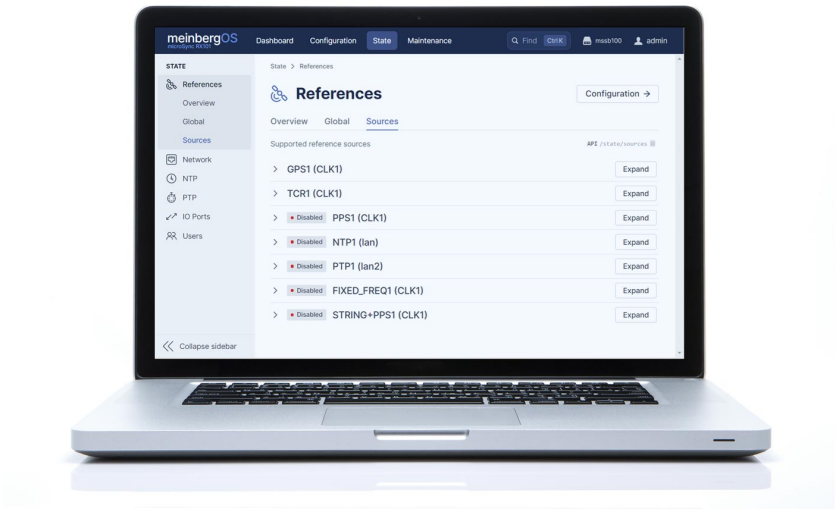
The Synchronization Experts.



MANUAL

meinbergOS 2024.12.4

Web Interface

Configuration and Management Manual

Meinberg Funkuhren GmbH & Co. KG

Table of Contents

1 Imprint and Legal Information

Publisher

Meinberg Funkuhren GmbH & Co. KG

Registered Place of Business:
Lange Wand 9
31812 Bad Pyrmont
Germany

Telephone:
+49 (0) 52 81 – 93 09 - 0

Fax:
+49 (0) 52 81 – 93 09 - 230

The company is registered in the "A" Register of Companies & Traders (Handelsregister A) maintained by the Local Court of Hanover (Amtsgericht Hannover) under the number:

17HRA 100322

Executive Management:	Heiko Gerstung Andre Hartmann Natalie Meinberg Daniel Boldt
Website:	https://www.meinbergglobal.com
Email:	info@meinberg.de

Document Publication Information

Manual Version:	1.2
Revision Date:	July 8, 2025
PDF Export Date:	August 26, 2025

2 Revision History (Manual)

The revision history relates to changes to this manual.

Version	Date	Revision Notes
1.0	2022-06-01	Initial version (based on meinbergOS *2022.05*)
1.01	2022-12-23	- Added options to use references only for time-of-day or phase sync, or not at all (statistical analysis only). - Other minor corrections.
1.1	2024-08-30	- Updated to reflect feature set of meinbergOS *2024.05* - Changes to presentation format (monospace typeface for filenames etc.) - Links to other chapters, external websites, and illustrations are now presented in a standardized format. - Added features specific to the microSync Broadcast systems.
1.2	2025-07-08	- Updated to reflect feature set of meinbergOS *2024.12.3* - Introduction reworded in light of Web Interface now being more firmly established (→ Chapter 4) - New chapter on use of deprecated and future removal of Meinberg Device Manager (→ Chapter 4.4) - Added information on new features in the system summary widget of the Header Bar (→ Chapter 5) - Improved description texts in Dashboard chapter (→ Chapter 6) - Added missing description of A/V Sync Outputs subsection to Configuration overview chapter (→ Chapter 7) - Corrected quotation marks so that they are correctly oriented and no longer straight - Added missing “Supported” entry (→ Chapter 8.1.3) - Added missing “Uptime” entry (→ Chapter 8.1.4) - Added guide on updating module firmware (→ Chapter 9.1.1) - Added guide on downgrading module firmware (→ Chapter 9.1.2) - Added information on external web and mail links (→ Chapter 4.2) - Removed redundant screenshot from “**State** → **Network**” (→ Chapter 8.4) - Clarification that exFAT file system not supported (→ Chapter 7.1.2, → Chapter 7.1.3) - More detailed description of VLAN ID rules according to IEEE 802.1Q (→ Chapter 7.5.2) - Removal of microSync-specific references in relation to the number of network ports (→ Chapter 8.2.1, → Chapter 7.5.3) - Fixed incorrect link to Meinberg Device Manager page (→ Chapter 9.2.1.3) - Fixed description of “No Signal” state of input connector (→ Chapter 8.2.1)

1.21	2025-07-18	- Updated to reflect feature set of meinbergOS *2024.12.4* - Added note regarding power supply state output in microSync^{XS} and microSync^{HR} device (➜ Chapter 8.1.3) - Reduced size of ➜ "Configuration - References" screenshot (➜ Chapter 7.2)

3 Copyright and Liability Exclusion

4 Introduction: meinbergOS Web Interface

Meinberg's microSync devices are managed using a feature-rich Web Interface that can be used to perform any configuration process quickly and easily while also allowing the device's status and condition to be monitored. It also allows new software versions to be installed and old versions to be archived.

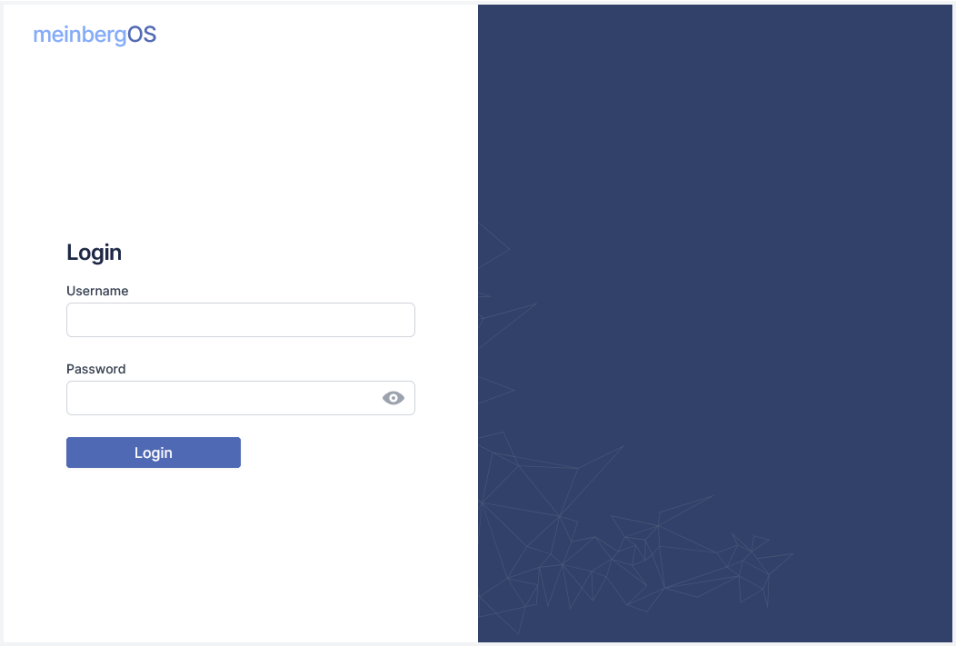


Figure 4.1: Login Page of meinbergOS Web Interface

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.

Once you have entered the IP address or hostname of your meinbergOS device into the address bar of your web browser, the login page will appear (Fig. 4.1).

The default account details are:

Username: `admin`
Password: `timeserver`

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.

Changing the Default Password

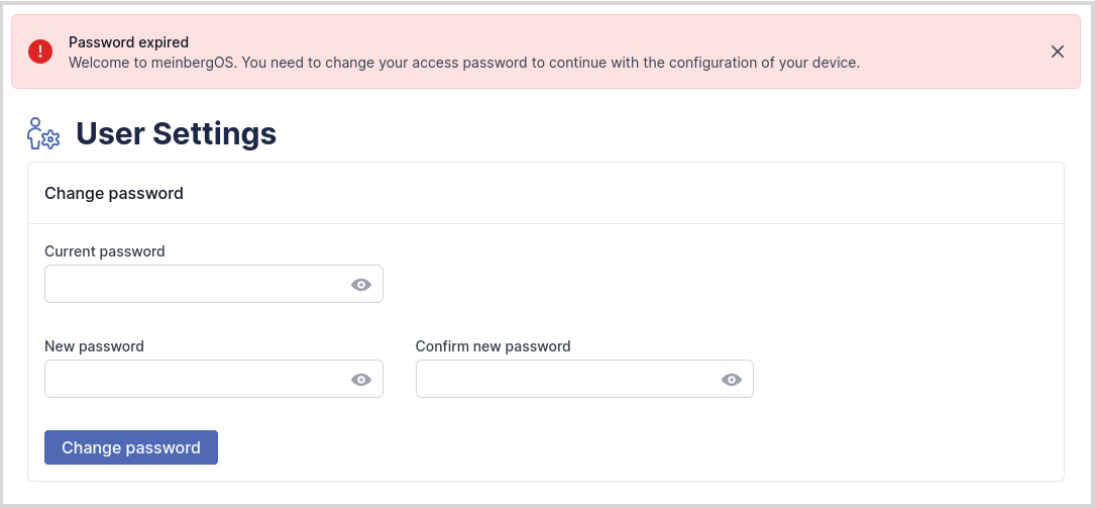


Figure 4.2: Changing the initial password

Once you have logged in for the first time, you will be prompted and required to change the default password for security reasons. Ensure that you select a secure password of at least eight characters with a mixture of uppercase, lowercase, numerical, and symbol characters. Selecting **Confirm New Password** will complete the password change process.

4.1 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.

4.2 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 → Chapter 6 ("Dashboard"), → Chapter 7 ("Configuration"), → Chapter 8 ("State"), and → Chapter 9 ("Maintenance").

Subsections of a given section of the meinbergOS Web Interface are described in second-level chapters beneath that section, for example → Chapter 7.5, "Configuration - Network".

Tabs under a subsection of the meinbergOS Web Interface are described in third-level chapters beneath that subsection, for example, → Chapter 7.5.2, "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 9.2.1.1, "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 and bold, with elements 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**.

Possible values and listed options for a configuration or status field are conventionally listed in *italics*. Example: You may select option *one*, *two*, or *three*.

Filenames, command line and other text entries are displayed in a `monospace typeface`. Example: The firmware is provided as an `.ufu` file.

References to other chapters in this manual are shown in blue, bold and with a right-facing arrow, and if the manual is viewed in a supported PDF reader, can be clicked on to directly jump to that chapter. Example: → Chapter 4.2.

Links to illustrations in the manual may also be provided, prefixed with the "Figure" symbol. Example: Fig. 4.3.

Links to external content are denoted by an external link symbol. Example: https://www.meinbergglobal.com.

Links designed to open an email client are denoted by an external mail symbol. Example: info@meinberg.de.

4.3 Basic Configuration Principles

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

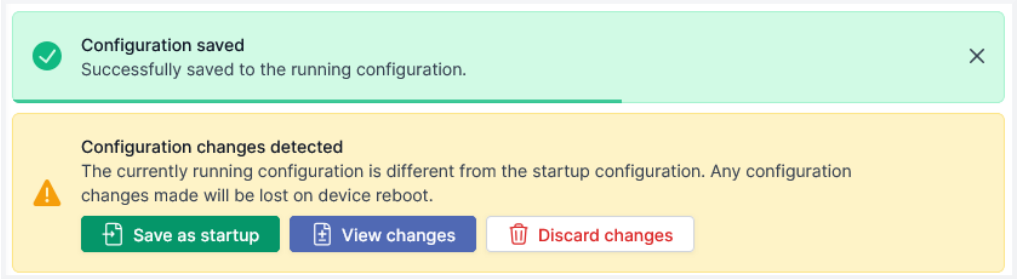


Figure 4.3: meinbergOS Web Interface: Saving Changes to the Running Configuration

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 Fig. 4.3 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. 4.3 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.

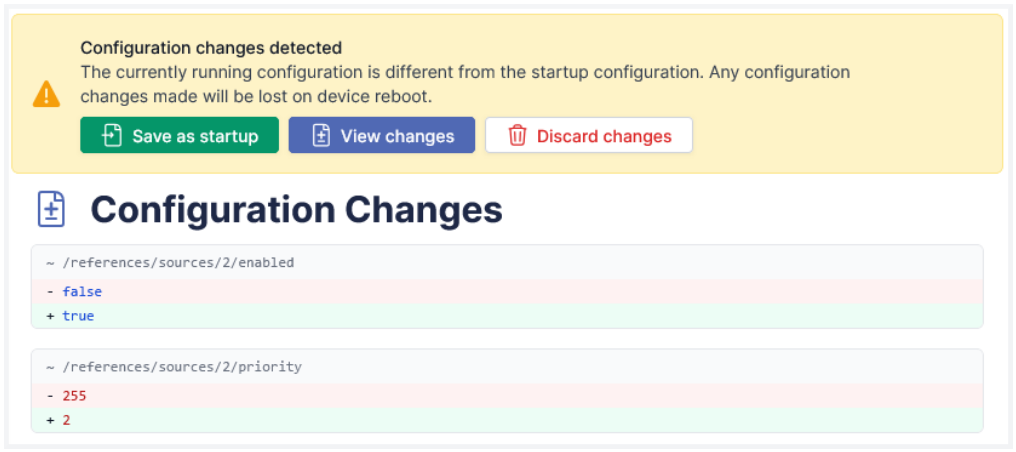


Figure 4.4: meinbergOS Web Interface: Reviewing Changes to the Configuration

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. 4.4).

To reject all changes to the configuration and re-apply the Startup Configuration, click on **Discard Changes**; note that any changes to the Running Configuration will be irrevocably lost as a result.

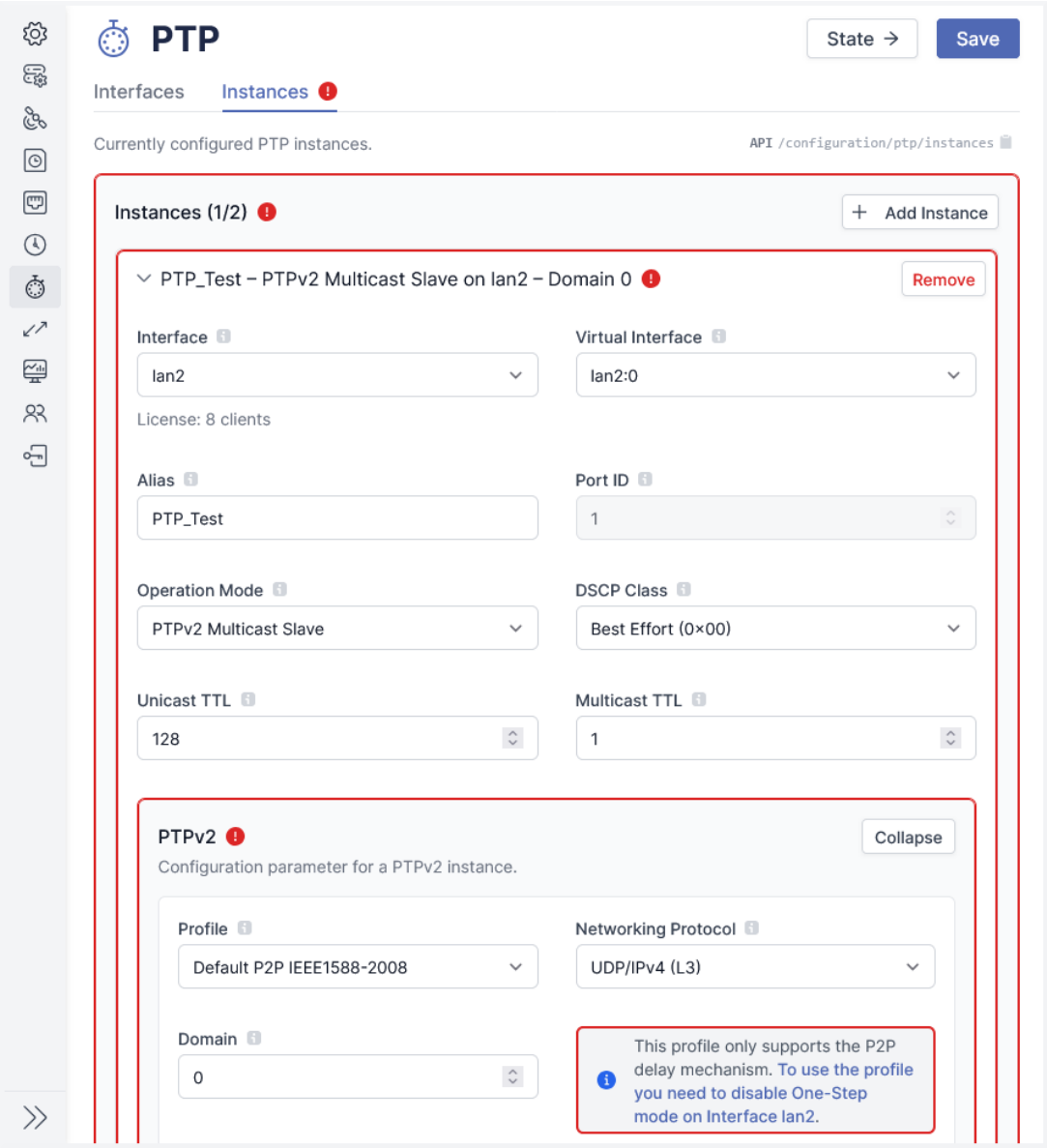


Figure 4.5: meinbergOS Web Interface: Detailed Indication of an Error in Configuration

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. 4.5 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 4.6: 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. 4.6), indicating what exactly has been changed.

4.4 Users of Meinberg Device Manager

The meinbergOS Web Interface was introduced in meinbergOS *2022.05*, marking the start of the deprecation of the use of Meinberg Device Manager for the management and monitoring of your meinbergOS device. With the release of meinbergOS *2024.05*, the meinbergOS Web Interface represented every function of the meinbergOS device and the use of Meinberg Device Manager was considered fully deprecated from this point.

The latest features introduced since meinbergOS *2024.05* are therefore not supported in Meinberg Device Manager. These include the new user management system, including support for TACACS+, LDAP, and Radius authentication, as well as a more advanced event monitoring system, which cannot be configured or monitored in Meinberg Device Manager.

The ongoing bugfixes, security fixes, and optimizations introduced into new releases of meinbergOS will also increasingly result in incompatibilities, an elevated risk of data loss, and configuration problems when continuing to manage your meinbergOS device using Meinberg Device Manager.

Support for Meinberg Device Manager is expected to be removed entirely in the next Major Release of meinbergOS. Accordingly, users of Meinberg Device Manager are strongly urged to transition to the Web Interface for management and monitoring tasks as soon as possible.

5 Header Bar

Figure 5.1: meinbergOS Web Interface: Header Bar

The **Header Bar** (Fig. 5.1) 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

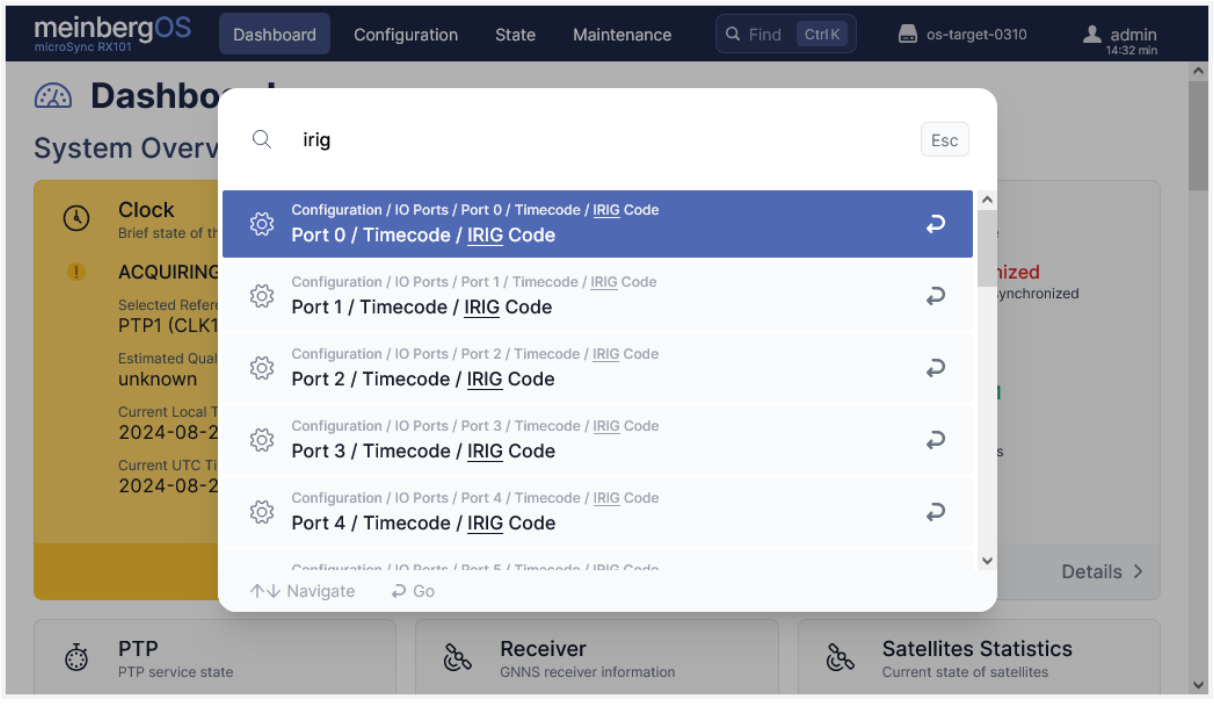


Figure 5.2: meinbergOS Web Interface: Find Anything

The **Find Anything** tool (Fig. 5.2) 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.

System Summary

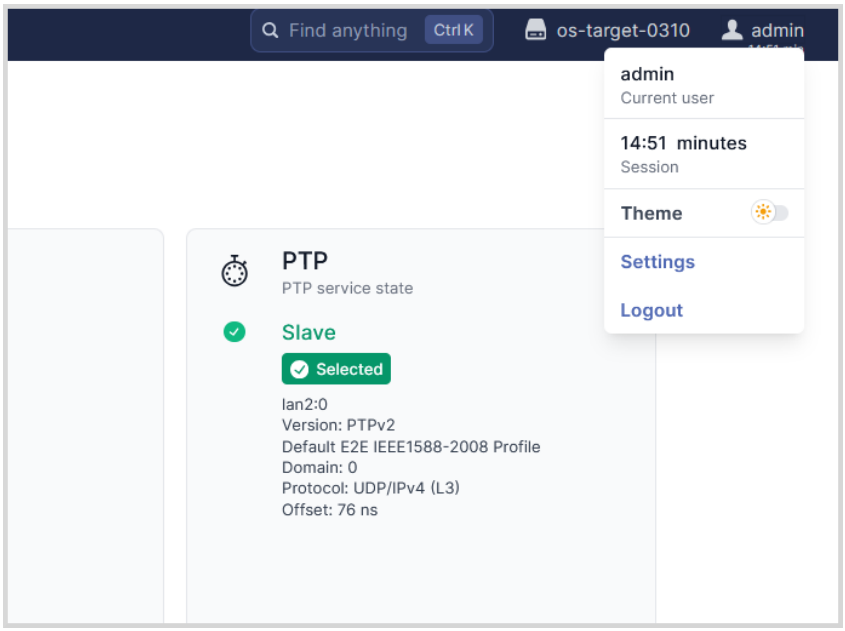


Figure 5.3: meinbergOS Web Interface: System Summary

The **System Summary** (Fig. 5.3) displays the current hostname of the meinbergOS device (*os-target-0310* in the example above) and can be selected to display information such as an overview of the currently configured network interfaces (including any information on network bonding), the current firmware version (and any available updates), the serial number, and the integrated reference clock type. It also provides direct links to update the meinbergOS firmware directly and download a diagnostic file.

User Menu

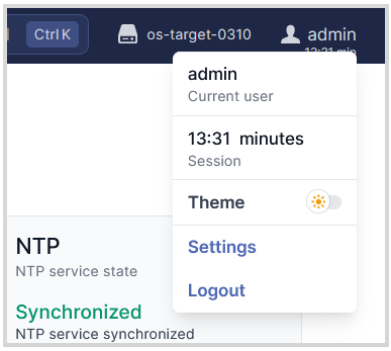


Figure 5.4: meinbergOS Web Interface: User Menu

The **User Menu** (Fig. 5.4) shows the current username and the remaining time of the current Web Interface session.

The "**Theme**" switch can be used to change the meinbergOS color scheme between *Light Mode* and *Dark Mode*. *Dark Mode* (Fig. 5.5) may be easier on the user's eyes when working in poorly lit environments.

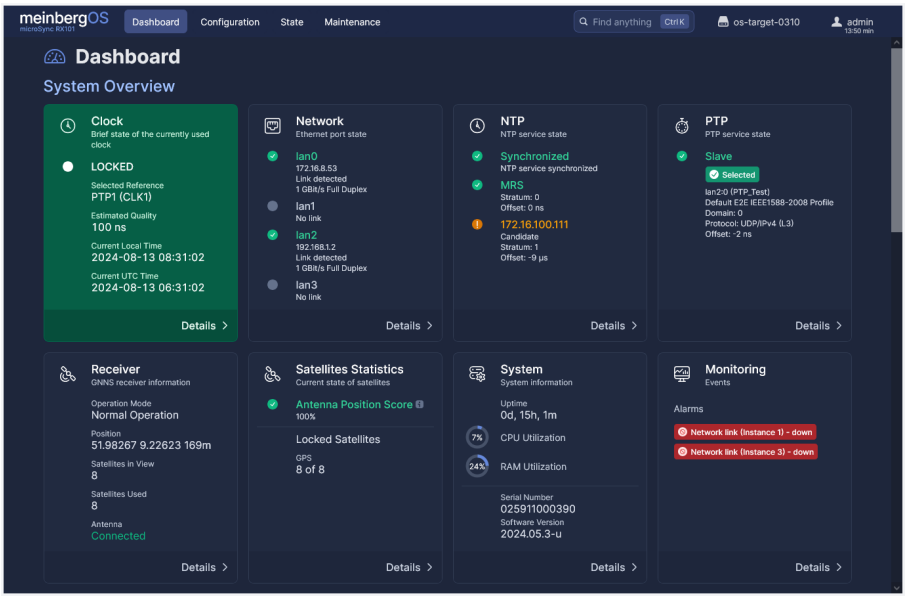


Figure 5.5: meinbergOS Web Interface: Dark Mode

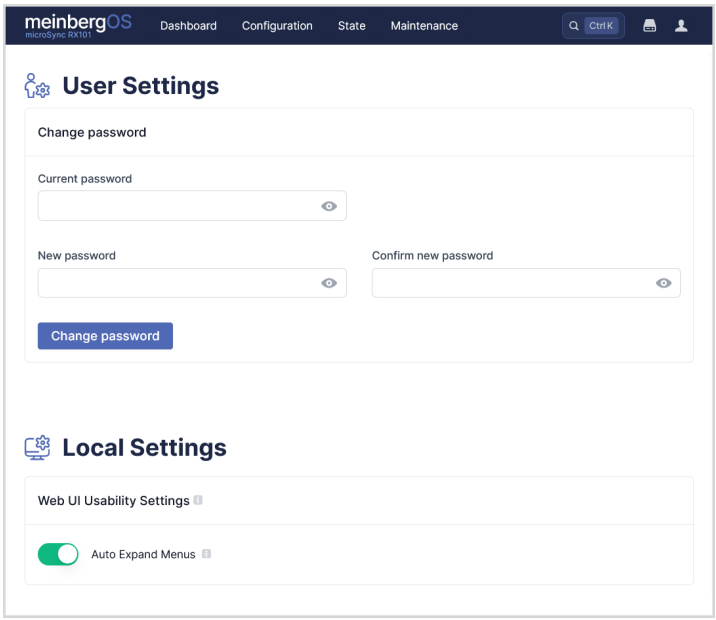


Figure 5.6: meinbergOS Web Interface: User Settings

The "**User Settings**" page (Fig. 5.6) can be used by the currently logged-in user to change their own password, which Meinberg expressly recommends doing once the system is set up.

Enabling the "**Auto Expand Menus**" option under **Web UI Usability Settings** will cause every collapsible panel element in the Web Interface to be expanded by default when a new page is opened.

6 Dashboard

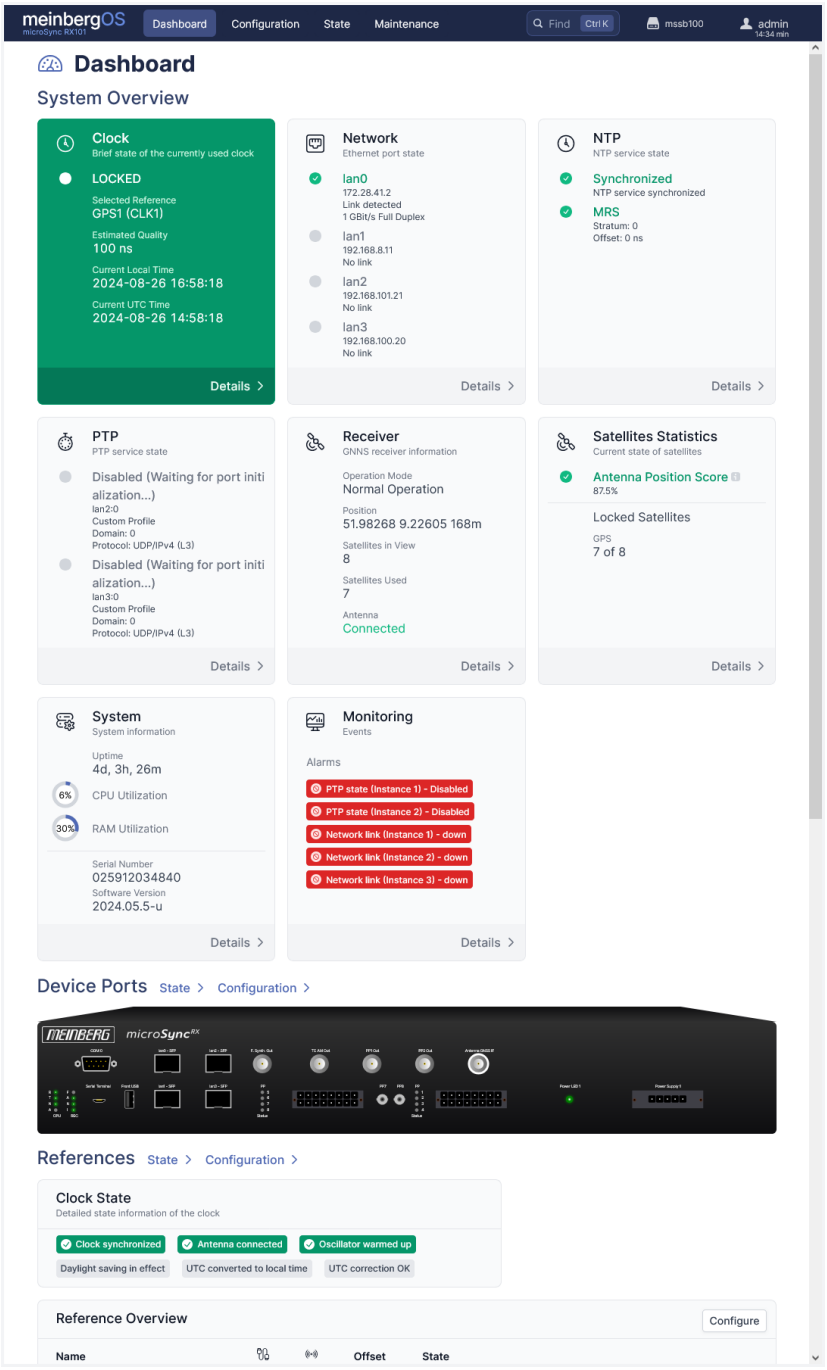


Figure 6.1: meinbergOS Web Interface Dashboard

The **Dashboard** (Fig. 6.1) provides an overview of the most important system information, including:

Clock:

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.

More information: → Chapter 8.2, "State - References" and → Chapter 8.3, "State - Receiver".

Network:

This tile shows a brief overview of the available network ports, including their link states and link modes displayed beneath each entry:

Green check mark: An active and functional network link has been detected on this network port. In this case, the link mode and, if appropriate, IP address will be displayed here.

Gray: No network link has been detected on this network port.

More information: → Chapter 8.4, "State - Network"

NTP:

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

Green check mark: The server is currently being used as a reference source.

Yellow exclamation mark: The server is reachable, but it is currently only a candidate reference and not in use as a reference source.

Red prohibition symbol: The server is not reachable by the meinbergOS device.

More information: → Chapter 8.5, "State - NTP"

PTP:

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

Gray circle: The instance of the PTP service is currently listening for other reachable clocks.

Yellow exclamation mark: The instance is either in Passive Mode or is an uncalibrated slave.

Green check mark: The instance is communicating with other PTP clocks in the network as a Master or Slave.

More information: → Chapter 8.6, "State - PTP"

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, and, if an antenna is connected, the number of satellites in view, and the number of satellites currently in use.

More information: → Chapter 8.3, "State - Receiver"

Satellites Statistics: This tile, which only appears if a valid antenna connection has been detected, provides statistics on the current satellite reception, including the *Antenna Position Score*.

More information: → Chapter 8.9, “State - Statistics”

System: This tile provides system information such as the current CPU usage, current meinbergOS version, serial number, and firmware version.

More information: → Chapter 8.1, “State - System”

Monitoring: This tile displays the last three *unacknowledged* alarms of particular relevance generated by the monitoring system. These potentially important alerts can be *acknowledged* by selecting the associated checkbox to hide them.

More information: → Chapter 8.8, “State - Monitoring”

Device Ports: This is a visual representation of your meinbergOS device. Each port can be hovered over with the cursor to provide a brief overview of the port, or clicked on to open the corresponding configuration section.

More information: → Chapter 8.7, “State - I/O Ports”

Clock State: This tile provides general information about the clock’s current state, including synchronization, UTC and Daylight Saving Time states.

More information: → Chapter 8.2, “State - References”

Reference Overview: This tile provides a general overview of all references supported by the meinbergOS device, whether a suitable reference source is connected, whether a signal is being received from that reference source, their current state flags, and their current offset.

More information: → Chapter 8.2, “State - References”

Interface Overview: This tile provides a more detailed overview of the current state of the system’s virtual interfaces, including their assigned addresses and their link state.

More information: → Chapter 8.4, “State - Network”

7 Configuration

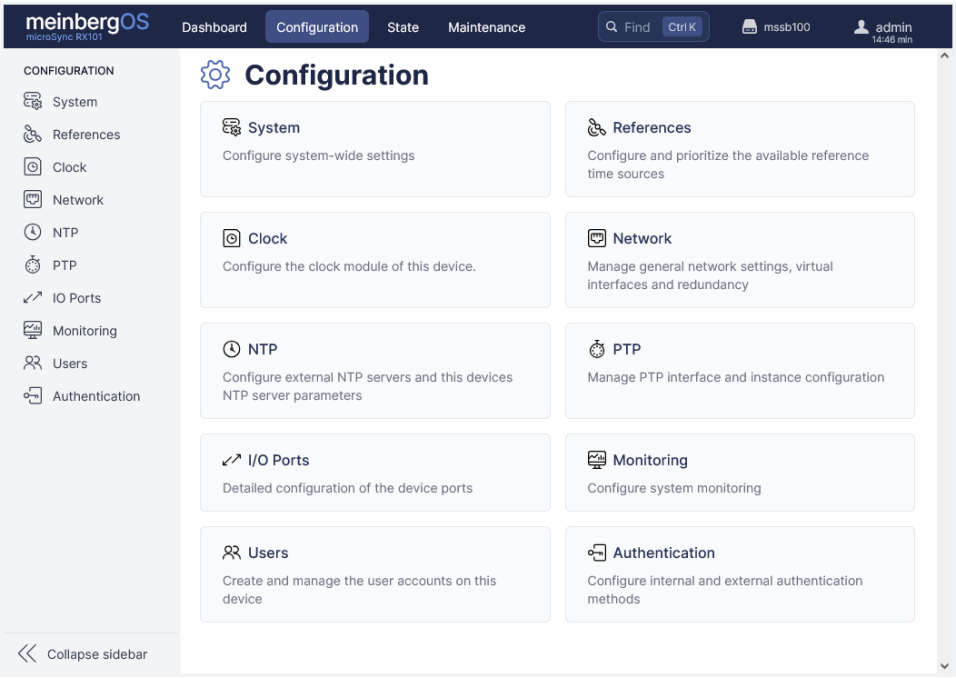


Figure 7.1: meinbergOS Web Interface: "Configuration" Section

The **Configuration** section (Figure Fig. 7.1) is where the fundamental system parameters are configured and managed.

Any changes to these subsections must generally be saved manually using the **Save** button at the top right or bottom left of the page, which applies any unsaved changes to the **Running Configuration** (see also → Chapter 4.3, "Basic Configuration Principles").

Any changes in a given subsection that have not yet been saved can be reverted to those of the current **Running Configuration** using the **Reset** button.

In many subsections, the **State** button at the top right provides easy access to the corresponding subsection in the **State** section, insofar as one exists.

System: This subsection accommodates a number of general system settings related to the meinbergOS web server, the use of external storage media, and the ability to execute a factory reset or configuration backup from the device's front panel.

More information: → Chapter 7.1, "Configuration - System"

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.

More information: → Chapter 7.2, "Configuration - References"

Clock: This subsection provides a number of receiver and I/O related options for your meinbergOS device's clock module, in particular relating to GNSS reception and the synchronization conditions for signal output.

More information: → Chapter 7.3, "Configuration - Clock"

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).

More information: → Chapter 7.5, "Configuration - Network"

A/V Sync Outputs: The A/V Sync Outputs is used to configure the A/V synchronization signal output capability of your meinbergOS device. This largely only relates to the time zone adjustments of A/V clock signals in general; individual A/V outputs are configured via the I/O Ports subsection (→ Chapter 7.8, "Configuration - I/O Ports").

Note: This subsection is only available on devices with an integrated I/O Video Signal Generator module (microSync HR7, RX7, RX8, TRX series).

More information: → Chapter 7.4, "Configuration - A/V Sync Outputs"

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.

More information: → Chapter 7.6, "Configuration - NTP"

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.

More information: → Chapter 7.7, "Configuration - PTP"

I/O 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.

More information: → Chapter 7.8, "Configuration - I/O Ports"

Monitoring: This subsection allows event monitoring and notifications via SNMP and syslog to be configured.

More information: → Chapter 7.9, "Configuration - Monitoring"

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

More information: → Chapter 7.10, "Configuration - Users"

Authentication: The **Authentication** subsection allows LDAP, RADIUS, and TACACS+ authentication to be enabled and configured, and also permits local authentication to be disabled if necessary and desired.

More information: → Chapter 7.11, "Configuration - Authentication"

7.1 Configuration - System

This subsection provides a number of miscellaneous system-wide options that relate to general system operation, grouped into three tabs: **Web Server**, **Storage**, and **Front Panel Actions**.

Web Server: This contains options related to the web server used for the meinbergOS Web Interface and REST API.

More information:

→ Chapter 7.1.1, "Configuration - System - Web Server"

Storage: This tab hosts options relating to the handling of external storage media (e.g., USB drives).

More information:

→ Chapter 7.1.2, "Configuration - System - Storage"

Front Panel Actions: This tab relates to the configuration of the factory reset and configuration backup functionality from the front panel.

More information:

→ Chapter 7.1.3, "Configuration - System - Front Panel Actions"

7.1.1 Configuration - System - Web Server

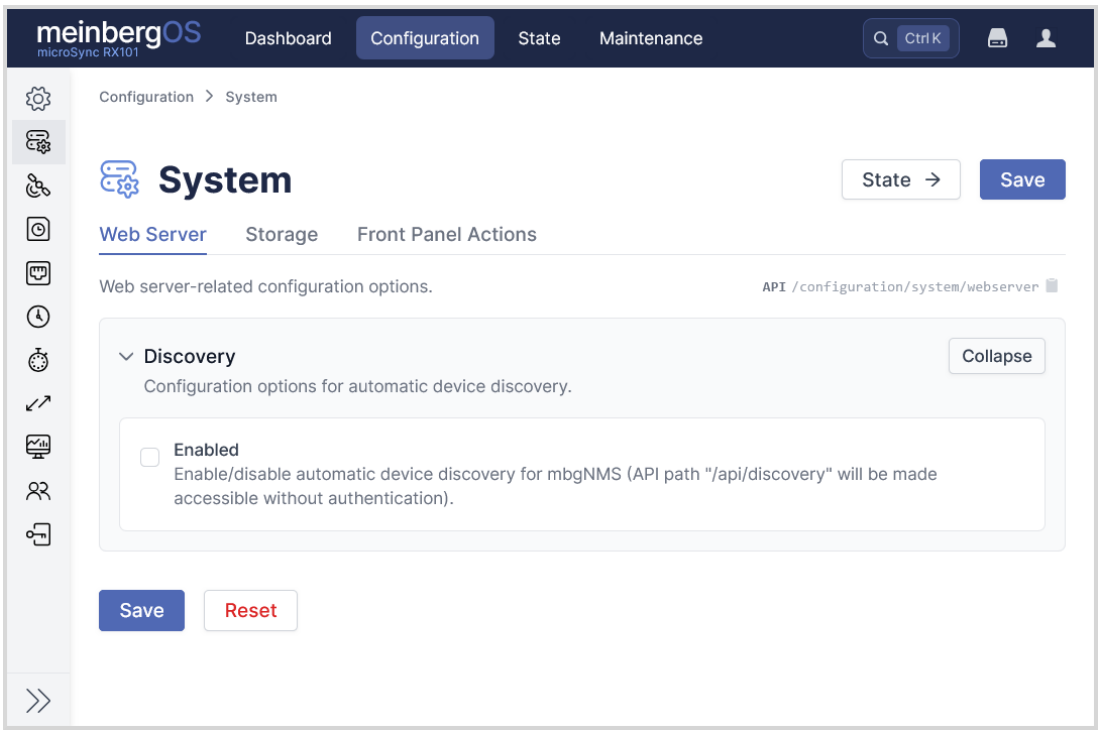


Figure 7.2: meinbergOS Web Interface: "Configuration → System → Web Server" Tab

Discovery: If enabled, the meinbergOS device will be advertised over the network to the automatic device discovery functionality of mbgNMS by exposing the API endpoint `/api/discovery` without any need for authentication.

7.1.2 Configuration - System - Storage

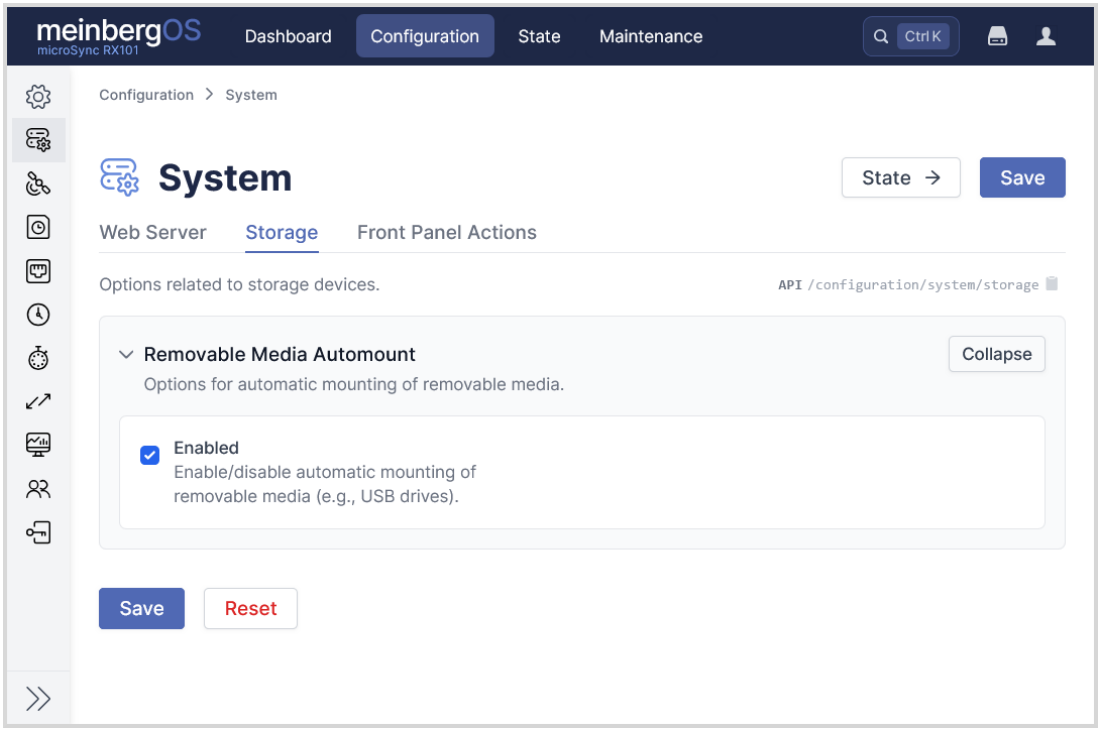


Figure 7.3: meinbergOS Web Interface: "Configuration → System → Storage" Tab

Removable Media Automount:

If enabled, meinbergOS will automatically mount any external storage media connected to the meinbergOS device via a USB port. This is required, for example, when copying data between the meinbergOS device and an external hard disk or flash drive.

It is also required for the → "Configuration - System - Front Panel Actions" functionality.

Any partitions on devices mounted in this fashion will be mounted to subdirectories of `/media`.

meinbergOS supports partitions on USB storage media formatted with ext2, ext3, ext4, FAT32, or NTFS file systems. Note that the exFAT file system is **not** supported.

7.1.3 Configuration - System - Front Panel Actions

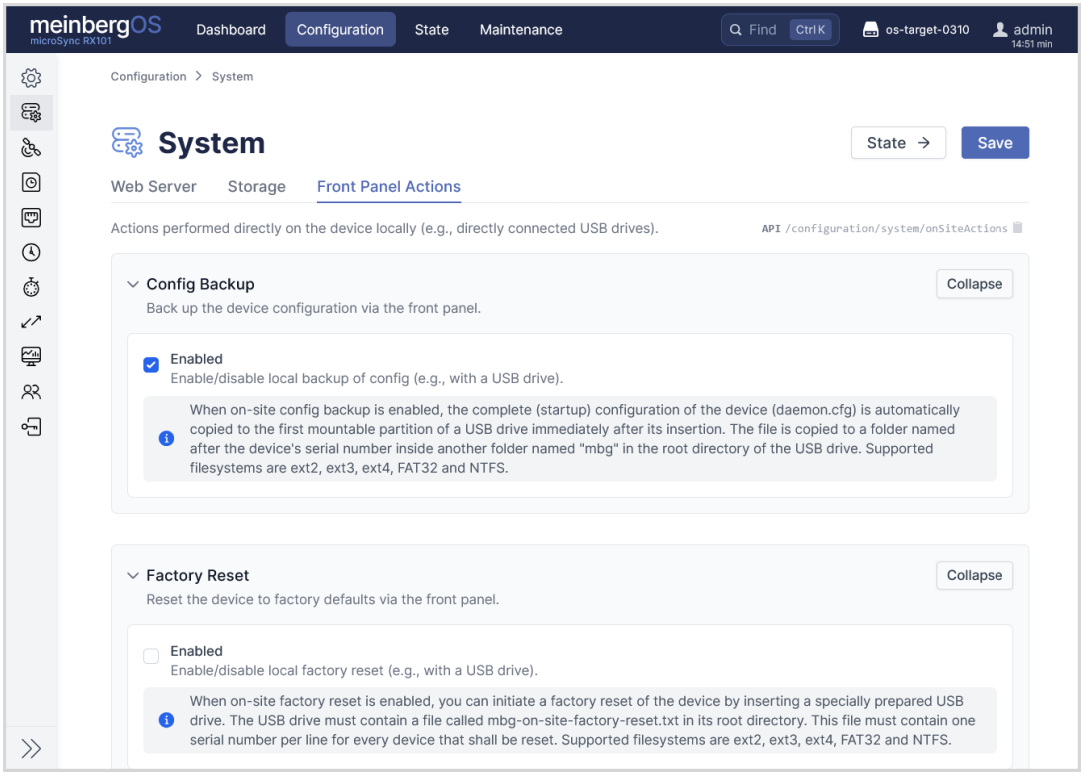


Figure 7.4: meinbergOS Web Interface: "Configuration → System → Front Panel Actions" Tab

Important!

The option **Removable Media Automount** under → Chapter 7.1.2, "Configuration - System - Storage" must be *enabled* before the Front Panel Config Backup or Factory Reset functionality can be activated.

Config Backup

Security Risk

Enabling the **Config Backup** option represents a **physical security risk** of **medium severity**; any adversary with physical access to the meinbergOS device and a USB storage medium will be able to acquire a copy of the device configuration, including a list of user accounts, encrypted passwords, and software license information.

If this option is enabled, the implementation of access control measures, in which physical access to the meinbergOS device is restricted, is strongly recommended.

Enabled:

If enabled, a backup of the configuration of this meinbergOS device to a USB storage medium can be triggered by inserting a suitably formatted USB storage medium. This will generate a folder on the storage medium named `mbg` and a subfolder within that folder with the serial number of the meinbergOS device, into which the configuration backup `daemon.cfg` (typically not larger than 50 kB in size) will be copied.

If the meinbergOS device is able to successfully copy the configuration backup to the USB storage medium, the **Alarm** LED will flash *green* three times. If the backup process fails for any reason, the **Alarm** LED will flash *red* three times.

meinbergOS supports partitions on USB storage media formatted with ext2, ext3, ext4, FAT32, or NTFS file systems. Note that the exFAT file system is **not** supported.

Factory Reset

Security Risk

Enabling the **Factory Reset** option represents a **physical security risk** of **high severity**; any adversary with physical access to the meinbergOS device and a prepared USB storage medium will be able to trigger a factory reset of the device with the potential of massive disruption to timing-sensitive infrastructure.

The information required to prepare the USB storage medium (the serial number) is typically printed on the device.

Accordingly, if this option is enabled, the implementation of access control measures, in which physical access to the meinbergOS device is restricted, is strongly recommended.

Enabled:

If enabled, a factory reset of this meinbergOS device can be triggered by inserting a specially prepared USB storage medium. This USB storage medium must contain a text file named `mbg-on-site-factory-reset.txt` in the root directory of any partition. This file must contain the serial number of the device on its own line in the text file for this USB device to be able to trigger a factory reset. This text file can contain multiple serial numbers (one per line) to allow a single USB drive to be used to perform a local factory reset on multiple meinbergOS devices; each of these devices must, of course, have **Factory Reset** enabled in the **Front Panel Actions** tab from the device itself.

meinbergOS supports USB storage media formatted with ext2, ext3, ext4, FAT32, or NTFS file systems. Note that the exFAT file system is **not** supported.

7.2 Configuration - References

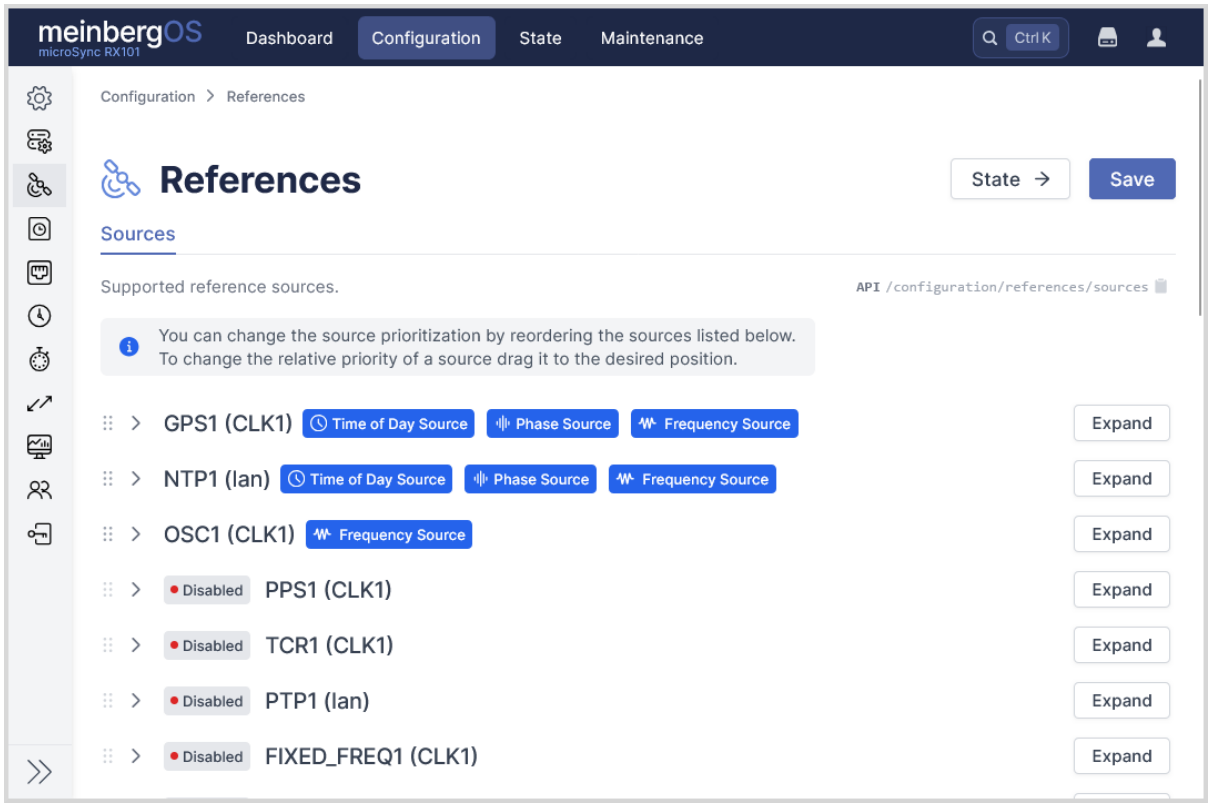


Figure 7.5: meinbergOS Web Interface: "Configuration → References" Subsection

This list in this subsection (Fig. 7.5) 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 specific signals available as reference sources will depend on your meinbergOS device; please consult your meinbergOS device's documentation for more information. However, all meinbergOS devices feature a reference source named **OSC1**; this is unique in that it forces the device to operate in Holdover Mode. This can be useful in conjunction with the **Precision** option described below for enforcing a temporary holdover period before a backup reference source is used, especially if the disciplined oscillator is known to be more accurate than the next reference source over a defined period of time (after which drift is assumed to take hold and it therefore becomes advisable to resyntonize the oscillator).

Each reference source in the list has up to three indicator badges alongside it that show if the reference source has been selected in this section as a candidate for the time-of-day, phase, and/or frequency reference, or if the reference source is only used for statistical analysis or an initial time-of-day adjustment.

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

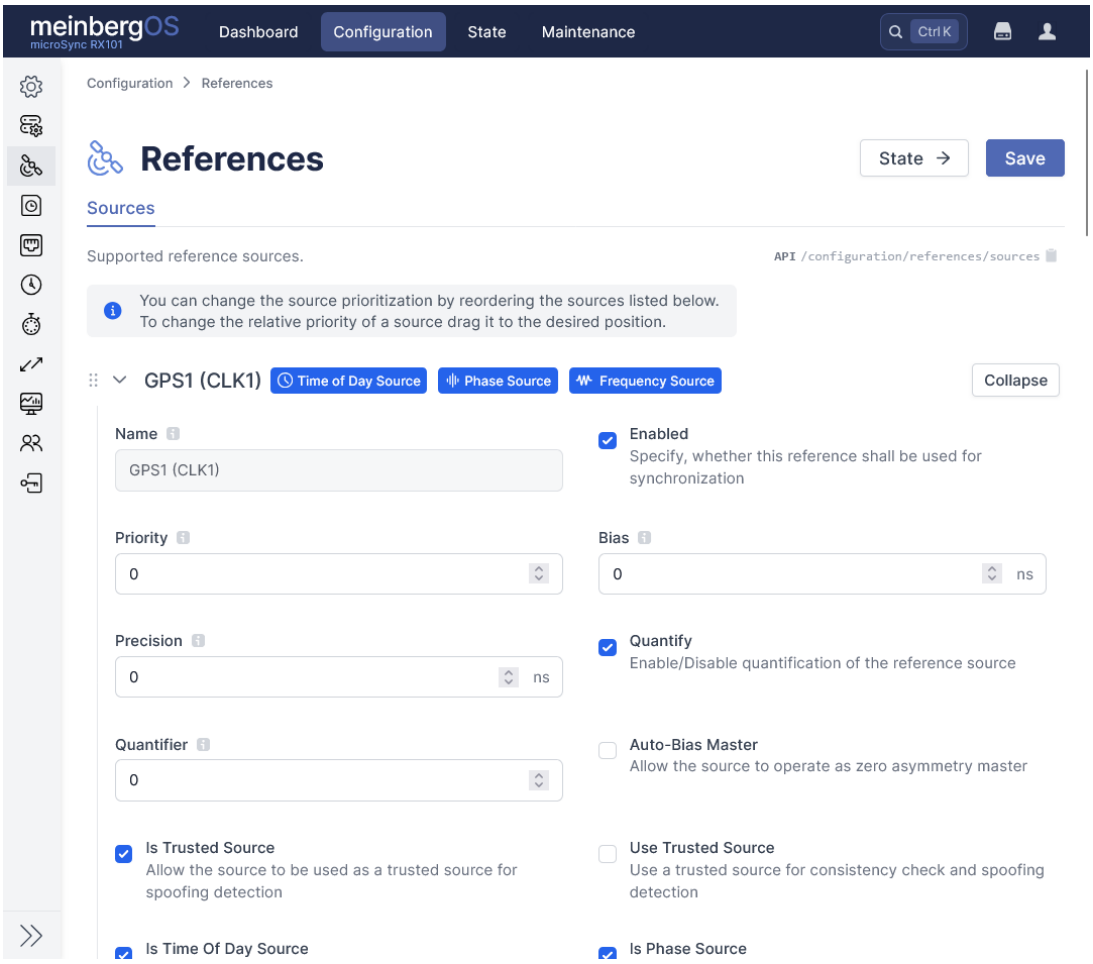


Figure 7.6: meinbergOS Web Interface: Expanded Reference Source

The configuration options for each reference source can be displayed by clicking on the panel or the corresponding **Expand** button (Fig. 7.5). 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. 7.6).

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. It is often inadvisable to switch straight from a more precise reference to a less precise one right after losing synchronization with a precise source, especially if the oscillator is disciplined. If the time inaccuracy caused by a drift in the holdover source is less than the fundamental precision of the 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.

Information:

Please note that the options "**Is Time of Day Source**" and "**Is Phase Source**" only limit which sources are used as time-of-day and phase sources if at least one reference source has this option enabled.

If no reference sources have "**Is Time of Day Source**" enabled, all active and functional reference sources capable of operating as a time-of-day reference will be considered as master time-of-day reference candidates.

Similarly, if no reference sources have "**Is Phase Source**" enabled, all active and functional reference sources capable of operating as a phase reference will be considered as master phase reference candidates.

Fast Lock:
(GPS, GNSS, PPS only) If enabled, the reference clock will adjust its frequency more rapidly, which may entail some initial frequency stability. Typically, this will allow a frequency lock to be achieved within 10 to 15 minutes. Note that this option only applies to the initial adjustment of the integrated oscillator; once the oscillator has been fully adjusted, the reference clock firmware will revert to the conventional approach of gradual adjustments.

Initial ToD:
(NTP only) If enabled, NTP will only be used as an initial time-of-day reference to set the time of day of the clock once. After the initial adjustment, the reference clock will use the next reference source in the order of priority for synchronization. Note that it requires NTP to be set as the Priority 0 reference.

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.

Reinitialize ToD Option:	This button allows a subsequent time-of-day synchronization to be performed manually with the NTP reference without having to restart the meinbergOS device. This can be useful for testing purposes or if drift in any primary frequency/phase sources results in time-of-day discrepancies.

7.3 Configuration - Clock

This subsection allows you to configure the receiver of your meinbergOS device's reference clock, specify the conditions under which the reference clock generates reference signals, configure the format of incoming time code signals, and adjust the time zone for conversion from UTC.

I/O Config: This tab provides options that govern the output of synchronization signals by the reference clock, including whether the clock should wait for synchronization or should output signals immediately. It also provides options for timecode and frequency synthesizer I/O.

More information: → Chapter 7.3.1, "Configuration - Clock - I/O Config"

Receiver: The **Receiver** tab contains a number of options that govern how an integrated receiver receives reference signals (e.g., GNSS signals), the handling of signal propagation delays over coaxial cable, and the timing loop adjustment behavior.

More information: → Chapter 7.3.2, "Configuration - Clock - Receiver"

Time Zone: This tab provides options that govern time zone and Daylight Saving Time handling, as well as the timescale used by the reference clock.

More information: → Chapter 7.3.3, "Configuration - Clock - Time Zone"

Initialization: This tab provides a number of options related to the re-initialization of the GNSS receiver and reference clock time.

More information: → Chapter 7.3.4, "Configuration - Clock - Initialization"

7.3.1 Configuration - Clock - I/O Config

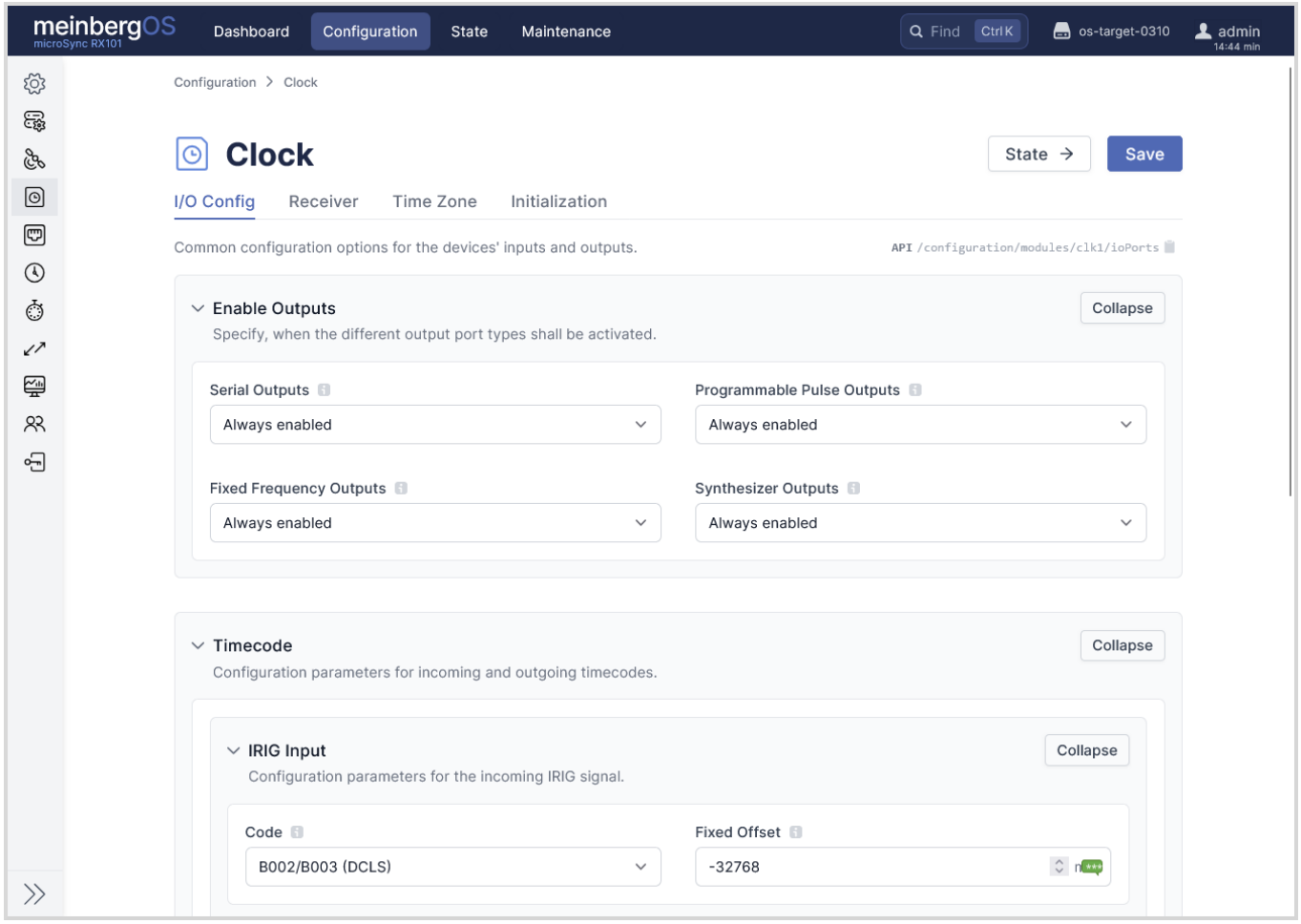


Figure 7.7: meinbergOS Web Interface: "Configuration → Clock - I/O Config" Tab

Enable Outputs

The **Enable Outputs** panel allows the output behavior of the signal outputs to be configured based on the synchronization state of the reference clock:

Serial Outputs: If this is set to *If Synchronized*, the serial string output will only be enabled when the reference clock is synchronized for the first time after a system start or reboot. If set to *Always Enabled*, serial strings will always be output via the serial interface, regardless of the synchronization state of the reference clock.

Programmable Pulse Outputs: If this is set to *If Synchronized*, the programmable pulse outputs will only be enabled when the reference clock is synchronized for the first time after a system start or reboot. If set to *Always Enabled*, programmable pulse signals will always be output, regardless of the synchronization state of the reference clock.

Fixed Frequency Outputs: If this is set to *If Synchronized*, the *fixed* frequency outputs (i.e. 10 MHz output, excluding the frequency synthesizer outputs) will only be enabled when the reference clock is synchronized for the first time after a system start or reboot. If set to *Always Enabled*, the fixed frequency signals will always be output, regardless of the synchronization state of the reference clock.

Synthesizer Outputs: If this is set to *If Synchronized*, the *synthesizer* frequency outputs will only be enabled when the reference clock is synchronized for the first time after a system start or reboot. If set to *Always Enabled*, the configured synthesizer frequency will always be output, regardless of the synchronization state of the reference clock.

Timecode

The **Timecode** panel allows timecode input and output behavior to be configured.

IRIG Input

Code: Specifies the timecode format that the IRIG input of your meinbergOS device should expect.

Fixed Offset: Specifies a manual offset from UTC that should be applied to the incoming timecode. This may be necessary for IRIG or AFNOR timecode delivered with an offset to UTC (such as a specific time zone), as these timecode formats do not contain time zone information.

IRIG Output

Code: Specifies the timecode format to be output via timecode outputs and programmable pulse outputs of your meinbergOS device.

Use Local Time: Normally, timecode such as IRIG is output as UTC. This can be overridden by enabling this checkbox, which will result in the current time zone offset being applied to the output time.

Synthesizer

Enabled: If checked, this activates frequency synthesizer output and displays the configuration parameters in this panel for frequency output.

Frequency: The frequency to be generated by the frequency synthesizer in Hz. This value must be in a range of `0.1` to `1,000,000` Hz (10 MHz). Frequencies of less than 1000 Hz may have a single decimal place applied, whereby the actual frequency will be rounded up to the next half, third, or quarter fraction, i.e., if `500.3` is entered, the synthesizer will generate a frequency of *(500 + 1/3) Hz*.

Note that the frequency synthesizer is designed to provide increased flexibility at the expense of minimal frequency instability. If you wish to output a 10 MHz frequency, please consider using the standard 10 MHz output instead, which provides a lower jitter compared to the synthesizer output.

Phase: If the output frequency is lower than 10,000 Hz (10 kHz), this parameter can be used to manually adjust the phase of the signal within a range of `0` to `359` degrees.

7.3.2 Configuration - Clock - Receiver

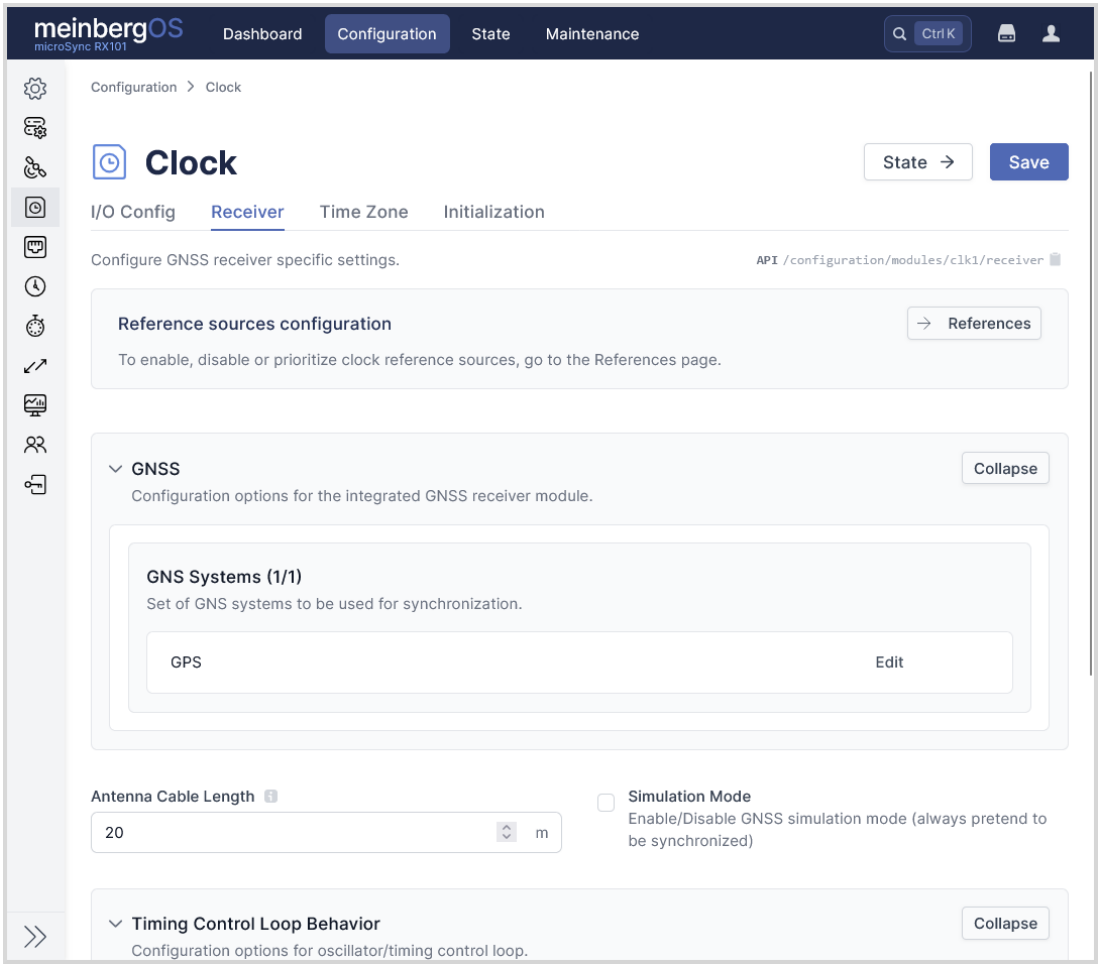


Figure 7.8: meinbergOS Web Interface: "Configuration → Clock → Receiver" Tab

GNS Systems: If your meinbergOS device features a "GNS" or ""GNS-UC" type receiver, this option allows you to select which GNSS constellations will be used for satellite reception. If your meinbergOS device features a "GPS" type receiver, the only option available here will be "GPS".

Antenna Cable Length: This value, specified in meters, is used to calculate the propagation delay of the signal along the cable between the GNSS antenna and the receiver. If your meinbergOS device features a "GPS" or "GNS-UC" type receiver, it will assume that you are using RG58 coaxial cable and assume a delay of 5 ns per meter of cable. If your meinbergOS device features a "GNS" type receiver, it will assume that you are using Belden H155 coaxial cable and assume a delay of 4 ns per meter of cable.

If you are using a GNSS signal splitter or distributor with a known signal delay of 4 ns or greater, this cable length can be adjusted to account for this processing delay accordingly. For example, if your GNSS signal splitter exhibits a delay of 22 ns and you are using a "GPS" type receiver, you can add a notional value of 4 meters to the cable length to compensate for 20 ns.

Simulation Mode: If enabled, the meinbergOS device will simulate a synchronized state at all times. This is useful, for example, if you wish to test certain functions of meinbergOS without connecting a properly installed antenna.

Timing Control Loop Behavior:

This option provides a number of presets that control how the reference clock synchronizes its internal oscillator to the reference signal and the conditions under which loss of phase-lock is assumed. By default, the reference clock assumes that the oscillator is no longer phase-locked if the reference signal and reference clock have an offset of greater than 10 μs, and will not adjust the clock in steps of any greater than 1000 ps per second.

This can be changed to the "**Power Utility Automation**" preset, where the oscillator is still considered phase-locked at an offset of 50 μs and corrections will be performed at a faster rate of up to 2500 ps per second, or to the "**Broadcast**" preset, at which adjustments will only be made with a maximum offset of 25 μs, the oscillator only retains its phase-locked state with a maximum offset of 25 μs, and corrections are performed at a rate of up to 2500 ps per second.

7.3.3 Configuration - Clock - Time Zone

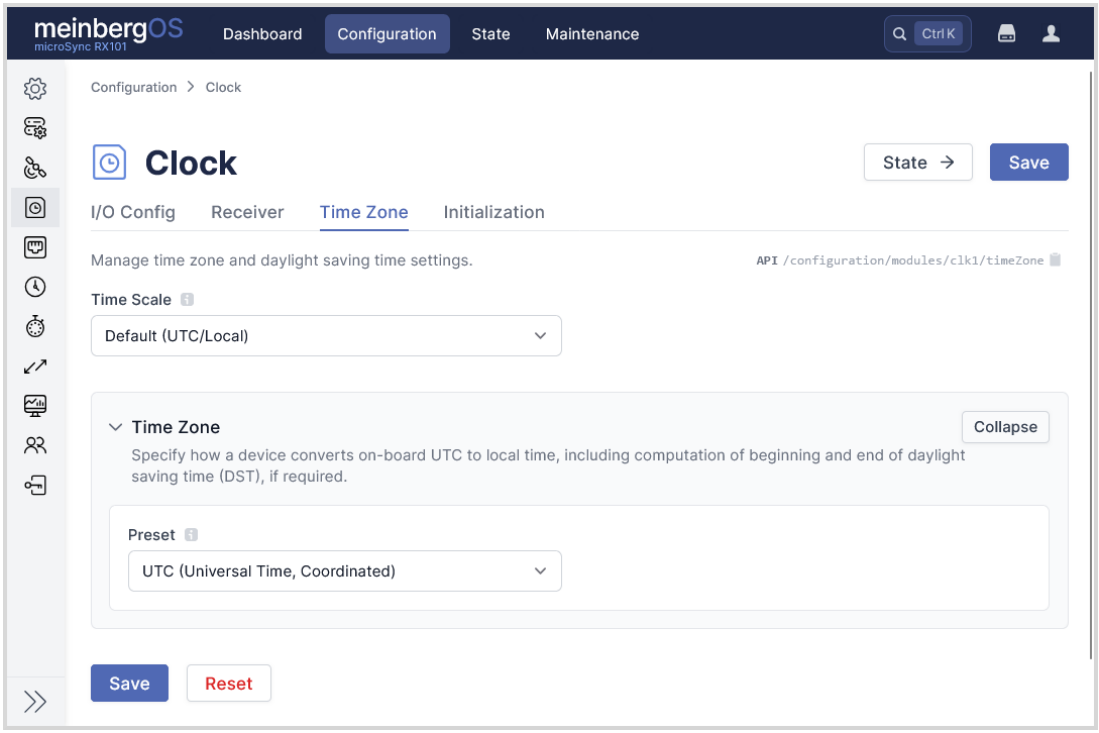


Figure 7.9: meinbergOS Web Interface: "Configuration → Clock - Time Zone" Tab

This tab is used to define which timescale and time zone is used by the reference clock for time-of-day output signals.

Time Scale: By default, your reference clock uses UTC/local time. However, if your application relies on GPS time or TAI, this can be set here to apply the appropriate offset.

Information:

Please note that the time zone settings described below will be disregarded if the time scale is set to anything other than *UTC/Local Time*.

Time Zone

Preset: This provides a selection of time zone presets for non-UTC time-of-day outputs. These presets govern the time offset relative to UTC as well as any date-specific time adjustments (Daylight Saving Time, Standard Time). You may also select the option *Custom* to define a time zone not included in the presets (see Fig. 7.10 below).

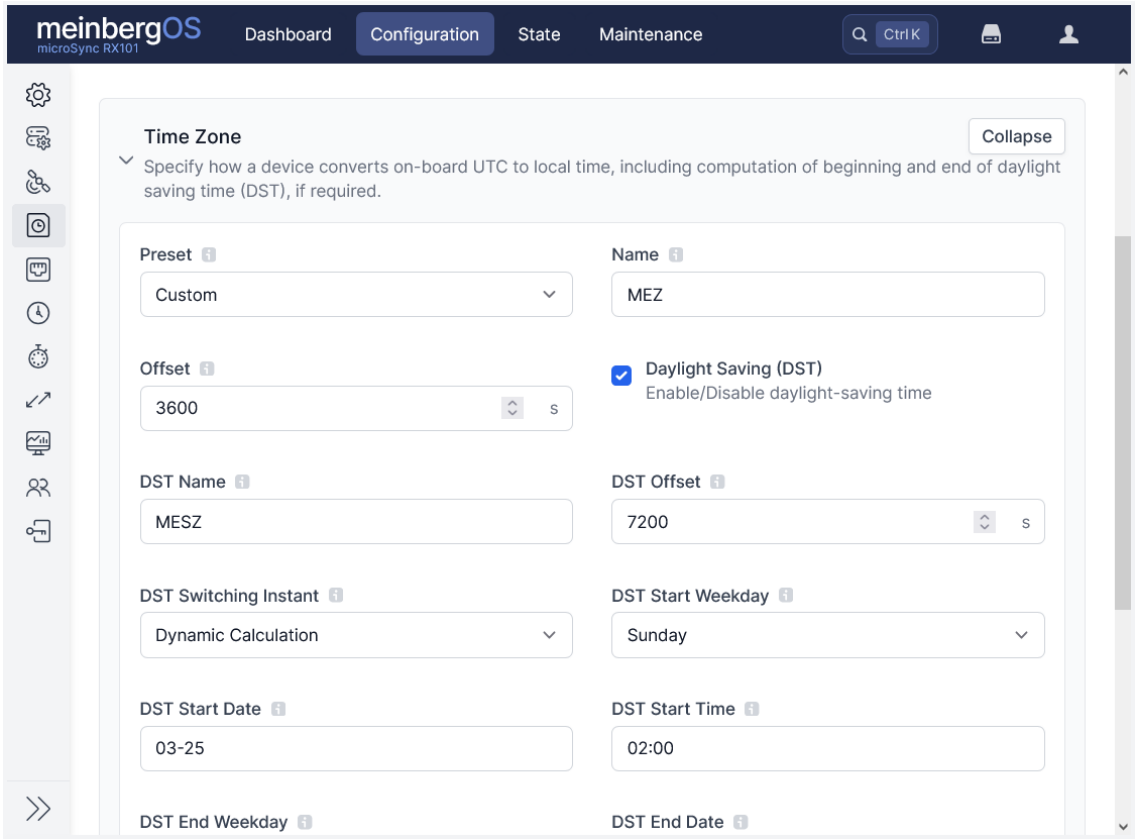


Figure 7.10: meinbergOS Web Interface: Custom Time Zone in "Configuration → Clock → Time Zone" Panel

Custom Time Zone

When defining a custom time zone, the name, offset and Daylight Saving Time conditions must be defined.

Name: This is used to specify a name for the custom time zone.

Offset: This is used to specify the offset in whole seconds of the custom time zone relative to UTC (3600 seconds = 1 hour). Negative values must be prefixed with a minus symbol.

Daylight Saving (DST): If enabled, this time zone will observe switching between a Standard Time and an Alternate Time (typically Daylight Saving Time) twice in a year and will allow you to configure the conditions defining the dates on which these switches are applied.

Daylight Saving Time Conditions

DST Name: This specifies the name of the Alternate Time standard (e.g., "Summertime" when the Alternate Time is in effect.

DST Offset: This specifies the offset of the Alternate Time standard **relative to UTC** (***not* relative to the original custom time zone**). For example, if the Standard Time of your custom time zone is two hours ahead of UTC (+7200 seconds) and the clock should go forward one hour when the Alternate Time enters effect, you would enter *10800* here (three hours ahead of UTC).

DST Switching Instant: This allows the time of year at which the clock switches between the Standard Time and Alternate Time to be defined either as fixed dates (*Static Date*) or according to dynamic weekday rules (*Dynamic Calculation*).

Static Date Options

If the Switching Instant is set to a static date, the following options will be available:

DST Start Date: The absolute date on which the Alternate Time will enter effect. Must be entered in the format *YYYY-MM-DD*.

DST Start Time: The **local time** of the time zone at which the Alternate Time will enter effect on the above date. Must be entered in the format *hh:mm*.

DST End Date: The absolute date on which the Alternate Time will cease effect and Standard Time will re-enter effect. Must be entered in the format *YYYY-MM-DD*.

DST End Time: The **local time** of the time zone at which the Alternate Time will cease effect on the above date and Standard Time will re-enter effect. Must be entered in the format *hh:mm*.

Dynamic Date Options

If the Switching Instant is set to be dynamically calculated, the following options will be available:

DST Start Weekday: The day of the week **of** or **after** the DST Start Date on which the Alternate Time will enter effect.

DST Start Date: The earliest date of the week in which the Alternate Time must enter effect. If this date falls on the day of the week specified above, this is the date on which the Alternate Time will enter effect. Otherwise, the Alternate Time will enter effect on the first date after this Start Date to fall on the specified day of the week. This date must be entered in the format *YYYY-MM-DD*.

DST Start Time: The **local time** of the time zone at which the Alternate Time will enter effect on the calculated start date. Must be entered in the format *hh:mm*.

DST End Weekday: The day of the week **of** or **after** the DST End Date on which the Alternate Time will cease effect and Standard Time will re-enter effect.

DST End Date: The earliest date of the week in which the Alternate Time must cease effect and the Standard Time must re-enter effect. If this date falls on the day of the week specified above, this is the date on which the Alternate Time will cease effect. Otherwise, the Standard Time will re-enter effect on the first date after this End Date to fall on the specified day of the week. This date must be entered in the format *YYYY-MM-DD*.

DST End Time: The **local time** of the time zone at which the Alternate Time will cease effect on the calculated end date and Standard Time will re-enter effect. Must be entered in the format *hh:mm*.

7.3.4 Configuration - Clock - Initialization

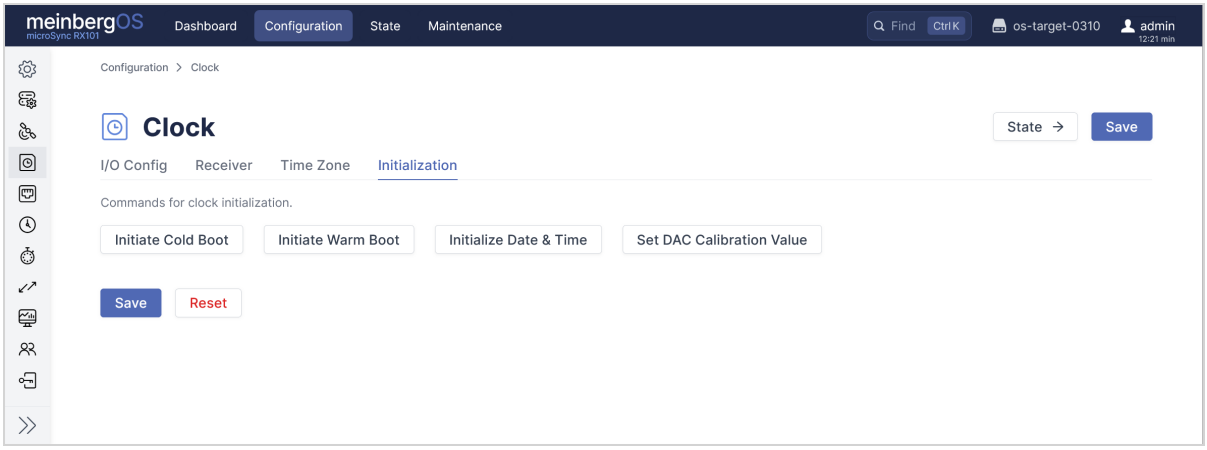


Figure 7.11: meinbergOS Web Interface: "Configuration → Clock - Initialization" Tab

Initiate Cold Boot: A **Cold Boot** will erase all almanac data (the up-to-date GNSS satellite trajectory data that allows approximate locations of satellite signals) and reinitialize the internal GNSS receiver. This has the effect of forcing the receiver to locate a single satellite, and when one is found, to download the full almanac from this satellite.

With a "GPS" type receiver, this process can take between 12.5 and 25 minutes, depending on the progress of the almanac transmission at the time of lock.

With a type "GNS" or "GNS-UC'" receiver, the process of locating four satellites for geopositioning will generally take less time.

Initiate Warm Boot: A **Warm Boot** will reinitialize the internal GNSS receiver while preserving the available almanac data. In this case, the reference clock will use the available almanac data to narrow down the search for sky signals.

The Time to First Fix in this case for any receiver type will generally be less than a minute.

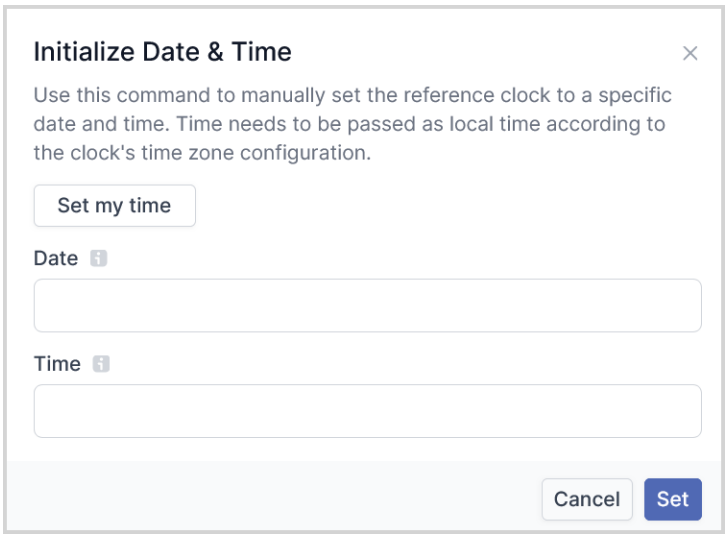


Figure 7.12: meinbergOS Web Interface: Setting the current time of the reference clock

Initialize Date & Time: This allows the clock to be manually set to a certain date & time, which may be necessary for the clock to synchronize to a reference source if the offset between the reference clock time and reference source time is too great.

This time must be set relative to the local time configured under ➜ Chapter 7.3.3, "Configuration - Clock - Time Zone". The button **Set My Time** can be selected to automatically acquire the current time from the device from which you are accessing the Web Interface.

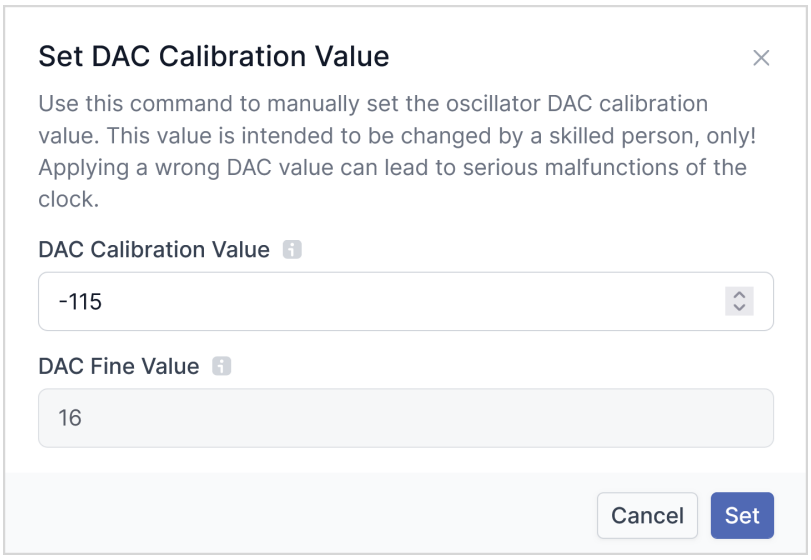


Figure 7.13: meinbergOS Web Interface: Setting the oscillator DAC calibration value of the reference clock

Set DAC Calibration Value: This dialog box is used to manually adjust the calibration values of the DAC (digital-analog converter) of the integrated oscillator, specifically when the oscillator is unable to achieve phase lock.

Important!

Please do not adjust these values without consulting with Meinberg Technical Support beforehand! The required DAC calibration values are specific to your meinbergOS device based on careful calibration of the oscillator during production.

These values are only intended to be manually adjusted by the user in exceptional circumstances, specifically when the integrated oscillator of the reference clock is out of phase to such an extent that the system will be unable to achieve phase lock without manual intervention. This can happen, for example, if a reference clock remains unsynchronized for very long periods of time.

If you discover that your meinbergOS device is unable to achieve phase lock despite successful synchronization with a reference signal, your device may need recalibration. In this case, please contact Meinberg Technical Support at techsupport@meinberg.de for assistance.

7.4 Configuration - A/V Sync Outputs

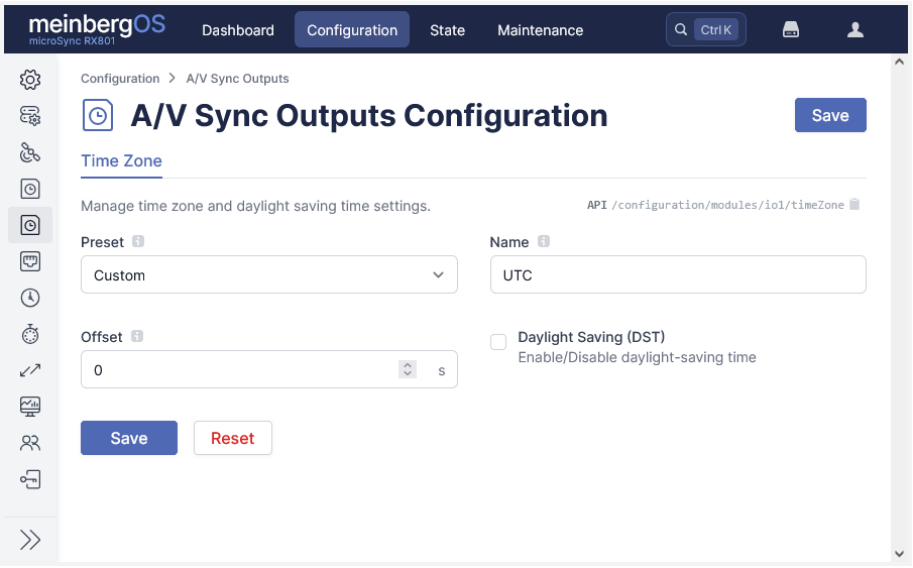


Figure 7.14: meinbergOS Web Interface: "Configuration → A/V Sync Outputs" Subsection

Information:

This subsection will only appear on devices with an integrated I/O Video Signal Generator module (microSync HR7, RX7, RX8, TRX8 series).

Time Zone

The **Time Zone** tab is used to configure how UTC time is converted to a local time zone for A/V time code output.

Preset: This provides a selection of time zone presets. These presets govern the time offset relative to UTC as well as any date-specific time adjustments (Daylight Saving Time, Standard Time). You may also select the option *Custom* to define a time zone not included in the presets (see Fig. 7.15 below).

Custom Time Zone

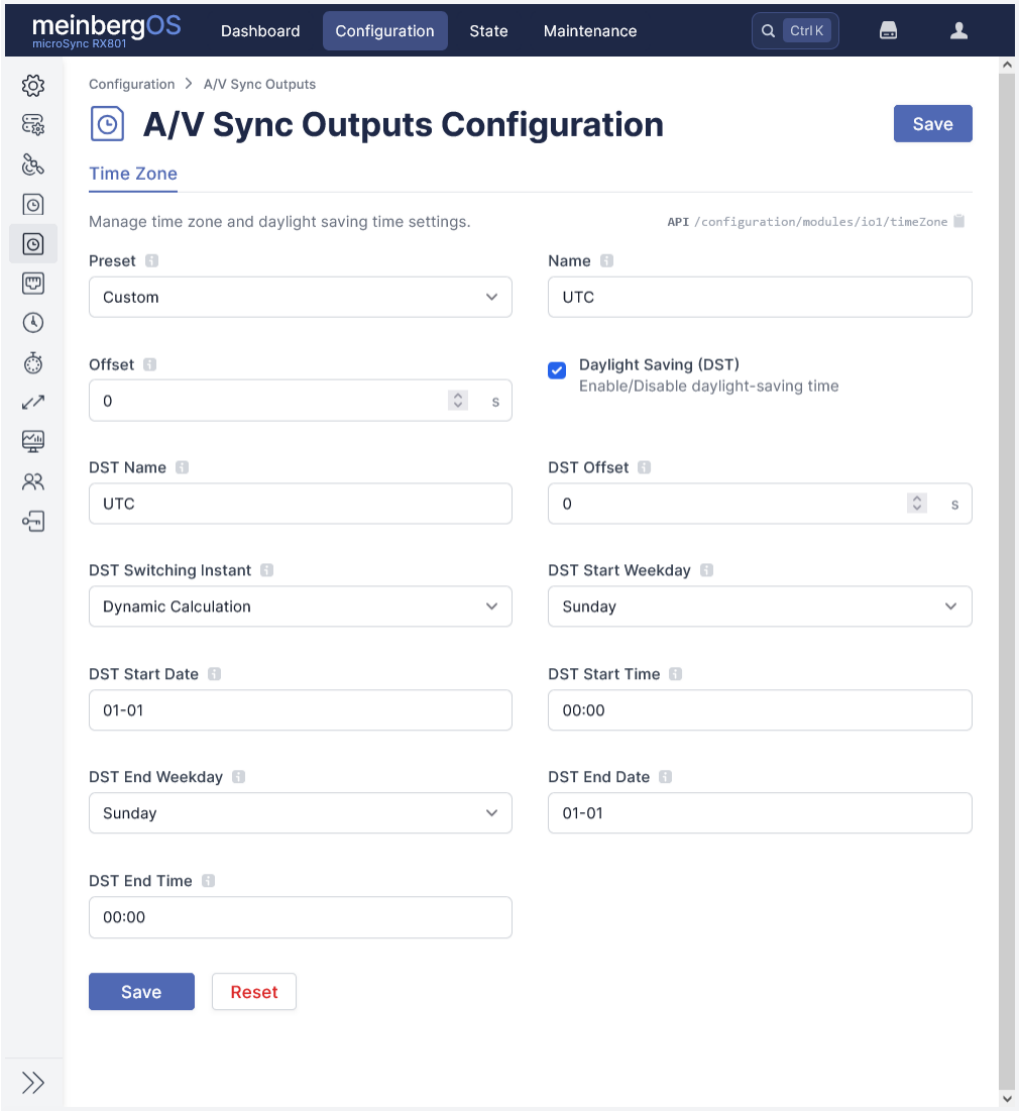


Figure 7.15: meinbergOS Web Interface: Custom Time Zone in "Configuration → A/V Sync Outputs → Time Zone" tab

When defining a custom time zone, the name, offset and Daylight Saving Time conditions must be defined.

Name: This is used to specify a name for the custom time zone.

Offset: This is used to specify the offset in whole seconds of the custom time zone relative to UTC (3600 seconds = 1 hour). Negative values must be prefixed with a minus symbol.

Daylight Saving (DST): If enabled, this time zone will observe switching between a Standard Time and an Alternate Time (typically Daylight Saving Time) twice in a year and will allow you to configure the conditions defining the dates on which these switches are applied.

Daylight Saving Time Conditions

DST Name: This specifies the name of the Alternate Time standard (e.g., "Summertime" when the Alternate Time is in effect.

DST Offset: This specifies the offset of the Alternate Time standard **relative to UTC** (***not* relative to the original custom time zone**). For example, if the Standard Time of your custom time zone is two hours ahead of UTC (+7200 seconds) and the clock should go forward one hour when the Alternate Time enters effect, you would enter *10800* here (three hours ahead of UTC).

DST Switching Instant: This allows the time of year at which the clock switches between the Standard Time and Alternate Time to be defined either as fixed dates (*Static Date*) or according to dynamic weekday rules (*Dynamic Calculation*).

Static Date Options

If the Switching Instant is set to a static date, the following options will be available:

DST Start Date: The absolute date on which the Alternate Time will enter effect. Must be entered in the format *YYYY-MM-DD*.

DST Start Time: The **local time** of the time zone at which the Alternate Time will enter effect on the above date. Must be entered in the format *hh:mm*.

DST End Date: The absolute date on which the Alternate Time will cease effect and Standard Time will re-enter effect. Must be entered in the format *YYYY-MM-DD*.

DST End Time: The **local time** of the time zone at which the Alternate Time will cease effect on the above date and Standard Time will re-enter effect. Must be entered in the format *hh:mm*.

Dynamic Date Options

If the Switching Instant is set to be dynamically calculated, the following options will be available:

DST Start Weekday: The day of the week **of** or **after** the DST Start Date on which the Alternate Time will enter effect.

DST Start Date: The earliest date of the week in which the Alternate Time must enter effect. If this date falls on the day of the week specified above, this is the date on which the Alternate Time will enter effect. Otherwise, the Alternate Time will enter effect on the first date after this Start Date to fall on the specified day of the week. This date must be entered in the format *YYYY-MM-DD*.

DST Start Time: The **local time** of the time zone at which the Alternate Time will enter effect on the calculated start date. Must be entered in the format *hh:mm*.

DST End Weekday: The day of the week **of** or **after** the DST End Date on which the Alternate Time will cease effect and Standard Time will re-enter effect.

DST End Date: The earliest date of the week in which the Alternate Time must cease effect and the Standard Time must re-enter effect. If this date falls on the day of the week specified above, this is the date on which the Alternate Time will cease effect. Otherwise, the Standard Time will re-enter effect on the first date after this End Date to fall on the specified day of the week. This date must be entered in the format *YYYY-MM-DD*.

DST End Time: The **local time** of the time zone at which the Alternate Time will cease effect on the calculated end date and Standard Time will re-enter effect. Must be entered in the format *hh:mm*.

7.5 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.

More information:

→ Chapter 7.5.1, "Configuration - Network - Main"

Interfaces:

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

More information:

→ Chapter 7.5.2, "Configuration - Network - Interfaces"

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.

More information:

→ Chapter 7.5.3, "Configuration - Network - PRP"

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.

More information:

→ Chapter 7.5.4, "Configuration - Network - Bonding"

Extended Configuration:

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

More information:

→ Chapter 7.5.5, "Configuration - Network - Extended Configuration"

IEC 61850:

The IEC 61850 functionality allows the meinbergOS device to communicate with other IEC 61850 IEDs (intelligent electronic devices) in accordance with the Manufacturing Message Specification (MMS), to export an IED Configuration Description file (ICD) for Substation Configuration Tools, and to import the resultant Configured IED Description (CID) file to configure the meinbergOS device.

More information:

→ Chapter 7.5.6, "Configuration - Network - IEC 61850"

7.5.1 Configuration - Network - Main

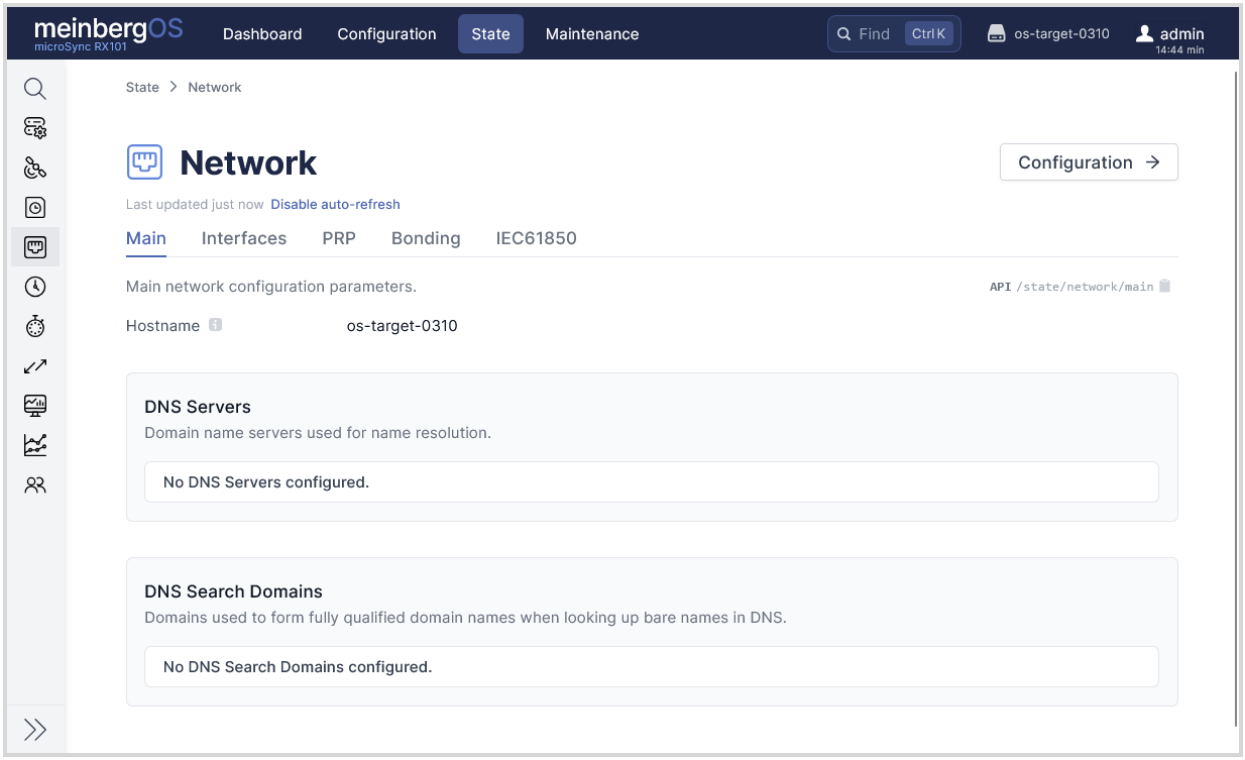


Figure 7.16: meinbergOS Web Interface: "Configuration → Network → Main" Tab

The "**Configuration** → **Network** → **Main**" tab (Fig. 7.16) 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 Domains:	Domains used to form fully qualified domain names when performing cleartext searches in DNS. You can specify up to three DNS search domains.

7.5.2 Configuration - Network - Interfaces

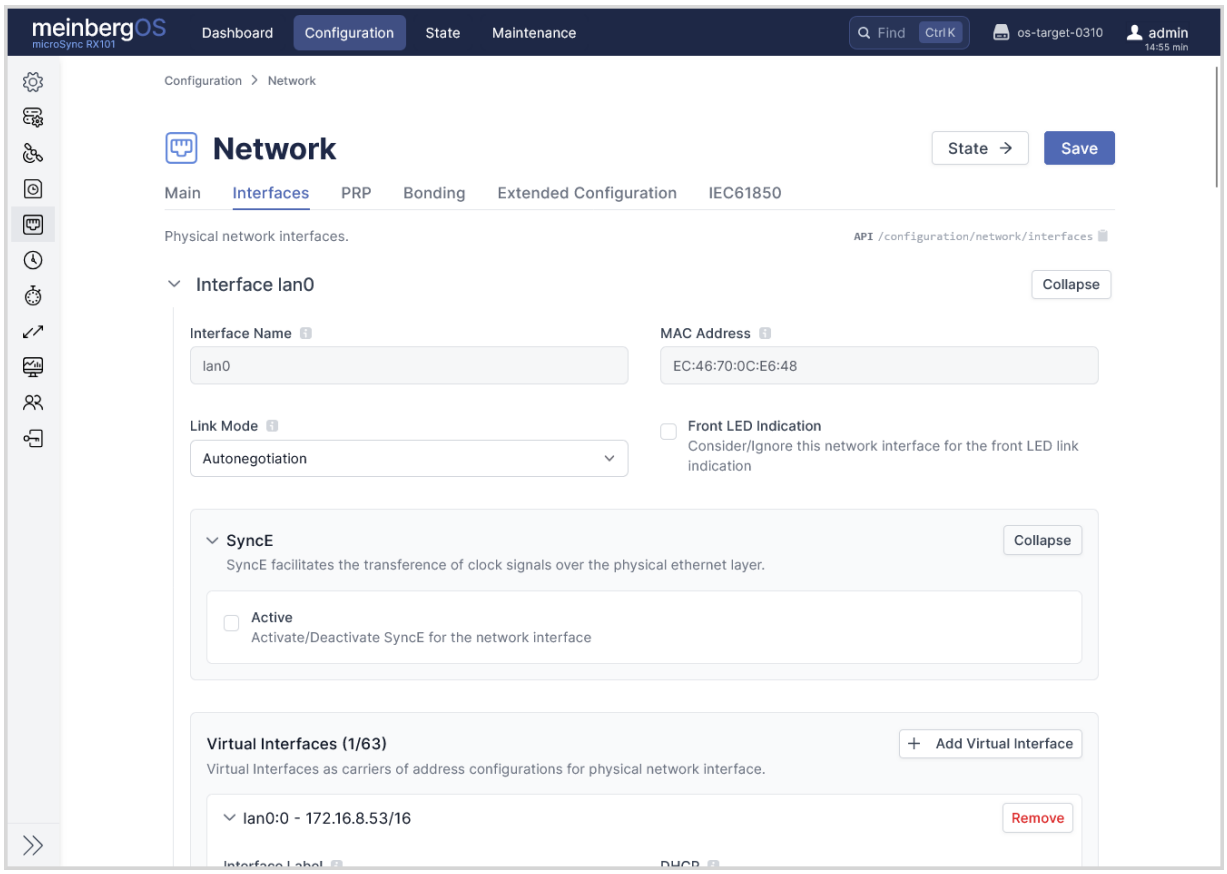


Figure 7.17: meinbergOS Web Interface: "Configuration → Network → Interfaces" Tab

The physical and virtual network interfaces and Synchronous Ethernet functionality are configured in this tab (Fig. 7.17).

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; autonegotiation enables two linked ports to negotiate the link speed and duplex mode automatically.

When using a copper-based (RJ45) SFP module, you will be able to 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)

When using an SFP module for fiber-optic connections, the link mode will typically be set by the SFP module.

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, the Quality Level is transmitted via the ESMC (Ethernet Synchronization Message Channel), whereas in *Slave* mode, the level received via the ESMC from the Master is applied.

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. This overrides any Quality Level that might be received from the Master via the ESMC.

Fixed Output SSM: This is used to set a fixed **Quality Level** for the SyncE output signal. This overrides any changes to the Quality Level that might be determined by the meinbergOS device depending on its synchronization state.

Minimum Input SSM: This specifies the minimum **Quality Level** received via the ESMC in conjunction with an input signal for it to be usable as a clock reference. 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.

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.

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.

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 (*0–4095*) that enables VLAN network traffic to be separated into discrete VLANs so that VLAN packets can be uniquely assigned to their respective VLANs. Please note that the values *0*, *1*, and *4095* have special applications under IEEE 802.1Q and should not be used.

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

This allows static routes to specified networks or hosts ot be defined 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.

7.5.3 Configuration - Network - PRP

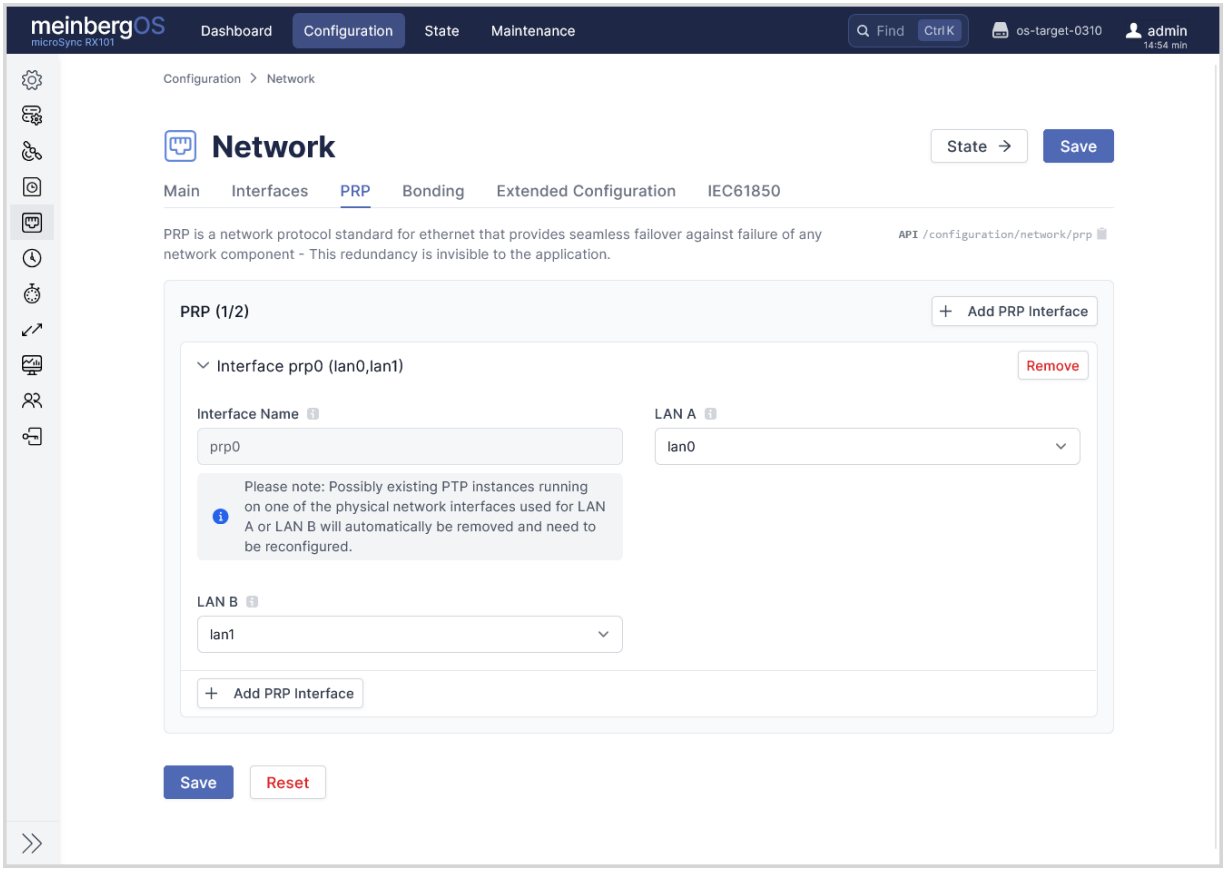


Figure 7.18: meinbergOS Web Interface: "Configuration → Network → PRP" Tab

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^{RX}) to two physically redundant networks, **LAN A** and **LAN B** (Fig. 7.18).

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 numbered physical interface that is connected to LAN A.

LAN B: The numbered physical interface that is connected to LAN B.

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.

7.5.4 Configuration - Network - Bonding

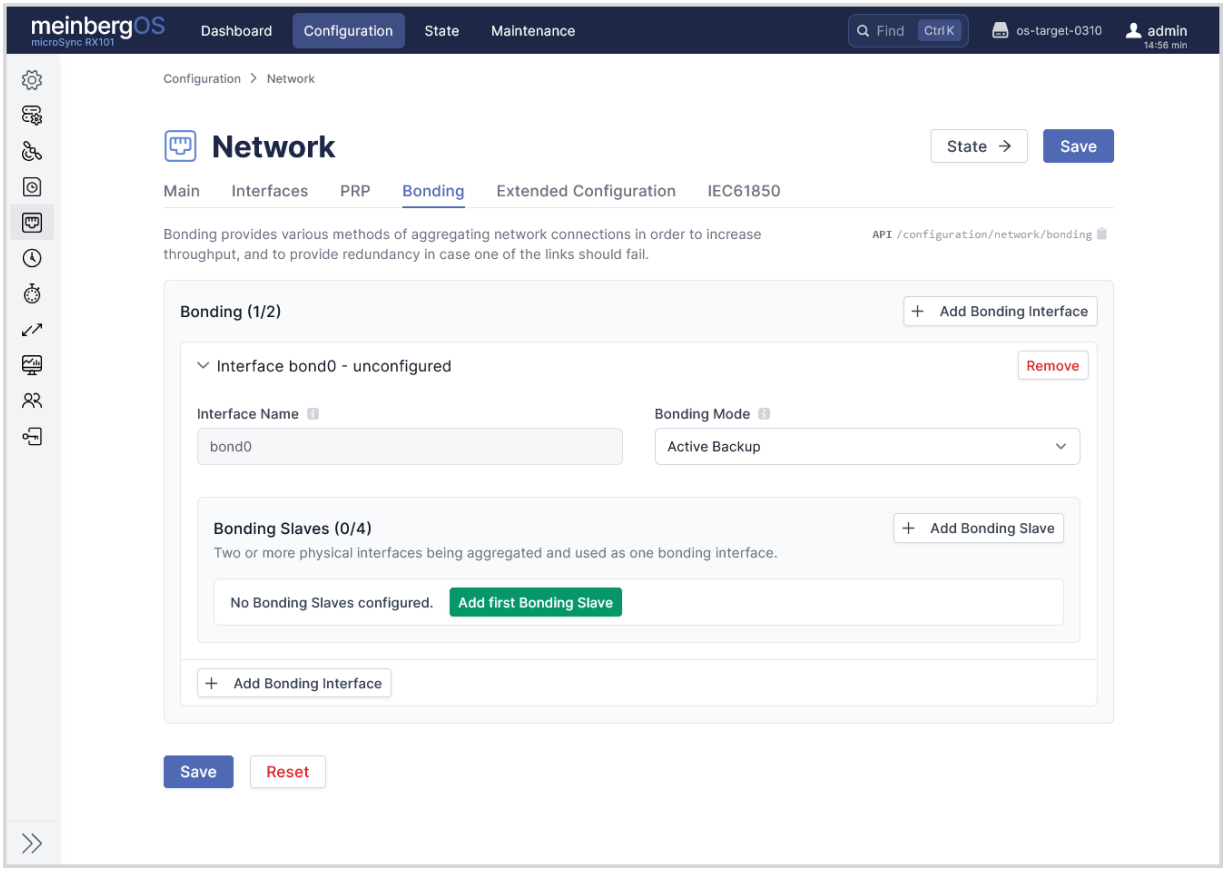


Figure 7.19: meinbergOS Web Interface: "Configuration → Network → Bonding" Tab

The tab "**Network** → **Bonding**" (Fig. 7.19) 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.

7.5.5 Configuration - Network - Extended Configuration

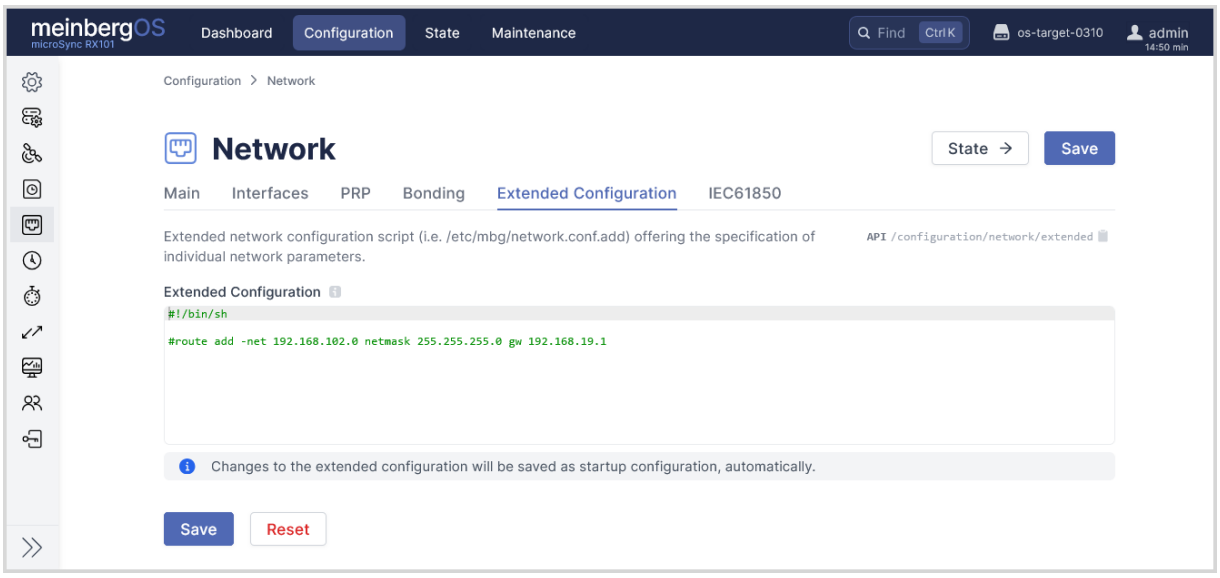


Figure 7.20: meinbergOS Web Interface: "Configuration → Network → Extended Network Configuration" Tab

The **Extended Configuration** tab (Fig. Fig. 7.20) 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.

7.5.6 Configuration - Network - IEC 61850

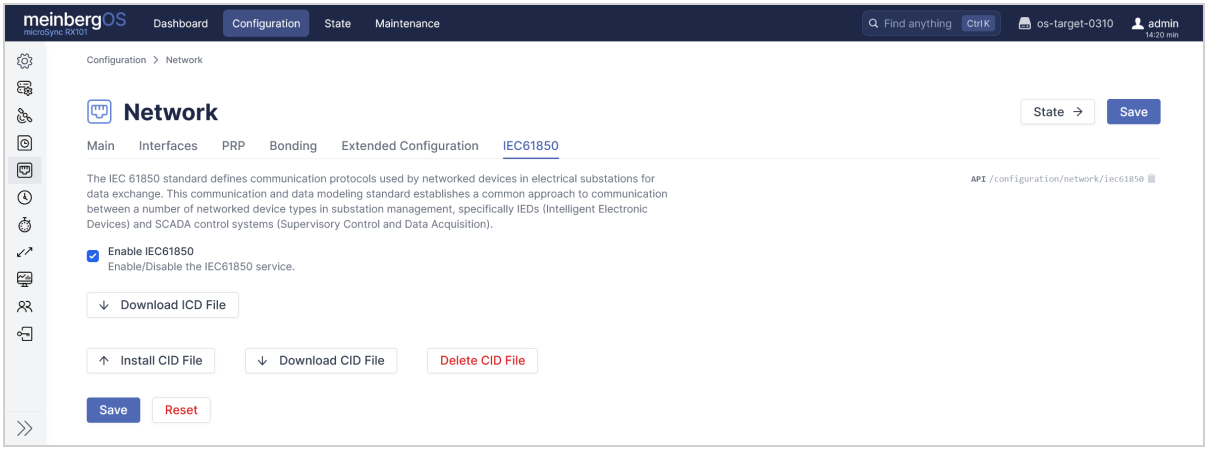


Figure 7.21: meinbergOS Web Interface: "Configuration → Network → IEC 61850" Tab

IEC 61850 is a power industry standard that defines communication protocols used by networked devices in electrical substations for data exchange between IEDs (Intelligent Electronic Devices) and other systems such as centralized SCADA control systems (Supervisory Control and Data Acquisition). meinbergOS devices support the MMS protocol, which IEC 61850 infrastructures use for remote configuration and monitoring, and CID & ICD files, which are used to allow a Substation Configuration Tool (SCT) to identify the capabilities of the meinbergOS device (which in the context of an IEC 61850 is an **IED**), and in turn to allow the meinbergOS device to configure itself based on the specifications provided by the SCT.

The tab "**Network → IEC 61850**" (Fig. 7.19) provides a number of options relating to the integrated MMS server as well as management of the device's CID and ICD files.

Security Risk

Enabling the **IEC 61850 MMS server** represents a **network security risk** of **high severity**; the MMS (Manufacturing Message Specification protocol) is an unencrypted, unauthenticated protocol in which data can be intercepted or malicious payloads can be readily introduced. There is currently no compliant method of authenticating MMS traffic or distributing it over an encryption layer.

For this reason, meinbergOS as of version 2024.12.4 does not allow any significant reconfiguration of the meinbergOS device over the MMS protocol beyond minor changes to PTP datasets. However, this can allow an adversary with network access to manipulate the prioritization of PTP master clock selection.

An adversary with network access to the meinbergOS device can acquire any configuration or state information that the CID file specifies.

If this option is enabled, the isolation of this meinbergOS device from insecure networks, in particular the public internet, is strongly recommended.

Enable IEC 61850: Enabling this checkbox activates the integrated MMS server of the meinbergOS device, allowing it to receive configuration data and receive and transmit reporting data.

Download ICD File: This button is used to download the ICD file that your Substation Configuration Tool requires to generate the CID file for your meinbergOS device. The file is generated by the meinbergOS device itself and contains a comprehensive description of your meinbergOS device's capabilities and interfaces (see ➜ Chapter 8.4.5, "State - Network - IEC 61850").

Install CID File: This button is used to upload a CID file (Configured IED Description) to the meinbergOS device to allow it to configure itself. This CID file is typically provided by the Substation Configuration Tool on the basis of the *ICD file*.

Download CID File: If a CID file has been uploaded to the meinbergOS device, this button will allow you to download a copy of it for backup purposes or for re-use with other meinbergOS devices when adopting a bottom-up strategy to substation design.

Delete CID File: This button will delete the stored CID file irrevocably from the meinbergOS device.

7.6 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.

More information:

→ Chapter 7.6.1, "Configuration - NTP - Server"

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

More information:

→ Chapter 7.6.2, "Configuration - NTP - Client"

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

More information:

→ Chapter 7.6.3, "Configuration - NTP - Symmetric Keys"

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

More information:

→ Chapter 7.6.4, "Configuration - NTP - Extended Configuration"

7.6.1 Configuration - NTP - Server

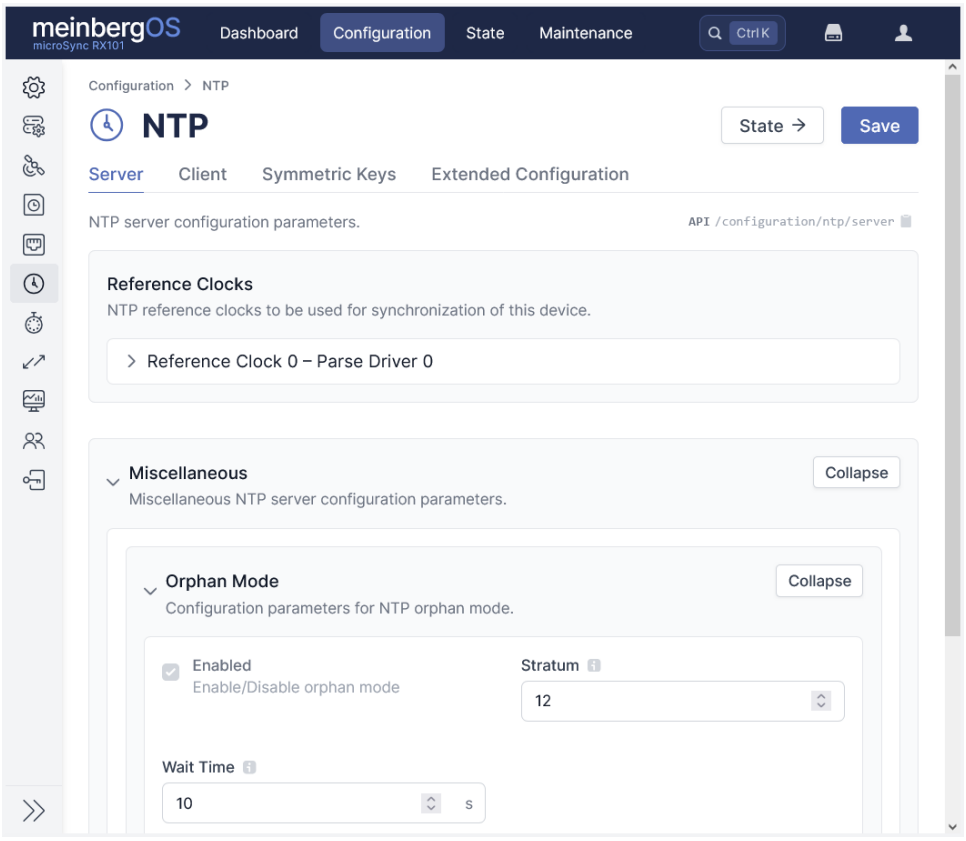


Figure 7.22: meinbergOS Web Interface: "Configuration → NTP → Server" Tab

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 → Chapter 7.6.2, "Configuration - NTP - Client").

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 how meinbergOS handles NTP traffic internally 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).

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.

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.

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.

7.6.2 Configuration - NTP - Client

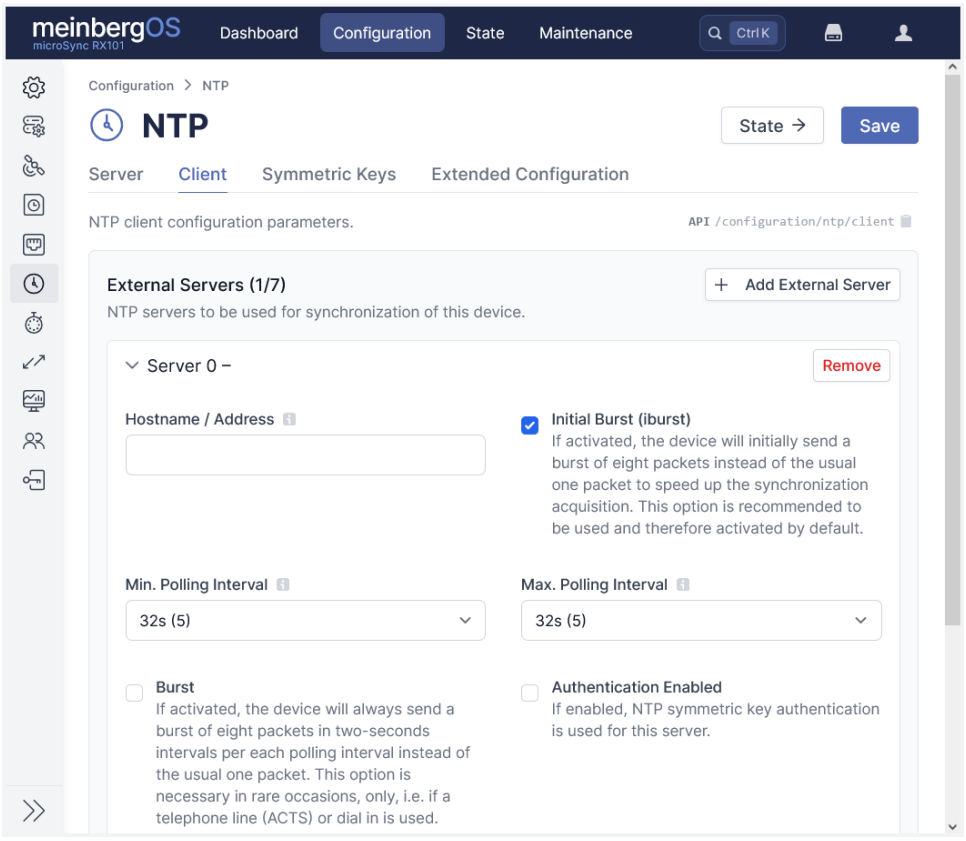


Figure 7.23: meinbergOS Web Interface: "Configuration → NTP → Client" Tab

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 → Chapter 7.6.1, "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.

Information:

When synchronizing your meinbergOS device to publicly accessible NTP servers operated by third parties over the internet, please exercise restraint in your use of the server's capacity. The use of very frequent polling rates and the enabling of *burst* in particular is generally frowned upon. It is advised to not poll a publicly accessible server more than once every 64 seconds.

Failure to observe these norms may result in access to the operators of these third-party servers limiting or prohibiting your meinbergOS device's access to the server.

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.

7.6.3 Configuration - NTP - Symmetric Keys

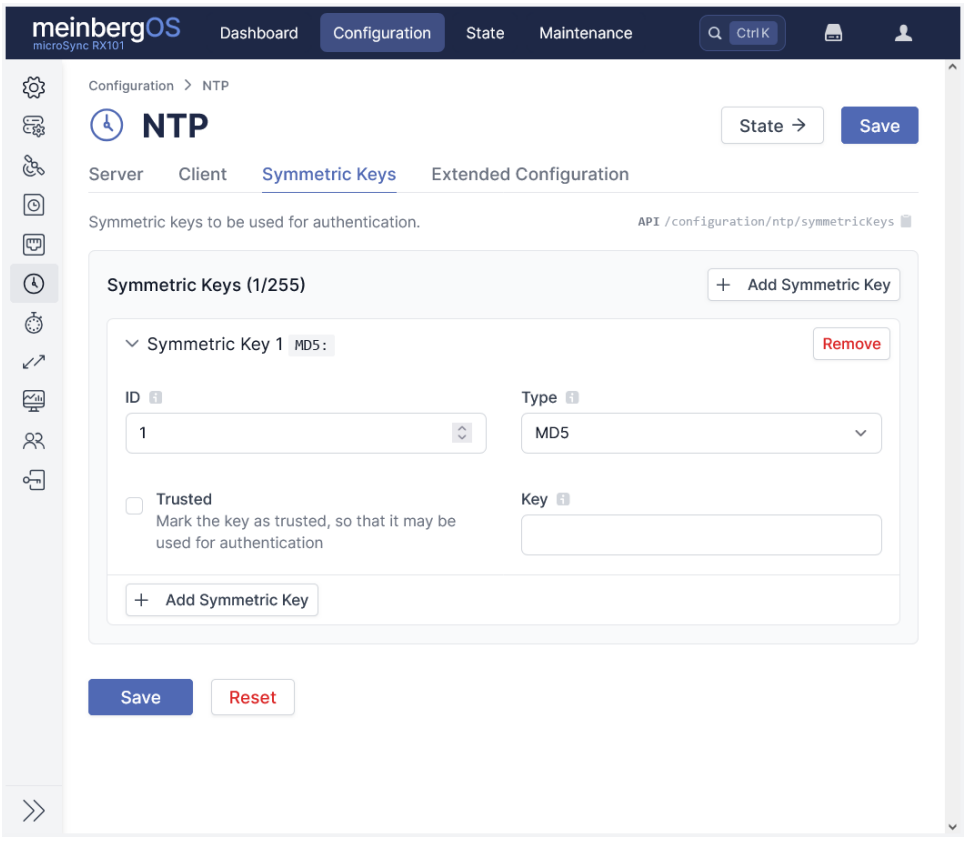


Figure 7.24: meinbergOS Web Interface: "Configuration → NTP → Symmetric Keys" Tab

This tab (Fig. 7.24) 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.

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`).

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.

7.6.4 Configuration - NTP - Extended Configuration

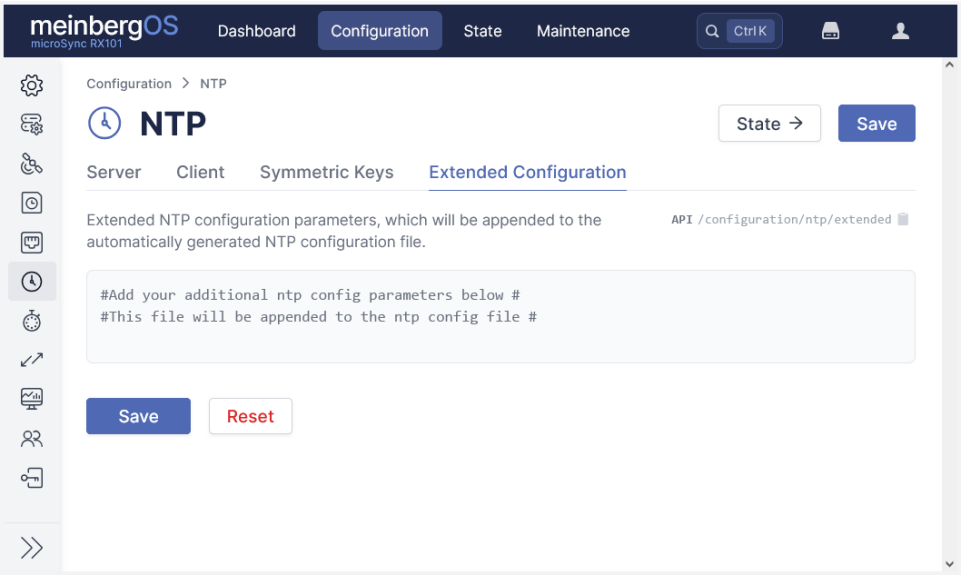


Figure 7.25: meinbergOS Web Interface: "Configuration → NTP → Extended Configuration" Tab

This tab (Fig. 7.25) 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.

7.7 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.

More information: ➜ Chapter 7.7.1, "Configuration - PTP - Interfaces"

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

More information: ➜ Chapter 7.7.2, "Configuration - PTP - Instances"

7.7.1 Configuration - PTP - Interfaces

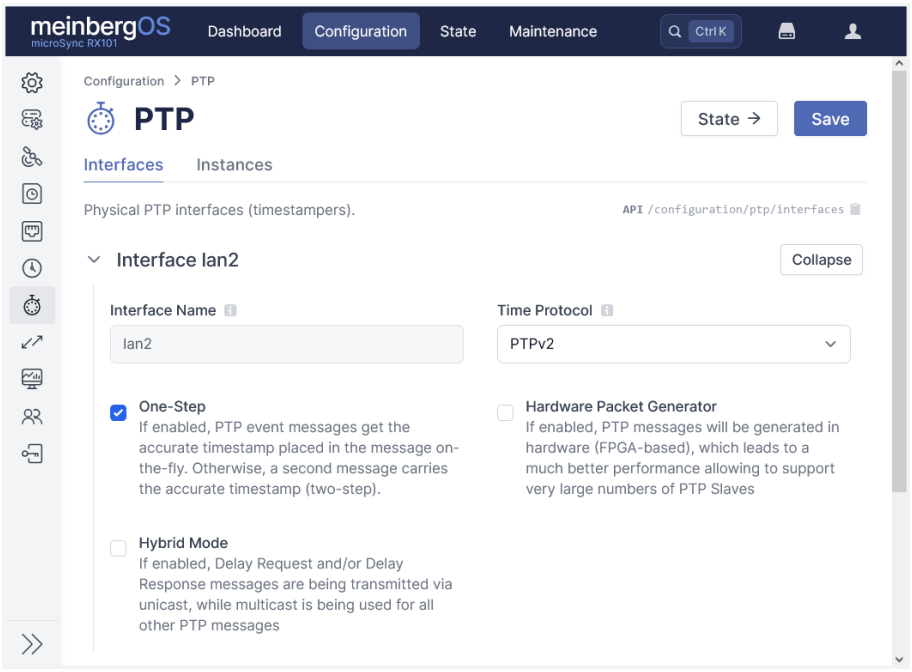


Figure 7.26: meinbergOS Web Interface: "Configuration → PTP → Interfaces" Tab

This tab (Fig. 7.26) 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. This is set by the firmware and cannot be edited.

Time Protocol: The PTP protocol version (*PTPv2* or *PTPv1*) employed by this interface for PTP communication.

Information:

PTPv1 is only available to select if your meinbergOS device has a **Performance Level C** license.

One-Step:
(PTPv2 only):
If enabled, PTP event messages will have an accurate timestamp placed directly in the **Sync** message on the fly. If disabled, the accurate timestamp will be transmitted in a second **Follow-Up** message (*two-step* mode).

Hardware Packet Generator:
(PTPv2 only)
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 PTPv2 and Layer 3 network protocols (UDP/IPv4 and UDP/IPv6). It can therefore not be used with any PTPv2 profile that requires Layer 2 IEEE 802.3 communication.

Hybrid Mode:
(PTPv2 only)
If enabled, **Delay Request** and/or **Delay Response** messages will be sent as unicast transmissions, while all other PTP messages will be sent as multicast transmissions.

7.7.2 Configuration - PTP - Instances

This tab (Fig. 7.27) 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. The options that appear here are dependent on whether *PTPv2* or *PTPv1* has been selected at the operating mode for the interface.

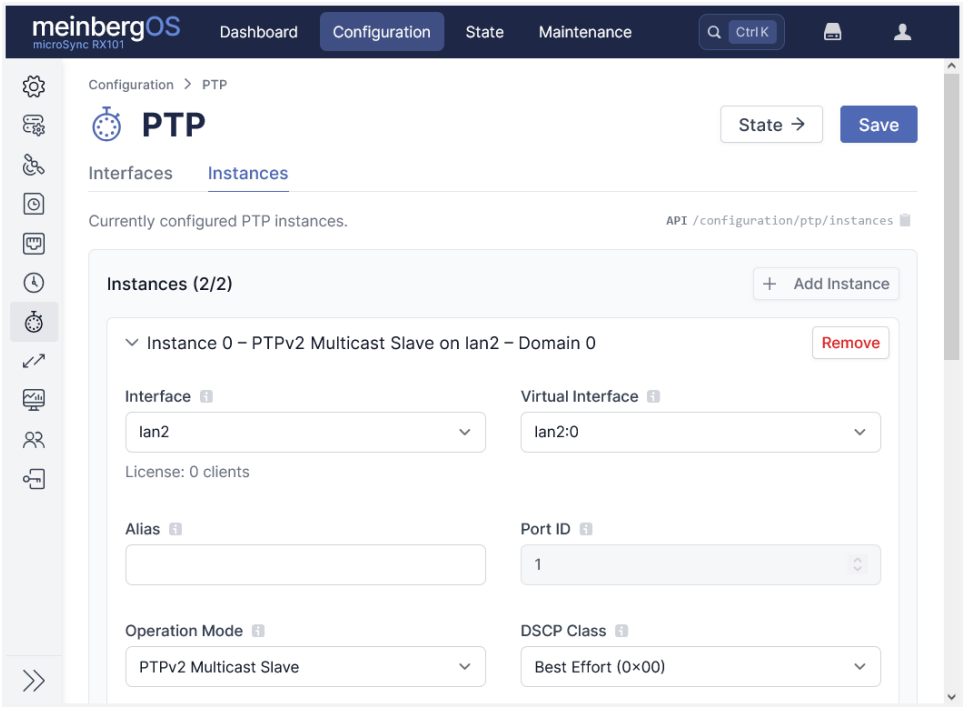


Figure 7.27: meinbergOS Web Interface: "Configuration → PTP → Instances" Tab for PTPv2 Operation

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

Virtual Interface: The virtual interface 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:
(PTPv2 only)

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*
- *Unicast Slave*
- *Multicast Master*
- *Unicast Master*
- *Multicast Auto*
- *Mixed Master*

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:
(PTPv2 only)

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

Multicast TTL:
(PTPv2 only)

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

Delay Asymmetry Compensation:
(PTPv2 only)

Enables/disables compensation for known delay asymmetry.

Asymmetry Compensation Value:
(PTPv2 only)

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:
(PTPv2 only)

Enables/disables packet counter statistics. This data can be viewed under "**State** → **PTP** → **Instances** → **Packet Counters**". Refer to
➜ Chapter 8.6.2, "State - PTP - Instances" for more information.

Enable BC (Boundary Clock) Mode: If *enabled*, and if the instance is synchronized to a PTP master, the meinbergOS device will transmit the **Parent Dataset** (the dataset of the Master to which the meinbergOS device is Slave) to the other local Master instance for redistribution to its own Slave clocks.

If *disabled*, and assuming that the other PTP instance is configured to be a PTP Master, the meinbergOS device will transmit the **Default Dataset** (the dataset of the local meinbergOS device) to that other instance for redistribution to its own Slave clocks.

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 directly accessible via the Web Interface. They can be acquired by generating a diagnostics file (→ Chapter 9.10, "Maintenance - Diagnostics File"), where they are located in the `ptp` folder.

Alternatively, the files can 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: This field serves as the primary determinant for the selection of the grandmaster by the Best Master Clock Algorithm. A clock with a *lower* **Priority 1** is prioritized over a clock with a *higher* **Priority 1**.

Conventionally, **Priority 1** 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: 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 **Priority 1**, **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 option will be grayed out if the selected profile mandates the use of the TAI timescale.

Information:

When using an arbitrary timescale, the timestamps of the PTP packets will follow the UTC timescale, provided that the reference clock is locked to a UTC reference source or a source that can be converted back to UTC.

If your reference source lacks the information required to trace its time back to UTC (i.e., local time without time zone information), the reference clock will still assume that this reference source is providing UTC time. If such a reference source is providing time on another timescale despite this assumption, any resultant errors will be reflected in the NTP server responses and PTP timestamps.

Enable Alternate Time Offset Indicator TLV: If enabled, a PTPv2 Alternate Time Offset Indicator TLV will be appended. The content of this TLV is derived automatically from the configured clock time zone. Prior to meinbergOS *2022.05.5*, this option was limited to the IEEE C37.238-2017 profile and has since been made available for all profiles, with the exception of IEEE C37.238-2011, which mandates that this option remain **enabled**.

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

Enable V1 Hardware Compatibility (Master/Auto Mode only): This option should be enabled if there are PTP clocks in your network that have PTPv2 Hardware Timestamper support but expect the **Sync** message length to be equal to that of a PTPv1 **Sync** message. Enabling this option will cause **Sync** messages to be padded with enough bytes to ensure that the messages meet the PTPv1 message size 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 in Holdover Mode (no reference signal available).

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 Minimum Quality

If *Master* or *Auto* mode is selected, the **Minimum Quality** parameters can be opened within the **PTPv2** panel to enable the minimum values for the quality parameters to be enforced for the Best Master Clock algorithm. The clock will never report values better than this while Minimum Quality is enabled, which can be useful to prevent dataset volatility (resulting in potentially frequent changes in master/slave relationships) when network conditions are unstable.

These settings do not appear or apply in *Slave* mode.

Information:

It is possible to have only individual minimum values enforced and the remainder handled as normal. Parameters that are not to be enforced should be set (or left at) a value of *0*.

Enabled:	If checked, minimum quality parameters will be applied, limiting the quality levels that a clock in Master mode can report to other clocks in the network. This must be enabled to configure the other parameters.
Clock Class:	Specifies the minimum possible value of the reported **Clock Class**.
Clock Accuracy:	Specifies the best possible reported **Clock Accuracy**.
Clock Variance:	Specifies the minimum possible value of the reported **Clock Variance**.

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.

Power IEEE C37.238-2011

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.

Telecom ITU-T G.8275.1

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).

SMPTE ST 2059-2

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*.

IEEE 802.1AS/AUTOSAR

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.

Power IEEE C37.238-2017

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.

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.

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

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 directly accessible via the Web Interface. They can be acquired by generating a diagnostics file (→ Chapter 9.10, "Maintenance - Diagnostics File"), where they are located in the `ptp` folder.

Alternatively, the files can 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`.

Enable BC (Boundary Clock) Mode: If *enabled*, and if the instance is synchronized to a PTP master, the meinbergOS device will transmit the **Parent Dataset** (the dataset of the Master to which the meinbergOS device is Slave) to the other local Master instance for redistribution to its own Slave clocks.

If *disabled*, and assuming that the other PTP instance is configured to be a PTP Master, the meinbergOS device will transmit the **Default Dataset** (the dataset of the local meinbergOS device) to that other instance for redistribution to its own Slave clocks.

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

PTPv1

Additional configuration parameters for PTPv1 instances.

Important!

Support for PTPv1 is only available on meinbergOS devices with a **Performance Level C** license. If your device does not have this license but you require PTPv1 support, please reach out to your Meinberg representative for more information on how to upgrade the license.

Stratum: A manually defined quality parameter for the Best Master Clock Algorithm (BMCA). A lower value here gives preference to this clock over others when selecting a master clock above any measured quality parameters such as clock variance and clock accuracy (but under **Preferred Master** below).

Preferred Master: Defines this instance as one of the preferred master clocks in the defined subdomain. This is one of the most dominant deciding factors in the BMCA, and a master clock will typically only be elected from the clocks configured with this flag, unless all clocks in this pool of preferred masters report that they are not synchronized to an external reference.

Subdomain: This is the subdomain used for this PTP device. Only devices with the same subdomain 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. The IEEE 1588-2002 standard recognizes the strings `_DFLT`, `_ALT1`, `_ALT2`, and `_ALT3`, but any string of up to 16 bytes in length can be used here.

Sync Interval: Specifies the interval between **Sync** messages when this clock is operating as a master.

7.7.3 Configuration - PTP - PTP Track Hound

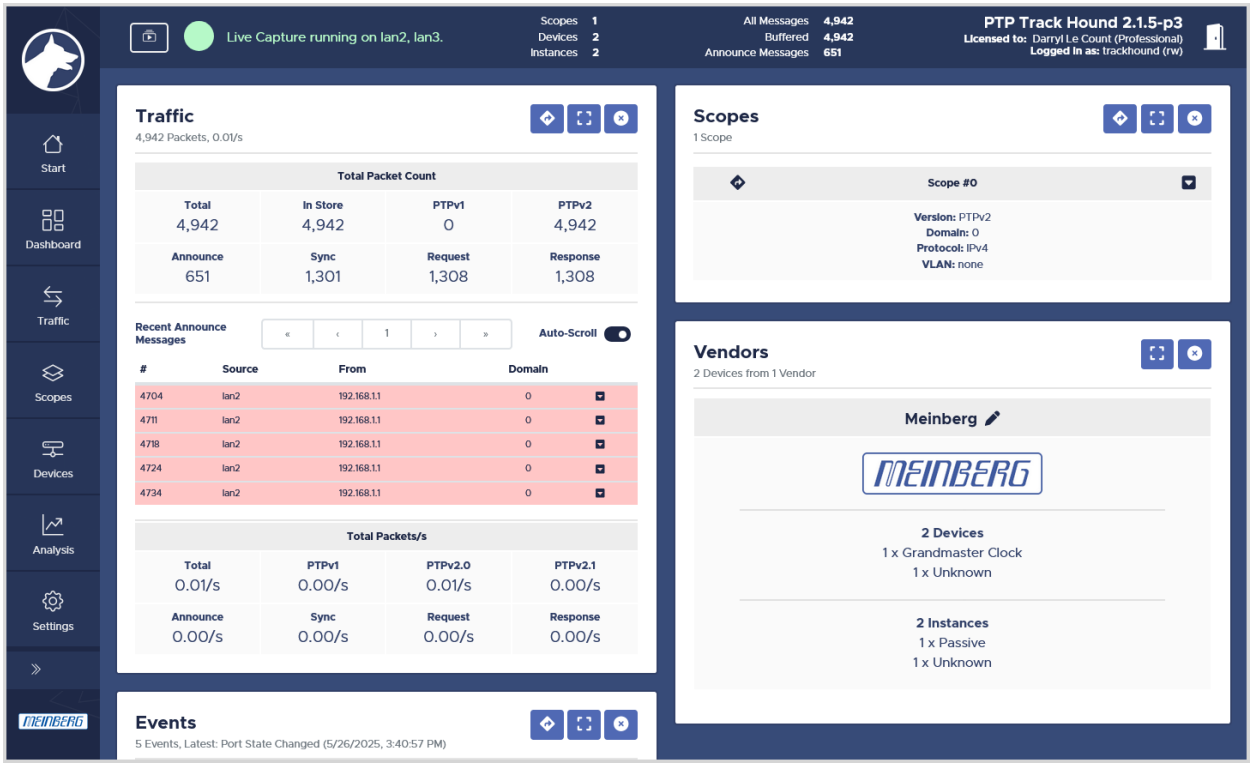


Figure 7.28: PTP Track Hound Web Interface

As of meinbergOS *2024.12*, Meinberg's PTP network monitoring solution **PTP Track Hound** is integrated into all meinbergOS devices. PTP Track Hound provides a wealth of monitoring, analysis, and reporting tools for PTP traffic, and all of these are managed via the separate PTP Track Hound Web Interface.

The version of PTP Track Hound integrated into your meinbergOS device features a free **Capture** license that allows it to not only capture and analyze PTP traffic received by your device but also to forward it to a central instance with a **Professional** license.

For further information, visit Meinberg's PTP Track Hound website at https://www.ptptrackhound.com, where you can also download the product documentation.

Configuration

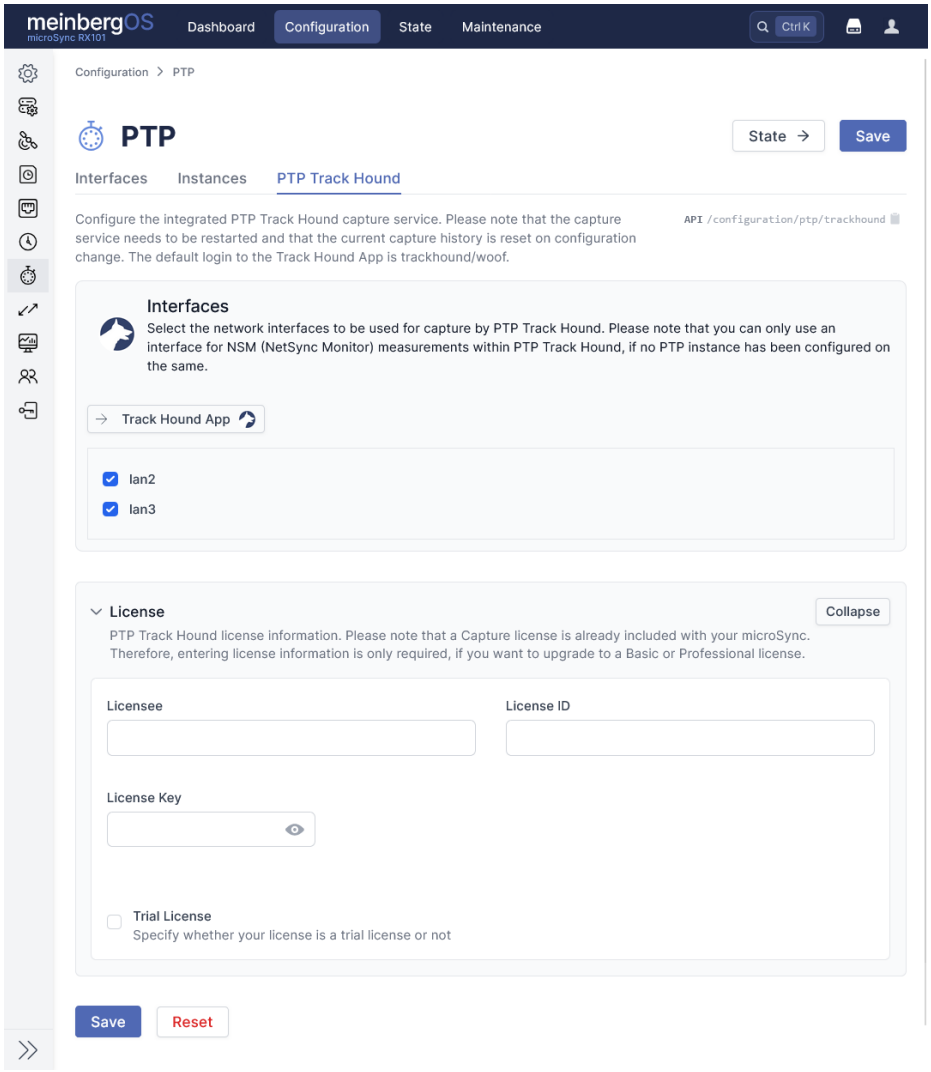


Figure 7.29: meinbergOS Web Interface: "Configuration → PTP → PTP Track Hound" Tab

Important!

Saving any changes to the PTP Track Hound configuration via the meinbergOS Web Interface will result in the PTP Track Hound capture service being restarted with a resultant loss of the current capture history.

If necessary, please save your capture history from the PTP Track Hound Web Interface before making any changes to the PTP Track Hound configuration.

Please refer to the chapter "**Exporting pcap Capture Files**" in the PTP Track Hound documentation for more information on how to backup the current capture history.

Unlike standalone PTP Track Hound installations on a PC, some of the configuration of the version of PTP Track Hound integrated into your meinbergOS device is performed via the meinbergOS Web Interface, specifically:

- the interfaces to be monitored,
- the licensing details.

Interfaces

This panel is used to select the interfaces of your meinbergOS device which the PTP Track Hound instance will monitor. Each checkbox represents a PTP-capable physical network interface on your device.

The transmission of management messages, performance of Capture Time Offset measurements, or performance of measurements using the NetSync Monitor protocol requires exclusive PTP access to the network port. As such, these features can only be enabled on an interface that has no PTP instance attached to it (and also requires a Basic or Professional license to be registered on the meinbergOS device). However, these ports can continue to be used for NTP, management, API access, and network monitoring.

Disabling all of the interfaces here will disable the PTP Track Hound service.

Assuming that the PTP Track Hound service is enabled, the button "**Track Hound App**" can be used to access the PTP Track Hound Web Interface directly. Please note that the account management for PTP Track Hound is entirely separate from that of meinbergOS and does not support remote authentication. A default account is configured for the first login:

Username: `trackhound`
Password: `woof`

License

This panel allows you to register your purchased or trial Basic or Professional license with your meinbergOS device. Each license consists of a licensee name, a license ID, and a license key, as well as an expiration date for trial licenses. All of this information must be provided **exactly** as provided by Meinberg.

Important!

PTP Track Hound on your meinbergOS device requires v2.1.x branch license keys to enable the full range of supported functions. While v2.0.x branch keys can be registered with PTP Track Hound, these licenses do not include support for the following functions:

- NetSync Monitor
- Statistical Analysis

For more information, visit https://www.ptptrackhound.com or contact Meinberg at ptptrackhound@meinberg.de.

7.8 Configuration - I/O Ports

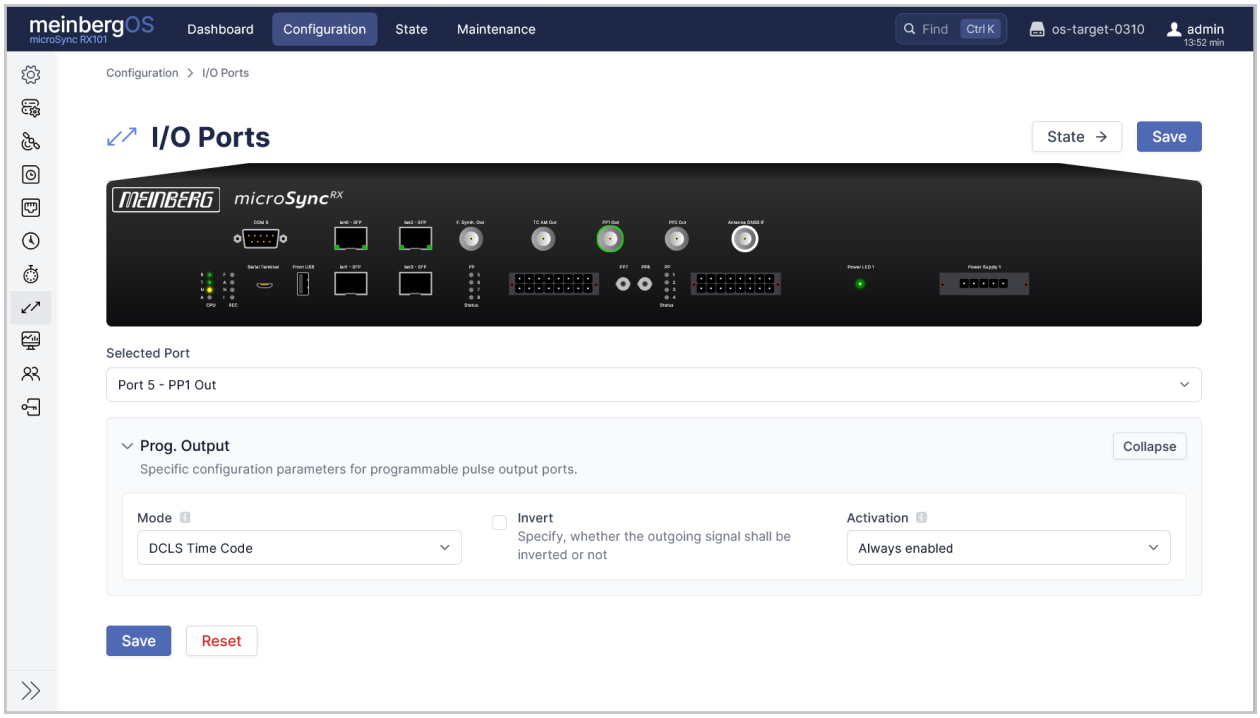


Figure 7.30: meinbergOS Web Interface: "Configuration → I/O Ports" Subsection

The "**Configuration → I/O Ports**" subsection (Fig. 7.30) provides a graphical representation of your physical meinbergOS (e.g., a microSync) with an overview of the available interfaces and visual status indicators.

Hovering with the cursor 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.

Selecting (clicking on) an indicator or connector will open the corresponding panel or subsection used to configure that connector (if configurable), or provide a link to the relevant **Configuration** subsection.

The interfaces shown in this subsection will vary depending on the specific meinbergOS device. Please refer to your meinbergOS device's manual for further information on these connectors and indicators.

7.9 Configuration - Monitoring

This subsection enables you to configure the handling of event notifications and logging for your meinbergOS device.

Events: The tab lists the different event types and the channels via which notifications for each event are issued (SNMP or syslog).

More information: → Chapter 7.9.1, "Configuration - Monitoring - Events"

SNMP: This tab provides the configuration options for monitoring over SNMP

More information: → Chapter 7.9.2, "Configuration - Monitoring - SNMP"

Syslog: This tab provides the configuration options for the transmission of events to a syslog server.

More information: → Chapter 7.9.3, "Configuration - Monitoring - Syslog"

7.9.1 Configuration - Monitoring - Events

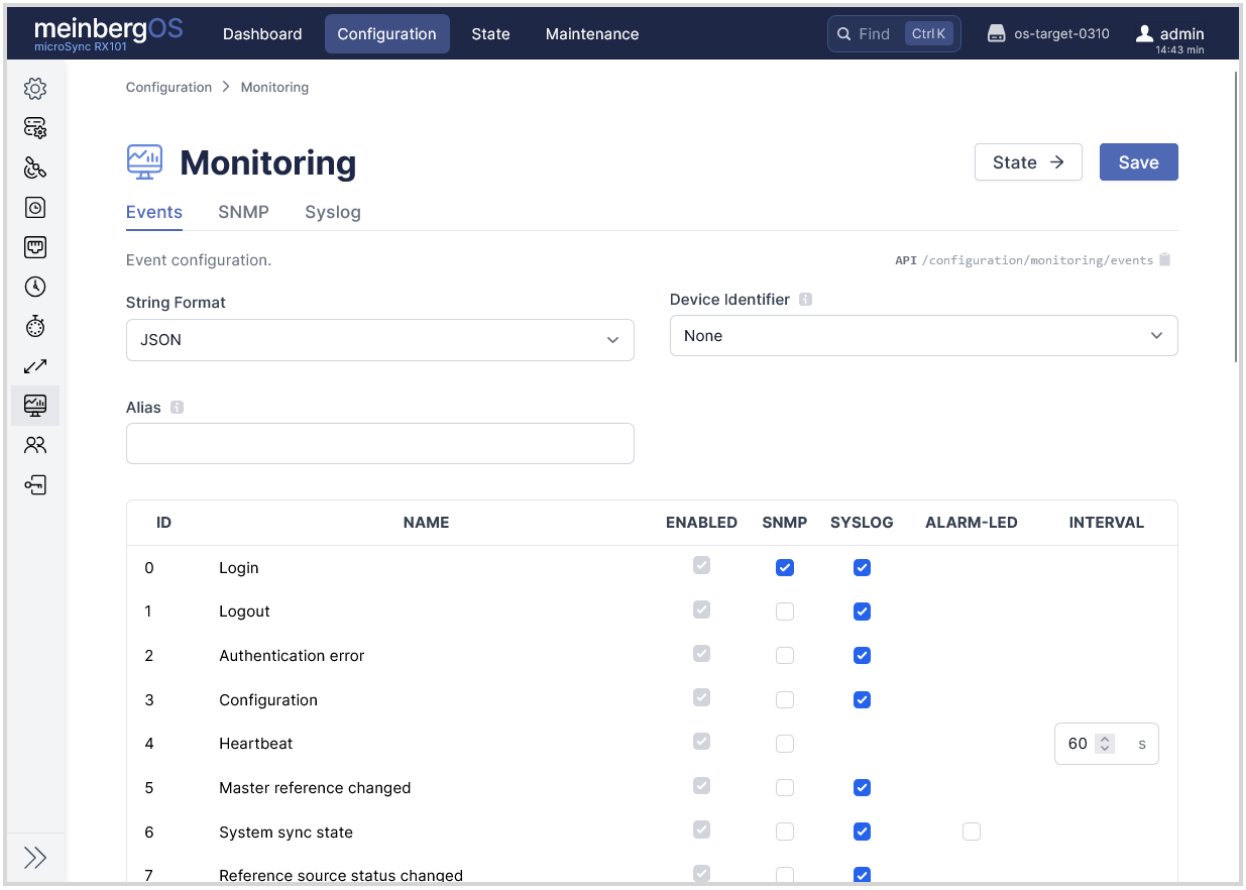


Figure 7.31: meinbergOS Web Interface: "Configuration → Monitoring → Events" Tab

This tab allows you to define for which events log entries or notifications will be generated as well as a number of other general options related to these.

String Format: The data structure that will be observed when transmitting event notifications or log entries. As of meinbergOS *2024.12.4*, only JSON is supported.

Device Identifier: Specifies how the device will be referred to in event notifications/log entries. If *None* is selected, no information on the related device will be included. If *Alias* is selected, the name entered under **Alias** in this same tab will be included in the event notifications/log entries. If *Serial Number* is selected, the serial number of the device will be included in the event notifications/log entries.

Alias: If *Alias* is selected as the **Device Identifier** above, this is the name that will be used to identify the device in event notifications and log entries.

The table beneath these options can be used to configure which notification types should be issued for each type of event:

Enabled: These checkboxes determine if the events are logged **internally**, such that they will be reported in the Events Log (see ➜ Chapter 9.6, "Maintenance - Events Log") and "**State** → **Monitoring**" (see ➜ Chapter 8.8, "State - Monitoring" subsection. Some of these checkboxes are grayed out; these events are considered essential and cannot be disabled in local logging. The others are optional events that can be disabled if they generate too many unnecessary local alerts.

SNMP: These checkboxes determine the events that are reported over SNMP and transmitted to the configured SNMP agents.

syslog: These checkboxes determine the events that are reported via the syslog protocol and are transmitted to the configured syslog servers. The *Heartbeat* event is not possible in this case as the syslog protocol is not typically intended for real-time monitoring.

Alarm LED: These checkboxes determine which events cause the physical **Alarm** LED on the meinbergOS device to light red. The possible choices here are limited to exceptional events that typically warrant administrator intervention.

Interval: This column only provides a numerical input option for the **Heartbeat** event to allow the user to specify how frequently the heartbeat signal should be transmitted.

7.9.2 Configuration - Monitoring - SNMP

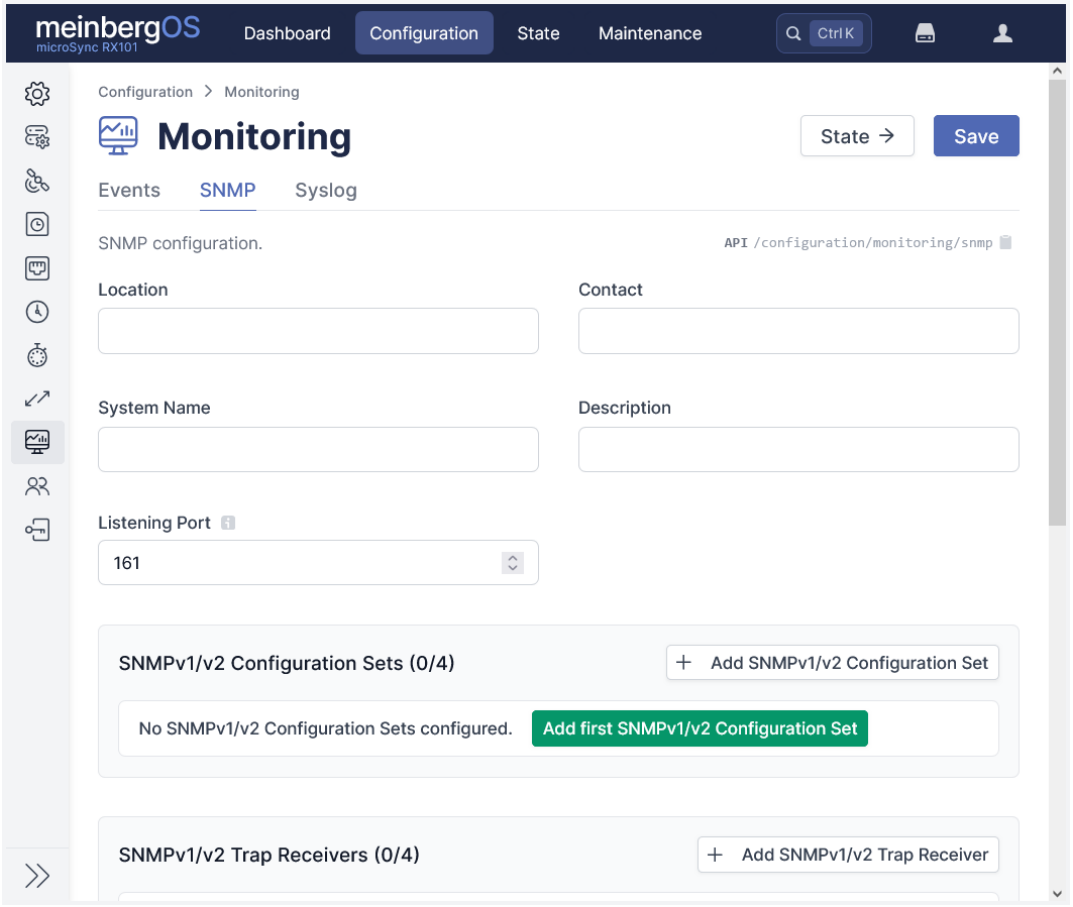


Figure 7.32: meinbergOS Web Interface: "Configuration → Monitoring → SNMP" Tab

This tab allows you to configure SNMP traps and polling for your meinbergOS device.

Location: This can be used to specify a physical location for the meinbergOS device, such as a rack number or server room, that will be transmitted via SNMP.

Contact: This can be used to name a contact person for the meinbergOS device to be transmitted via SNMP.

System Name: This can be used to assign an identifiable name to the meinbergOS device to be transmitted via SNMP.

Description: This can be used to assign an additional descriptive text for the meinbergOS device that will be transmitted via SNMP for display in an SNMP manager.

Listening Port: The port on which the meinbergOS device will listen for GET and SET requests from an SNMP manager. This is *161* as standard, but can be set to another port if the SNMP manager is configured to send requests on another port.

SNMPv1/v2 Configuration Sets

These options relate to how the meinbergOS device will handle incoming SNMPv1 and SNMPv2c GET and SET requests transmitted by SNMP managers.

Version: The SNMP version to be used; this will depend on what your SNMP management solution supports.

Access Type: Specifies which requests the meinbergOS device will accept from an SNMP manager. If *Read-only* is selected, the SNMP manager will only be able to send GET requests to receive data from the meinbergOS device. If *Read-write* is selected, the SNMP manager will also be able to modify data on the meinbergOS device by means of SET requests.

Community (User Level): Specifies the required community of the SNMP manager. The options in this list draw upon the user levels configured for this meinbergOS device (see → Chapter 7.10.3, "Configuration - Users - Levels").

SNMPv1/v2 Trap Receivers

These options relate to how the meinbergOS device will transmit SNMPv1 and/or SNMPv2c traps to SNMP managers within the network.

Version: The SNMP version to be used; this will depend on what your SNMP management solution supports.

Receiver Address: The address or hostname of the SNMP trap receiver (i.e., SNMP manager).

Destination Port: The UDP port number on which the trap receiver expects to receive SNMP traps. The standard port for SNMP traps is *162*, but this can be set to another value if your SNMP manager is configured to receive traps on another port.

Community (User Level): Specifies the required community of the SNMP manager. The options in this list draw upon the user levels configured for this meinbergOS device (see → Chapter 7.10.3, "Configuration - Users - Levels").

SNMPv3 Configuration Sets

These options relate to how the meinbergOS device will handle incoming SNMPv3 GET and SET requests transmitted by SNMP managers.

Access Type: Specifies which requests the meinbergOS device will accept from an SNMPv3 manager. If *read-only* is selected, the SNMP manager will only be able to send GET requests to receive data from the meinbergOS device. If *read-write* is selected, the SNMP manager will also be able to modify data on the meinbergOS device by means of SET requests.

User Name: Specifies the user defined on the meinbergOS device that the SNMP manager must use to log in to the meinbergOS device.

Security Level: Specifies which combination of *auth* (authentication) and *priv* (encryption) should be used in communications with the SNMP manager. This will depend largely on the common encryption types supported by meinbergOS and your SNMP manager for authentication and encryption, and also whether the SNMP manager is used to exclusively monitor or also control the meinbergOS device.

Authentication Protocol: If *auth* is enabled in the security level, this is used to select which cryptographic function will be used to hash the data: *None*, *MD5*, *SHA*, *SHA224*, *SHA256*, *SHA384*, *SHA512*

Authentication Password: If *auth* is enabled in the security level, this is used to define the shared secret between the meinbergOS device and the SNMPv3 manager that will allow each SNMPv3 message to be authenticated by the recipient.

Privacy Protocol: If *priv* is enabled in the security level, this is used to select which cryptographic function will be used to encrypt the data: *None*, *DES*, *AES*, *AES192*, *AES256*.

Privacy Password: If *priv* is enabled in the security level, this is used to define the shared secret between the meinbergOS device and the SNMPv3 manager that will allow a recipient in possession of this shared secret to decrypt SNMPv3 messages.

Additional Configuration: This text box can be used to specify additional parameters to append to the SNMP configuration. The inputs here should follow the structure and syntax of the file `snmpd.conf` used by Net-SNMP.

7.9.3 Configuration - Monitoring - Syslog

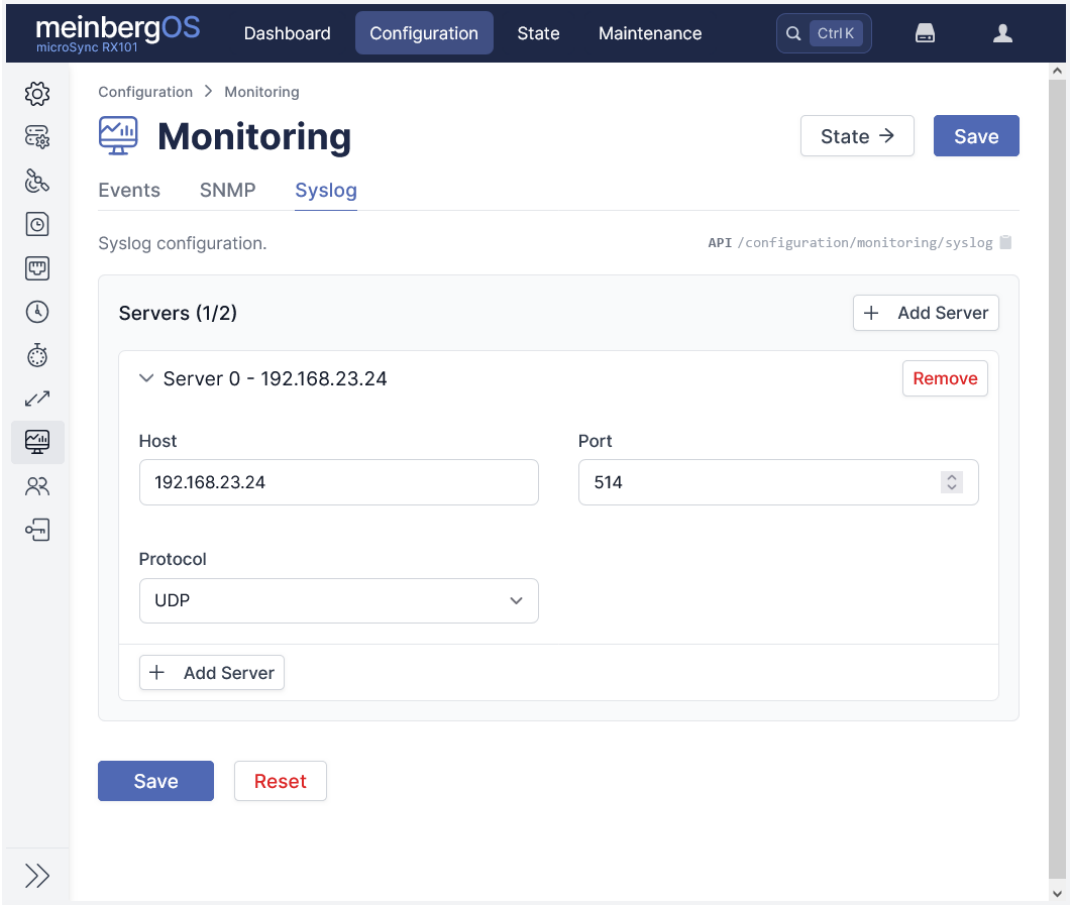


Figure 7.33: meinbergOS Web Interface: "Configuration → Monitoring → Syslog" Tab

This tab allows you to configure *syslog* servers that will receive event notifications from your meinbergOS device. To add a server, click on the button "**+ Add Server**".

Host: The address or hostname of the *syslog* server.

Port: The port on which the *syslog* server instance will receive the notifications. The standard port for *syslog* is *514*, but this can be changed if your *syslog* server is listening for notifications on a different port.

Protocol: The protocol via which syslog notifications will be sent by the meinbergOS device. As of meinbergOS *2024.12.4*, only *UDP* is supported.

7.10 Configuration - Users

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

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

More information: ➜ Chapter 7.10.1, "Configuration - Users - Local Accounts"

Remote Accounts: This tab is where the meinbergOS device's *remote* user accounts (accounts that are looked up via RADIUS and TACACS+ authentication services) are managed. It provides functions for creating and deleting remote accounts as well as assigning or revoking permissions.

More information: ➜ Chapter 7.10.2, "Configuration - Users - Remote Accounts"

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

More information: ➜ Chapter 7.10.3, "Configuration - Users - Levels"

Password Rules: This tab allows minimum standards to be defined regarding the security of user account passwords, including minimum length, diversity of character types, and similarity to previous passwords.

More information: ➜ Chapter 7.10.4, "Configuration - Users - Password Rules"

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 and out of the ability to perform a factory reset.

7.10.1 Configuration - Users - Local Accounts

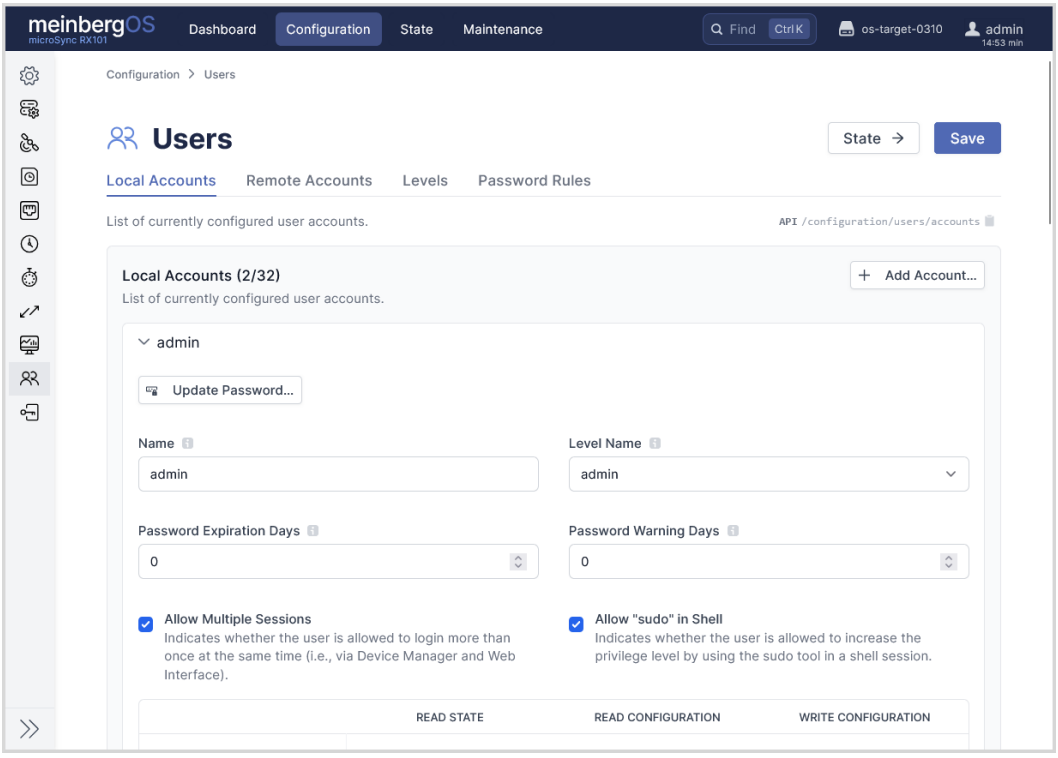


Figure 7.34: meinbergOS Web Interface: "Configuration → Users → Local Accounts" Tab

Important!

meinbergOS *2024.12* introduces a fundamental change to how users are managed within meinbergOS. Since *2024.12.0*, permissions are no longer assigned on a **per-user** basis, but rather on a **per-level** basis. As such, all users must be assigned a user level and this level dictates most of the permissions assigned to that user.

As such, if you have recently upgraded to meinbergOS *2024.12.4* from a previous version, a review of your user permissions is strongly recommended.

The following settings can be modified in this tab (Fig. 7.34):

Name:	The unique name of the user account.
Level Name:	The user level to which this user is to be assigned. This user level dictates the permissions that the user will have. For more information, please refer to → Chapter 7.10.3, "Configuration - Users - Levels".
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 CLI (Shell), another via the Web Interface).
Allow "sudo" in Shell:	Specifies whether the account is granted elevated privileges in a shell session when using the **sudo** tool.

At the bottom of each user's panel is a table showing the read/write permissions of the user. These permissions are derived from the selected user level. Once changes to the user have been saved, the current permissions from the selected user level will be reflected in this table.

Information:

For more information on the effects of the various permissions on users accounts, please refer to → Chapter 11.1, "User Permissions".

7.10.2 Configuration - Users - Remote Accounts

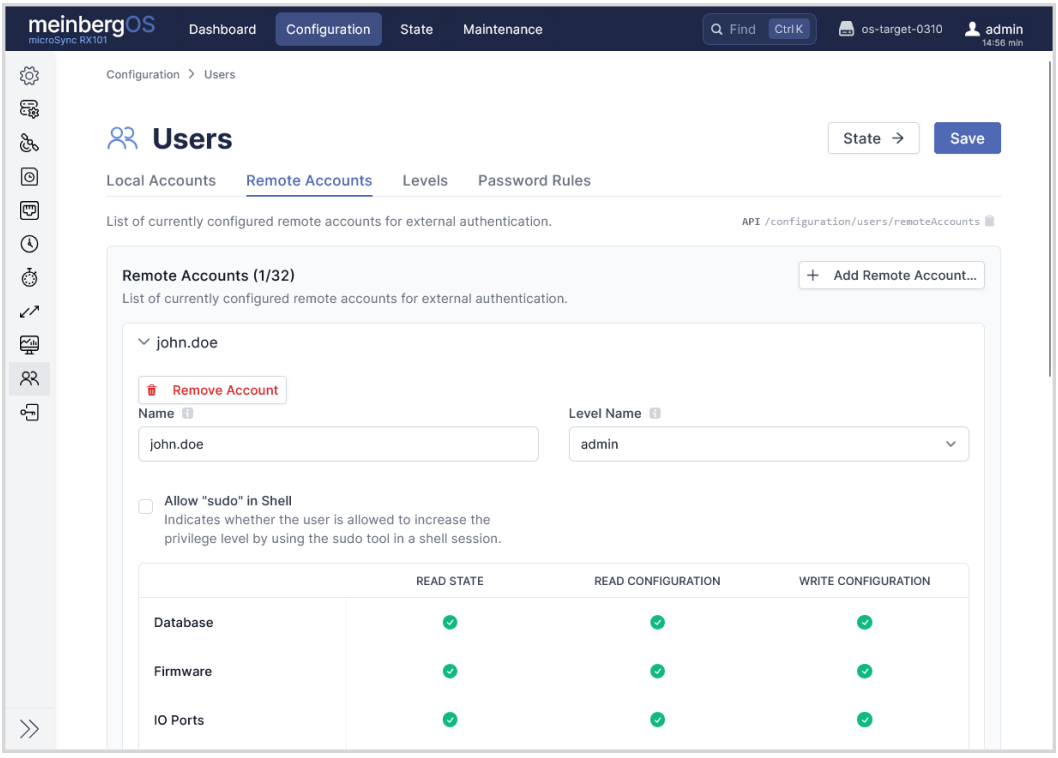


Figure 7.35: meinbergOS Web Interface: "Configuration → Users → Remote Accounts" Tab

Information:

The manual creation of remote accounts on your meinbergOS device is only required for RADIUS and TACACS+ authentication where no user level has been defined as an external template for RADIUS/-TACACS+. It is **not** required for LDAP authentication.

The following settings can be modified in this tab (Fig. 7.34).

Name: The unique name of the user account.

Level Name: The user level to which this user is to be assigned. This user level dictates the permissions that the user will have. For more information, please refer to → Chapter 7.10.3, "Configuration - Users - Levels".

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

At the bottom of each user's panel is a table showing the read/write permissions of the user. These permissions are derived from the selected user level. Once changes to the user have been saved, the current permissions from the selected user level will be reflected in this table.

Information:

For more information on the effects of the various permissions on user accounts, please refer to → Chapter 11.1, "User Permissions".

For more information on the configuration of remote acccounts, please refer to → Chapter 7.11, "Configuration - Authentication".

7.10.3 Configuration - Users - Levels

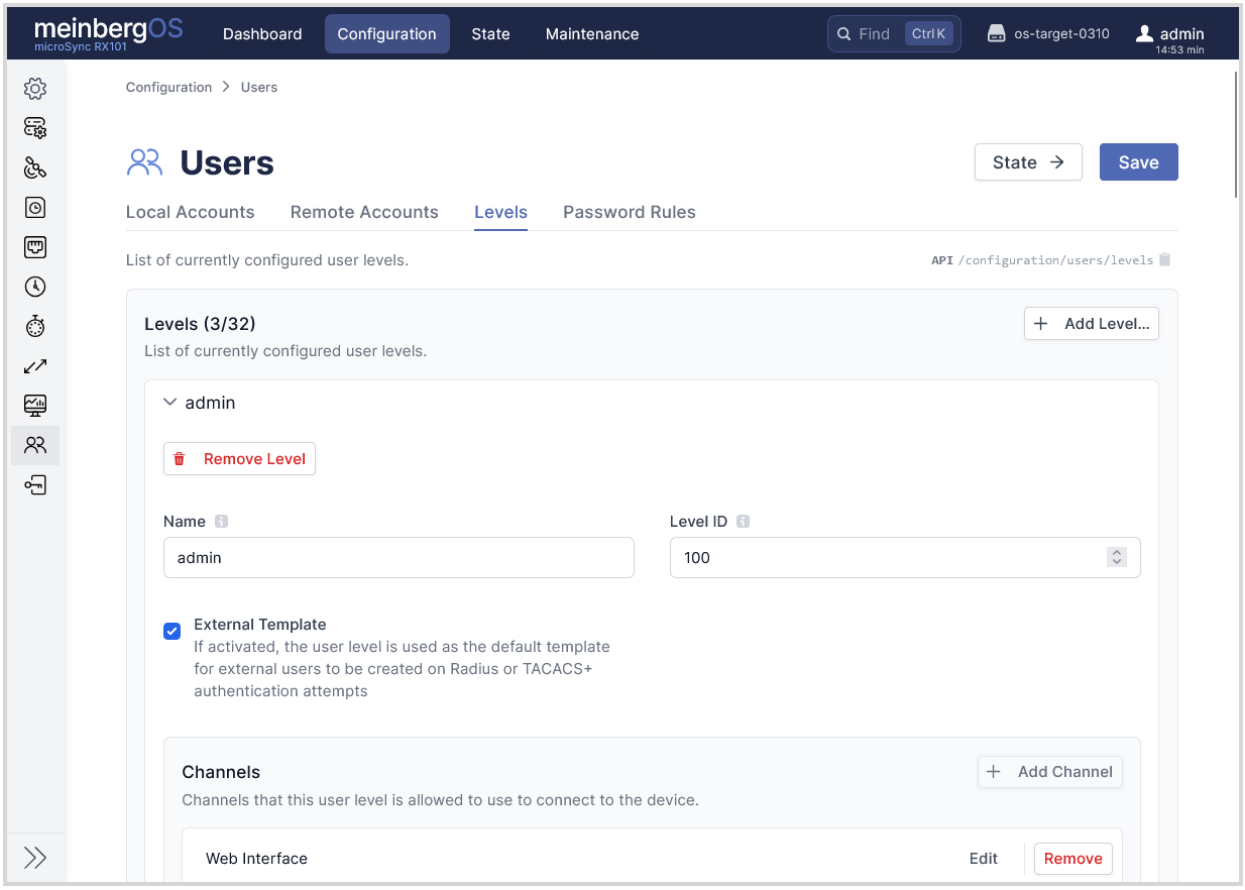


Figure 7.36: meinbergOS Web Interface: "Configuration → Users → Accounts" Tab

The "**Configuration → Users → Levels**" tab (Fig. 7.36) is used to define or modify the user levels that provide the basis for the security definition of user accounts. User levels establish the permissions that user accounts possess, and changes to these user levels filter down to the member user accounts.

It is also possible to define a user level as an "external template" that lays out the permissions for accounts created for authentication via RADIUS or TACACS+.

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.

External Template: If enabled, this template will be used to set the permissions of new Remote Accounts created via RADIUS and TACACS+ authentication (i.e., meinbergOS accounts that are created automatically as a result of successful RADIUS or TACACS+ authentication).

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

Important!

Removing Web Interface access from a user level which the current user is a member of will cause the account to be immediately logged out, and it will only be possible to regain access through another account with another user level or via a channel that has been enabled for the user level.

Permissions: This table lists a variety of permissions for your meinbergOS device; if you wish to enable or disable all read/write permissions for a certain element, select "**All**".

Information:

For more information on the effects of the various permissions on user accounts, please refer to → Chapter 11.1, "User Permissions".

7.10.4 Configuration - Users - Password Rules

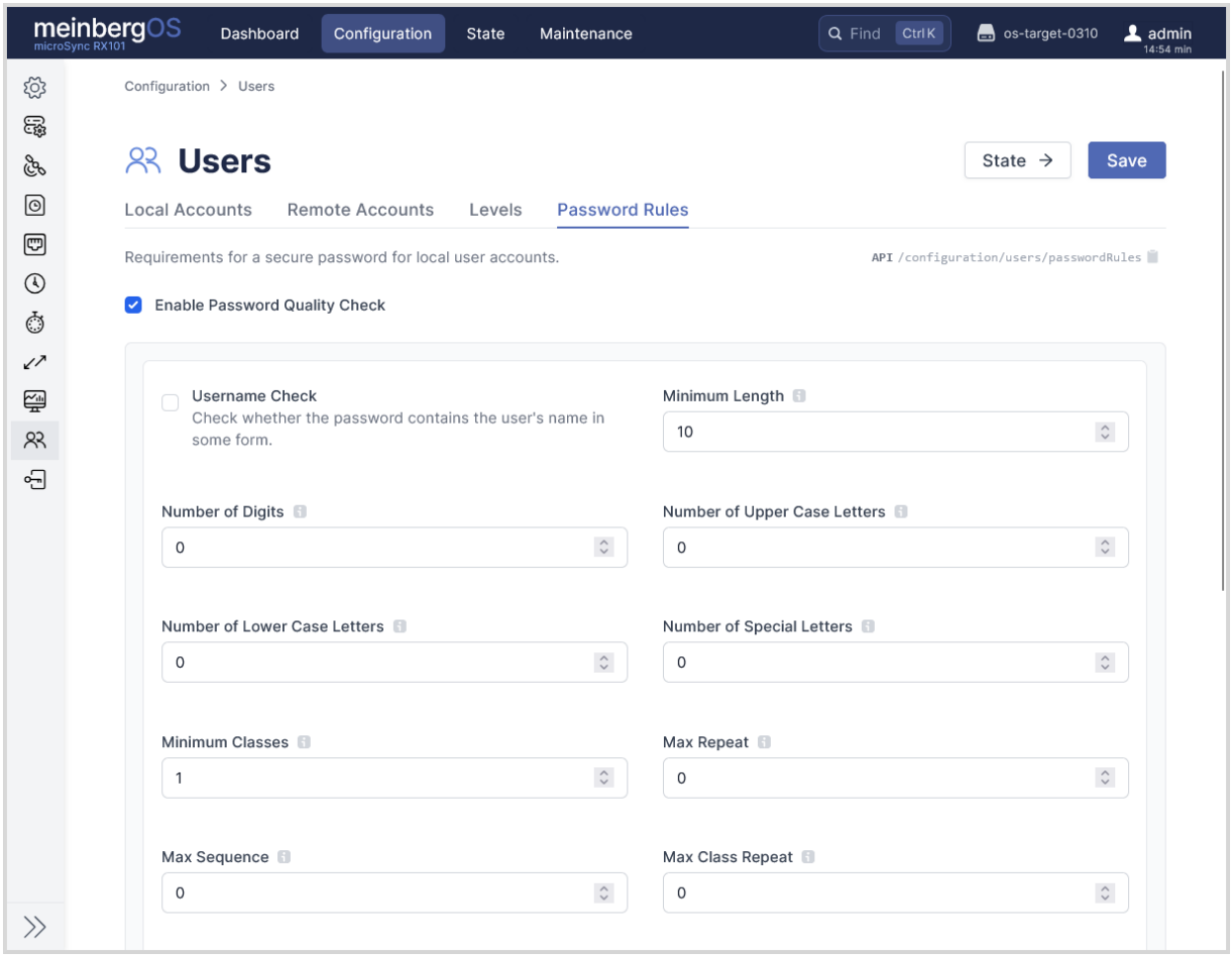


Figure 7.37: meinbergOS Web Interface: "Configuration → Users → Password Rules" Tab

Information:

These options only concern the rules regarding the definition of the local passwords themselves in terms of character usage and similarity.

Password validity time policies for local accounts are configured on a per-user basis under "**Configuration - Users - Local Accounts**".

Password validity time policies *and* password definition rules for remote accounts are governed by your directory services and account authentication infrastructure.

The "**Configuration** → **Users** → **Password Rules**" tab (Fig. 7.37) is used to define or modify the rules that define the formulation of new passwords, including character counts, similarities with previous passwords, forbidden words, and character repetition.

Enable Password Quality Check: If enabled, password changes will be monitored for compliance with quality rules as defined using the options below.

Username Check: If enabled, the password quality control will check if the password contains the username in some form.

Minimum Length: The minimum number of characters required for a new password.

Number of Digits: The number of numerical digits required in any new password.

Number of Upper Case Letters: The number of upper case letters required in any new password.

Number of Lower Case Letters: The number of lower case letters required in any new password.

Number of Special Letters: The number of special characters (symbols and other characters that do not classify as numerical characters, upper case letters, or lower case letters) required in any new password.

Minimum Classes: The minimum number of character classes (numerical digits, upper case letters, lower case letters, special characters) that must be present in any new password. Please note that the values *0* (check disabled) and *1* (one class required at minimum) are functionally identical.

For example, if set to *2*, the passwords `PasSword` (upper and lower cases) and `password123` (lower case and numerical characters) would be permitted, but the password `PASSWORD` (only upper case) would be rejected.

Max Repeat: The maximum permitted number of consecutive repetitions of a single character in any new password.

For example, if set to *3*, the passwords `password123` and `password111` would be permitted, but the password `password1111` would be rejected, as this password contains four consecutive uses of the character `1`. If this value is set to *1*, on the other hand, none of the aforementioned passwords would be permitted, as not only do some contain repetitions of the character `1`, but the word *password* itself also contains a repetition of the letter *s*.

Max Sequence: The maximum permitted number of sequential characters of the same type in any new password. Sequential characters can be forward or reverse sequences, e.g., `12345`, `98765`, `abcde`, `ZYXWV`.

For example, if set to *3*, the passwords `password123` and `abc123` would be permitted, but the password `passWORD1234` would be rejected, as this password contains the four sequential characters `1234`.

Max Class Repeat: The maximum permitted number of consecutive characters of the same type in any new password.

For example, if set to *3*, the passwords `paSSwoRD123` and `PAS_sWo-RD111` would be permitted, but the password `passWORD123` would be rejected, as this password contains four consecutive lower case letters and four consecutive upper case letters.

Similarity Check: This specifies the minimum number of characters that must be different from the previous password to be permitted.

For example, if set to *2* and the old password is `password`, the passwords `p1a2ssword` and `paSSword` will be rejected, whereas `p1a2s3S4w5O6r7D8` would be accepted.

7.11 Configuration - Authentication

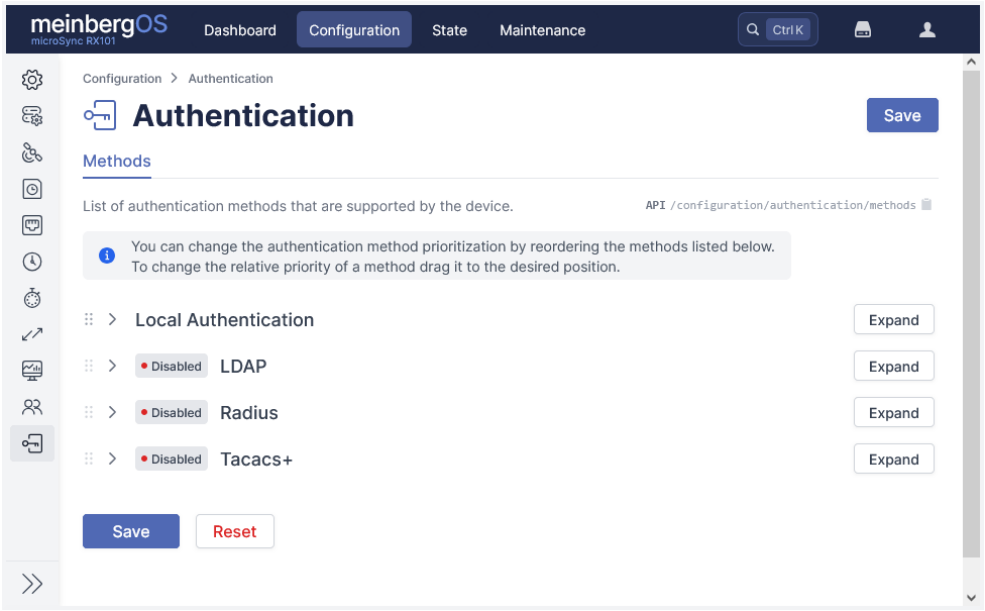


Figure 7.38: meinbergOS Web Interface: "Configuration → Authentication" Tab

The **Authentication** subsection of the **Configuration** section allows you to configure various supported remote authentication standards for use with external user directories.

7.11.1 Local Authentication

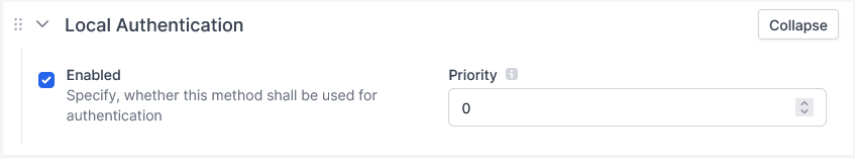


Figure 7.39: meinbergOS Web Interface: Configuring Local Authentication

Local authentication is enabled by default and draws on the local user directory (refer to ➜ Chapter 7.10.1, "Configuration - Users - Local Accounts") for user lookup and authentication.

Please note that no local account can have the same name as an explicitly defined remote account, and it should therefore not generally be possible for the same username & password combination to be authenticated both locally and remotely. However, if an account attempts to authenticate via RADIUS/TACACS+ on the meinbergOS device and that account already exists locally, authentication will be performed using the local credentials for security purposes.

Enabled: Unchecking this box will disable the use of the local users for authentication.

Important!

Meinberg explicitly advises against disabling Local Authentication.

Without a functional external authentication server that is accessible by the meinbergOS device, disabling Local Authentication will result in the meinbergOS device becoming wholly inaccessible with no avenue for authentication. If this occurs, the device will either need to be reset to factory default settings using a Local Factory Reset USB key, or it will need to be sent to Meinberg for repair.

Never disable Local Authentication without having first fully configured and tested your external authentication server access!

If you must exclusively use Remote Authentication with Local Authentication disabled, the preparation of a Local Factory Reset USB key is strongly recommended.

Refer to ➜ Chapter 7.1.3, "Configuration - System - Front Panel Actions" for more information.

Priority: Determines the priority of local authentication for lookup and authentication.

7.11.2 LDAP Authentication

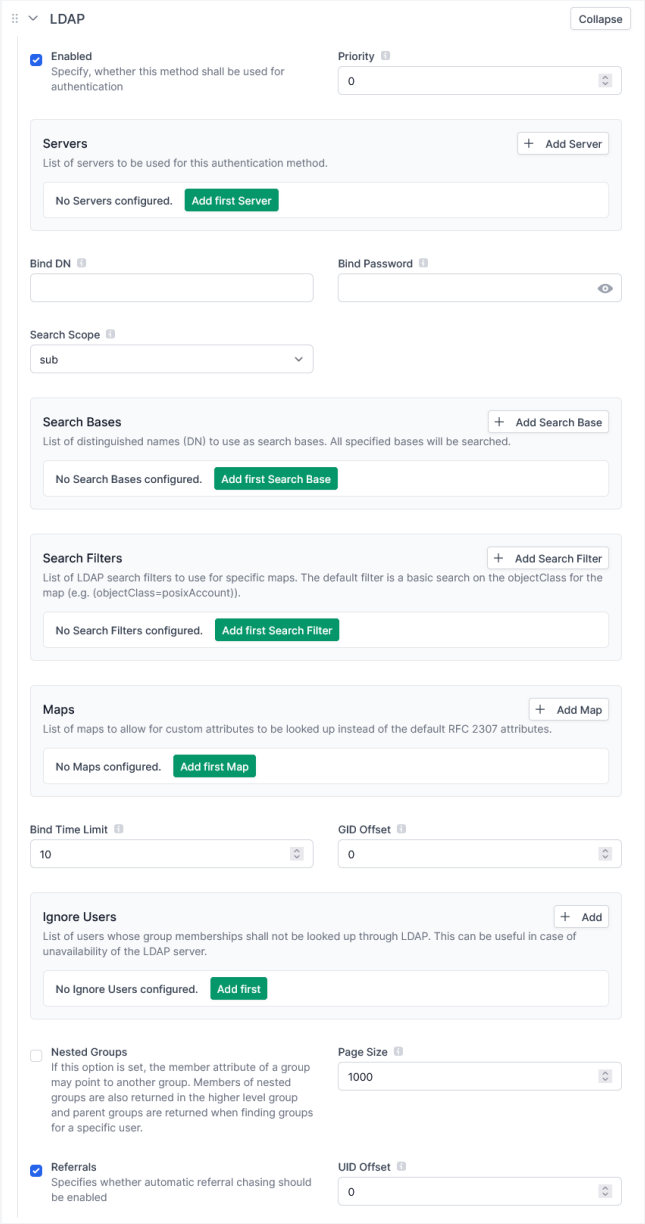


Figure 7.40: meinbergOS Web Interface: Configuring LDAP Authentication

LDAP authentication performs lookup and authentication on one or more specified LDAP (Lightweight Directory Access Protocol) servers.

Information:

meinbergOS uses *nss-pam-ldapd* for lookup and authentication. Accordingly, it is guided by the *nss-pam-ldapd* implementation of group membership for lookups. For more information on *nss-pam-ldapd*, please refer to the project Github page at https://github.com/arthurdejong/nss-pam-ldapd.

Important!

The LDAP implementation in meinbergOS *2024.12.4* requires the directory server to provide a `gidnumber` (group ID) value. If no group ID number is included in the authentication response and `gidnumber` is not mapped via the meinbergOS device, any authentication attempt will fail.

Enabled: Checking this box will enable the use of LDAP authentication.

Priority: Determines the priority of LDAP authentication for lookup and authentication. This field is only displayed if LDAP is enabled.

If accounts with the same username and password exist on multiple remote authentication servers, the authentication will be executed using the authentication method with the highest priority (lowest value).

If accounts with the same username but different passwords exist on multiple remote authentication servers, meinbergOS will continue to process the list in priority order, even if authentication fails on a higher authentication method due to a password mismatch.

Servers: Specifies which servers will be queried for LDAP authentication. Refer to "**Managing LDAP Servers to Query**" below.

Bind DN: If left empty, the meinbergOS device will perform lookups on each LDAP server anonymously. If a Distinguished Name is entered here, this name will be used for binding when performing lookups on each LDAP server.

Bind Password: In conjunction with the Distinguished Name, this is the password required by an LDAP server to allow lookups to be performed.

Search Scope: If *one* is selected, only the direct children of the configured search bases will be searched. If *sub*, the search will drill down to the deepest levels of the tree from each of the search bases.

Search Bases: Specifies distinguished names used for LDAP lookup. Refer to "**Managing LDAP Search Bases**" below.

Search Filters: Specifies search filters used for simplifying LDAP query responses. Refer to "**Managing LDAP Search Filters**" below.

Maps: Specifies attribute maps for custom attributes not defined by RFC 2307/RFC 2307bis. Refer to "**Managing LDAP Search Maps**" below.

Bind Time Limit: Specifies the maximum time in seconds allowed for the meinbergOS device server to bind to an LDAP server. This is set to *10 seconds* by default.

GID Offset: Specifies an offset that is applied to all numeric LDAP Group IDs. This can be helpful for preventing user ID collisions with local user groups or for compatibility purposes when using ObjectSID attributes.

Ignore Users: Specifies any users that should **not** be looked up via LDAP. Refer to "**Managing User Exclusions from LDAP Lookup**" below.

Nested Groups: If enabled, the member attribute of a group may point to another group. When higher-level groups are looked up, members of nested groups will also be returned. When looking up groups for a specific user, all parent groups will be returned.

Page Size: If set to a value greater than zero, this will prompt the LDAP server to return results in 'paged' form, i.e., it will return no more than this maximum number of results for each request, such that another request must be submitted to obtain additional results.

Referrals: If enabled, referrals will be automatically 'chased', i.e., servers provided as referrals in results lists will be queried. If disabled, servers provided as referrals in results lists will be disregarded.

UID Offset: Specifies an offset that is applied to all numeric LDAP User IDs. This can be helpful for preventing user ID collisions with local users or for compatibility purposes when using ObjectSID attributes.

Managing LDAP Servers to Query

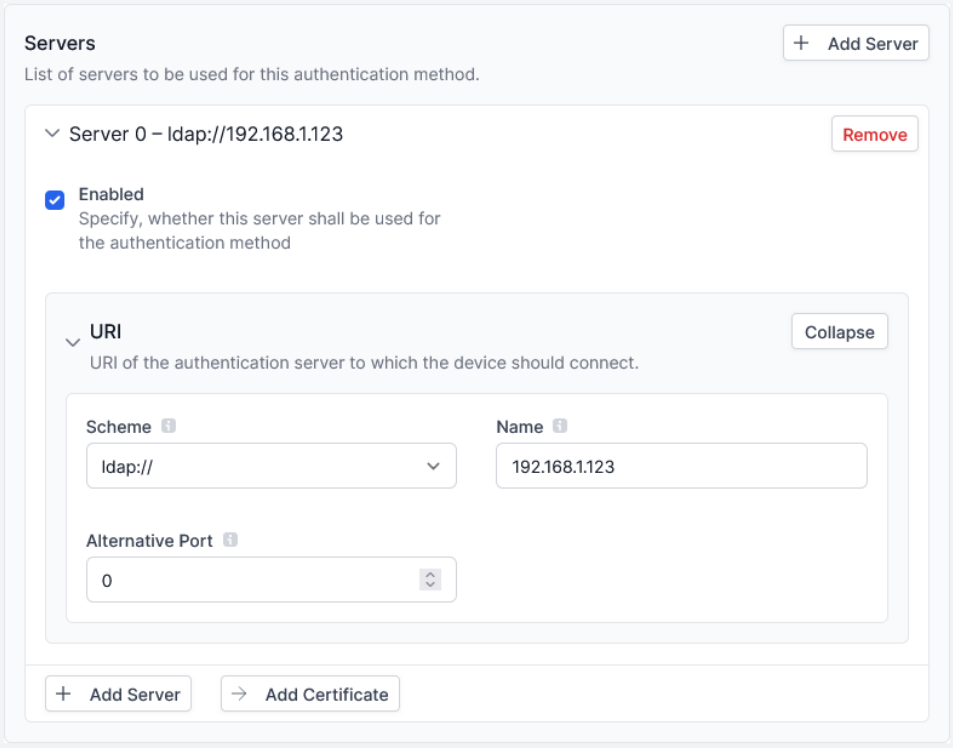


Figure 7.41: meinbergOS Web Interface: Configuring Servers for LDAP Authentication

To add an LDAP server to be bound when authenticating externally via LDAP or LDAPS, click on **+Add Server** or **+Add First Server** under the LDAP panel.

Enabled: Specifies whether this server should be used for LDAP queries. Disabling a server without deleting it allows LDAP lookups to that server to be disabled temporarily, for example if the server is briefly unavailable.

Scheme: Specifies whether the URI used to connect to the LDAP server should be prefixed with `ldap://` (unencrypted LDAP) or `ldaps://` (LDAP over TLS/SSL).

Name: The URI of the LDAP/LDAPS server. This can be a domain-style name or a literal IP address.

Alternative Port: If this value is set to *0*, the meinbergOS device will assume that LDAP connections are to be performed over Port *389* for servers with an `ldap://` prefix or Port *636* for servers with an `ldaps://` prefix. Setting this value to anything other than *0* will override this assumption regardless of the prefix and connect over the specified port.

To remove a server definition, click on the red **Remove** button.

Managing LDAP Search Bases

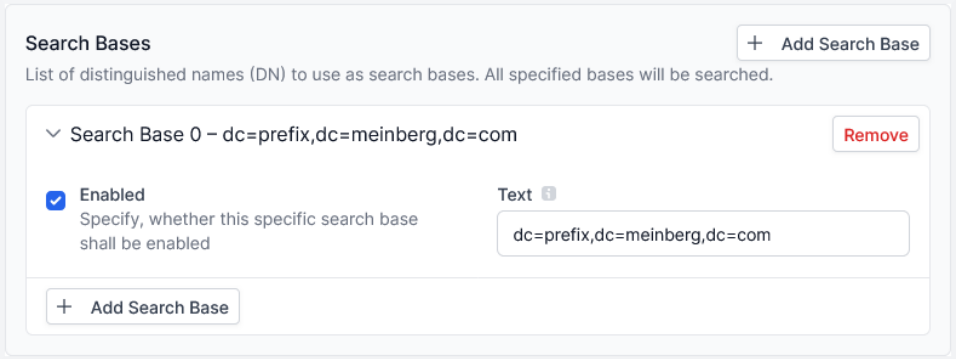


Figure 7.42: meinbergOS Web Interface: Configuring Search Bases for LDAP Authentication

To define a new search base for LDAP searches, **+Add Search Base** or **+Add First Search Base**.

Information:

All configured search bases will be used for all searches, regardless of server.

Enabled: If selected, this search base will be used for LDAP/LDAPS search queries.

Text: This is the search base query and follows the typical LDAP search base syntax (e.g., `ou=groups,dc=example,dc=com`.

To remove a search base, click on the red **Remove** button.

Managing LDAP Search Filters

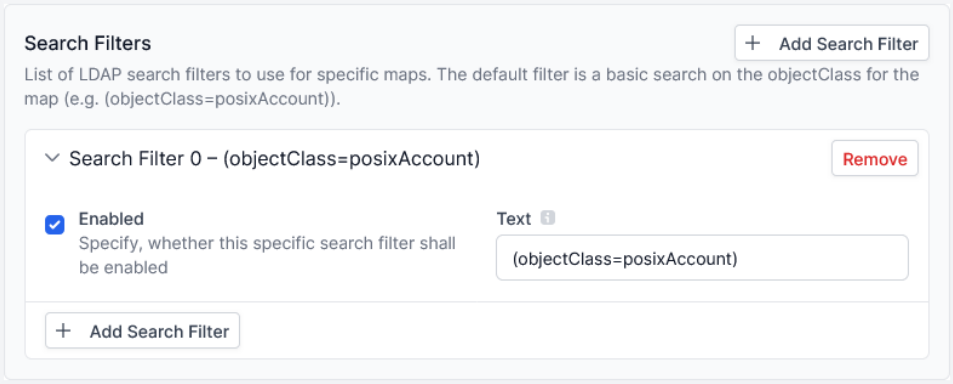


Figure 7.43: meinbergOS Web Interface: Configuring Search Filters for LDAP Lookup

To define a new search filter for LDAP searches, **+Add Search Filter** or **+Add First Search Filter**.

Enabled: If selected, this search filter will be used for LDAP/LDAPS search queries.

Text: This is the search filter expression and follows the standard LDAP search filter syntax.

Information:

For more information on formulating custom LDAP search filters, visit the LDAP filters information page of the official LDAP Project at https://www.openldap.org/doc/admin24/access-control.html.

To remove a search filter, click on the red **Remove** button.

Managing LDAP Attribute Maps

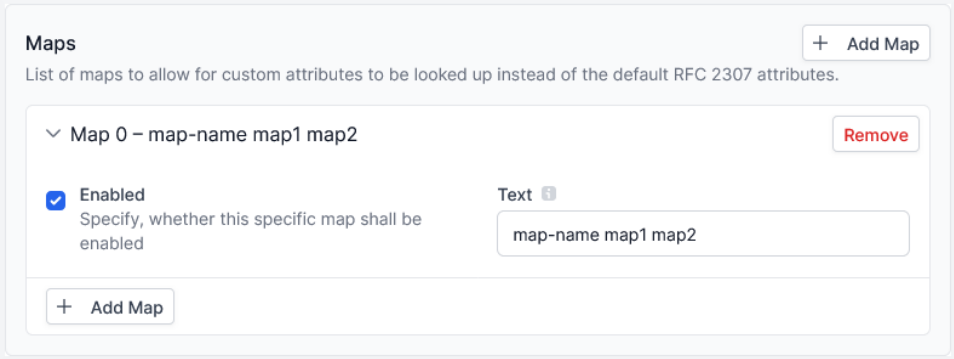


Figure 7.44: meinbergOS Web Interface: Configuring Attribute Maps for LDAP Authentication

By default, users and groups are queried based on the standard LDAP attributes defined in RFC 2307 and RFC 2307bis. If other non-standard attributes are in use, you may define a new search map for LDAP searches by selecting **+Add Map** or **+Add First Map**.

Enabled: If selected, this map will be used to lookup user and group attributes.

Text: This is the search map expression.

To remove a search map, click on the red **Remove** button.

Managing User Exclusions from LDAP Lookup

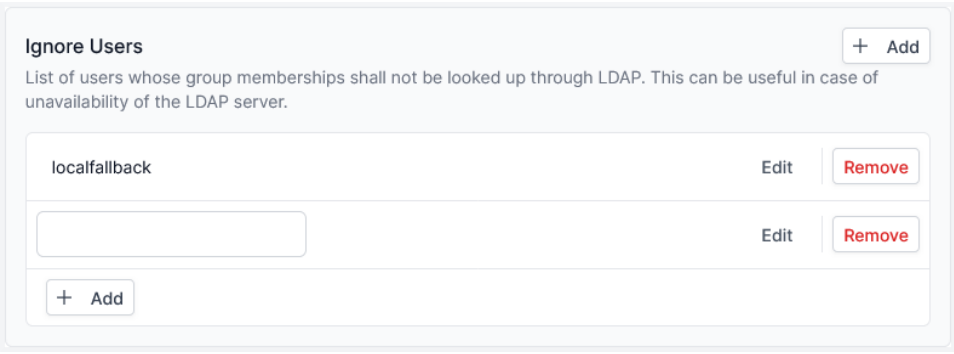


Figure 7.45: meinbergOS Web Interface: Defining Users to be Disregarded in LDAP Authentication

Specific users can be excluded from LDAP lookup during authentication attempts. This can be useful, for example, if the LDAP server is unavailable and a local fallback account is required. In the **Ignore Users** panel, you can define a user to be ignored during LDAP lookups by selecting **+Add** or **Add First** and entering the name.

This name can be modified later by selecting **Edit** or removed by selecting the red **Remove** button.

7.11.3 RADIUS Authentication

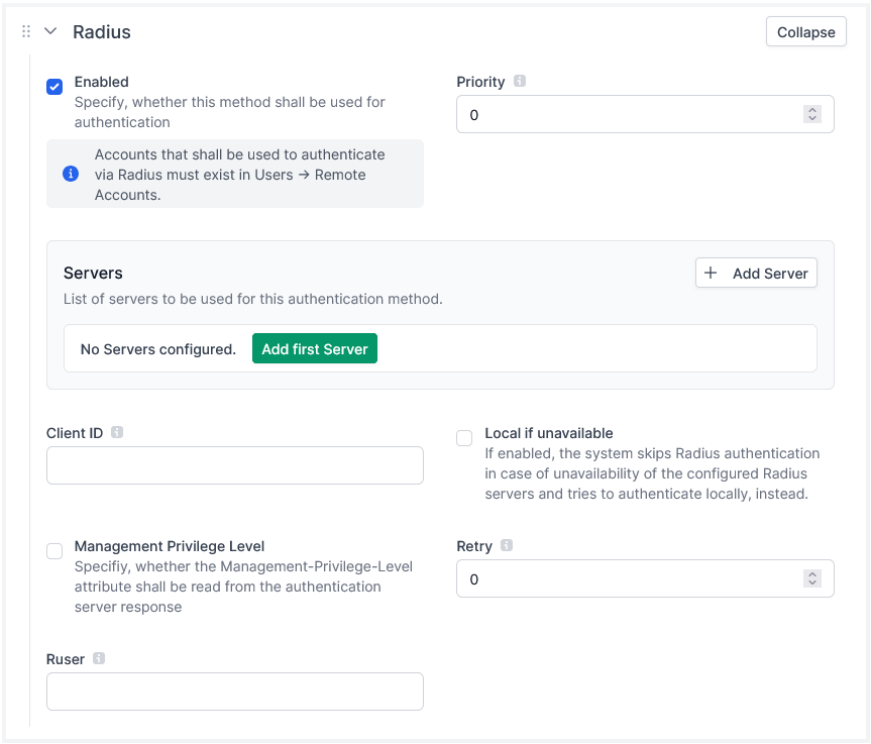


Figure 7.46: meinbergOS Web Interface: Configuring RADIUS Authentication

RADIUS authentication performs lookup and authentication on one or more specified RADIUS servers (refer to → Chapter 7.10.2, "Configuration - Users - Remote Accounts" for more information).

Important!

When authenticating a user against a RADIUS directory service, the following order of priority will be observed in determining the user's authorization level:

- Any Management Privilege Level as provided by the RADIUS server (only if the option **Management Privilege Level** is explicitly enabled)
- The External Template set on the meinbergOS device as the default user level
- A remote account defined explicitly on the meinbergOS device that matches the RADIUS server username

If no Management Privilege Level is provided by the RADIUS server, no External Template is defined, and no corresponding remote account has been created beforehand for the user, authentication will fail regardless of the validity of the credentials.

Please note that if an External Template has been defined, any user configured on the RADIUS server to access the meinbergOS device will automatically recreate their remote account on the meinbergOS if authenticated by the RADIUS server even if the remote account on the meinbergOS device itself has been deleted beforehand.

If you wish to be able to revoke or limit a user's access to the meinbergOS server, you will need to either remove the user from your RADIUS server entirely, prohibit the user via the RADIUS configuration from logging in to the meinbergOS device's IP address, or disable the External Template (see → Chapter 7.10.3, "Configuration - Users - Levels").

Enabled: Checking this box will enable the use of RADIUS authentication.

Priority: Determines the priority of RADIUS authentication for lookup and authentication. This field is only displayed if RADIUS is enabled.

If accounts with the same username and password exist on multiple remote authentication servers, the authentication will be executed using the authentication method with the highest priority (lowest value).

If accounts with the same username but different passwords exist on multiple remote authentication servers, meinbergOS will continue to process the list in priority order, even if authentication fails on a higher authentication method due to a password mismatch.

Servers: Specifies which servers will be queried for RADIUS authentication. Refer to "**Managing RADIUS Servers to Query**" below.

Client ID: Specifies the NAS identifier that will be sent on all outgoing RADIUS communication.

Local If Unavailable: If enabled, the system will skip RADIUS authentication if the configured RADIUS servers are unavailable and will attempt to perform local authentication instead.

Management Privilege Level: If enabled, meinbergOS will prioritize any Management Privilege Level attribute provided by the RADIUS server for the user in assigning the user level. If the server provides no Management Privilege Level for the user, meinbergOS will fall back to any defined External Template or, lacking that, to a defined remote account.

Retry: Specifies the maximum number of consecutive connection attempts with a RADIUS server before authentication is considered to have failed.

Ruser: If your RADIUS server implementation expects a specific value for PAM_RUSER during authentication requests, this can be entered here.

Managing RADIUS Servers to Query

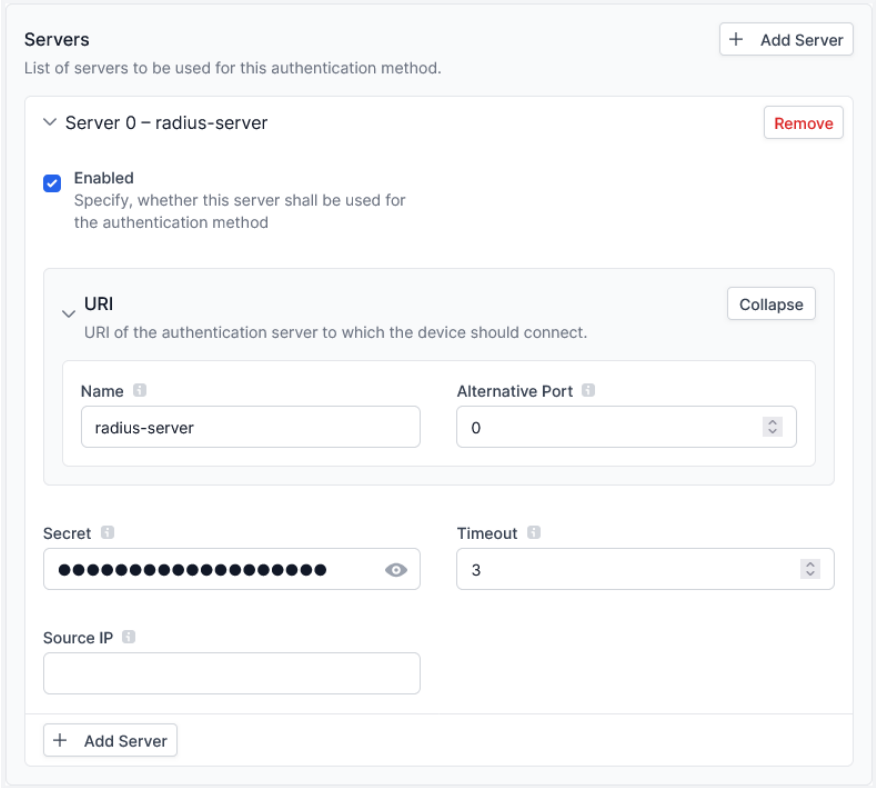


Figure 7.47: meinbergOS Web Interface: Configuring Servers for RADIUS Authentication

To define a new RADIUS server, select **+Add Server** or **+Add First Server** under the RADIUS panel.

Name: The URI of the RADIUS server. This can be a domain-style name or a literal IP address.

Alternative Port: If this value is set to 0, the meinbergOS device will assume that RADIUS authentication connections are to be performed over Port *1812*. Setting this value to anything other than *0* will override this assumption regardless of the prefix and connect over the specified port.

Secret: The shared secret (common password) used by both the meinbergOS device and RADIUS authentication server to encrypt passwords and server responses.

Timeout: The number of seconds that the meinbergOS device will wait for before a connection is deemed to have timed out.

Source IP: Specifies an optional IP address to be sent as the "source IP address" for authentication requests sent to the server.

To remove a server definition, click on the red **Remove** button.

7.11.4 TACACS+ Authentication

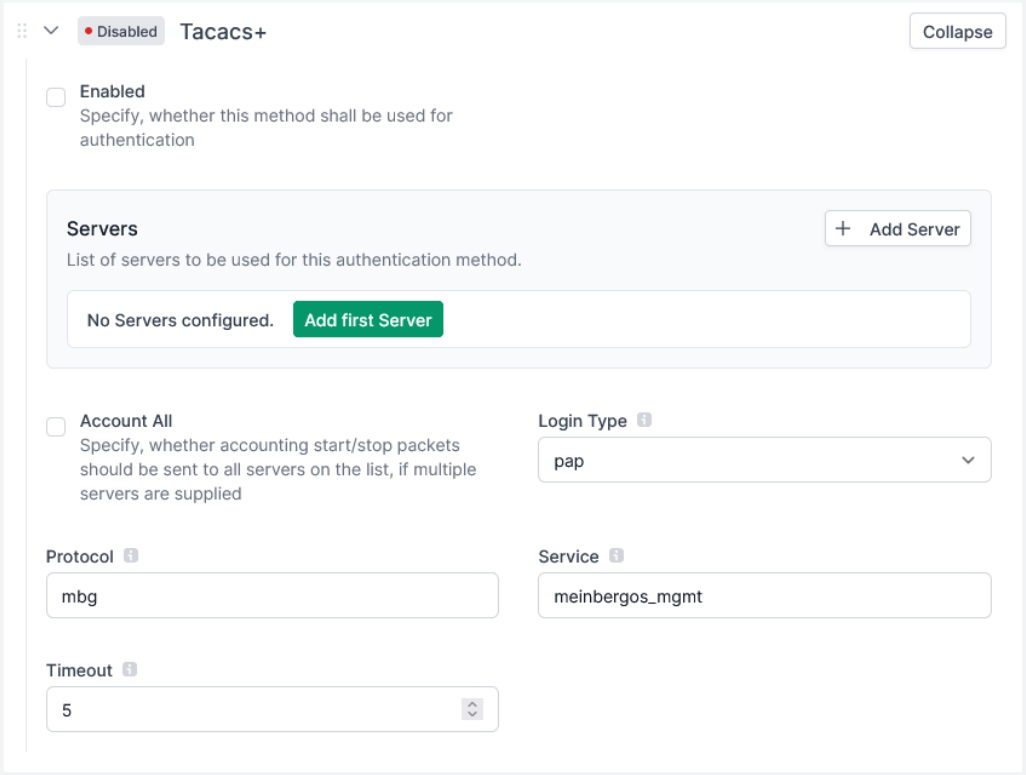


Figure 7.48: meinbergOS Web Interface: Configuring TACACS+ Authentication

TACACS+ authentication performs lookup and authentication on one or more specified TACACS+ servers (refer to → Chapter 7.10.2, "Configuration - Users - Remote Accounts" for more information).

Important!

When authenticating a user against a TACACS+ directory service, the following order of priority will be observed in determining the user's authorization level:

- A remote account defined explicitly on the meinbergOS device that matches the TACACS+ server username
- The External Template set on the meinbergOS device as the default user level

If no External Template is defined and no corresponding remote account has been created beforehand for the user, authentication will fail regardless of the validity of the credentials.

Please note that if an External Template has been defined, any user configured on the TACACS+ server to access the meinbergOS device will automatically recreate their remote account on the meinbergOS device if authenticated by the TACACS+ server, even if the remote account on the meinbergOS device itself has been deleted beforehand.

If you wish to be able to revoke or limit a user's access to the meinbergOS server, you will need to either remove the user from your TACACS+ server entirely, prohibit the user via the TACACS+ configuration from logging in to the meinbergOS device's IP address, or disable the External Template (see → Chapter 7.10.3, "Configuration - Users - Levels").

Enabled: Checking this box will enable the use of TACACS+ authentication.

Priority: Determines the priority of TACACS+ authentication for lookup and authentication. This field is only displayed if TACACS+ is enabled.

If accounts with the same username and password exist on multiple remote authentication servers, the authentication will be executed using the authentication method with the highest priority (lowest value).

If accounts with the same username but different passwords exist on multiple remote authentication servers, meinbergOS will continue to process the list in priority order, even if authentication fails on a higher authentication method due to a password mismatch.

Servers: Specifies which servers will be queried for TACACS+ authentication. Refer to "**Managing TACACS+ Servers to Query**" below.

Account All: If enabled, accounting start & stop packets will be sent to all TACACS+ servers configured on the meinbergOS device.

Login Type: Specifies the login protocol to be used: *login*, *PAP*, or *CHAP*.

Protocol: Specifies the TACACS+ protocol to be used for authorization and accounting.

Service: Specifies the TACACS+ service name to be used for authorization and accounting.

Timeout: Specifies how long a connection should be attempted for before timing out.

Managing TACACS+ Servers to Query

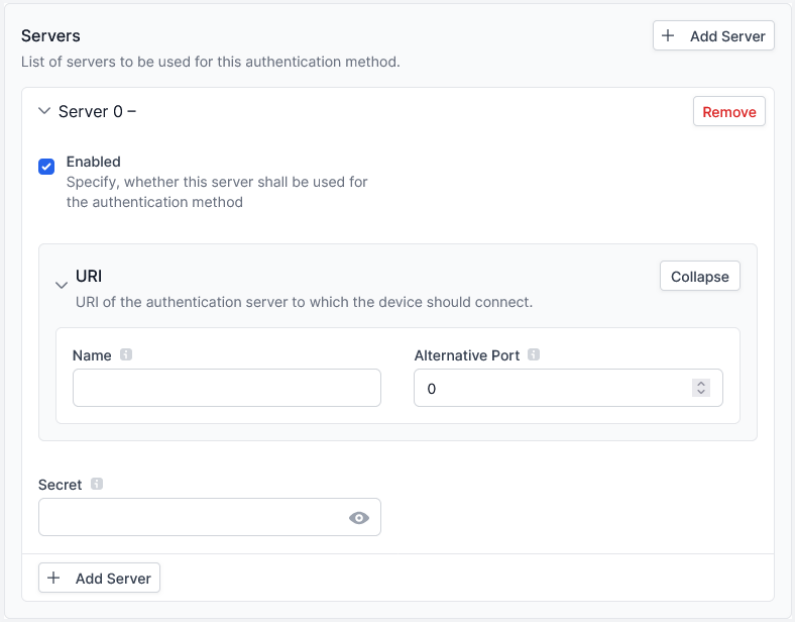


Figure 7.49: meinbergOS Web Interface: Configuring Servers for TACACS+ Authentication

To define a new TACACS+ server, select **+Add Server** or **+Add First Server** under the TACACS+ panel.

Name: The URI of the TACACS+ server. This can be a domain-style name or a literal IP address.

Alternative Port: If this value is set to 0, the meinbergOS device will assume that TACACS+ authentication connections are to be established over TCP Port 49. Setting this value to anything other than 0 will override this assumption regardless of the prefix and connect over the specified port.

Secret: The shared secret (common password) used by both the meinbergOS device and TACACS+ authentication server to encrypt passwords and server responses.

To remove a server definition, click on the red **Remove** button.

8 State

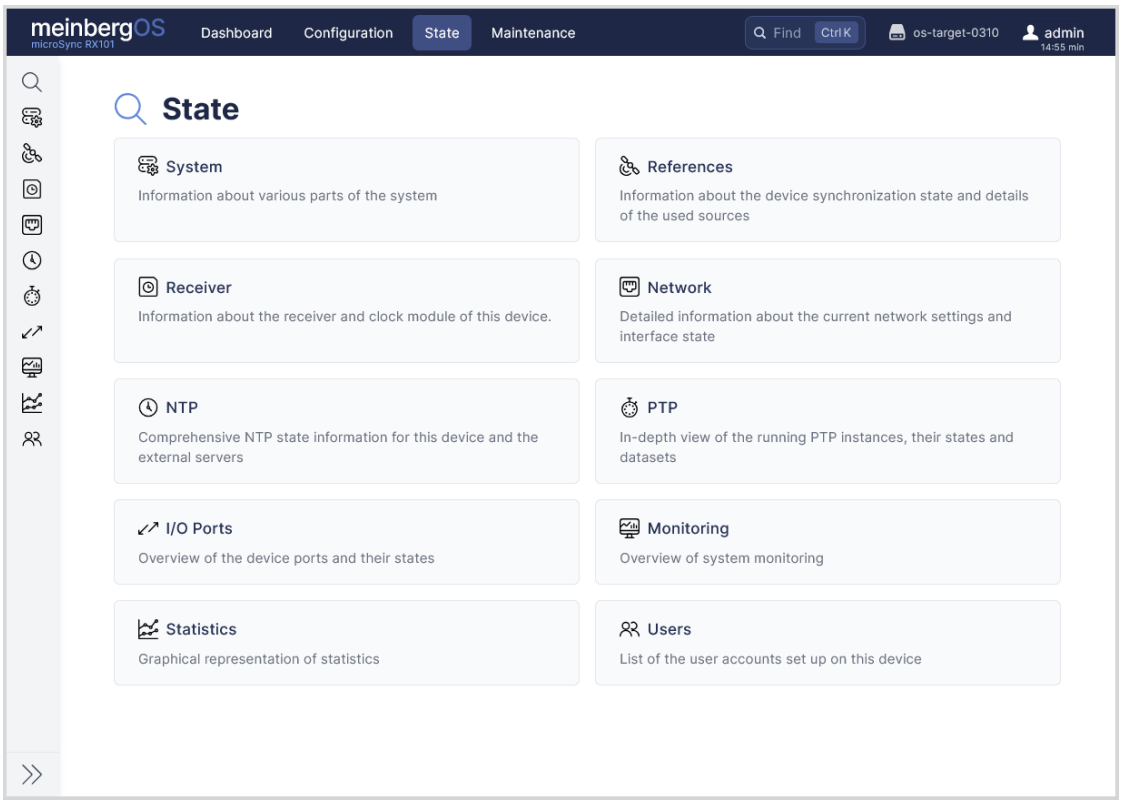


Figure 8.1: meinbergOS Web Interface: "State" Section

The **State** section of the meinbergOS Web Interface (Fig. 8.1) provides you with a wealth of information about the status of your meinbergOS device, including an overview of the various reference sources, network connectivity and redundancy, NTP and PTP functionality, I/O ports, and user access.

In many subsections, the "**Configuration**" button at the top right provides easy access to the corresponding subsection in the **Configuration** section, insofar as one exists.

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.

8.1 State - System

The "**State** → **System**" 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.

Firmware: This tab hosts information about the current meinbergOS version.

More information: → Chapter 8.1.1, "State - System - Firmware"

Hardware: This tab hosts information about the hardware on which this version of meinbergOS is currently running.

More information: → Chapter 8.1.2, "State - System - Hardware"

Power Supplies: This tab hosts information about the power supply capabilities of the meinbergOS device, both regarding currently installed power supply modules and general hardware support.

More information: → Chapter 8.1.3, "State - System - Power Supplies"

Resources: This tab hosts information about the current usage and availability of system resources, as well as the current uptime of the system since the last start or restart.

More information: → Chapter 8.1.4, "State - System - Resources"

8.1.1 State - System - Firmware

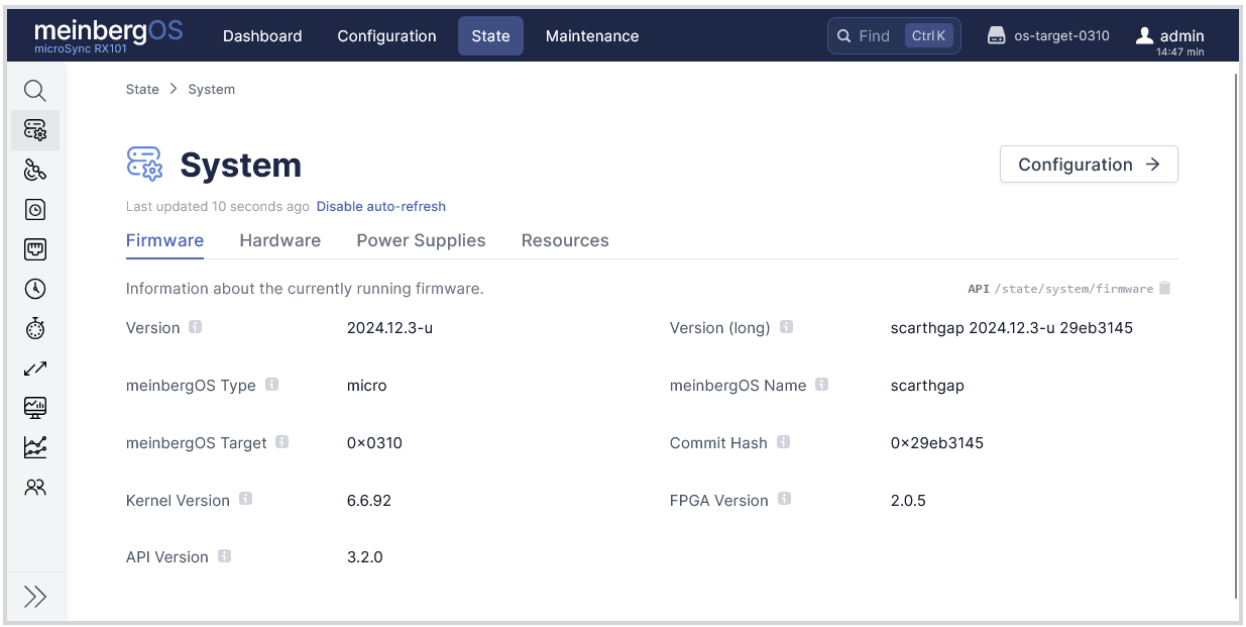


Figure 8.2: meinbergOS Web Interface: "State → System → Firmware" Tab

This tab hosts information about the current meinbergOS version and a number of its components as well as the current FPGA design.

Version: The meinbergOS version number that is currently activated and running.

Version (Long): The full meinbergOS version identifier, including the major version code name (**meinbergOS Name**) and the most recent commit hash. This is generally only useful when using early releases of meinbergOS provided directly by Meinberg and discussing these with Meinberg's Technical Support or developers.

meinbergOS Type: The type of meinbergOS build that is currently running on this device. This will generally be *micro*.

meinbergOS Name: The code name of the meinbergOS main version that is currently activated and running. In the case of meinbergOS *2024.12*, this is *scarthgap*. meinbergOS version codenames follow those of the Yocto version that Meinberg uses to develop each embedded OS version.

meinbergOS Target: This value represents a unique identifier for the CPU and its generation and variant to allow meinbergOS to correctly identify appropriate software updates.

Commit Hash: This value is the hash identifier for the most recent commit to Meinberg's internal meinbergOS *git* repository. For end users, this value is only useful when installing a development version of the operating system provided directly by a Meinberg technician or engineer and discussing this version with Meinberg.

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.

API Version: The version of the REST API used in the currently activated meinbergOS version.

8.1.2 State - System - Hardware

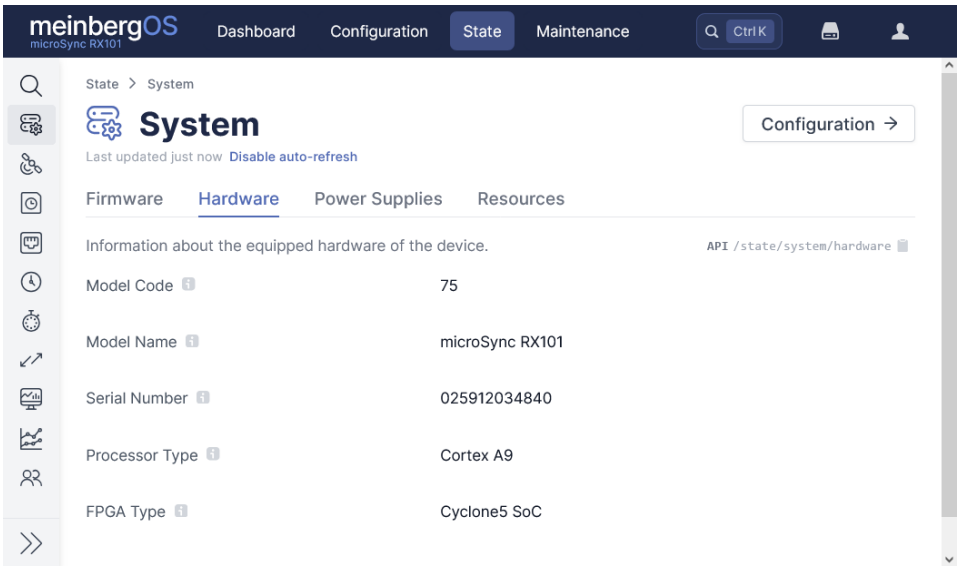


Figure 8.3: meinbergOS Web Interface: "State → System → Hardware" Tab

This tab hosts information about the hardware and model designation of the 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.

8.1.3 State - System - Power Supplies

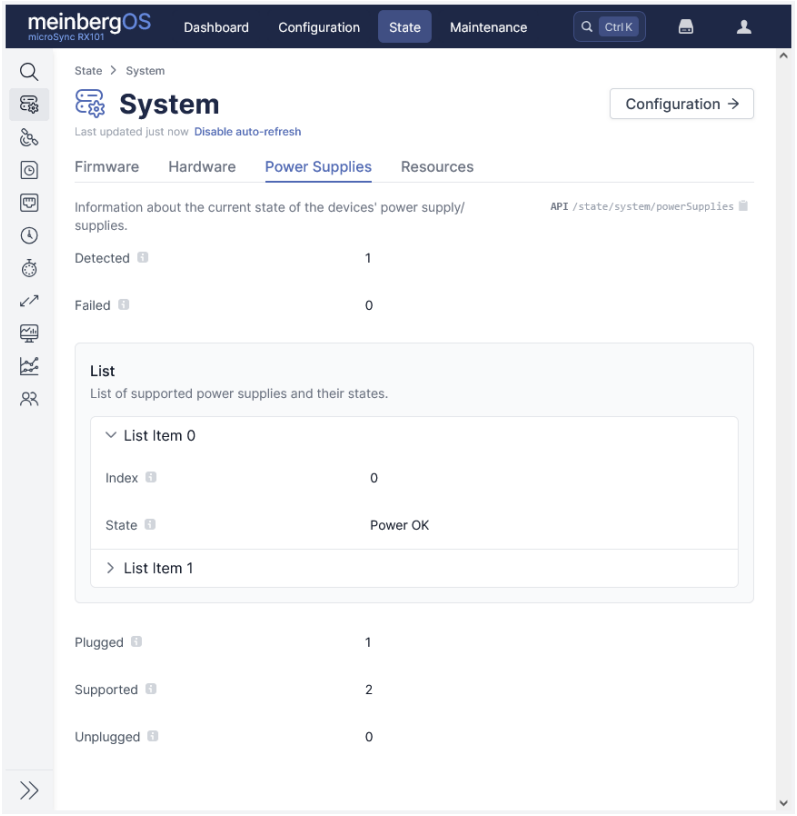


Figure 8.4: meinbergOS Web Interface: "State → System → Power Supplies" Tab

Information:

The information in this tab is primarily intended for users of meinbergOS devices such as the microSync^{RX} with user-replaceable, hot-pluggable power supply modules. While this tab is visible in devices with non-modular power supply units such as the microSync^{HR} or microSync^{XS}, the information of limited relevance for those devices.

This tab hosts information about the power supply modules of the meinbergOS device.

Detected: The current number of power supply modules installed in the meinbergOS device and successfully detected.

Failed: The current number of power supply modules installed in the meinbergOS device for which problems have been identified.

List: This shows an expandable and collapsible list of the installed power supplies, showing their current reported operating state.

Plugged: The number of power supply modules currently plugged in, whether successfully detected or otherwise.

Supported: The total number of theoretically supported power supply modules, i.e., the number of power supply module bays in the meinbergOS device.

Unplugged: The total number of power supply slots that previously had a module plugged in but now do not since last boot.

8.1.4 State - System - Resources

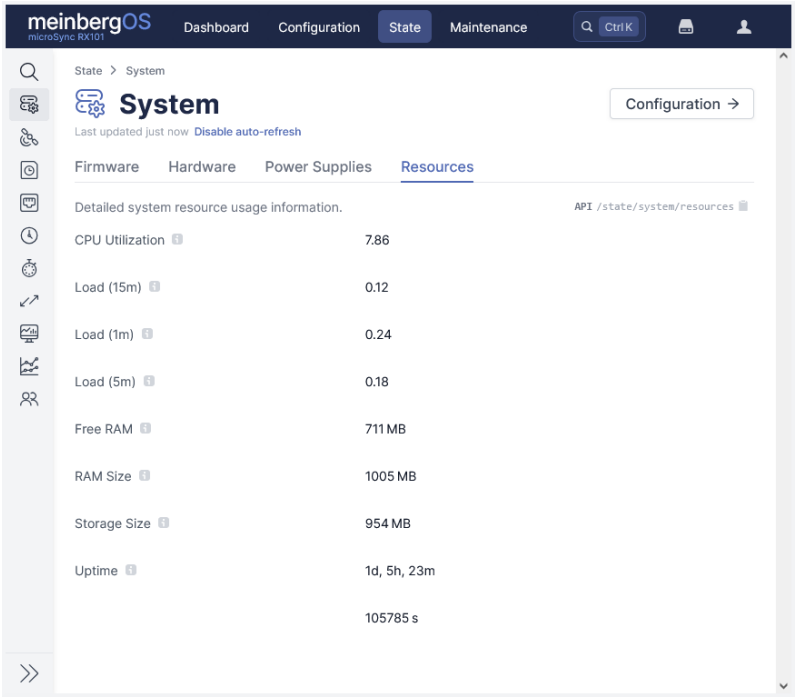


Figure 8.5: meinbergOS Web Interface: "State → System → Resources" Tab

This tab hosts information about the current resource usage and general system resource availability of the meinbergOS device.

CPU Utilization: The current utilization of the CPU as a percentage of the full CPU capacity.

Load (15m): The average system load over the previous fifteen minutes.

Load (1m): The average system load over the previous minute.

Load (5m): The average system load over the previous five minutes.

Free RAM: The available free system RAM of the system.

RAM Size: The total RAM installed in the meinbergOS device.

Storage Size: The total capacity of the storage medium installed in the meinbergOS device.

Uptime: The length of time that the meinbergOS device has been operational for since the last reset or power cycle.

8.2 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.

More information: ➜ Chapter 8.2.1, "State - References - Overview"

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

More information: ➜ Chapter 8.2.2, "State - References - Global"

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

More information: ➜ Chapter 8.2.3, "State - References - Sources"

8.2.1 State - References - Overview

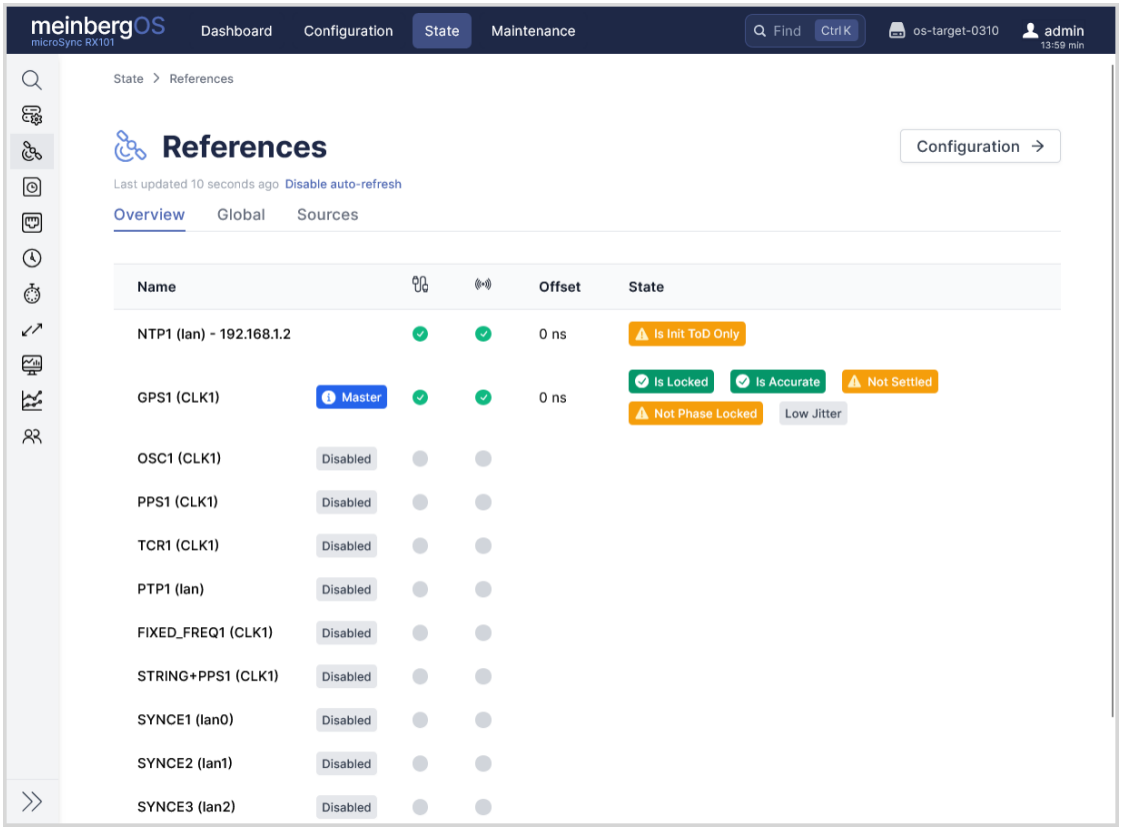


Figure 8.6: meinbergOS Web Interface: "State → References → Overview" Tab

The "**State** → **References** → **Overview**" tab (Fig. 8.6) provides a summary of your clock references and their synchronization status.

Hovering over the line of any reference in the list will reveal a **Configure** button on the right that can be used to open the corresponding configuration page for that reference source.

Refer to → Chapter 7.2, "Configuration - References" for more information.

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:	Time signal communication over a non-specific network interface. If the source is enabled and active, the current instance number (e.g., *I0*) and the virtual interface will be displayed after the name, e.g., **PTP1 (lan) - I0 (lan2:0)**.
lan*X*:	Time signal communication over a specific numbered physical network interface (e.g. *lan0*)

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 Checkmark:	Indicates that a wired connection is established with the signal source.
Red Prohibition Sign:	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 Checkmark:	Indicates that a viable signal has been detected over the connected cable.
Red Prohibition Sign:	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. This can be useful for diagnosing issues with signal jitter, as the reference clock will typically automatically adjust for stable offset values, and so any resultant offset will generally be attributable to unpredictable *changes* in this offset.

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:	There is no viable signal detected, regardless of whether there is a wired connection or not.

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.

8.2.2 State - References - Global

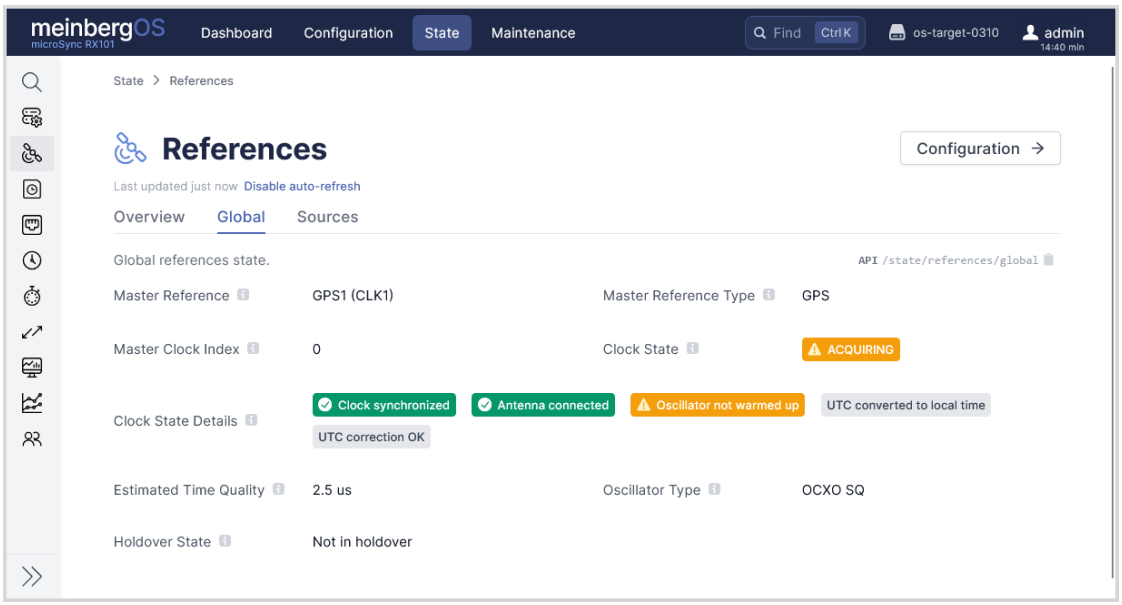


Figure 8.7: meinbergOS Web Interface: "State → References → Global" Tab

The "**State → References → Global**" tab (Fig. 8.7) 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 reference clock that this clock signal is synchronizing.

Master Reference Type: Indicates the overall type of the master reference signal.

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

Clock State: The current state of the internal oscillator relative to the reference source. This may be *Free Run*, *Acquiring* or *Locked*.

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

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

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.

Clock State Details:	This provides more detailed information about the current signal acquisition, synchronization, and adjustment state of the reference clock in the form of green (positive), yellow (temporary alert), red (error alert), and gray (general information) tags (see below).

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 meinbergOS device 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) are deemed 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 to be applied at the next possible insertion date.

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 an external source.

Holdover Mode: The clock is temporarily running off its internal oscillator, as no previously used input source signal is currently available.

8.2.3 State - References - Sources

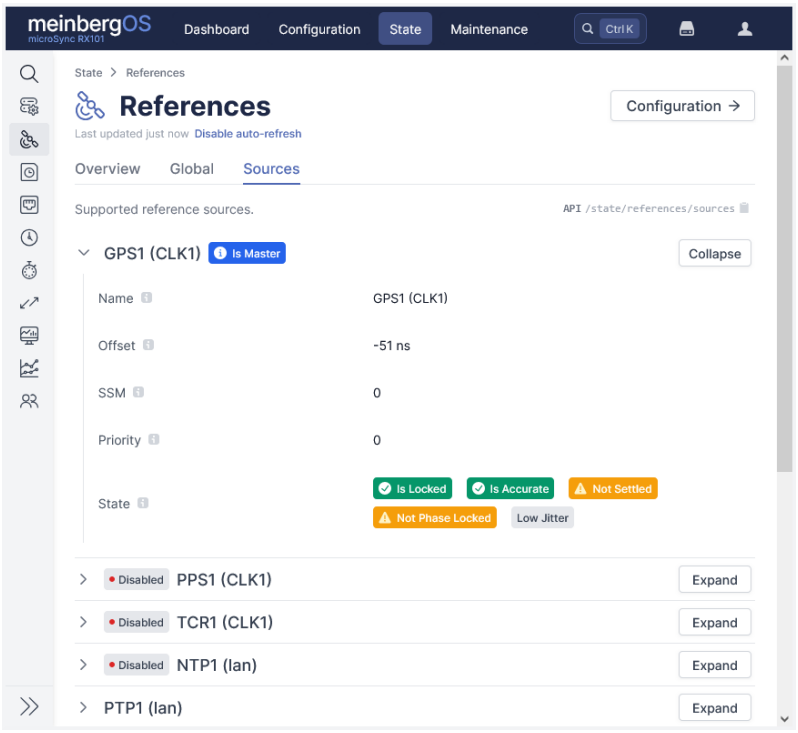


Figure 8.8: meinbergOS Web Interface: "State → References → Sources" Tab

The "**State** → **References** → **Sources**" tab (Fig. 8.8) 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 Synchronous Ethernet.
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 8.2.1, "State - References - Overview" for more details.
Additional Info:	Provides additional information about the source as supported (such as IP address).

8.3 State - Receiver

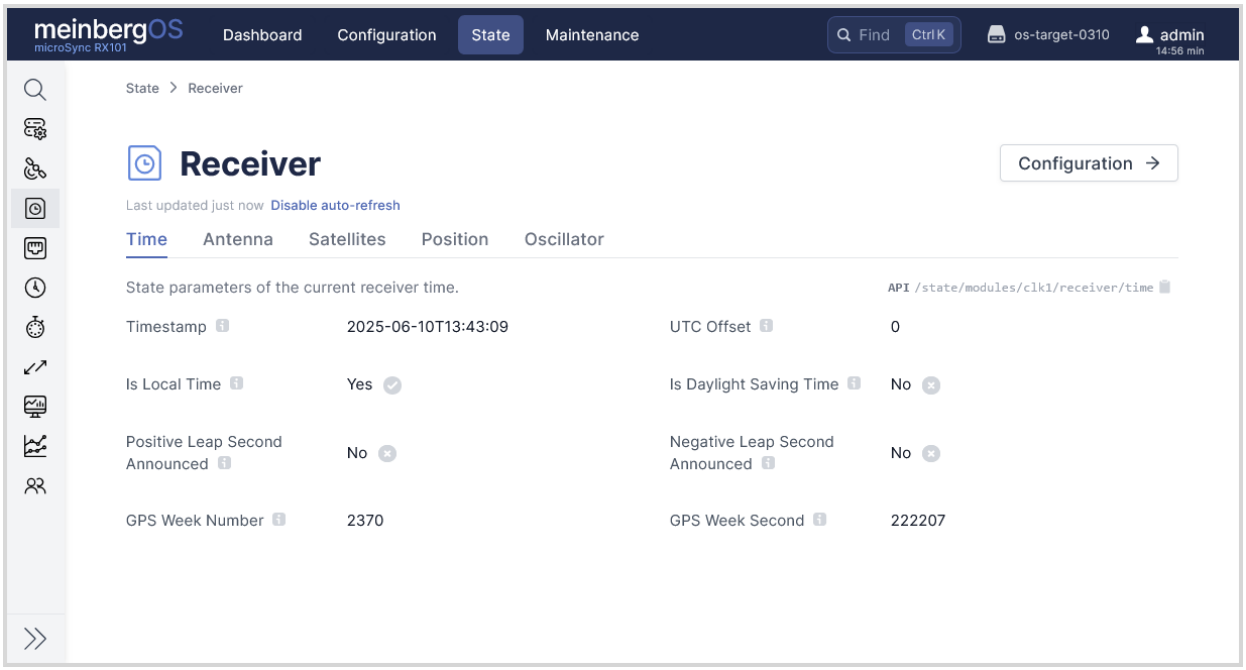


Figure 8.9: meinbergOS Web Interface: "State → Receiver → Time"

The **Receiver** subsection provides information about the receiver integrated into the meinbergOS device.

Time: This tab hosts information about the current time of the reference clock.

More information: → Chapter 8.3.1, "State - Receiver - Time"

Antenna: This tab hosts information about the connection between the meinbergOS device and an external antenna.

More information: → Chapter 8.3.2, "State - Receiver - Antenna"

Satellites: This tab hosts information about the current satellite reception.

More information: → Chapter 8.3.3, "State - Receiver - Satellites"

Position: This tab hosts information about the current position determined by means of GNSS geopositioning.

More information: → Chapter 8.3.4, "State - Receiver - Position"

Oscillator: This tab hosts information about the current calibration values of the integrated oscillator.

More information: → Chapter 8.3.5, "State - Receiver - Oscillator"

8.3.1 State - Receiver - Time

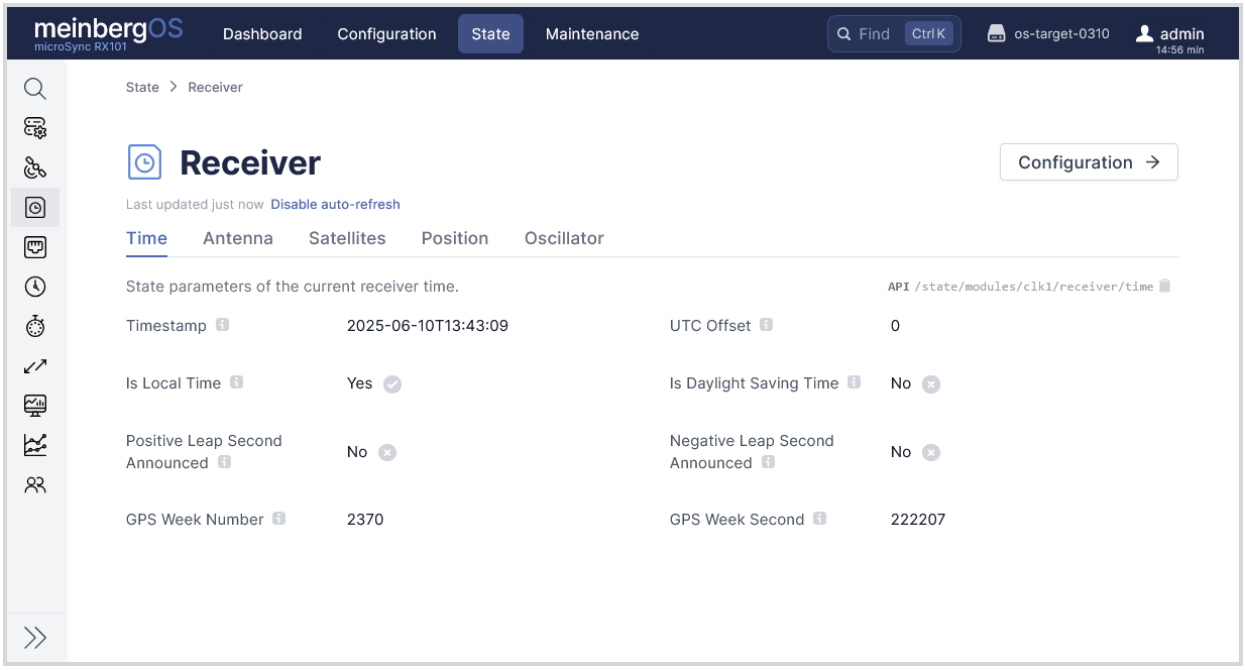


Figure 8.10: meinbergOS Web Interface: "State → Receiver → Time"

The **Time** tab 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 always show *No*.

Positive Leap Second Announced: This indicates if the upstream time source has provided the receiver with an announcement of a positive leap second (61 seconds in the last minute of the day) to be applied at the next possible time. Leap seconds are typically introduced at the end of July or December of a given year.

Negative Leap Second Announced:	This indicates if the upstream time source has provided the receiver with an announcement of a negative leap second (59 seconds in the last minute of the day) to be applied at the next possible time. Leap seconds are typically introduced at the end of July or December of a given year.
GPS Week Number:	This is the current GPS week number (*0–1023*) since the last GPS week number rollover in the current epoch.
GPS Week Second:	This is the current second in the current GPS week as of the last page refresh.

8.3.2 State - Receiver - Antenna

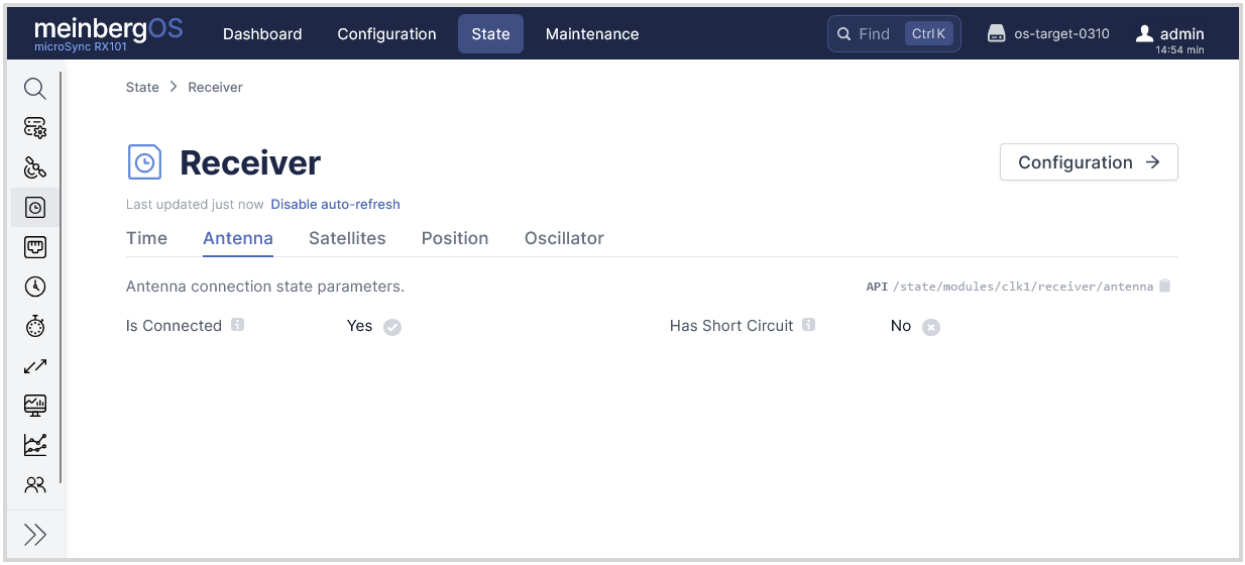


Figure 8.11: meinbergOS Web Interface: "State → Receiver → Antenna"

The **Antenna** tab 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).

8.3.3 State - Receiver - Satellites

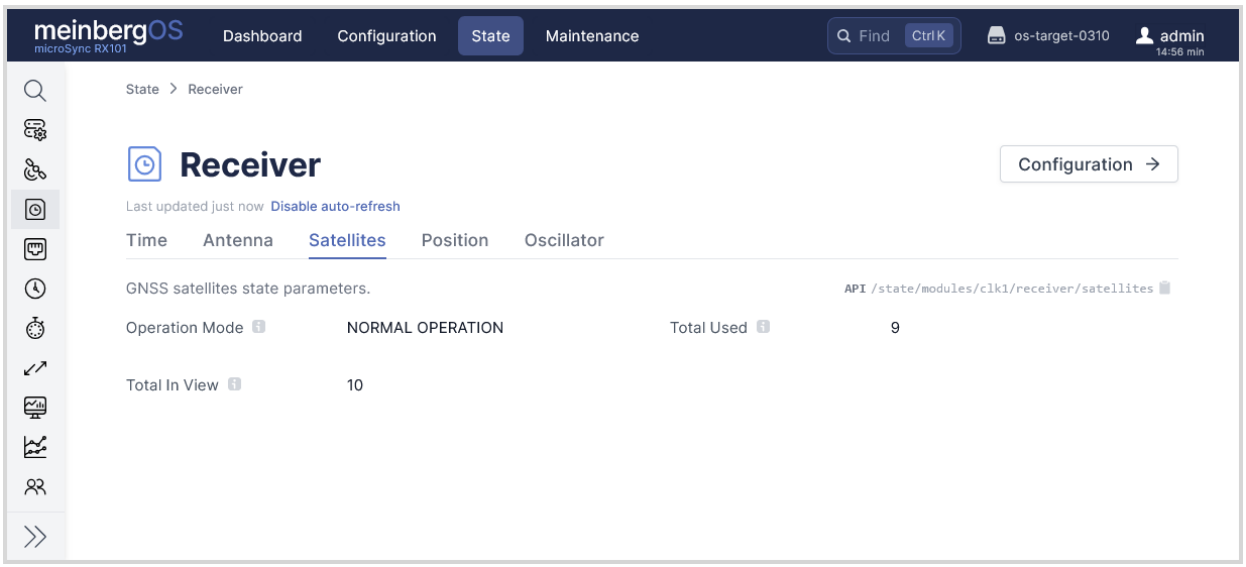


Figure 8.12: meinbergOS Web Interface: "State → Receiver → Satellites"

The **Satellites** tab 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.

8.3.4 State - Receiver - Position

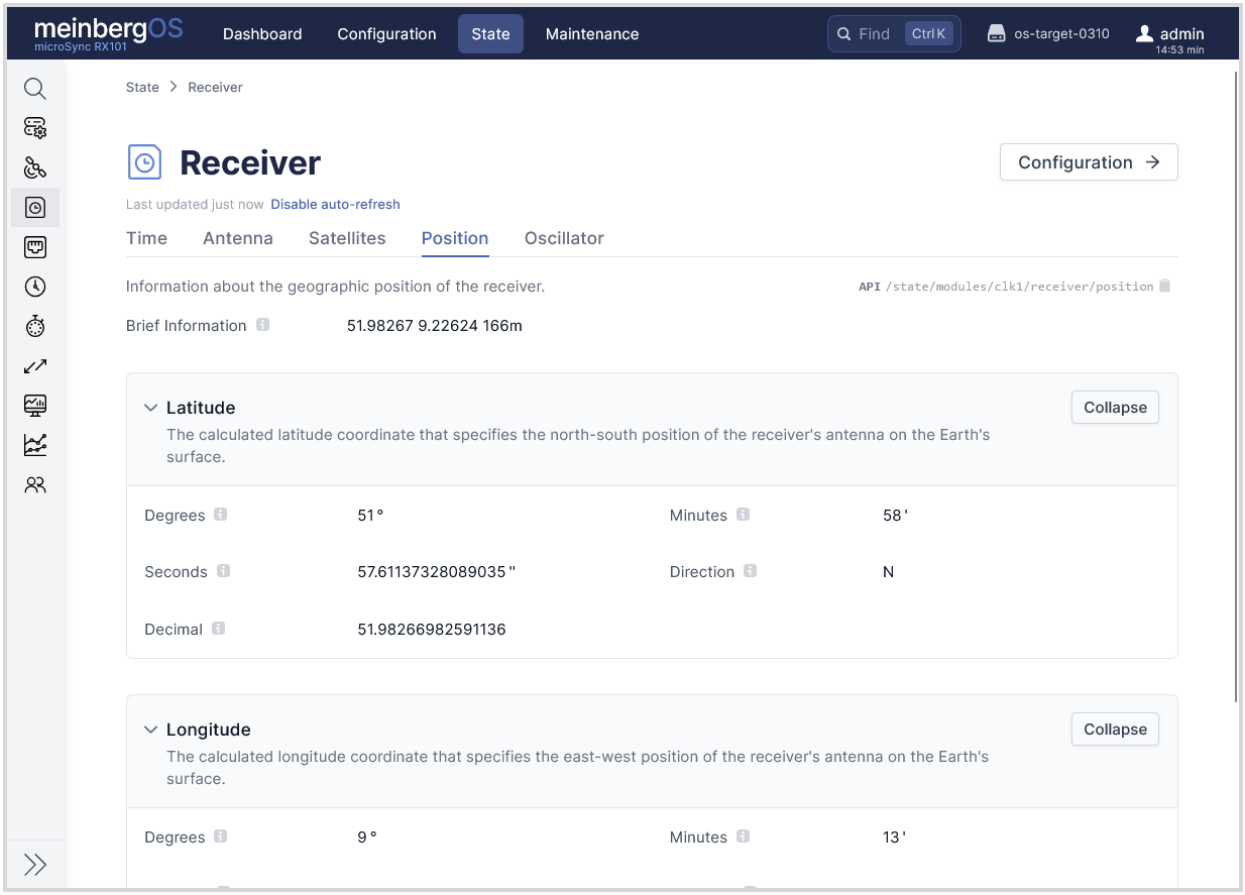


Figure 8.13: meinbergOS Web Interface: "State → Receiver → Position"

The **Position** tab provides detailed information about the calculated geographical position of the antenna. The **Brief Information** summarizes the geographical coordinates in decimal degrees and the altitude above sea level in meters, while the **Latitude** and **Longitude** panels can be expanded accordingly to obtain more precise geolocation information.

8.3.5 State - Receiver - Oscillator

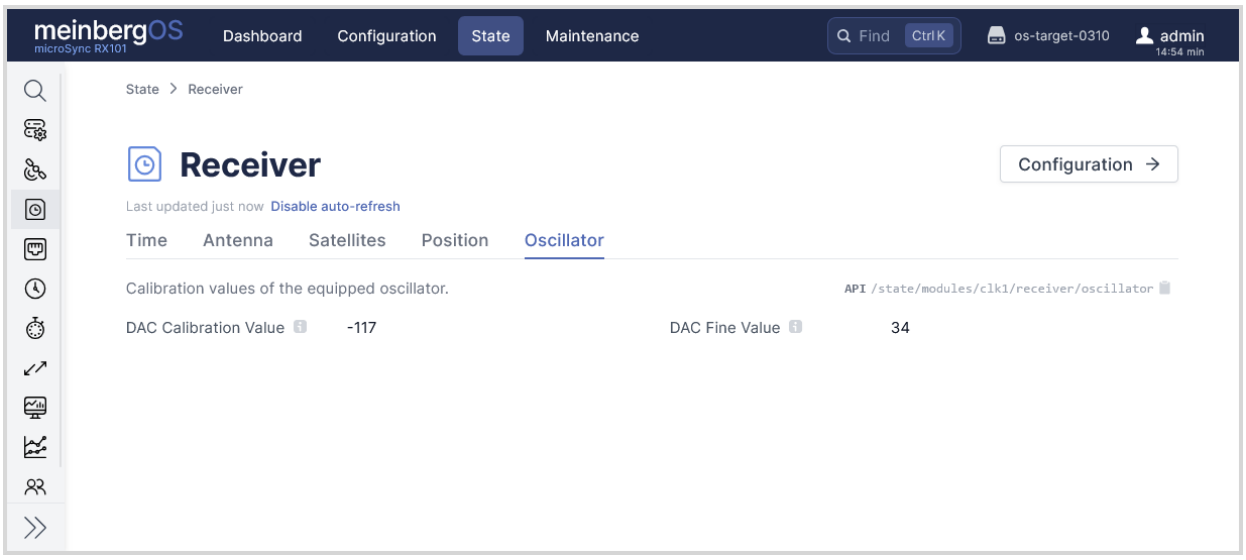


Figure 8.14: meinbergOS Web Interface: "State → Receiver → Oscillator"

The **Oscillator** tab provides calibration information on the receiver's internal oscillator, specifically the coarse and fine calibration values of the digital-to-analog converter (DAC).

8.4 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.

More information: → Chapter 8.4.1, "State - Network - Main"

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.

More information: → Chapter 8.4.2, "State - Network - Interfaces"

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

More information: → Chapter 8.4.3, "State - Network - PRP"

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

More information: → Chapter 8.4.4, "State - Network - Bonding"

IEC 61850: The **IEC 61850** tab provides access to the device's internally generated ICD file and also the currently imported CID file, and also provides a readout of the state of the meinbergOS device's MMS server.

More information: → Chapter 8.4.5, "State - Network - IEC 61850"

8.4.1 State - Network - Main

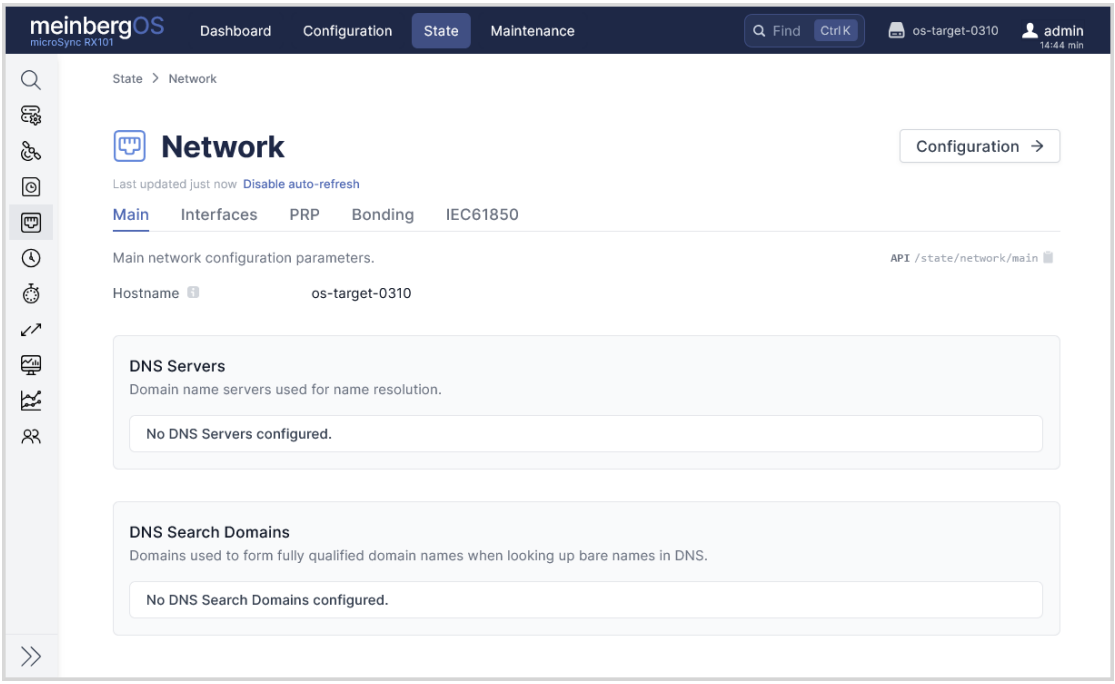


Figure 8.15: meinbergOS Web Interface: "State → Network → Main" Tab

The "**State** → **Network** → **Main**" tab (Fig. 8.15) provides a summary of your primary network configuration.

Hostname: The current hostname of the meinbergOS device, as defined under ➜ Chapter 7.5.1, "Configuration - Network - Main".

Default Gateway (IPv4): The IPv4 address of the default network gateway, provided that an IPv4 default gateway is configured. If IPv4 networking is not configured or an IPv4 default gateway is not defined, this entry will not appear.

Default Gateway (IPv6): The IPv4 address of the default network gateway, provided that an IPv6 default gateway is configured. If IPv6 networking is not configured or an IPv6 default gateway is not defined, this entry will not appear.

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

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

8.4.2 State - Network - Interfaces

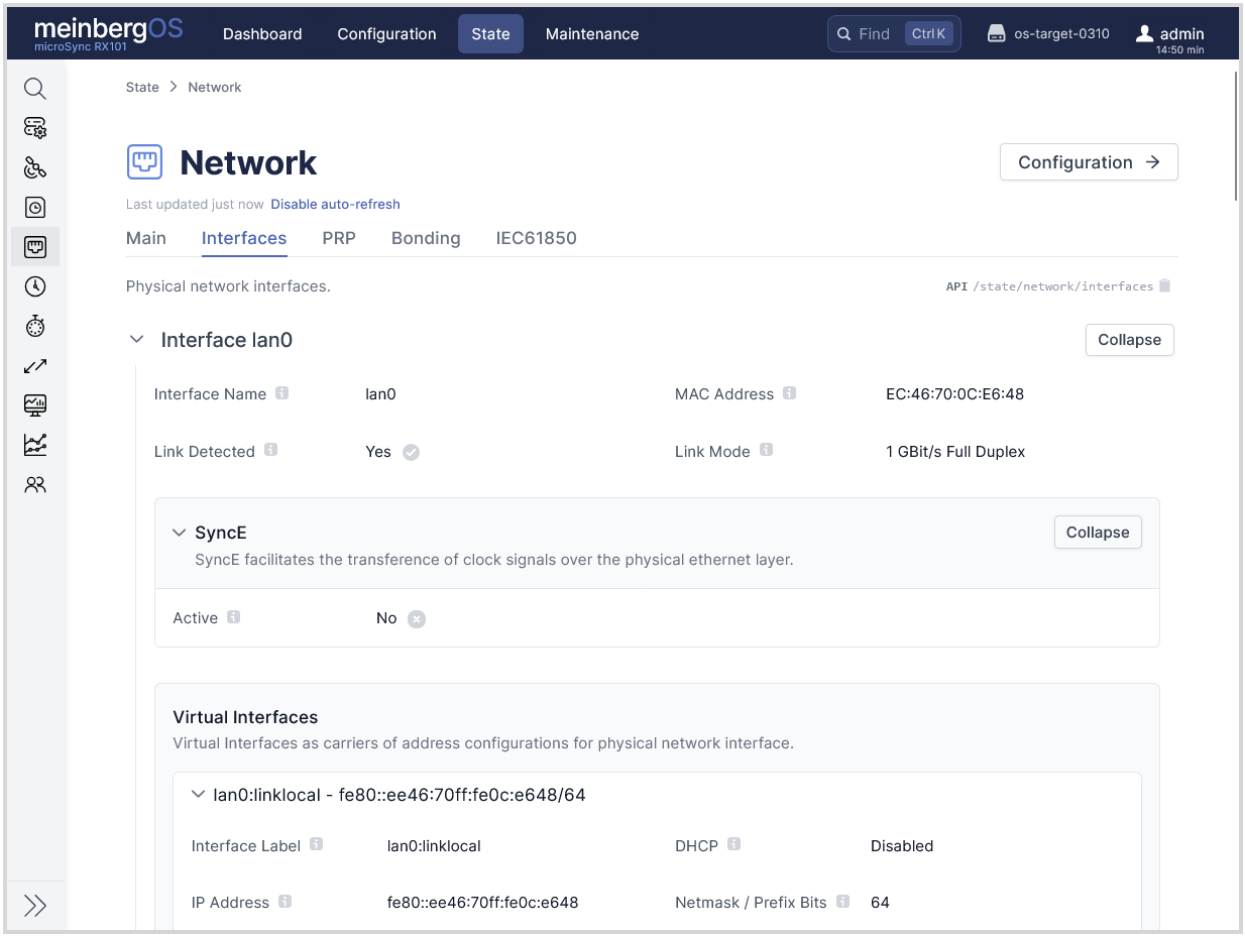


Figure 8.16: meinbergOS Web Interface: "State → Network → Interfaces" Tab

The "**State** → **Network** → **Interfaces**" tab (Fig. 8.16) 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 .

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. Refer to ➜ Chapter 8.4.3, "State - Network - PRP" for more information about PRP.

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, prefix bits for the netmask, as well as any static routes to specific networks or hosts for that virtual interface.

8.4.3 State - Network - PRP

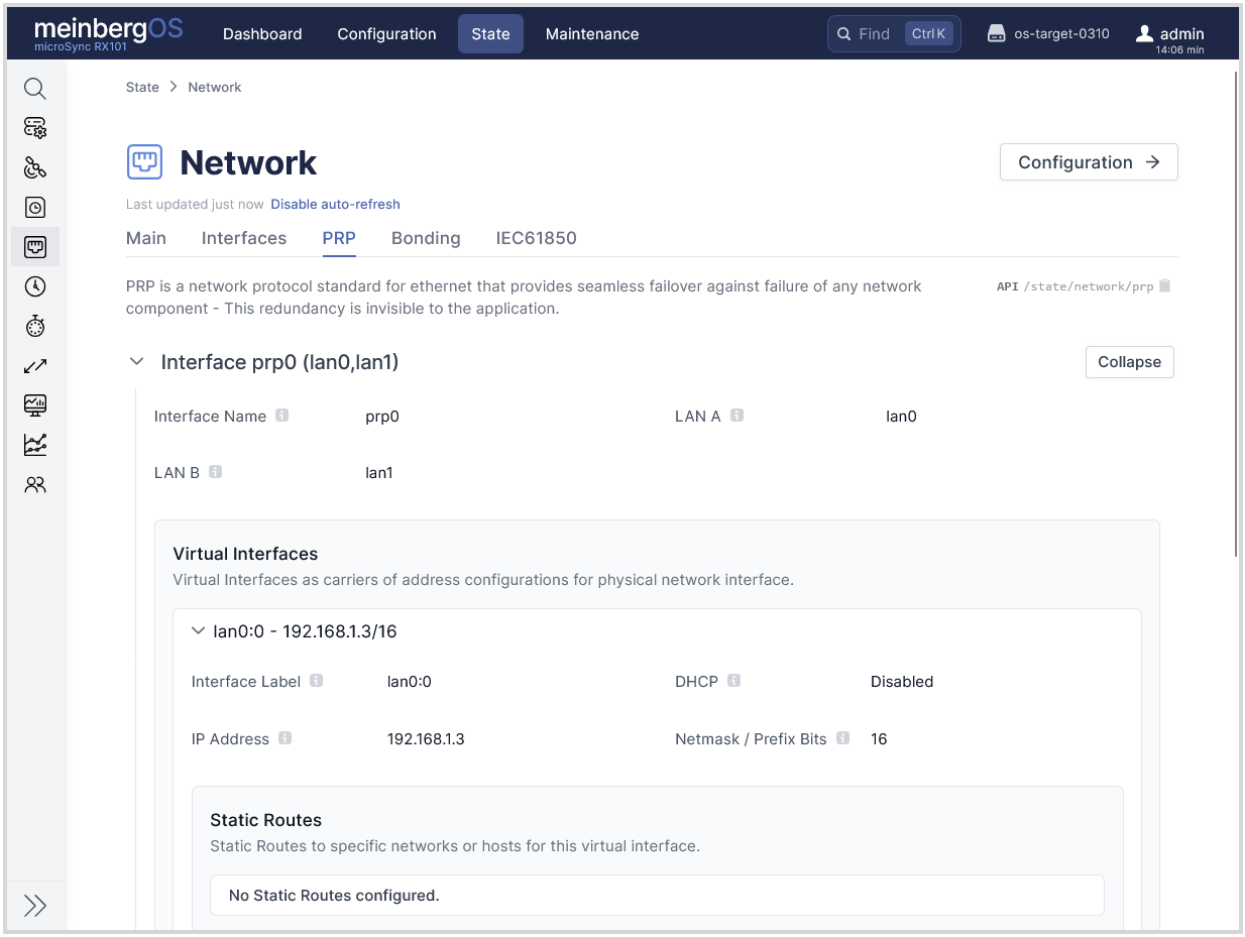


Figure 8.17: meinbergOS Web Interface: "State → Network → PRP" Tab

The "**State → Network → PRP**" tab (Fig. 8.17) 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 → Chapter 7.5.3, "Configuration - Network - PRP".

LAN B: The physical Ethernet interface that serves as the second PRP path, as configured under → Chapter 7.5.3, "Configuration - Network - PRP".

Each PRP interface panel also features a sub-panel showing the virtual interfaces assigned to that PRP interface. Refer to → Chapter 7.5.2, "Configuration - Network - Interfaces" and → Chapter 8.4.2, "State - Network - Interfaces" for more information.

8.4.4 State - Network - Bonding

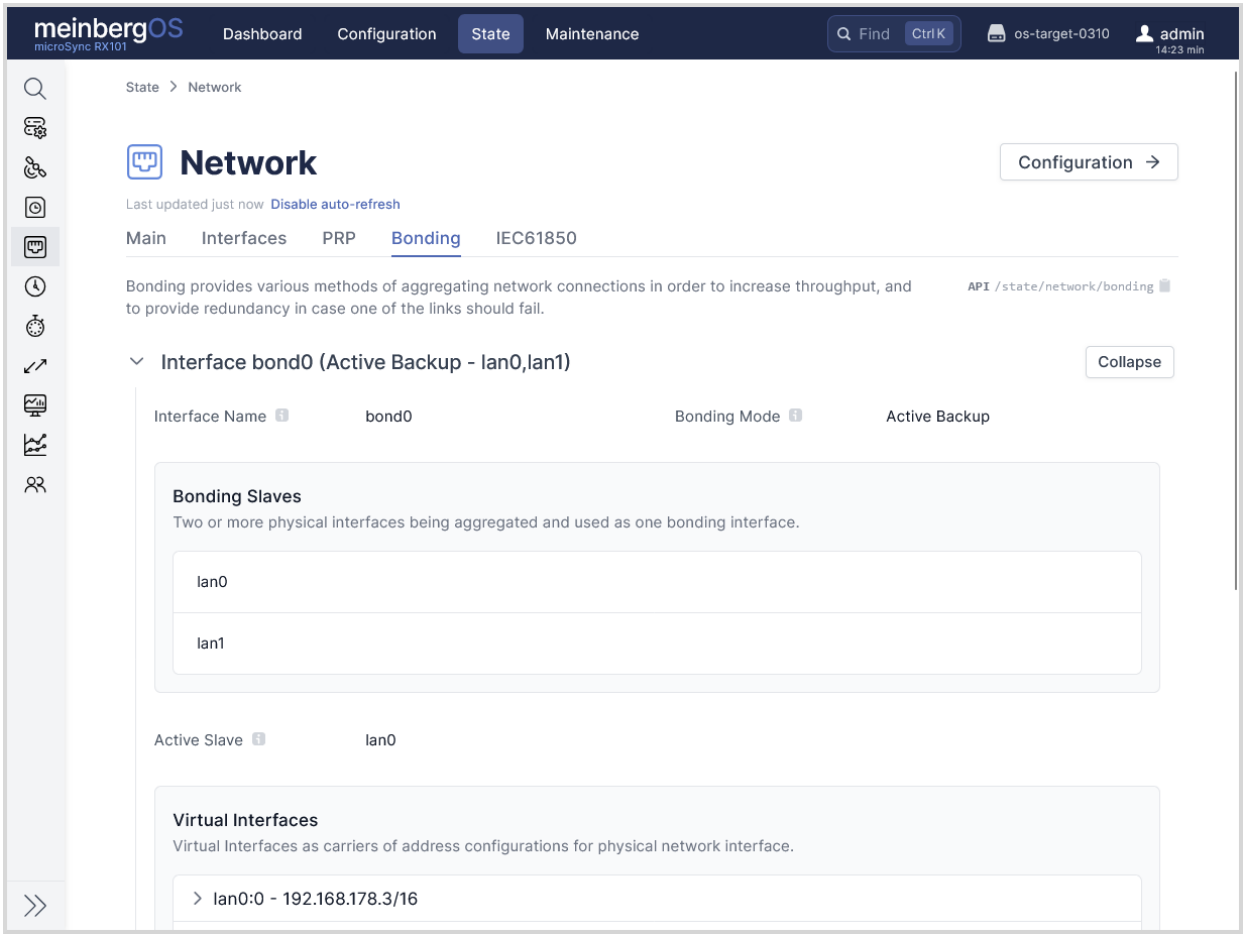


Figure 8.18: meinbergOS Web Interface: "State → Network → Bonding" Tab

The "**State** → **Network** → **Bonding**" tab (Fig. 8.18) 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)*". Refer to → Chapter 7.5.4, "Configuration - Network - Bonding" for more information on how these modes work.

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

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

8.4.5 State - Network - IEC 61850

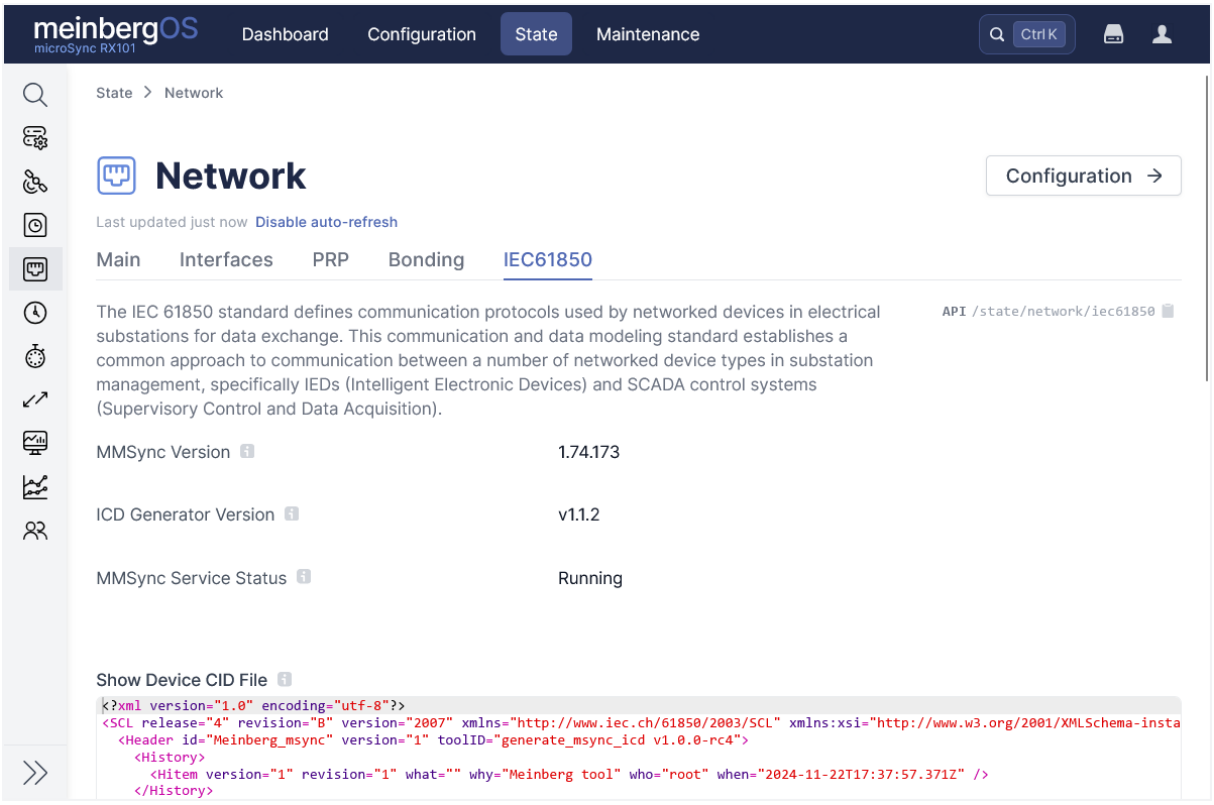


Figure 8.19: meinbergOS Web Interface: "State → Network → IEC 61850" Tab

The "**State → Network → IEC 61850**" tab (Fig. 8.19) provides access to status information as well as important configuration data for IEC 61850 networks used in the power industry.

MMSync Version: Specifies the current version of the integrated IEC 61850 MMS server *MMSync*.

ICD Generator Version: Specifies the current version of the integrated ICD generator tool. This tool generates a bespoke ICD file tailored to your specific meinbergOS device to be uploaded to your Substation Configuration Tool.

MMSync Service Status: Specifies the current state of the integrated MMS server (*Stopped*, *Running*).

There are also two XML text boxes located beneath these status readouts.

The first, the **CID file** (*Configured IED Description*) is the file exported by the Substation Configuration Tool and which the meinbergOS device uses as a basis for its own configuration and communication. It will only typically be displayed once a CID file has been uploaded.

Below that is the **ICD file** (*IED Capability Description*), which is the larger file generated by the meinbergOS device itself to be imported into your Substation Configuration Tool. It contains a comprehensive description of your meinbergOS device's capabilities and interfaces.

Buttons to download these files are provided beneath each text box.

8.5 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.

More information: ➜ Chapter 8.5.1, "State - NTP - Main"

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

More information: ➜ Chapter 8.5.2, "State - NTP - Server"

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

More information: ➜ Chapter 8.5.3, "State - NTP - Client"

8.5.1 State - NTP - Main

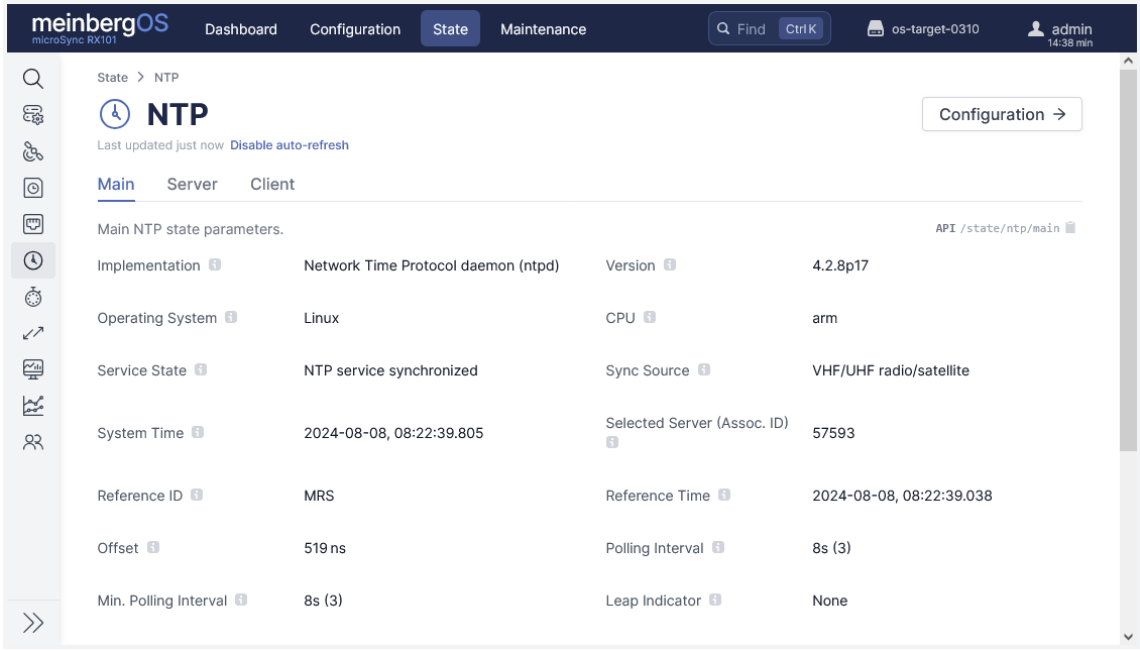


Figure 8.20: meinbergOS Web Interface: "State → NTP → Main" Tab

The "**State → NTP → Main**" tab (Fig. 8.20) 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 under which this NTP implementation is running. This should always read "*Linux*" for your meinbergOS device.

CPU: The type of CPU for which this implementation of NTP has been compiled for. For most meinbergOS 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 8.2, "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 Multi-Reference Source system employed by 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 ➜ Chapter 7.6.1, "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*.

8.5.2 State - NTP - Server

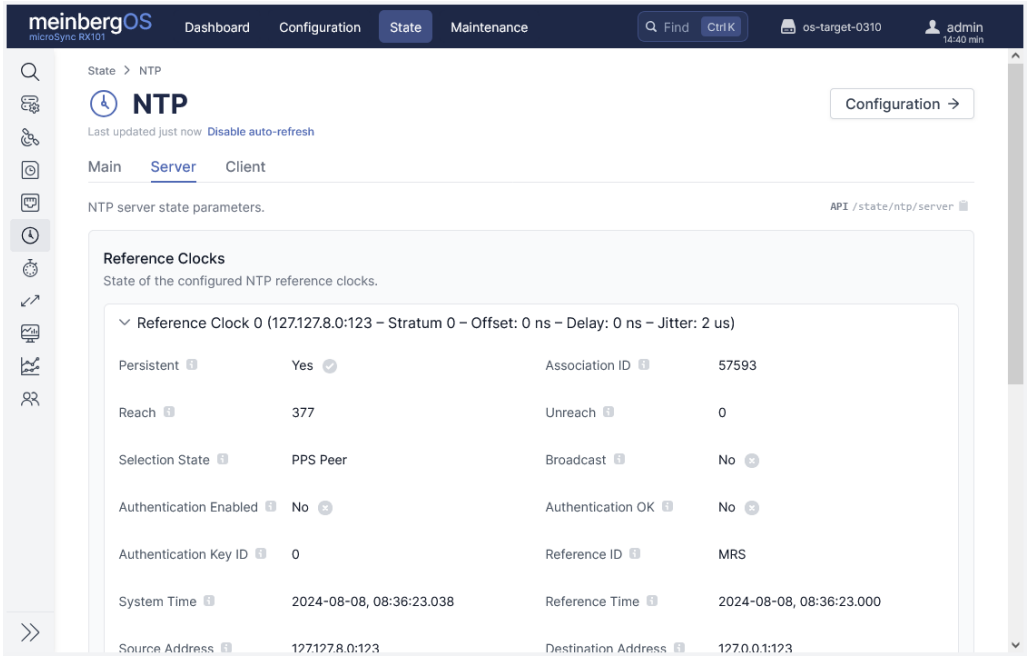


Figure 8.21: meinbergOS Web Interface: "State → NTP → Server" Tab

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 refer to → Chapter 8.5.3, "State - NTP - Client".

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.

Following start-up, each bit of the shift register should gradually fill up with ones until the octal value continuously reads "*377*". This value indicates that each of the last eight polling intervals were successful, because *3* = `111` and *7* = `111` and thus equivalent to the binary value `11-111-111`.

Any other value than *377* in this case may be indicative of an internal system error, as it simply represents the local NTP client polling the local NTP server.

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 a 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 State - NTP - Client

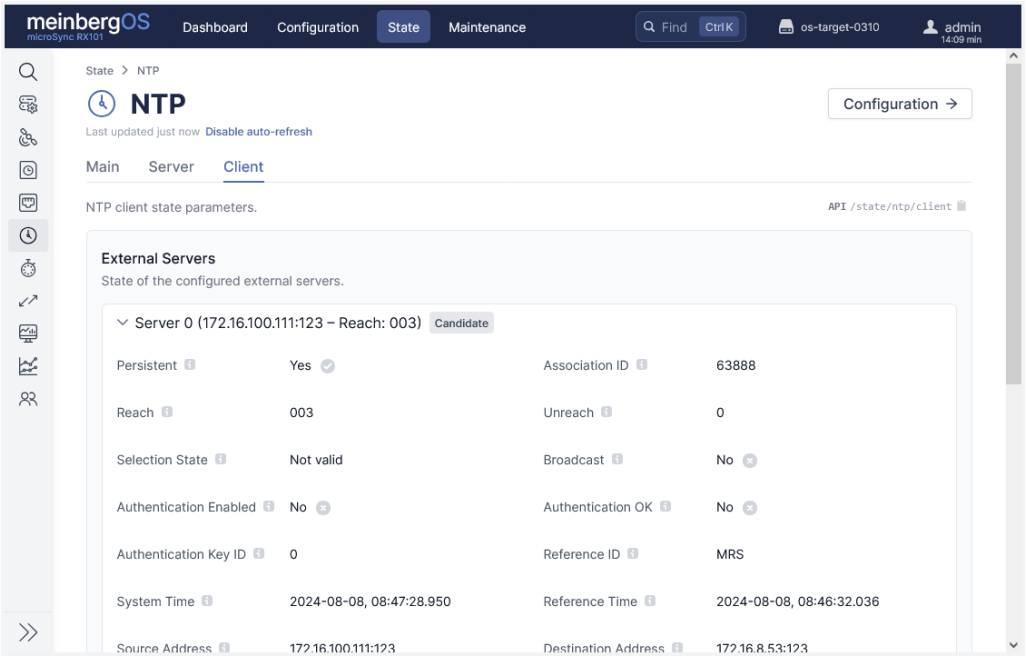


Figure 8.22: meinbergOS Web Interface: "State → NTP → Client" Tab

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 refer to → Chapter 8.5.2, "State - NTP - Server".

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.

Following start-up, the shift register will start at `00000000` and each bit of the shift register will shift left at each polling interval to accommodate the outcome of the latest polling attempt (`1` = successful, `0` = failed).

Ideally, it should gradually fill up with ones until the octal value continuously reads "*377*". This value indicates that each of the last eight polling intervals were successful, because *3* = `11` and *7* = `111` and thus equivalent to the binary value `11-111-111`.

A value of *000* after a start-up period (combined with a continuously increasing **Unreach** value) indicates that the server is not reachable at all. Any value other than *000* or *377* after the start-up phase may be indicative of other network or server issues such as congestion.

Unreach: The total number of unsuccessful polling intervals since last (re)boot or since the last restart of the NTP daemon. Taken in conjunction with the **Reach** value above, this can be used to diagnose network or server issues of an intermittent or persistent nature.

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.

8.6 State - PTP

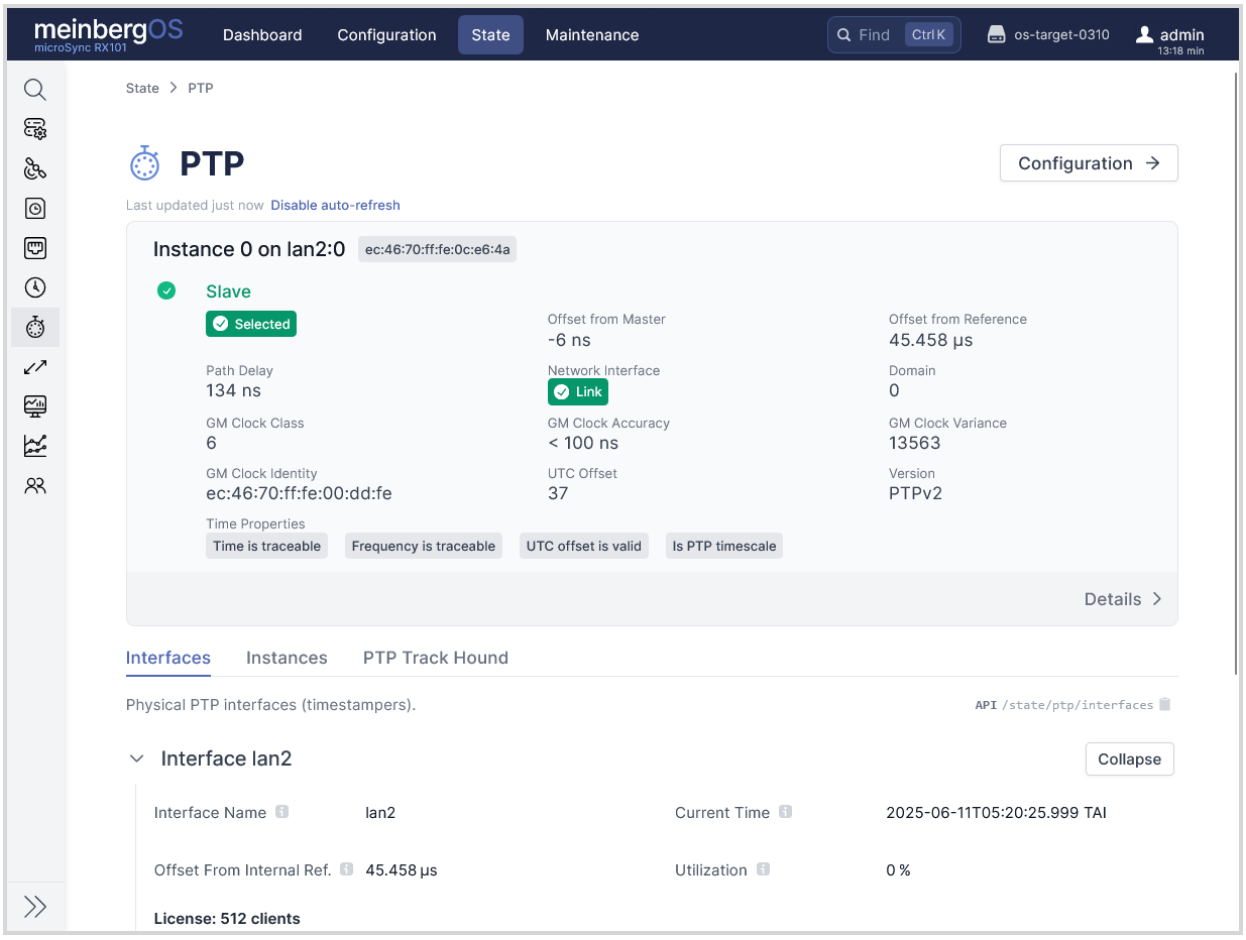


Figure 8.23: meinbergOS Web Interface: "State → PTP" Subsection

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** (→ Chapter 8.6.1, "State - PTP - Interfaces"), which provides information on the PTP-related states of the PTP-enabled virtual interfaces, and **Instances** (→ Chapter 8.6.2, "State - PTP - 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.

Master/Slave: Specifies whether this instance is operating in *Master* or *Slave* mode.

Offset from Master: Specifies the current offset of the PTP clock in the network controller relative to the master clock. Only applies to clocks operating in *Slave* mode.

Offset from Reference: Specifies the current offset of the PTP clock in the network interface controller relative to the internal reference (the integrated oscillator). Only applies to clocks operating in *Slave* mode.

Path Delay: Specifies the current mean path delay relative to the current master clock. Only applies to clocks operating in *Slave* mode.

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.

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.

8.6.1 State - PTP - Interfaces

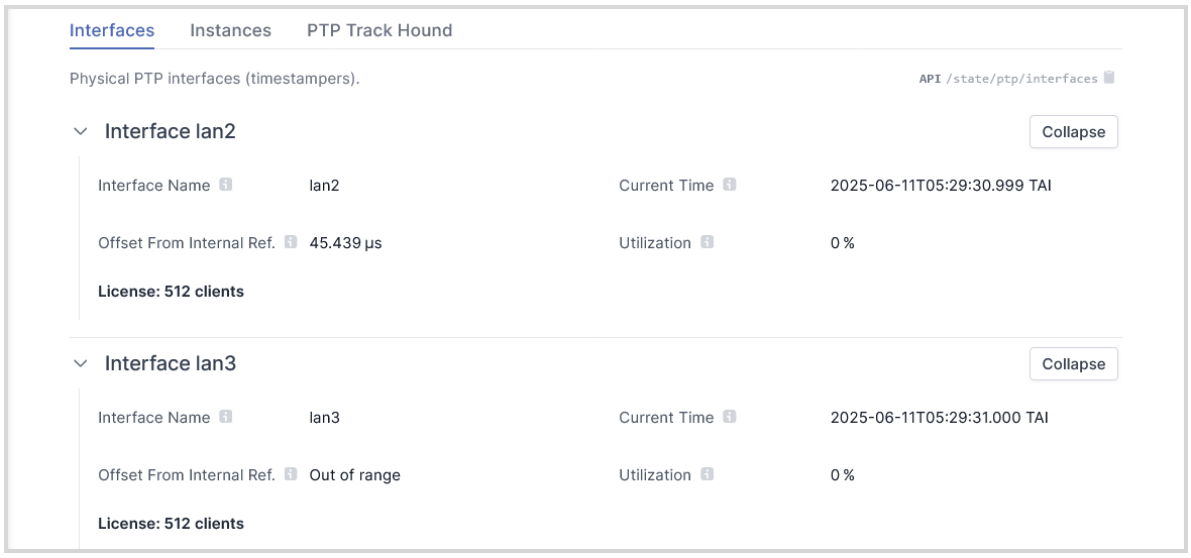


Figure 8.24: meinbergOS Web Interface: "State → PTP → Interfaces" Tab

The tab "**State → PTP → Interfaces**" (Fig. 8.24) 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.

License: The maximum number of clients permitted to operate as Slaves (Performance Level) to this PTP instance operating as a Master.

8.6.2 State - PTP - Instances

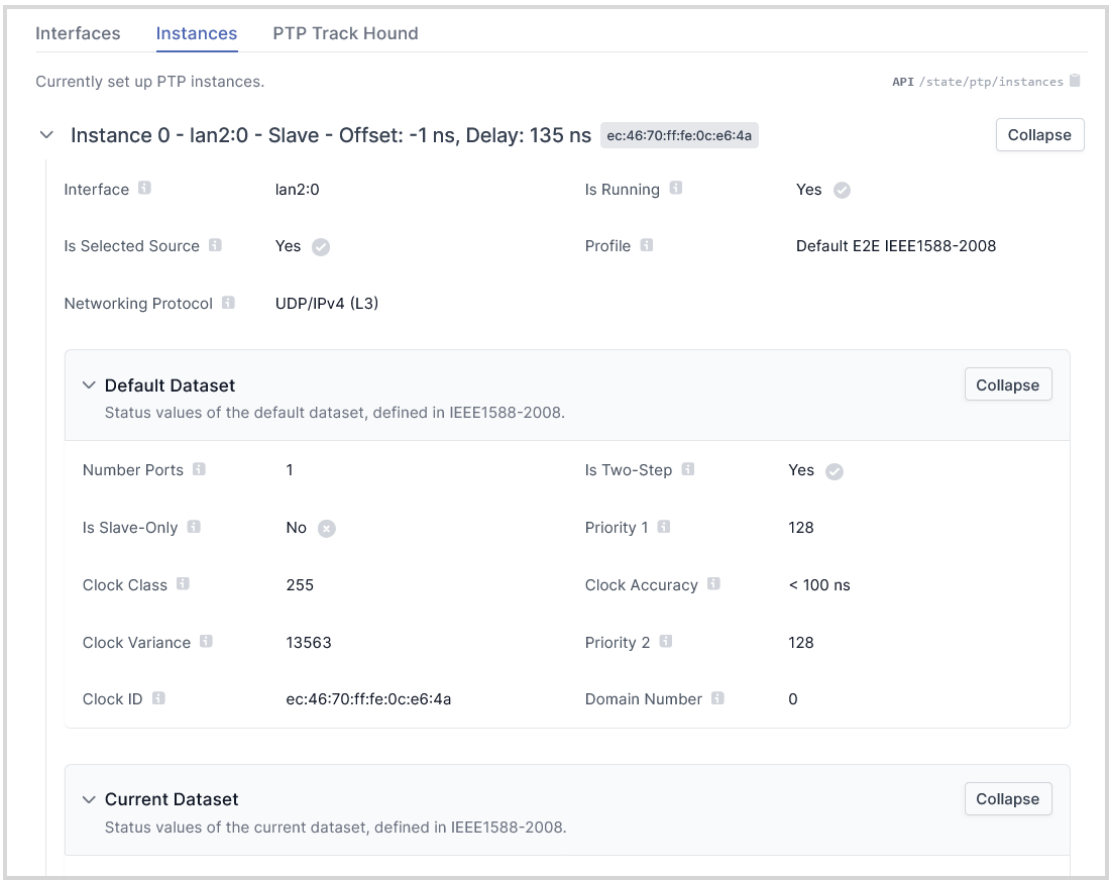


Figure 8.25: meinbergOS Web Interface: "State → PTP → Instances" Tab

The tab "**State → PTP → Instances**" (Fig. 8.25) provides information about the defined PTP instances.

Interface: The virtual interface 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.

Is Selected Source: Indicates whether this PTP instance is currently selected as the meinbergOS device's PTP reference source.

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 otherwise 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 Boundary Clock 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.

8.6.3 State - PTP - PTP Track Hound

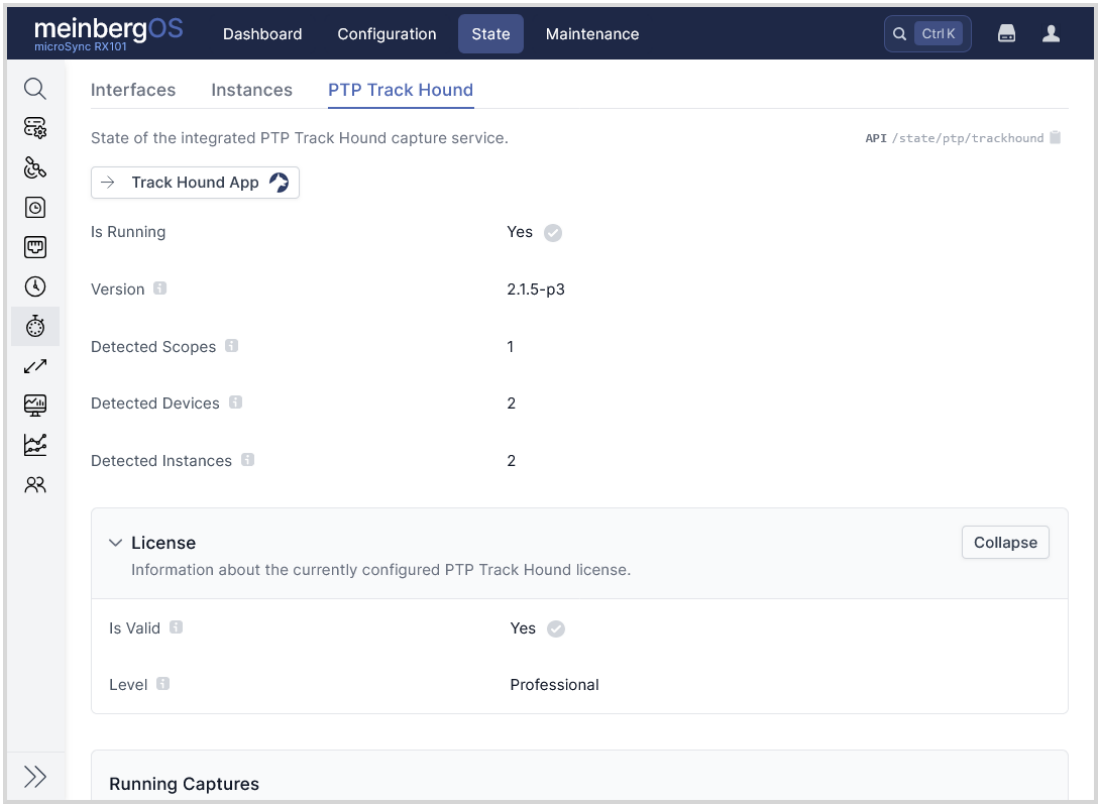


Figure 8.26: meinbergOS Web Interface: "State → PTP → PTP Track Hound" Tab

As of meinbergOS *2024.12*, Meinberg's PTP network monitoring solution **PTP Track Hound** is integrated into all meinbergOS devices. PTP Track Hound provides a wealth of monitoring, analysis, and reporting tools for PTP traffic, and all of these are managed via the separate PTP Track Hound Web Interface.

This tab (Fig. 8.26) provides information about the current state of the integrated PTP Track Hound on your meinbergOS device.

For more information, visit Meinberg's PTP Track Hound website at https://www.ptptrackhound.com, where you can also download the product documentation for PTP Track Hound.

Track Hound App: This button provides convenient direct access to the PTP Track Hound Web Interface. It does not appear if the PTP Track Hound service is not enabled.

Is Running: Specifies whether the PTP Track Hound service is running. If no interfaces are enabled for PTP Track Hound monitoring, meinbergOS will disable the PTP Track Hound service, this entry will show *No*, and all of the following information will not be displayed.

Version: Shows the current PTP Track Hound version running on the meinbergOS device. Please note that PTP Track Hound versions are bound to the meinbergOS firmware version. PTP Track Hound cannot be updated individually; updates are introduced through meinbergOS firmware updates.

Detected Scopes: The number of **scopes** identified by PTP Track Hound based on the instances that it has detected. A scope is defined as a group of clocks that are capable of serving and receiving time to and from one another. This means that all clocks within a scope must share a common network protocol, PTP version (PTPv2 and PTPv2.1 are treated as a single version), PTP domain or subdomain, VLAN tag, and Grandmaster clock, and are assumed to be able to reach one another within a shared network or subnet.

Detected Devices: The number of discrete devices detected by PTP Track Hound.

Detected Instances: The number of **instances** running on the detected devices. An instance is a PTP 'session' running on a device. A boundary clock device, for example, will typically host at least two instances: one Master and one or more Slaves.

License

This provides information about the license registered on the meinbergOS device, if any.

Is Valid: If a valid license has been registered under "**Configuration** → **PTP** → **PTP Track Hound**, this will show *Yes*. If not, this will show *No* and the license will default to the pre-installed **Capture License**.

Level: Indicates the level of the registered license, which may be *Capture*, *Basic*, or *Professional*. If no paid license is registered, this will default to the pre-installed *Capture* license.

Running Captures

This provides information about the capture instances currently running on the meinbergOS device.

Type: The type of capture performed on this interface: *Interface* or *Remote*. An *interface capture instance* involves the network port directly receiving PTP traffic, whereas a *remote capture instance* involves PTP traffic captured at another device's network port being forwarded to the PTP Track Hound instance.

Name: If the capture is an *interface capture instance*, this will be the name of the physical interface that is receiving the traffic data. If the capture is a *remote capture instance*, this will show the hostname or IP address of the source of the capture data.

Management Messages Enabled: Specifies if this capture instance has been configured to transmit management messages.

Capture Time Offsets Enabled:	Specifies if this capture instance has been configured to perform Capture Time Offset (CTO) measurements.
NetSync Monitor Enabled:	Specifies if this capture instance has been configured to perform offset and path delay measurement using the NetSync Monitor protocol (NSM).
Hardware Timestamps Enabled:	Specifies if this capture instance is using the hardware timestamper integrated into the network controller. If there is a PTP instance running concurrently on this port, then the hardware timestamper will not be used. If there is no PTP instance, then the hardware timestamper will be used.

Packet Statistics

These are the statistical analyses of the captured data.

Total Count

Total:	The total number of PTP messages received by this capture instance thus far.
In Memory:	The total number of PTP messages currently held in the capture log. As long as the memory buffer has not been filled, this will generally be equal to the value **Total** described above. However, as the memory buffer becomes full, older messages will be purged from the capture log and the **Total** and **In Memory** values will diverge accordingly.
PTPv1:	The total number of PTPv1 messages counted in the current capture instance.
PTPv2.0:	The total number of PTPv2.0 messages counted in the current capture instance.
PTPv2.1:	The total number of PTPv2.1 messages counted in the current capture instance.
PTPv2.x:	The combined number of PTPv2.0 and PTPv2.1 messages counted in the current capture instance.
Announce Messages:	The total number of Announce messages counted in the current capture instance.
Sync Messages:	The total number of Sync messages counted in the current capture instance.
Follow Ups:	The total number of Follow-Up messages counted in the current capture instance.

Delay Requests: The total number of Delay Request messages counted in the current capture instance.

Delay Responses: The total number of Delay Response messages counted in the current capture instance.

Peer Delay Requests: The total number of Peer Delay Request messages counted in the current capture instance.

Peer Delay Responses: The total number of Peer Delay Response messages counted in the current capture instance.

Peer Delay Response Follow Ups: The total number of Peer Delay Response Follow-Up messages counted in the current capture instance.

Monitoring Requests: The total number of NetSync Monitor requests counted in the current capture instance.

Monitoring Responses: The total number of NetSync Monitor responses counted in the current capture instance.

Management Messages: The total number of Management messages counted in the current capture instance.

Signaling Messages: The total number of Signal messages counted in the current capture instance.

Per Second

Total: The average number of PTP messages counted per second by this capture instance thus far.

PTPv1: The average number of PTPv1 messages counted per second by this capture instance thus far.

PTPv2.0: The average number of PTPv2.0 messages counted per second by this capture instance thus far.

PTPv2.1: The average number of PTPv2.1 messages counted per second by this capture instance thus far.

PTPv2.x:	The average number of PTPv2.0 and PTPv2.1 messages counted per second by this capture instance thus far.
Announce Messages:	The average number of Announce messages counted per second by this capture instance thus far.
Sync Messages:	The average number of Sync messages counted per second by this capture instance thus far.
Follow Ups:	The average number of Follow-Up messages counted per second by this capture instance thus far.
Delay Requests:	The average number of Delay Request messages counted per second by this capture instance thus far.
Delay Responses:	The average number of Delay Response messages counted per second by this capture instance thus far.
Peer Delay Requests:	The average number of Peer Delay Request messages counted per second by this capture instance thus far.
Peer Delay Responses:	The average number of Peer Delay Response messages counted per second by this capture instance thus far.
Peer Delay Response Follow Ups:	The average number of Peer Delay Response Follow-Up messages counted per second by this capture instance thus far.
Monitoring Requests:	The average number of NetSync Monitor request messages counted per second by this capture instance thus far.
Monitoring Responses:	The average number of NetSync Monitor response messages counted per second by this capture instance thus far.
Management Messages:	The average number of Management messages counted per second by this capture instance thus far.
Signaling Messages:	The average number of Signal messages counted per second by this capture instance thus far.

Memory Usage

Maximum Percentage:	The configured maximum percentage of memory allocable for capture, model, and statistical data.
Maximum Memory:	The absolute amount of memory allocable for capture, model, and statistical data.
Used:	The amount of memory currently used for capture, model, and statistical data.
Model and Statistics:	The amount of memory currently used for model and statistical data.
Captured Packets:	The amount of memory currently used for captured PTP messages.

8.7 State - I/O Ports

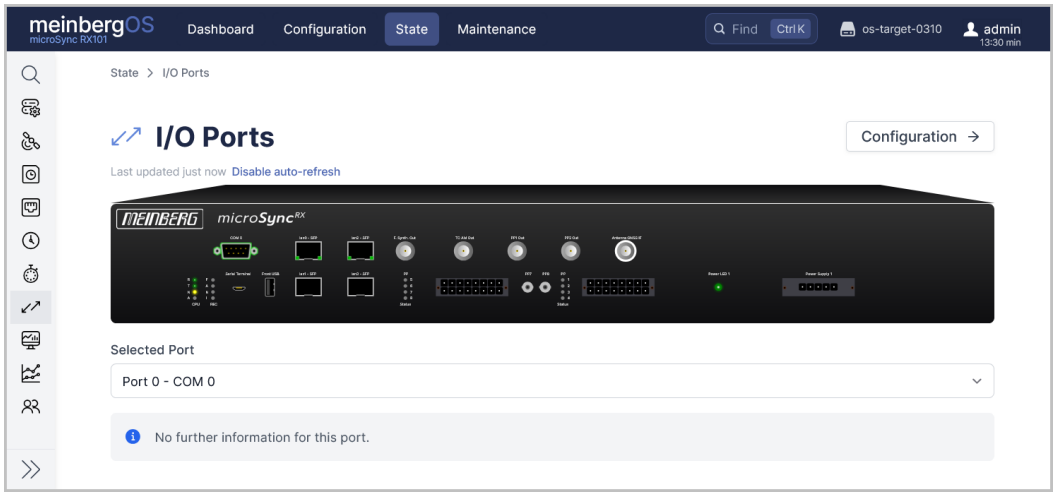


Figure 8.27: meinbergOS Web Interface: "State → IO Ports" Subsection

The "**State → I/O Ports**" subsection (Fig. 8.27) provides a graphical representation of your physical meinbergOS device (for example, a microSync).

Hovering with the cursor 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 certain connectors or pins will provide a link to the subsection or tab of the **State** section where further information about the operating state of that interface can be obtained.

For more information, please refer to → Chapter 7.8, "Configuration - I/O Ports".

8.8 State - Monitoring

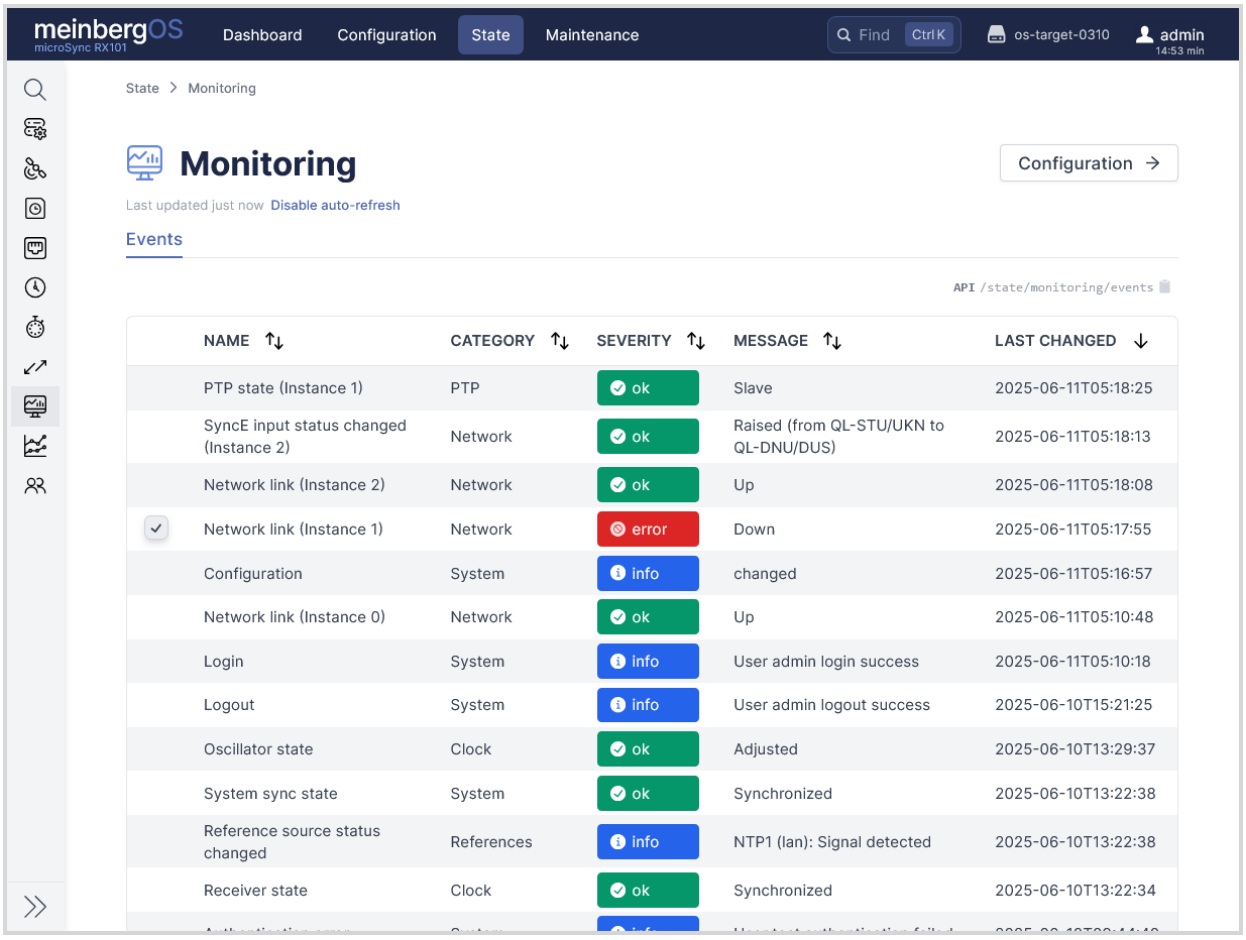


Figure 8.28: meinbergOS Web Interface: "State → Monitoring" subsection

The **Monitoring** subsection contains a table of monitored events and components. Each of these events and components is listed alongside a category, the severity of the most recent event, a description of the most recent event, and the date of the last update.

Only those events marked for monitoring via SNMP or *syslog* or both under → Chapter 7.9, "Configuration - Monitoring" will be listed here.

Each event can be marked:

- "**OK**" (green), meaning that the event or component is within normal operating parameters,
- "**Info**" (blue), meaning that something has occurred in relation to the event or component that may be of interest or concern,
- "**Warning**" (yellow), meaning that something has occurred in relation to the event or component that is likely to be indicative of a problem,
- "**Error**" (red), meaning that the event or component has fallen outside of operating parameters or is in a fault state.

Potentially important events feature a checkbox in the left column that indicates that they can be *acknowledged*. Until such an event is acknowledged, it will be prominently displayed on the Dashboard (see → Chapter 6, "Dashboard"). Once it is acknowledged, the checkbox will be replaced by a green checkmark.

The following event types are recognized:

Antenna:	Monitors the physical connection state of the antenna.
Authentication Error:	Monitors authentication failures (e.g., incorrect password entries).
Certificate Event:	Monitors changes to the SSL/TLS certificate for HTTPS web server use.
Certificate Validity:	Monitors the validity of the SSL/TLS certificate for HTTPS web server use and generates an alarm upon its expiry.
Configuration:	Monitors configuration changes.
CPU Load:	Monitors the current load on the internal CPU.
Heartbeat:	A regular pulse signal, sent at the configured frequency, that can be detected by other devices so that the meinbergOS device is known to be running.
Leap Second:	Monitors known leap second announcements.
Login:	Monitors the most recent login attempt.
Logout:	Monitors the most recent logout action.
Master Reference Changed:	Monitors changes in the current master reference signal.
Memory:	Monitors current system RAM usage.
Network Link:	Monitors network link states on the corresponding network port (e.g., instance 0 = port *lan0*).
NTP State:	Monitors the state of the internal NTP service.
Oscillator State:	Monitors the calibration state of the integrated oscillator.
Password Validity:	Monitors the validity of user passwords and generates an alert upon expiry of any user password.

Power Supply State:	Monitors the state or absence of each power supply module. There will be one entry per power supply bay (even if a power supply module is not installed in one of them).
PTP State:	Monitors the state of each configured PTP instance. There will be one entry per configured PTP instance.
Reference Source Status Changed:	Monitors the availability or unavailability of reference signals in general, including those not currently being used as the master reference.
Reboot:	Monitors system reboots.
Receiver State:	Monitors events related to GNSS reception.
SyncE Input Status Changed:	Monitors the state of an incoming Synchronous Ethernet reference signal.
System Sync State:	Monitors the synchronization state of the clock with the reference source.
Temperature:	Monitors system temperature.
Watchdog:	Monitors the System Watchdog for any alerts related to core meinbergOS processes.

8.9 State - Statistics

Figure 8.29: meinbergOS Web Interface: "State → Statistics" subsection

The **Statistics** subsection provides a variety of statistical analysis options for evaluating GNSS reception and reference clock performance over time.

Using the **Source** drop-down menu at the top, you can select between and reference source (*Sysref*) and GNSS receiver (*Satellites*) performance.

Reference Source Analysis (Sysref)

In this mode, the default graph shows the current offset in nanoseconds of the current master reference source.

Additional statistics can be displayed for selected reference sources by enabling the corresponding check-boxes on the right.

Figure 8.30: meinbergOS Web Interface: Selecting References for the Statistics Graph

The colored checkboxes at the top, below the drop-down menu, as shown in Fig. 8.30 represent the various reference source types supported by your meinbergOS device. Enabling any of these checkboxes will cause the selected statistics for that reference source to be additionally displayed in the graph.

The vertical scale of the graph can be adjusted by holding the **left mouse button** down and dragging it to pan up and down, or by using the **scroll wheel** to zoom the scale in and out. The graphs of statistics that are numerical in nature—**Offset**, **Mean Offset**, **Outage Count**, **Span**, and **Standard Deviation**—will scale automatically with the adjusted y-axis.

Those statistics that are represented by a simple boolean dataset (*true*/*false*) do not scale with adjustments made to the vertical axis; the points on the timeline where the value is *true* are at the top of the graph, while

the points on the timeline where the value is *false* are in the center of the graph, regardless of the configured scale. This concerns the values **Has Signal**, **Is Accurate**, **Is Connected**, **Is Locked**, **Is Master**, **Is Phase Locked**, **Is Settled**, **ITU Limit Violated**, **Low Jitter**, and **Has Signal**. The meanings of these flags are described in more detail in ➜ Chapter 8.2.1, "State - References - Overview".

The x-axis scale by default encompasses the full timeframe of the available dataset. Once the assigned memory for statistics data is full, the oldest data will be purged to make space for new data, and will disappear from the graph accordingly. The displayed time scale can be reduced or enlarged by dragging the points on the bar beneath the x-axis; The closer together the points are, the lower the scale.

GNSS Reception Analysis (Satellites)

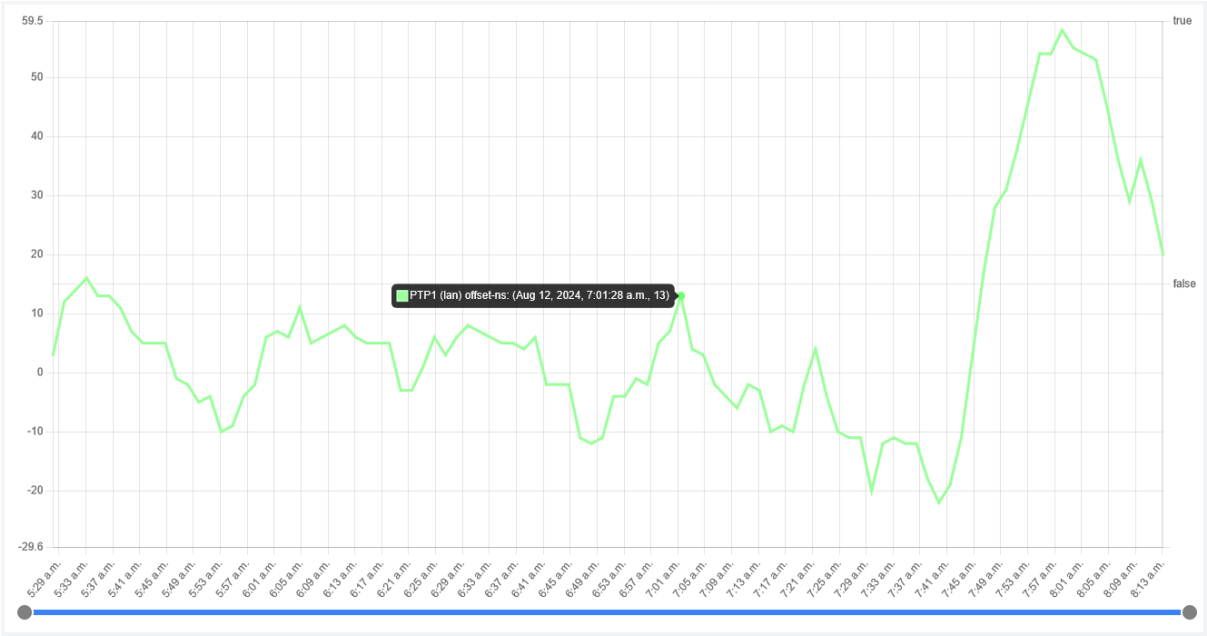


Figure 8.31: meinbergOS Web Interface: Displaying Data for a Point in a Graph

In this mode the graph displays a variety of statistics related to GNSS reception.

Additional statistics can be displayed for selected reference sources by enabling the corresponding checkboxes on the right. Please note that statistics for Galileo, GLONASS, and BeiDou reception will only be displayed if your GNSS receiver is capable of receiving these constellations.

The **Antenna Position Score** is a value calculated using an algorithm that draws upon current satellite locks and historical data in order to evaluate the quality of the position of the antenna. It is calculated by dividing the number of currently locked satellites by the nuber of satellites that should theoretically be in view. A value of 70 % or better indicates a good antenna position.

The colored checkboxes at the top below the drop-down menu represent the reference clocks of your meinbergOS device; if you only have one (as is the case for all current microSync time servers), this of course will be the only one displayed. Enabling this checkbox will cause the selected statistics for that reference source to be additionally displayed in the graph.

The vertical scale of the graph can be adjusted by holding the **left mouse button** down and dragging it to pan up and down, or by using the **scroll wheel** to zoom the scale in and out. The graphs will scale automatically with the adjusted y-axis.

The x-axis scale is set to a 24-hour timeframe by default, running from midnight to midnight. As such, the dataset can encompass GNSS reception over the course of a full day. The time scale displayed in the graph

can be reduced or enlarged by dragging the gray points on the blue bar beneath the x-axis; The closer together the points are, the lower the scale.

The data corresponding to any point in an active graph can be displayed by hovering over any point in the graph with the mouse cursor. The data will be shown in a black tooltip as shown in Fig. 8.31.

Exporting & Importing Data

Figure 8.32: meinbergOS Web Interface: Export & Import Buttons

The current dataset can be exported at any time by clicking on the **Export** at the top right of the page (Fig. 8.32). This will trigger a browser download of a JSON file containing all the current data points for the current source selected in the drop-down menu (*Sysref* or *Satellites*).

Note that **all** reference sources or integrated clocks and **all** statistics will be included in the JSON output, regardless of whether the graph for certain reference sources or clocks is enabled at the time of output.

An exported dataset can be reimported at any time for review by clicking on the **Import** button. This will prompt you to select a JSON file on your local device. Once successfully imported, the data source shown in the drop-down menu will change to **Uploaded JSON** and you will be able to review the data contained in the imported file in the graph.

8.9.1 State - Statistics - Reserved Memory

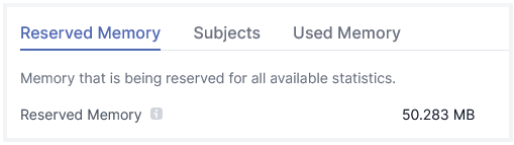


Figure 8.33: meinbergOS Web Interface: "State → Statistics → Reserved Memory" Tab

The tab "**State** → **Statistics** → **Reserved Memory**" (Fig. 8.33) provides a readout of the *maximum* amount of memory reserved by your meinbergOS device for reference source and GNSS reception statistics.

The amount of memory currently used for statistics is provided under the tab → "State - Statistics - Used Memory".

8.9.2 State - Statistics - Subjects

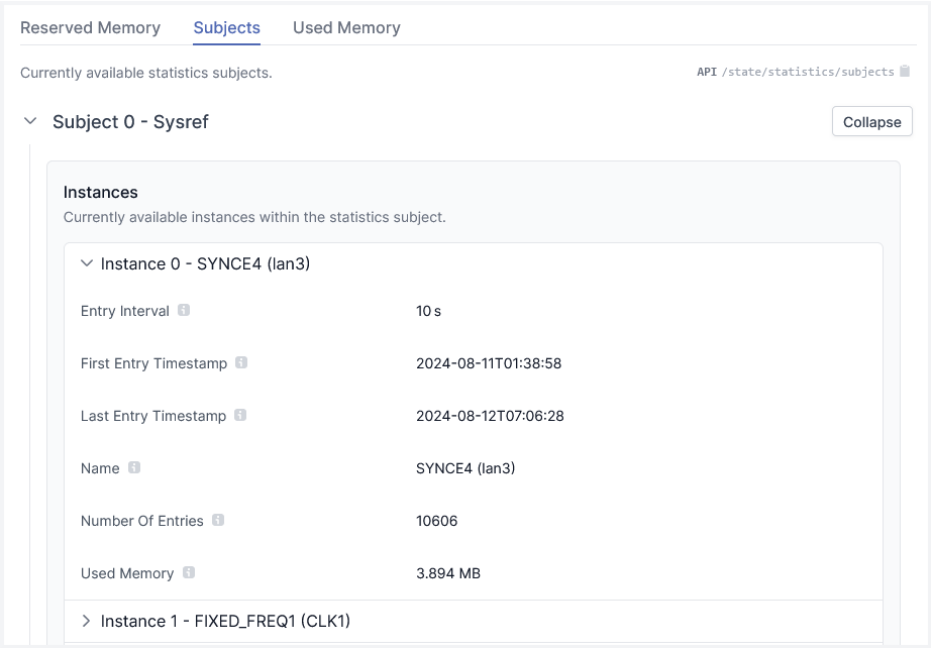


Figure 8.34: meinbergOS Web Interface: "State → Statistics → Subjects" Tab

The "**State** → **Statistics** → **Subjects**" tab (Fig. 8.34) provides information about the statistics stored for that each particular subject, be it a reference source (**Sysref**) or GNSS receiver (**Satellites**). Expanding each panel will display a series of subpanels that can themselves be expanded or collapsed to display relevant information on the statistical collection.

If the memory reserved for statistics is full, the oldest data point will be erased to make space for the latest data.

Entry Interval:	The frequency at which data is sampled.
First Entry Timestamp:	The timestamp of the earliest data point available in memory for that subject.
Last Entry Timestamp:	The timestamp of the most recent data point available in memory for that subject.
Name:	The name under which statistics for this subject are stored. This name is accordingly used for graphs and JSON output.
Number of Entries:	The number of data samples currently stored in memory for this subject.
Used Memory:	The amount of reserved memory used for the storage of statistics for this subject.

Information:

Please note that it is not possible at this time to modify the data sampling rate or subject names.

8.9.3 State - Statistics - Used Memory

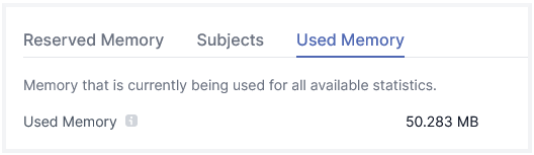


Figure 8.35: meinbergOS Web Interface: "State → Statistics → Used Memory" Tab

The tab "**State** → **Statistics** → **Used Memory**" (Fig. 8.35) provides a readout of the amount of memory *currently* used by your meinbergOS device for reference source and GNSS reception statistics.

8.10 State - Users

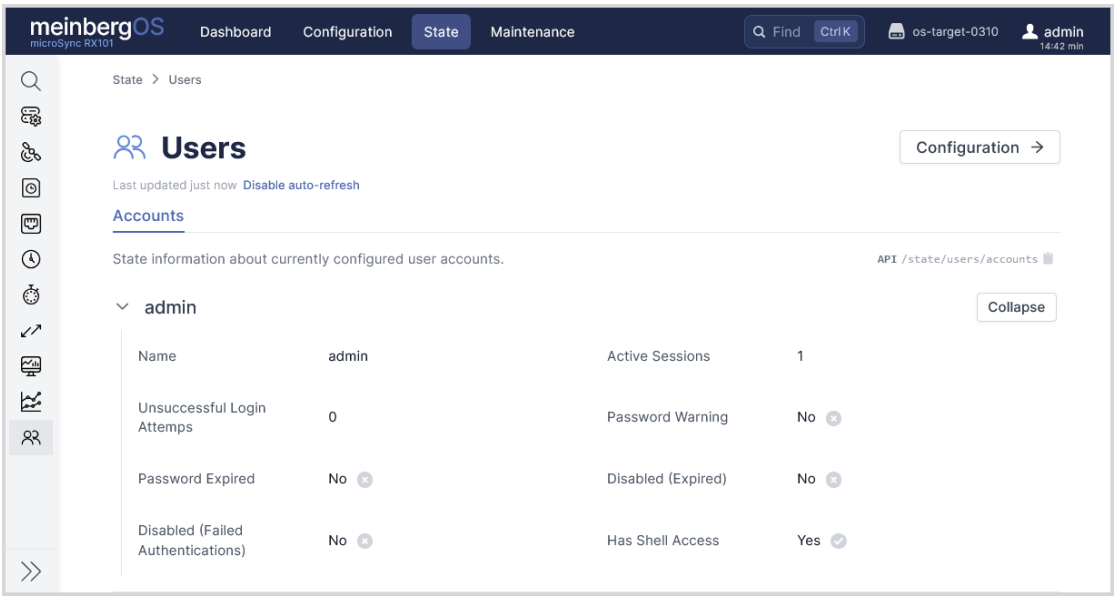


Figure 8.36: meinbergOS Web Interface: "State → Users" Subsection

The "**State → Users**" subsection (Fig. 8.36) provides a summary of all users currently configured on the system. Click on the username 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 since account creation or the last successful login. Once this is account is used to successfully log in, the counter is reset to *0*.

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.

Has Shell Access: If this account is configured to allow access via the shell channel (which is necessary, for example, to access logs, GNSS statistics etc.), this will show *Yes*.

9 Maintenance

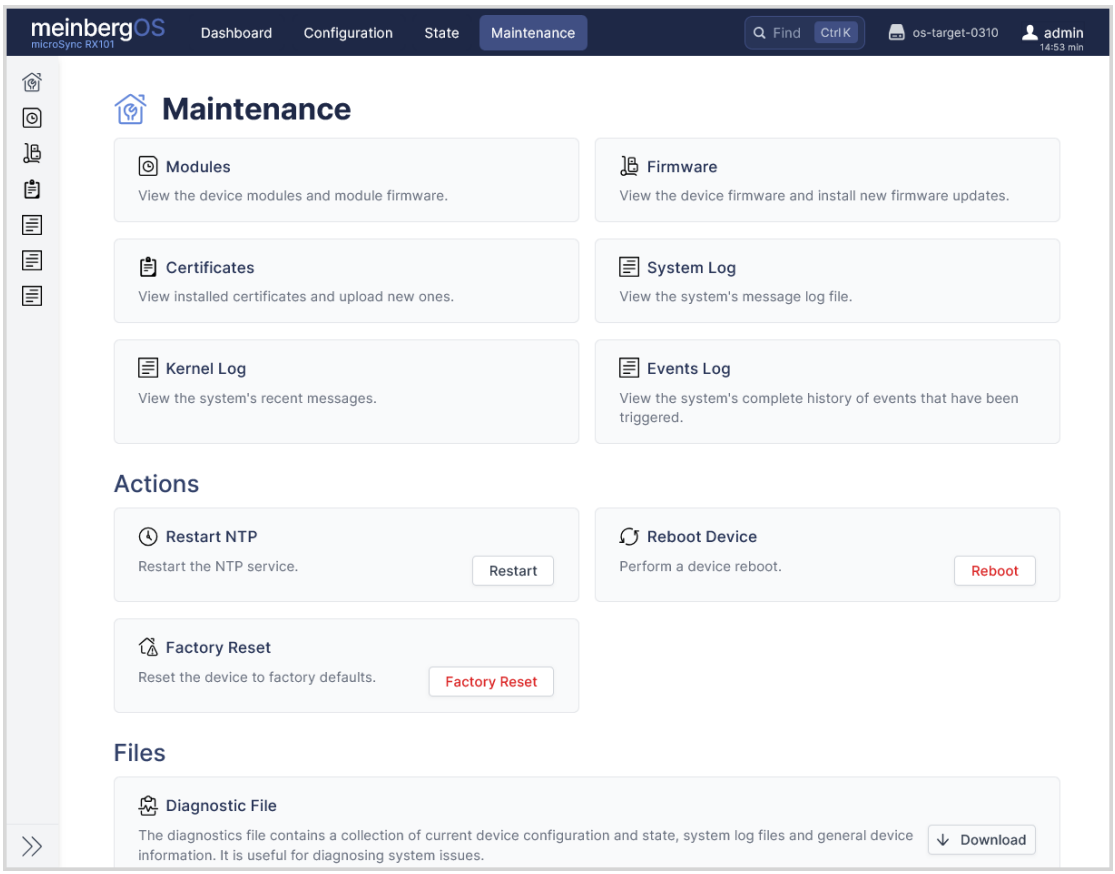


Figure 9.1: meinbergOS Web Interface: "Maintenance" Section

The **Maintenance** section (Fig. 9.1) 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.

9.1 Maintenance - Modules

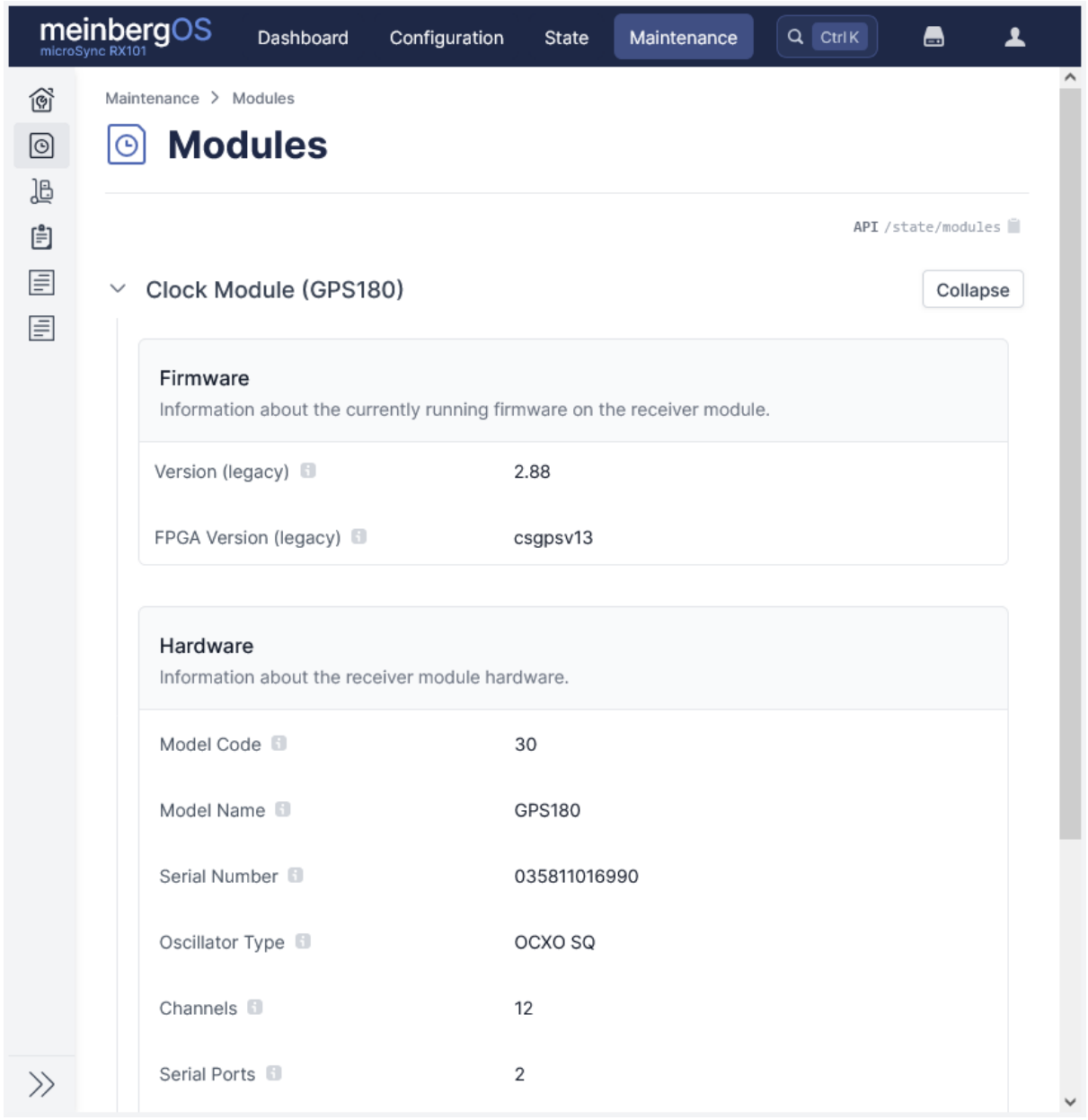


Figure 9.2: meinbergOS Web Interface: "Maintenance → Modules" Subsection

The "**Maintenance → Modules**" subsection (Fig. 9.2) 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 that are supported by the clock module and can be output 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.

I/O Module (Video Signal Generator)

microSync Broadcast systems also feature a Video Signal Generator I/O module.

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 clock module.

Model Name: The product name assigned by the manufacturer for the clock module.

Serial Number: The serial number of the clock module.

String Types: Number of string types that are supported by the clock module and can be output through the serial port.

Ticks per Second: The maximum timing resolution supported by the clock module.

9.1.1 Guide: Updating Module Firmware

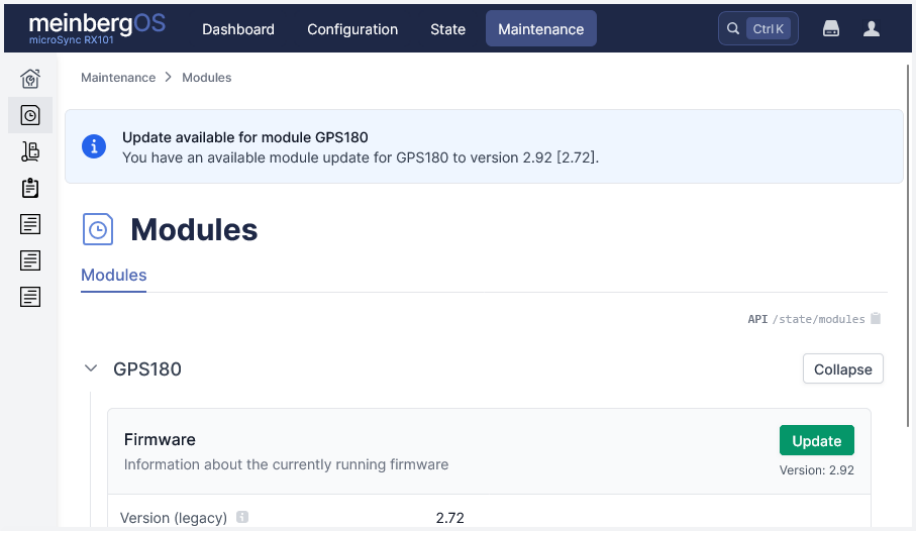


Figure 9.3: meinbergOS Web Interface – Notification of an Available Module Firmware Update

Important!

When updating certain modules, the meinbergOS will lose synchronization during the update process. This is especially true of reference clock updates, which may run for several minutes in free-run mode while the reference clock reinitializes, but can also affect other modules if the reference clock is synchronized to their inputs.

Please ensure that any critical applications that are dependent on receiving precise timing from the meinbergOS are prepared for possible timing discontinuities.

Firmware updates for modules integrated into your meinbergOS device are included in meinbergOS firmware updates. When such a module firmware update is available in the currently running version of meinbergOS, a prominent notification to this effect will be displayed at the top of the "**Maintenance** → **Modules**" section as shown in Fig. 9.3.

Selecting the green **Update** button next to the module panel will bring up a prompt in which you should confirm that you wish to install the firmware update. The updated module firmware will then be written to the integrated module, and after less than a minute, you should be notified that the firmware has successfully installed and you will be able to return to the meinbergOS Web Interface.

9.1.2 Guide: Downgrading Module Firmware

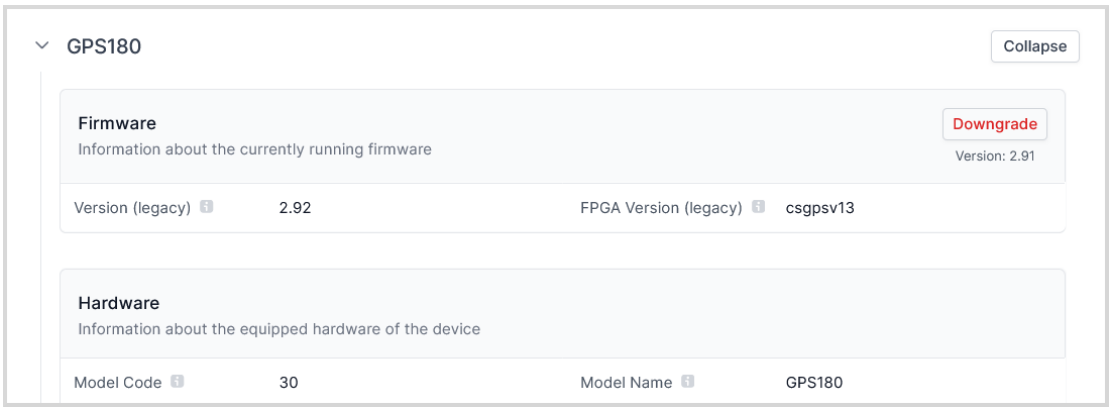


Figure 9.4: meinbergOS Web Interface – Notification of an Available Module Firmware Downgrade

Information:

Typically, it will not be necessary to downgrade the firmware of the modules even when running an earlier version of meinbergOS as future module firmware versions are designed to remain backwards compatible with earlier meinbergOS versions. This option exists only as a tool for the event that compatibility issues might arise between a given meinbergOS release and module firmware version.

The ability to downgrade module firmware was introduced in meinbergOS *2024.12.1* and allows any module firmware to be downgraded manually to a module firmware version integrated into an earlier meinbergOS release. Please note that as before, it is **not** possible to downgrade module firmware to any version integrated into meinbergOS versions prior to *2024.12.1* via the meinbergOS Web Interface.

Important!

When downgrading certain modules, the meinbergOS will lose synchronization during the update process. This is especially true of reference clock updates, which may run for several minutes in free-run mode while the reference clock reinitializes, but can also affect other modules if the reference clock is synchronized to their inputs.

Please ensure that any critical applications that are dependent on receiving precise timing from the meinbergOS are prepared for possible timing discontinuities.

When a meinbergOS version is downgraded to an earlier version and that earlier meinbergOS version contains an earlier module firmware version, you will see the option to downgrade the module firmware in the form of the "**Downgrade**" button at the top of the "**Maintenance** → **Modules**" section as shown in Fig. 9.4.

Selecting the **Downgrade** button next to the module panel will bring up a prompt in which you should confirm that you wish to install the older firmware version. The module firmware will then be written to the integrated module, and after less than a minute, you should be notified that the firmware has successfully installed and you will be able to return to the meinbergOS Web Interface.

9.2 Maintenance - Firmware

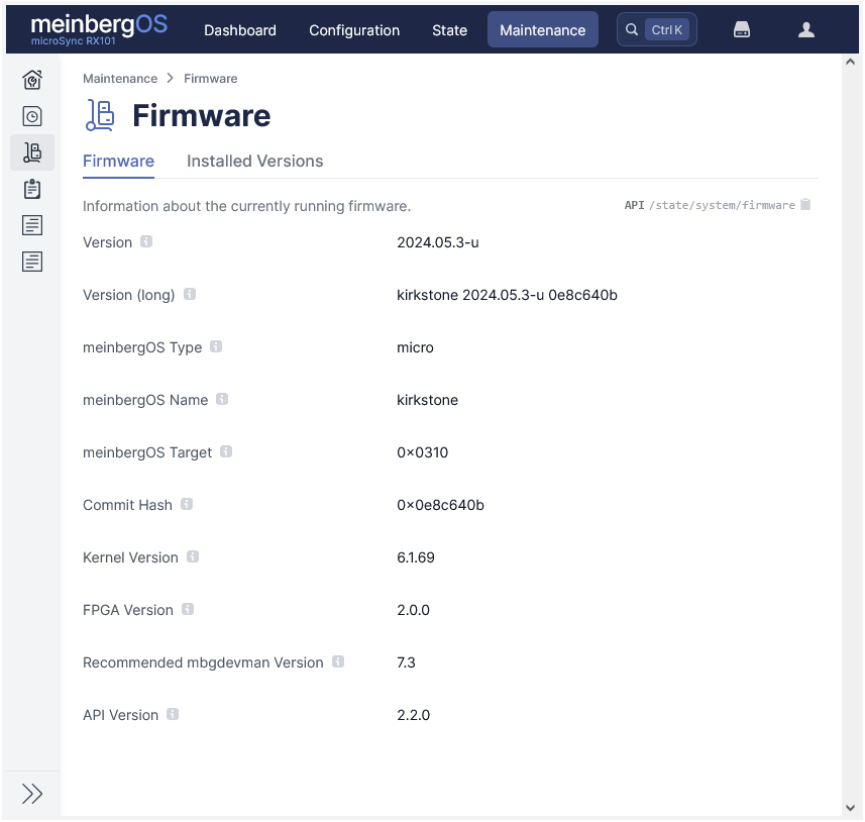


Figure 9.5: meinbergOS Web Interface: "Maintenance → Firmware" Tab

The "**Maintenance** → **Firmware**" section provides information and functionality related to the installed and running versions of meinbergOS on your meinbergOS device.

The default tab hosts information about the currently running meinbergOS version and a number of its components as well as the current FPGA design.

Information:

The information provided by this tab is identical to the information provided under → Chapter 8.1.1, "State - System - Firmware".

Version: The meinbergOS version number that is currently activated and running.

Version (Long): The full meinbergOS version identifier, including the major version code name (**meinbergOS Name**) and the most recent commit hash. This is generally only useful when using early releases of meinbergOS provided directly by Meinberg and discussing these with Meinberg's Technical Support or developers.

meinbergOS Type: The type of meinbergOS build that is currently running on this device. This will generally be *micro*.

meinbergOS Name: The code name of the meinbergOS main version that is currently activated and running. In the case of meinbergOS *2024.12*, this is *scarthgap*. meinbergOS version codenames follow those of the Yocto version that Meinberg uses to develop each embedded OS version.

meinbergOS Target: This value represents a unique identifier for the CPU and its generation and variant to allow meinbergOS to correctly identify appropriate software updates.

Commit Hash: This value is the hash identifier for the most recent commit to Meinberg's internal, non-public meinbergOS *git* repository. For end users, this value is only useful when installing a development version of the operating system provided directly by a Meinberg technician or engineer and discussing this version with Meinberg.

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.

API Version: The version of the REST API used in the currently activated meinbergOS version.

9.2.1 Maintenance - Firmware - Installed Versions

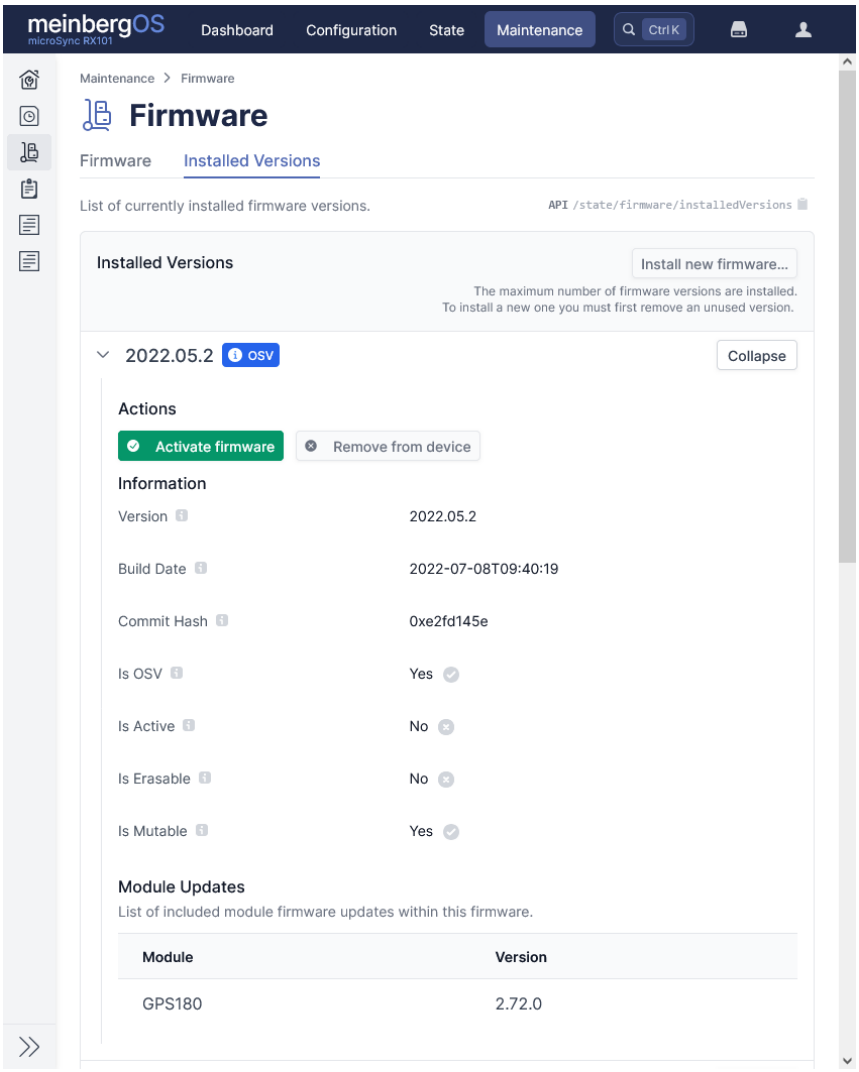


Figure 9.6: meinbergOS Web Interface: "Maintenance → Firmware → Installed Versions" Tab

This is the list of currently installed meinbergOS versions. The version that is marked with a green **Active** tag is the meinbergOS version that is currently activated on your meinbergOS device. The version that is marked with a blue **OSV** tag is the meinbergOS version that your meinbergOS device was originally shipped with.

The following information is provided for each meinbergOS version installed:

Version: The version number of this firmware.

Build Date: The date and time of this build of the firmware version.

Commit Hash: This value is the hash identifier for the most recent commit to Meinberg's internal, non-public meinbergOS *git* repository at the time of that version's release. For end users, this value is only useful when installing a development version of the operating system provided directly by a Meinberg technician or engineer and discussing this version with Meinberg, as it allows Meinberg to trace potential issues back to code commits.

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.

Please refer to → Chapter 9.1.1, "Guide: Updating Module Firmware" for more information.

9.2.1.1 Guide: Installing a New Firmware Version

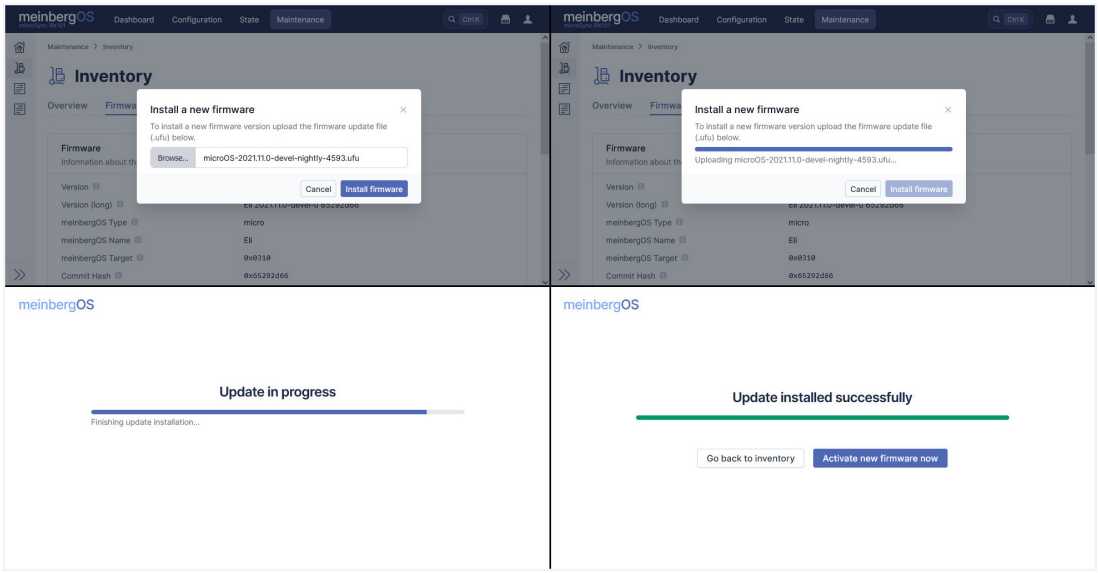


Figure 9.7: meinbergOS Web Interface: Installing a New Firmware Version

Important!

- You may have a maximum of **four** meinbergOS versions installed at any one time. This has been reduced in meinbergOS *2024.12* from five meinbergOS versions as the increasing number of features cause the size of the firmware to increase.
- 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.
- Your ability to downgrade to an older version of meinbergOS may be dependent on the hardware integrated into your meinbergOS device. If you attempt to install a version of meinbergOS that predates support for your device, the installation process will fail with a corresponding error message.

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. 📖 Fig. 9.5). You will then be prompted to select the `.ufu` firmware update file; click on **Browse...** in the dialog box that appears (📖 Fig. 9.7, 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. 9.7, top right).

The installation process will take a brief moment (📖 Fig. 9.7, 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. 9.7, 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 to force a reload by refreshing your browser.

Unsigned Firmware Files

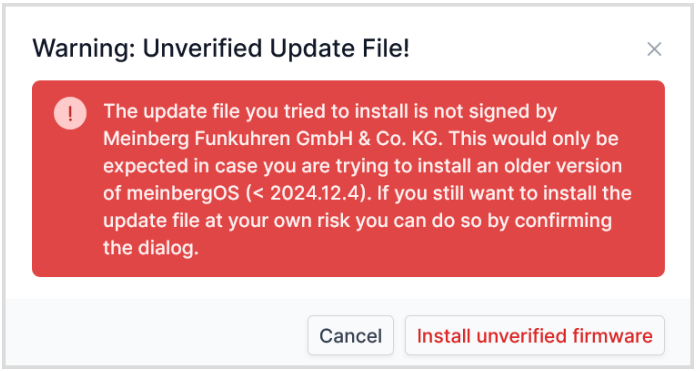


Figure 9.8: meinbergOS Web Interface: Installing an unsigned meinbergOS version

As of meinbergOS *2024.12.4*, any firmware updates to be installed must be signed as evidence of their authenticity and integrity.

When attempting to install a firmware update that is not signed, the prominent warning message shown in Fig. 9.8 will be displayed, which will need to be acknowledged at the user's own risk before installing the unverified firmware version.

Security Risk

Installing an unsigned firmware update, especially with a version number *2024.12.4* or greater, represents a security risk of **high severity**; any such firmware update is very likely to be compromised in terms of its integrity and/or security.

Any firmware update predating *2024.12.4*, including legitimate versions, are also unsigned; therefore, when installing such an older version of meinbergOS while a version of meinbergOS with firmware signature support is activated, this prominent warning message will be displayed. Even so, older meinbergOS versions are subject to the same risks of tampering.

For this reason, Meinberg strongly advises against installing any unsigned firmware update.

9.2.1.2 Guide: Removing a Firmware Version from the Inventory

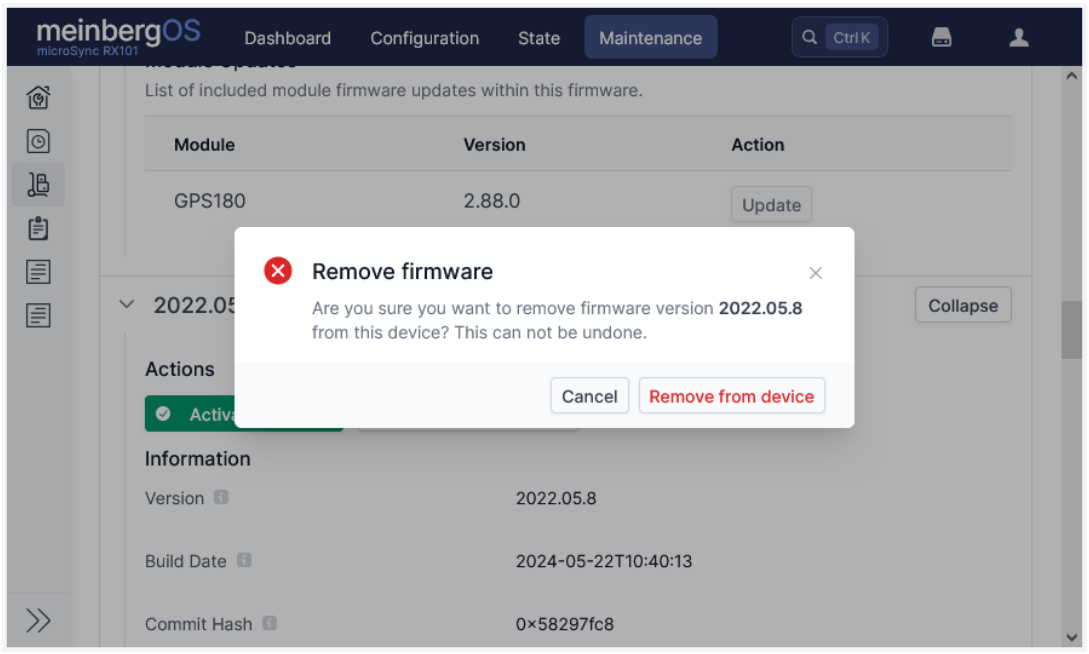


Figure 9.9: meinbergOS Web Interface: Removing a Firmware Version

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 disabled for that version of the firmware.

9.2.1.3 Guide: Activating an Installed Firmware Version

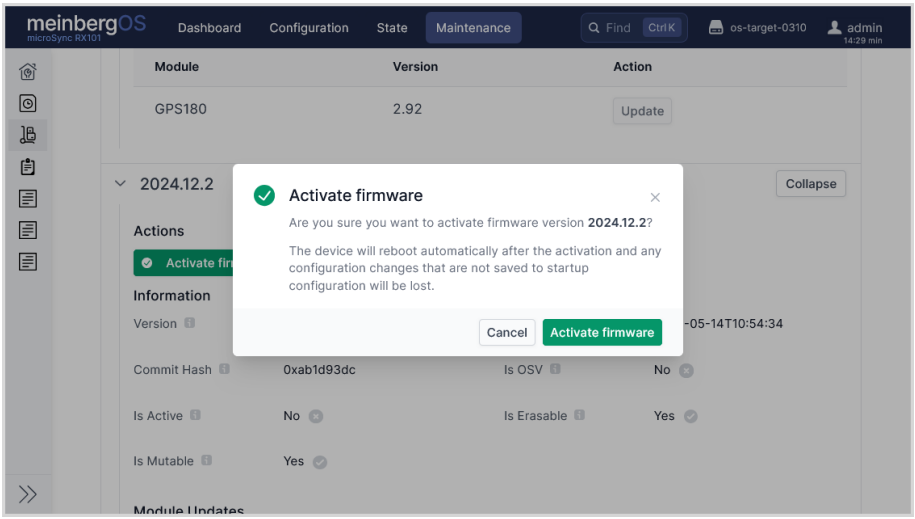


Figure 9.10: meinbergOS Web Interface: Activating a Firmware Version

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. 9.10). 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!

As of meinbergOS *2024.05.5*, it is not possible to downgrade directly to a version of meinbergOS earlier than *2022.05.0*; attempting to do so will result in an error message. Meinberg strongly advises against attempting to activate any such older version of meinbergOS by indirect means.

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 http://mbg.link/mbgdevman for more information.

9.3 Maintenance - Certificates

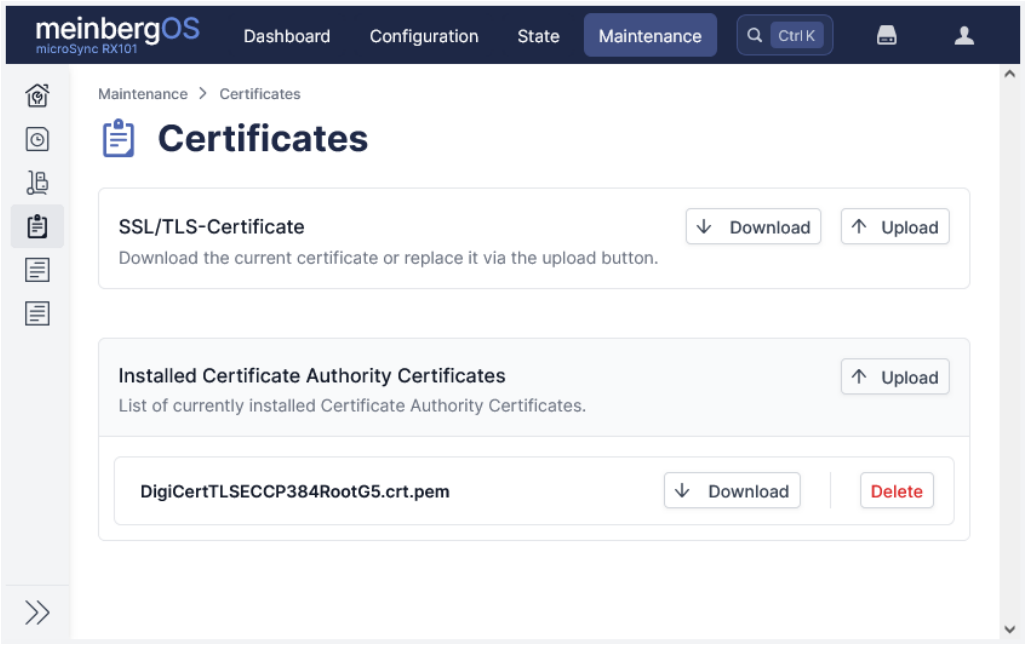


Figure 9.11: meinbergOS Web Interface: "Maintenance → Certificates" Subsection

The "**Maintenance → Certificates**" subsection is used to manage cryptographic certificates required for the integrated Web Server that provides both the meinbergOS Web Interface and the REST API.

SSL/TLS Certificate

Download: This button triggers a browser download of the meinbergOS device's own SSL/TLS certificate in `.pem` format, containing the private key and certificate.

Upload: This button is used to upload a newly signed or completely new SSL/TLS certificate in `.pem` format.

Important!

SSL/TLS certificates that are password-protected by means of encrypted private keys are **not** supported by meinbergOS.

Installed Certificate Authority Certificates

SSL/TLS certificates may be required to establish trust between the meinbergOS device and another system with which an encrypted connection is established (e.g., an LDAP server over an LDAPS connection). The Certificate Authority (CA) in this case can be an internal CA that is only recognized within a specific institution (e.g., a single local network), in which case the **public** certificate of that internal CA should be uploaded, or a public CA, in which case the **published** certificate of that CA should be uploaded.

Upload: This allows a Certificate Authority certificate to be uploaded in `.pem`, `.crt`, or `.cer` format.

Download: This triggers a browser download of the Certificate Authority certificate in the format in which it was originally uploaded.

Delete: This allows a CA certificate to be deleted. Please note that this process is irreversible; if the certificate is still valid and is required for a chain of trust, you must ensure that it is available elsewhere before deleting it from your meinbergOS device.

9.4 Maintenance - System Log

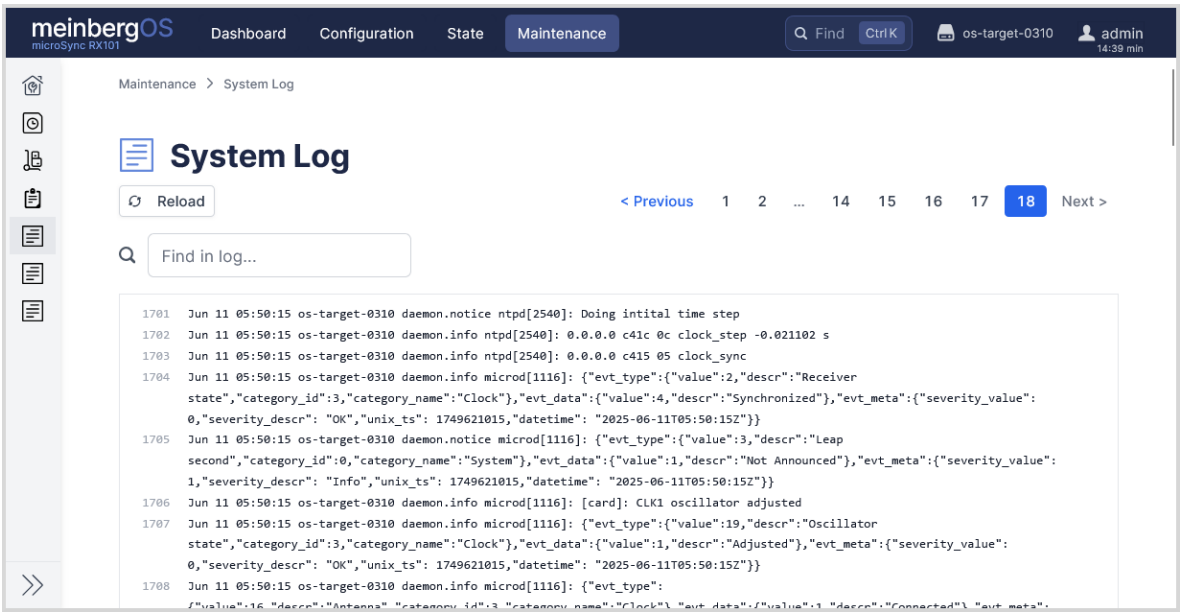


Figure 9.12: meinbergOS Web Interface: System Log

The "**Maintenance** → **System Log**" subsection (Fig. 9.12) 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. For convenience, this file is also included in the diagnostics file, which can be downloaded conveniently from the **Maintenance** section (see → Chapter 9.10, "Maintenance - Diagnostics File").

The search box can be used to filter the entries so that only those containing the entered string are displayed.

Information:

The user must have the **Shell** channel permission to be able to read the System Log. Refer to → Chapter 7.10, "Configuration - Users" and → Chapter 11.1, "User Permissions" for further information.

9.5 Maintenance - Kernel Log

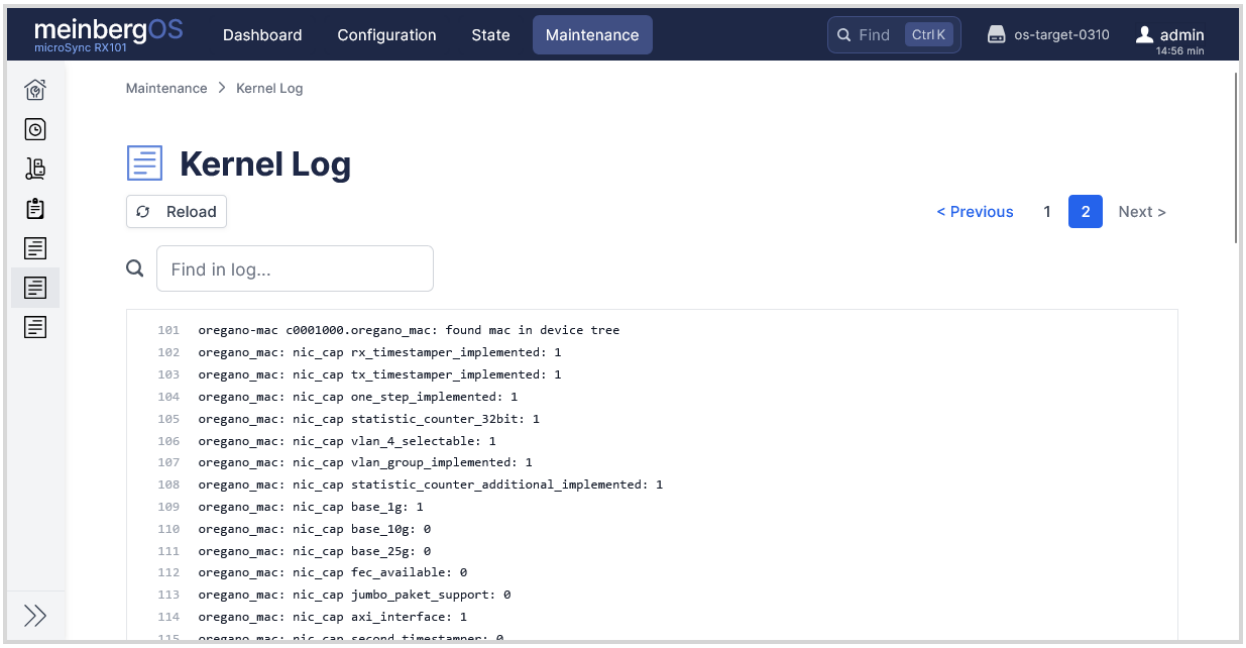


Figure 9.13: meinbergOS Web Interface: Kernel Log

The "**Maintenance** → **Kernel Log**" (Fig. 9.13) subsection provides access to the device's Linux Kernel log, which mainly provides hardware-related information.

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. For convenience, this file is also included in the diagnostics file, which can be downloaded conveniently from the **Maintenance** section (see → Chapter 9.10, "Maintenance - Diagnostics File").

The search box can be used to filter the entries so that only those containing the entered string are displayed.

Information:

The user must have the **Shell** channel permission to be able to read the Kernel Log. Refer to → Chapter 7.10, "Configuration - Users" and → Chapter 11.1, "User Permissions" for further information.

9.6 Maintenance - Events Log

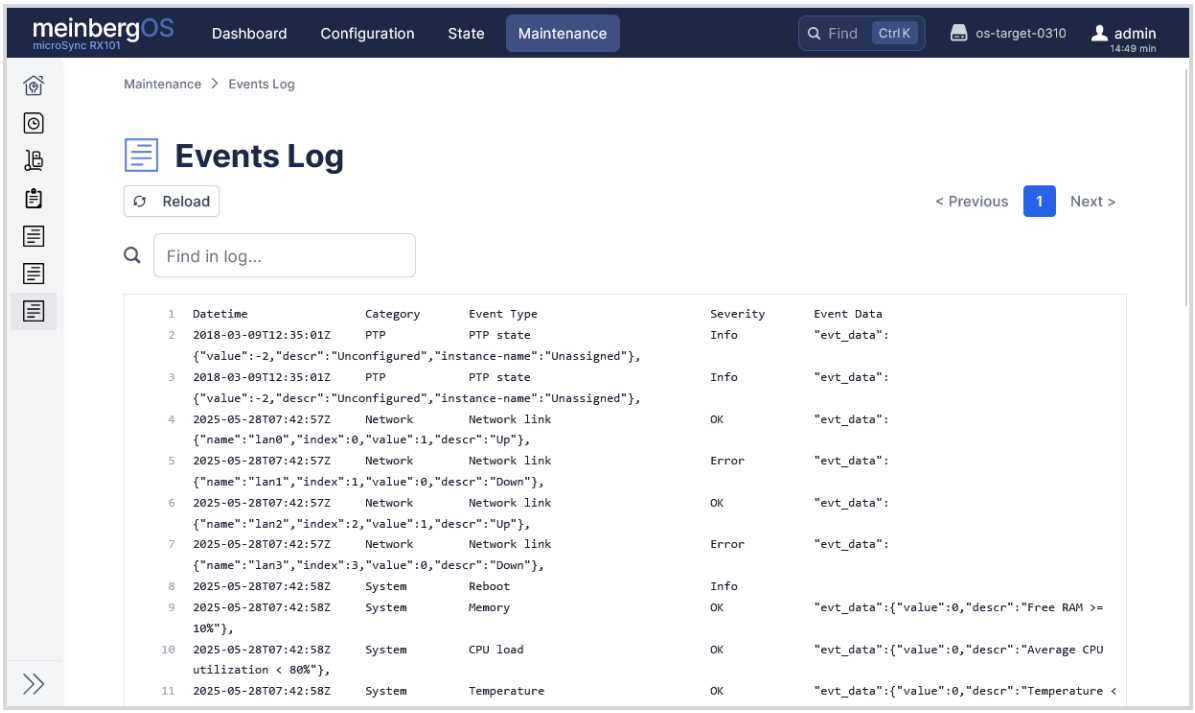


Figure 9.14: meinbergOS Web Interface: Events Log

The "**Maintenance** → **Events Log**" (Fig. 9.14) subsection provides access to the meinbergOS events log, which provides a historical timeline of operational events reported under → "State - Monitoring".

This information can be useful for troubleshooting synchronization and network issues and reviewing the events leading up to a specific situation; when contacting Meinberg Technical Support, you may be prompted to provide a copy of it. For convenience, this file is also included in the diagnostics file, which can be downloaded conveniently from the **Maintenance** section (see → Chapter 9.10, "Maintenance - Diagnostics File").

The search box can be used to filter the entries so that only those containing the entered string are displayed.

Information:

The user must have the **Shell** channel permission to be able to read the Events Log. Refer to → Chapter 7.10, "Configuration - Users" and → Chapter 11.1, "User Permissions" for further information.

9.7 Maintenance - Restart NTP

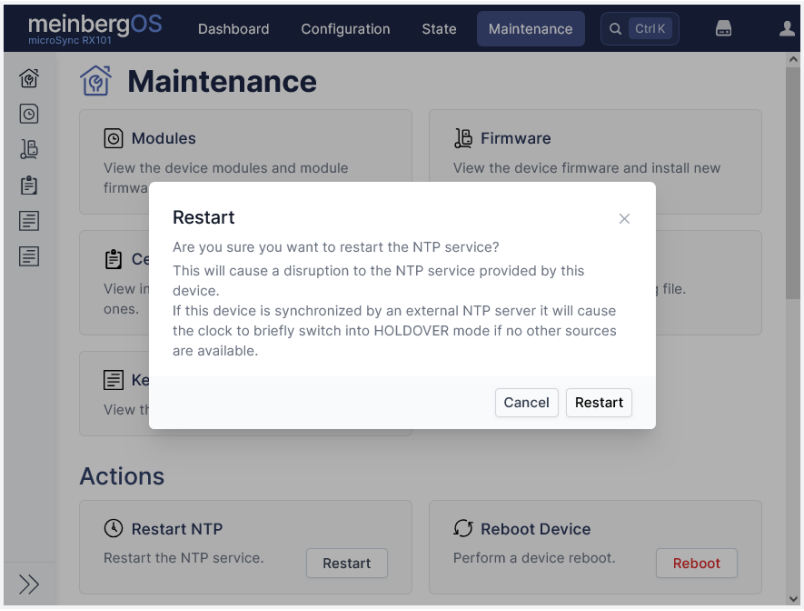


Figure 9.15: meinbergOS Web Interface: Restarting the NTP Service

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.

Important!

The user executing the **Restart NTP** operation *from the Web Interface* must have the *Read State* permission in the **System** field. Even if a user does not have this permission, the NTP service can also be restarted from the command line using the command `sudo ntpd restart` as long as the user has *Shell* and `sudo` permissions.

For more information, please refer to → Chapter 7.10, "Configuration - Users" and → Chapter 11.1, "User Permissions".

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.

9.8 Maintenance - Reboot Device

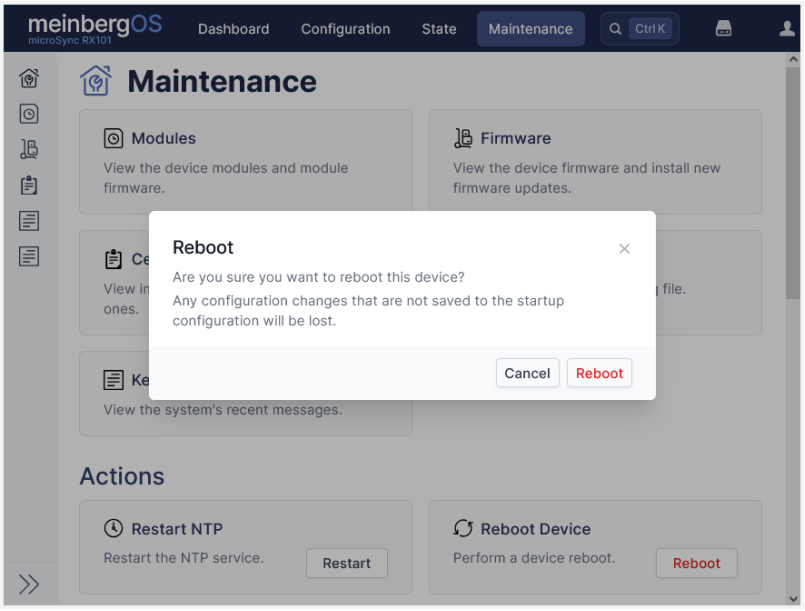


Figure 9.16: meinbergOS Web Interface: Reboot Device

The **Reboot Device** button can be used to restart the meinbergOS device as needed (Fig. 9.16). 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.

Important!

The user executing the **Reboot Device** operation *from the Web Interface* must have the *Read State* permission in the **System** field. Even if a user does not have this permission, the device can also be rebooted from the command line using the command `sudo reboot` as long as the user has *Shell* and `sudo` permissions.

For more information, please refer to → Chapter 7.10, "Configuration - Users" and → Chapter 11.1, "User Permissions".

Information:

Changes to the current configuration will be lost upon rebooting the device unless they have been saved as the Startup Configuration.

9.9 Maintenance - Factory Reset

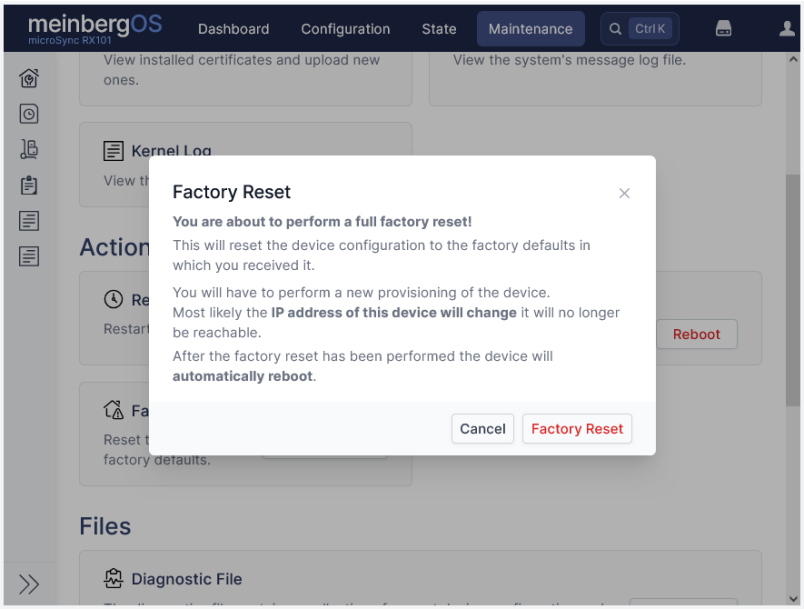


Figure 9.17: meinbergOS Web Interface: Factory Reset

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 accounts 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!

- The user executing the **Factory Reset** operation *from the Web Interface* must have the *Read State* permission in the **System** field. Even if a user does not have this permission, a factory reset can also be performed from the command line using the command `sudo reset_to_factory` as long as the user has *Shell* and `sudo` permissions.

  For more information on this, please refer to → Chapter 7.10, "Configuration - Users" and → Chapter 11.1, "User Permissions".

- 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.

9.10 Maintenance - Diagnostics File

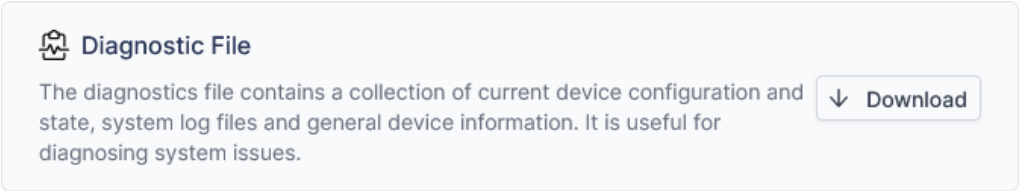


Figure 9.18: meinbergOS Web Interface: Downloading a diagnostics file

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.

9.11 Maintenance - Configuration Backup and Restore

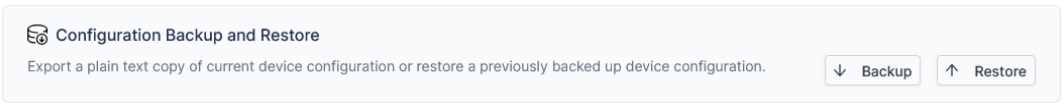


Figure 9.19: meinbergOS Web Interface: Backing up and restoring configuration files

This option allows you to manage full configurations for your meinbergOS device. Configuration backups can be kept in order to restore a working configuration from a less optimal state, to have multiple configurations optimized for different applications, or to roll out a single configuration to multiple meinbergOS devices.

Clicking on the **Backup** button (Fig. 9.19) will trigger a browser download of the current meinbergOS configuration file `daemon.cfg`.

Clicking on the **Restore** button conversely allows you to upload a previously downloaded or prepared configuration file. Once restored, your meinbergOS device will reboot and apply the new configuration.

9.12 Maintenance - Install License Upgrade

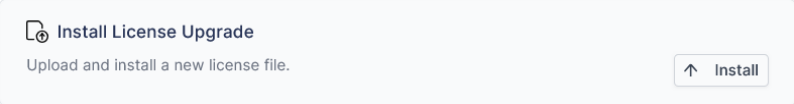


Figure 9.20: meinbergOS Web Interface: Performance Level license upgrade panel

This option allows you to install license upgrades for your meinbergOS device's PTP functionality to increase the number of PTP clocks that can be served by your meinbergOS device at once and to enable PTPv1 support.

These license upgrade files are only available directly from Meinberg and are bound to a specific device serial number. This means that you will need a separate license upgrade file for each of your meinbergOS devices.

9.12.1 Guide: Installing a License Upgrade

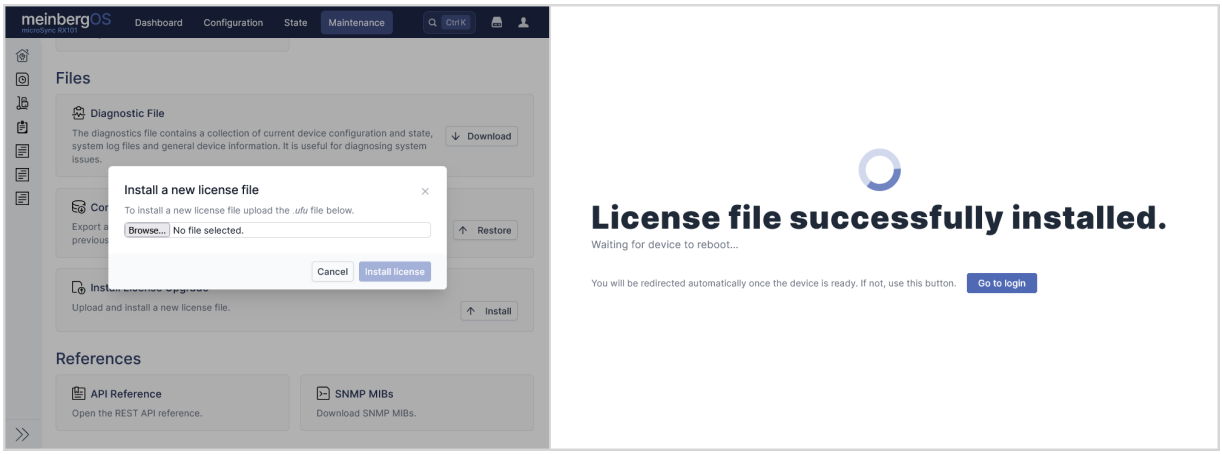


Figure 9.21: meinbergOS Web Interface: Upgrading the Performance Level license file

You may click on the **Install** button as shown in Fig. 9.20, upon which you will be prompted to select the `.ufu` file that you have been provided with by Meinberg or your authorized Meinberg distributor. Select the file before clicking on **Install License** as shown in Fig. 9.21.

Your license will now be installed; once this process is complete, your meinbergOS device will reboot with the new license. You can verify that it has been correctly applied by consulting "**State** → **PTP** → **Interfaces**"; the appropriate number of clients for your license will be displayed under each interface (see also Fig. 8.24 in → Chapter 8.6.1, "State - PTP - Interfaces":

PL-A: 8 clients

PL-B: 256 clients

PL-C: 512 clients

9.13 Maintenance - API Reference

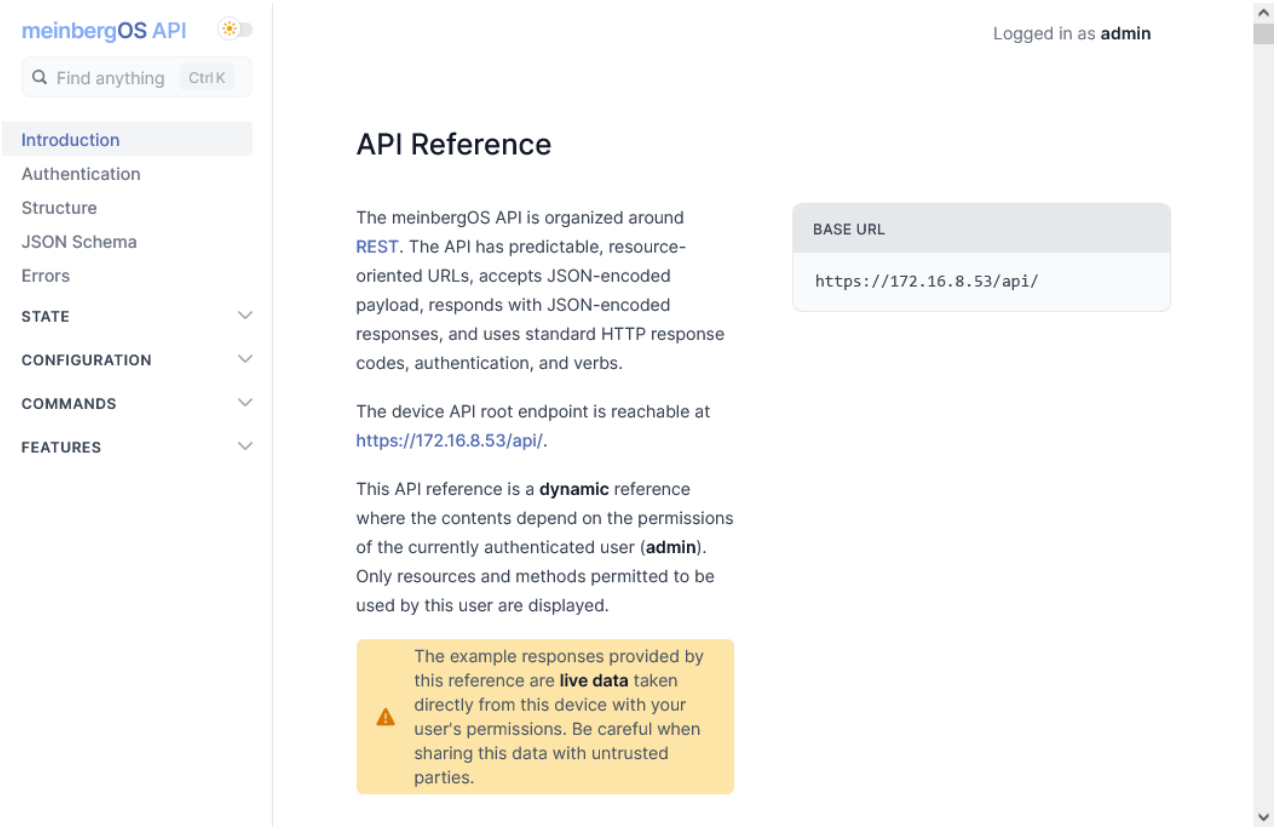


Figure 9.22: meinbergOS-Web Interface: API Reference

Selecting the **API Reference** button will open a reference guide that provides detailed information about the REST API that external applications can use to interact securely and logically with the meinbergOS device via *HTTPS*.

9.14 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.

10 Your Opinion Matters to Us

This user manual is intended to assist you with the set-up and use of this 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

11 Technical Appendix

11.1 User Permissions

meinbergOS employs a detailed user permissions concept to allow a system administrator to fine-tune the operations that any given group of users ('user levels') can execute and the data that any given user can access, whether these are user accounts representing individual humans or user accounts performed to enable access by external applications and appliances (e.g., API access).

This chapter provides more information on the effects of granting or withholding individual permissions in the context of user management in meinbergOS.

Channel Access Permissions

A channel in the context of meinbergOS user management is any method that a user can use to connect to, perform operations on, and acquire data from the meinbergOS device. As of meinbergOS *2024.12*, the following channels are recognised:

Web Interface: Access to the *Web Interface* channel allows a user to access the meinbergOS Web Interface via a web browser. Access to this channel is also required for any account that requires access to the meinbergOS REST API.

Device Manager: The *Meinberg Device Manager* channel allows a user to access the meinbergOS device using the free Meinberg Device Manager software. Please note that as of meinbergOS *2024.05*, the use of Meinberg Device Manager for the management of meinbergOS device is considered to be deprecated and users are encouraged to use the Web Interface to operate their system. As such, if you no longer require Meinberg Device Manager to manage your meinbergOS device, the deactivation of this channel is recommended.

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, and for downloading a diagnostic file archive.

SNMP: Allows access to the meinbergOS device's SNMP interface for remote monitoring and control of the meinbergOS device using an SNMP tool. Enabling or disabling the SNMP *channel* does not affect the user's access to the SNMP *configuration* via the Web Interface.

Configuration & State Access Permissions

Specifies the read & write permissions of this user to access and modify individual configuration options & state data.

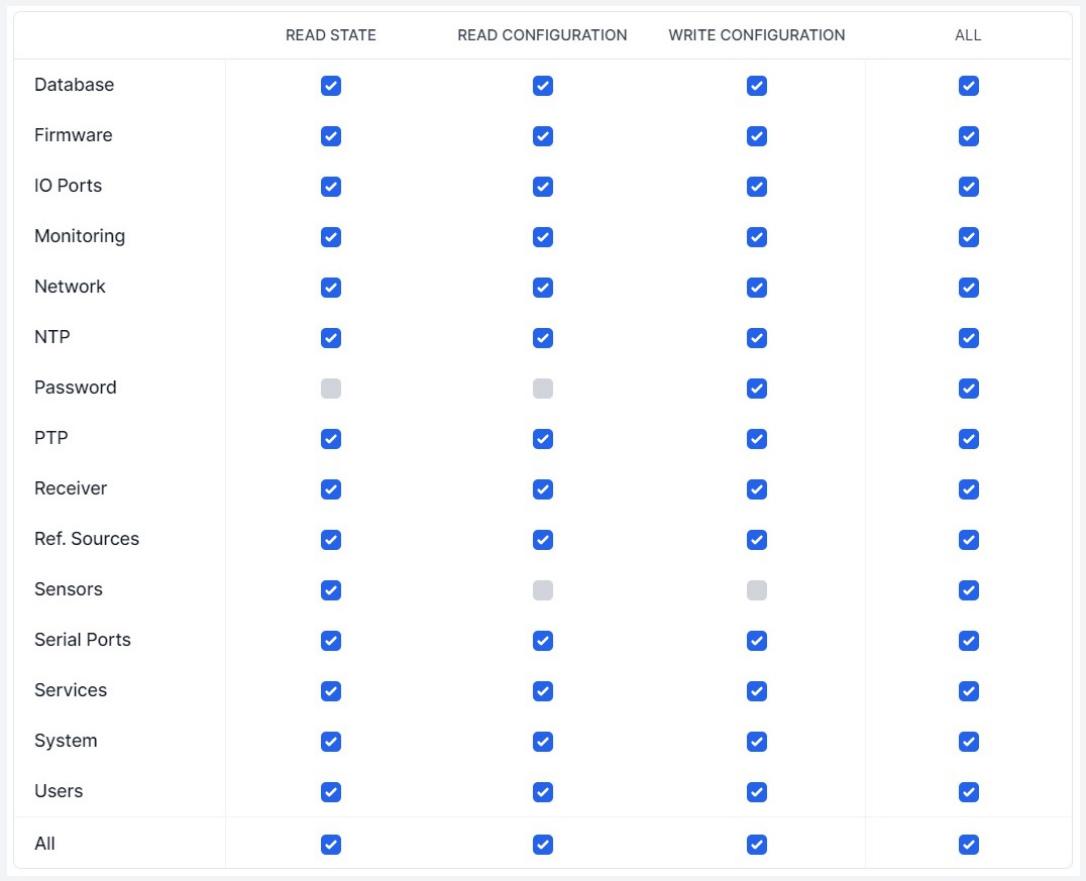


Figure 11.1: meinbergOS Web Interface: User Permissions

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, to remove any of the installed 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, although it must be accessed from the **State** section.

Monitoring:

Read Configuration: Grants the account access to the **Monitoring** subsection of the **Configuration** section, allowing it to read the SNMP, syslog, and Events configurations.

Write Configuration: Allows the user to modify the settings of the **Monitoring** configuration subsection, providing access to the *SNMP*, *syslog*, and *Events* tabs.

Read State: Provides access to the **Monitoring** subsection in the **State** section.

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) the configuration options for the **Clock** and **Receiver** subsections available in the **Configuration** section.

Write Configuration: Allows the user to modify the configuration options for the **Clock** and **Receiver** subsections available in the **Configuration** section.

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

Read Configuration: Allows the user to view (but not modify) the **Clock** subsection in the **Configuration** section and thus the current **Clock** and **Receiver** configuration.

Write Configuration: Allows the user to modify options related to the internal clock module and its receiver.

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:

A user that possesses the **IO Ports** configuration permissions can enable Simulation Mode and adjust the offset for cable length-related signal propagation delays via the **IO Ports** configuration subsection, even if that user has been denied permission to write the **Receiver** configuration.

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.

Read State: Allows the user to open the **IO Ports** subsection in the **State** section.

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
→ Chapter 9, "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 is required to provide the user with read access to the **System** configuration options in the meinbergOS Web Interface. It is also required to view the system log and kernel log, to reboot the device, to perform a factory reset, or to download a diagnostic file.

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 directly within the Web Interface, although these logs can be accessed if needed via the command line (with the **Shell** channel permission) or by downloading the diagnostics file (with the **System Write Configuration** permission).

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.

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.

11.2 Time String Formats

11.2.1 Meinberg Standard Time String

The Meinberg Standard time string is a sequence of 32 ASCII characters, starting with the character <STX> (Start of Text, ASCII code 02h) and terminated with the character <ETX> (End of Text, ASCII code 03h). 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 the 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 pattern synchronized DCF77: Clock has synchronized since last reset
	v:	"*"	GPS: Receiver has not yet verified its position PZF/DCF77: Clock currently in free-run mode
		" "	(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 Time active
	"S"	(CEST) Central European Summer Time, Daylight Saving Time inactive	
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		

11.2.2 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, it does not contain UTC time or time adjusted to any local time zone. Instead, it contains GPS time without the UTC adjustments. 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 the 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 while leap second)

uv Clock status characters:

u:	"#"	Clock is in free-run mode (no exact synchronization)
	" "	(Space, ASCII code 20h) Clock is synchronized (base accuracy is achieved)
v:	"*"	Receiver has not yet verified its position
	" "	(Space, ASCII code 20h) Receiver has determined its position

G Time zone identifier "GPS Time"

y Announcement of clock jump during last hour before discontinuity comes into effect:

"A"	Announcement of leap second insertion
" "	(Space, ASCII code 20h) nothing announced

lll Number of leap seconds between GPS time and UTC (UTC = GPS time + number of leap seconds)

<ETX> End of Text, ASCII code 03h

11.2.3 Meinberg Capture Time String

The Meinberg Capture time string is a sequence of 31 ASCII characters, terminated with the sequence <CR> (Carriage Return, ASCII code 0Dh) and <LF> (Line Feed, ASCII code 0Ah). 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, number of input		
<SP>	Space (ASCII code 20h)		
dd.mm.yy	Capture date:		
	dd	Day of the month	(01–31)
	mm	Month	(01–12)
	yy	Year without 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		

11.2.4 ATIS Time String

The ATIS standard Time String is a sequence of 23 ASCII characters terminated with a <CR» (Carriage Return) character. The standard interface configuration for this string type is 2400 Baud, 7E1. The format is as follows:

<GID><ABS><TSQ><CC><CS><ST>*yymmddhhmmsswcc*<GID><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:

<GID>	Address of the Receiver, ASCII code 7Fh	
<ABS>	Originator of Message, '0', ASCII code 30h	
<TSQ>	Telegram Number, '0', ASCII code 30h	
<CC>	Command Code 'S' (for 'SET'), ASCII code 53h	
<CS>	Command Code 'A' (for 'ALL'), ASCII code 41h	
<ST>	Time Status 'C' (for valid time), ASCII code 43h	
yymmdd	The current date:	
	yy Year of the Century	(00–99)
	mm Month	(01–12)
	dd Day of month	(01–31)
hhmmss	the current time:	
	hh hours	(00–23)
	mm minutes	(00–59)
	ss seconds	(00–59, or 60 during leap second)
w	Day of the Week	(1–7, 1 = 31h = Monday)
cc	Checksum in hexadecimal, generated from all characters including GID, ABS, TSQ, CC, ST, etc.	
<CR>	Carriage Return, ASCII code 0Dh	

11.2.5 SAT Time String

The SAT time string is a sequence of 29 ASCII characters, starting with the character <STX> (Start of Text, ASCII code 02h) and terminated with the character <ETX> (End of Text, ASCII code 03h). The format is as follows:

<STX>*dd.mm.yy/w/hh:mm:ss*x*x*x*x*u*v<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 the month	(01–31)
	mm	Month	(01–12)
	yy	Year without century	(00–99)
w	The day of the week (1 = Monday)		
hh:mm:ss	The current time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 during leap second)
xxxx	Time zone identifier:		
	"UTC"	Universal Time Coordinated, formerly GMT	
	"CET"	European Standard Time, daylight saving disabled	
	"CEST"	Central European Summer Time, Daylight Saving Time active	
u	Clock status characters:		
	"#"	Clock has not synchronized since last reset	
	" "	(Space, ASCII code 20h) Clock has synchronized since last reset	
v	Announcement for time jump during last hour before event:		
	"!"	Announcement of start or end of Daylight Saving Time	
	" "(Space, ASCII code 20h) nothing announced		
<CR>	Carriage Return, ASCII code 0Dh		
<LF>	Line Feed, ASCII code 0Ah		
<ETX>	End of Text, ASCII code 03h		

11.2.6 Uni Erlangen Time String (NTP)

The Uni Erlangen time string (NTP) is a sequence of 66 ASCII characters, starting with the character <STX> (Start of Text, ASCII code 02h) and terminated with the character <ETX> (End of Text, ASCII code 03h). 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 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 the month	(01–31)
mm	Month	(01–12)
yy	Year (without 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)

v Positive/negative sign for offset of local time zone relative to UTC

oo:oo Offset of local time zone relative to UTC in hours and minutes

ac Clock status:

a:	"#"	Clock has not synchronized since reset
	" "	(Space, ASCII code 20h) Clock has synchronized since reset
c:	"*"	GPS receiver has not verified its position
	" "	(Space, ASCII code 20h) GPS receiver has determined its position

d Time zone identifier:

"S"	CEST	Central European Summer Time
" "	CET	Central European Time

f Announcement of clock jump during last hour before discontinuity comes into effect:

"!"	Announcement of start or end of Daylight Saving Time
" "	(Space, ASCII code 20h) nothing announced

g Announcement of clock jump during last hour before discontinuity comes into effect:

"A"	Announcement of leap second
" "	(Space, ASCII code 20h) nothing announced

i Leap second

"L"	Leap second is currently to be inserted (only active in 60th second)
" "	(Space, ASCII code 20h) No leap second announced

bbb.bbbb Geographical latitude of the receiver position in degrees
Leading zeroes are padded with spaces (ASCII code 20h)

n	Geographical hemisphere, possible characters are: "N" North of Equator "S" South of Equator
lll.llll	Geographical longitude of the receiver position in degrees Leading zeroes are padded with spaces (ASCII code 20h)
e	Prime meridian hemisphere, possible characters are: "E" East of Greenwich Meridian "W" West of Greenwich Meridian
hhhh	Altitude in meters of receiver position above WGS84 ellispoid Leading zeroes are padded with spaces (ASCII code 20h)
<ETX>	End of Text, ASCII code 03h

11.2.7 NMEA 0183 String (RMC)

The NMEA 0183 RMC time string is a sequence of 65 ASCII characters, starting with the string "$GPRMC" and terminated with the sequence <CR> (Carriage Return, ASCII code 0Dh) und <LF> (Line Feed, ASCII code 0Ah). 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 as defined below:

$	Start character, ASCII code 24h sent with one-bit accuracy at the change of each second		
GP	Device ID, in this case "GP" for GPS		
RMC	Message type ID, in this case "RMC"		
hhmmss.ss	The current time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 during leap second)
	ff	Fractional seconds	(1/10 ; 1/100)
A	Status (A = Time data valid, V = Time data not valid)		
bbbb.bb	Geographical latitude of the receiver position in degrees Leading zeroes are padded with spaces (ASCII code 20h)		
n	Geographical hemisphere, possible characters are:		
	"N"	North of Equator	
	"S"	South of Equator	
lllll.ll	Geographical longitude of the receiver position in degrees Leading zeroes are padded with spaces (ASCII code 20h)		
e	Prime meridian hemisphere, possible characters are:		
	"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	Current Date:		
	dd	Day of the month	(01–31)
	mm	Month	(01–12)
	yy	Year of Century	(00–99)
a	Magnetic variation E/W		
hh	Checksum (XOR sum of all characters except "$" and "*")		
<CR>	Carriage Return, ASCII code 0Dh		
<LF>	Line Feed, ASCII code 0Ah		

11.2.8 NMEA 0183 Time String (GGA)

The NMEA 0183 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 as defined below:

$	Start character, ASCII code 24h sent with one-bit accuracy at the change of each second
GP	Device ID, in this case "GP" for GPS
GGA	Message type ID, in this case "GGA"
hhmmss.ss	The current time: *hh* Hours (00–23) *mm* Minutes (00–59) *ss* Seconds (00–59, or 60 while leap second) *ff* Fractional seconds (1/10 ; 1/100)
bbbb.bbbbb	Geographical latitude of receiver position in degrees Leading zeroes are padded with spaces (ASCII code 20h)
n	Geographical hemisphere, possible characters are: "N" North of Equator "S" South of Equator
lllll.lllll	Geographical longitude of the receiver position in degrees Leading zeroes are padded with spaces (ASCII code 20h)
e	Prime meridian hemisphere, possible characters are: "E" East of Greenwich Meridian "W" West of Greenwich Meridian
A	Position determined (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 sum of all characters except "$" and "*")
<CR>	Carriage Return, ASCII code 0Dh
<LF>	Line Feed, ASCII code 0Ah

11.2.9 NMEA 0183 Time String (ZDA)

The NMEA 0183 ZDA time 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)		

11.2.10 ABB SPA Time String

The ABB SPA string is a sequence of 32 ASCII characters, starting with the string ">900WD:" and terminated with the character <CR> (Carriage Return). The format is as follows:

>900WD:*yy-mm-dd[lt]SP>hh.mm;ss.fff:cc*<CR>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are directly part of the time string. The groups of characters as defined below:

yy-mm-dd	Current Date:		
	yy	Year without century	(00–99)
	mm	Month	(01–12)
	dd	Day of the month	(01–31)
	<SP>	Space (ASCII code 20h)	
hh.mm;ss.fff	Current Time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 during leap second)
	fff	Milliseconds	(000–999)
cc	Checksum. This is calculated as the XOR sum of the preceding characters. The resultant 8-bit value is reported as a hex value in the form of two ASCII characters (0–9 or A–F)		
<CR>	Carriage Return (ASCII code 0Dh)		

11.2.11 Computime Time String

The Computime time string is a sequence of 24 ASCII characters, starting with the character `T` and terminated with the character `<LF>` (Line Feed, ASCII code 0Ah). The format is as follows:

`T:`*`yy:mm:dd:ww:hh:mm:ss`*`<CR><LF>`

The letters printed in italics are replaced by ASCII numbers whereas the other characters are unalterable parts of the time string. The groups of characters as defined below:

`T` — Start character
Sent with one-bit accuracy at the change of each second

`yy:mm:dd` — The current date:

`yy`	Year without century	(00–99)
`mm`	Month	(01–12)
`dd`	Day of the month	(01–31)
`ww`	Day of the week	(01–07, 01 = Monday)

`hh:mm:ss` — The current time:

`hh`	Hours	(00–23)
`mm`	Minutes	(00–59)
`ss`	Seconds	(00–59, or 60 during leap second)

`<CR>` — Carriage Return, ASCII code 0Dh

`<LF>` — Line Feed, ASCII code 0Ah

11.2.12 RACAL Time String

The RACAL 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)		

11.2.13 SYSPLEX-1 Time String

The SYSPLEX 1 time string is a sequence of 16 ASCII characters, starting with the character <SOH> (Start of Header, ASCII code 01h) and terminated with the character <LF> (Line Feed, ASCII code 0Ah).

Important!

To ensure that the time string can be correctly output and displayed through your terminal software of choice, a "C" must be sent (once, without quotes).

The format is as follows:

<SOH>*ddd*:*hh*:*mm*:*ss*q<CR><LF>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are unalterable parts 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 the Year		(001–366)	
hh:mm:ss	The current time:			
	hh	Hours	(00–23)	
	mm	Minutes	(00–59)	
	ss	Seconds	(00–59, or 60 during leap second)	
	q	Clock Status:	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			

11.2.14 ION Time String

The ION time string is a sequence of 16 ASCII characters, starting with the character <SOH> (Start of Header, ASCII code 01h) and terminated with the character <LF> (Line Feed, ASCII code 0Ah). 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)	Time Sync (GPS Lock)
			"?" (ASCII code 3Fh)	No Time Sync (GPS Fail)
<CR>	Carriage Return (ASCII code 0Dh)			
<LF>	Line Feed (ASCII code 0Ah)			

11.2.15 ION Blanked Time String

The ION time string is a sequence of 16 ASCII characters, starting with the character <SOH> (Start of Header, ASCII code 01h) and terminated with the character <LF> (Line Feed, ASCII code 0Ah). The format is as follows:

<SOH>*ttt:hh:mm:ss*q<CR><LF>

Important!

The blanking interval lasts for 2 minutes and 30 seconds and is inserted every five minutes.

The letters printed in italics are replaced by ASCII numbers whereas the other characters are unalterable parts 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 the year		(001–366)	
hh:mm:ss	The current time:			
	hh	Hours	(00–23)	
	mm	Minutes	(00–59)	
	ss	Seconds	(00–59, or 60 during leap second)	
	q	Clock Status:	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			

11.2.16 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 start of the second is marked by the leading edge of the start bit of the string. The string is 15 characters long and is sent once a 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 numbers whereas the other characters are unalterable elements of the string. The groups of characters 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 in hours (HH), minutes (MM), seconds (SS)
<CR>	Carriage Return, ASCII code 0Dh
<LF>	Line Feed, ASCII code 0Ah

11.2.17 6021 Time String

The 6021 time string is a sequence of 18 ASCII characters starting with the <STX> (Start of Text, ASCII code 02h) ASCII control character and terminated with the sequence <LF> (Line Feed, ASCII code 0Ah), <CR> (Carriage Return, ASCII code 0Dh), <ETX> (End of Text, ASCII code 03h).

It is broadly identical to the ➜ "Freelance Time String", but with a different order to the termination sequence.

The format is as follows:

<STX>*C9hhmmssddmmyy*<LF><CR><ETX>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<STX> Start of Text, ASCII code 02h

C Clock status. This is represented as an ASCII nibble*, whereby each bit in the binary sequence has the following meaning:

Bit 0 (LSB)	Leap second announced (1) / not announced (0)
Bit 1	Leap second active (1) / not active (0)
Bit 2	Real-time clock time valid (1) / invalid (0)
Bit 3 (MSB)	Clock is synchronized (1) / not synchronized (0)

Example: If the clock outputs C (ASCII code 0x43h) at this position, this corresponds to a binary value of *1100*, indicating that the RTC time is valid and the clock is synchronized, and that no leap second has been announced, nor is one in effect.

9 UTC status of clock and day of the week. This is represented as an ASCII nibble*, whereby the three least significant bits represent the day of the week and may be any value between 1 and 7 (corresponding to Monday to Sunday). The most significant bit represents the UTC state and will be 1 if set to UTC and 0 if it is a local time zone. Thus, if the clock is outputting local (non-UTC) time, this will be in a range of 1–7, whereas if the clock is outputting UTC time, this value will be in a range of 9–F.

Example: If the clock outputs 9 (ASCII code 0x39h) at this position, this corresponds to a binary value of *1001*. The most significant bit of *1* here indicates that the clock is running on UTC time, while the 3-bit value represented by the least significant bits *001* indicates that the day is Monday.

hhmmss Current time:

hh	Hours	(00–23)
mm	Minutes	(00–59)
ss	Seconds	(00–59, or 60 during leap second)

ddmmyy Current date:

dd	Day	(01–31)
mm	Month	(01–12)
yy	Last two digits of year	(00–99)

<LF>	Line Feed (ASCII code 0Ah)
<CR>	Carriage Return (ASCII code 0Dh)
<ETX>	End of Text (ASCII code 03h)

* With ASCII nibbles, the actual ASCII character itself (0–9, A–F, ASCII codes *0x30h–0x39h* and *0x41h–0x46h*) represents the hexadecimal equivalent of a 4-bit binary sequence. For example, if the clock outputs "A" at these positions, this is equivalent to a binary sequence of *0x1010b*. Please note that it is not the binary equivalent of the ASCII code (*0x41h*) itself.

11.2.18 Freelance Time String

The Freelance time string is a sequence of 18 ASCII characters starting with the <STX> (Start of Text, ASCII code 02h) ASCII control character and terminated with the sequence <CR> (Carriage Return, ASCII code 0Dh), <LF> (Line Feed, ASCII code 0Ah), <ETX> (End of Text, ASCII code 03h).

It is broadly identical to the ➜ "6021 Time String", but with a different order to the termination sequence.

The format is as follows:

<STX>*C9hhmmssddmmyy*<CR><LF><ETX>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<STX> Start of Text, ASCII code 02h

C Clock status. This is represented as an ASCII nibble*, whereby each bit in the binary sequence has the following meaning:

Bit 0 (LSB)	Leap second announced (1) / not announced (0)
Bit 1	Leap second active (1) / not active (0)
Bit 2	Real-time clock time valid (1) / invalid (0)
Bit 3 (MSB)	Clock is synchronized (1) / not synchronized (0)

Example: If the clock outputs C (ASCII code 0x43h) at this position, this corresponds to a binary value of *1100*, indicating that the RTC time is valid and the clock is synchronized, and that no leap second has been announced, nor is one in effect.

9 UTC status of clock and day of the week. This is represented as an ASCII nibble*, whereby the three least significant bits represent the day of the week and may be any value between 1 and 7 (corresponding to Monday to Sunday). The most significant bit represents the UTC state and will be 1 if set to UTC and 0 if it is a local time zone. Thus, if the clock is outputting local (non-UTC) time, this will be in a range of 1–7, whereas if the clock is outputting UTC time, this value will be in a range of 9–F.

Example: If the clock outputs 9 (ASCII code 0x39h) at this position, this corresponds to a binary value of *1001*. The most significant bit of *1* here indicates that the clock is running on UTC time, while the 3-bit value represented by the least significant bits *001* indicates that the day is Monday.

hhmmss Current time:

hh	Hours	(00–23)
mm	Minutes	(00–59)
ss	Seconds	(00–59, or 60 during leap second)

ddmmyy Current date:

dd	Day	(01–31)
mm	Month	(01–12)
yy	Last two digits of year	(00–99)

<CR>	Carriage Return (ASCII code 0Dh)
<LF>	Line Feed (ASCII code 0Ah)
<ETX>	End of Text (ASCII code 03h)

* With ASCII nibbles, the actual ASCII character itself (0–9, A–F, ASCII codes *0x30h–0x39h* and *0x41h–0x46h*) represents the hexadecimal equivalent of a 4-bit binary sequence. For example, if the clock outputs "A" at these positions, this is equivalent to a binary sequence of *0x1010b*. Please note that it is not the binary equivalent of the ASCII code (*0x41h*) itself.

11.2.19 ITU-G8271-Y.1366 Time-of-Day Message

The ITU-G8271-Y.1366 standard stipulates the transmission of this time message at 9600 Baud with framing of 8N1. The message data should be sent no sooner than 1 ms after the rising edge of the PPS signal and transmission must be completed within 500 ms. The message should be sent once a second and mark the rising edge of the PPS.

The ITU-G8271-Y.1366 time message itself output by Meinberg clocks is always a sequence of 21 bytes. While the standard briefly references the use of two ASCII characters for the first two characters, it should be noted that this message is not an ASCII string in the typical sense. Multi-octet values are transmitted as big-endian values, while each byte is transmitted with the least-significant bit **first**. Accordingly, while the first two characters are deemed to represent the ASCII characters "C" (ASCII code 0x43h, binary `00101011`) and "M" (ASCII code 0x4Dh, binary `01001101`) respectively, these are transmitted as `11010100` and `10110010`.

The standard byte sequence (least significant bit first in each byte) is as defined below:

Byte No.	Meaning
0–1	Always 0x43h followed by 0x4Dh. These are Sync Characters 1 & 2 respectively and are used as a delimiter between messages.
2	The message class. This will always carry a value of 0x01h.
3	The message ID. In the time-of-day messages provided by Meinberg clocks this will always be 0x01h.
4–5	The payload length, expressed as an unsigned 16-bit integer, not including the sync characters, message class, message ID, or checksum. In the time-of-day messages provided by Meinberg clocks this will always be 0x0Eh.
6–11	PTP time, or the number of seconds in the TAI timescale. This is expressed as an unsigned 48-bit integer.
12	This byte is reserved for future use and is set to 0x00h.
13	Contains a number of time status flags: **Bit 0:** Positive leap second pending **Bit 1:** Negative leap second pending **Bit 2:** UTC offset valid **Bit 3:** Reserved **Bit 4:** Time is traceable to a primary frequency standard **Bit 5:** Frequency is traceable to a primary frequency standard **Bit 6:** Reserved **Bit 7:** Reserved
14–15	Current offset between TAI and UTC in seconds, expressed as an unsigned 32-bit integer.
16–19	This byte is reserved for future use and is set to 0x00h.
20	An 8-bit cyclic redundancy check value calculated on the basis of bytes 2–19.

11.2.20 CISCO ASCII Time String

The CISCO ASCII time string is a sequence of at least 73 ASCII characters. The format is as follows:

*.A.*mjdxx*,*yy*/*mm*/*dd*,*hh*:*mm*:*ss*,*+3600.0*,*12N34.567*,*123W45.678*,+1234,
EV<SP>GPS<SP>FLT

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:

*	Sync state of clock: *: Clock is synchronized to reference !: Clock is not synchronized
A	The format revision. With Meinberg clocks, this will always be 'A'.
mjdxx	The current date in Modified Julian Date format.
yy/mm/dd	The current date in Gregorian *yy*/*mm*/*dd* format.
hh:mm:ss	The current time in 24-hour format.
+3600	The current local time offset in seconds. If the clock is outputting UTC time, this will be 00000.0. If the clock is outputting local time, however, the first character will be the sign (– or +) and the subsequent digits up to the period character are the offset. For example, if CET is set as the time zone, this will show +3600.
0	Indicator of a pending leap second.
12N34.567	The current latitude of the GNSS receiver. If the time reference is not a GNSS receiver, this will show 00 00.000.
123W45.678	The current longitude of the GNSS receiver. If the time reference is not a GNSS receiver, this will show 000 00.000
+1234	The current altitude above sea level of the GNSS receiver. If the time reference is not a GNSS receiver, this will show +0000.
EV	Indicates the level of any current alarm state of the clock: EV: Non-error event MN: Minor error MJ: Major error CL: Critical error
GPS	Indicates the source of the current error (e.g., 'GPS' for GPS receiver).
FLT	Indicates the cause of the current error (e.g., 'FLT' for hardware fault).

11.2.21 NTP Type 4 Time String

The NTP Type 4 time string is a sequence of 24 ASCII characters. The format is as follows:

?<SP>*yy*<SP>*ddd*<SP>*hh:mm:ss.SSSL*<SP>S

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:

?	Sync state of clock:		
	Space:	Clock is synchronized to reference	
	'?':	Clock is not synchronized	
yy	Year of the century		(00–99)
ddd	Day of the year		(001–366)
hh:mm:ss.SSS	Current time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 while leap second)
	SSS	Milliseconds	(000–999)
L	Leap second announcement:		
	Space:	No leap second announcement	
	'L':	Leap second pending	
S	Daylight Savings Time indicator:		
	'S':	Standard Time (wintertime)	
	'D':	Daylight Savings Time (summertime)	

11.3 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

11.4 Overview of Programmable Signals

Meinberg systems with programmable pulse outputs provide the following signal options; the actual range of available signal options will vary from system to system:

Idle

Selecting "**Idle**" allows individual programmable outputs to be disabled individually.

Timer

In "**Timer**" mode, the output simulates a timer with a fixed daily schedule. It is possible to configure three switch-on and three switch-off times for each day and each output. In order to set a timer, both the switch-on time ("**ON**") and the corresponding switch-off time ("**OFF**") must be set. If the switch-on time is later than the switch-off time, the switching scheduler will interpret this to mean that the switch-off time is on the next day, which will keep the signal enabled through midnight.

Thus, if a program was set with a switch-on time of *23:45:00* and a switch-off time of *0:30:00*, this would cause the output to be enabled on day *n* at 11:45 p.m., and then to be disabled on day *n+1* at 12:30 a.m. If any of these three programs are to be left disabled, simply enter the same times into the "**ON**" and "**OFF**" fields. The "**Signal**" selector specifies the active state for the timer periods. Selecting "*Normal*" will put the output in a low state outside of switch-on periods and in a high state during switch-on periods ("active high"). Conversely, selecting "*Inverted*" will place the output in a high state outside of switch-on periods and in a low state during switch-on periods ("active low").

Single Shot

"**Single Shot**" mode generates a single pulse of defined length once per day. The time of day when the pulse is to be generated can be set via the "**Time**" value. The value "**Length**" allows the pulse length to be set in 10 ms increments and may be any value in the range of *10 ms* to *10000 ms* (10 seconds). Entries that are not multiples of 10 ms will be rounded down.

Cyclic Pulse

"**Cyclic Pulse**" mode is used to generate cyclically repeating pulses. The time between two pulses is defined, and this value must always be provided in hours, minutes, and seconds. It is important to note that the pulse train is always synchronized with 0:00.00 local time, so that the first pulse on any given day will always be output at midnight, and is repeated at the specified cycle interval henceforth. Thus, if a cycle duration of *2 s* is specified, this will result in pulses being triggered at 0:00.00, 0:00.02, 0:00.04 and so on. While it is possible to set any cycle time between 0 and 24 hours, these repetitions are usually only useful if the time between pulses is always the same. For example, if a cycle time of *1:45.00* is set, this will output pulses at intervals of 6300 seconds. However, between the last pulse of any given day and the pulse at midnight on the following day, there will be an interval of just 4500 seconds.

Pulse-per-Second, Pulse-per-Minute, Pulse-per-Hour

These three modes generate pulses of defined length once per second, once per minute, or once per hour respectively. The configuration options for all three modes are the same. The value "**Pulse Length**" specifies the length of the pulse and can be between *10 ms* and *10000 ms* (10 seconds).

DCF77 Marks

In "**DCF77 Marks**" mode the selected output simulates the time string transmitted by the German DCF77 time code transmitter. The output pulses 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.

DCF77-like M59

Sends a 500 ms pulse at the 59-second mark.

The "**Timeout**" field can be used to enter how many minutes the system should wait while in free-run mode before DCF77 simulation is suspended. Entering *0* here will disable the timeout function, so that the DCF77 simulation will continue running perpetually until manually disabled.

Position OK, Time Sync, All Sync

There are three different modes available for outputting the synchronization status of the clock. The "**Position OK**" mode outputs a signal whenever the GNSS receiver is receiving enough satellites to determine its position.

In "**Time Sync**" mode, a signal is only output as long as the clock's internal timebase is synchronized to the GNSS reference. The "**All Sync**" mode requires both of the above states to be true—for a signal to be passed through the output, there must be sufficient satellites for positioning, **and** the internal timebase must be synchronized to the reference constellation's timebase.

DCLS Timecode

DC level shift timecode. The timecode output here is configured in the "**Clock**" → "**IRIG Settings**" section of the Web Interface.

1 MHz Frequency, 5 MHz Frequency, 10 MHz Frequency

These modes are used to output a fixed frequency of 1, 5, or 10 MHz respectively, using a PPS signal as an absolute phase reference (i.e., the falling edge of the signal is synchronized with the rising edge of the PPS signal).

Synthesizer Frequency

This mode is used to output a custom frequency, which is defined using the "**Clock**" → "**Synthesizer**" section of the Web Interface.

Time Slots per Minute

This mode divides each minute up into a number of equal time slots, which can be individually enabled during those seconds of each minute. For example, if *six* time slots are selected, the user can set whether a signal should be output during the 0–10-second, 10–20 second, 20–30 second, 30–40 second, 40–50 second, and 50–60 second slots. If only the *10–20 second* slot is selected, a signal will only be output between 10 and 20 seconds of each minute and disabled outside of that.

PTTI 1PPS

This mode is used to pass a PPS signal of 20 μs pulse width through the output.

11.5 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
AUTOSAR	Multicast Slave	L2	0–15 (0)	P2P	n/a	n/a	7.8125–128000 ms (125 ms)	1000 ms	Y

11.6 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

12 List of Illustrations