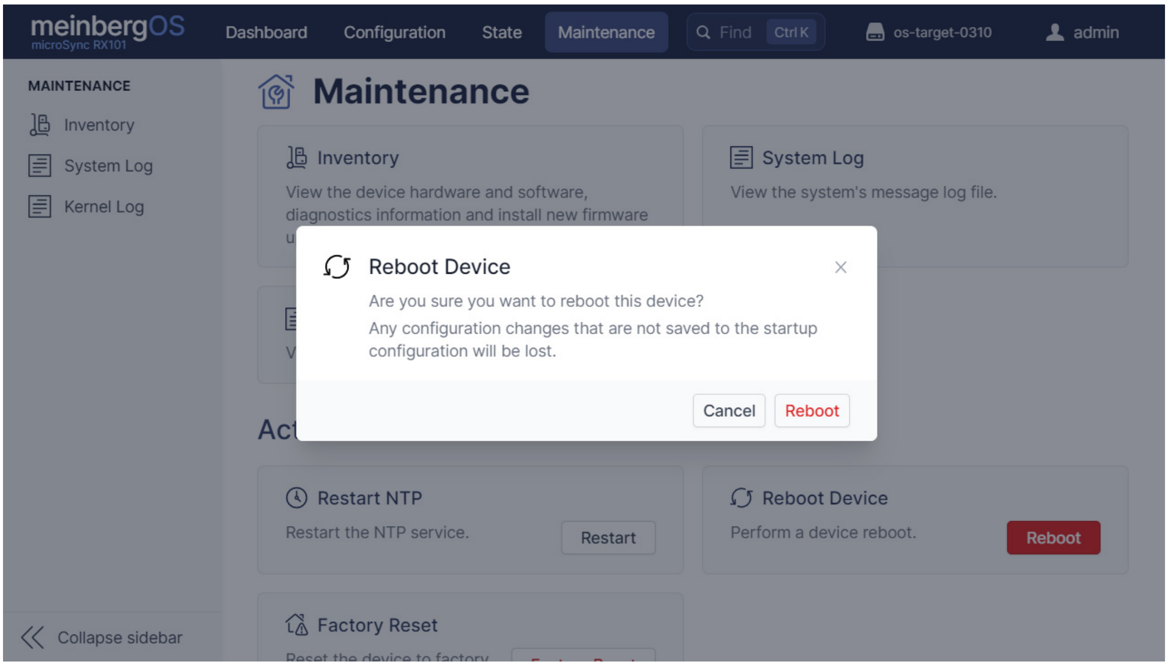


Figure 8.55: meinbergOS Web Interface: Reboot Device

The **Reboot Device** button can be used to restart the meinbergOS device as needed (Fig. 8.55). A reboot may help to resolve certain problems and can reset certain other states; for example, if a short-circuit has been detected in the antenna connection, the meinbergOS device will need to be rebooted once the cause of the short-circuit has been eliminated.

Information:

Changes to the current configuration will be lost upon rebooting the device unless they have been saved as the Startup Configuration.

8.6.6 Maintenance - Factory Reset

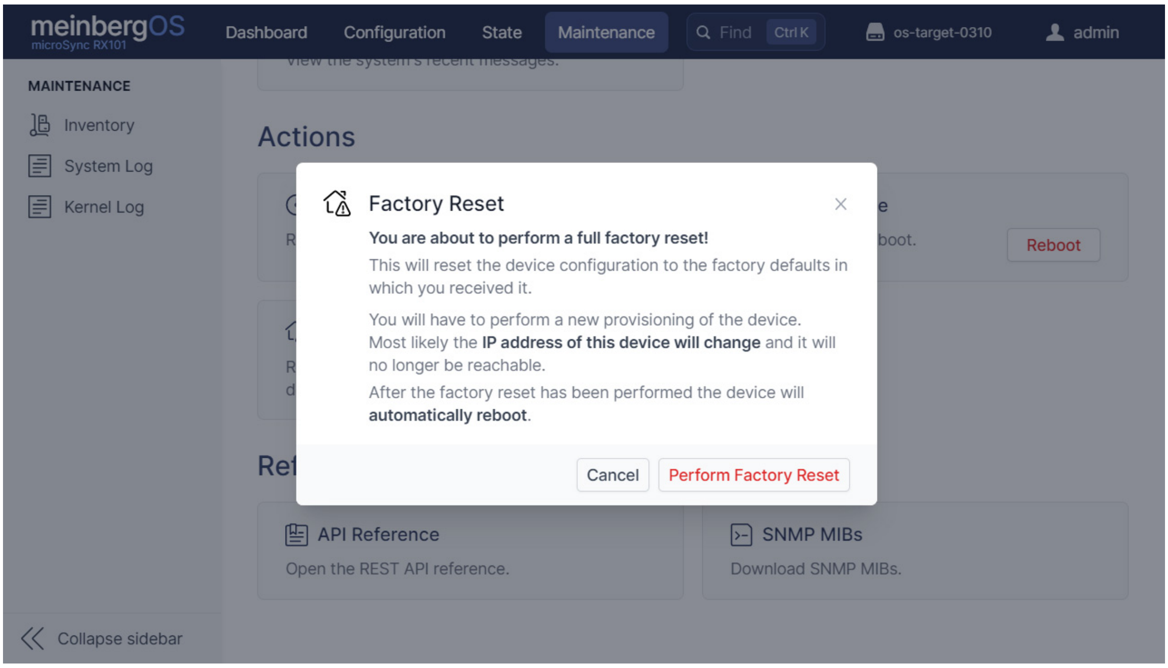


Figure 8.56: meinbergOS Web Interface: Factory Reset

This option will perform a full factory reset of the meinbergOS device and restore the configuration as it was at the time of shipping. This will cause the erasure of all data, namely the system configuration (including the Startup Configuration), almanac data, system and kernel logs. It will also delete all user profiles and reinstate the *admin* account with its default password *timeserver*.

After a factory reset, all installed firmware versions remain installed and the activated version remains activated. The **Factory Reset** function does **not** restore the activated firmware version to the Originally Shipped Version (OSV).

Important!

Depending on your network configuration, a factory reset may render your meinbergOS device inaccessible from the device from which you perform the factory reset. In this case, you may need to establish a direct wired connection with the meinbergOS device.

Please refer to the manual of your meinbergOS device for further information on re-configuring your meinbergOS device's network settings.

8.6.7 Maintenance - API Reference

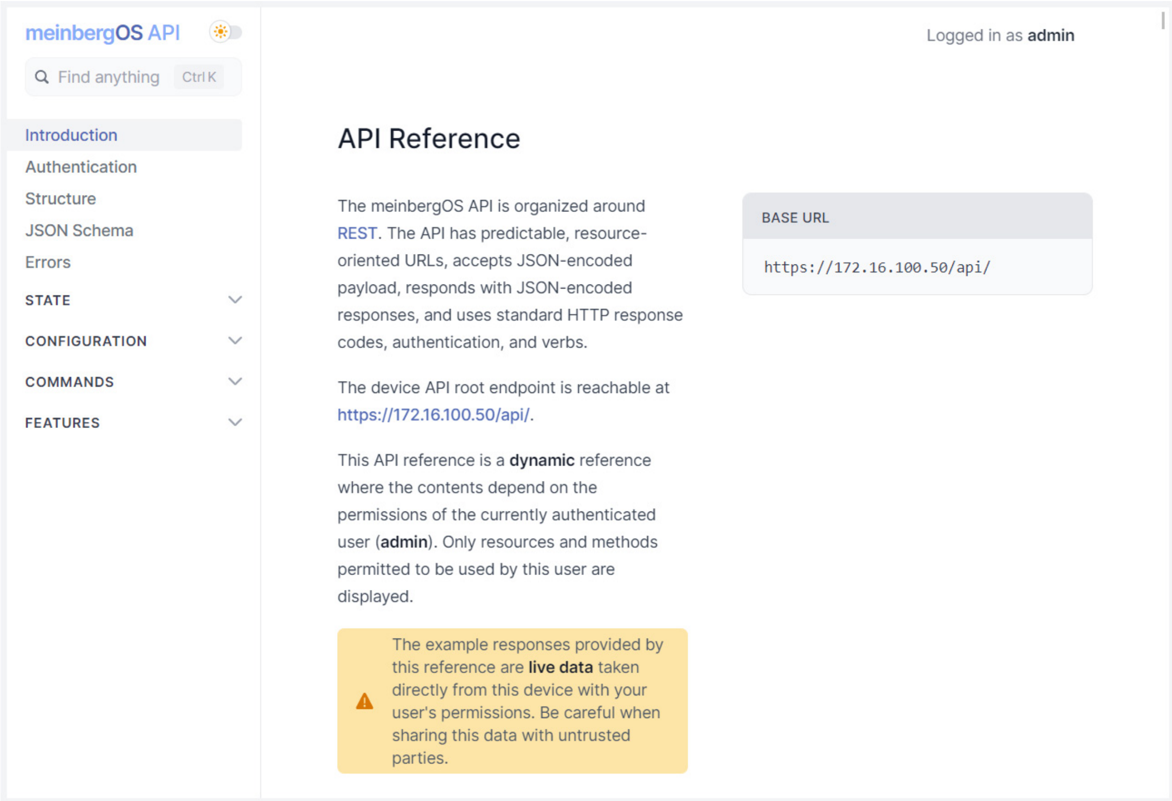


Figure 8.57: meinbergOS-Web Interface: API Reference

Selecting the **API Reference** button will open a reference guide that provides detailed information about the RESTful API that external applications can use to interact securely and logically with the meinbergOS device via *HTTPS*.

8.6.8 Maintenance - SNMP MIBs

This provides access to the Meinberg root and meinbergOS-specific MIB files (Management Information Base); these are downloadable directly from the meinbergOS device and define the network objects usable by a suitable SNMP management solution for the purpose of remotely monitoring the meinbergOS device.

9 Configuration and Monitoring with Meinberg Device Manager

Meinberg Device Manager: Management and Monitoring Software for Windows and Linux
The Meinberg Device Manager software is available for free download on the Meinberg homepage. You can download the software here:

https://www.meinbergglobal.com/english/sw/mbg-devman.htm

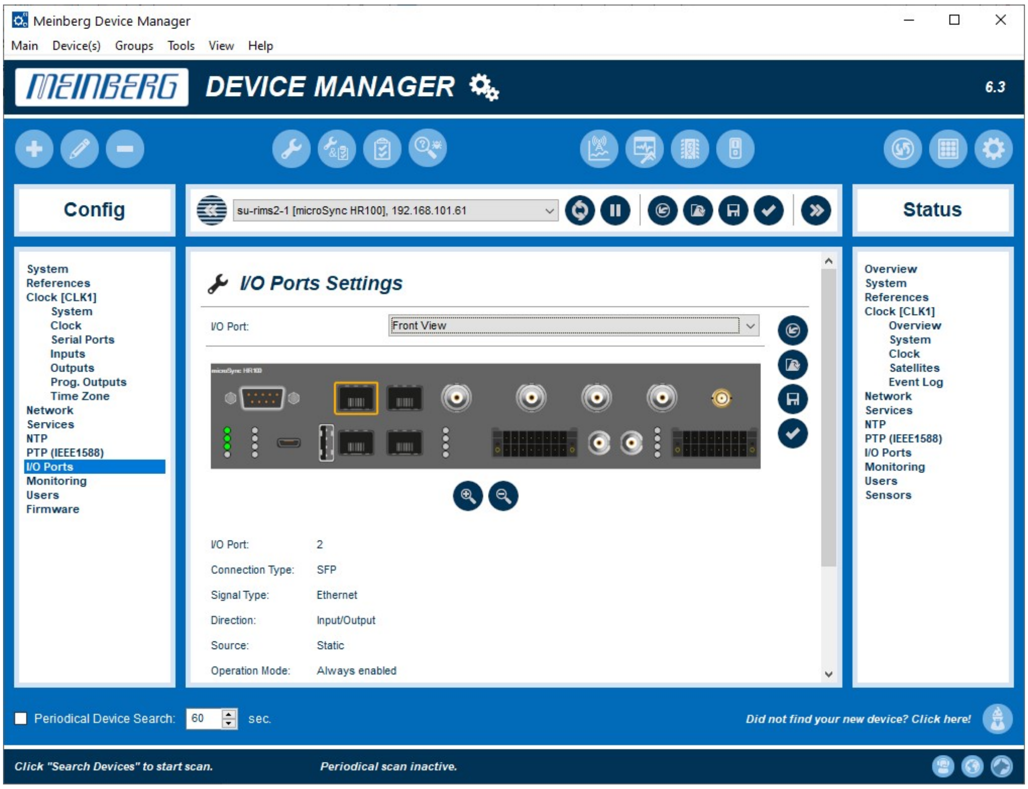


Figure: Meinberg Device Manager – input and output signals of a microSync^{HR} system

Documentation
For the documentation about configuration and system monitoring of microSync systems with the **Meinberg Device Manager** software a comprehensive manual is available on our website. You can download the document (PDF) here:

https://www.meinbergglobal.com/download/docs/manuals/english/meinberg-device-manager.pdf

9.1 Maintenance, Servicing and Repairing

9.1.1 Firmware Updates

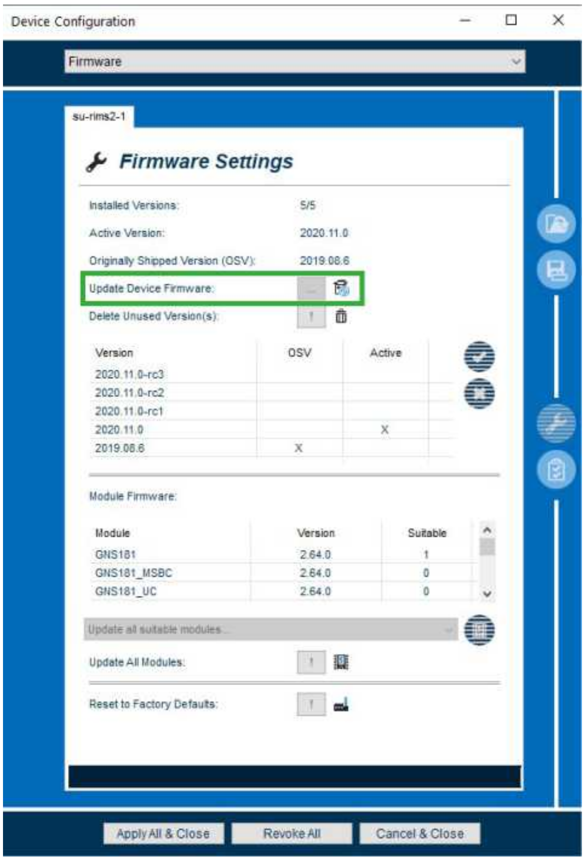
On our firmware download page under

https://www.meinbergglobal.com/english/sw/firmware.htm

you can download or request the latest meinbergOS updates free of charge. If you need an older version, you can request it from our support. Select the option "Specified Firmware-Version" and enter the version of the currently used firmware and the desired firmware version (e.g. meinbergOS 2019.08.5).

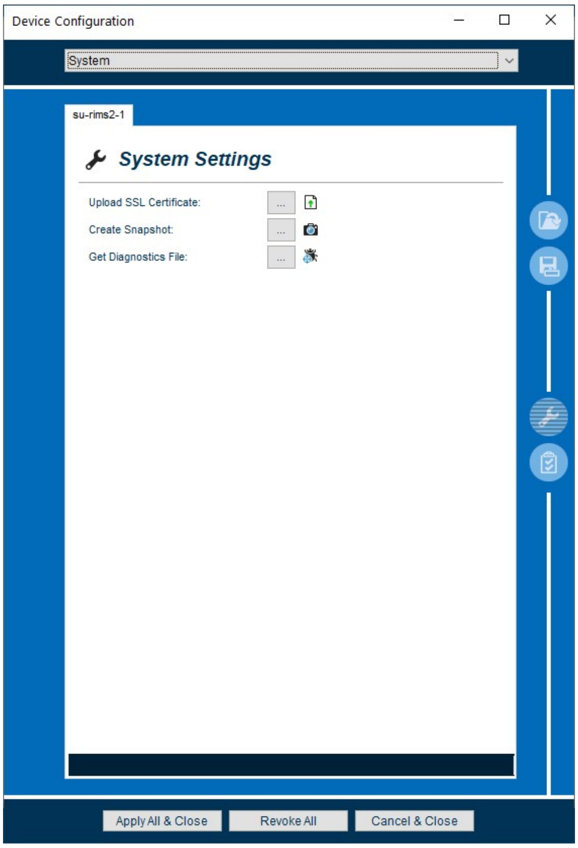
Note:
From firmware version 2022.05.1 onwards, a comprehensive Web-UI is available, via which you can also perform firmware updates. However, you still have to copy this version to your system with the Meinberg Device Manager software and activate it so that you can use the web interface.

This does not apply to systems that are delivered with meinbergOS version 2022.05.1 or later.



9.1.2 Troubleshooting and Alarming

If you encounter a problem with your microSync system, you can contact our technical support at any time. In order to be able to perform a quick and targeted diagnosis of your system, please provide us with a diagnostic file of the microSync system concerned. You can create this diagnostic file with the Meinberg Device Manager software. Select the menu "Configure Device(s) -> System Settings" and then use the button **Get Diagnostics File**. With the button "Create Snapshot" you can also create a text file with the current configuration. This file is also helpful for our employees in solving the problem.



If these files are too big to send by mail, you can also use our upload page:
https://www.meinbergglobal.com/upload/

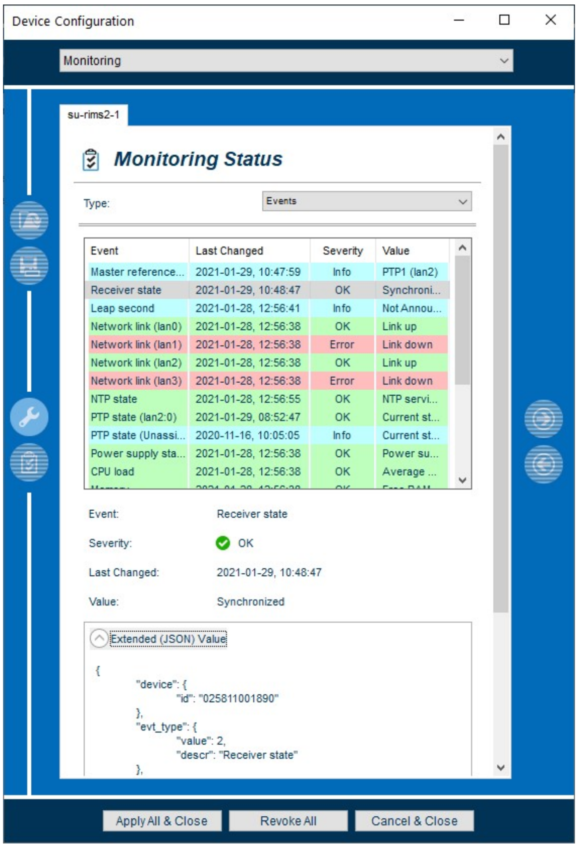
Please enter the serial number of your device again and, if already available, a support ticket number.

Otherwise there are a lot of tools available for self-help. Please also read the chapter Support Information.

9.1.2.1 System Error Messages

Event Log
In the menu "Show Device(s) Status → Clock → Event Log" you are able to display the last 20 events registered by the receiver. Here you can see the exact time and date when the event occurred. In addition, the severity of the event and the event type is displayed (e.g. Level = Error, Type = Warm Boot).

Monitoring Status
In the menu "Monitoring Status" you can read out further system messages with the time of the event and the severity. The individual events are highlighted in color using a tabular overview so that the severity can be recognized immediately (e.g. Network Link | Severity = Error | Descr. = Down | Color = red).



10 Support Information

In this chapter you will learn about different levels of support at the Meinberg Company. In general, the Basic Customer Support level is included in the price you pay for your Meinberg product and demands no additional costs. It includes free e-mail, phone support and free lifetime firmware updates for the lifetime of your product, i.e. for as long as you choose to use it.

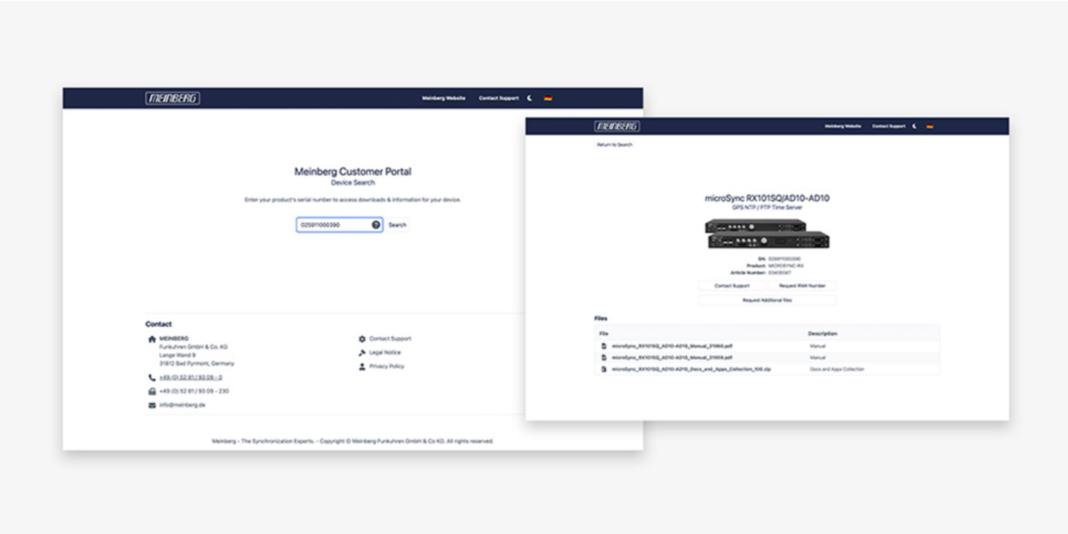
Depending on the product this level also includes a 3 year hardware warranty. You can extend the hardware warranty period after the standard warranty of your Meinberg product ends.

The chapter includes:

- The Meinberg Customer Portal
- Basic Customer Support
- Support Ticket System
- How to download a Diagnostic File
- Self-Help Online Tools
- NTP and IEEE 1588-PTP online tutorials.
- The Meinberg Academy introduction and offerings.
- Meinberg Newsletter
- How-To-Videos on our YouTube channel

10.1 Meinberg Customer Portal - Software and Documentation

End users of Meinberg products are provided with technical support, full documentation and software downloads through our Support Centre - all in one place: https://meinberg.support



No Registration required
There's no need to register; simply enter your product's serial number at https://www.meinberg.support and you'll have everything you need to get your Meinberg system up and running—or perhaps back up and running, as the case may be—with up-to-date installation and reference manuals, downloads for drivers, remote monitoring, configuration tools, and SNMP MIB files, direct links to contact Meinberg's Technical Support team, and the ability to easily request additional files.

The Meinberg Customer Portal vastly simplifies how you access support, software, and documentation, and ensures that you always have the latest versions of downloadable tools and manuals at your disposal.

10.2 Basic Customer Support

Contact Meinberg via e-mail or phone.

Technischer Support	
E-Mail	techsupport@meinberg.de
Service-Hotline	+49 (0) 5281 / 9309-888
Service-Zeiten	Mo. – Do. 8:00 – 17:00, Fr. 8:00 – 16:00 (MEZ/MESZ) Nicht erreichbar an Sa./So. und an gesetzl. Feiertagen

Büro (Vertrieb/Einkauf)	
E-Mail	info@meinberg.de
Service-Hotline	+49 (0) 5281 / 9309-888
Bürozeiten	Mo. – Do. 7:30 – 17:00, Fr. 07:30 – 15:00 (MEZ/MESZ) Nicht erreichbar an Sa./So. und an gesetzl. Feiertagen

MEINBERG Remote Support

In order to assist you with configuration, installation, monitoring and diagnostics of your Meinberg products, you can download a remote support software that allows Meinberg technical support to remote control your computer.

By following this link;

https://www.meinbergglobal.com/english/support/remote.htm

you can find all necessary information and to download the support.

Firmware Updates

To check if an update is available for your system, please visit;

https://www.meinbergglobal.com/english/sw/firmware.htm

Available firmware updates will be provided as downloadable package. On request we can also send you older firmware versions.

10.3 Support Ticket System

Meinberg assists you quickly and directly on questions regarding the initial setup of your devices, troubleshooting or if you want to update the hard- or software. We offer free support for the whole lifetime of your Meinberg product.

- You can request a support ticket online: https://www.meinbergglobal.com/english/support/tech-support.htm. Choose either the option **Support Ticket Request** or **Advanced Customer Support** if you have purchased an ACS contract from us and wish to use this service.
- Or send a mail to techsupport@meinberg.de with a description of your issue. A support ticket will automatically be opened. Our support engineers will contact you as soon as possible. It is always helpful for our engineers to receive a diagnostic file when you send a ticket. The diagnostic file includes all status data of a microSync system logged since the last reboot and can be downloaded from all microSync devices. The file format of the diagnostic file is a tar.gz archive (also see chapter How to download a Diagnostic File how to generate this file on your system.

10.4 How to download a Diagnostic File

In most support cases the first action is to ask the customer to download the diagnostic file, because it is very helpful at identifying the current state of your microSync System and finding possible errors. Therefore we recommend that you attach your Diagnostic File when sending a ticket request to our support department.

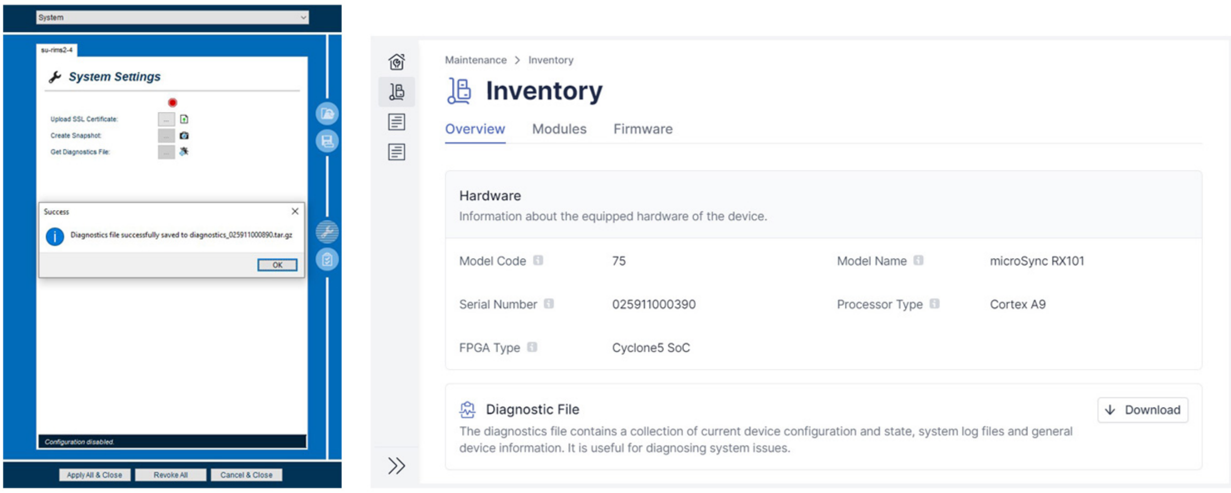


Figure: Download of the diagnostic file via the Meinberg Device Manager menu "System" and via the web interface under "Maintenance → Inventory".

The diagnostic file includes all status data of a microSync system logged since the last reboot. This file can be downloaded from all microSync devices by using the Meinberg Device Manager software or, from firmware version 2022.05.1, also via the meinbergOS Web-UI. The file format of the diagnostic file is a tar.gz. archive. The archive contains all the important configuration and logfiles in Text and JSON format.

10.5 Self-Help Online Tools

Here is the list of some informative websites where you can query different information about the Meinberg Systems.

1. Meinberg Customer Portal - Documentation, software, driver, product pictures and many more:
https://www.meinberg.support/

2. Meinberg Homepage - general:
https://www.meinbergglobal.com/

3. NTP Download:
https://www.meinbergglobal.com/english/sw/ntp.htm

4. NTP Time Server Monitor:
https://www.meinbergglobal.com/english/sw/ntp-server-monitor.htm

5. microSync firmware update request online form:
https://www.meinbergglobal.com/english/sw/firmware.htm

6. Download page for Meinberg drivers and software:
https://www.meinbergglobal.com/english/sw/

7. All Meinberg manuals (english and german language):
https://www.meinbergglobal.com/english/docs/

8. Meinberg Newsletter and subscription page:
https://www.meinbergglobal.com/english/company/news.htm

9. NTP / IEEE 1588-PTP online tutorials from Meinberg:
http://blog.meinbergglobal.com/

10. Meinberg Knowledgebase:
https://kb.meinbergglobal.com/

11. FAQs about Meinberg products:
https://www.meinbergglobal.com/english/faq/

12. Selection of the Meinberg whitepapers:
https://www.meinbergglobal.com/english/info/#whitepaper

13. GPS / GNSS Antenna Installation and mounting:
https://www.meinbergglobal.com/english/info/gps-antenna-mount.htm

14. NTP support page and documentation:
http://support.ntp.org/bin/view/Support/WebHome

10.6 NTP and IEEE 1588-PTP online tutorials

A team of Meinberg engineers are writing online tutorials covering topics on IEEE 1588 PTP, NTP, synchronization setups and configurations used in different industries.

The tutorials can be found at: https://blog.meinbergglobal.com/

The blog provides you also the opportunity to write a comment or a question to our experts and get their reply.

Categories: Configuration Guidelines, IEEE 1588, Industry Applications, NTP and Security.

10.7 The Meinberg Academy Introduction and Offerings

Meinberg Sync Academy (MSA) is an institution within the Meinberg Company which takes care for education and expert knowledge dissemination in the field of time and frequency synchronization. The academy offers tutorials and courses on the latest synchronization technologies such as NTP, IEEE 1588-PTP, synchronization networks for different industries: telecom, power, broadcasting, professional audio/video, finance, IT and Enterprise Networks. The MSA courses include both, theoretical lectures and practical hands-on labs.

If you are planning or re-designing synchronization for your networks and you need additional knowledge, see our agenda for the upcoming courses.

Courses:	MBG Product Training, NTP Complete, PTP Complete Customized Trainings, Online Trainings and Course Calendar.
Contact Phone:	+49 (0) 5281 93093-0
E-Mail:	info@meinberg.de
Internet:	https://www.meinbergglobal.com/english/support/meinberg-sync-academy.htm

10.8 Meinberg Newsletter

Meinberg publishes regularly up-to-date information, technical news, firmware updates and security advisory by the Meinberg Newsletter in both the English and German language.
Subscribe to the newsletter here:

https://www.meinbergglobal.com/english/contact/newslett.htm

10.9 How-to Videos on our YouTube Channel

We provide you with some useful videos on our YouTube channel (https://www.youtube.com/c/meinberg). For our microSync systems you can find two videos here, which show you the initial installation via serial interface and network.

Configuration via the serial Interface (USB)
https://youtu.be/NzCo5ia8QYE

Configuration with the Meinberg Device Manager Software
https://youtu.be/drEN7Psw88o

11 Technical Appendix

11.1 meinbergOS Software Specifications

Network Protocols:	IPv4, IPv6 NTPv3, NTPv4 PTPv2 IEC 62439-3 (PRP) DHCP, DHCPv6 DSCP IEEE 802.1q VLAN filtering/tagging IEEE 802.1p QOS SNMPv1/v2/v3 Remote Syslog Support (UDP)
PTP Profiles:	IEEE 1588v2 Default Profile IEEE C.37.238-2011 Power Profile IEEE C.37.238-2017 Power Profile IEC/IEEE 61850-9-3 Power Utility Profile Enterprise Profile ITU-T G.8265.1, ITU-T G.8275.1, ITU-T G.8275.2 Telecom Profiles SMPTE ST 2059-2 Broadcast Profile IEEE 802.1AS TSN/AVB Profile AES67 Media Profile DOCSIS 3.1

11.2 Antenna and Receiver Information

There are 2 types of radio signals commonly used for timing applications: **satellite signals from Global Navigation Satellite Systems (GNSS)**, and **long wave signals** from specific time code transmitters operated by some countries.

Most GNSS signals can be received world-wide, while long wave signals can only be received up to a certain distance around the transmitting station. Also, GNSS receivers can usually track the signals from several satellites at the same time, so the signal propagation delay can be determined and compensated automatically, while long wave receivers usually receive only the signal from a single station. Last but not least the available bandwidths and signal propagation characteristics are another reason why GNSS reception usually yields a higher degree of time accuracy than long wave reception.

11.2.1 Reference Time Sources

11.2.1.1 Meinberg GPS Receiver

The satellite radio clock was developed with the aim of providing users with a highly accurate time and frequency reference. High accuracy and the possibility of worldwide use, 24 hours a day, are the main features of this system, which receives its time information from the satellites of the Global Positioning System. The Global Positioning System (GPS) is a satellite-based system for radio-positioning, navigation, and time-transfer.

This system has been installed by the United States Department of Defense (Defense Department) and provides two levels of accuracy: the Standard Positioning Services (SPS) and the Precise Positioning Services (PPS).

The structure of the sent data of the PLC has been released and the reception has been made available for general use, while the time and navigation data of the even more accurate PPS are transmitted encrypted and therefore only accessible to certain users (mostly military). The principle of location and time determination with the aid of a GPS receiver is based on the most possible accurate measurement of the signal propagation time from the individual satellites to the receiver.

The GPS satellites orbit the earth on six orbital tracks in 20,000 km of altitude once in about 12 hours. This ensures that at any time at least four satellites are in sight at any point on the earth. Four satellites must be received at the same time so that the receiver can determine its spatial position (x, y, z) and the deviation of its clock from the GPS system time.

Control stations on earth measure the orbits of the satellites and record the deviations of the atomic clocks carried on board from the GPS system time. The determined data are sent to the satellites and sent to earth as navigation data by the satellites. The highly precise track data of the satellites, called ephemerides, are needed so that the receiver can calculate the exact position of the satellites in space at any time. A set of track data with reduced accuracy is called almanac. With the aid of the almanacs, the receiver calculates at approximately known position and time, which of the satellites are visible from its location. Each of the satellites transmits its own ephemerides as well as the almanacs of all existing satellites. The GPS clock operates with the "Standard Positioning Service". The data stream of the satellites are decoded and evaluated by the microprocessor of the system, like that the GPS system time is reproduced with a deviation of less than 100 nsec.

Different running times of the signals from the satellites to the receiver are automatically compensated by determining the receiver position. By tracking the main oscillator, a frequency accuracy of 1e-12 is achieved, depending on the oscillator type. At the same time, the age-related drift is compensated. The current correction value of the oscillator is stored in a non-volatile memory of the system.

11.2.1.2 Meinberg GNSS Receiver (GPS, GLONASS, Galileo, BeiDou)

High accuracy and the possibility of the world wide operation around the clock are the main features of the system, which receive his time information from the satellites of the American GPS (Global Positioning System), the European Galileo, the Russian GLONASS (Global Navigation Satellite System) and the Chinese BeiDou.

The Global Positioning System (GPS) is a GNSS operated by the US department of defense. Its purpose is to provide position, velocity and time for civilian and defense users on a global basis. The system currently consists of 32 medium earth orbit satellites and several ground control stations.

GLONASS is a GNSS operated by Russian Federation department of defense. Its purpose is to provide position, velocity and time for civilian and defense users on a global basis. The system consists of 24 medium earth orbit satellites and ground control stations. The GLONASS satellites circle the earth once on three orbital lanes in height of 19100km in about 12 hours.

Galileo is a GNSS operated by the European Union. Its purpose is to provide position, velocity and time for civilian users on a global basis. The system is currently not fully operational. It is eventually expected to consist of 30 medium earth orbit satellites. At the time of writing (early 2016), the Galileo system was still under development with only a few fully operational SVs. Therefore, the precise performance and reliability of u-blox receivers when receiving Galileo signals is effectively impossible to guarantee.

BeiDou is a GNSS operated by China. Its purpose is to initially provide position, velocity and time for users in Asia. In a later stage when the system is fully deployed it will have worldwide coverage. The full system will consist of five geostationary, five inclined geosynchronous and 27 medium earth orbit satellites, as well as control, upload and monitoring stations.

Characteristics
The GNS module is a combined GPS / Galileo / GLONASS / BeiDou receiver and operates with the "Standard Positioning Service" (GPS) or "Standard Precision" (Galileo, GLONASS, BeiDou). The data stream from the satellites is decoded by the microprocessor of the system. By analyzing the data, the GNSS system time can be reproduced very precisely. Different running times of the signals from the satellites to the receiver are automatically compensated by determining the receiver position. By tracking the main oscillator (Oven Controlled Xtal Oscillator, OCXO) a high frequency accuracy is achieved. At the same time, the aging-induced drift of the quartz is compensated. The current correction value for the oscillator is stored in a non-volatile memory of the system. This receiver is suitable not only for stationary operation but also for mobile use.

11.2.1.3 Meinberg GNS-UC Receiver (GPS and Galileo)

microSync - GPS/Galileo based Time Synchronization for Stationary and Mobile Applications using Meinberg Antenna/Converter Technology

The microSync unit has a special receiver concept which is able to capture GPS and Galileo signals using a standard Meinberg antenna/converter unit. The configuration supports to select one of these to be used exclusively or the combination of the sources.

The receiver is capable of operating during high speed movement and delivers reliable and highly precise synchronization solutions in stationary installations and on fast moving vehicles, such as aircraft, ships or trucks.

The variety of inputs/outputs makes this receiver the first choice for a broad range of applications, including time and frequency synchronization tasks and the measurement of asynchronous time events.

The microSync with its integrated GNSS receiver provides accurate time with ultimate precision both in stationary and mobile environments by supporting long antenna cables because of the Meinberg antenna/converter technology.

Key Features

- RS-232 interface
- 10 MHz reference frequency output
- Pulses per second and per minute
- Up to 4 programmable pulse outputs
- Frequency Synthesizer

Description
The microSync offers satellite based time synchronization at the highest accuracy standards for fixed or mobile applications. It is suitable to be deployed in data centers or on board of cars, trucks, aircrafts, ships and other moving platforms. The satellite receiver can determine its position even at a maximum acceleration of up to 4 g, at a maximum speed of 500 m/s and at an altitude of up to 18,000 meters.

The microSync is used to manage high accurate timing and measurement tasks. The board is able to generate fixed and programmable standard frequencies with very high accuracy and stability. Various oscillator options allow to meet different requirements concerning the accurracy of the outputs in the most cost efficient way. The pulse generator of the GNS181-UC generates pulses per second and per minute. As an option four programmable outputs are available. The pulses are synchronized to the UTC second.

The module provides two inputs for measurement of asynchronous time events. These capture events can be read via a serial interface. The board uses a binary interface protocol to receive configuation parameters and exchange status information with external equipment via its RS-232 interfaces.

MRS capability
The oscillator of the GNS181-UC can be disciplined by an external reference source (e.g. 1PPS, 10 MHz, IRIG, PPS + String).

11.2.2 GNSS Signal Reception

The satellites of most **Global Navigation Satellite Systems (GNSS)** like **GPS**, **GLONASS**, and **Galileo** are not stationary but circle round the globe in periods of several hours. Only few GNSS systems like the Chinese **Beidou** system work with stationary satellites. Such systems can only be received in certain regions of the Earth.

GNSS receivers need to track at least four satellites to determine their own position in space (x, y, z) as well as their time offset from the GNSS system time (t). Only if the receiver can determine its own position accurately the propagation delay of the satellite signals can also be compensated accurately, which is requirement to yield an accurate time. If the receiver position can only be determined less accurately then the accuracy of the derived time is also degraded.

GNSS satellite signals can only be received directly if no building is in the line-of-sight from the antenna to the satellite. The signals can eventually be reflected at buildings, etc., and the reflected signals can then be received. However, in this case the true signal propagation path is longer than expected, which causes a small error in the computed position, which in turn yields less accurate time.

Since most of the satellites are not stationary, the antenna has to be installed in a location with as much clear view of the sky as possible (e.g. on a rooftop) to allow for continuous, reliable reception and operation. Best reception is achieved when the antenna has a free view of 8° angular elevation above the horizon. If this is not possible then the antenna should be installed with the best free view to the sky in direction of the equator. Since the satellite orbits are located between latitudes 55° North and 55° South, this allows for the best possible reception.

Meinberg provides their own GPS receivers which operate with an antenna/converter unit and thus allow for very long antenna cables, but some devices also include GNSS receivers which support other satellite systems like GLONASS, or Galileo in addition to GPS. These receivers usually require a different type of antenna equipment which is described in chapter (4.1.2).

11.2.2.1 Meinberg GPS Antenna/Converter

11.2.2.2 Introduction

The Meinberg **GPS antenna/converter unit** combines a standard GPS patch antenna with a frequency converter which translates the original 1.5 GHz signal received from the GPS satellites to an intermediate frequency, so a standard coaxial cable type like RG58 can be used for antenna cable lengths up to 300 meters (1000 ft). If a low-loss cable type like RG213 is used then even 700 meters (2300 ft) between receiver and antenna are possible without requirement for an additional amplifier.

Surge protectors are optionally available and should be used in the antenna line to protect the receiver from high voltages spikes e.g. due to lightning strikes close to the antenna. The antenna/converter unit is remotely powered by the connected GPS receiver via the antenna cable, so no external power supply is required near the location of the antenna if a coaxial cable is used.

If more than a single GPS receiver are to be operated then a **GPS antenna splitter** can be used to distribute the GPS signal from a single antenna. The GPS antenna splitter provides 4 outputs and can be cascaded to supply even more than 4 receivers with the GPS signal.

Alternatively there is also a **GPS Optical Antenna Link (GOAL)** available which uses a fiber optic connection between the antenna and the receiver which allows for a length up to 2000 meters (6500 ft), and provides a high level of insulation and surge protection due to the optical transmission. Since the fiber optic connection is unable to provide the antenna with DC current, an extra power supply is required in this case at the location of the antenna.

Due to the specific requirements for remote powering and frequency conversion the Meinberg GPS equipment is not necessarily compatible with GPS equipment from 3rd party manufacturers.

11.2.2.3 Mounting and Installation of the GPS Antenna

Proper installation of the GPS antenna/converter unit is illustrated in the figure below:

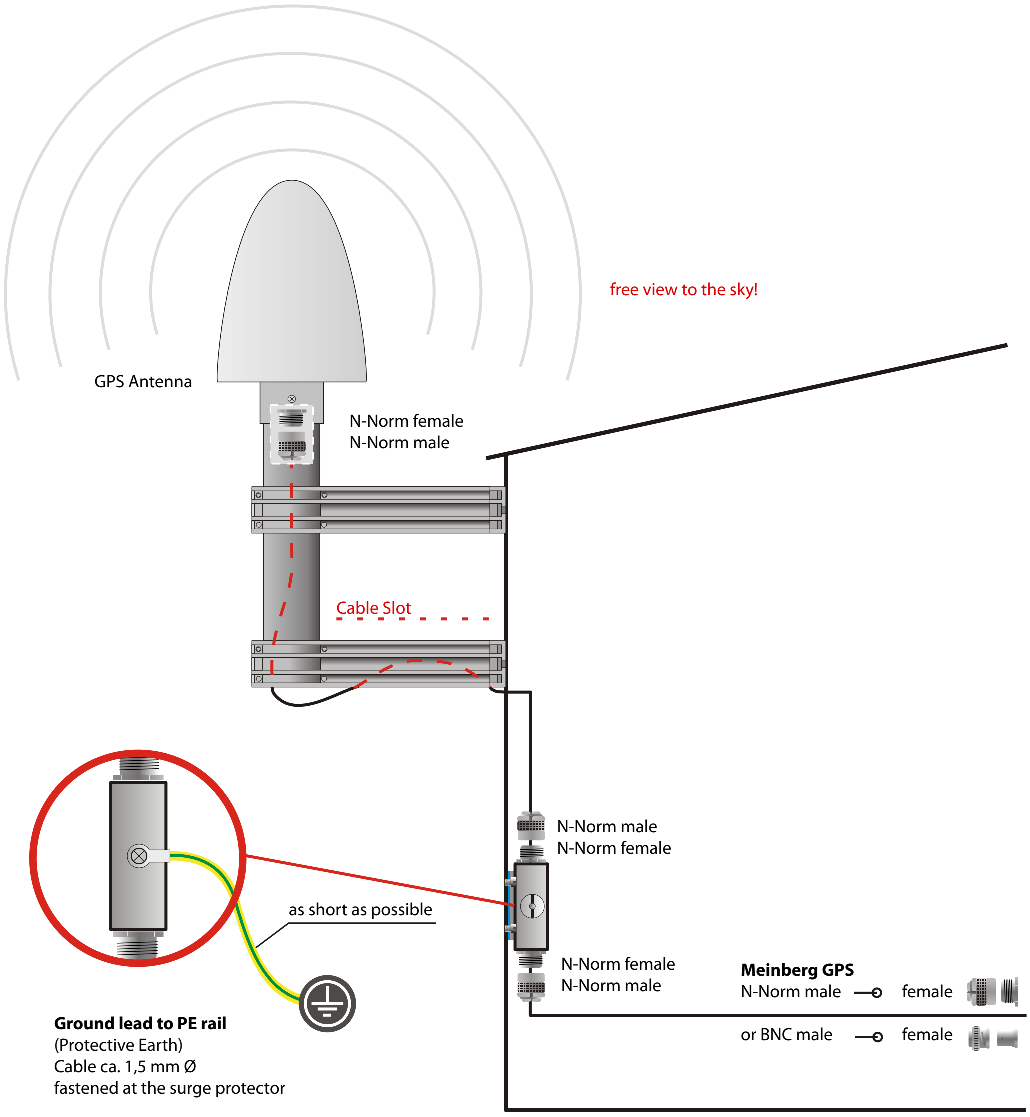


Figure: GPS Antenna mounted on a pole with a free view of the sky. The optional surge protector keeps high voltage strikes through the antenna cable away from the receiver.

Danger!

Do not mount the antenna without an effective fall arrester!

Danger of death from falling!

- Ensure that you work safely when installing antennas!
- Never work without an effective fall arrester!

Danger!

Do not work on the antenna system during thunderstorms!

Danger of death from electric shock!

- Do not carry out any work on the antenna system or the antenna cable if there is a risk of lightning strike.
- Do not carry out any work on the antenna system if it is not possible to maintain the prescribed safe distance to exposed lines and electrical substations.

Mounting material (plastic pole and holders, clamps for wall or pole mounting) is shipped with all Meinberg GPS antennae for easy installation. A standard RG58 antenna cable of 20 meters length is included by default. If a different cable length is required then this can be ordered accordingly.

Surge protectors should be installed indoors, directly where the antenna cable comes in. The optionally delivered protection kit is not for outdoor usage. The ground lead should be kept as short as possible and has to be connected to building's ground rod.

Up to four GPS receivers can be fed by a single antenna/down-converter unit by using an antenna splitter which can optionally be cascaded. The total length of an antenna cable from the antenna to each receiver must not exceed the specified maximum length according to the cable type. The position of the splitter in the antenna line does not matter.

Note:
If the antenna cable is assembled locally instead of using a cable shipped with the GPS receiver it has to be made sure that the connectors have been soldered and assembled properly, and that there is no short-circuit in the cable or in one of the connectors. Otherwise GPS reception may be degraded, or the GPS receiver can even be damaged.

11.2.2.4 General GNSS Antennae

Some Meinberg devices use alternate GNSS receivers which support other satellite systems like GLONASS, Galileo or BeiDou, in addition to GPS. These receivers can't be operated directly with the standard Meinberg antenna/converter unit described in chapter "Meinberg GPS Receiver", so they require a different kind of antenna.

There are two different antenna versions available, one of which is more suited for stationary installation, while the other one should be preferred for mobile applications.

11.2.2.5 GNSS Antenna for Stationary Installation

The **Multi GNSS Antenna** is an active GNSS antenna which can receive the signals of the GPS, GLONASS, Galileo and Beidou satellite systems. It is very well suited for stationary installations, operates with a 5V DC supply voltage provided by the receiver, and has an integrated surge protection.

Danger!

Do not mount the antenna without an effective fall arrester!

Danger of death from falling!

- Ensure that you work safely when installing antennas!
- Never work without an effective fall arrester!

Danger!

Do not work on the antenna system during thunderstorms!

Danger of death from electric shock!

- Do not carry out any work on the antenna system or the antenna cable if there is a risk of lightning strike.
- Do not carry out any work on the antenna system if it is not possible to maintain the prescribed safe distance to exposed lines and electrical substations.

The antenna cable length can be up to 70 meters if a H155 low-loss coaxial cable is used.

Mounting and Installation of the GNSS/L1 Antenna

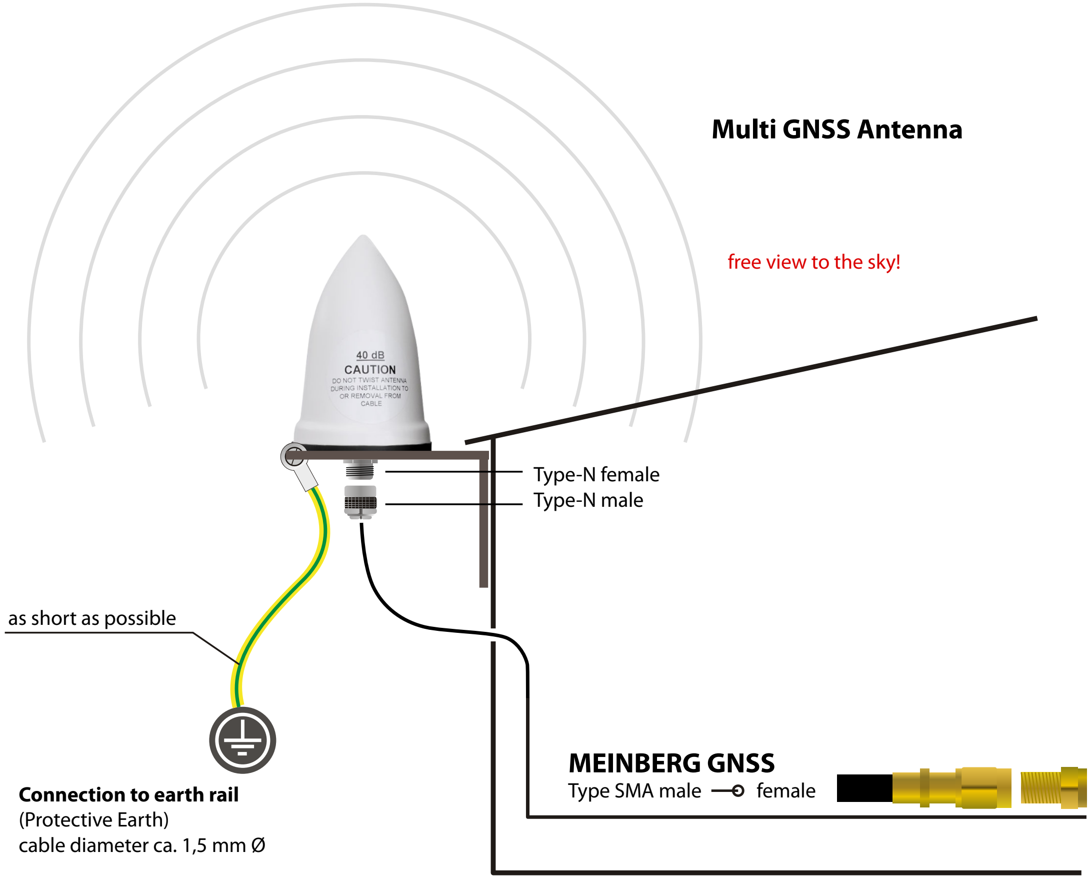


Figure: Schematic diagram of mounting the Multi GNSS Antenna

11.2.2.6 GNSS Antenna for Mobile Applications

The **RV-76G** is an active GNSS antenna which can receive the signals of the GPS, GLONASS, and Galileo satellite systems. It operates with a 5V DC supply voltage provided by the receiver, and should be preferred for mobile applications. However, the maximum length of the antenna cable is limited depending on the cable type, e.g. 5 meters with RG174/U cable, so this antenna is less suitable for stationary installations.

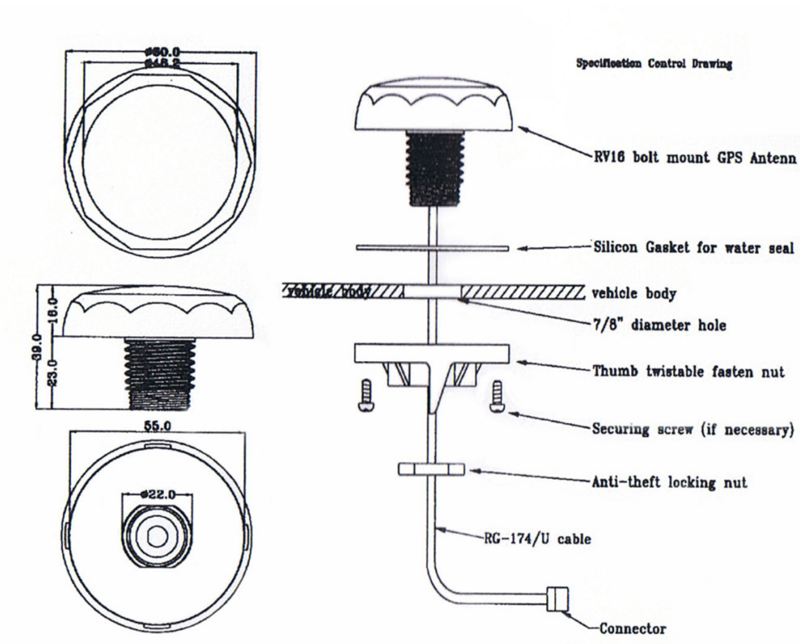


Figure: Installation drawing RV-76G antenna

Danger!

Do not mount the antenna without an effective fall arrester!

Danger of death from falling!

- Ensure that you work safely when installing antennas!
- Never work without an effective fall arrester!

Danger!

Do not work on the antenna system during thunderstorms!

Danger of death from electric shock!

- Do not carry out any work on the antenna system or the antenna cable if there is a risk of lightning strike.
- Do not carry out any work on the antenna system if it is not possible to maintain the prescribed safe distance to exposed lines and electrical substations.

11.2.2.7 Powering up a GNSS Receiver

If both the antenna and the power supply have been connected the system is ready to operate. Depending on the type of oscillator installed in the receiver it takes about 10 seconds (OCXO-LQ) until 3 minutes (OCXO-MQ / HQ) until the oscillator has warmed up and reached the required frequency accuracy.

If the receiver has some valid almanac data in its battery buffered memory and the receiver's position has not changed significantly since its last operation the receiver can determine which satellites are in view. Only a single satellite needs to be received to synchronize and generate output pulses, so synchronization can be achieved at least one minute (OCXO-LQ) until 10 minutes (OCXO-MQ / HQ) after power-up. After 20 minutes of operation the OCXO is fully adjusted and the generated frequencies are within the specified tolerances.

If the receiver position has changed by some hundred kilometers since last operation, the expected satellites may not be in view after power-up. In this case the receiver switches to **Warm Boot** mode where it starts scanning for all possible satellites one after the other. Once the receiver can track at least 4 satellites at the same time it updates its own position and switches to **Normal Operation**.

If no valid data can be found in the battery buffered memory, e.g. because the battery has been disconnected or replaced, the receiver has to scan for satellites and collect the current almanac and ephemeris data first. This mode is called **Cold Boot**, and it takes at least 12 minutes until all required data have been collected. The reason is that the satellites send all data repeatedly once every 12 minutes. After data collection is complete the receiver switches to **Warm Boot** mode to scan for more satellites, and finally enters **Normal Operation**.

In the default configuration neither pulse and synthesizer outputs, nor the serial ports are enabled after power-up until synchronization has been achieved. However, it is possible to configure some or all of those outputs to be enabled immediately after power-up.

If the system starts up in a new environment (e. g. receiver position has changed or new power supply has been installed) it can take some minutes until the oscillator's output frequency has been adjusted properly. In this case the accuracy of the output frequency and pulses is also reduced until the receiver's control loops have settled again.

Via the Meinberg Device Manager software (menu "Status → Clock → Satellites") you can check the number of satellites that are in view (i.e. above the horizon) and considered good (i.e. are healthy and can be tracked).

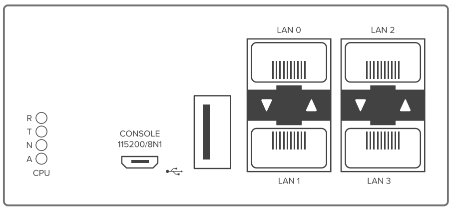
11.2.3 Cable Types

Antenna Type	Cable Type	Maximum Cable Length
Meinberg GPS Antenna	RG58	300 m / 1000 ft
Meinberg GPS Antenna	RG213	700 m / 2300 ft
Multi GNSS Antenna	Belden H155	70 m / 230 ft
Long Wave Antenna *	RG58	300 m / 1000 ft
Fiber Optic **	Fiber Optic	2000 m / 6500 ft

* DCF77 (Germany, Middle Europe), MSF (GB), WWVB (US), JJY (Japan)
** Fiber Optic - GOAL - GPS Optical Antenna Link; DOAL - DCF Optical Antenna Link

11.3 Technical Specifications of used Modules

11.3.1 Technical Specifications - CPU



CPU:	825 MHz Cortex A9 Dual Core on SOC
Ethernet Interfaces:	4 x GBIT SFP - Slot
LAN 0, 1:	Management / NTP 10/100/1000Mbit RJ45 or 1000FX
LAN 2, 3	Management / NTP / PTP 10/100/1000Mbit RJ45 or 1000FX Synchronous Ethernet: Master and Slave Capability Compliant to ITU-T G.8261, G.8262 and G.8264 Ethernet Synchronization Messaging Channel (ESMC)
USB Interfaces:	<u>USB to serial console</u> Micro-USB type B <u>USB Host</u> USB connector CPU management USB type A
Profiles:	IEEE 1588v2 Default Profile Enterprise Profile IEC 61850-9-3 Power Profile IEEE C.37.238-2011 Power Profile IEEE C.37.238-2017 Power Profile ITU-T G.8265.1 Telecom Frequency Profile ITU-T G.8275.1 Telecom Phase / Time Profile (full timing support) ITU-T G.8275.2 Telecom Phase / Time Profile (partial timing support) SMPTE ST 2059-2 Broadcast Profile IEEE 802.1AS TSN/AVB Profile AES67 Media Profile DOCSIS 3.1
PTP Modes:	Multicast/Unicast Layer 2 (IEEE 802.3) Multicast/Unicast Layer 3 (UDP IPv4/IPv6) Hybrid Mode E2E / P2P Delay Mechanism Up to 128 messages/second per client
1588 Clock Mode:	1-Step, 2-Step for both Master and Slave operation
Time Stamp Accuracy:	8 ns
NTP Req./Sec:	10,000
NTP Mode:	NTP Server mode

Network Protocols:	IPv4, IPv6 DHCP, DHCPv6 DSCP IEEE 802.1q VLAN filtering/tagging IEEE 802.1p QOS

LED Indicators

R (Receiver)

green:	the reference clock (e.g. build-in GNSS) provides a valid time
red:	the reference clock does not provide a valid time

T (Time Service)

green:	NTP is synchronized to the reference clock, e.g. GNSS
red:	NTP is not synchronized or switched to the "local clock"

N (Network)

green:	all monitored network interfaces are connected ("Link up")
red:	at least one of the monitored network interfaces is faulty

A (Alarm)

off:	no error
red:	general error

Available Client Licenses:

License	Unicast Clients	Delay Req./s
PL-A	8	1024
PL-B	256	32768
PL-C	512	65536

Recommended and tested Transceivers from other Vendors

Mode	Vendor/Type	Distance
MULTI MODE:	AVAGO AFBR-5710PZ	550 m
	FINISAR FTLF8524P3BNL	500 m
	Cisco GLC-SX-MMD	500 m
SINGLE MODE:	AVAGO AFCT-5710PZ	10 km
	FINISAR FTLF1318P3BTL	10 km
	SMARTOPTICS SO-SFP-L120D-C63	80 km
RJ-45:	AVAGO ABCU-5740RZ	100 m
	FINISAR FCLF8521P2BTL	100 m

11.3.2 Technical Specifications GNSS Receiver

Time to Sychronization:
one minute with known receiver position and valid almanac
12 minutes if invalid battery buffered memory

Pulse Outputs:
HR and RX systems: eight programmable outputs (PP 1 - PP 8)
Timer, Single Shot, Cyclic Pulse, Pulse Per Second / Minute / Hour, DCF77 Marks, Position OK, Time Sync, All Sync, DCLS Time Code, Serial Time String, 10 MHz Frequency, Synthesizer Frequency, PTTI 1PPS

DC-insulated by optocouplers
$U_{CEmax} = 55$ V, $I_{Cmax} = 50$ mA, $P_{tot} = 150$ mW, $V_{iso} = 5000$ V

pulse delay: t_{on} e.g. 20 μsec ($I_C = 10$ mA)
t_{off} e.g. 3 μsec ($I_C = 10$ mA)

Accuracy of Pulses:
after synchronization and 20 minutes of operation
OCXO SQ/MQ/HQ/DHQ: better than $\pm$50 nsec

better than $\pm$2 μsec during the first 20 minutes of operation

Frequency Outputs:
10 MHz, TTL level into 50 Ohm
1 MHz, TTL level
100 kHz, TTL level

Frequency Synthesizer:
1/8 Hz up to 10 MHz

Accuracy of Synthesizer:
base accuracy depends on system accuracy
1/8 Hz to 10 kHz — Phase syncron with pulse output P_SEC
10 kHz to 10 MHz — frequency deviation < 0.0047 Hz

Synthesizer Outputs:
F_SYNTH: TTL level

Serial Ports:
asynchronous serial port RS-232
Baud Rate: 300, 600, 1200, 2400, 4800, 9600, 19200 Baud
Framing: 7E1, 7E2, 7N2, 7O1, 7O2, 8E1, 8N1, 8N2, 8O1

Default Setting:
COM 0: 19200, 8N1
Meinberg Standard time string, per second

Time Code Outputs:
Unbalanced modulated sine wave signal:
3 V_{pp} (MARK), 1 V_{pp} (SPACE) into 50 Ω

PWM DCLS-signal: TTL into 50 Ω, active-high or -low

GNS Receiver

Type of receiver:	GPS/GLONASS/Galileo/BeiDou receiver Number of channels: 72 Frequency band: GNSS L1 GPS: 1575.42 ±10 MHz GLONASS: 1602-1615 MHz Galileo: 1542.5 MHz BeiDou: 1561.09 MHz	
Antenna:	Combined GPS/GLONASS antenna	
	3 dB Bandwidth:	1590 ±30 MHz
	Impedance:	50 Ω
	Gain:	40 ±4 dB
Cable length:	max. 70 m	low-loss cable (Belden H155)
Antenna Connector:	SMA female	
Power Supply for Antenna:	5 V, 100 mA - continuous short circuit protection, automatic recovery power supply via antenna cable	

GPS Receiver

Receiver:	12 channel C/A code receiver with external antenna/converter unit
Antenna:	antenna/converter unit with remote power supply
Cable length:	max. 300 m (RG58 coax-cable)
Antenna Connector:	BNC female
Power Supply for Antenna:	15 V DC, continuous short circuit protection, automatic recovery isolation voltage 1000 VDC, provided via antenna cable

GNS-UC Receiver

Type of receiver:	72 channel receiver GPS/Galileo	
	Frequency band:	
	GPS:	L1C/A
	Galileo:	E1B/C
Cable length:	max. 300 m (RG58 coax-cable)	
Antenna Connector:	BNC female	
Power Supply for Antenna:	15 V DC, continuous short circuit protection, automatic recovery isolation voltage 1000 VDC, provided via antenna cable	

11.4 Network Time Protocol (NTP)

The public domain software package called NTP (Network Time Protocol) is an implementation of the same named TCP/IP network protocol. NTP has been initiated in the 1980's by Dave L. Mills who was trying to achieve a high accuracy time synchronization for computers across the network. The protocol and related algorithms have been specified in several RFCs. Since then NTP has continuously been optimitzed and is at present time widely used around the world. The protocol supports an accuracy of time down to nanoseconds. However, the maximun achievable accuracy also depends on the operating system and the network performance.

Currently there are two versions of NTP which can be used intermixed: NTP v3 is the latest released version which runs very stable on many operating systems. NTP v4 has some improvements over NTP v3 and has better support for some operating systems. Additionally, there's also a simplified version of the protocol called SNTP (Simple Network Time Protocol). SNTP uses the same TCP/IP packet structure like NTP but due to the simpler algorithms, it provides only very reduced precision. The NTP package contains a background program (daemon or service) which synchronizes the computer's system time to one or more external reference time sources which can be either other devices on the network, or a radio clock which is connected to the computer.

Additionally, the NTP distribution contains programs which can be used to control or monitor the time synchronization status, and a complete set of documentation in HTML format.

More information about the Network Time Protocol can be found at:
https://www.meinbergglobal.com/english/info/ntp.htm

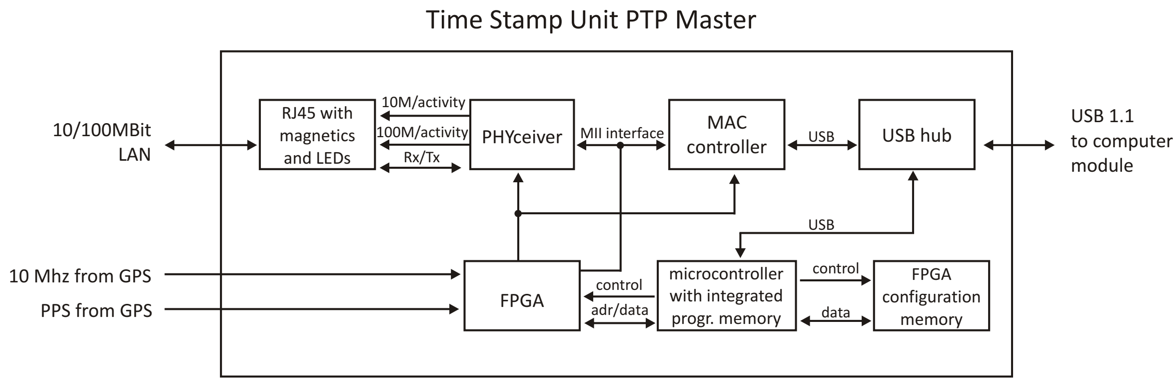
11.5 The Precision Time Protocol (PTP) / IEEE 1588

Precision Time Protocol (PTP or IEEE 1588) is a time synchronization protocol that offers sub-microsecond accuracy over a standard Ethernet connection. This accuracy can be achieved by adding a hardware timestamping unit to the network ports that are used for PTP time synchronization. The timestamping unit captures the exact time when a PTP synchronization packet is sent or received. These timestamps are then taken into account to compensate for transfer delays introduced by the Ethernet network.

In PTP networks there is only one recognized active source of time, referred to as the Grandmaster Clock. If two or more Grandmaster Clocks exist in a single network, an algorithm defined in the PTP standard is used to determine which one is the „best“ source of time. This "Best Master Clock" algorithm must be implemented on every PTP/IEEE1588 compliant system to insure that all clients („Slave Clocks“) will select the same Grandmaster. The remaining deselected Grandmaster Clocks will „step back“ and enter a passive mode, meaning that they do not send synchronization packets as long as that is being done by the designated Grandmaster.

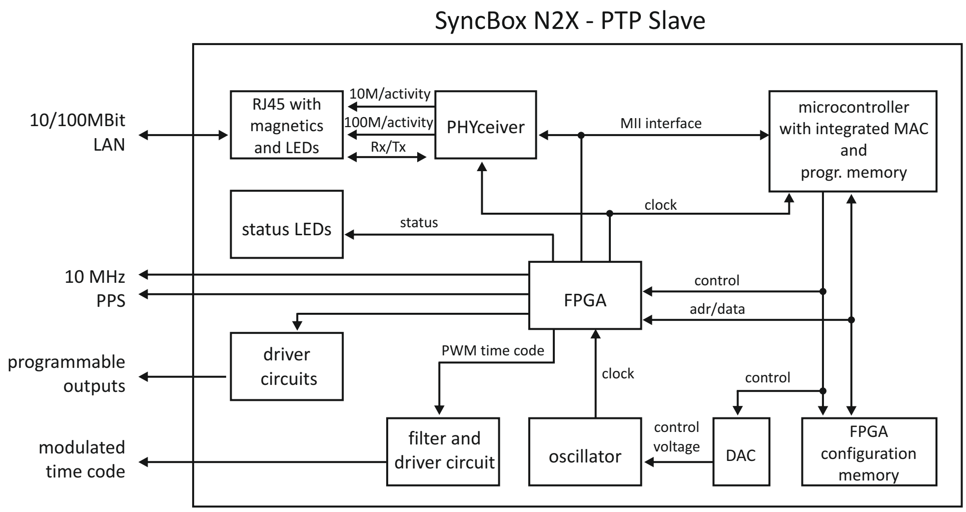
The existing network infrastructure components play a big role in a PTP network and directly influence the level of accuracy that can be achieved by the clients. Asymmetric network connections degrade the accuracy, therefore classic layer 2 and 3 Ethernet switches with their “store and forward” technology are not suitable for PTP networks and should be avoided. With activating the HQ-Filter (see chapter HQ-Filter) the Jitter can be eliminated. Simple Ethernet hubs with fixed pass-through times are not a problem. In large networks, special switches with built-in PTP functionality help to maintain high accuracy even over several subnets and longer distances. These components act as "Boundary Clocks" (BC) or "Transparent Clocks" (TC). They compensate their internal packet processing times by using timestamping units on each port. When acting as a Boundary Clock, they synchronize to the Grandmaster clock, and in turn act as a Master to the other subnets they are connected to. When acting as a Transparent Clock, then the "residence time" of the Masters’ Sync-Packet is measured and added to the packet as a correction value. Internally the PTP timescale TAI (see chapter Timescale in Global Parameters).

11.5.1 Functionality in Master Systems



After power up, the module accepts the absolute time information (PTP seconds) of a reference time source (e.g. GNSS reference clock) only once, and the PTP nanoseconds are set to zero. If the oscillator frequency of the reference time source has reached its nominal value, the nanoseconds are reset again. This procedure leads to a maximum deviation of 20 nsec of the pulse per second (1PPS) of the PTP Master compared to the 1PPS of the GNSS reference clock. The reference clock of the PTP board's time stamp unit (50 MHz) is derived from the GNSS disciplined oscillator of the reference time source using a PLL (Phase Locked Loop) of the FPGA. This achieves a direct coupling of the time stamp unit to the GNSS system.

11.5.2 Functionality in Slave Systems



After decoding valid time information from a PTP Master, the system sets its own PTP seconds and nanoseconds accordingly. The PTP offset calculated by the PTP driver software is used to adjust the master oscillator of the PTP Slave. This allows the PTP Slave to generate very high accuracy output signals (10 MHz/1PPS/IRIG).

11.5.3 PTPv2 IEEE 1588-2008 Configuration Guide

Setting up all devices in a PTP synchronization infrastructure is one of the most important parts in a network time synchronization project. The settings of the involved Grandmaster clocks as the source of time and the end devices ("Slaves") have to match in order to allow them to synchronize and avoid problems later, when the PTP infrastructure is deployed to production environments. In addition to that, the use of PTP aware network infrastructure components, namely network switches, introduces another set of parameters that have to be harmonized with the masters and slaves in a PTP setup.

It is therefore very important to start with making decisions how the to-be-installed PTP synchronization solution should operate, e.g. should the communication between the devices be based on multicast or unicast network traffic or how often should the masters send SYNC messages to the slaves.

This chapter lists the most important options and their implications on a synchronization environment in general. A detailed explanation of the configuration settings within the Meinberg Device Manager configuration menu can be found later within this documentation.

11.5.3.1 General Options

The following general mode options have to be decided before deploying the infrastructure:

1) Layer 2 (Ethernet) or Layer 3 (UDP/IPv4) connections
2) Multicast or Unicast
3) Two-Step or One-Step Operation
4) End-to-End or Peer-to-Peer Delay Mechanism

The above options need to be defined for the whole setup, if devices do not stick to the same settings, they will not be able to establish a working synchronization link.

11.5.3.2 Network Layer 2 or Layer 3

PTP/IEEE 1588-2008 offers a number of so-called mappings on different network communication layers. For Meinberg products you can choose between running PTP over IEEE 802.3 Ethernet connections (network Layer 2) or UDP/IPv4 connections (Layer 3).

Layer 3 is the recommended mode, because it works in most environments. For Layer 2 mode the network needs to be able to provide Ethernet connections between master and slave devices, which is often not the case when your network is divided into different network segments and you have no layer 2 routing capabilities in your network infrastructure.

The only benefit of using Layer 2 mode would be a reduced traffic load, because the transmitted network frames do not need to include the IP and UDP header, saving 28 bytes per PTP packet/frame. Due to the fact that PTP is a low traffic protocol (when compared to other protocols), the reduced bandwidth consumption only plays a role when low-bandwidth network links (e.g. 2Mbit/s) have to be used or in pay-per-traffic scenarios, for example over leased-line connections.

11.5.3.3 Multicast or Unicast

The initial version of PTP (IEEE 1588-2002 also known as PTPv1) was a multicast-only protocol. Multicast mode has the great advantage that the master clock needs to send only one SYNC packet to a Multicast address and it is received by all slave devices that listen to that multicast address.

In version 2 of the protocol (IEEE 1588-2008) the unicast mode was introduced in addition to the multicast mode. In unicast mode, the master has to send one packet each to every slave device, requiring much more CPU performance on the master and producing orders of magnitudes more traffic.

On the other hand, some switches might block multicast traffic, so that in certain environments, Unicast mode has to be used.

11.5.3.4 Two-Step or One-Step

The PTP protocol requires the master to periodically send SYNC messages to the slave devices. The hardware time stamping approach of PTP requires that the master records the exact time when such a SYNC packet is going on the network wire and needs to communicate this time stamp to the slaves. This can be achieved by either sending this time stamp in a separate packet (a so-called FOLLOW-UP message) or by directly manipulating the outgoing SYNC message, writing the hardware time stamp directly into the packet just before it leaves the network port.

11.5.3.5 End-To-End (E2E) or Peer-To-Peer (P2P) Delay Measurements

In addition to receiving the SYNC/FOLLOWUP messages a PTP slave device needs to be able to measure the network delay, i.e. the time it took the SYNC message to traverse the network path between the master and the slave. This delay is required to correct the received time information accordingly and it is measured by the slave in a configured interval (more about the message intervals later). A delay measurement is performed by sending a so-called DELAY_REQUEST to the master which timestamps it and returns the timestamp in a DELAY_RESPONSE message.

IEEE 1588-2008 offers two different mechanisms for performing the delay measurements. A slave can either measure the delay all the way to the master, this is called End-To-End (or E2E in short) or to its direct network neighbors (which would in almost all cases be a switch – or two in a redundant setup), using the Peer-To-Peer delay measurement mechanism (P2P). The delay measurements of all links between the master and the slave are then added and accumulated while a SYNC packet is traversing the network.

The advantage of this method is that it can dramatically reduce the degradation of accuracy after topology changes. For example: in a redundant network ring topology the network delay will be affected when the ring breaks open and network traffic needs to be redirected and flows into the other direction. A PTP slave in a sync infrastructure using E2E would in this case apply the wrong delay correction calculations until it performs the next delay measurement (and finds out that the network path delay has changed). The same scenario in a P2P setup would see much less time error, because the delay of all changed network links were already available.

The drawback: the P2P approach requires that all involved PTP devices and all switches support this mechanism. A switch/hub without P2P support would in the best case simply pass the so-called PDELAY messages through and as a result degrade the accuracy of the delay measurements. In the worst case it would block/drop the PDELAY messages completely, which effectively would result in no delay measurements at all.

So, E2E is the only available choice if you are running PTP traffic through non-PTP-aware switches. It is a reasonable choice if you are not using redundant network topologies or can accept that the delay measurements are wrong for a certain amount of time.

11.5.3.6 Mode Recommendations

Meinberg recommends to set up your PTP infrastructure to use Layer 3, Multicast, Two-Step and End-To-End Delay measurements if that is possible. This will provide the largest possible compatibility and reduces interoperability problems.

11.5.3.7 Message Rate Settings

The decision between the different general mode options is mainly dictated on the network environment in which the PTP infrastructure is installed. In addition to the mode selection, a number of intervals for certain types of PTP network messages needs to be defined. In most cases, the default values as defined in the standard are a safe bet, but there are applications and scenarios where a custom message rate is required.

A possible example is a situation where the PTP infrastructure is integrated within an environment with high network load. In this case, the PTP packets can be affected by the effect of packet delay variation (PDV). An increase of the PTP message rate(s) can avoid synchronization problems due to packet queuing within non-PTP compliant switches which might cause false measurements. At higher rates, these false measurements can be detected and corrected faster as compared to lower rates at the cost of increased traffic.

The message rates for the following message types can be changed:

1) ANNOUNCE messages
2) SYNC/FOLLOWUP messages
3) (P)DELAY_REQUEST messages

11.5.3.8 ANNOUNCE Messages

These PTP messages are used to inform the PTP network participants about existing and available master clock devices. They include a number of values that indicate the potential synchronization accuracy.

The procedure used to decide which of the available devices (that could become masters) is selected is called the "best master clock algorithm" (BMCA). The values that are used in this BMCA are read from the ANNOUNCE messages that potential masters send out periodically.

The rate at which these messages are sent out are directly affecting the time that is required by a slave device to select a master and to switch to a different master in case the selected one fails.

Multiple devices can simultaneously transmit ANNOUNCE messages during periods in which no master has been selected (yet). This happens for example when a PTP network is powered up, i.e. all devices are starting to work at the same time. In this case all devices that consider themselves (based on their configuration and status) being capable of providing synchronization to all the other PTP devices will start to send out ANNOUNCE messages. They will receive the other candidates' ANNOUNCE messages as well and perform the BMCA. If they determine that another candidate is more suitable to become the master clock, they stop sending ANNOUNCE messages and either become slave devices or go into "PASSIVE" mode, waiting for the selected master to stop sending ANNOUNCE messages. This is determined to be the case when no ANNOUNCE message is received within 3 ANNOUNCE message intervals.

As an example, if the ANNOUNCE interval has been configured to be 2 seconds (one message every 2 seconds, the default value), the master is considered to have failed when no message has been received for 6 seconds.

In order to choose a master (a backup master clock or the primary one during initialization) the devices require to receive at least two consecutive ANNOUNCE messages. Continuing our example, it would take the 6 seconds to determine that the current master has failed and another 4 seconds to select the new one. That means an ANNOUNCE interval of 2 seconds translates into at least 10 seconds of "switching time" and 4 seconds of "initial master clock selection time". So, choosing a shorter ANNOUNCE message interval will allow a faster switching to a backup master clock, but it can lead to false positives when the chosen interval is too short for the network environment.

11.5.3.9 SYNC/FOLLOWUP Messages

The selected master clock sends out SYNC (and, in Two-Step environments, the corresponding FOLLOWUP) messages in a configured interval. This interval (default value is one SYNC/FOLLOWUP packet every second) determines how often the slave devices receive synchronization data that allows them to adjust their internal clocks in order to follow the master clock time. Between receiving two SYNC messages, a slave clock runs free with the stability determined by its own internal time base, for example a crystal oscillator. One important factor for deciding on the SYNC interval is the stability of this oscillator. A very good oscillator requires a lower SYNC message rate than a cheaper, low-accuracy model. On the other hand you directly affect the required network bandwidth by changing the SYNC interval.

For Meinberg slave devices, the default one-SYNC-every-second setting is more than enough to achieve the highest possible synchronization accuracy.

11.5.3.10 (P)DELAY_REQUEST Messages

As explained in the General Mode Options chapter (see the "End-To-End or Peer-to-Peer" section), the delay measurements are an important factor for achieving the required accuracy. Especially in E2E mode, the network path delay measurements play a crucial part in the synchronization process. Per default, the slaves will perform delay measurements every 8 seconds, resulting in sending and receiving one packet. This can be increased in case the network path delay variation in the network is relatively large (i.e. the time it takes for the SYNC message to reach the slave varies a lot) or the slave devices have to tightly follow the master and adjust their time base (oscillator) very often due to its instability.

Meinberg slave devices will limit the effect of an outdated path delay measurement by using filters and optimized PLL algorithms. This avoids that a clock "jumps around" and basically monitors the time difference to the master clock carefully for a certain amount of time before adjusting its own clock. With a low cost time base this is not possible, because the instability (i.e. temperature-dependent drift and overall short term stability/aging effects) and therefore these slaves would require to perform as many delay measurements and receive as many SYNC/FOLLOWUP messages as possible.

For P2P mode the delay request interval is not as critical, simply because the delay variation on a single-hop link (i.e. from your slave device to its switch) is very stable and does not change dramatically in typical environments.

Current firmware versions of Meinberg Grandmaster clocks (V5.32a and older) do not offer changing the Delay message rate in Multicast mode, it is fixed to one delay request every 8 seconds. Since this is actually a value that is transmitted in the DELAY_RESPONSE message as a maximum value, the slave devices are not allowed to perform delay measurements more often.

11.6 Description of Time Code Formats

Each IRIG format carries a designation comprising a letter followed by three numerical digits. The letter and each of the digits represents a characteristic property of the corresponding IRIG code.

Depending on your Meinberg product, more or less time code formats are supported.

A002:	1000 pps, DCLS, pulse-width coded, no carrier Time of year (BCD)
A003:	1000 pps, DCLS, pulse-width coded, no carrier Time of year (BCD), time of day (SBS)
A132:	1000 pps, AM sine-wave signal, 10 kHz carrier frequency Time of year (BCD)
A133:	1000 pps, AM sine-wave signal, 10 kHz carrier frequency Time of year (BCD), time of day (SBS)
B002:	100 pps, DCLS, pulse-width coded, no carrier Time of year (BCD)
B003:	100 pps, DCLS, pulse-width coded, no carrier Time of year (BCD), time of day (SBS)
B006:	100 pps, DCLS, pulse-width coded, no carrier Time of year (BCD), calendar year (BCD)
B007:	100 pps, DCLS, pulse-width coded, no carrier Time of year (BCD), year, time of day (SBS)
B122:	100 pps, AM sine-wave signal, 1 kHz carrier frequency Time of year (BCD)
B123:	100 pps, AM sine-wave signal, 1 kHz carrier frequency Time of year (BCD), time of day (SBS)
B126:	100 pps, AM sine-wave signal, 1 kHz carrier frequency Time of year (BCD), calendar year (BCD)
B127:	100 pps, AM sine-wave signal, 1 kHz carrier frequency Time of year (BCD), calendar year (BCD), time of day (SBS)
E002:	10 pps, DCLS, pulse-width coded, no carrier Time of year (BCD)
E112:	10 pps, AM sine wave signal, 100 Hz carrier frequency Time of year (BCD)
G002:	10000 pps, DCLS, pulse-width coded, no carrier Time of year (BCD)
G006:	10000 pps, DCLS, pulse-width coded, no carrier Time of year (BCD), calendar year (BCD)
G142:	10000 pps, AM sine-wave signal, 100 kHz carrier frequency Time of year (BCD)
G146:	10000 pps, AM sine-wave signal, 100 kHz carrier frequency Time of year (BCD), calendar year (BCD)

Abbreviations:

BCD = Binary-Coded Decimal, SBS = Straight Binary Seconds

In addition to the original IRIG standards, there are also other specifications issued by other bodies that define specific extensions.

AFNOR:	Code according to NF S87-500, 100 pps, AM sine-wave signal, 1 kHz carrier frequency, BCD time of year, complete date, SBS time of day, signal level specified by standard.
IEEE 1344:	Code according to IEEE 1344-1995, 100 pps, AM sine wave signal, 1kHz carrier frequency, BCD time of year, SBS time of day, IEEE 1344 extensions for date, time zone, Daylight Saving Time, and leap seconds in Control Functions (CF) segment. (See also table "Structure of CF segment in IEEE 1344 mode")
IEEE C37.118:	Identical to IEEE 1344, but with UTC offset +/- sign bit reversed
NASA 36:	100 pps, AM sine wave signal, 1 kHz carrier frequency, resolution: 10 ms (DCLS), 1 ms (modulated carrier) BCD time of year: 30 bits - seconds, minutes, hours, and days

11.7 Description of Programmable Pulse Outputs

In microSync systems the following modes are available for the programmable pulse outputs:

Idle
Selecting "Idle" deactivates the output.

Timer
This mode simulates a programmable day assigned timer. Three turn-off and turn-on times are programmable for each output. If you want to program a switchtime, change the turn-on time "On" and the corresponding turn-off time "Off". A turn-on time later than the turn-off time would cause a switch program running over midnight. For example a program "On"10.45.00, "Off" 9.30.00 would cause an active ouput from 10.45 to 9.30 (the next day!). If one or more of the three switching times are unused just enter the same time into the values "On" and "Off". In this case the switch time does not affect the output.

Single Shot
Selecting Singls Shot generates a single pulse of defined length once per day. You can enter the time when the pulse is generated with the "Time" value. The value "Length" determines the pulse duration. The pulse duration can vary from 10 msec to 10 sec in steps of 10 msec.

Cyclic Pulse
The value of "Time" determines the time between two consecutive pulses. This cycle time must be entered as hours, minutes and seconds. The pulse train is synchronized at 0:00 o'clock local time, so the first pulse of a day always occurs at midnight. A cycle time of 2 seconds for example, would cause pulses at 0:00:00, 0:00:02, 0:00:04 etc. Basically it is possible to enter any cycle time between 0 and 24 hours, however usually a cycle times that cause a constant distance between all consecutive pulses make sense.

For example: a cycle time of 1 hour 45 minutes would cause a pulse every 6300 seconds (starting from 0 o'clock). The appearing distance between the last pulse of a day and the first pulse of the next day (0:00:00 o'clock) would be only 4500 sec. The value in entry field "Cycle" turns red, when entering a time that causes this asymmetry.

Pulses Per Second, Per Min, Per Hour
These modes generate pulses of defined length once per second, once per minute or once per hour. "Length" determines the pulse duration (10 msec...10 sec).

DCF77 Marks
In "DCF77 Marks" mode the selected output simulates the time string transmitted by the German DCF77 time code transmitter. The pulses output are the 100 ms and 200 ms pulses (logical 0/1) typical for the DCF77 code. The absence of the 59-second mark is used to signal that the next minute will begin with the following second mark.

If you want DCF simulation to be disabled when the clock is in free running mode, you can enter the delay (given in minutes) for deactivating the DCF-Simulation with the "Timeout" value. DCF Simulation is never suspended, if the delay value is zero.

Sync Mode
There are three different modes available for outputting the synchronization state of the clock.

Position OK, Time Sync and All Sync
The Mode 'Position OK' activates the output when the receiver has sufficient satellites in view to calculate its position. In "Time Sync" mode the respective output is activated when the clocks internal timebase is synchronized to the GPS timing. The "All Sync" Mode performs a logical AND operation of the both states previously mentioned, i.e. the output is activated if the position can be calculated AND the internal timebase is synchronized to the GPS timing.

DCLS Time Code
DC Level Shift Time Code. The selection of the time code is done by the Meinberg Device Manager menu "Outputs Settings".

10 MHz Frequency
This mode is used to output a fixed frequency of 10 MHz, using a PPS signal as an absolute phase reference (i.e., the falling edge of the 10 MHz signal is synchronized with the rising edge of the PPS signal).

Note: The 10 MHz frequency signal is only switched on when the oscillator changes to the "Warmed Up" state, regardless of the preset activation (if sync, always). If the reference clock is running asynchronously, this 10 MHz frequency remains until a deviation in free-running of more than ± 10 [[micro]]s is exceeded. From this point on, this signal is switched off.

DCF77-like M59
A 500 ms pulse is sent at the 59-second mark.

If you want DCF simulation to be disabled when the clock is in free running mode, you can enter the delay (given in minutes) for deactivating the DCF-Simulation with the "Timeout" value. DCF Simulation is never suspended, if the delay value is zero.

Synth. Frequency
The output of the frequency synthesizer is also done via the "Outputs Settings" menu.

PTTI 1PPS
In this mode, a non-inverted PPS of 20 microseconds pulse length is available at the selected output.

11.8 Available Time Telegrams

11.8.1 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 as follows:

<STX>D:*dd.mm.yy*;T:*w*;U:*hh.mm.ss*;*uvxy*<ETX>

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters as defined below:

<STX>	Start-of-Text, ASCII code 02h sent with one-bit accuracy at the change of each second		
dd.mm.yy	The 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 time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 during leap second)
uv	Clock status characters (depending on clock type):		
	u:	'#'	GPS: Clock is in free-run mode (no exact synchronization) PZF: Time frame not synchronized DCF77: Clock has not synchronized since last reset
	' '	(space, 20h) GPS: Clock is synchronized (base accuracy is reached) PZF: Time frame is synchronized DCF77: Clock has synchronized since last reset	
	v:	'*' GPS: Receiver has not checked its position PZF/DCF77: Clock currently running off XTAL	
	' '	(space, 20h) GPS: Receiver has determined its position PZF/DCF77: Clock is synchronized 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	Announcement of clock jump during last hour before jump enters 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		

11.8.2 Format of the Meinberg GPS Time String

The Meinberg GPS 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. Unlike the Meinberg Standard Time String, the Meinberg GPS Time String does not carry any local time zone or UTC data; it simply carries the direct GPS time without any conversion into UTC. The format is as follows:

`<STX>D:`*`dd.mm.yy;T:w;U:hh.mm.ss;uvGy;lll`*`<ETX>`

The letters printed in *italics* are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters as defined below:

`<STX>` Start-of-Text, ASCII code 02h

`dd.mm.yy` The 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:
u: '#' Clock is in free-run mode (no exact synchronization)
' ' (Space, 20h)
Clock is synchronized (base accuracy is achieved)

v: '*' Receiver has not checked its position
' ' (Space, 20h)
Receiver has determined its position

`G` 'GPS time' time zone indicator

`y` Announcement of clock jump during last hour before jump enters effect:
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

11.8.3 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) sequence. The format is as follows:

`CH`*`x<SP>dd.mm.yy_hh:mm:ss.fffffff`*`<CR><LF>`

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters as defined below:

`x`	0 or 1 corresponding on the number of the capture input		
`<SP>`	Space, ASCII code 20h		
`dd.mm.yy`	Capture date:		
	`dd`	Day of Month	(01–31)
	`mm`	Month	(01–12)
	`yy`	Year of the Century	(00–99)
`hh:mm:ss.fffffff`	Capture time:		
	`hh`	Hours	(00–23)
	`mm`	Minutes	(00–59)
	`ss`	Seconds	(00–59, or 60 during leap second)
	`fffffff`	Fractions of second, 7 digits	
`<CR>`	Carriage Return, ASCII code 0Dh		
`<LF>`	Line Feed, ASCII code 0Ah		

11.8.4 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 as follows:

<STX>*dd.mm.yy/w/hh:mm:ssxxxxuv*<ETX>

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

`<STX>` Start-of-Text, ASCII code 02h sent with one-bit accuracy at the change of each second

`dd.mm.yy` The 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 time:

hh	Hours	(00–23)
mm	Minutes	(00–59)
ss	Seconds	(00–59, or 60 during 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 since last reset
' '	(Space, 20h) Clock has synchronized since last reset

`v` Announcement of clock jump during last hour before jump enters 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

11.8.5 Format of the Uni Erlangen String (NTP)

The Uni Erlangen String (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 as follows:

`<STX>`*`dd.mm.yy; w; hh:mm:ss; voo:oo; acdfg i;bbb.bbbbn lll.lllle hhhhm`*`<ETX>`

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

`<STX>`	Start-of-Text, ASCII code 02h sent with one-bit accuracy at the change of each second		
`dd.mm.yy`	The date:		
	dd	Day of Month	(01–31)
	mm	Month	(01–12)
	yy	Year of Century	(00–99)
`w`	Day of the week		(1–7, 1 = Monday)
`hh.mm.ss`	The time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 during leap second)
`v`	-/+ sign of the offset of local timezone relative to UTC		
`oo:oo`	Offset of local time zone relative to UTC in hours and minutes		
`ac`	Clock status characters:		
	a:	'#'	Clock has not synchronized since reset
		' '	(Space, 20h) Clock has synchronized since 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 Time enabled
	' '	CET	European Standard Time, Daylight Saving Time disabled
`f`	Announcement of clock jump during last hour before jump enters effect:		
	'!'	Announcement of start or end of Daylight Saving Time	
	' '	(Space, 20h) nothing announced	
`g`	Announcement of clock jump during last hour before jump enters effect:		
	'A'	Announcement of leap second insertion	
	' '	(Space, 20h) nothing announced	
`i`	Leap second insertion		
	'L'	Leap second is currently to be inserted (only active in 60th second)	
	' '	(Space, 20h) No leap second to be inserted	
`bbb.bbbb`	Geographical latitude of receiver position in degrees Leading characters padded by Space characters (20h)		

`n` Latitudinal hemisphere, with the following characters possible:
- 'N' North of Equator
- 'S' South of Equator

`lll.llll` Geographical longitude of receiver position in degrees
Leading characters padded by Space characters (20h)

`e` Longitudinal hemisphere, with the following characters possible:
- 'E' East of Greenwich Meridian
- 'W' West of Greenwich Meridian

`hhhh` Altitude above WGS84 ellipsoid in meters
Leading characters padded by Space characters (20h)

`<ETX>` End-of-Text, ASCII code 03h

11.8.6 Format of the NMEA 0183 String (RMC)

The NMEA 0183 RMC String is a sequence of 65 ASCII characters starting with the string '$GPRMC' and ending with the characters <CR> (Carriage Return) and <LF> (Line Feed). The format is as follows:

`$GPRMC,`*`hhmmss.ff`*`,`*`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-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

`$`	Start character, ASCII code 24h sent with one-bit accuracy at the change of each second
`GP`	Talker ID, in this case "GP" for GPS
`RMC`	Message type ID, in this case "RMC"
`hhmmss.ss`	The time: `hh` Hours (00–23) `mm` Minutes (00–59) `ss` Seconds (00–59, or 60 during leap second) `ff` Fractions of Seconds (1/10 ; 1/100)
`A`	Status (A = Time Data Valid, V = Time Data not Valid)
`bbbb.bb`	Geographical latitude of receiver position in degrees Leading characters padded by space characters (ASCII code 20h)
`n`	Latitudinal hemisphere, with the following characters possible: "N" North of Equator "S" South of Equator
`lllll.ll`	Geographical longitude of receiver position in degrees Leading characters padded by space characters (ASCII code 20h)
`e`	Longitudinal hemisphere, with following characters possible: "E" East of Greenwich Meridian "W" West of Greenwich Meridian
`0.0,0.0`	Speed over the ground in knots and track angle in degrees. With a Meinberg GPS clock, these values are always 0.0, With GNS clocks, the values are calculated by the receiver for mobile applications
`ddmmyy`	The date: `dd` Day of Month (01–31) `mm` Month (01–12) `yy` Year of the Century (00–99)
`a`	Magnetic Variation E/W
`hh`	Checksum (XOR of all characters except "$" and "*")
`<CR>`	Carriage Return, ASCII code 0Dh
`<LF>`	Line Feed, ASCII code 0Ah

11.8.7 Format of the NMEA 0183 String (GGA)

The NMEA 0193 GGA String is a sequence of characters starting with the string "$GPGGA" and ending with the characters <CR> (Carriage Return) and <LF> (Line Feed). The format is as follows:

$GPGGA,*hhmmss.ff*,*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-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

$	Start character, ASCII code 24h sent with one-bit accuracy at the change of each second
GP	Talker ID, in this case "GP" for GPS
GGA	Message type ID, in this case "GGA"
hhmmss.ss	The time: *hh* Hours (00–23) *mm* Minutes (00–59) *ss* Seconds (00–59, or 60 while leap second) *ff* Fractions of Seconds (1/10 ; 1/100)
bbbb.bbbbb	Geographical latitude of receiver position in degrees Leading characters padded by space characters (ASCII code 20h)
n	Latitudinal hemisphere, with the following characters possible: "N" North of Equator "S" South of Equator
lllll.lllll	Geographical longitude of receiver position in degrees Leading characters padded by space characters (20h)
e	Longitudinal hemisphere, with following characters possible: "E" East of Greenwich Meridian "W" West of Greenwich Meridian
A	Position fixed (1 = yes, 0 = no)
vv	Number of satellites used (0–12)
hhh.h	HDOP (Horizontal Dilution of Precision)
aaa.h	Mean Sea Level Altitude (MSL Altitude = WGS84 Altitude - Geoid Separation)
M	Meters (unit as fixed value)
ggg.g	Geoid Separation (WGS84 Altitude - MSL Altitude)
M	Meters (unit as fixed value)
cs	Checksum (XOR of all characters except "$" and "*")
<CR>	Carriage Return, ASCII code 0Dh
<LF>	Line Feed, ASCII code 0Ah

11.8.8 Format of the NMEA 0183 String (ZDA)

The NMEA 0183 ZDA String is a sequence of 38 ASCII characters starting with the string "$GPZDA" 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 time zone.

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

$	Start character, ASCII Code 24h sent with one-bit accuracy at change of second		
hhmmss.ss	UTC time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 during leap second)
HH,II	The local time zone (offset to UTC):		
	HH	Hours	(00–±13)
	II	Minutes	(00–59)
dd,mm,yy	The date:		
	dd	Day of Month	(01–31)
	mm	Month	(01–12)
	yyyy	Year	(0000–9999)
cs	Checksum (XOR of all characters except "$" and "*")		
<CR>	Carriage Return, ASCII code 0Dh		
<LF>	Line Feed, ASCII code 0Ah		

11.8.9 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 as follows:

```
>900WD:yy-mm-tt_hh.mm;ss.fff:cc<CR>
```

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

yy-mm-tt	The date:		
	yy	Year of the Century	(00–99)
	mm	Month	(01–12)
	dd	Day of Month	(01–31)
	<SP>	Space (ASCII code 20h)	
hh.mm;ss.fff	The time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 during leap second)
	fff	Milliseconds	(000–999)
cc	Checksum calculated as XOR sum of the preceding characters. The resultant 8-bit value is reported as a hex value in the form of two ASCII characters (2 ASCII characters 0–9 or A–F)		
<CR>	Carriage Return, ASCII code 0Dh		

11.8.10 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 as follows:

`T:`*`yy:mm:dd:ww:hh:mm:ss`*`<CR><LF>`

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

`T`	Start character sent with one-bit accuracy at the change of each second		
`yy:mm:dd`	The date:		
	`yy`	Year of Century	(00–99)
	`mm`	Month	(01–12)
	`dd`	Day of Month	(01–31)
	`ww`	Day of Week	(01–07, 01 = monday)
`hh:mm:ss`	The time:		
	`hh`	Hours	(00–23)
	`mm`	Minutes	(00–59)
	`ss`	Seconds	(00–59, or 60 during leap second)
`<CR>`	Carriage Return, ASCII code 0Dh		
`<LF>`	Line Feed, ASCII code 0Ah		

11.8.11 Format of the RACAL Standard Time String

The RACAL Standard Time String is a sequence of 16 ASCII characters started by a `X` character and terminated by the `<CR>` (Carriage Return, ASCII code 0Dh) character. The format is as follows:

`XGU`*yymmddhhmmss*`<CR>`

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

`X`	Start character, ASCII code 58h Sent with one-bit accuracy at the change of each second		
`G`	Control character, ASCII code 47h		
`U`	Control character, ASCII code 55h		
`yymmdd`	Current date:		
	`yy`	Year of Century	(00–99)
	`mm`	Month	(01–12)
	`dd`	Day of Month	(01–31)
`hh:mm:ss`	Current time:		
	`hh`	Hours	(00–23)
	`mm`	Minutes	(00–59)
	`ss`	Seconds	(00–59, or 60 during leap second)
`<CR>`	Carriage Return, ASCII code 0Dh		

11.8.12 Format of the SYSPLEX-1 Time String

The SYSPLEX-1 time string is a sequence of 16 ASCII characters starting with the <SOH> (Start-of-Header) ASCII control character and terminated with the <LF> (Line Feed, ASCII code 0Ah) character.

Important!

To ensure that the time string can be correctly output and displayed through any given terminal program, a singular "C" (not include quotation marks) must be input.

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 code 01h sent with one-bit accuracy at the change of each second			
ddd	Day of Year		(001–366)	
hh:mm:ss	Current time:			
	hh	Hours	(00–23)	
	mm	Minutes	(00–59)	
	ss	Seconds	(00–59, or 60 during leap second)	
	q	Quality Indicator	Space (ASCII code 20h)	Time Sync (GPS Lock)
			"?" (ASCII code 3Fh)	No Time Sync (GPS Fail)
<CR>	Carriage Return (ASCII code 0Dh)			
<LF>	Line Feed (ASCII code 0Ah)			

11.8.13 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 code 01h) ASCII control character and ending with the `<LF>` (Line Feed, ASCII code 0Ah) character. The format is as follows:

<SOH>*ddd:hh:mm:ssq*<CR><LF>

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters as defined below:

<SOH>	Start of Header (ASCII code 01h) sent with one-bit accuracy at the change of each second			
ddd	Day of Year		(001–366)	
hh:mm:ss	Current time:			
	hh	Hours	(00–23)	
	mm	Minutes	(00–59)	
	ss	Seconds	(00–59, or 60 while leap second)	
	q	Quality Indicator	Space (ASCII code 20h) "?" (ASCII code 3Fh)	Time Sync (GPS Lock) No Time Sync (GPS Fail)
<CR>	Carriage Return (ASCII code 0Dh)			
<LF>	Line Feed (ASCII code 0Ah)			

11.8.14 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 code 01h) ASCII control character and ending with the <LF> (Line Feed, ASCII code 0Ah) character. The format is as follows:

<SOH>ddd:hh:mm:ssq<CR><LF>

Important!

The blanking interval of is 2 minutes and 30 seconds long and is added every 5 minutes.

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters as defined below:

<SOH>	Start of Header (ASCII code 01h) sent with one-bit accuracy at the change of each second			
ddd	Day of Year		(001–366)	
hh:mm:ss	Current time:			
	hh	Hours	(00–23)	
	mm	Minutes	(00–59)	
	ss	Seconds	(00–59, or 60 while leap second)	
	q	Quality Indicator	Space (ASCII code 20h)	Time Sync (GPS Lock)
			"?" (ASCII code 3Fh)	No Time Sync (GPS Fail)
<CR>	Carriage Return (ASCII code 0Dh)			
<LF>	Line Feed (ASCII code 0Ah)			

11.8.15 Format of the IRIG-J Timecode

The IRIG-J timecode consists of a string of ASCII characters sent in "701" format, i.e.,:

- 1 Start Bit
- 7 Data Bits
- 1 Parity Bit (odd)
- 1 Stop Bit

The on-time marker of the string is the leading edge of the start bit. The timecode consists of 15 characters, sent once per second at a baud rate of 300 or greater. The format is as follows:

`<SOH>`*`DDD:HH:MM:SS`*`<CR><LF>`

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

`<SOH>`	"Start of Header" (ASCII code 01h)
`DDD`	Day of the year (ordinal date, 1–366)
`HH`, `MM`, `SS`	Time of the start bit, specified in hours (`HH`), minutes (`MM`), seconds (`SS`)
`<CR>`	"Carriage Return" (ASCII code 0Dh)
`<LF>`	"Line Feed" (ASCII code 0Ah)

11.9 Supported PTPv2 Profiles

This is a list of the PTPv2 profiles supported by your product and the corresponding settings.

PTP Profile	**Operation Modes**	**OSI Layer/Network Protocol**	**PTP Domain** (Default)	**Delay Mechanism**	**Announce Receipt Timeout (Default)**	**Announce Interval (Default)**	**Sync Interval (Default)**	**(Peer) Delay Req. Interval (Default)**	**PTP Timescale Required?**
Default E2E IEEE1588-2008	Any except Mixed Master	L2/ L3	0–255 (0)	E2E	2–10 (2)	2000 ms	1000 ms	1000–128000 ms	Y
Default P2P IEEE1588-2008	Multicast	L2/ L3	0–255 (0)	P2P	2–10 (2)	2000 ms	1000 ms	1000 ms	Y
Power IEEE C37.238-2011	Multicast	L2	0–255 (0)	P2P	2–3 (2)	1000 ms	1000 ms	1000 ms	Y
Power IEEE C37.238-2017	Multicast	L2	0–127, 254 (254)	P2P	3	1000 ms	1000 ms	1000 ms	Y
Utility IEC 61850-9-3	Multicast	L2	0–255 (0)	P2P	3	1000 ms	1000 ms	1000 ms	Y
Telecom ITU-T G.8265.1	Unicast	L3	4–23 (4)	E2E	2	62.5–16000 ms (125 ms)	7.8125–128000 ms (62.5 ms)	7.8125–128000 ms (62.5 ms)	N
Telecom ITU-T G.8275.1	Multicast	L2	24–43 (24)	E2E	3–10 (3)	128 ms	62.5 ms	62.5 ms	Y
Telecom ITU-T G.8275.2	Unicast	L3	44–63 (44)	E2E	2	125–1000 ms (125 ms)	7.8125–1000 ms (7.8125 ms)	7.8125–1000 ms (7.8125 ms)	Y
DOCSIS 3.1	Multicast	L2	24–43 (24)	E2E	3–10 (3)	128 ms	62.5 ms	62.5 ms	Y

PTP Profile	Operation Modes	OSI Layer/Network Protocol	PTP Domain (Default)	Delay Mechanism	Announce Receipt Timeout (Default)	Announce Interval (Default)	Sync Interval (Default)	(Peer) Delay Req. Interval (Default)	PTP Timescale Required?
SMPTE ST 2059-2	Any	L3	0–127 (127)	Any	2–10 (2)	125–2000 ms (250 ms)	7.8125–500 ms (125 ms)	7.8125–500 ms	N
AES67 Media	Multicast	UDP/ IPv4 (L3)	0–255 (0)	Any	2–10 (2)	1000–16000 ms (2000 ms)	-62.5–2000ms (125 ms)	1000 ms–32000 ms (1000 ms)	N
IEEE 802.1AS	Multicast	L2	0	P2P	2–10 (2)	62.5–16000 ms (1000 ms)	7.8125–128000 ms (125 ms)	1000 ms	Y

11.10 SSM Quality Levels

When using SyncE, the following flags are used to denote or set the recognized SSM Quality Levels:

QL-STU/UKN: Quality unknown

QL-PRS: Primary Reference Source

QL-PRC: Primary Reference Clock

QL-INV3: Not used

QL-SSU-A/TNC: Synchronization Supply Unit A or Transit Node Clock

QL-INV5: Not used

QL-INV6: Not used

QL-ST2: Stratum 2 Clock

QL-SSU-B: Synchronization Supply Unit B

QL-INV9: Not used

QL-EEC2/ST3: Ethernet Equipment Clock 2

QL-EEC1/SEC: Ethernet Equipment Clock 1 / SDH Equipment Clock

QL-SMC: SONET Minimum Clock

QL-ST3E: Stratum 3E Clock

QL-PROV: Can be provided by network operator

QL-DNU/DUS: Do not use for synchronization

11.11 Third Party Software

11.11.1 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:

12 Your Opinion Matters to Us

This user manual is intended to assist you with the setup and use of software for use with your Meinberg product. We hope that it provides you with all of the information that you require to properly and efficiently use your Meinberg product to its fullest potential.

Be a part of the ongoing improvement of the information contained in this manual. Please contact our Technical Support team if you have any suggestions for improvements or technical questions that are relevant to the manual.

Meinberg – Technical Support

Phone: +49 (0) 5281 – 9309- 888
Email: techsupport@meinberg.de

13 List of Illustrations