Time & Frequency
Made in Germany Solutions

hopf unified management application

Customer Manual

COPYRIGHT © 1972 – 2025 *hopf* Elektronik GmbH
All rights reserved.

AUTOR: hopf - POSCH Markus
DOCUMENT: HOPF_HUMA_CUSTOMER-MANUAL_V1101_EN.DOCX
VERSION: v11.01
DATE: 17.12.2025

1 Table of Contents

2 Change History

VERSION	DATE	EDITOR	CHANGE DESCRIPTION
0100	08.03.2020	SCR	Document creation
0300	19.07.2023	POM	Adapted document for huma® version 03xx
0600	01.12.2023	POM	Adapted document for huma® version 06xx
0601	12.03.2024	POM	Added description for the following features: Trusted certificates Step when offset >= 100ms GNSS firewall RFC8915(NTS) Added more information on how to: Apply activation keys Generate signed configuration and update files Generate a device certificate (used for e.g. HTTPS)
0700	08.07.2024	POM	Adapted PTP time service and sync source description for the new implementation Adapted SYSLOG description for the new implementation Adapted SNMP description for the new implementation Added NTP time service time base description Added SINEC H1 page description
0800	29.10.2024	POM	Added description for the following new features: PTP v2.0 mode Leap seconds status information Set leap seconds action Firewall rules CIDR extension SIMEAS R option for DCF output

0900	14.03.2025	POM	Added description for the following new features: Capture network packets Configuration of minimum needed satellites with configurable C/N0 PTP advanced settings: Ignore UDP checksum Overwrite 0.0.0.0 source IP VLAN ID appending VLAN filter PTP over PRP with 2 instances SNMPv3 traps
1000	07.07.2025	POM	Correction of allowed characters for password Improved description for the following features: Freeze functionality NTP symmetric keys Added description for the following new features: Redirect HTTP to HTTPS Ping action Network interface enable / disable Network firewall alarm GNSS receiver jamming detection PTP accuracy clamping Switch relay permanent after device is started Added description for the following new status values: Network packet counters PTP status values
1101	01.12.2025	POM	Added description for the following new features: SINEC H1 correction value calculation (status byte 1) GNSS antenna velocity and height sections LED blinking for system and boards Performance section of boards with operation system GNSS Receiver debug SYSLOG port configuration

Unused configuration values for PTP as sync source have been removed

Peers section on NTP time service page has been removed

3 Preliminary Remarks

This software product is the result of an intensive effort by ***hopf*** to combine all its programs into a single unit called huma®. It is highly flexible, versatile and easy to use. huma® is based on components that are interchangeable throughout the application and rely on a unified design and functionality.

This document version is valid for huma® version **v1101**. You can check your huma® version on the login page, see chapter 6.1 Login

4 Requirements

The minimum requirement for the **huma®** Web edition is an **HTML5** browser with JavaScript enabled and a working connection to the ***hopf*** device.

The browser must support at least **ECMAScript 2016** (ES2016) for basic functionality and **CSS 3** for basic design.

Additionally, the browser technology "**Local Storage**" has to be activated with a minimum storage capacity of 1MB.

All modern browsers meet the previously explained requirements by default.

huma® has been tested and works best with Chromium based browsers (**Google Chrome** *(Version > 89)*, **Edge** *(Version > 89)*, **Opera** *(Version > 75)*, **Brave** *(Version > 1.23)*, ...) and **Mozilla Firefox** *(Version > 87)*. ***hopf*** does not grant (full) functionality on any other browser.

Edge Legacy (the major version of Edge prior to 2020) is not tested and therefore not recommended.

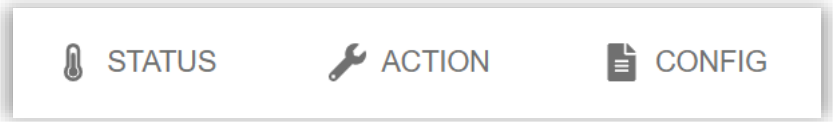
5 Handling

The main goal of huma® is to provide easy and safe interaction with a *hopf* device. To facilitate the handling almost every component has a **tooltip** (5.8) that becomes visible when the mouse is hovered over it.

As for security, this application is based on a system that uses a configuration file. A valid configuration file must follow a certain structure in order to be sent to the device and later understood by its internal software.

5.1 Basic Usage

In general, huma® consists of three types of pages (see 5.3.3.2):



- **Status**

  Pages that indicate status information without any user interaction.

- **Action**

  Pages that allow triggering actions on the device that **immediately take effect**.

- **Config**

  Pages that allow changing config values **in the browser but not on the device**.

  Changing a value and then pressing the "OK button" on such a page will not change the config value on the device immediately!

  For the changes to take effect on the device, a new config file must be generated and then uploaded. For more information on handling config pages please, see 5.4.

5.2 Security

For *hopf* Elektronik GmbH security has the highest priority. This is exactly why we have used a different approach for changing configuration values.

Changing configuration values directly through any web application carries many potential security risks, especially if the application is exposed to the internet. To avoid such risks, our software is built on a system based on entire config files. Instead of changing each specific value individually, which exposes numerous communication channels in the network, we have only one point where we exchange the configuration with the device.

This approach also enables us to implement another optional high security feature: "Signed Configs". *hopf* devices can be configured to allow only config files that are signed and validated to further enhance security.

The format of the config file is **JavaScript Object Notation** (JSON). The file structure resembles the basic device structure and its boards allocation.

5.2.1 Hardening Security

In order to harden the security, the following steps can be done:

1. Under 6.5.5.1.1, select either the **Medium** or **High** security profile, when signed config and update files should be used, select the corresponding public key under Advanced and Signature public key, otherwise turn off Signed config files required and Signed update files required.
2. Navigate to all Time Service Pages and activate/deactivate the desired Time Services (see 6.6.4)
3. Navigate to the Firewall Page of each network-capable device and add the activated Network Time Services as Allow rules (to see which rule should be added, hover over the toast "Firewall forbids activated service"; see 5.7.1)

5.2.2 Good Practice

The following list describes ways to increase the security of huma® and the device:

1. Use a predefined Security Profile (**Medium** or **High**)

   As described in 6.5.5.1 a profile will adjust many security settings automatically to values defined by the *hopf* security team. This includes also the firewalls from all boards.

   The profile **Medium** is purposely built for systems with high security needs and generally the recommended way to harden the security. **High** is used for special needs where the usage of huma® is highly restricted.

2. Keep the Firewalls restricted

   By default, there is a firewall rule that denies every network traffic. This rule has always the lowest priority and can be overruled by any additional rule. Don't add a rule that allow all services. Add only specific rules that are really necessary with only the interface, direction and protocol that are really needed for the service to work (not just **any** or **both**).

3. Turn off unused services

   Services that are not used (e.g., only HTTPS is used to access huma® and not HTTP) should not only be prohibited by the firewall, but generally turned off on the corresponding config page.

4. Configure Strong & Non-Default Passwords

   Ensure that all used passwords have suitably strong values. Passwords should have at least 10 characters and **should not** be common default passwords (like "admin" or "password")

   Furthermore, avoid using the same password across multiple devices.

5.3 General Layout

Most of the pages of huma® have a layout that consists of three main components.

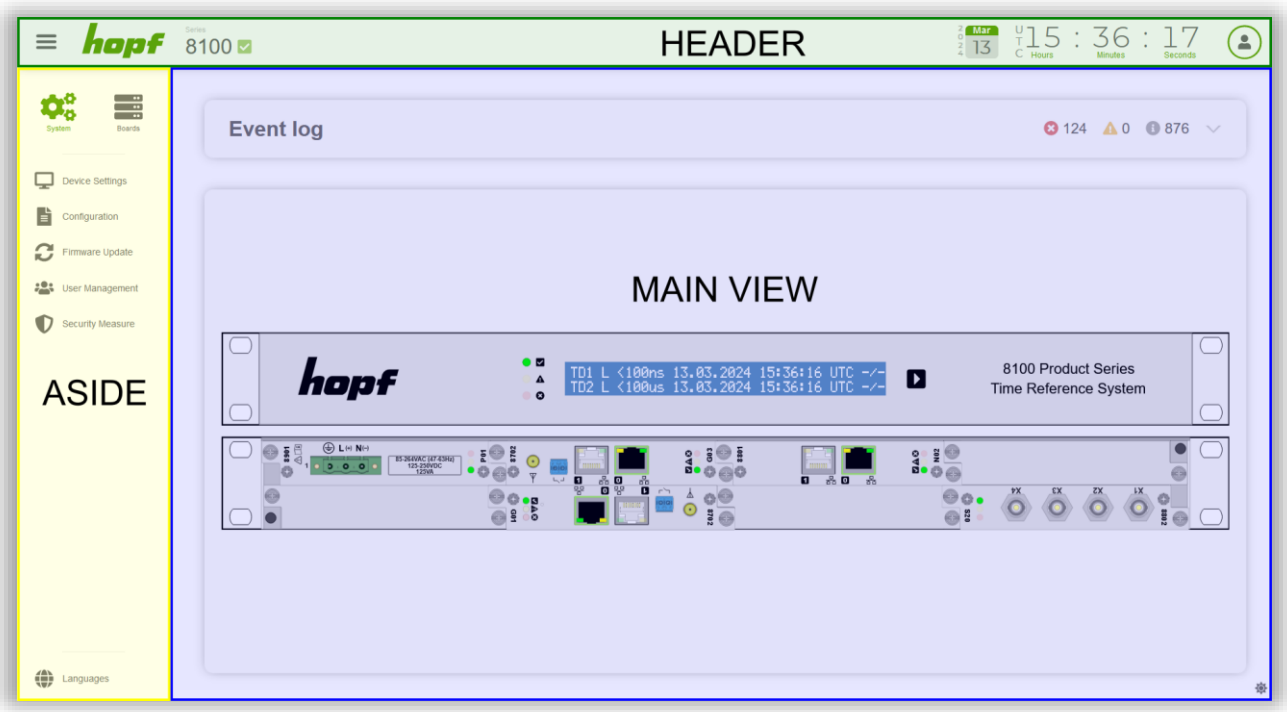


Figure 1 Screenshot visualizing the basic layout

5.3.1 Header

The header provides basic device information and functionalities that are always available to the user.

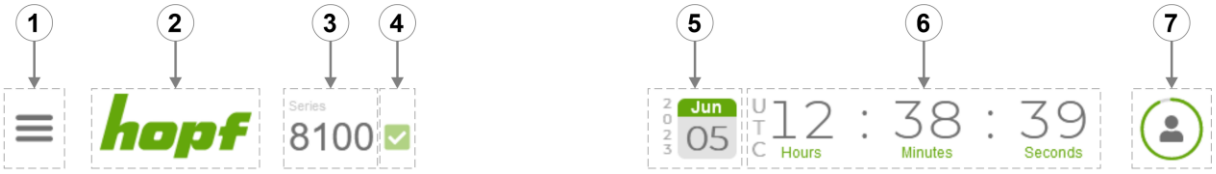
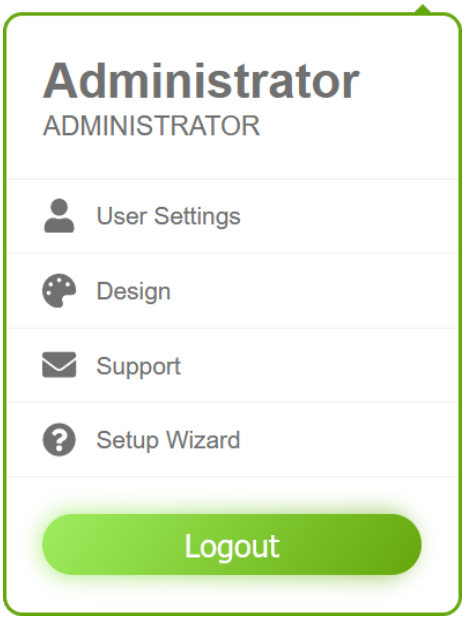


Figure 2 Components of the header

All components of the header are listed below starting from left.

	Label	Description
1	Aside Toggle Button	Pressing this button shows or hides the **ASIDE** menu (see 5.3.2).
2	Company Logo	This component not only represents the company logo, but also acts as a button that, when triggered, leads to the **start page** featuring the **event list** (see 6.2).
3	Product Series	The product series to which the device belongs. Hovering over this component will display a tooltip showing the hostname of the device.
4	System Status	A global status indicator of the entire device which also acts as a button that, when triggered, leads to the **start page** featuring the **event list** (see 6.2). The system status not only indicates the general status of the device itself, but also summarizes the status of its installed boards. Hovering over this component will display a tooltip showing all currently active events of the device.
5	Device Date Output	Accurately displays the current date of the device. The visualization may change slightly depending on the timezone and language setting. This component is optional and can be hidden completely or partially (only the year can be hidden) under 6.5.1.1.3.
6	Device Time Output	Accurately displays the current time of the device. The visualization may change slightly depending on the time settings from Device Settings (see 6.5.1.1.3) and language setting. The system time set in 6.6.4.2.2 is not displayed here.

7	User Menu	This component has two functionalities. It acts as a button and at the same time as an indicator. It indicates the time remaining before a logout occurs. This so called "Inactivity duration" can be changed under 6.5.5.1.1. It starts as a full circle and gets smaller every second, changing color to orange after 50 percent and to red in the last 15 percent until the circle disappears completely.  Pressing this button can either show or hide the user menu. The user menu consists (starting from the top) of the username, the role(s) the user obsess, a link to the user settings, a link to the design settings, a link to the support page, a link to the setup wizard page and a logout button. 

5.3.2 Aside Menu

The aside menu is responsible for the main navigation in huma®. It allows navigation to all system pages and board pages. It also provides the user with the ability to change the language on every page.

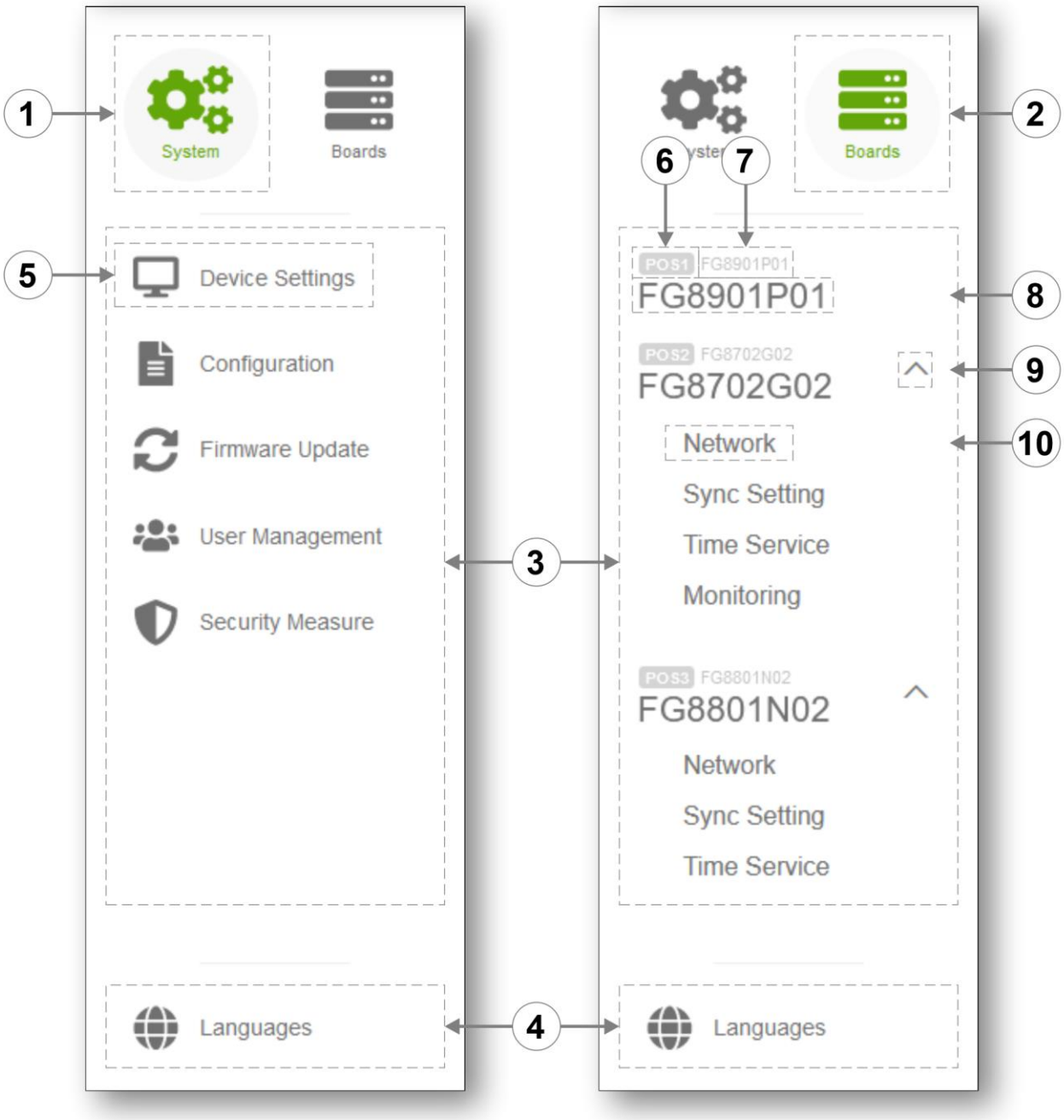
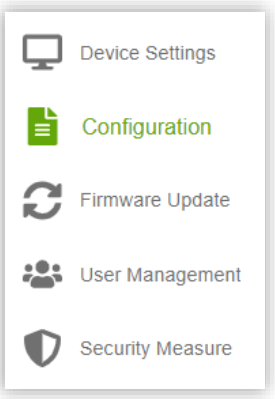
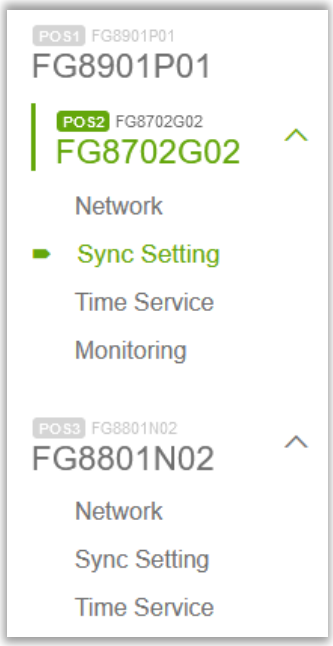
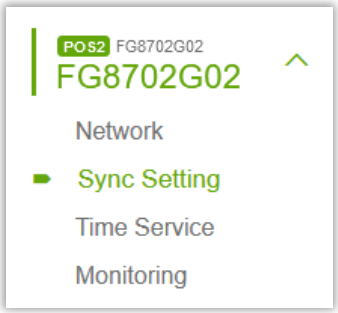


Figure 3 Both views of the aside menu

	Label	Description
1	System Menu Item	This menu item contains all system pages of the device. System pages affect the entire system and not just a specific board. They focus on management and maintenance of the system.
2	Boards Menu Item	This menu item contains all board pages of the device. Each board page takes care of an individual board which is inserted into the system.
3	Navigation List	The area that displays a list of all available navigations. The list switches dynamically between system pages and board pages depending on the selected menu item.
4	Language Selection	A language selection that is always available. Changing a language with this component does not have any effect on the device. It is just a localized setting that is stored in the browser and is not associated with the user.
5	System Page Link	Pressing a system page navigation link will lead to the desired system page. When the user is on a system page, the corresponding system page navigation link will be highlighted. 
6	Board Position	Shows the current position of a board in the device.
7	Product Name	Shows the product name of a board.
8	Board Name	This component displays the name of the board and also acts as a navigation link leading to the board's general status and action page. Hovering over this component reveals a tooltip with detailed status information about the board. The board name can be customized (see 6.6.1.1.3). When the user is on any board page, the corresponding board name (8), the board position (6), the product name (7) and the board subpages toggle button (9) will be highlighted.

		
9	Board Subpages Toggle Button	Pressing this button toggles the list of board subpage links (10). By default, the board subpage links are hidden. The button changes its orientation according to its state. 
10	Board Subpage Link	Pressing a board subpage link will lead to the desired board page. When the user is on any board page except Board Overview (see 6.6.1), the corresponding board page link (10) will be highlighted. Additionally, the board position (6), the product name (7), the board name (8) and the board subpages toggle button (9) are highlighted. 

5.3.2.1 Difference between System Pages and Board Pages

huma® is a unified user interface for all *hopf* products, this involves fully integrated and modular systems. This means that a fully integrated system also has the distinction between system and boards, even if there is only one physical device. The system pages are still used for system-wide management and maintenance, and the board page handles only the specific board functionalities and settings.

Fully integrated systems to which expansion devices are attached, are treated similarly to a modular system. The expansion devices will appear under the Boards Menu Item (similar to modules that are inserted into a modular system) where each one can be configured specifically.

5.3.3 Main View

The content of the main view area is dynamically adapted to the corresponding page the user is on. There are different use cases and functions for each page, which is why each page looks different. In general, a standard page consists of **sections** (see 5.3.3.3).

All board pages and system pages have the same navigation component in the main view. The navigation component consists of **Tabs** (see 5.3.3.1) and **Subtabs** (see 5.3.3.2).

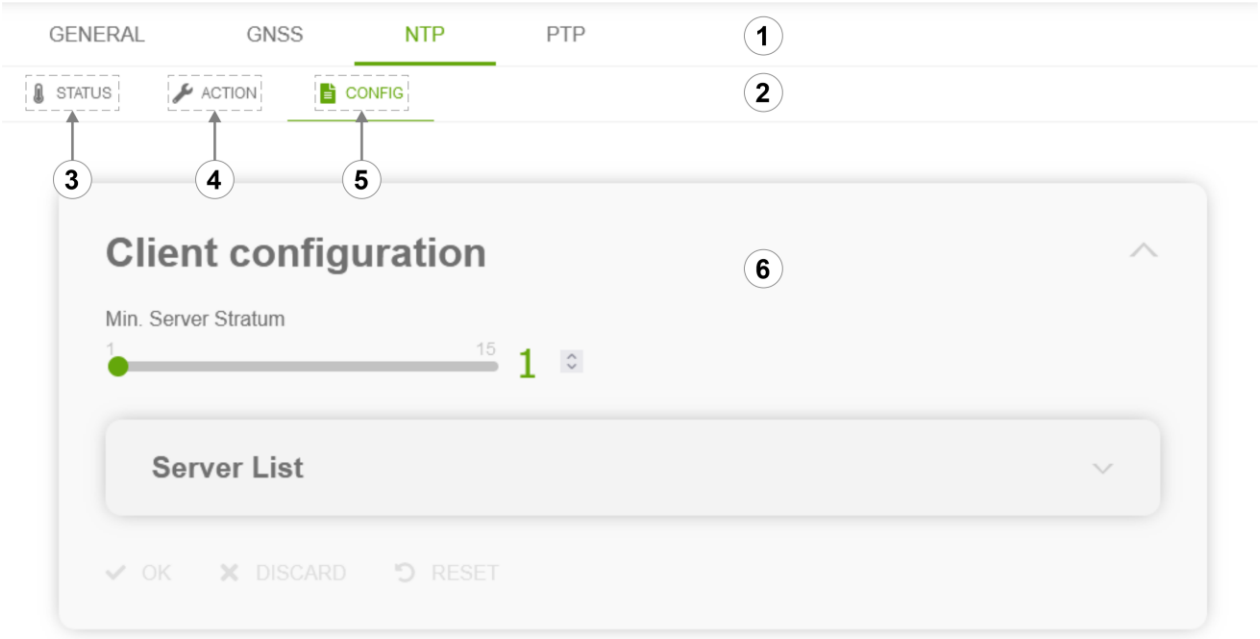


Figure 4 Navigation component and section under the board subpage "NTP"

5.3.3.1 Tab

A tab (1) is a navigation component that represents a specific category of a system or board page. It consists of **Subtabs**.

5.3.3.2 Subtab

A subtab (2) is a navigation component that represents a specific functionality of a **tab** of a system or board page.

There are three predefined Subtabs. A tab holds at least one out of three Subtabs:

5.3.3.2.1 Status

Pages that can be found under the Status subtab (3) primarily display status information of the device or certain services. This status information is always up to date, as they are automatically queried at periodic intervals.

5.3.3.2.2 Action

Action pages (4) contain the functionality to trigger events and actions on the device. These actions are immediate and change the device directly. An example of an action is the device reboot that immediately triggers a reboot of the device.

5.3.3.2.3 Config

Config pages (5) are the primary way to change a setting on a device. Unlike the action pages, the config pages do not interact directly with the device and changes only take place after the config upload. For more information on handling config pages please, see 5.4.

5.3.3.3 Section

A section (6) is a collection of components that have a similar purpose. They are visually placed in a box to distinguish them from other components with different purposes.

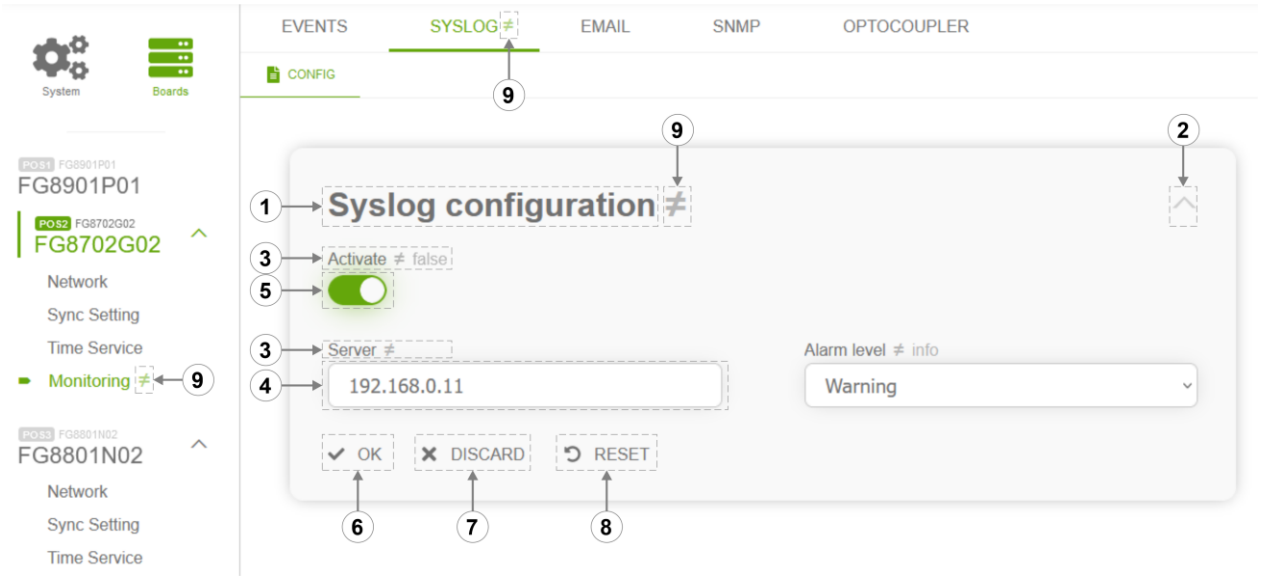
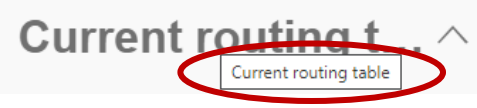
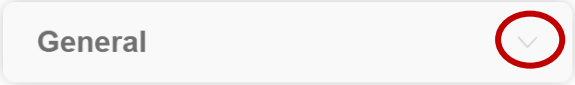
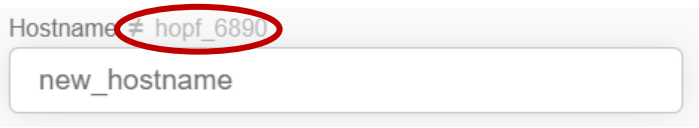
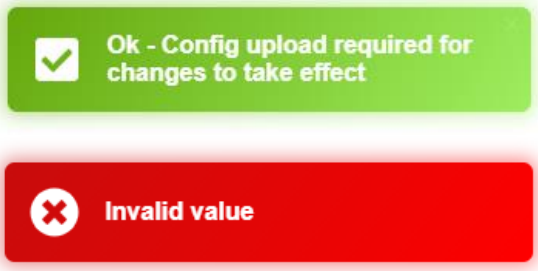


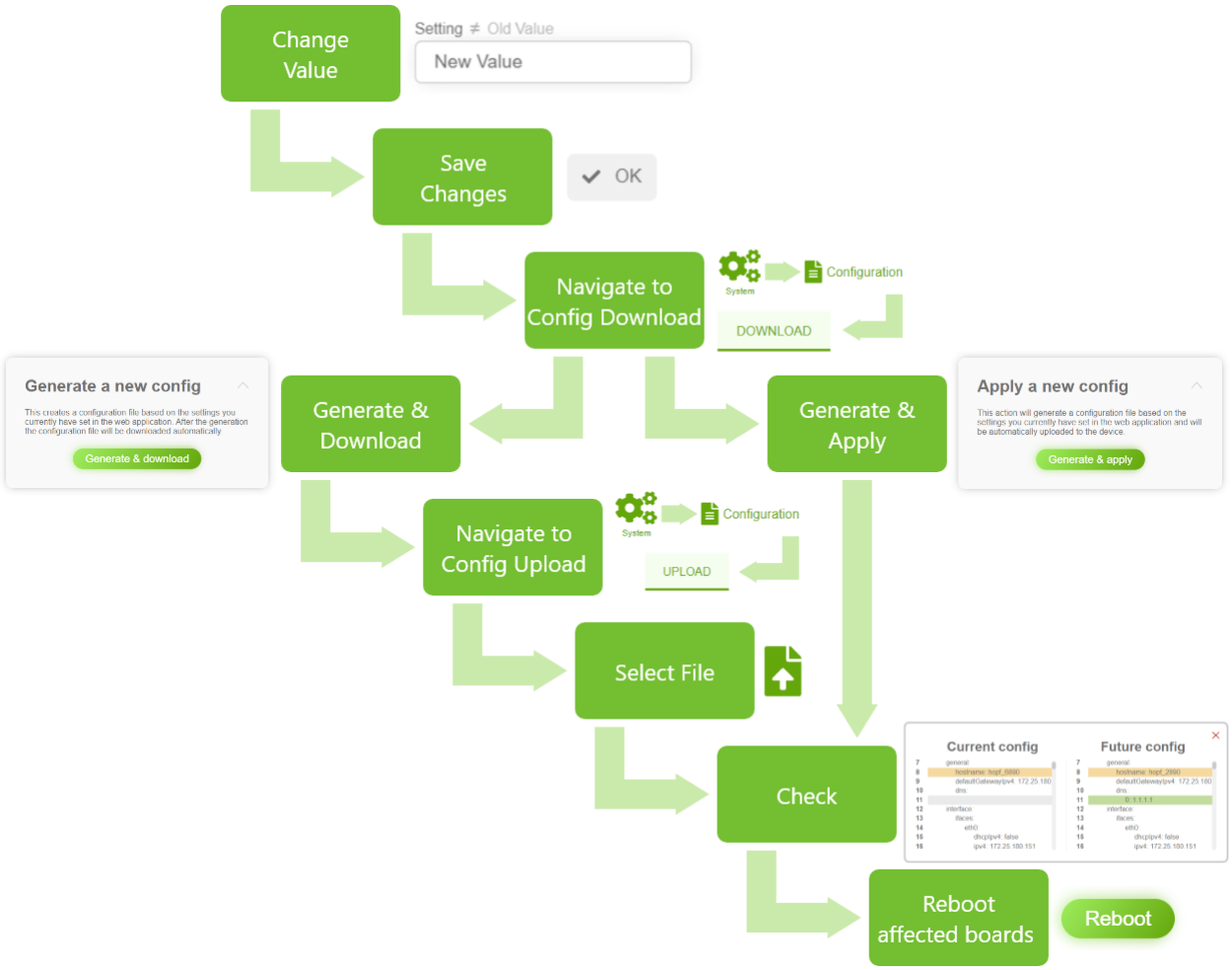
Figure 5 An example of a section that is placed under an config page

	Label	Description
1	Title	The title of a section. If the title text is too long, it will be truncated. To see the full title, move the mouse pointer over the title to display a small Browser-Quick Info. 
2	Collapse Button	This button either expands or hides the section. By default, the sections are expanded. The button changes its orientation according to its state. 
3	Label	A label is placed above an input or a status output. It describes the purpose of a subsequent field. A label is always provided with a tooltip, which can contain additional information such as the minimum or maximum values of an input field. The current setting of the device will be displayed next to the label of an input, if the input value differs from it. 

4	Input Field	An input field allows the user to enter data that can be used for various purposes. The entered data is immediately validated by the browser's input validation and also later on the server. If the entered data is invalid, the component is highlighted in red and can display an error message **provided by the browser**. Since the error message originates from the browser, the design of the error message and also the language depends on the used browser and its language settings.  Under config sections the input field is initially filled with the actual setting of the device.
5	Input On/Off Switch	This component allows the user to toggle a setting (either on or off). The value is set to **true** if the inner circle is placed on the **right** and the component has the accent color of the used theme as background (the accent color of "***hopf*** default" is **green**). The value is set to **false** if the inner circle is placed on the **left** and the component has a grey background color. 
6	Ok Button	This component is only available in sections under the config subtab. Pressing this button triggers a validation of all input fields of this section. If the inputs are valid, they are **temporarily** stored in the browser storage. **Pressing the OK button does not change any data on the device.** The current settings of the device stay the same. Only the values stored in the browser storage are replaced by the input field data of this section. Depending on whether the entered data is valid or invalid, a toast (see 5.7) is displayed containing a corresponding message **provided by huma®**.

		
7	Discard Button	This component is only available in sections under the config subtab. Input field values that have been changed by the user but **not** yet stored in the browser storage (by pressing the Ok button) will be rejected. In other words, it discards all entered values before they have been stored in the browser storage. **Pressing the Discard button does not change any data on the device.**
8	Reset Button	This component is only available in sections under the config subtab. It overrides the values of all input fields of a section with the actual settings of the device. **Pressing the Reset button does not change any data on the device.**
9	Value Changed	This component indicates that the settings of the browser storage differ to the settings on the device. The settings affect higher-level elements in the hierarchy. If the config value of an input field has changed, the section, the tab and the board subpage link will display the "Value Changed" component.

5.4 Change Device Configuration



To change the configuration of a device, the user must upload a complete configuration file. The configuration file can be changed and created with huma®. The following list describes the steps necessary to change device settings:

1. **Change the desired value(s)**
    a. Navigate to the "Config" Subtab (see 5.3.3.2.3) of the desired board or system page(s).
    b. Edit the input field value(s) of the section(s) that should be changed.
    c. Store the changed values in the browser storage by pressing the Ok Button of the section(s)

2. **Generate config file**

    a. After changing the desired value(s), navigate to the Config Download page (see 6.5.2.1.1)

    b. To generate a new config from the values that are stored in the browser storage, choose either **Generate a new config** or **Apply a new Config**.

    Generate a new config: Generates and automatically downloads a config file. This allows the user to sign this config file to further increase security and also allows the config to be duplicated to another device. Signed configs can be made mandatory under 6.5.5.1.1. The location of the downloaded file is depended on the browser (and its settings) and operating system.

    Apply a new config: Generates a config file and prepares the generated config file for an upload. The user is automatically navigated to the upload page. This option skips the user to **Step 3.c.**

3. **Upload generated config file**

    a. Navigate to the Config Upload Page (see 6.5.2.2.1)

    b. Upload the generated (and signed, if applicable) config file by Drag and Drop[1] or by opening the file explorer by clicking on the upload area and selecting it.

    c. After the upload, the user will be presented with an overview of all affected boards with all changed settings. After carefully checking and validating the changes, press **Apply config**.

    d. If the application of the config file was successful, the user must restart the affected boards in order for the settings to take effect.

[1] Drag and Drop is a pointing device gesture in which the user selects a virtual object by "grabbing" it and dragging it to a different location or onto another virtual object.

5.5 Status

There are two different ways to indicate a status in huma®. One way is a simple output of the status text and the other one is a status output with an icon to resemble the type of a status.

Simple status outputs always use the accent color of the used theme. The accent color of the default theme "*hopf* default" is **green**. The color does not have any meaning in a simple status output (**Green does not automatically mean Ok!**).

In contrast, status outputs with an icon use **four different colors** to resemble the type of status.

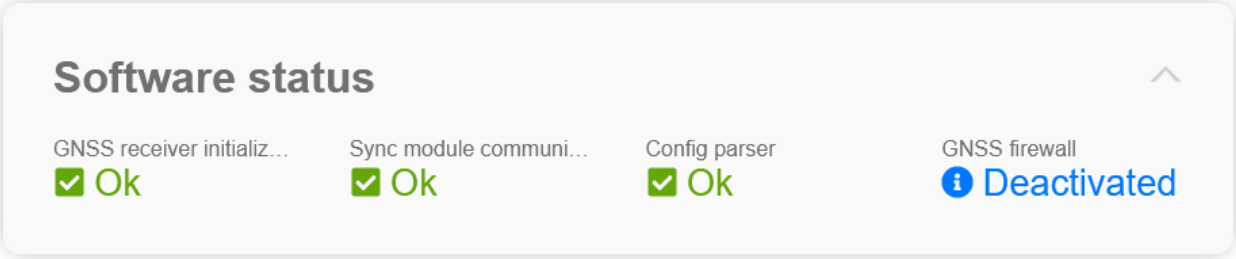


Figure 6 In this status section only the color of "GNSS firewall" bear a meaning

5.5.1 Colors

Color	Status Type
Green	Ok
Orange	Warn
Red	Error
Blue	Not initialized

5.6 Events

hopf devices can trigger different events. An event consists of two main components: the event code and the event type. The event code is a unique identifier for a particular event.

The event type categorizes an occurring event into a specific class. Depending on the event type, the visual representations of events change accordingly. There are four predefined event types for all occurring events: **error**, **warn**, **info** and **ignore**. For the event type **ignore** all visual components disappears completely (e.g., toasts, event log messages). The event type for an event can be changed under 6.6.5.1.1.

The user can setup certain monitoring services (e.g., Email) to receive an automatic notification about the event if the event type is even or higher a certain "Alarm Level".

For example, if the user sets the alarm level **warn** for email, the user will only receive a notification if the event type is **warn** or **error**. Events with the event type **info** or **ignore** will not be sent to the user.

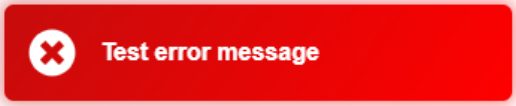
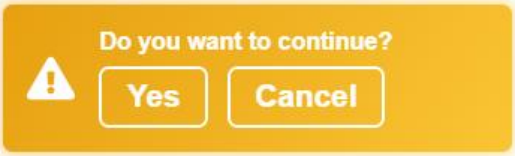
The event log on the start page (see 6.2.1) always contains a list of all occurred events (except events with the event type **ignore**).

5.7 Toast

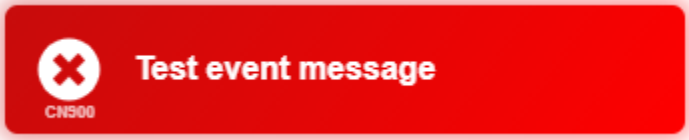
A toast is a visual message component that communicates certain events and information to the user without forcing them to react to this notification immediately, unlike conventional pop-up windows. By hovering over the toast, a close button will appear which allows removing the toast.

In general toasts are placed in the bottom right corner and are completely decoupled from the layout (exception are Main View Toasts; see 5.7.1).

A toast can not only visualize occurring events but also other information like user warning, timeouts or confirmation messages.

Toast Type	Description
info	 Info toasts use the accent color of the used theme. The accent color of the default theme "*hopf* default" is green. The color does not have any meaning in this specific toast (Green does not automatically mean Ok!).
success	
warn	
error	
timer	
confirm	

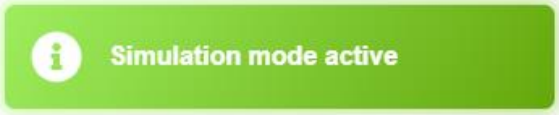
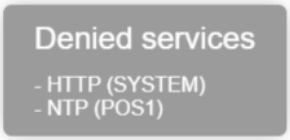
Toasts that visualize occurred events have the event code underneath the toast icon:



5.7.1 Main View Toasts

Main View Toasts are displayed on the upper right corner (underneath the header 5.3.1) inside of the Main View (see 5.3.3). They occur when an important status or setting is currently active.

The most important Main View Toasts are described in the following table:

Toast	Description
	Indicates that a firmware file is currently being uploaded to the device (see 6.5.3.1.1).
	Indicates that a firmware file is already uploaded to the device and fully validated, but a restart that will activate the firmware is missing. Under normal circumstances this toast **should not appear**.
	Indicates that the simulation mode is currently active (see 6.6.3.1.3; Synchronization sources).
	Indicates that a leap second adjustment will be made at the end of the day. The announcement originates from the sync source.
	Indicates that one or more activated services are forbidden due to a firewall rule. Adjust the firewall in order to fully enable a certain service. Hovering over this toast will reveal a tooltip indicating which services are forbidden and their exact position. 

5.8 Tooltip

A tooltip is a visual text box component that appears when hovering over another component. It holds information about that hovered component (such as a description of a button's function, or what an abbreviation stands for). The tooltip is displayed continuously as long as the user hovers over the component.

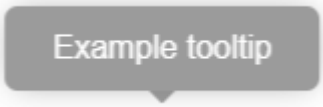


Figure 7 An example tooltip

The tooltip can change its content dynamically. It provides the user with much more details than just the component labels. It is highly recommended to hover over a component to learn more about its functionality or to find a more detailed explanation in case of misunderstanding.

Almost every text in huma® contains a tooltip. The same applies to input components, where not the input field itself, but its input label contains the tooltip.

Some components have two text boxes that appear when hovering over them: the tooltip, an huma®-specific component described here, and the Quick Info, which is provided by the browser. The Quick Info can appear when a text is cut off due to insufficient space. It then displays the full text of the component when hovering over. Unlike the tooltip with its huma®-specific design, the Quick Info design varies depending on the browser and operating system used.

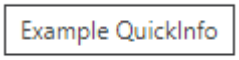


Figure 8 An example of a Quick Info in Google Chrome

5.9 Offline Capabilities

If the web application huma® loses the connection to the device, the application is still useable to a certain degree. The navigation to all pages is still possible, but all components of an action page are deactivated and status pages do not hold any status information.

A lost connection is indicated through multiple ways:

- A toast with the message **Server not reachable** (event code CN901) will appear
- A **Retry connecting** button will be placed next to the System Status (see 6.2.1; Component 4)
- Device Time Output (see 5.3.1; Component 6) will show **TIME NOT AVAILABLE**

Pressing the **Retry connecting** button will attempt to re-establish the connection to the device.

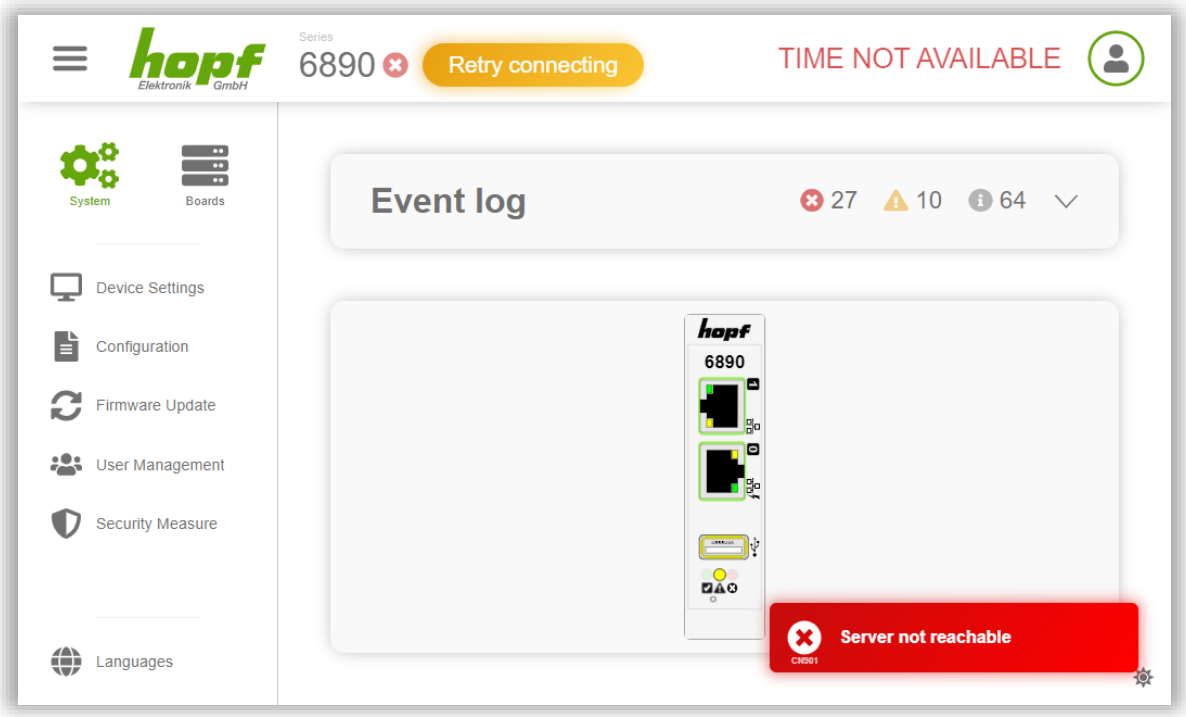


Figure 9 A screenshot of the start page with a lost connection

5.10 Customization

huma® is fully customizable. Among other things, the language, the entire theme, font and space sizes, and animation speed can be changed. All design settings are stored only in the browser storage. There is no interaction with the device. This also means that the settings are not linked to a user. All design changes are just saved in the currently used browser.

Most design adjustments can be made on the **design page** (see 6.4). The link to the design page is placed in the User Menu of the Header (see 5.3.1; Component 7).

Notice: The Design page (see 6.4) is different to the Config page of the Device Interface (see 6.5.1.1.3). The settings made on the Config page are the **initial design values** that each user will encounter when huma® is first launched in a browser. The settings that each user can make individually on the Design page always overrule the settings on the Config page.

5.10.1 Language

Multiple languages are supported natively in huma®. Changing the language not only changes the language of the texts themselves, but also the used formats (for example dates and currencies). The language selection can be found at the bottom left **on all pages**.

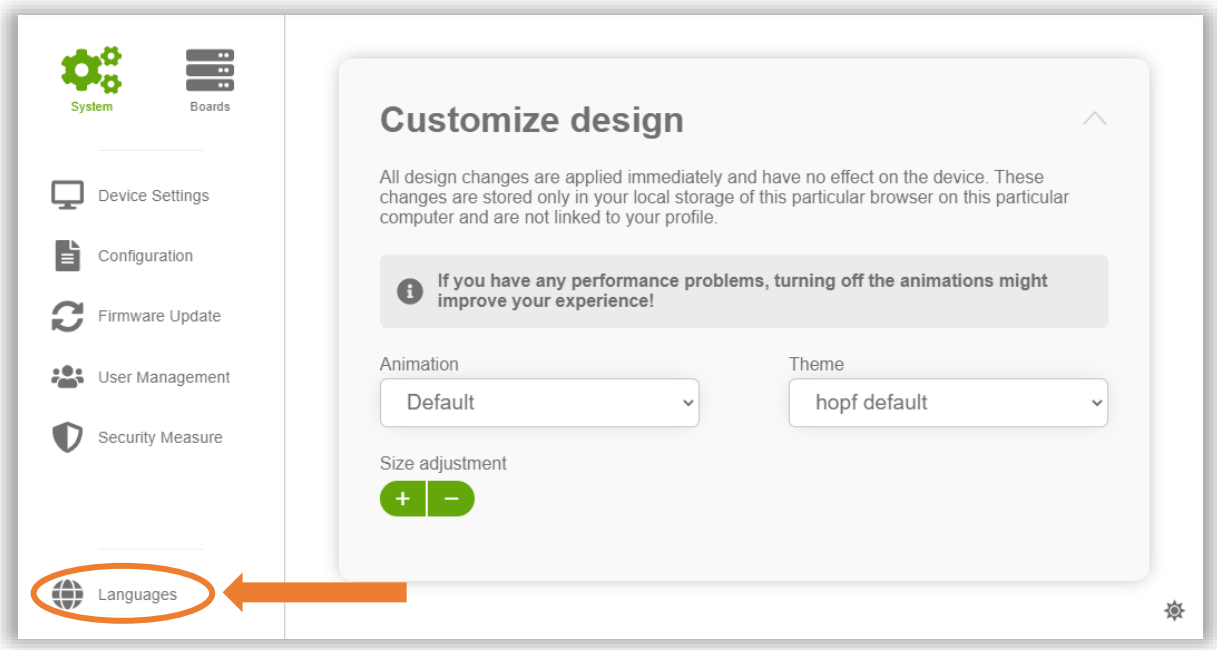


Figure 10 The language selection in the bottom left corner

huma® supports by default **British English** (en-GB) and **German** (de). The German and British English language pack uses the **24-hour time system**.

The language and its (time) formats do not influence the device in any way. It only changes the visual representation of the data coming from the device.

5.10.2 Themes and Dark Mode

The design of huma® with all its components is based on customizable themes. The standard theme is called "*hopf* default". Other themes are also made available for people with visual impairments. Switching to a different theme can be done on the design page with a select component labelled "Theme".

Every theme has a light and a dark variant. This allows easy switching between the light mode and the dark mode for each theme with just one click.

The button for switching between light and dark mode is located in the bottom right corner on **all pages**.

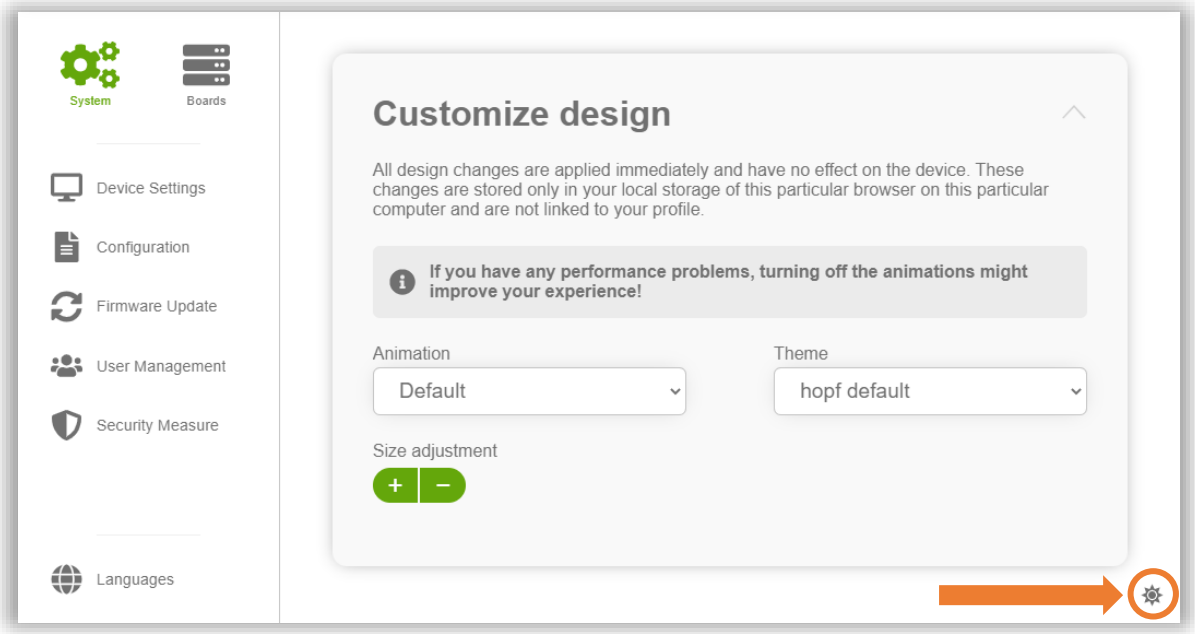


Figure 11 The dark mode switcher on the bottom right corner

5.10.3 Animation

huma® features a series of discreet and short animations that provide a more pleasant user experience and ease of use. The speed of these animations is also adjustable under the design page. Furthermore, it can be turned off altogether.

It is recommended to turn off the animation if the used computer has very limited hardware capabilities and/or the animations are jerky as well as in case of general performance problems.

5.10.4 Font and Space Size

The design page includes a component (labelled "Size adjustment") to adjust the default size of all fonts and spaces (e.g., between components). Pressing the plus button increases the sizes and pressing the minus button decreases them.

This feature is primarily important for a browser who does not offer adjustable zoom levels. In addition, resizing with this component instead of the browser zoom offers the advantage of a controlled flow in an environment where layouts and sizes are always displayed correctly. This cannot be guaranteed with the browser zoom, so resizing with this component is recommended.

6 Pages

All pages that can be found in huma® are explained in detail in this chapter.

The technical documentation of each *hopf* product lists all supported huma® pages.

Most pages are based on the general layout. The common components of the general layout will not be explained here; instead, the information can be found in chapter 5.3.

6.1 Login

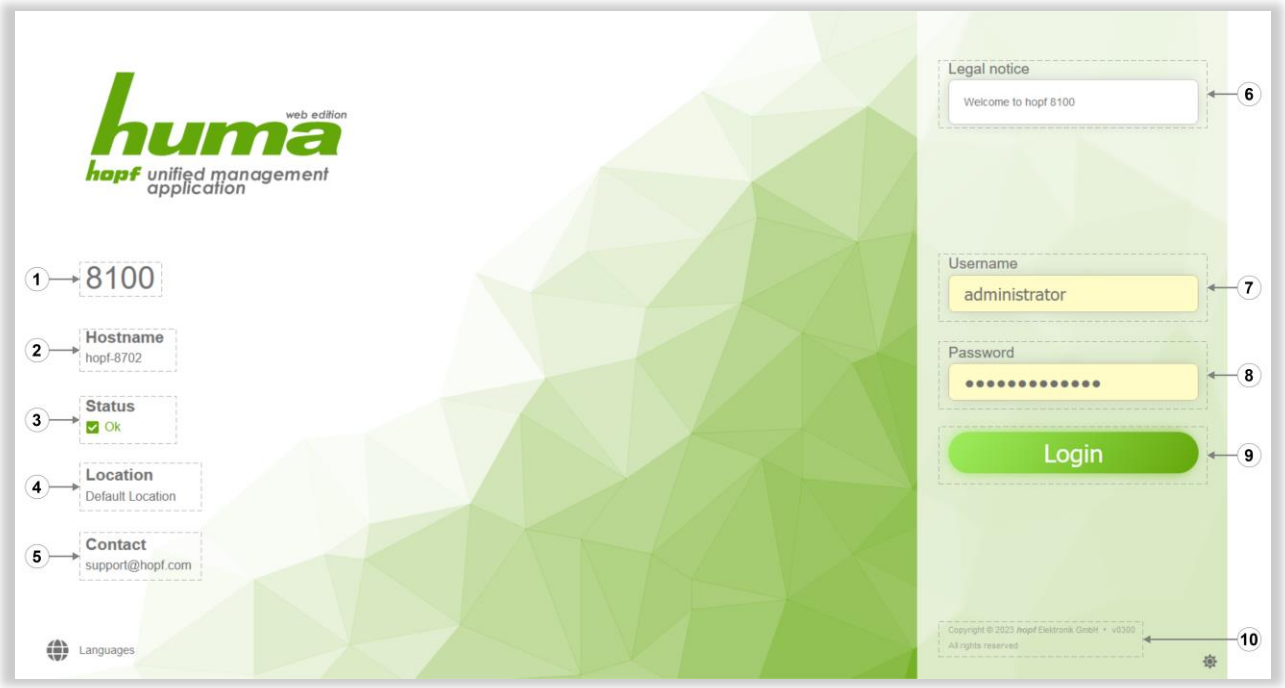


Figure 12 Login page with activated public status and banner

The login page is built in its own layout. A possible status section is placed on the left and the actual login section on the right. The status section is only available if the **public status** setting has been explicitly enabled in the config. Otherwise, the communication channel for status will be completely closed. This setting can be changed under 6.5.5.1.1.

	Label	Description
1	Product Series	The product series to which the device belongs.
2	Hostname	The currently set host name of the device. This is a config value and can be changed (after config upload) under 6.6.2.1.1.
3	System Status	It represents the same status as in the header (see 5.3.1; Component 4). The system status not only indicates the general status of the device itself, but also summarizes the status of its installed boards. If the device is running flawlessly, but one of its boards has an error, the system status will be at least "warn" or even "error".
4	Device Location	The location, specified in the config, where the device is situated. This is a config value and can be changed (after config upload) under 6.5.1.1.3.
5	Contact Information	The contact information is specified in the config. This is a config value and can be changed (after config upload) under 6.5.1.1.3.
6	Banner	The banner is specified in the config. Its main purpose is to present customizable information to the user. The information text is encoded in UTF-8. This is a config value and can be changed (after config upload) under 6.5.1.1.3.
7	Username Input	The username input accepts only alphanumeric inputs. The number of characters has to be between 3 and 20.
8	Password Input	The password input accepts maximal 100 characters.

9	Login Button	Pressing the login button will attempt to log the user in with the specified credentials from the username (7) and password (8) input. In case of a successful login, the user will be normally[2] redirected to the start page. If the login is unsuccessful, a toast with an error message is displayed.  After several failed login attempts, the user is prohibited from making further attempts for a certain period of time. Configuration details about the cooldown can be found under 6.5.5.1.1. 
10	Additional Information	In this component additional information can be found, such as the huma® version 

[2] Navigating to a specific page from the browser address bar without the user being logged in will redirect the user to the login page. After a successful login, the user will be brought to the previously entered page instead of the start page. After factory default the user will be brought to the Setup wizard page until he clicks the Finish setup button on the Setup wizard page.

6.2 Start Page

The start page contains essential information about the device. One of the most important components on this page is the **event log**. There is also a component that visualizes the entire device, including live (status) information and also interaction options.

The start page can be reached in several ways. After the login, the user will be forwarded to this page by default. Additionally, clicking on the components **Company logo** or **Device status** in the header (see 5.3.1; Component 3 and 4) leads to the start page.

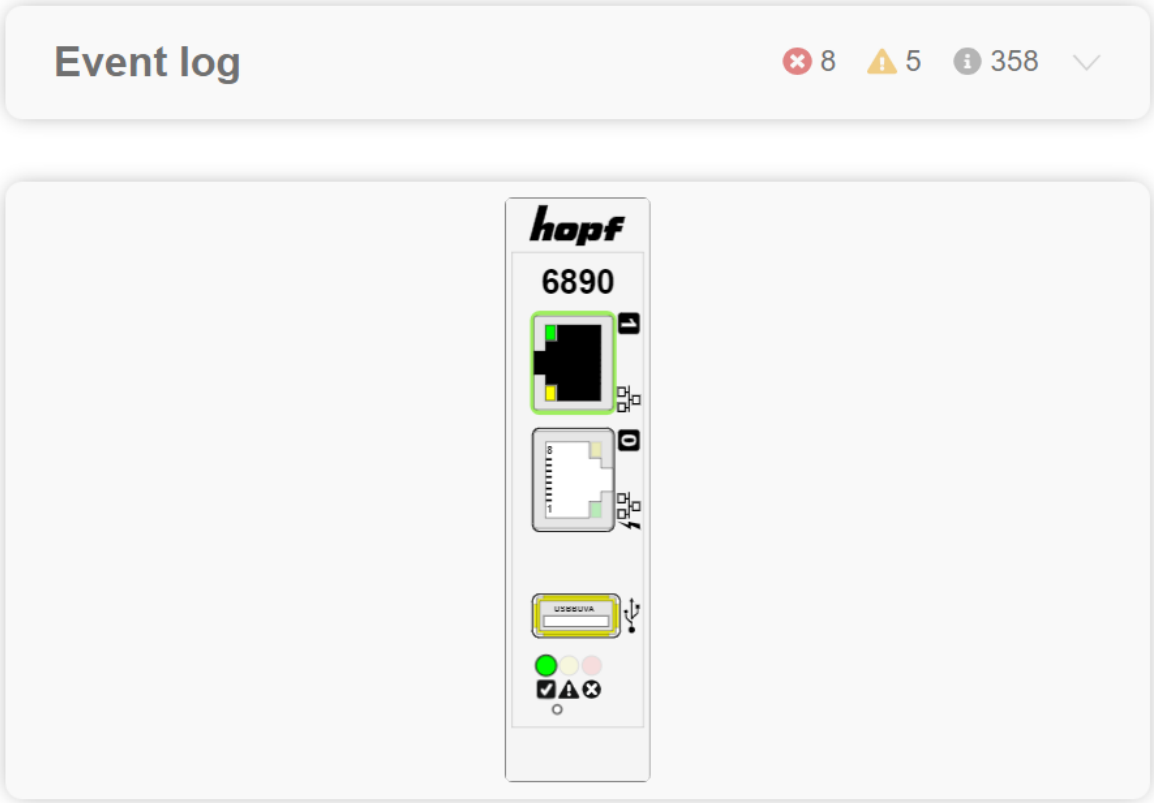


Figure 13 Start Page of device 6890

6.2.1 Event Log

The event log is a list containing all occurred events, which can be filtered and modified.

By default, this component is collapsed and the device view is expanded. However, an event preview always shows how many events have occurred for each type. Disabling the **collapse event log** setting in the config reverses this behaviour (see 6.5.1.1.3).

The event date is in the format **DD/MM/YYYY** in English language an **DD.MM.YYYY** in German language.

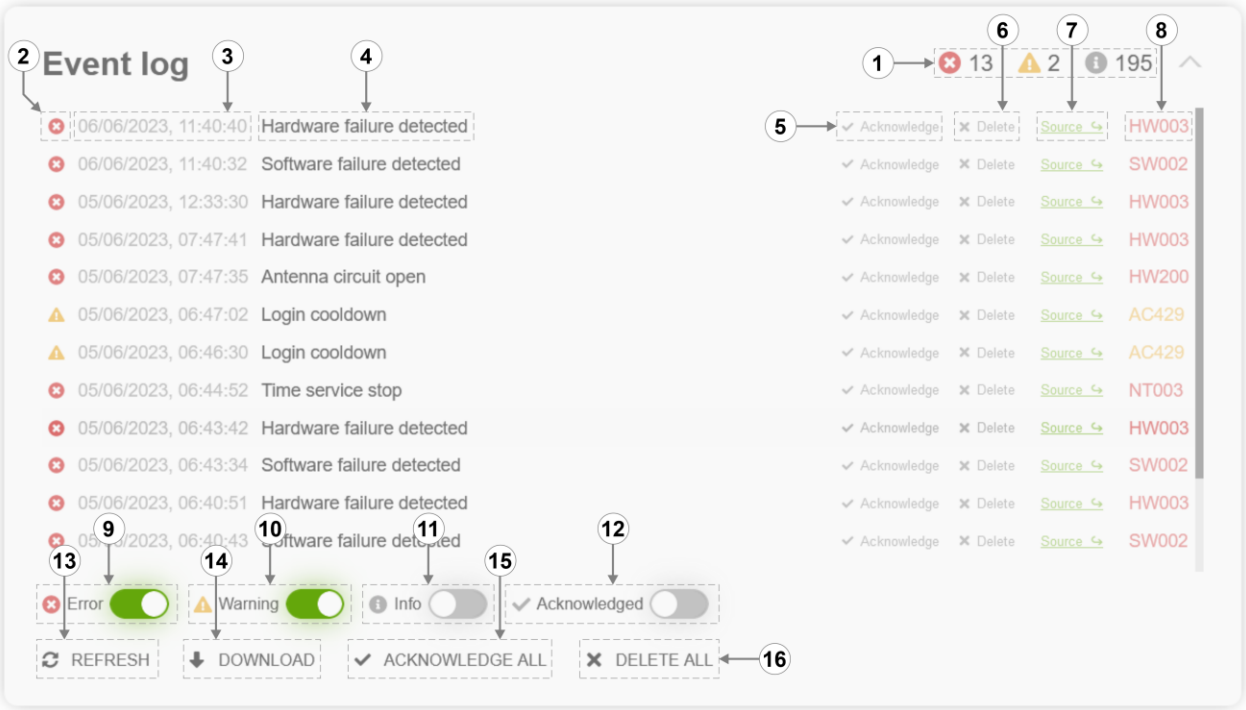


Figure 14 Expanded event log with Info and Acknowledged filter disabled

	Label	Description
1	Event Preview	The event preview shows how many events have occurred for each type. It is displayed in both collapsed and expanded states.
2	Event Type	The event type of a certain event.
3	Event Timestamp	The timestamp indicates exactly when a certain event occurred. The visualization may change slightly depending on the timezone and language setting.
4	Event Message	The event message explains a certain event in the language set by the user.
5	Acknowledge Button	Pressing this button will acknowledge a certain event. Acknowledged events can be filtered out so that the user only encounters events that have not yet been seen.

6	Delete Button	Pressing this button will delete a certain event from the event list.
7	Source Link	Each event has an originating source. This link leads to the position where the event occurred.
8	Event Code	The event code of a certain event.
9	Error Filter	Filter for all events with event type "error".
10	Warning Filter	Filter for all events with event type "warn".
11	Info Filter	Filter for all events with event type "info".
12	Acknowledge Filter	Filter for all events that are already acknowledged.
13	Refresh Button	Refreshes the event list.
14	Download Button	Downloads the event list. The downloaded event list is in CSV format.
15	Acknowledge All Button	Pressing this button acknowledges all events that have not yet been acknowledged.
16	Delete All Button	Pressing this button will delete all events from the event list.

6.2.2 Device View

The device view shows the current state of the *hopf* device virtually in huma®. This component is not just a static image, but highly dynamic. For example, the activated status LEDs light up, the text on the screens corresponds to reality and the arrangement of the boards is displayed correctly. Additionally, most parts of the image have tooltips with detailed information and the boards are clickable, which takes the user to the appropriate board status page.

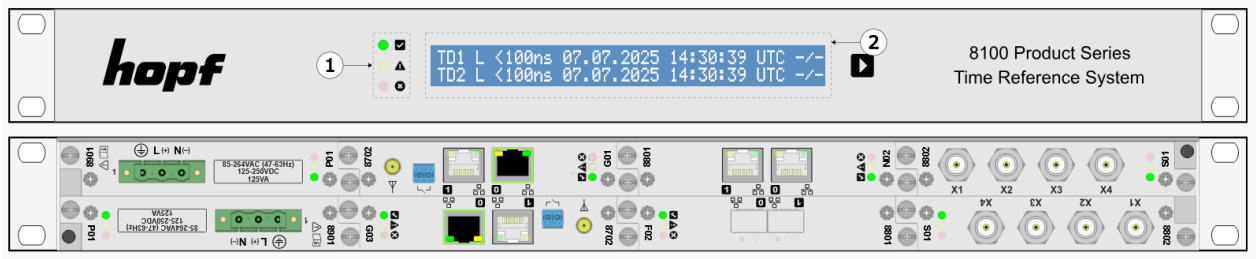


Figure 15 The Device View from device 8100 with five boards installed

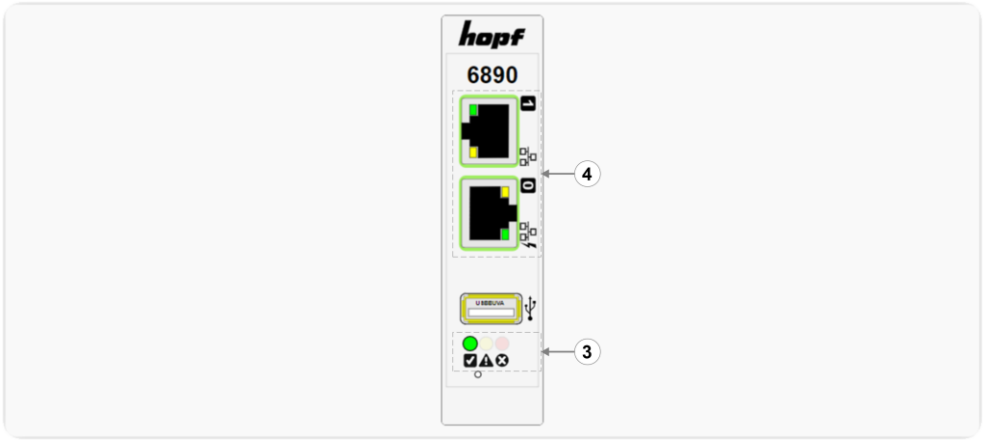


Figure 16 The Device View from device 6890

Since every *hopf* device is different, only the components that are common to the product portfolio are explained here:

	Label	Description
1	System Status LED	Devices that can accommodate multiple boards in their physical unit are equipped with a System Status LED. It consists of three different LEDs. The colors are defined under 5.5.1. It represents the same status as in the header (see 5.3.1; Component 4)
2	Info Display	This component mirrors the text on the physical device's display exactly as it appears.

3	Board Status LED	Devices that have status LEDs and cannot accommodate multiple boards are equipped with a Board Status LED. It consists of three different LEDs. The colors are defined under 5.5.1. It represents the same status as in the board status page (see 6.6.1.1.1)
4	Network Interface Indicator	Depending on whether an interface is Up or Down, the representation is changed.

6.3 User Settings Page

The User Settings Page can be reached by pressing the corresponding link in the User Menu (see 5.3.1; Component 7). This page consists of the section "Change password" and "Local storage".

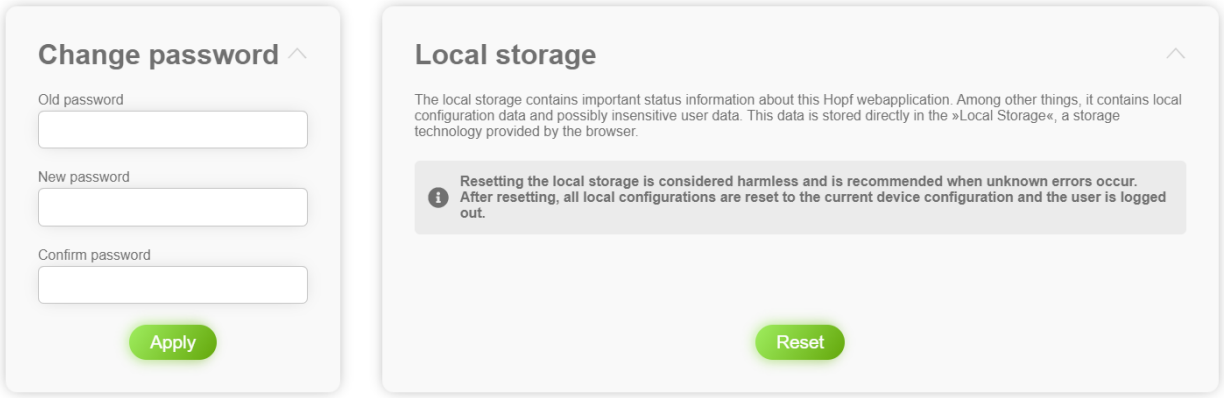


Figure 17 User Settings Page

The "Change password" section is only available if the user is logged in with the Login Method "Local Device" (see 6.5.4.3.1). The user can change their own password there.

Changing the password requires entering the old password and the new password. In addition, the new password must be entered twice to ensure correct entry.

Only alphanumeric and following characters are accepted when entering the password:

_ - * ! / = ? [ ] .

The number of characters has to be between 6 and 20.

The "Local storage" section is concerned about the browser storage. All values stored in the browser, such as config values currently set by the user (but not uploaded) and non-sensitive user data, can be reset under the "Local storage" section. It is recommended to reset the local storage in case of unknown errors.

6.4 Design Page

The Design Page can be reached by pressing the corresponding link in the User Menu (see 5.3.1; Component 7).

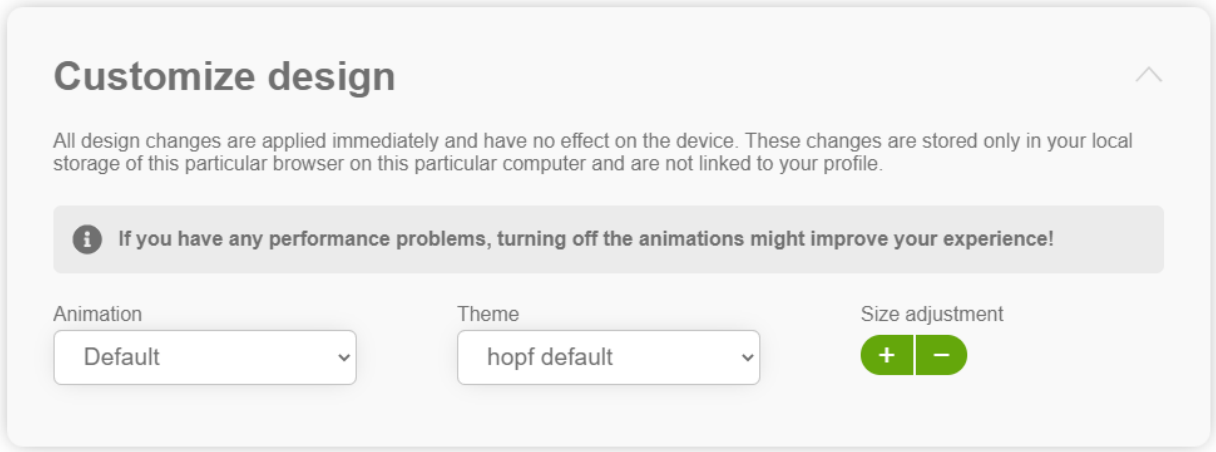


Figure 18 Design Page

Various design changes can be made on the Design Page with its three customization components.

The initial values of all the components on this page originate from the config settings, set on the Device Settings general config page (see 6.5.1.1.3).

All settings on this page are stored only in the browser storage and overrule the initially set values. There is no interaction with the device. This also means that the settings are not linked to a user. All design changes are saved in the currently used browser.

For example, if a user changes the theme in Google Chrome and then uses Mozilla Firefox, the user will encounter the default theme and not the theme set in Google Chrome.

Input Label	**Description**
Animation	Off – Animation is turned off Slow – Animation duration: 0.5 seconds Default – Animation duration: 0.3 seconds Fast – Animation duration: 0.16 seconds
Theme	***hopf*** default – Default colors are white, gray and ***hopf*** green Color blind – All colors from "***hopf*** default" are adapted for users with Protanopia or Deuteranopia

	Color blind (Monochromacy) – All colors from "*hopf* default" are adapted for users with Monochromacy High contrast – Gray colors from "*hopf* default" are changed to black colors to increase contrast
Size adjustment	The default size value (for font and space size) is 10, which is equivalent to 1rem or 16 pixels. Min: 5 (= 0.5rem = 8 pixel) Max: 50 (= 5rem = 80 pixel)

6.5 System Pages

This chapter describes all pages that can be found in the aside menu under the System menu item (see 5.3.2; Component 1). **All those pages have in common that they concern the whole system and not only a specific board.**

6.5.1 Device Settings

The "Device Settings" summarizes all pages with basic (system-wide) device functions.

6.5.1.1 General

This tab contains pages that cover system-wide status information, reboots and resets as well as configuration settings.

6.5.1.1.1 Status

This page provides a section with all system status information and a section with the Device View (see 6.2.2). Clicking on a board in the Device View will lead to the status page of the board (see 6.6.1.1.1).

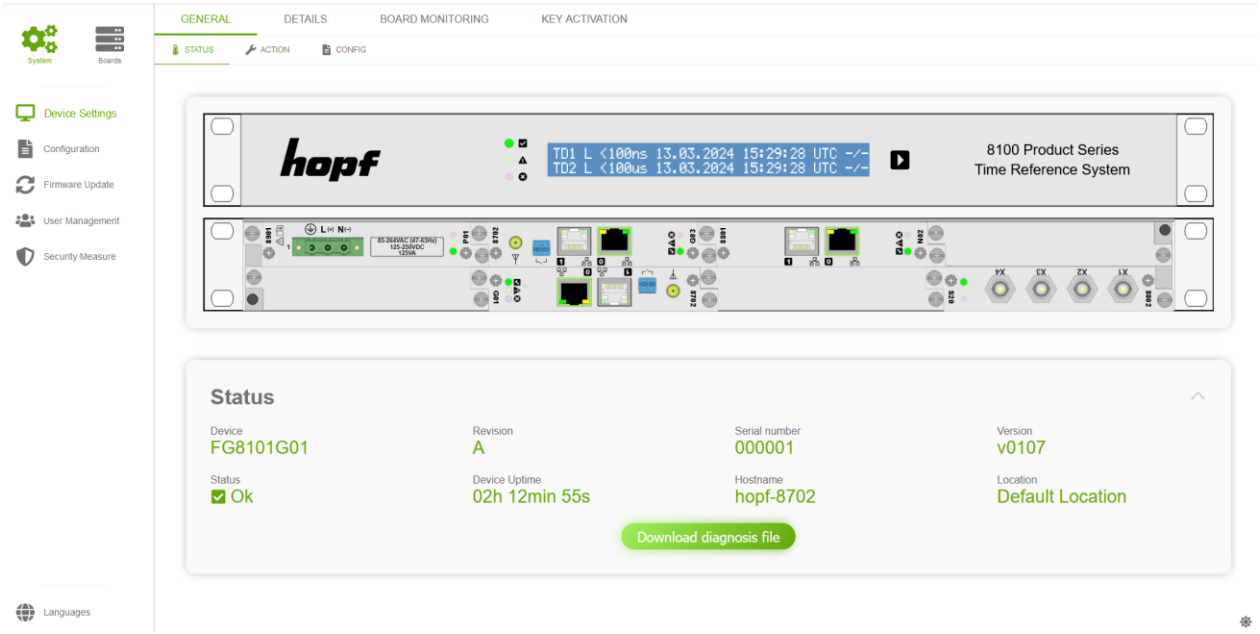


Figure 19 A screenshot of the status page of device 8101

Status Label	Description
Device	The exact product name.
Revision	Hardware device revision
Serial number	The serial number of the device.
Version	The version of the system software of the device.
Status	It represents the same status as in the header (see 5.3.1; Component 4). The system status not only indicates the general status of the device itself, but also summarizes the status of its installed boards. If the device is running flawlessly, but one of its boards has an error, the system status will be at least "warn" or even "error".
Device Uptime	Indicates how long the device has been in operation since the last restart.
Hostname	The currently set host name of the device. This is a config value and can be changed (after config upload) under 6.6.2.1.3.
Location	The location, specified in the config, where the device is situated. This is a config value which can be changed (after config upload) under 6.5.1.1.3.
Download diagnosis file	Pressing this button will download a diagnostic file that will assist the *hopf* service team in finding specific errors on the device. The downloaded file includes the logs of the entire system (all boards).

6.5.1.1.2 Action

On this action page, the entire device with all its boards can be rebooted or reset to factory settings.

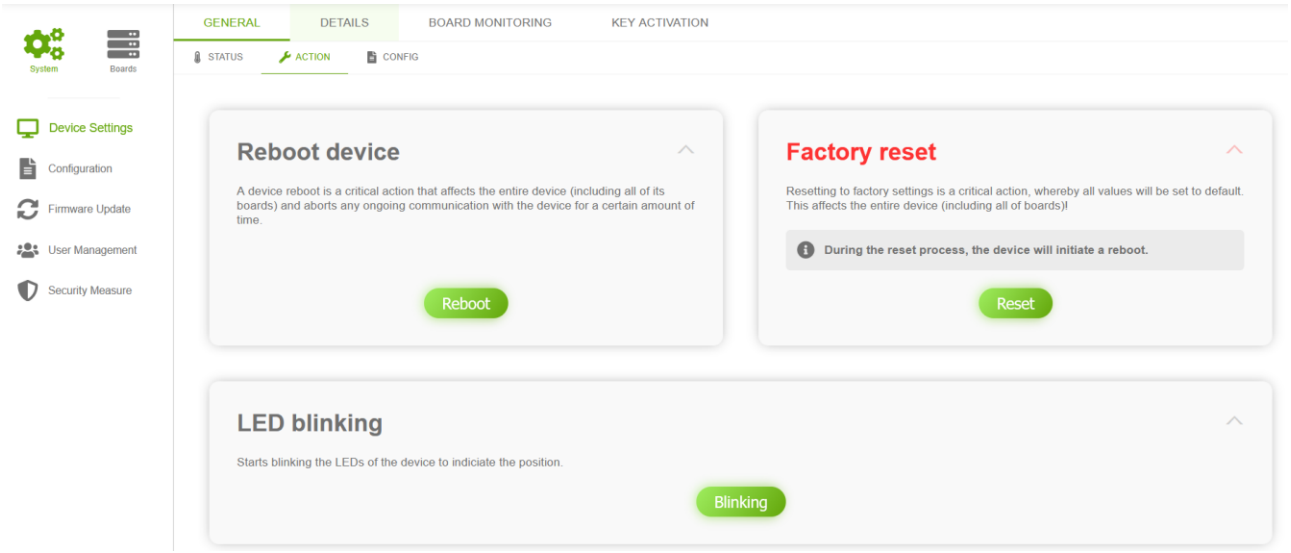


Figure 20 Action page of the general device settings

With the Blinking button in the LED blinking section, you can send a trigger to the device, to start a blinking sequence on its front panel LEDs. This section is only available if the device has LEDs on its front panel.

6.5.1.1.3 Config

The default huma® interface settings can be changed on this config page.

The design-related settings on this page define the **initial design values** that each user will encounter when huma® is first launched in a browser. The settings that each user can make individually on the Design page (see 6.4) always overrule the settings on this page.

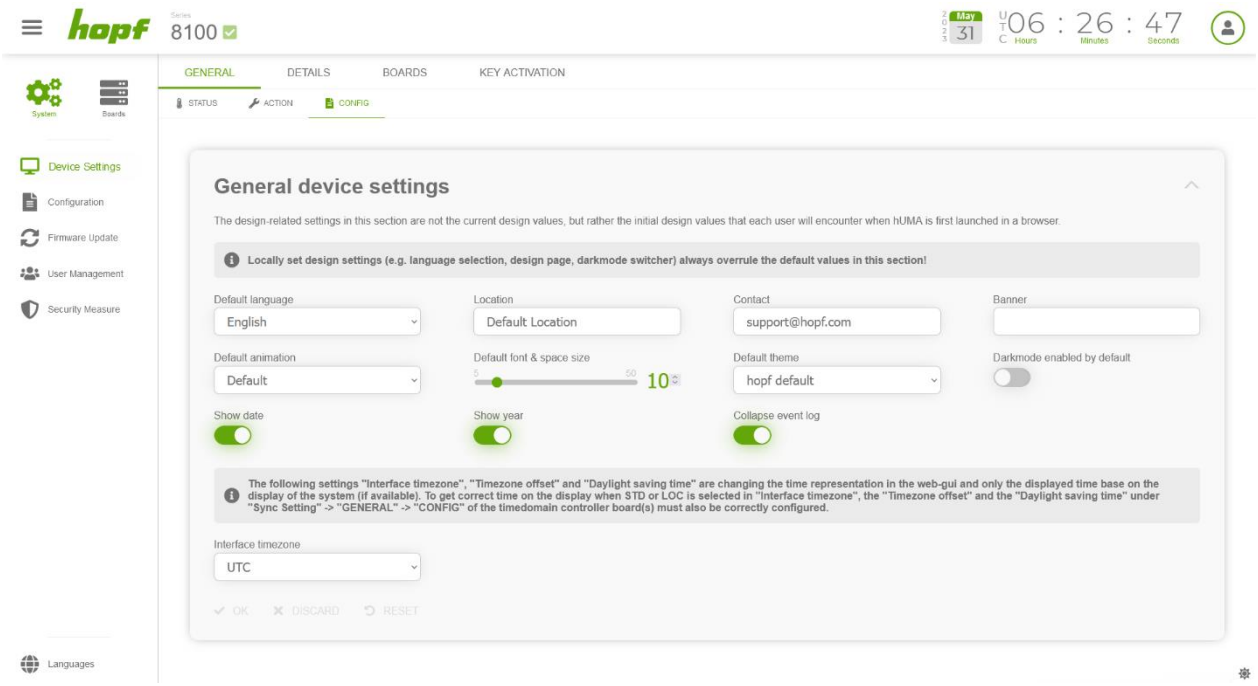
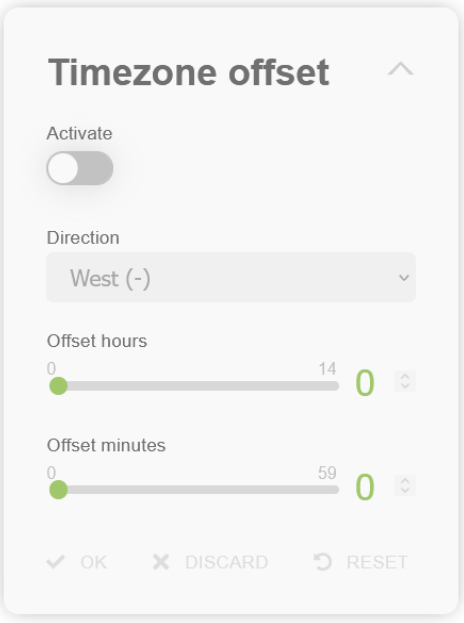
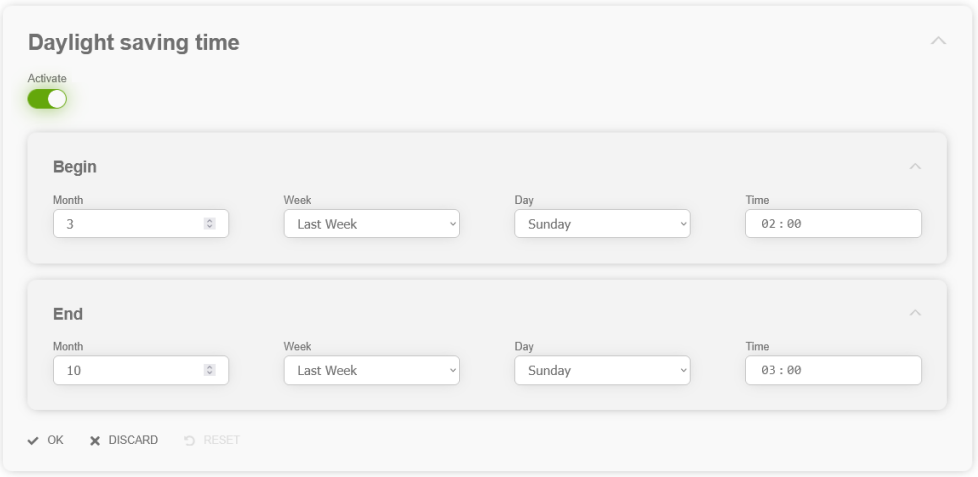


Figure 21 Config page of the general device settings

Input Label	Description
Device language	This setting changes the default language of the device. The language selection component will use the default language as its **initial value**. Every user can still change the initial value (default language) to a personally preferred language without affecting the device.
Location	The location where the device is situated can be set here. It is displayed on the login page and is used as a value for the SNMP object "syslocation" (OID: 1.3.6.1.2.1.1.6)
Contact	The contact information can be set here. It is displayed on the login page and is used as a value for the SNMP object "syscontact" (OID: 1.3.6.1.2.1.1.4)
Banner	The banner is displayed on the login page. Its main purpose is to present customizable information to the user. The information text is encoded in UTF-8. If it is empty the banner is not displayed on the login page.
Default animation	This setting changes the default speed of all animations. For more information on the individual speed levels, see the "Animation" component in 6.4.

	This setting is used as the **initial value** for the "Animation" component on the Design Page (see 6.4).
Default space & font size	This setting changes the default sizes of the huma® webpage and its components. The default value 10 is the optimal value for Full HD devices. Resizing is recommended if the majority of company devices are not Full HD devices. This setting is used as the **initial value** for the "Size adjustment" component on the Design Page (see 6.4).
Default theme	This setting changes the default theme of the device. This setting is used as the **initial value** for the "Theme" component on the Design Page (see 6.4).
Darkmode enabled by default	This setting specifies whether the dark mode is activated by default. The dark mode switcher (see 5.10.2) will use the default language as its **initial value**.
Show date	Specify whether the month and day from the device time should be displayed in the header (see 5.3.1; Component 5).
Show year	Specify whether the year from the device time should be displayed in the header (see 5.3.1; Component 5). This setting can only be enabled if "Show date" is enabled.
Collapse event log	Specify whether the event log on the start page should be collapsed by default (see 6.2.1).
Interface timezone	This setting changes all times and dates displayed in huma®. The change only alters the visual representation of the data coming from the device and has no effect on how the device generates its time outputs. Activating the timezone STD will reveal the "Timezone offset" section. In this section the timezone offset can be configured for the time that is shown in huma®. This is only visually and has no influence on the device time. 

	If LOC is enabled, the "Daylight saving time" section is displayed in addition to the "Timezone offset" section. In this section the daylight-saving time can be configured for the time that is shown in huma®. This is only visually and has no influence on the device time. The LOC time must be set in the time input field. 

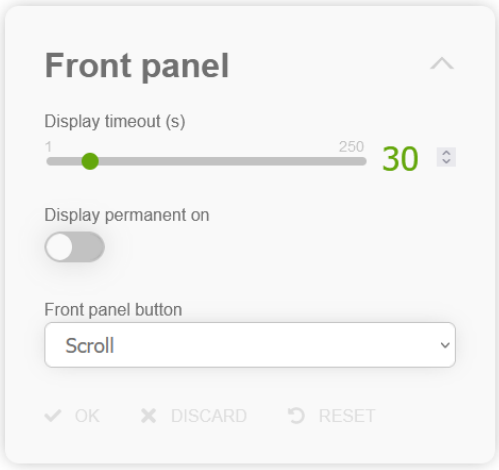


Figure 22 front panel settings

The front panel section is only visible for systems with a display on their front panel and it allows to configure the display and the front panel button behaviour.

Input Label	**Description**
Display timeout (s)	This value is the amount of time that the display is active after a press of the front panel button, when "Display permanent on" is disabled.
Display permanent on	When disabled, the display enters the standby mode, when the display timeout expires since the last press of the front panel button.

	When enabled, the display does not enter the standby mode after the timeout. Hint: initially the display starts in the standby mode, the front panel button must be pressed at least once to activate the display.
Front panel button	The functionality of a long press of the front panel button can be configured here. **Scroll**: when the button is pressed for more than 500ms, the display scrolls to the next page **On/Off**: when the button is pressed for more than 500ms, the display enters the standby mode, if it was active

6.5.1.2 Details

Pages whose main purpose is to display detailed status information of the system.

6.5.1.2.1 Status

The "System details" section shows detailed status information of the system. Its content is product specific, so it can vary from product to product.

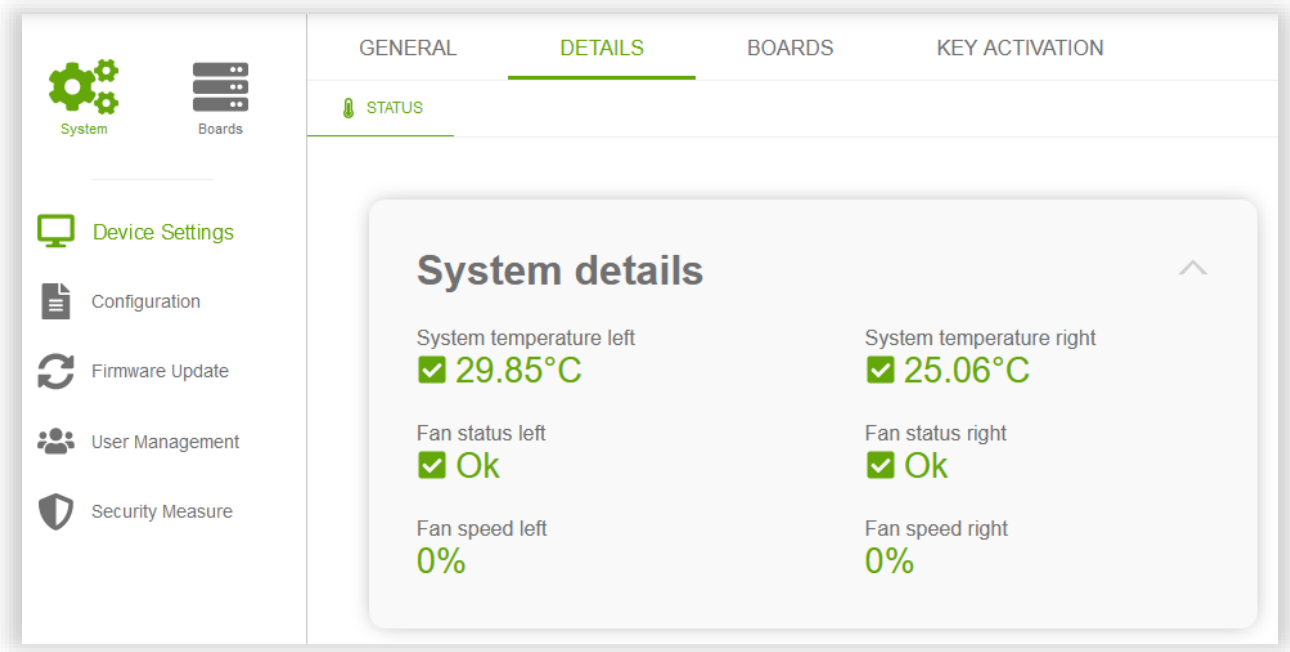


Figure 23 An example of a system details section

6.5.1.3 Board Monitoring

Page whose main purpose is to manage the board monitoring functionality.

6.5.1.3.1 Config

There are two sections on this configuration page. The section "Board monitoring" contains a drop down, for each position of the system. These drop downs enable the monitoring functionality for each position. E.g., when a FG8803S02 should be monitored on POS 3, select the corresponding article number in the drop down for POS 3. When no board or a board with another article number is detected in POS 3, the system will enter the error state. If a position should not be monitored select "-" for that position.

The second section displays the system, with an overlay that shows the positions, article numbers and configured names of all equipped board.

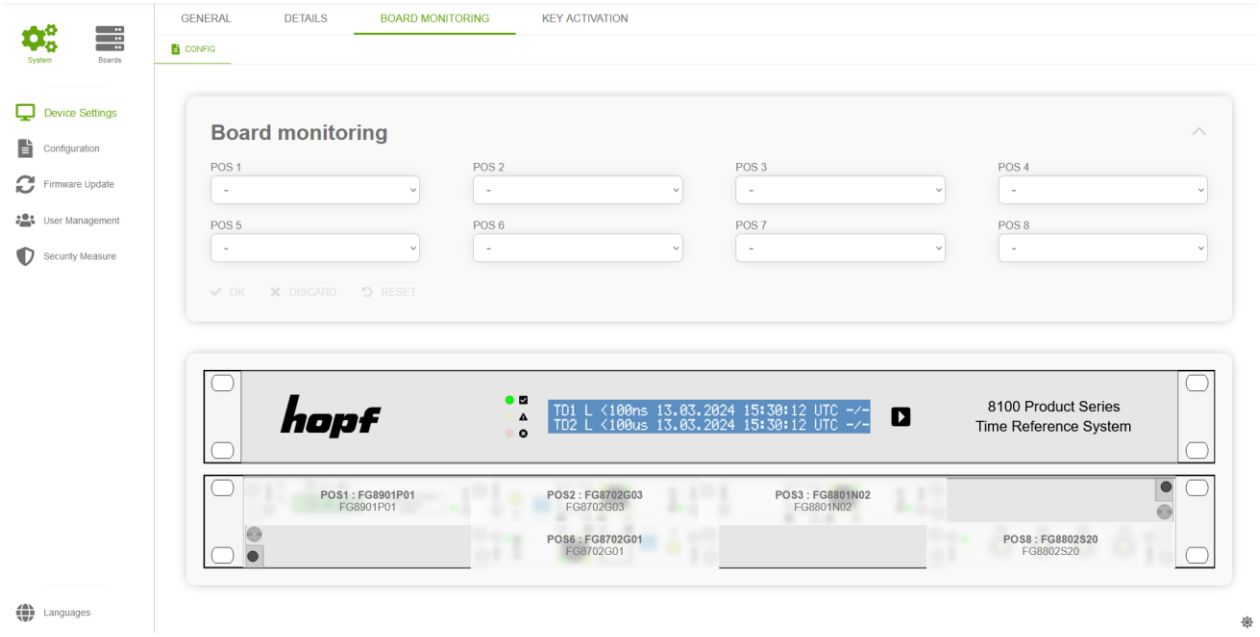


Figure 24 This config page has a device view to visualize the board names

6.5.1.4 Key Activation

Everything concerning features and their activation keys can be found here.

A feature is a product extension that can be purchased to significantly enhance the functionality of the device. After a purchase the obtained activation key must be entered under the action page to unlock the functionality.

6.5.1.4.1 Status

This status page lists all of the activated features on the device.

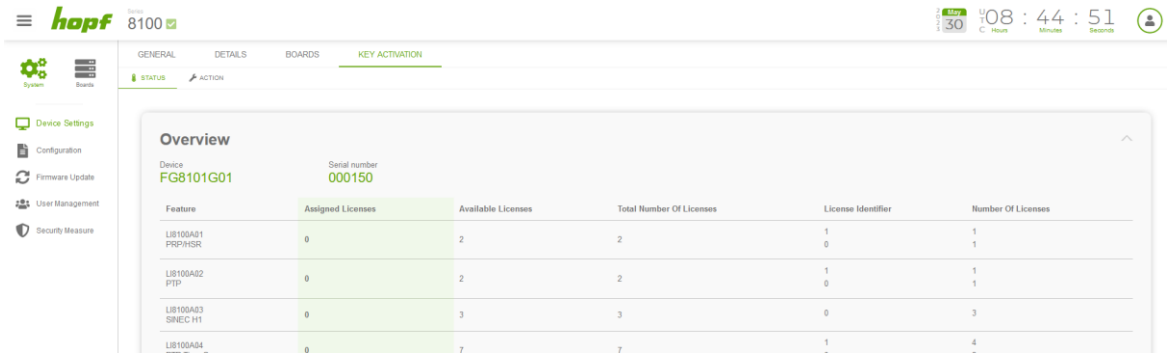


Figure 25 An example of the activation key status page

Table Column Label	Description
Feature	The feature name.
Assigned Licenses	Indicates how many of the "Total Number Of Licenses" of a feature are assigned to a board.
Available Licenses	Indicates how many of the "Total Number Of Licenses" of a feature are not assigned to a board.
Total Number Of Licenses	Specifies how many feature-unlocks are made available by all activation keys for the given feature. An activation key does not necessarily mean only one feature unlock, instead an activation key could unlock a feature more than once. For example, one activation key can unlock a feature three times, so "Total Number Of Licenses" would indicate the number three.
License Identifier	Licenses for the same feature on the same device are distinguished via the License Identifier. It can be used to check if a specific activation key has already been applied on the system
Number Of Licenses	Specifies how many feature-unlocks are made available by the activation key with this License Identifier.

6.5.1.4.2 Action

On this page keys can be activated, fully reset and assigned.

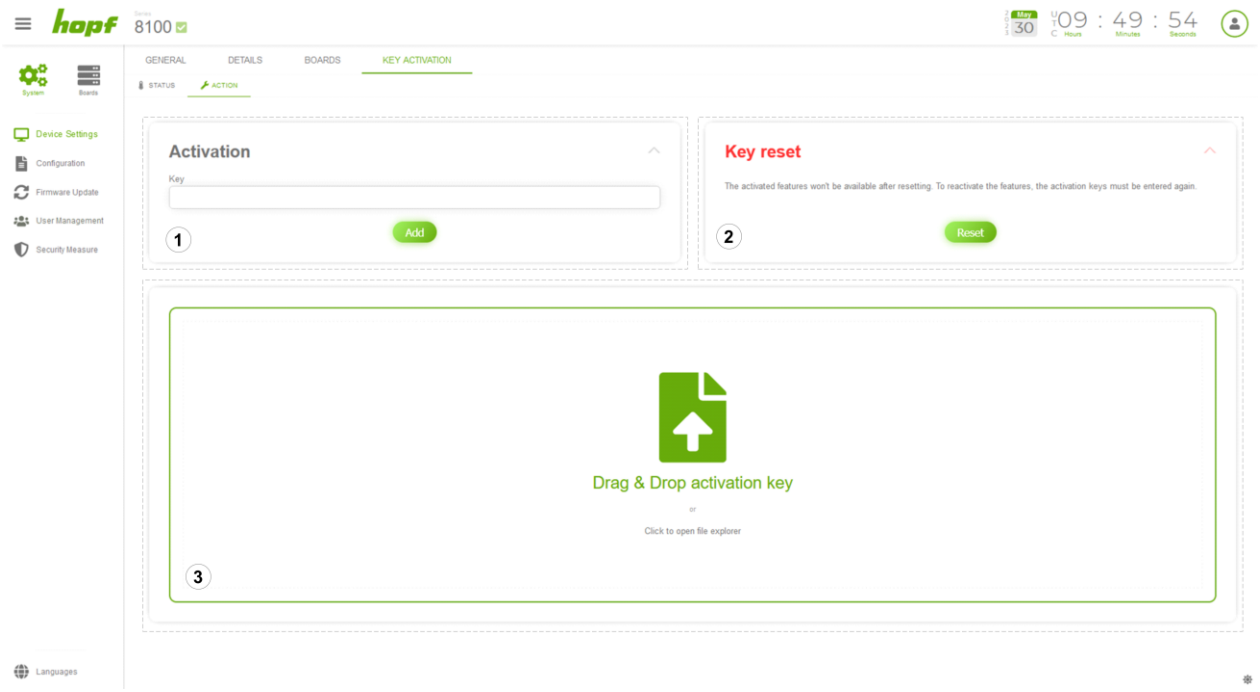


Figure 26 This screenshot illustrates the key assignment process

	Label	Description
1	Activation	The user has to enter a valid activation key that was purchased from ***hopf*** Elektronik GmbH. The activation key is Base64 coded.
2	Key reset	A key reset removes all activated activation keys from the device. The activation keys do not lose their validity after the key reset. They can still be re-entered and are fully functional.
3	Drag & Drop activation key	Instead of entering the activation key manually or via scanner to the Activation text field, the PDF file of the activation key can be added via drag and drop or by opening the file explorer by clicking on this area and selecting it.

Applying an activation key:

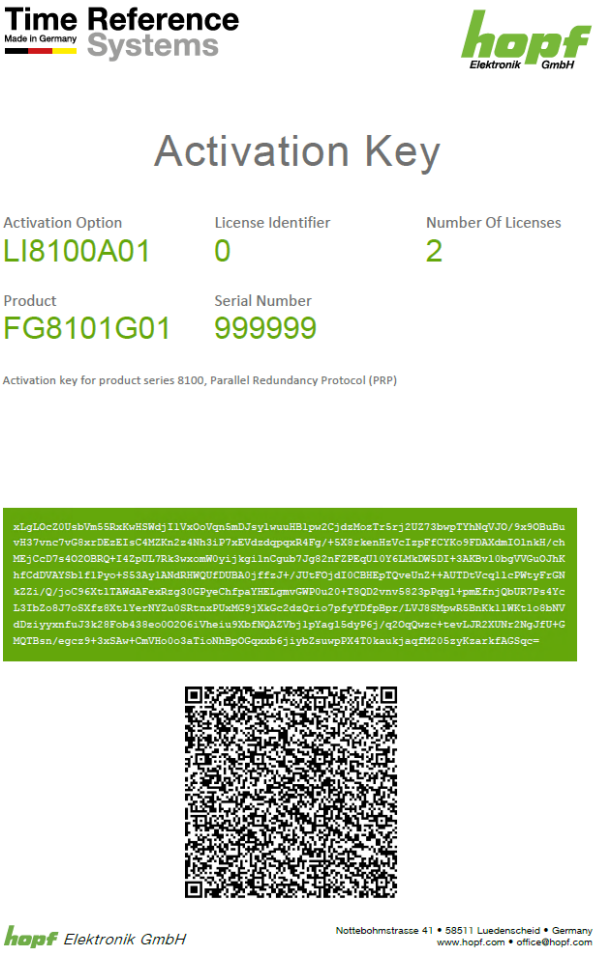
Activation keys can be applied in one of the following four ways:

1) Drag & Drop: the activation key PDF file received from ***hopf*** can be dragged and dropped to the Drag & Drop activation key area to apply the activation key

2) File selection: click the Drag & Drop activation key area to open a file browser. Select the activation key PDF file received from ***hopf*** and click the open button

3) Scanner: click in the text field in the **Activation** section and scan the QR-code in the activation key PDF file and click the **Add** button in the **Activation** section

4) Manually: manually enter the activation key from the activation key PDF in the text field in the **Activation** section and click the **Add** button in the **Activation** section.
Attention: do not add any carriage return. E.g. when you mark the whole activation key in the activation key PDF file and copy it to the clipboard (CTRL+C), the carriage returns are also copied. In this case paste the copied activation key in any editor (CTRL+V), remove the carriage returns, mark the whole text (CTRL+A), copy it to the clipboard (CTRL+C) and paste (CTRL+V) that text in the text field of the Activation section


Time Reference Systems
Made in Germany

hopf Elektronik GmbH

Activation Key

Activation Option
LI8100A01

License Identifier
0

Number Of Licenses
2

Product
FG8101G01

Serial Number
999999

Activation key for product series 8100, Parallel Redundancy Protocol (PRP)

xLgLOc20UsbVm55RxKwHSWdjI1VxOoVqn5mDJsylvuuHBlpw2CjdsMozTr5rj2U273bwpTYhNqVJO/9x9OBuBu
vH37vnc7vG8xrDEzEIsC4MZKn2s4Nh3iP7xEVdsdqpqxR4Fg/+5X8rkenHsVcIzpFfCYKo9FDAXdmIOlnkH/ch
MEjCcD7s4O2OBRQ+I4ZpUL7Rk3wxcmW0yijkgilnCgub7Jg82nFZPEqUl0Y6LMkDW5DI+3AKBvl0bgVVGuOJhK
hfCdDVAYSblflPyo+S53AylANdRHWQUfDUBAOjffsJ+/JUtFOjdI0CBHEpIQveUnZ++AUTDtVcqllcPWtyFrGN
kZZi/Q/joC96Xt1TAWdAFexRzg30GPyeChfpaYHELgmvGWP0u20+T8QD2vnv5823pPqgl+pmEfnjQbUR7Ps4Yc
L3IbZo8J7oSXfs8XtlYerNYZu0SRtnxPUxMG9jXkGc2dsQrio7pfyYDfpBpr/LVJ8SMpwR5BnKllWKtlo8bNV
dDziyyxnfuJ3k28Fob438eo0O206iVheiu9XbfNQAZVbjlpYaql5dyP6j/q2OqQwxc+tevLJR2XUNz2NgJfU+G
MQIBsn/egcz9+3xSAw+CmVHo0o3aIiNhBpOGqxxb6jiybZsuwpPX4I0kaukjaqfM205zyKzarkfAGSqc=

hopf Elektronik GmbH

Nottebohmstrasse 41 • 58511 Luedenscheid • Germany
www.hopf.com • office@hopf.com

Figure 27 activation key example

The above figure shows an example of an activation key PDF file. The text in the green box is the activation key that can be manually entered in the text field of the **Activation** section.

6.5.2 Configuration

The configuration download and upload pages are located here.

6.5.2.1 Download

6.5.2.1.1 Action

This action page allows the user to generate new configuration files and download existing configuration files.

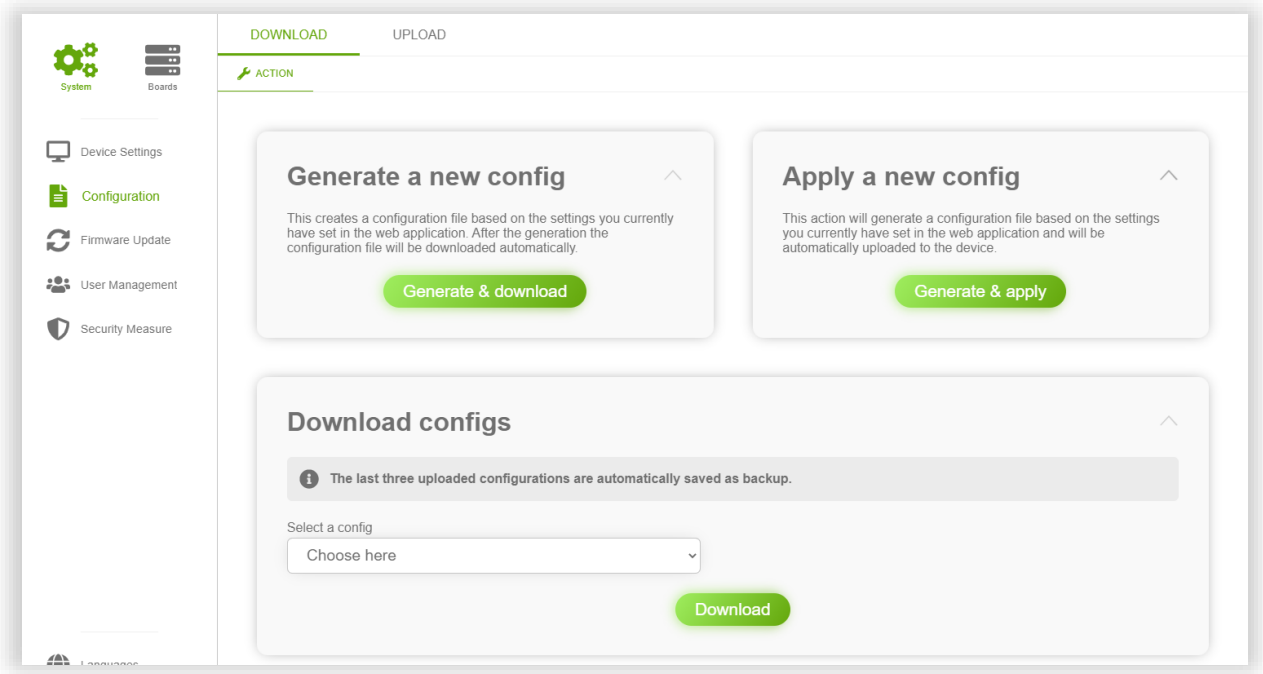


Figure 28 Configuration Page

New configuration files are generated from the values set by the user, which are stored in the browser storage.

Generate a new config: Generates and automatically downloads a config file. This allows the user to sign this config file to further increase security. Signed configs can be made mandatory under 6.5.5.1.1.

Apply a new config: Generates a config file and prepares the generated config file for an upload. The user is automatically navigated to the upload page.

Download config: Instead of generating a new config file, it downloads an existing config file from the server. There are three configuration files available for download. The currently applied config and two backup config files. The backup config files are created automatically. These are the two previously uploaded configs (if available).

6.5.2.2 Upload

6.5.2.2.1 Action

Uploading new config files is made possible on this page. The process is divided into three steps, each of them has a different view.

All steps are displayed in the upper area in the form of a progress bar. By clicking on the step number, users can jump back to a previous step.

Step 1

In the first step, the user must choose a config file, either by Drag and Drop of the file to the upload area or by opening the file explorer by clicking on the upload area and then selecting the file.

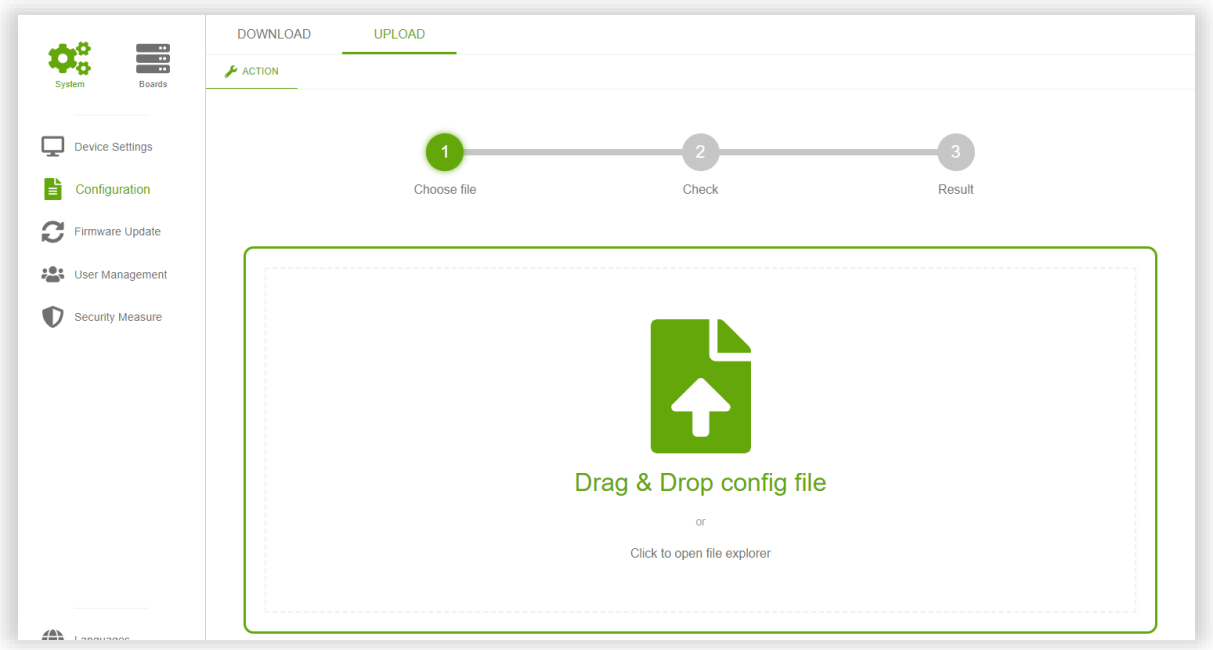


Figure 29 Drag and Drop config file

If signed config files are required (see 6.5.5.1.1) the uploaded file has to be in the ZIP file format. The ZIP file must contain the config file (the name has to be **config.json**) and the corresponding signature file (the name has to be **config.sig**). The signature file has to use **SHA256** as the message digest algorithm and **PKCS#1 v1.5** as the padding scheme.

In case signed configs are not required, only the config file (**config.json**) has to be uploaded.

If the file is not valid an error toast (see 5.7) will be shown with a corresponding error message.

Step 2

After the file has been chosen, the user will be taken to step 2. An overview of how the device will be affected by the new configuration is displayed here.

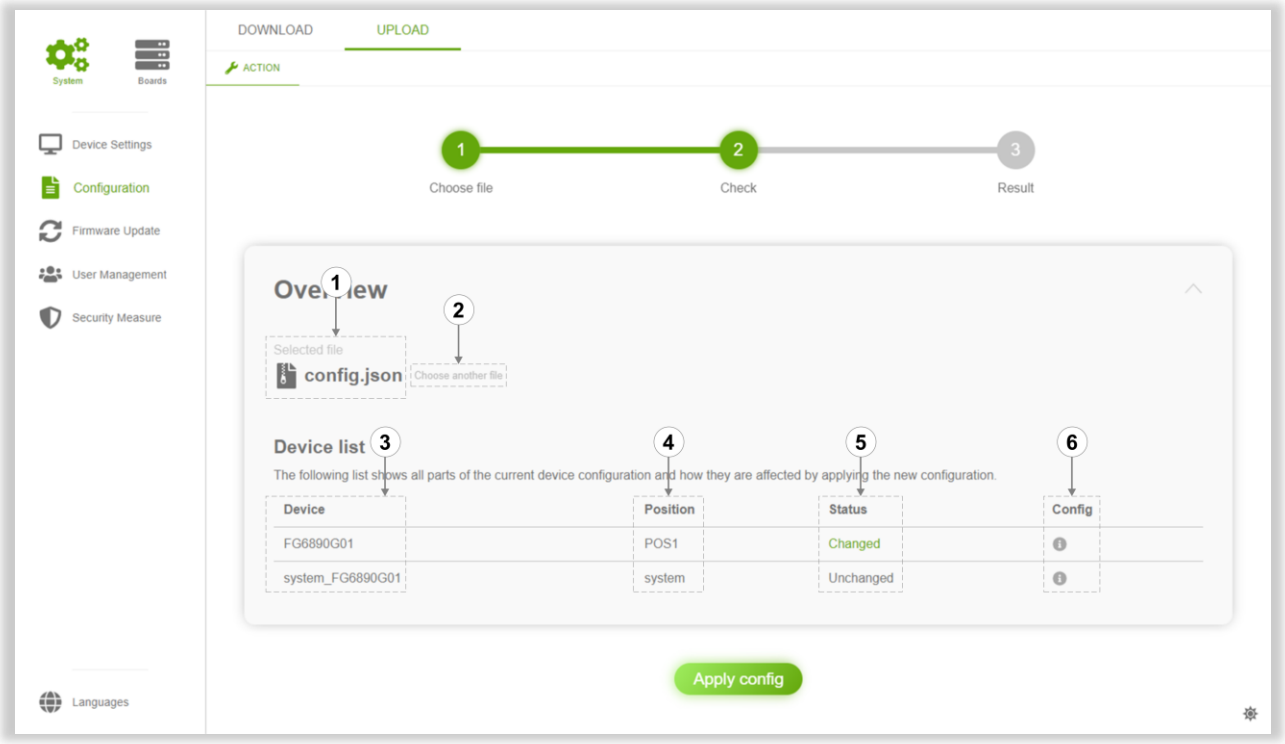
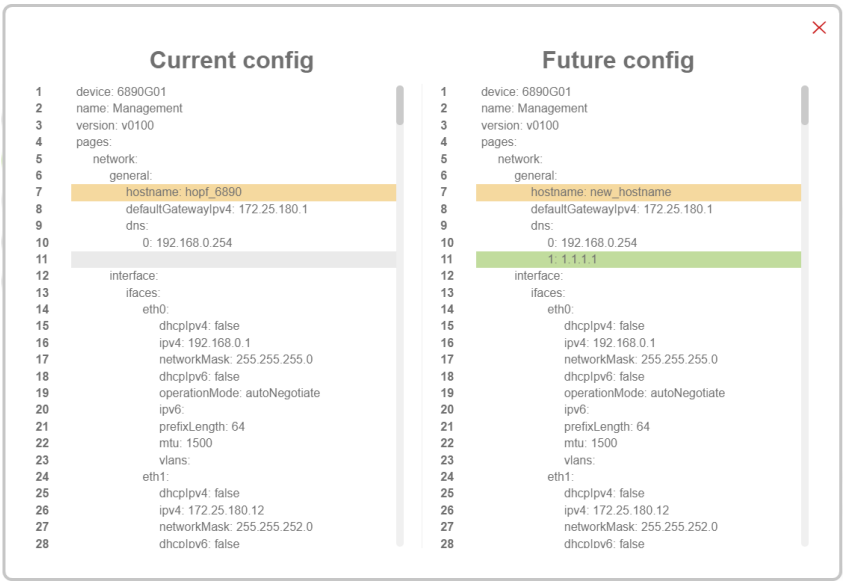


Figure 30 In this step an overview visualizing the config changes is presented

	Label	Description
1	Selected file	The name of the currently selected config file. If the upload was performed via the "Apply a new config" section (see 6.5.2.1.1), the selected file name will be "automatic_generated_config.json"
2	Choose another file	By pressing this button, the user returns to the first step.
3	Device	The device name.
4	Position	The position of the device.
5	Status	Changed – The new config file will change the configuration on this device. Unchanged – The new config file does not affect this device.

6	Config	Pressing the info button opens a popup with a comparison view of the current config and the future config. Changes are indicated with the colors yellow, red and green. Yellow means that an existing value has been edited, red that something has been removed and green that something has been added. 

Step 3

Step 3 displays either a success result or an error result after applying the configuration in step 2. In case of an error, the user receives a detailed error message explaining why the action was not successful.

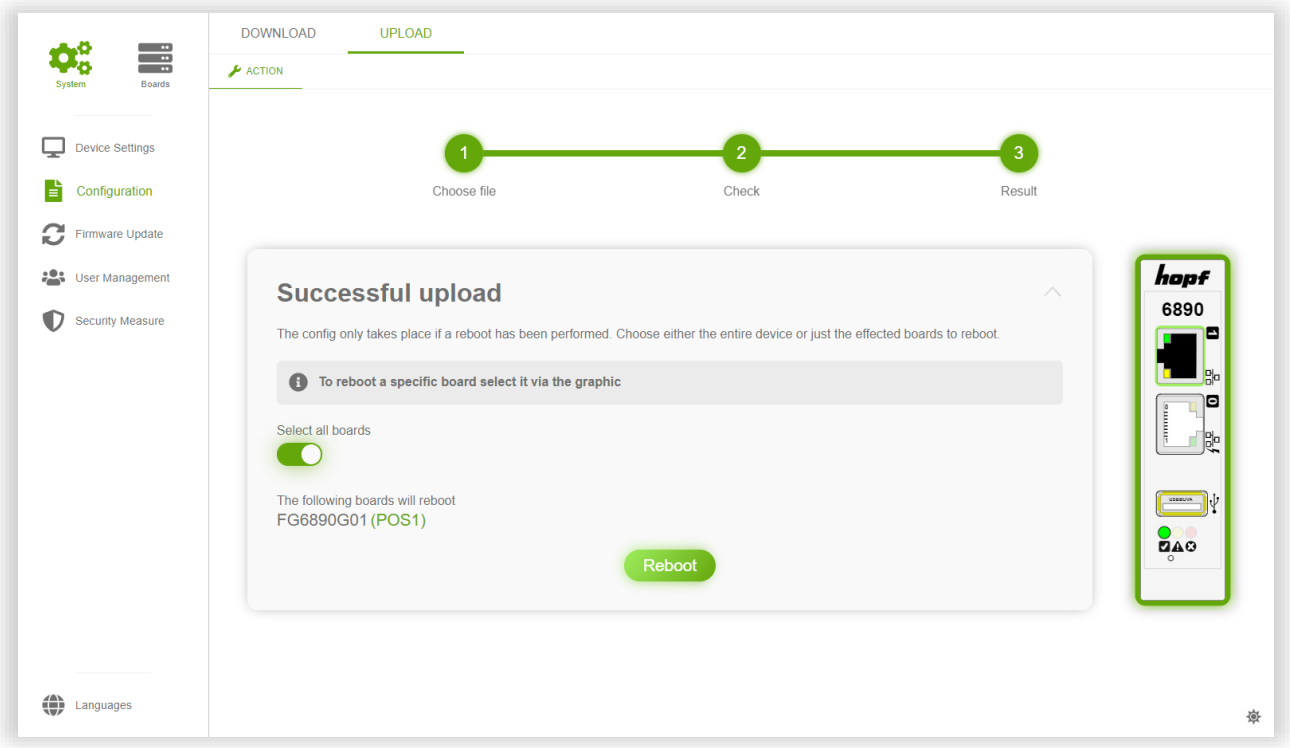


Figure 31 If the upload was successful, the restart controls are displayed

If the upload was successful, a reboot must be initiated for the changes to take effect. However, a reboot is only necessary for the boards that are affected by the config upload. The boards that need to be rebooted can be selected from the Device View by clicking on the corresponding board. Selected boards are highlighted with the accent color of the theme. After pressing the reboot button, a page appears where the user has to wait until the device is done with this action. Once the reboot is complete, the user will be redirected to the login page.

6.5.3 Firmware Update

A firmware update on the device by the user is made possible under this item.

6.5.3.1 Upload

6.5.3.1.1 Action

The process of uploading a new firmware is similar to the config upload. It is also split up in three steps, indicated by a progress bar.

If a firmware update is already in progress or even completely uploaded, but a required restart is missing this action is disabled.

Step 1

Only official firmware files provided by ***hopf*** can be uploaded. Choosing a file is similar to step 1 of Config Upload (see 6.5.2.2.1).

If signed update files are required (see 6.5.5.1.1), rename the update file to **update.zip**, generate the signature for this file and store the signature with file name **update.sig**. Generate a ZIP-file containing update.zip and update.sig and choose that file for the upload. The signature file has to use **SHA256** as the message digest algorithm and **PKCS#1 v1.5** as the padding scheme.

In case signed updates are not required, only the update file (the file **without** a file ending) has to be uploaded.

Step 2

In step 2, the user is presented with an overview of the selected firmware file. It gives the user details about the uploaded firmware file. Via Perform Update the boards that should be updated can be selected, if they are affected by the update.

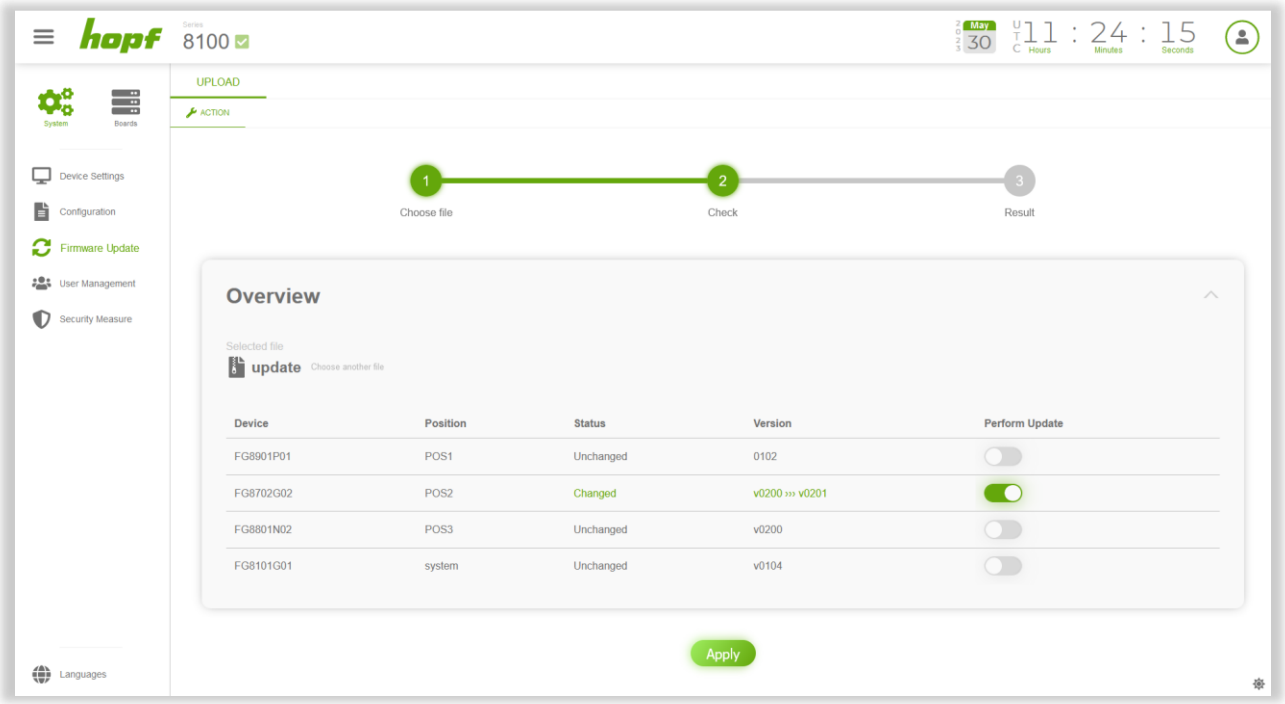


Figure 32 In this step an overview visualizing the structure of the firmware file is presented

Perform Update toggle button representation	**Description**
	Board is not affected by the firmware update. Update of the board cannot be enabled
	Board is affected by the firmware update and will **not** be updated after clicking the Apply button
	Board is affected by the firmware update and will be updated after clicking the Apply button

Step 3

If the upload was successful, a reboot is initiated automatically. The user is redirected to a page where he has to wait until the device has performed the reboot action.

If the upload has not been successful, an error result page will be displayed.

Notice: Major updates may change huma® to such an extent that a hard reload may be required after the update. This can be done by pressing ⇧ Shift + F5 in Google Chrome and Mozilla Firefox.

6.5.4 User Management

The item "User Management" consists of pages that take care of the administration of all users.

6.5.4.1 Roles

Roles are a set of permissions (rights) that can be assigned to a user. In huma® a user can have multiple roles. The permissions of all roles held by a user are simply merged together.

6.5.4.1.1 Config

On this config page user roles can be added, removed and modified.

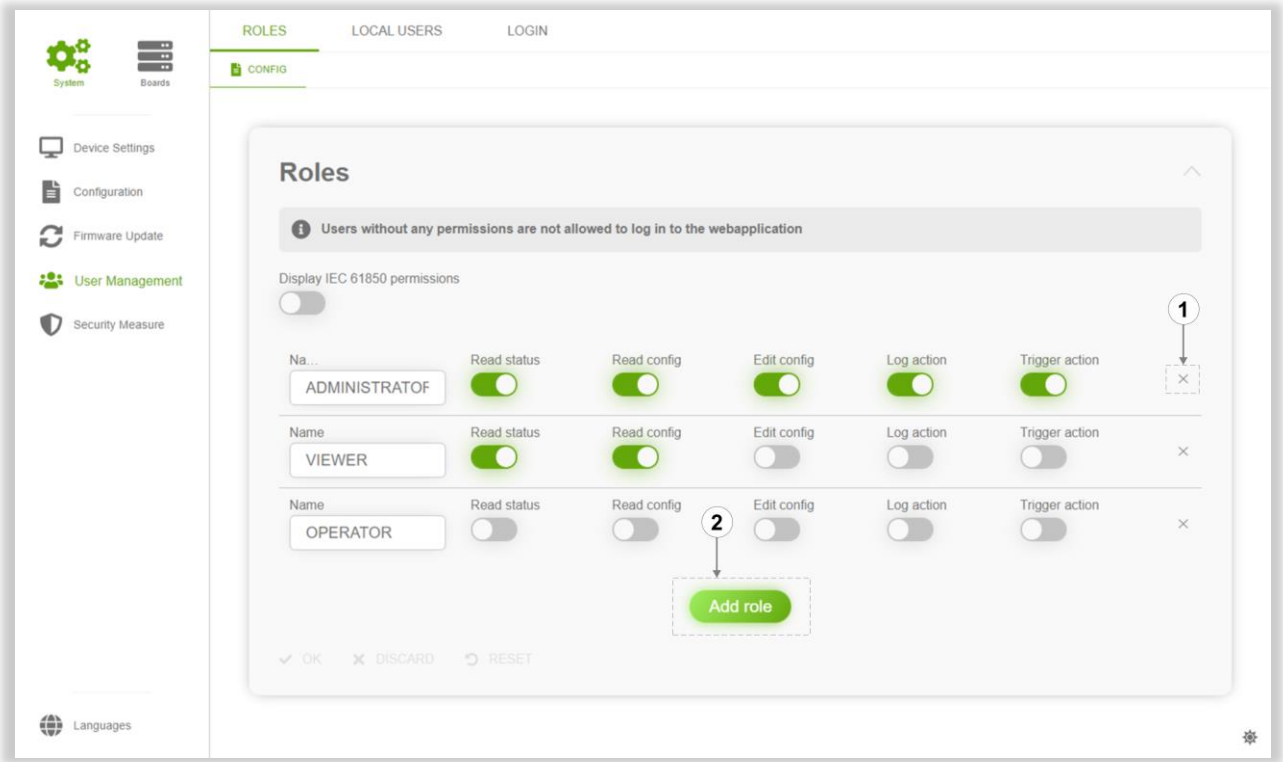


Figure 33 User roles

	Label	Description
1	Delete Button	Pressing this button will remove the role.
2	Add role	Pressing this button will add a new role.

Input Label	Description
Display IEC 61850 permissions	This setting will display the official IEC 61850 permission **names** instead of the default permission names. Fundamentally, they are built on the same set of the rights. The following list explains how IEC 61850 permissions compare to standard permissions: **READVALUES** = Read status + Read config **CONFIG** = Edit config **REPORTING** = Log action **CONTROL** = Trigger action **DATASET** = Log action + Trigger action
Name	The editable role name.
Read status	Allows the user to view status pages. **Users can't affect the device with this permission.**
Read config	Allows the user to view config pages. **Users can't affect the device with this permission.**
Edit config	Allows the user to edit values on config pages. The "Edit config" right has no direct influence on the device, because in order to change the device config, the user must upload a new config. Uploading a new config is only possible with the "Trigger action" right. **Users can't affect the device with this permission.**
Log action	Allows the user to acknowledge and delete log entries. **Users can affect the device with this permission slightly.**
Trigger action	Allows the user to view action pages and trigger actions. **Users can affect the device with this permission.**

6.5.4.2 Local Users

Pages for administering users who are handled on the device and not on an external authorization system such as Radius are located under "Local Users".

6.5.4.2.1 Action

On this action page a user can change the password of local users. To do this, the desired user must be selected and the new password entered twice to ensure correct input.

Only alphanumeric and following characters are accepted when entering the password:

_ - * ! / = ? [ ] .

The number of characters has to be between 6 and 20.

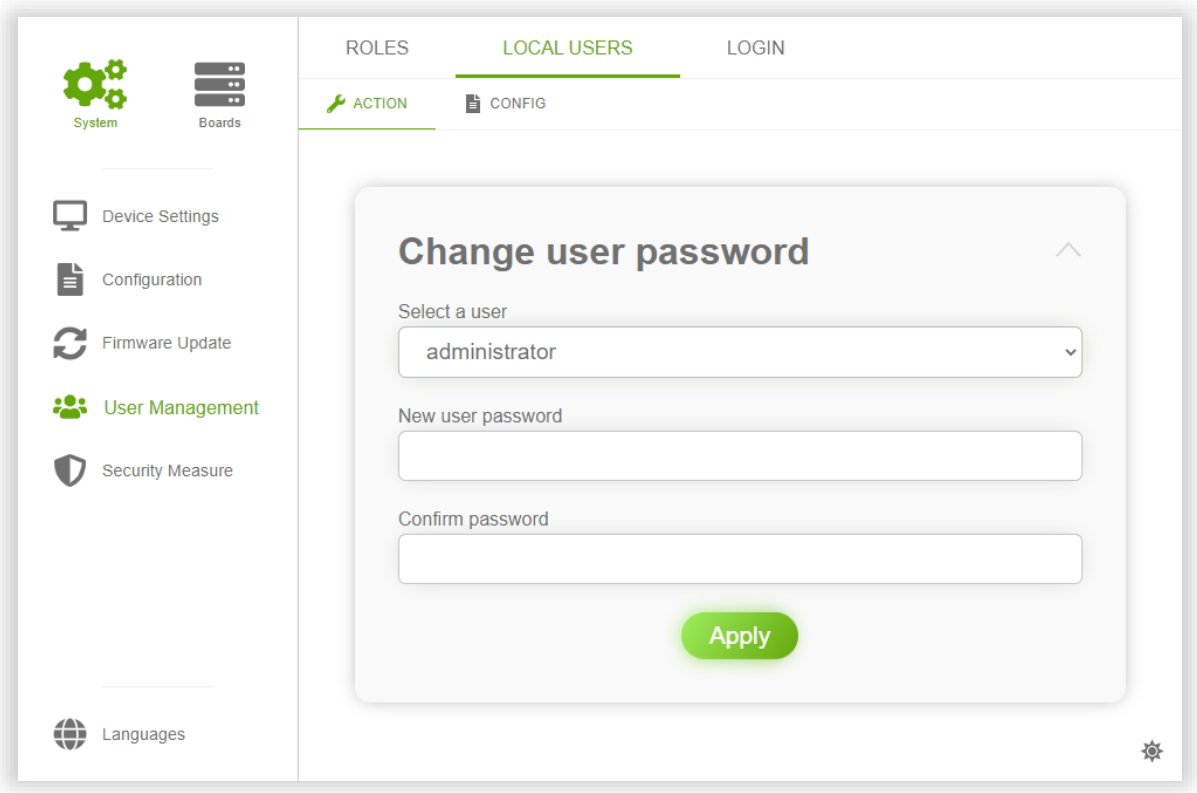


Figure 34 Changing password of the user "administrator"

6.5.4.2.2 Config

This page allows assigning specific roles to a local user. A user can occupy several roles at once.

There are 5 predefined users. The number of users cannot be changed, but users can be deactivated.

Deactivating a user works by assigning **one role** to the user for which **no permissions are enabled**.

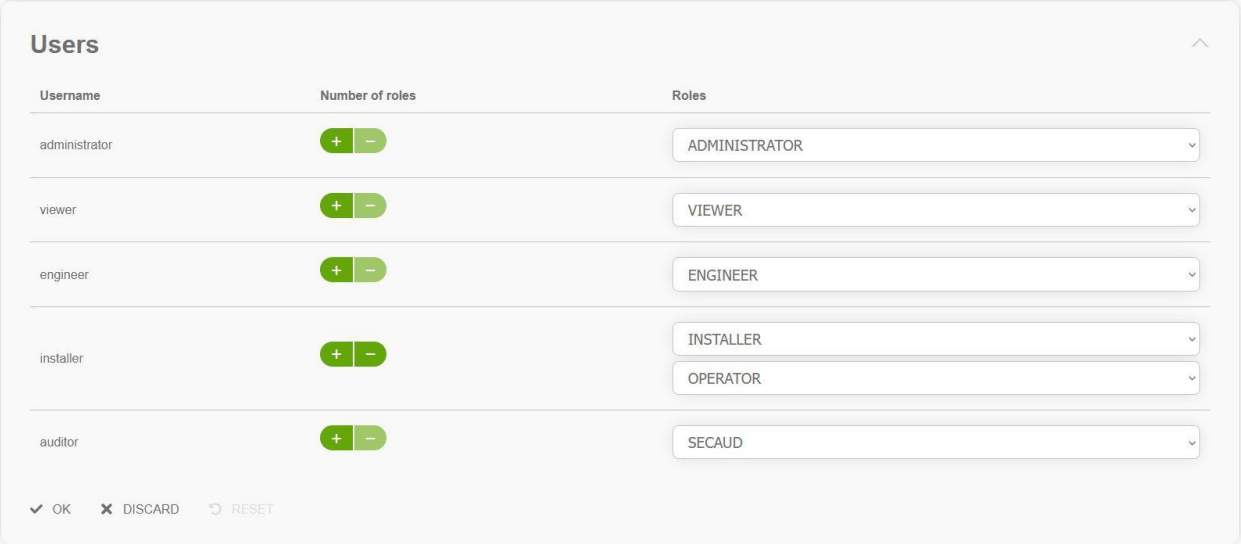


Figure 35 In this example the installer user has two roles

Table Column Label	**Description**
Username	The predefined and fixed username.
Number of roles	A role selector can be added to a user by pressing the plus button or removed by pressing the minus button. Each user must have at least one role. Assign a role without permissions to deactivate the user.
Roles	Each selector allows choosing a specific role for a user.

6.5.4.3 Login

6.5.4.3.1 Config

All settings to select the desired login scheme can be found here.

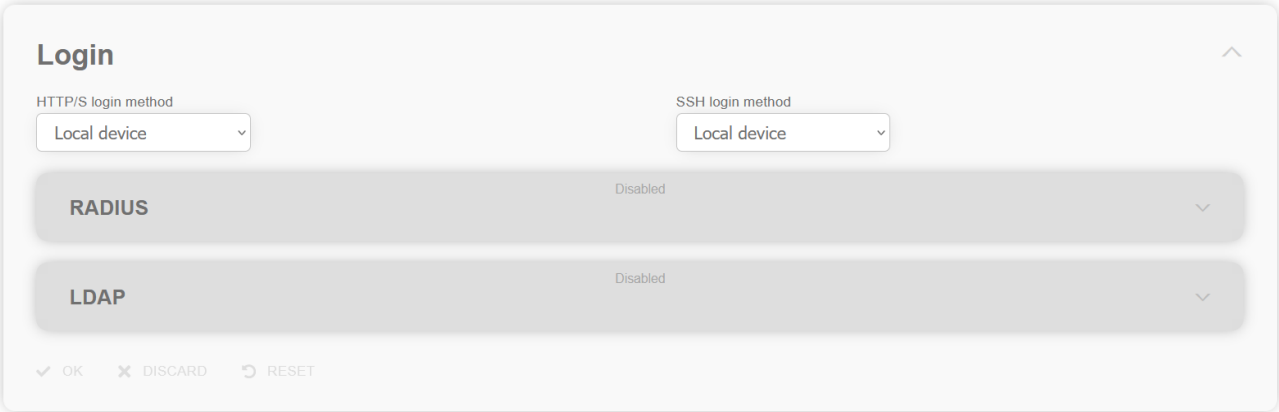


Figure 36 In this example RADIUS is selected for HTTP/S

Input Label	Description
HTTP/S login method	This setting specifies the login method for HTTP/S.
SSH login method	This setting specifies the login method for SSH.
Local as fallback	If the option "Local device" was not selected in the HTTP login method or SSH login method components, the local device is still offered as a fallback option. The fallback occurs when the corresponding RADIUS or LDAP service is not reachable (timeout).

Currently the following login methods are supported:

6.5.4.3.1.1 Local Device

Authentication and authorization are based on users and rights stored on the device.

6.5.4.3.1.2 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol, that provides centralized Authentication, Authorization and Accounting management.

The information which roles are assigned to a given user is transmitted as a string via the "filter-id" attribute in the radius ACCESS-ACCEPT response. If multiple roles need to be assigned, they must be transmitted comma-separated. (This behaviour changes when "IEC 61850" is selected, see table below). For example, if the user "maint" shall have the two roles "config" and "view", the filter-id string in the ACCESS-ACCEPT response needs to be "config,view".

If RADIUS is selected as login method, the following settings will appear:

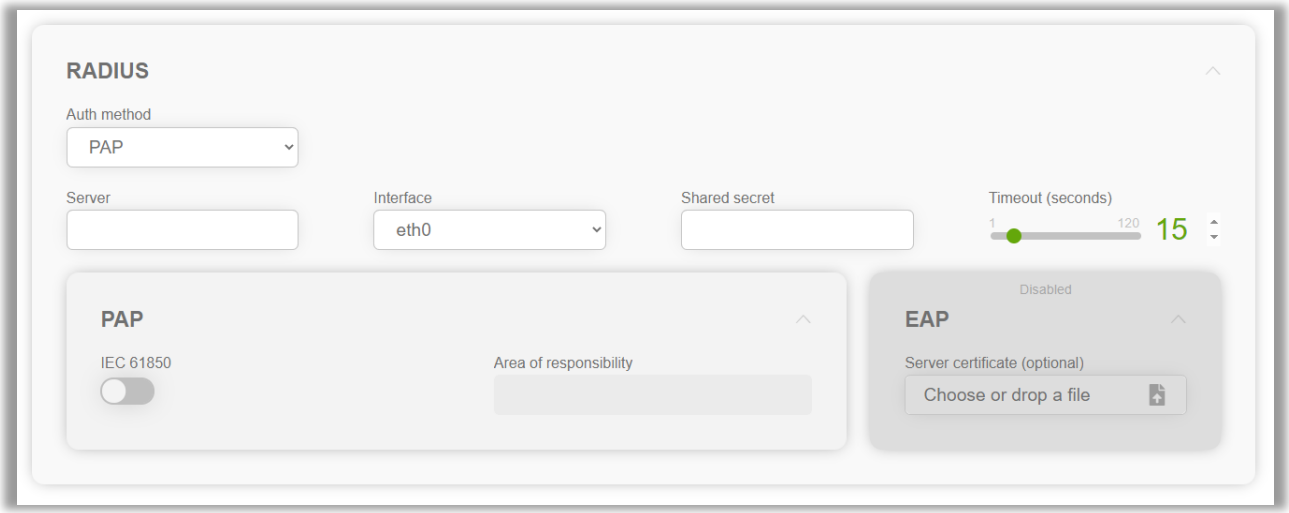


Figure 37 RADIUS config page

Input Label	Description
Auth method	The auth method can be set to PAP (Password Authentication Protocol) or EAP (Extensible Authentication Protocol). Depending on the selected Auth method the subsection "PAP" or "EAP" will be enabled.
Server	This setting specifies the network address of the RADIUS server.
Shared secret	Used to secure the communication between the system and the radius server.
Timeout	Timeout after which a radius request will be considered failed.
IEC 61850	If enabled, receive radius authentication tokens according to the mentioned standard. If disabled, receive user roles via radius attribute "filter-id" (comma separated).
Area of responsibility	Defines the area of responsibility for radius authentication tokens according to IEC61850. Roles which are not within the area of responsibility will be ignored.
Server certificate (optional)	Upload the server certificate here if the server certificate of the RADIUS server is not trusted (e.g., self-signed). This option is only available if EAP is used.

Example with Windows Server 2019:

1. Prepare Active Directory Users and Computers

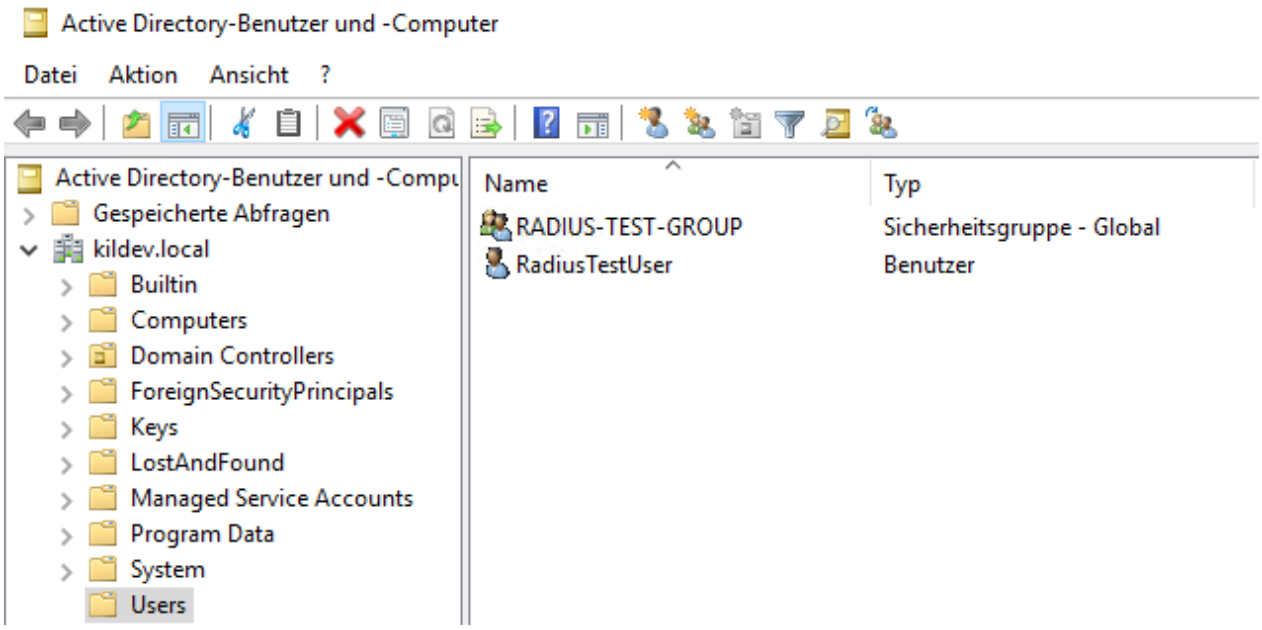


Figure 38 An example of the RADIUS user configuration

Create a group of authorized users to authenticate with RADIUS (in the above figure the group is RADIUS-TEST-GROUP)

Add a user to the radius group (in the above figure RadiusTestUser)

2. Installation of the RADIUS service

Install the Network Policy and Access Services server role and reboot the server if necessary.

3. Configuration of the RADIUS service

Start 'Windows Administrative Tools' / 'Network Policy Server'

Register your RADIUS server in Active Directory so that it can query the user and group database.

In Network Policy Server, right-click NPS (Local) and click Register Server in Active Directory.

3.1. Create a new network policy

Go to the Network Policies page under Network Policy Server and add a policy for the RADIUS access of the huma® device.

In Network Policy Server, right click on the 'NPS (Local)' / 'Policies' / Network Policies branch and select 'New'

Enter a 'Policy name' (e.g., RADIUS-TEST) ➔ 'Next'

In the Condition Description area, click 'Add...'

Select 'UserGroups' and then 'Add...'

Add the correct user group via the 'Add Groups …' button (in our example it's the RADIUS-TEST-GROUP group) ➔ 'OK'

Click the 'Next' button on the 'New Network Policy' window

Select 'Access granted' ➔ 'Next'

Click 'Add…' to add 'EAP Type' 'Microsoft: Protected EAP (PEAP)' and deselect everything under 'Less secure authentication methods: ' ➔ 'Next'

Click 'Next' on the 'Configure Constraints' window

Select 'Standard' under 'RADIUS Attributes' and add the attribute 'Filter-Id' with a value matching a role configured on your huma® device via the 'Add…' button (e.g., ADMINISTRATOR, when you have not renamed the roles on the huma® device) ➔ 'Next'

Click 'Finish' on the 'Completing New Network Policy' window

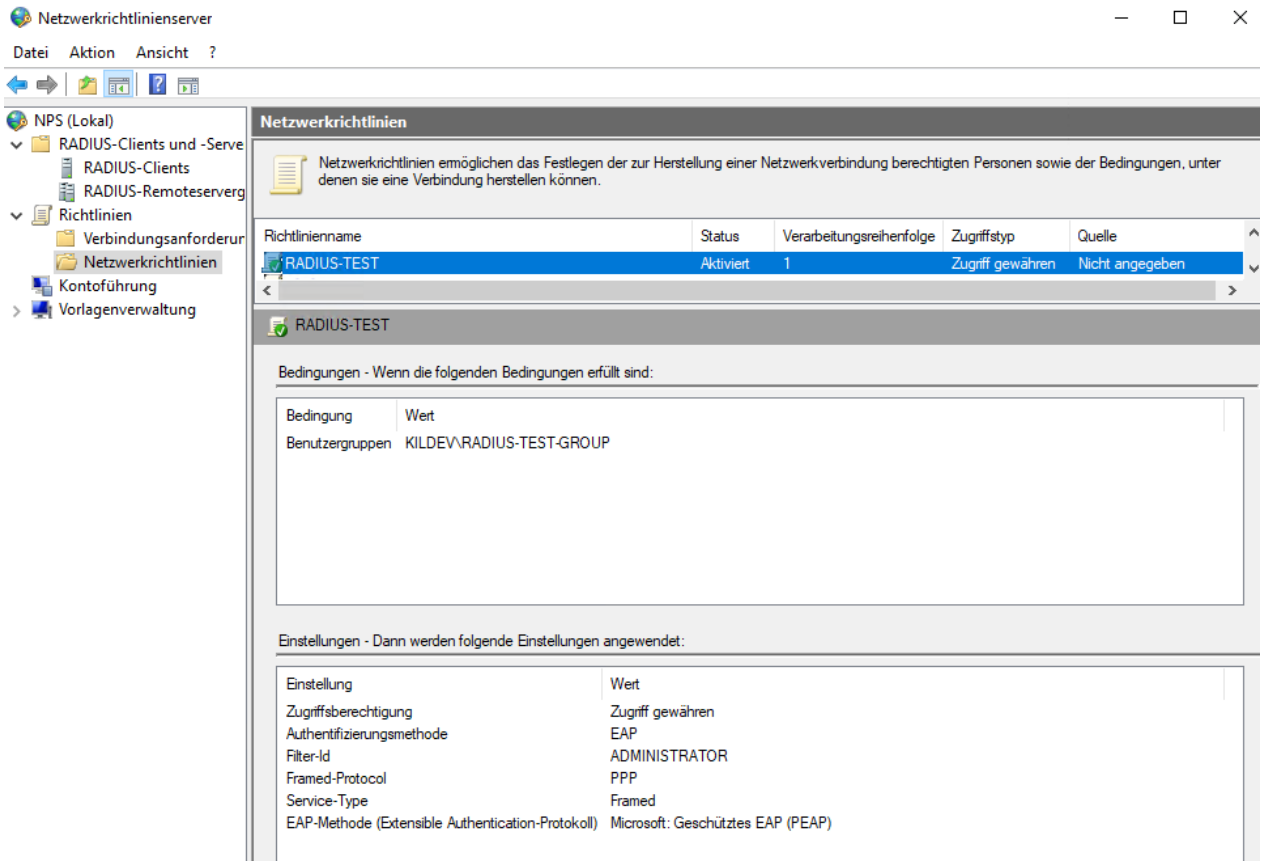


Figure 39 RADIUS network policy configuration example

The Filter-ID is used by the huma® device to check the access rights. In the above figure the Filter-ID value ADMINISTRATOR has been added to the RADIUS-TEST policy. And under Terms the user group created for the RADIUS users must be added, in this example RADIUS-TEST-GROUP.

3.2. Creating a RADIUS client

Last thing that has to be done is to add the huma® device to the RADIUS-Clients.

In Network Policy Server, right-click on the 'NPS (local)' / 'RADIUS Clients and Servers' / 'RADIUS Clients' branch and select 'New'

Enter a 'Display Name' (e.g., HOPF Device), a Client 'Address' (e.g., 192.168.0.1) and a 'Shared Secret' (e.g., ABC).

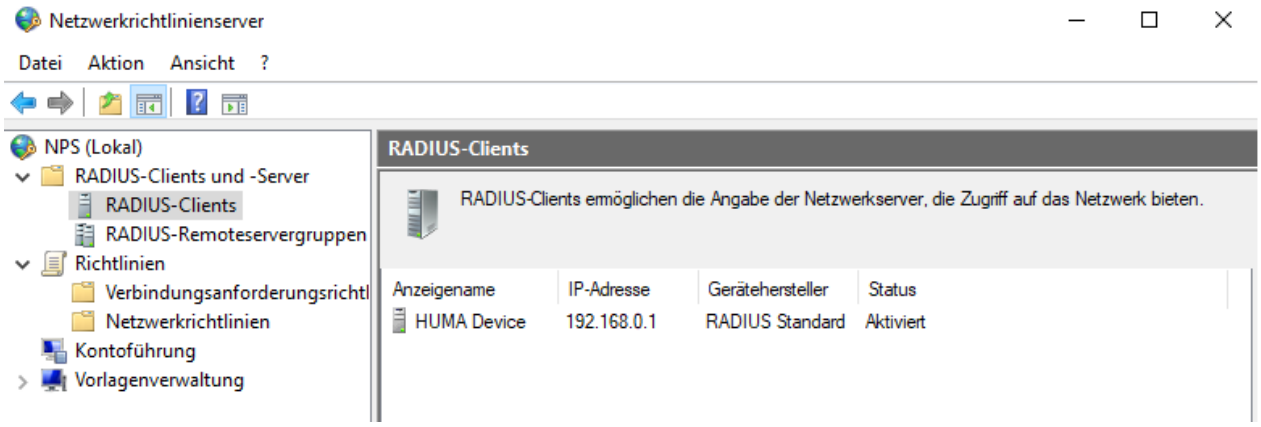


Figure 40 RADIUS client configuration example

The huma® configuration for this example is shown below. The IP address of the RADIUS server is 192.168.0.2 and the shared secret for the huma® Device is ABC.

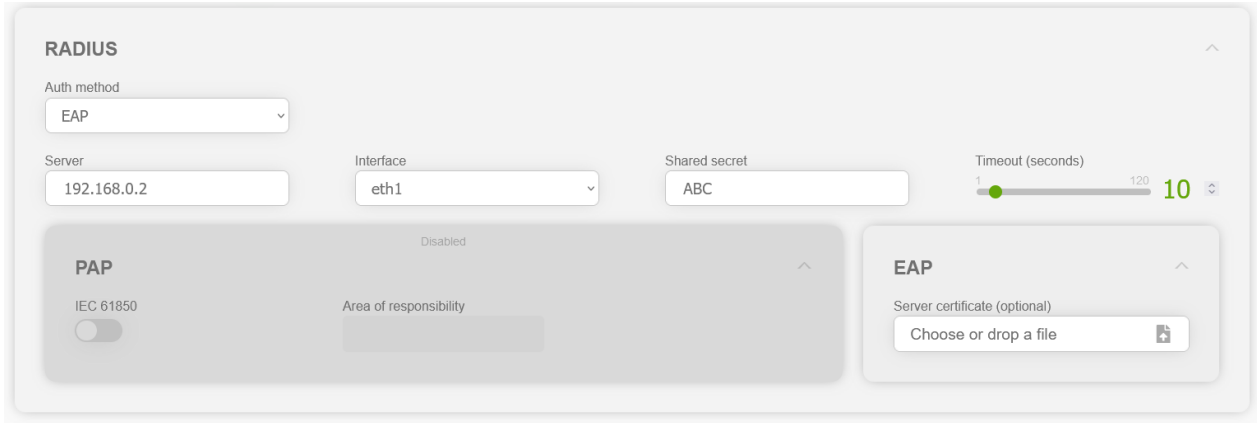


Figure 41 Example of the RADIUS configuration on the huma® device

6.5.4.3.1.3 LDAP

Lightweight Directory Access Protocol (LDAP) user authentication is the process of validating a username and password combination with a directory server.

The information which roles are assigned to a given user is queried from the LDAP server by checking the "memberOf" attribute of the active directory user account. "memberOf" values that do not correspond to any role configured on the device are ignored. For example, if user "maint" shall have the two roles "config" and "view" the LDAP user account of "maint" must be a member of the LDAP groups "config" and "view".

The LDAP user account must be a valid POSIX account to be able to login to the ***hopf*** device. This means it must have an assignment for the following attributes:

gidNumber: use any valid posix group-id

uid: use any valid posix uid. It is recommended to use the same name LDAP username

uidNumber: use any valid posix user-id. Only user-ids greater than 1,000 will work.

objectClass: must contain the value "posixAccount"

If LDAP is selected as a login method, the following settings will appear:

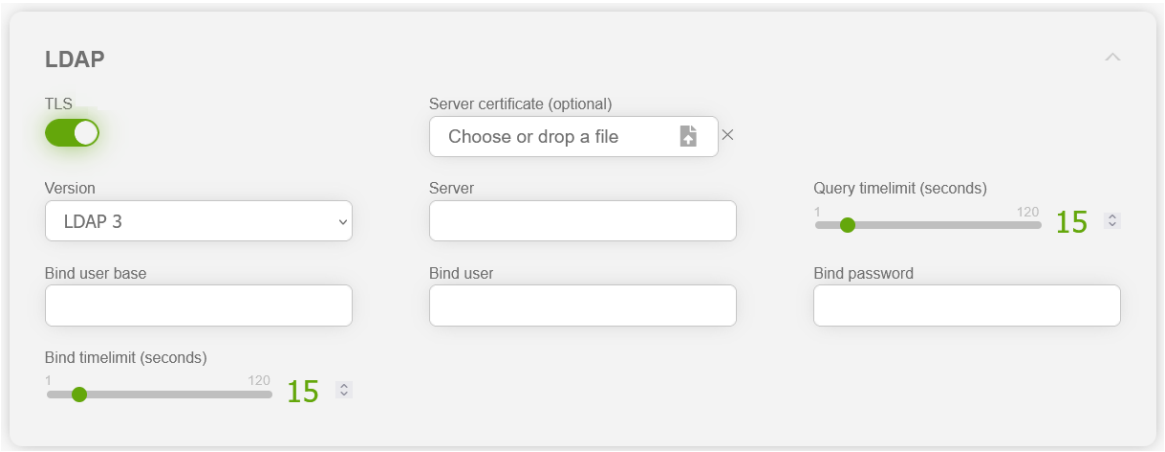


Figure 42 LDAP configuration section

Input Label	Description
TLS	Enabling this setting will use Transport Layer Security (TLS) as transport protocol for LDAP.
Server certificate (optional)	Upload the server certificate here if the server certificate of the LDAP server is not trusted (e.g., self-signed).
Version	This setting specifies the LDAP version used.
Server	This setting specifies the network address of the LDAP server.
Query timelimit	Time after which a LDAP query will be considered failed.
Bind user base	The user base is the starting point ("base DN") an LDAP server uses when searching for user's authentication within your directory.
Bind user	The username the device will use to bind to the LDAP server.
Bind password	The password of the user the device will use to bind to the LDAP server.
Bind timelimit	Time after which the LDAP bind process will be considered failed.

Example with Windows Server 2019:

Go to the Users folder in the Active Directory Users and Computers panel.

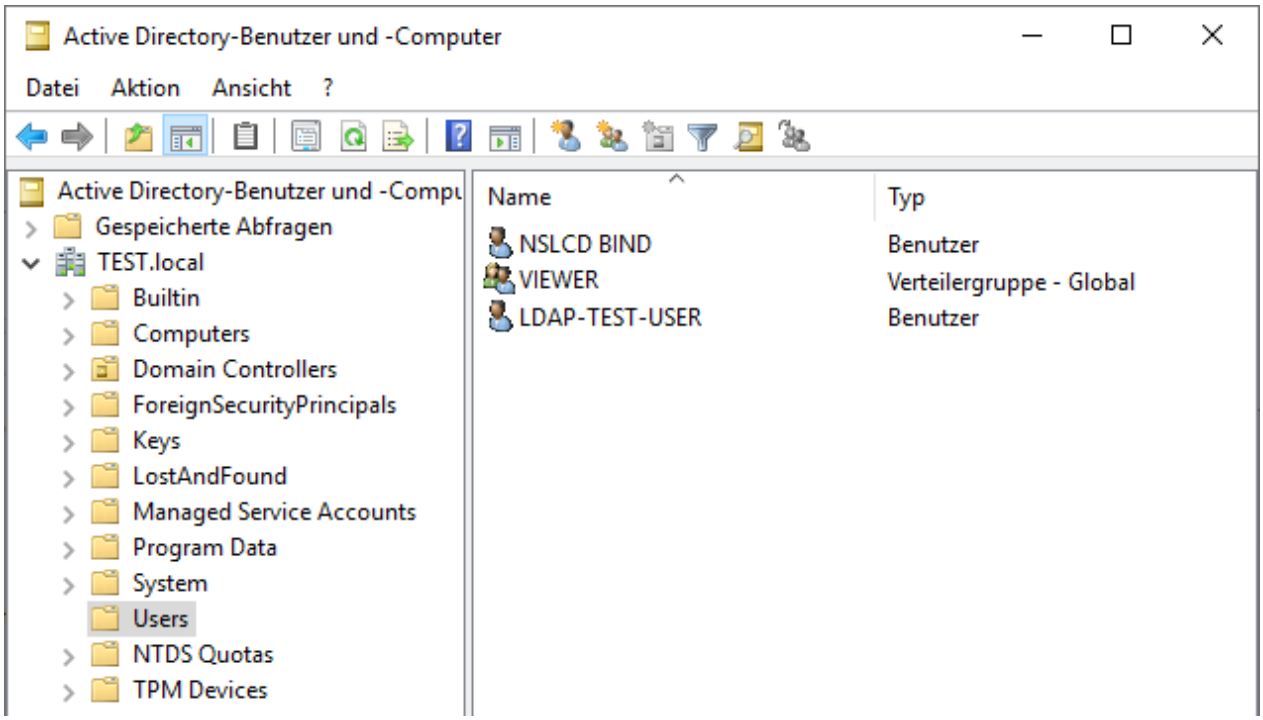
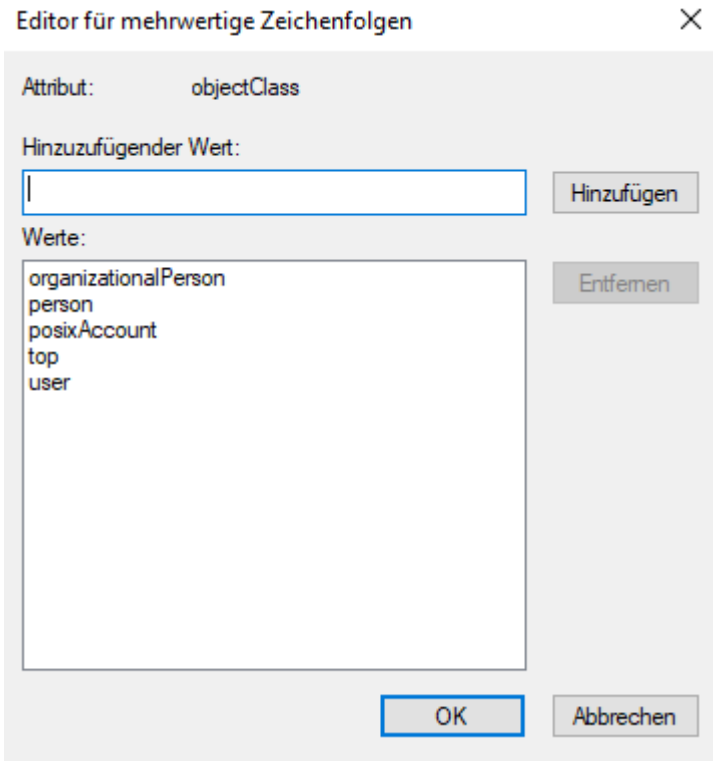


Figure 43 Windows server 2019 LDAP user's example

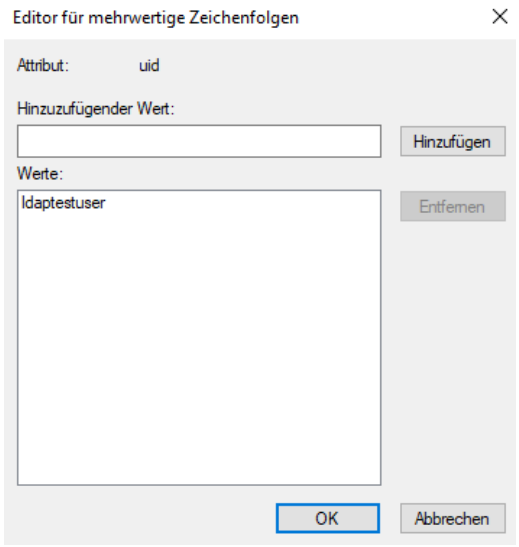
Create a LDAP bind user (NSLCD BIND in the figure above has user name "nslcd-bind" and password "ldapbind")

Create a group with identical name as one of your roles in your huma® device, see 6.5.4.1.1 (in the above figure VIEWER group has been used)

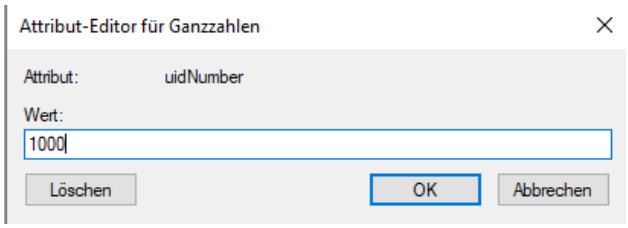
Add a user to the group (in the above figure LDAP-TEST-USER has been added to the VIEWER group, its login name is ldaptestuser). Change the Attributes of the user with the Attribut-Editor as follows:



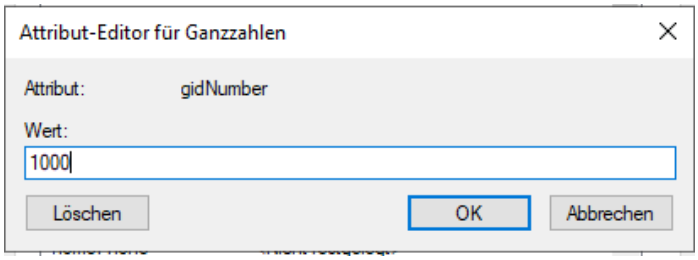
Add posixAccount to objectClass



uid must be identical to the login name



uidNumber must be set to 1000



gidNumber must be set to 1000

To be able to login with the LDAP-TEST-USER, the LDAP section must be configured as shown in the following figure.

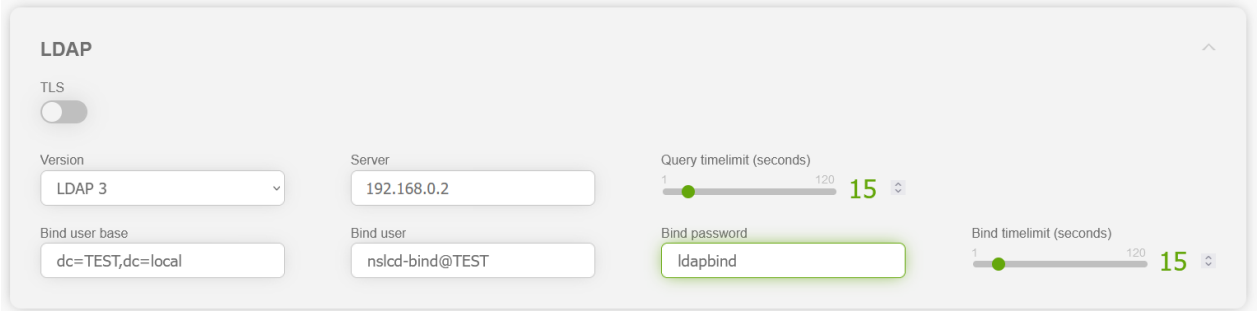


Figure 44 LDAP configuration example

The IP-address of the LDAP server is 192.168.0.2.

6.5.5 Security Measure

All security-related pages are provided under this item.

6.5.5.1 Profile

6.5.5.1.1 Config

huma® provides a set of predefined security settings in the form of a profile. These profiles can be selected on this page. Pressing a profile button overwrites the configuration values with the corresponding profile values. Not only the settings on this page are affected by a profile, but also all firewall pages of all boards (see 6.6.2.4.1) are overwritten according to the selected profile. The changed values can still be edited normally and may differ from the profile settings.

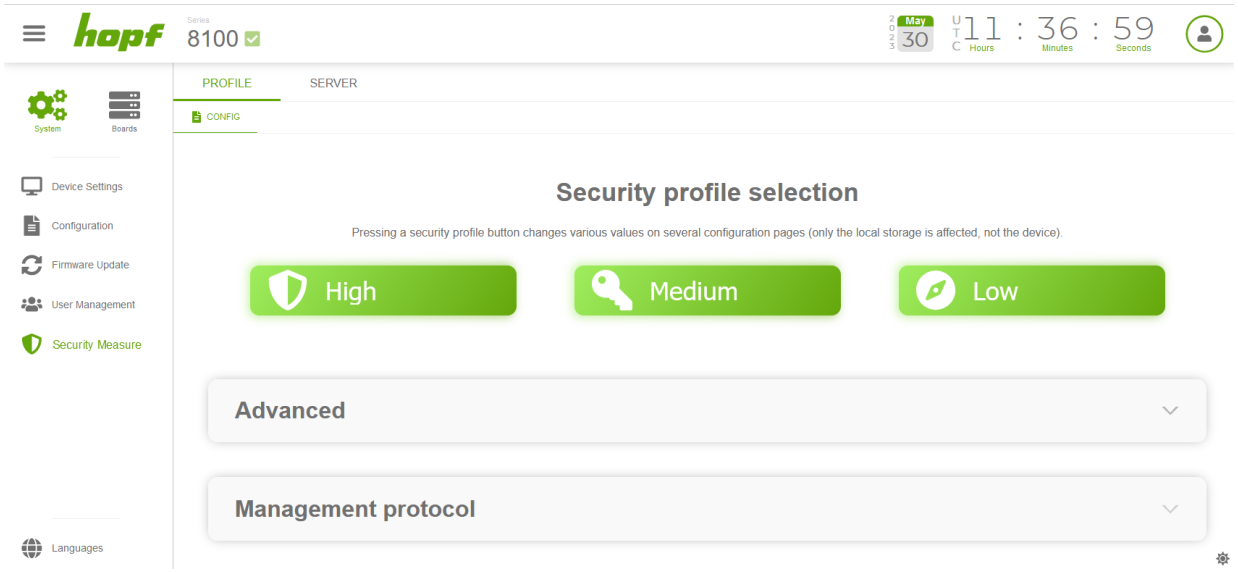


Figure 45 Security profile page

There are three predefined profiles (for detailed settings see caption "Profile settings" down below in this chapter):

High	Medium	Low
- Very high security settings - Persistent user deactivated - Short-lived authentication token - Highly restricted firewall	- High security settings - Persistent user activated - Mid-lived authentication token - Restricted firewall	- Sufficient security settings - Persistent user activated - Standard authentication token - Open firewall

This config page also consists of two sections filled with security settings. Pressing a profile button will overwrite these settings (besides the firewall settings).

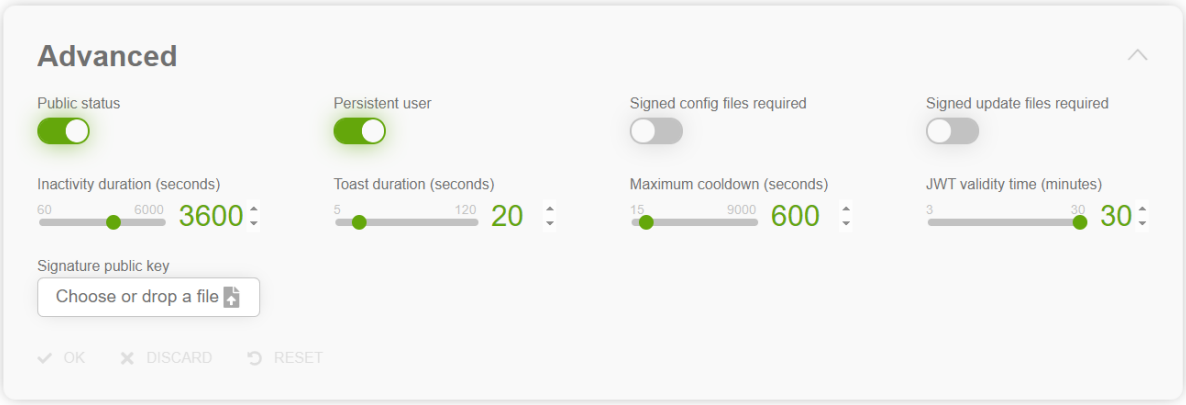


Figure 46 Security measure advanced configuration section

Input Label	**Description**
Public status	Status information of the device can be made publicly visible on the login page with this setting (see 6.1).
Persistent user	User information (**NOT** the password) can be stored persistently in the "Local Storage". Activation increases the likelihood of stealing user information through an XSS attack, but is still **recommended due to its practicality and low risk!** **Disabling this setting is unrecommended**, as the user will have to log in each time the web application is refreshed (e.g., by pressing F5 or when the board structure should be reloaded because a board has been added to the device).
Signed config files required	If enabled, config files must be signed using a valid private key (RSA) before uploading. **Note:** The corresponding public must be added via Signature public key
Signed update files required	If enabled, firmware update files must be signed using a valid private key (RSA) before uploading. **Note:** The corresponding public must be added via Signature public key
Inactivity duration (seconds)	Automatic logout after a certain number of inactive seconds.
Toast duration (seconds)	Duration in which a toast notification (see 5.7) is visible.
Maximum cooldown (seconds)	The maximum login cooldown time of failed attempts (see 6.1; Component 9). The cooldown time is incremented linearly after each failed attempt. This value defines a maximum limit for the cooldown time.
JWT validity time (minutes)	Duration of how long a JSON web token is valid before it expires.

Signature public key	The public key as PEM file, to verify the signature of the signed config/update file.

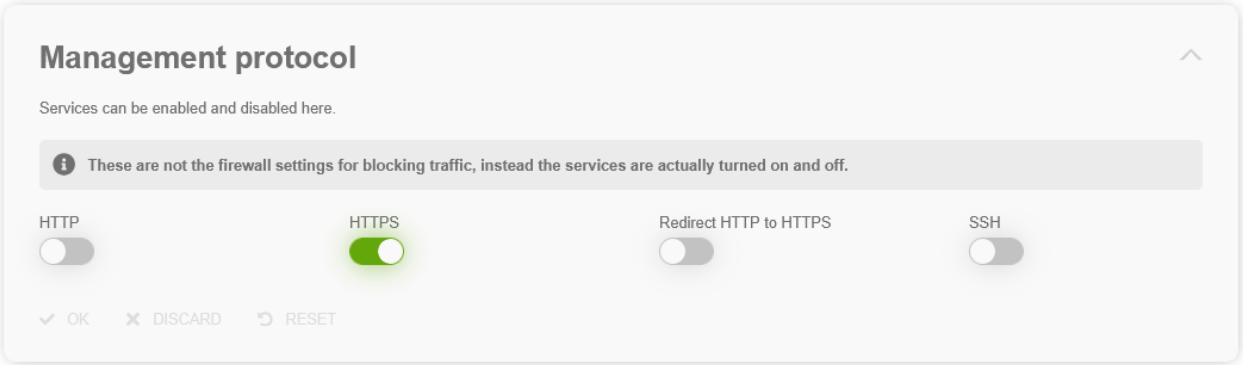


Figure 47 Management protocol configuration section

Input Label	Description
HTTP	The "HTTP" service can be turned on or off.
HTTPS	The "HTTPS" service can be turned on or off.
Redirect HTTP to HTTPS	When enabled, HTTP requests to the device are redirected to HTTPS. **Remark:** The redirecting of HTTP requests only works, when HTTP is allowed in the firewall rules of the management board of the system.
SSH	The "SSH" service can be turned on or off.

Profile settings

Setting	High	Medium	Low
Advanced			
Public status	False	False	True
Persistent user	False	True	True
Signed config files required	True	True	False
Signed update files required	True	True	False
Inactivity duration (seconds)	300	900	3600

Notification duration (seconds)	30	20	20
Maximum cooldown (seconds)	9000	7200	600
Management protocol			
HTTP	False	False	False
HTTPS	True	True	True
SSH	False	True	True
Firewall of the Management Board			
Priority 1	Interface: "any" Service: "https" Policy: "allow" Direction: "both" Remote IP: "" Protocol: "tcp"	Interface: "any" Service: "ssh" Policy: "allow" Direction: "both" Remote IP: "" Protocol: "tcp"	Interface: "any" Service: "any" Policy: "allow" Direction: "both" Remote IP: "" Protocol: "both"
Priority 2	Interface: "any" Service: "any" Policy: "deny" Direction: "both" Remote IP: "" Protocol: "both"	Interface: "any" Service: "https" Policy: "allow" Direction: "both" Remote IP: "" Protocol: "tcp"	Interface: "any" Service: "any" Policy: "deny" Direction: "both" Remote IP: "" Protocol: "both"
Priority 3	---	Interface: "any" Service: "any" Policy: "deny" Direction: "both" Remote IP: "" Protocol: "both"	---
Firewall(s)			
Priority 1	Interface: "any" Service: "any" Policy: "deny" Direction: "both" Remote IP: "" Protocol: "both"	Interface: "any" Service: "any" Policy: "deny" Direction: "both" Remote IP: "" Protocol: "both"	Interface: "any" Service: "any" Policy: "deny" Direction: "both" Remote IP: "" Protocol: "both"

Notice: On all profiles (except **Low**) the network time output is filtered by the firewall and thus deactivated. To enable the network time output, add a firewall rule that allows the corresponding network traffic. To find out which network time output is forbidden, check out the toast "Firewall forbids activated service" (see 5.7.1).

6.5.5.2 Server

The pages under "Server" are focused on the security settings of the web server and its components.

6.5.5.2.1 Status

This status page shows how long a Json Web Token (JWT) secret is in use.

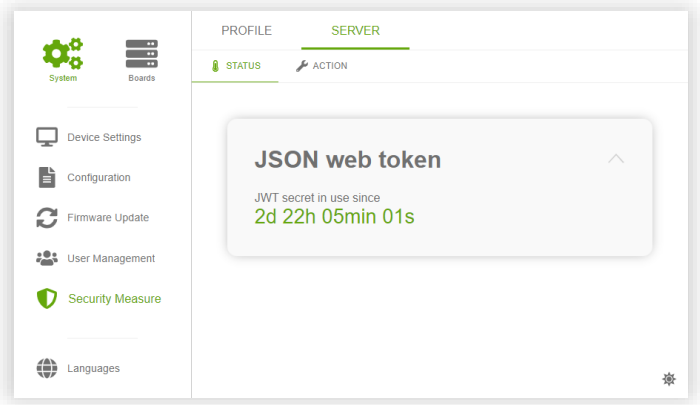


Figure 48 The use time of the JWT secret shown dynamically

6.5.5.2.2 Action

There are two different server security sections on this page. The section called "Generate new JWT secret" contains a button that generates a new JWT secret on the server when pressed. It is recommended to refresh the JWT secret at least once a year.

The "Device Certificate" section has a form to upload a certificate file. This provides the option to encrypt all TLS based connections on the device with a user-supplied SSL server certificate, instead of the default self-signed certificate contained in the device.

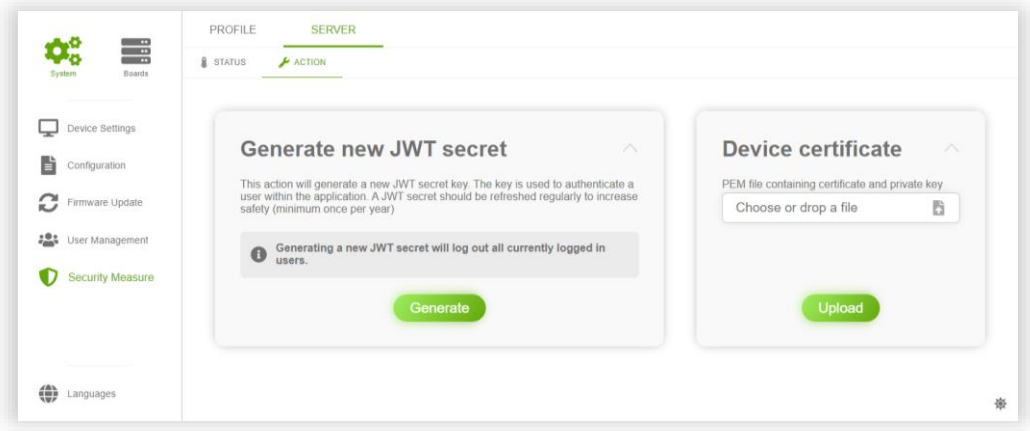


Figure 49 Security Measure server action page

Device certificate generation and format:

ECC and RSA based X509 certificates are supported.

e.g. rsa:2048, rsa:4096, prime256v1, …

The certificate must be a *.pem file and it must contain the private kay and the certificate.

Example content of such a file:

-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIG0rKdFrNQFFYoNu9VD8qCLun1WuWdpLZJR9RNFZQKWIoAoGCCqGSM49
AwEHoUQDQgAEXSD+WLB5Lg1isJw7gYUCrSO1uOa0tP5+pH2CLput+MBLQT3IVQ43
ke5acJup5mrKKtWBxKnTcL1TGONG1eQheQ==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICCzCCAbGgAwIBAgIUbGotAqTfxkyKhuHFISJtwYZV+MEwCgYIKoZIzj0EAwIw
WzELMAkGA1UEBhMCc3MxCjAIBgNVBAgMAWQxCjAIBgNVBAcMAWYxCjAIBgNVBAoM
AWcxCjAIBgNVBAsMAWgxCjAIBgNVBAMMAWoxEDAOBgkqhkiG9w0BCQEWAWswHhcN
MjMxMjA3MTUzMzE3WhcNMjQxMjAxMTUzMzE3WjBbMQswCQYDVQQGEwJzczEKMAgG
A1UECAwBZDEKMAgGA1UEBwwBZjEKMAgGA1UECgwBZzEKMAgGA1UECwwBaDEKMAgG
A1UEAwwBajEQMA4GCSqGSIb3DQEJARYBazBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABF0g/liweS4NYrCcO4GFAq0jtbjmtLT+fqR9gi6brfjAS0E9yFUON5HuWnCb
qeZqyirVgcSp03C9UxjjRtXkIXmjUzBRMB0GA1UdDgQWBBT6WYEsLyfnaAJ5cKRp
taWG5A8+ozAfBgNVHSMEGDAWgBT6WYEsLyfnaAJ5cKRptaWG5A8+ozAPBgNVHRMB
Af8EBTADAQH/MAoGCCqGSM49BAMCA0gAMEUCIQCp3JQvjbruwO6gS46HQJWUNxyi
ry+YNkspiDC8hggoHwIgRp4AsFRTuChp72rUZj8K76c2HFzkLq+Y97dq3ipcibI=
-----END CERTIFICATE-----

Example to generate a proper rsa:2048 certificate.pem file with OpenSSL:

openssl req -newkey rsa:2048 -new -nodes -x509 -days 365 -keyout certificate.pem -out certificate.pem

Example to generate a proper prime256v1 certificate.pem file with OpenSSL:

openssl ecparam -name prime256v1 -genkey -noout -out certificate.key

openssl req -new -x509 -key certificate.key -out certificate.crt -days 365

cat certificate.key certificate.crt > certificate.pem

6.6 Board Pages

This chapter describes all pages that can be found in the aside component under the Boards Menu Item (see 5.3.2; Component 2). **All those pages have in common that they concern only one specific board.**

6.6.1 Board Overview

"Board Overview" is reached by pressing the "Board Name" component in the aside menu (see 5.3.2; Component 8). It consists of basic status information and reboot and factory reset action of the board.

6.6.1.1 General

6.6.1.1.1 Status

This page provides a section with all board status information and a section with the Device View (see 6.2.2), where the current board is highlighted. Clicking on a board other than the current one will lead to the status page of the board.

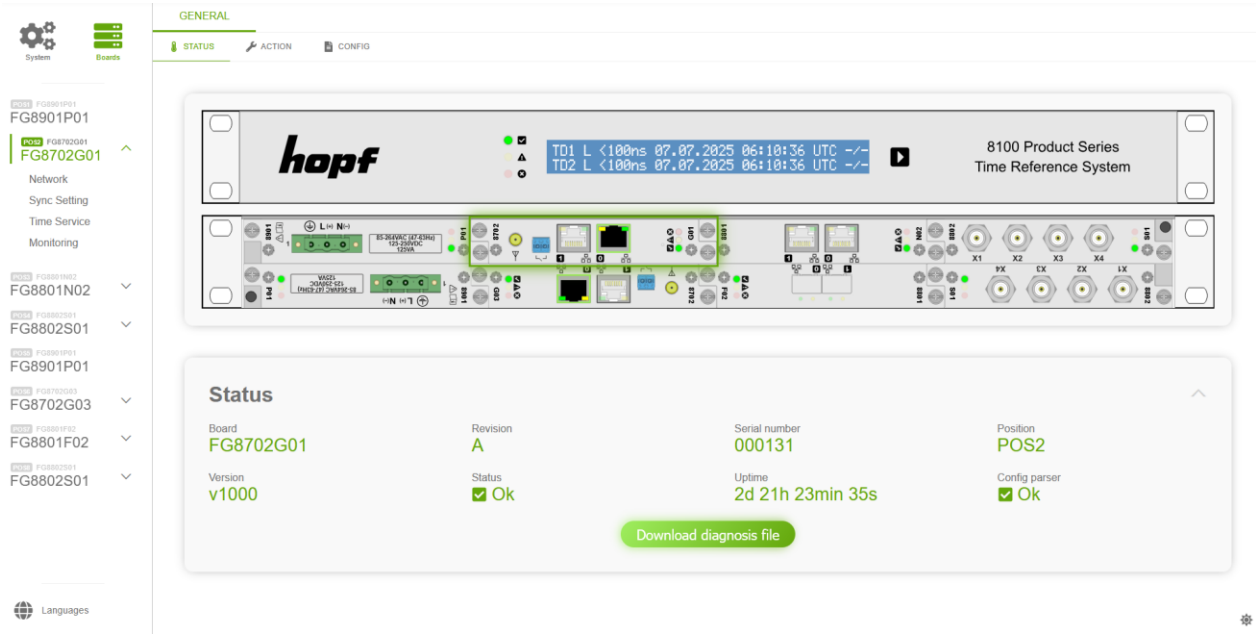


Figure 50 Board status overview example

Status Label	Description
Board	The exact product name.
Revision	Hardware device revision
Serial number	The serial number of the board.
Position	Position of the board in the system
Version	The software version of the board.
Status	It displays the current board status.
Uptime	Indicates how long the board has been in operation since the last restart.
Config parser	In case of an error, the config file could not be parsed correctly and the board is working with the default configuration.
Download diagnosis file	Pressing this button will download a diagnostic file that will assist the *hopf* service team in finding specific errors on the board.

6.6.1.1.2 Action

On this action page, the board can be rebooted or reset to factory settings.

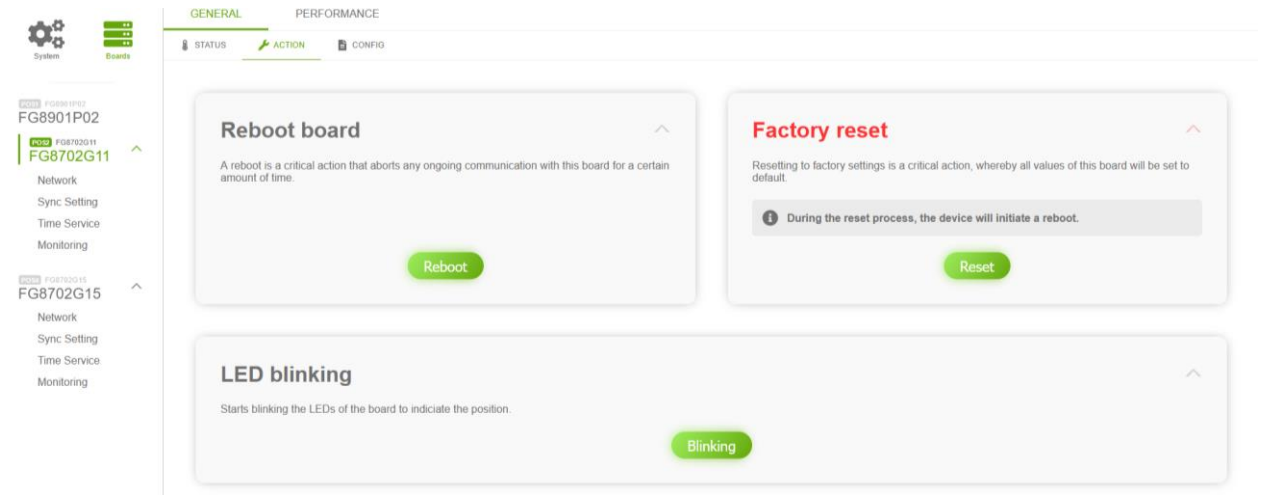


Figure 51 Board overview action example

With the Blinking button in the LED blinking section, you can send a trigger to the board, to start a blinking sequence on its panel LEDs.

6.6.1.1.3 Config

On this page, the displayed board name can be configured and the freeze functionality can be enabled.

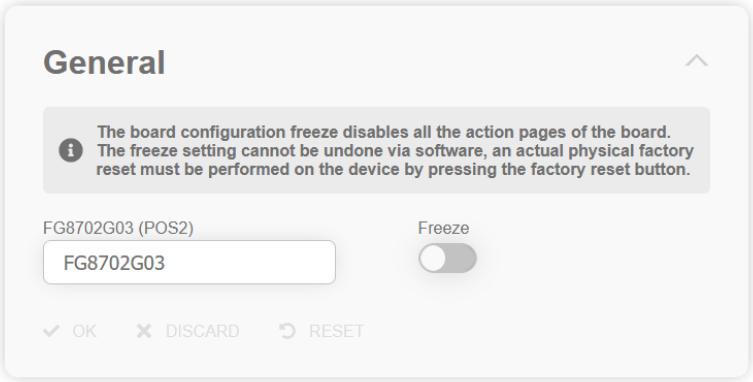


Figure 52 Example of a board general config page

The configured board name is used in the aside menu (see 5.3.2).

6.6.1.1.3.1 Freeze functionality

Boards can be frozen. This security feature is unique to ***hopf*** products. When activated for a board, the board will not accept actions from action pages (e.g., board reboot, configuration update). This means, that even if an attacker has access to the device (e.g., when he has stolen the password) or if he has compromised the management board of the device, he cannot make any changes to the frozen board. An attacker needs physical access to the board to deactivate the freeze functionality.

If the time domain controller board(s) and the service provider board(s) are all frozen, an attacker cannot compromise the time services of the service provider.

This setting cannot be undone via software, a physical factory reset must be performed on the board, for most boards via their front panel buttons or their dip switches.

When a board is frozen, a snowflake symbol is shown next to the "Board Name" component in the aside menu (see 5.3.2; Component 8).

Figure 53 Frozen board with the snowflake indication

6.6.1.2 Details

6.6.1.2.1 Status

This page contains board specific status information that do not fit into the pages, described in the following chapters.

Power supply units display their voltage, current and temperature status in a dedicated section.

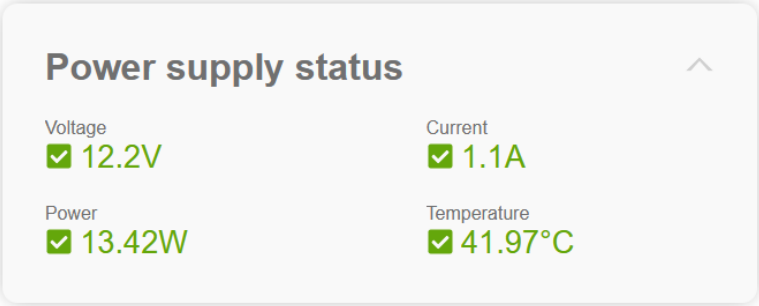


Figure 54 Example of detail status page content for a power supply unit

Boards operating an operating system display their CPU, flash and RAM usage in a performance and status section.

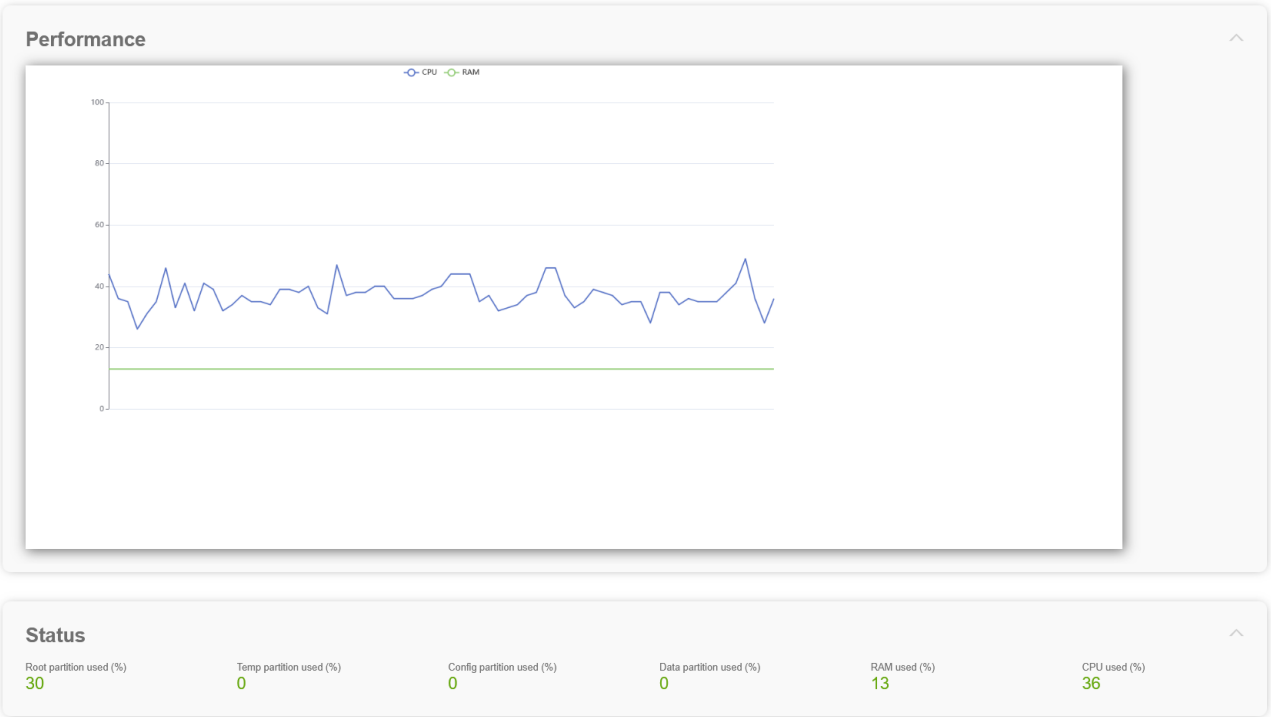


Figure 55 Example of a detail status page content for a board operating with an operating system

6.6.2 Network

Pages with network-specific functionalities are listed under this item.

6.6.2.1 General

6.6.2.1.1 Status

This page shows all certificates of the trust list

Figure 56 Example of the trusted certificates section

Trusted certificates are needed for RFC8915 (**N**etwork **T**ime **S**ecurity (short NTS) feature of NTP).

6.6.2.1.2 Action

The actions on this page can be used to add and remove certificates to / from the trust list.

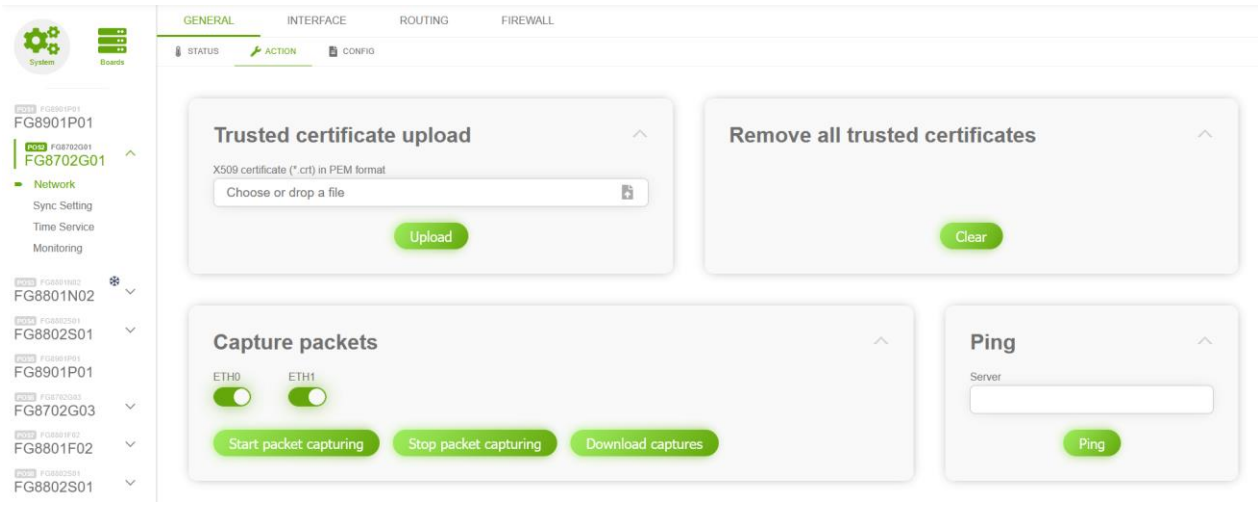


Figure 57 Network general action

The uploaded certificate via Trusted certificate upload must be a X509 certificate in PEM format.

Capture packets can be used to capture the network traffic of the device where the action has been triggered. Under normal operation this action is not needed, but in some support cases this action can help

to analyse the problem. In those cases, the *hopf* support team will request the capture.
The generated file is encrypted, to prevent information leaks during the transmission of the file to the *hopf* support team.

To capture the network packets, the corresponding interface(s) must be selected and afterwards the Start packet capturing button must be clicked. This action starts the capturing.

Afterwards the Stop packet capturing button must be clicked, to stop the capturing.

The last step is to click the Download captures button, to perform the download of the encrypted capture file. The download is only successful, when the capturing has been stopped.

The action has a maximum limit of packets that can be captured, to prevent the creation of captures that fill up the whole RAM.

The ping action can be used to check reachability of other network devices. The IPv4 or IPv6 address of the device that should be pinged must be entered in the Server text field and afterwards the Ping button must be clicked. A toast in the bottom right corner will show the result of the ping.

Figure 58 Possible ping action toasts

6.6.2.1.3 Config

The general network configuration can be set here. Both IPv4 and IPv6 addresses can be entered.

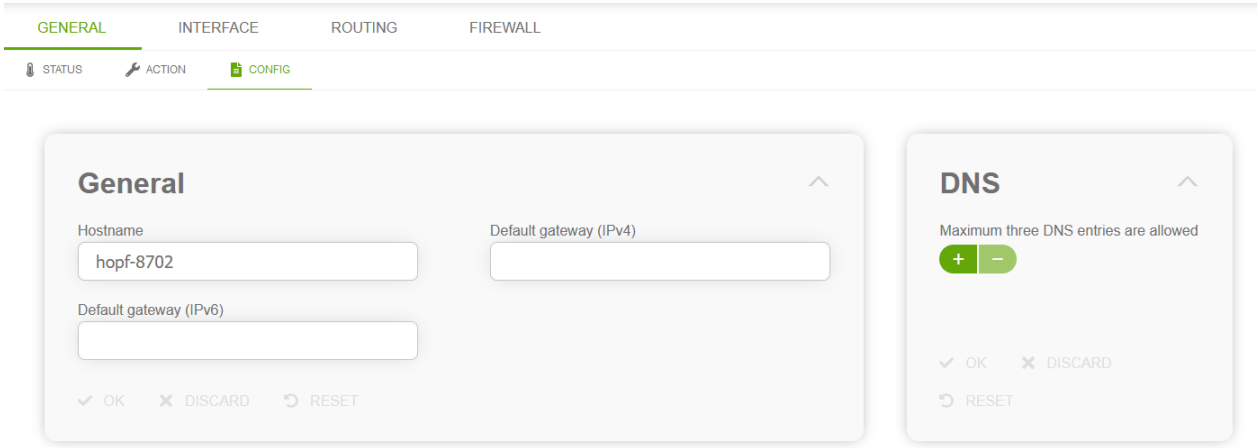


Figure 59 Example of general network settings

Input Label	Description
Hostname	This setting changes the hostname.
Default gateway (IPv4)	This setting changes the IPv4 default gateway.
Default gateway (IPv6)	This setting changes the IPv6 default gateway.
DNS <NUMBER>	The IP address (IPv4 or IPv6) of the DNS server should be entered if you wish to use the Fully-Qualified Host Name (hostname.domainname) or work with reverse lookup.

	Label	Description
1	DNS Stepper	Pressing the plus button will add an DNS input and pressing the minus will remove the last DNS input. A maximum of three DNS are allowed.

6.6.2.2 Interface

6.6.2.2.1 Status

This status page shows whether a particular interface is in use (up) or not (down) as well as the corresponding MAC address, speed, duplex mode, auto-negotiation mode and packet counters.

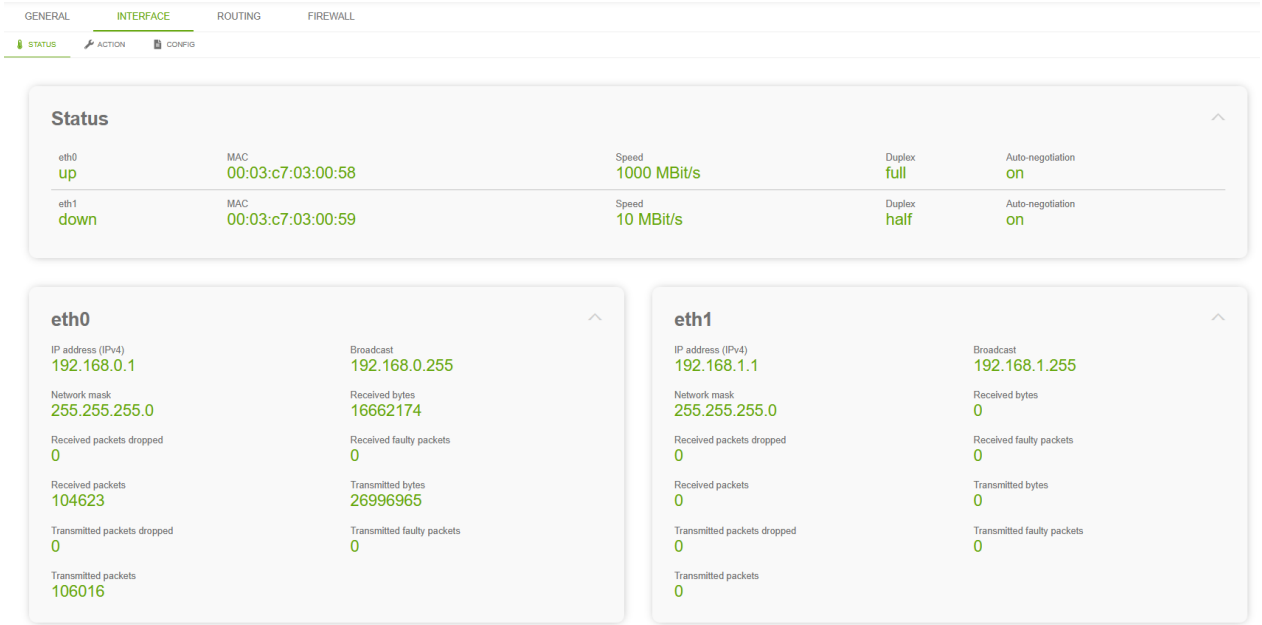


Figure 60 Example of network status page content

6.6.2.2.2 Action

The packet counters on the status page can be cleared with the Clear network interface status data action.

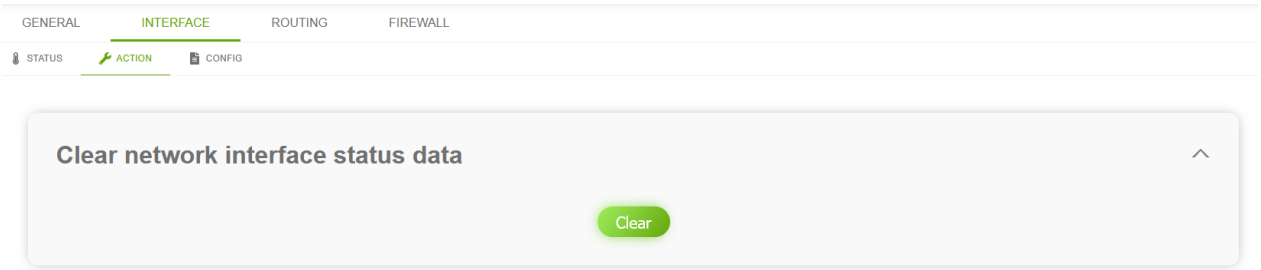


Figure 61 Clear network interface status data action

6.6.2.2.3 Config

This config page consists of the sections "Interface", "Bonding" and "PRP".

6.6.2.2.3.1 Interface

All of the interfaces are listed under the interface section. Each interface has the same settings, respectively IPv4, IPv6, MAC and VLAN.

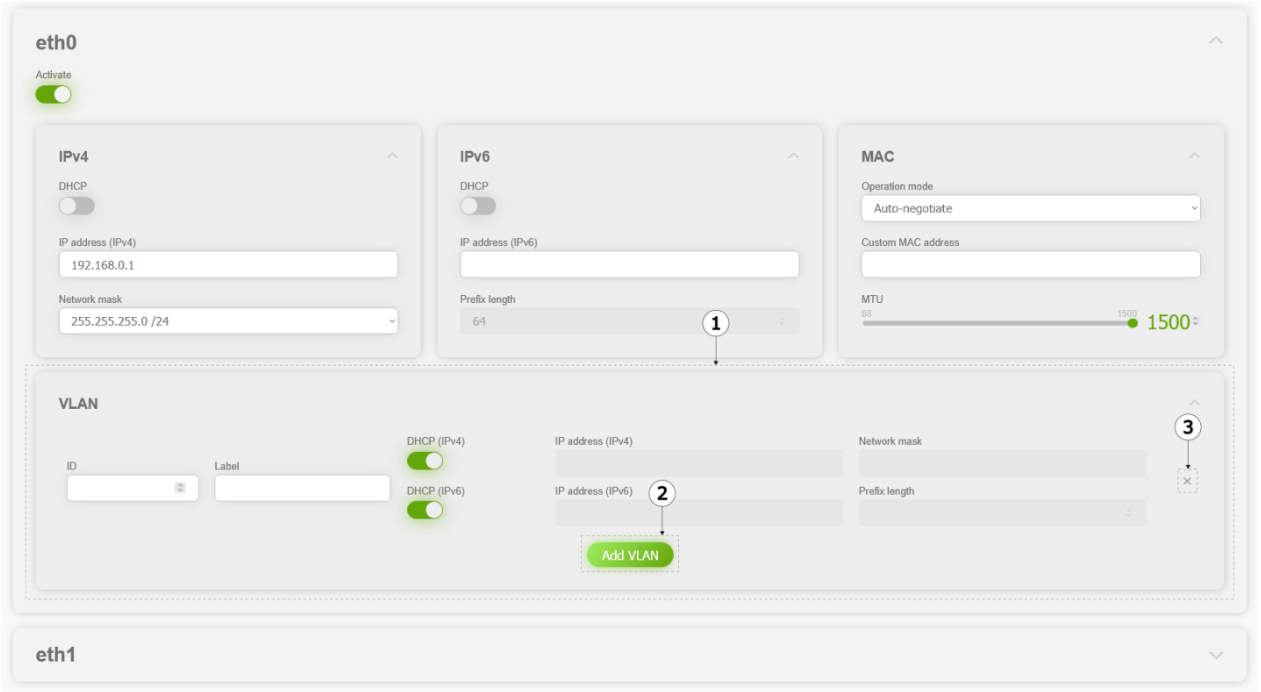


Figure 62 Example of a network interface configuration section

Input Label	Description
Activate	Enables / disables the whole network interface. This setting is ignored when the network interface is used in bonding or PRP.
DHCP	This setting toggles DHCP for a certain settings group (IPv4, IPv6, VLAN IPv4 and VLAN IPv6).
IP address (IPv4)	If DHCP is not used for IPv4, the IPv4 address needs to be entered here.
Network mask	If DHCP is not used for IPv4, the network mask needs to be entered here.
IP address (IPv6)	If DHCP is not used for IPv6, the IPv6 address can be entered here. IPv6 address is not mandatory and can be left empty.
Prefix length	If DHCP is not used for IPv6, the length of the network address for IPv6 must be entered here, if the IPv6 address is set.
Operation mode	The network device usually adjusts the data stream and duplex mode to the device to which it is connected (e.g., HUB, SWITCH) automatically. If the network device requires a certain speed or duplex mode, this can be configured via this setting. The value should only be changed in special cases. The automatic setting (Auto negotiate) is normally used. For boards with SFP modules the "Auto-detect" option is supported. When this option is selected, the supported operation mode of the inserted SFP module is determined and then that operation mode is configured for the corresponding interface.
Custom MAC address	The MAC address assigned from *hopf* can be changed to any user-defined MAC address. The interface identifies itself with the user-defined MAC address to the network if a Custom MAC address was entered. If the input field value is empty, the MAC address provided by *hopf* is used.
MTU	The Maximum Transmission Unit describes the maximum size of a data packet of a protocol of the network layer (layer 3 of OSI model), measured in octets which can be transferred into the frame of a net of the security layer (layer 2 of OSI model) without fragmentation.
ID	An explicit VLAN ID must be configured for each VLAN interface.
Label	This input can be filled out with a designation or a comment to easily keep the configured VLANs apart.

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

6.6.2.2.3.2 Bonding

The feature Bonding (also known as NIC Bonding, NIC Teaming, Link Bundling, EtherChannel) enables to bundle two or more physical network interfaces to one logical network interface. Only the interfaces of one board can be used for bonding.

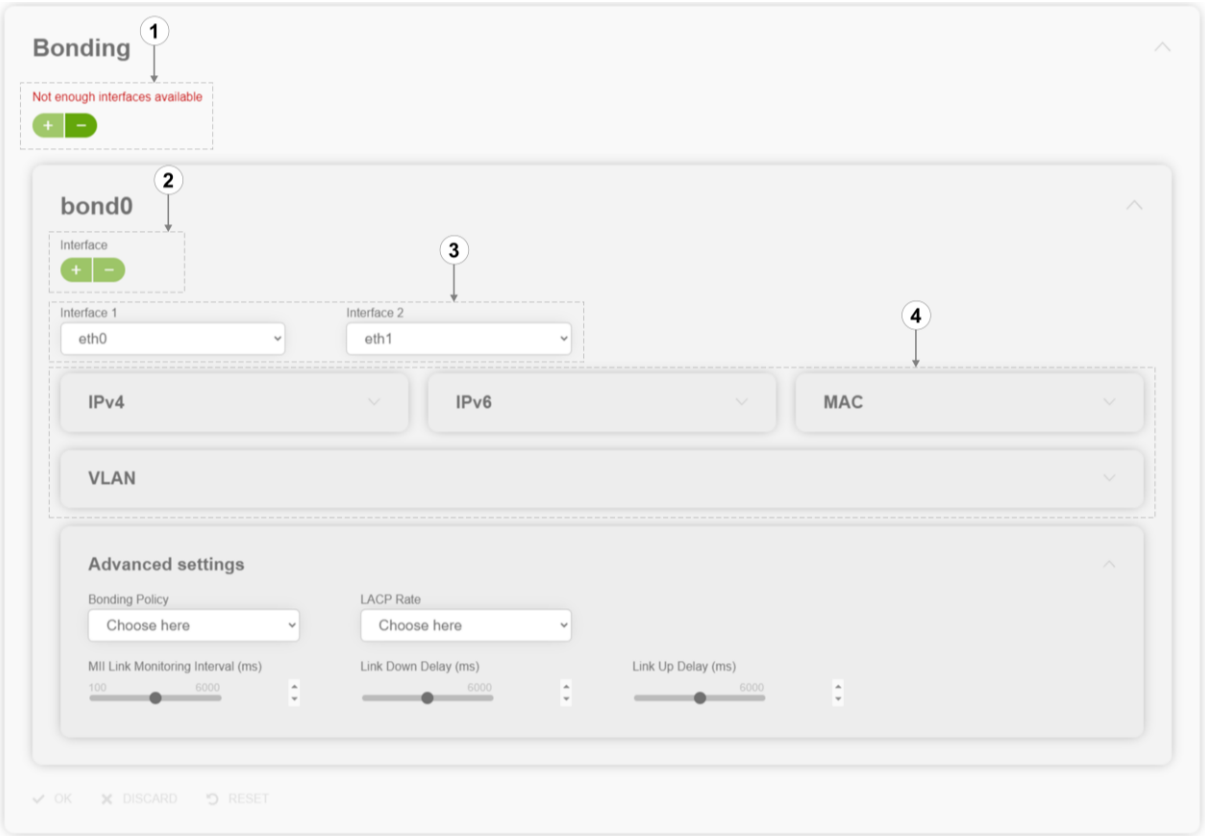


Figure 63 Network interface bonding configuration section

	Label	Description
1	Bonding Stepper	Pressing the plus button will create a new Bonding Interface and pressing the minus button will remove the last Bonding Interface. Adding a new Bonding Interface requires a minimum of two available interfaces.
2	Interface Stepper	Each Bonding Interface must have at least two interfaces. Additional interfaces can be added with the Interface Stepper. It adds or removes a Bonding Interface Selector (3).
3	Bonding Interface Selectors	Each selector allows choosing a specific interface for the Bonding Interface.
4	Bonding Interface Settings	Each bonding interface consists of the same interface settings described in this chapter under "Interface" (IPv4, IPv6, MAC, VLAN).

A bonding interface additionally includes the "Advanced settings" section with new input components, which are described below:

Input Label	Description
Bonding policy	Round-Robin In this case the network interfaces, starting with ETH0, are transmitting sequentially whereby a distribution of load and a higher tolerance for errors are achieved. In that mode the network interfaces must be connected to the same network switch. Active Backup Only one of the network interfaces is sending and receiving. If an error occurs, the other network interface assumes responsibility for the process. The network interfaces do not have to be connected to the same network switch. From the outside the MAC address of the association is only visible on one network interface to avoid a mix-up. This mode supports tolerance for errors. Balance XOR Source and target are permanently assigned with one another via the MAC address of the network interfaces. The network interfaces must be connected to the same network switch. This mode supports distribution of load and tolerance for errors. Broadcast In this mode the computer sends its data via all available network interfaces which enables the use of several network switches. This fact leads to a high tolerance for errors, but this mode does not enable distribution of load. IEEE 802.3ad Dynamic Link Aggregation

	The network interfaces are going to be bundled (Trunking) in this mode. It is mandatory that the network interfaces are configured with the same transmission rate and duplex setting. Bundling is made dynamically via the Link Aggregation Control Protocol (LACP). This mode supports distribution of load as well as tolerance for errors. Adaptive Transmit Load Balancing (TLB) Outbound data traffic is split on the network interfaces in accordance with the current load, depending on the interface speed adjusted. The network interfaces do not have to be connected on the same network switch. This mode supports distribution of load and tolerance for errors.
LACP rate	Indicates the link partner's request frequency to transfer LACP packets in IEEE 802.3ad mode.
MII link monitoring interval (ms)	Indicates the interval in milliseconds for observing the MII-connection.
Link down delay (ms)	Determines the delay time in milliseconds to deactivate a connection after a link error is detected. This value needs to be a multiple of the MII link monitoring interval.
Link up delay (ms)	Determines the delay time in milliseconds to enable a conjunction after a connection is detected. This value needs to be a multiple of the MII link monitoring interval.

6.6.2.2.3.3 PRP

The feature PRP (Parallel Redundancy Protocol) enables to bundle two physical network interfaces to one logical network interface. Each network interface is connected to an independent LAN (Local Area Network). If one of the two LANs has got a failure, usage of PRP ensures that no network packet is lost and the connection is maintained via the other independent LAN.

The PRP settings are similar to "Bonding". Only the number of interfaces is fixed to two for each PRP interface and there are no advanced settings nor VLAN.

Figure 64 PRP configuration section

6.6.2.3 Routing

6.6.2.3.1 Status

The routing status shows all currently set routes by the user and the operating system.

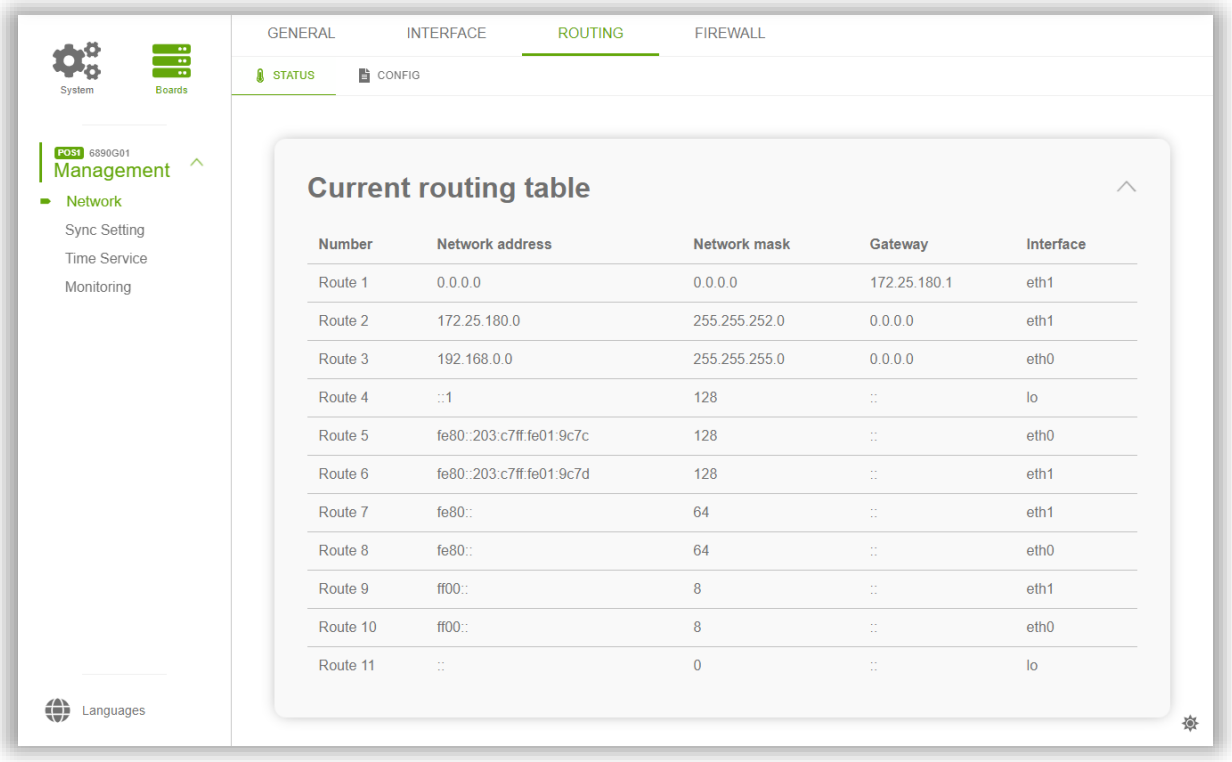


Figure 65 Routing status page example

6.6.2.3.2 Config

Additional static routes can be configured through this config page. It displays all current static routes set by the user.

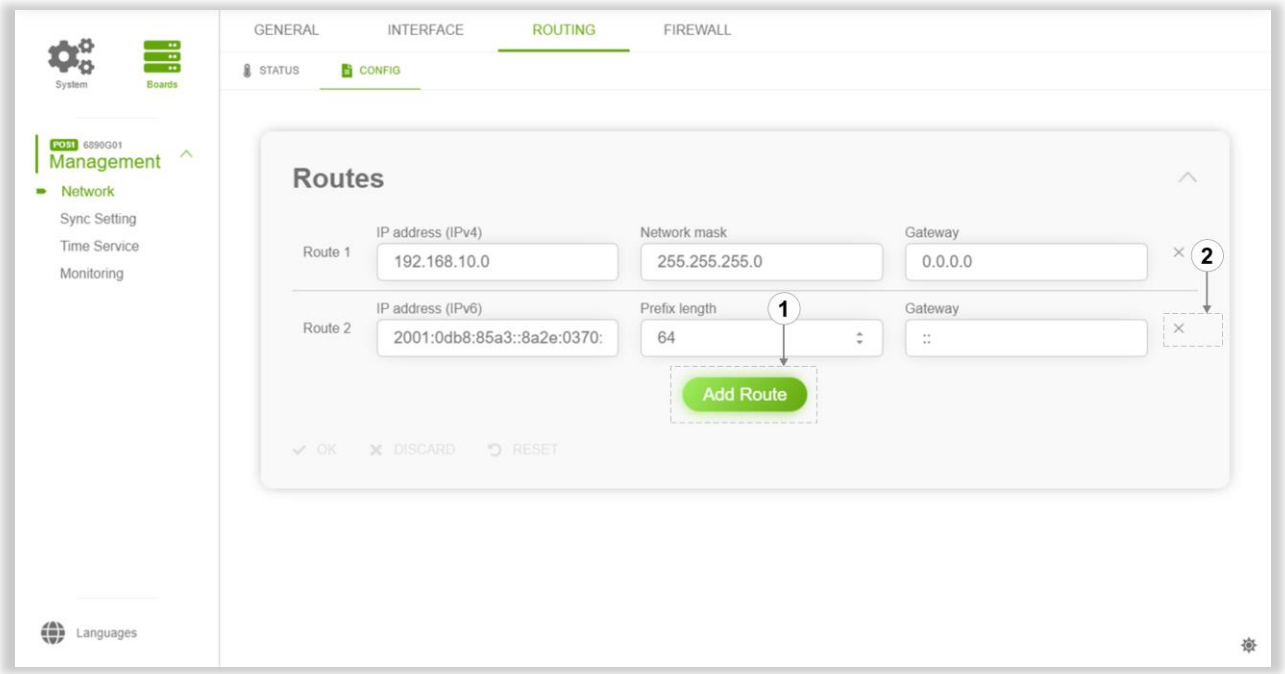


Figure 66 Routing config page with two routes

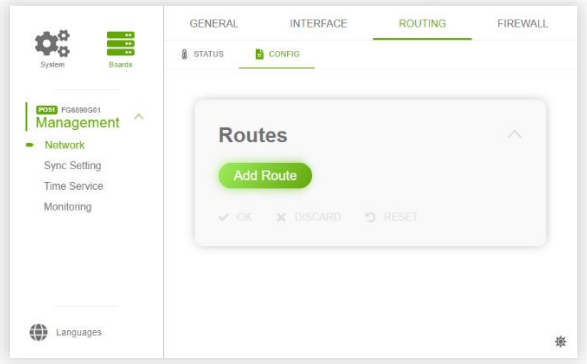


Figure 67 Routing config page without any routes

	Label	Description
1	Add Route	Pressing this button will add a new route.
2	Delete Button	Pressing this button will remove a route.

Input Label	Description
IP address	This input field allows entering both an IPv4 address and IPv6 address. The detected IP version will change this input label and also the following input components.
Network mask	**If an IPv4 address was entered, this network mask is displayed.**
Prefix length	**If an IPv6 address was entered, this prefix length is displayed.**
Gateway	If an IPv4 address has been entered, the gateway must also be an IPv4 address; for IPv6 it must be an IPv6 address.

6.6.2.4 Firewall

6.6.2.4.1 Config

This configuration page allows you to change the firewall and the firewall alarm options. Firewall rules can be added, removed and changed.

One rule that blocks any traffic is predefined. It has the lowest priority and can't be deleted.

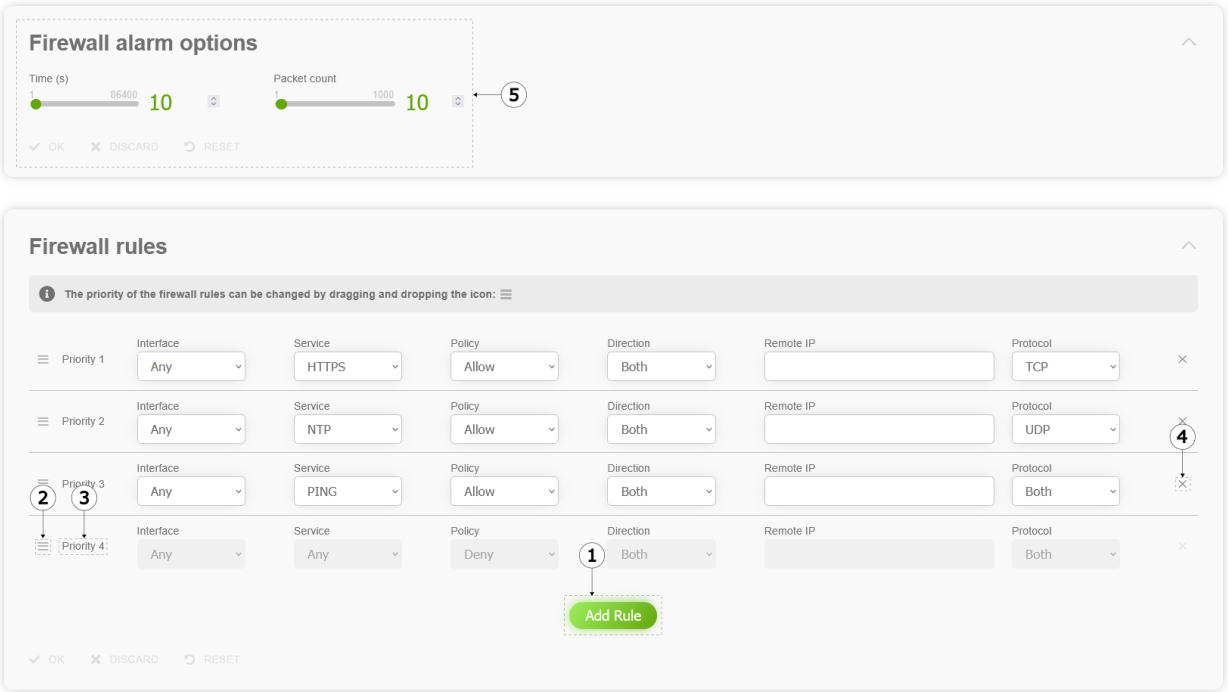


Figure 68 Network firewall configuration section

	Label	Description
1	Add Rule	Pressing this button will add a new rule.
2	Priority Dragger	A firewall rule has priority over another rule if the priority is placed higher in the list. Changing the priority can be done using this dragger component. Holding this icon with the left mouse button, allows dragging the rule to a desired priority position.
3	Priority Number	Indicates the priority of a rule (lower numbers have higher priorities). The lower the priority number, the higher the priority (for example a rule with "Priority 1" has the highest priority).
4	Delete Button	Pressing this button will remove a rule.
5	Firewall alarm options	This section configures the parameters for the firewall alarm. To trigger an alarm at least Packet count packets must be dropped by the firewall during a Time (s) interval. **Hint:** Time (s) unit is seconds.

Input Label	Description
Interface	This setting determines which interface (including VLAN, Bonding and PRP) this firewall rule applies to.
Service	The service where this firewall rule takes effect.
Policy	The Policy field determines whether the rule permits or blocks traffic that matches the criteria specified in this rule.
Directions	Traffic can be matched to in[coming], out[going] or both directions.
Remote IP	Remote IP address that is permitted to access the internal resource. IPv4/IPv6 address (e.g. 192.168.0.1, 1::1) or IPv4/IPv6 address ranges in CIDR notation (e.g. 192.168.0.1/24, 1::1/64) are accepted. Allowed IPv4 prefix length value in CIDR notation: 1 to 32 Allowed IPv6 prefix length value in CIDR notation: 1 to 128 Only one IPv4/IPv6 address or IPv4/IPv6 address range is accepted. When a firewall rule should be applied for more than one IPv4/IPv6 address or IPv4/IPv6 address range, an additional rule must be added.
Protocol	In the Protocol field, TCP traffic, UDP traffic or both can be specified.

6.6.3 Sync Setting

"Sync Settings" summarizes all pages focusing on synchronization sources.

6.6.3.1 General

6.6.3.1.1 Status

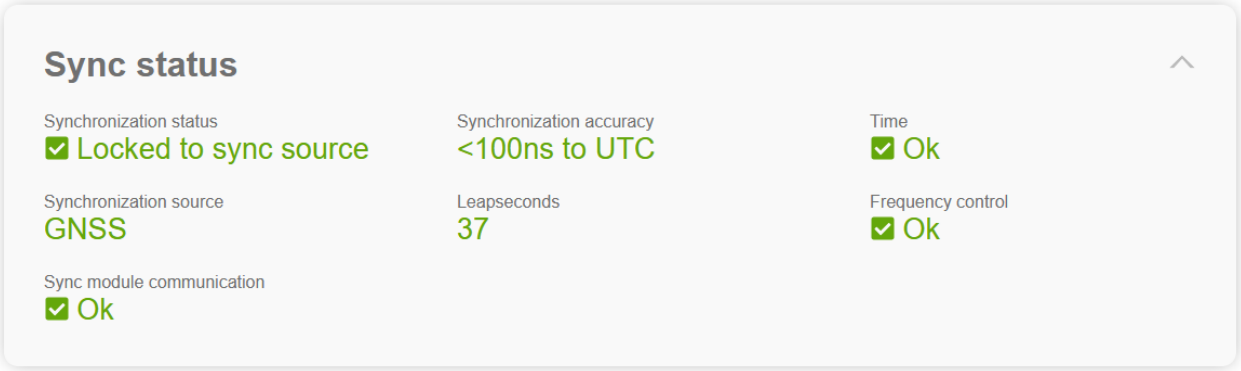


Figure 69 Example of the general synchronization status page

Status Label	Description
Synchronization status	It displays the current synchronization status. Not initialized – The device has never been synced to a sync source or the communication to the sync module is lost Crystal mode – The device has lost the sync source and is now running in free wheel mode using the internal oscillator Locked to sync source – The device is locked to a sync source
Synchronization accuracy	Device time is within: >= 10 ms to UTC < 10 ms to UTC < 1 ms to UTC < 100 us to UTC < 10 us to UTC < 1 us to UTC < 100 ns to UTC
Time	Is only used in Crystal mode state, in all other states it can be ignored. Error – When Synchronization status is "Crystal mode" and Synchronization source is not "-" Time status Error indicates, that the internal clock has an offset greater 1s to the synchronization source. It follows that the synchronization source is ignored. In that case the Execute time jump action described in 6.6.3.1.2 must be performed to accept the synchronization source. In other cases, this value can be ignored. Ok – Indicates, that the above-described scenario is not active

Synchronization source	It displays the current synchronization source. - – Indicates that no synchronization source is present <>– Indicates that the synchronization source is changing In every other case the name of the synchronization source is displayed
Leap seconds	Number of leap seconds (this equals the difference between TAI and UTC time base) The value 32767 indicates, that the number of leap seconds is not known (e.g. when a sync source is used, which does not transmit the number of leap seconds, like NTP, and the number of leap seconds has not been received or set before switching to this sync source)
Frequency control	In case of an error a problem with the internal oscillator regulation of the Sync Source have occurred. The specified accuracy of the Sync Source cannot be guaranteed anymore.
Sync module communication	Displays the communication status to the synchronization module.

6.6.3.1.2 Action

This page enables the adjustment of UTC time including the date in the Sync Source.

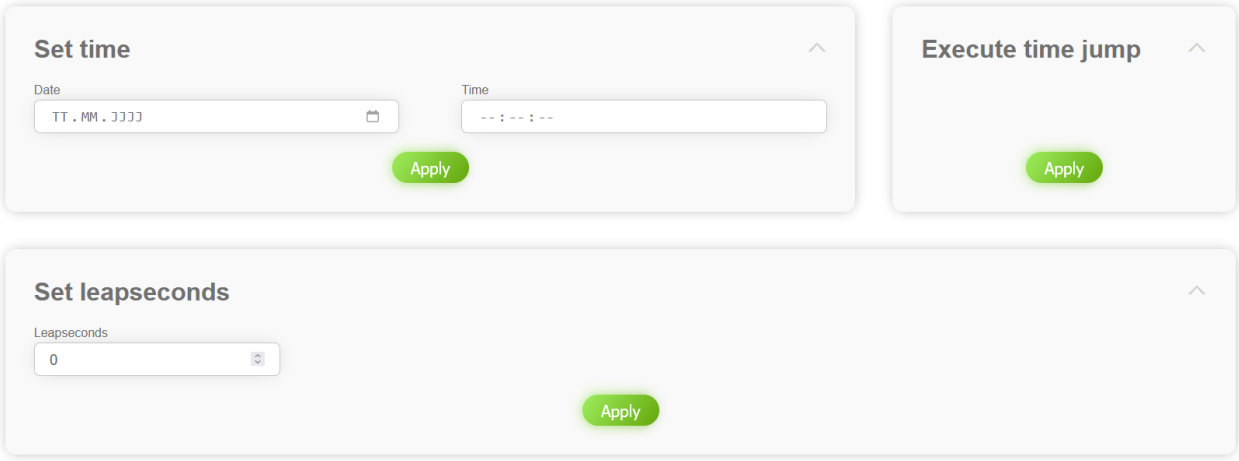


Figure 70 General synchronization action page

Set time (only available on TDC boards):

Via Set time the time of the board can be set.

The UTC time must always be set. The local time is internally calculated by the device based on the difference time (timezone offset) and the summer / winter time changeover (daylight saving time).

Clicking on the field date opens a browser-specific calendar; clicking on the field time opens a browser-specific time selector (if the used browser offers this functionality).

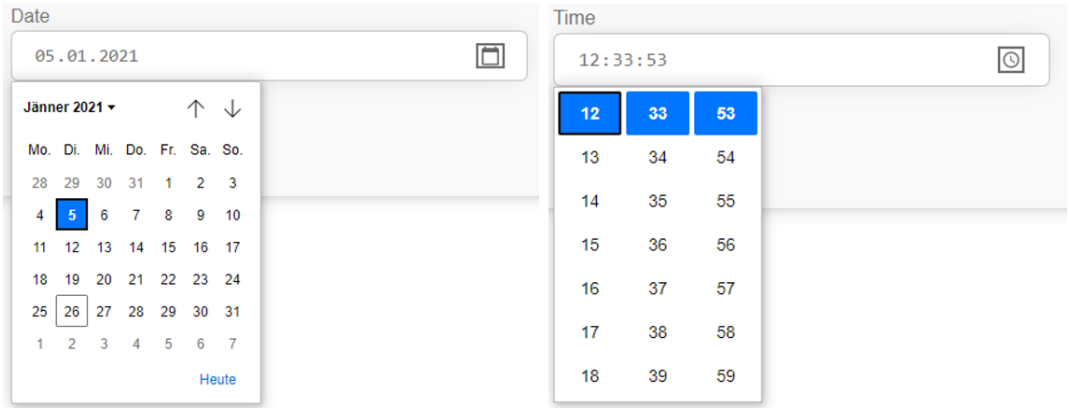


Figure 71 The calendar and time selector provided by Google Chrome

Execute time jump:

This function forces the board to go to Synchronization status Not initialized. That state is the only state in which boards are allowed to perform time jumps.

This action can solve issues when the board does not synchronize.

Set leapseconds (only available on TDC boards):

Via Set leapseconds, the number of leap seconds can be set. This action has only an effect, when a sync source is used, that does not transmit the number of leap seconds, like NTP.

6.6.3.1.3 Config

This config page consists of several sections.

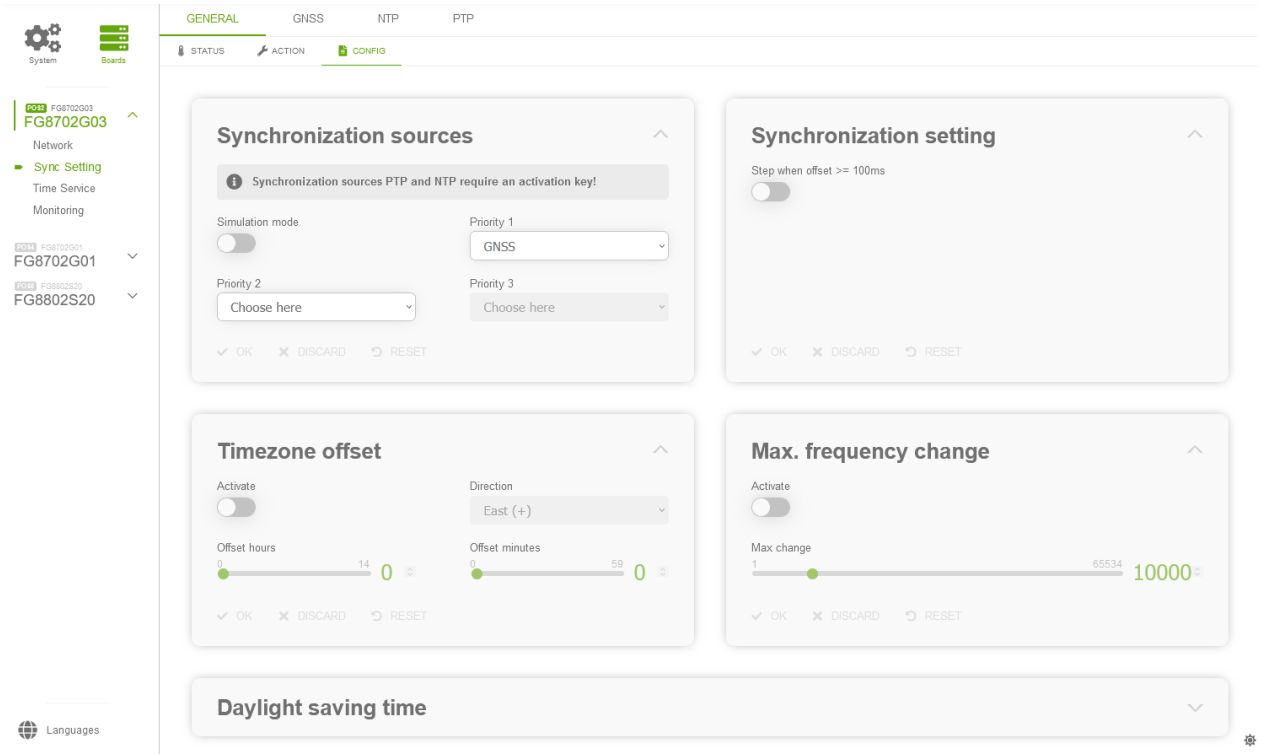


Figure 72 General synchronization configuration page

Synchronization sources for TDC boards

If multiple synchronization sources are supported by the board, the sources that should be used must be configured here, with the desired priorities. The lower the priority number (e.g., Priority 1), the higher the priority. Synchronization sources that should be completely ignored can be deselected with a delete button next to the drop-down selector. At least one sync source must be selected as Priority 1.

This section also provides a setting to turn simulation mode on and off. When simulation mode is turned on, the system will act as if it would be synchronized to a perfect time source (offset to UTC will always be <100ns). The time that is distributed in simulation mode can be set using the set time function (see 6.6.3.1.2).

Notice: To use the simulation mode, unplug all sync sources from the device.

Synchronization sources for non-TDC boards

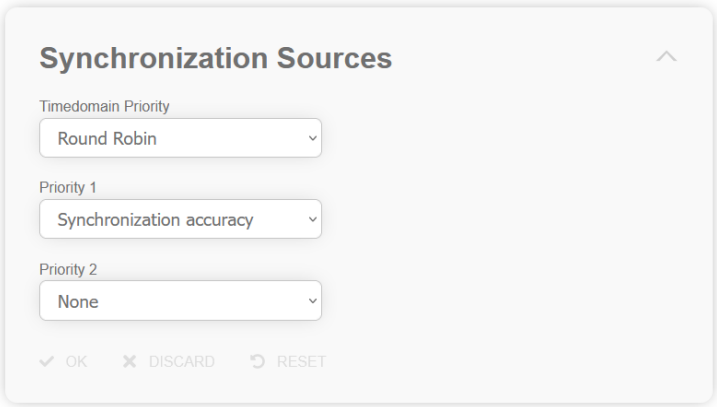


Figure 73 Synchronization sources section for non-TDC boards

The synchronization sources section for non-TDC boards looks different to the one of TDC boards. The non-TDC-boards version has three drop downs for timedomain priority, priority 1 and priority 2 to configure which timedomain should be used for synchronization in systems with more than one timedomain.

Timedomain priority defines which timedomains should be validated and what should happen if they have the same quality.

Priority 1 and priority 2 define how the quality of the timedomains is determined. Priority 1 has higher priority than priority 2.

Timedomain priority selection	**Description**
Only TD1	The board will ignore timedomain 2 and only synchronize to timedomain 1
Only TD2	The board will ignore timedomain 1 and only synchronize to timedomain 2
Round Robin	The timedomain with the higher quality will be selected as synchronization source. If both timedomains have the same quality, the actually used timedomain will stay the selected one.
Priority TD1	The timedomain with the higher quality will be selected as synchronization source. If both timedomains have the same quality, timedomain 1 will be selected.
Priority TD2	The timedomain with the higher quality will be selected as synchronization source. If both timedomains have the same quality, timedomain 2 will be selected.

Priority x selection	Description
Synchronization accuracy	The timedomain with the better synchronization accuracy is treated as the one with better quality.
Synchronization status	The timedomain with better synchronization status is treated as the one with better quality.
None	Both timedomains have the same quality for this priority (if priority 1 and 2 are set to None, TD1 is selected as timedomain with the best quality)

Synchronization setting

Input Label	Description
Step when offset >= 100ms	When enabled, the internal clock is allowed to perform time steps when the offset to the synchronization source is greater 100ms.

Warning: this functionality should only be enabled, while testing or in rare cases where no synchronization sources are available after booting, but time services are needed and time inaccuracy of more than 100ms to UTC does not matter because it is only needed, that clients within the application are synchronized to each other, but not to UTC, but when a synchronization source is available the time should be stepped towards UTC. In such a case it is possible to set the time via the Set time action (see 6.6.3.1.2). When a synchronization source is available the board will perform a step towards the time of the synchronization source, when this flag is enabled. In that case the flag should be enabled on every board of the system. Keep in mind, that that flag also makes the application vulnerable for spoofing attacks or unstable synchronization sources. If the application in the above scenario is only synchronized via PTP, it is better to enable the Immediate service start feature of PTP (see 6.6.4.3.2).

Timezone Offset (only available on TDC boards)

This section offers Local Time settings for the Sync Source. Time services that can be configured to output STD or LOC and that do not have their own Local Time settings, use the settings from this section for time calculation. Changing the time here will not influence the header component "Device Time Output" (see 5.3.1; Component 6).

Input Label	Description
Activate	The timezone offset can be turned on or off.
Direction	The direction, where the time deviates from the world time. East – Corresponds to east West – Corresponds to west of the Prime-Meridian (Greenwich)
Offset hours	Timezone offset input of the full hour (0-13)
Offset minutes	Timezone offset input of minutes (0-59)

Daylight saving time (only available on TDC boards)

Setting of the changeover times for summer/winter time in the Sync Source.

This section is used to define the point of time at which the changeover to Daylight Saving Time or winter time occurs during the course of the year. The exact times are automatically calculated for the running year.

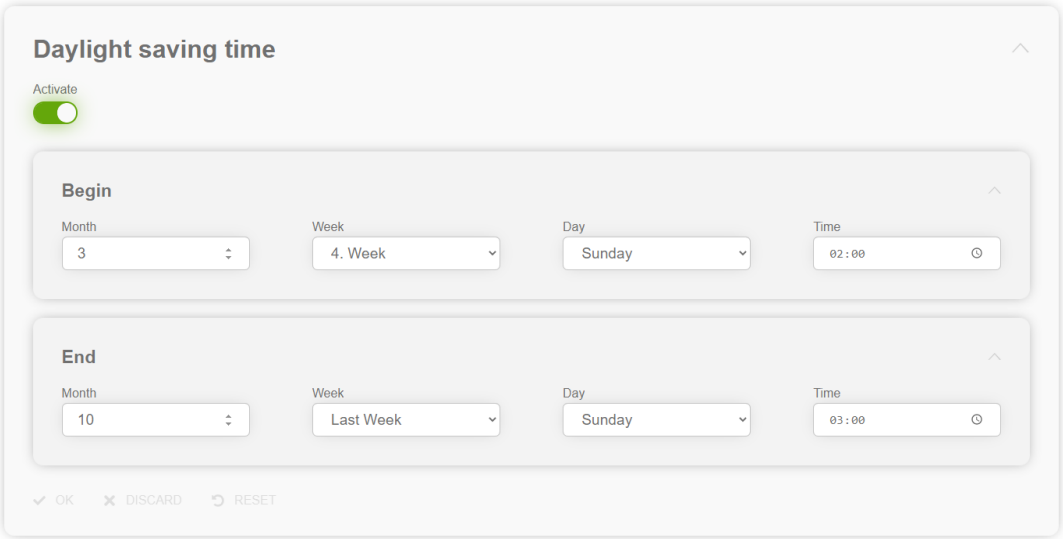


Figure 74 Daylight saving time configuration section

Begin – Changeover time for standard time to Daylight Saving Time

End – Changeover time for Daylight Saving Time to standard time

Input Label	Description
Month	The month when the changeover should be processed.
Week	At which occurrence of that particular weekday in that month the changeover is going to take place.
Day	The day of the week when the changeover should be processed.
Time	The time in hours and minutes when the changeover should be processed. The LOC (Local time) time must be set in the time input field.

Max. frequency change

Via this section a maximum frequency change of the boards clock can be configured. It only takes effect, when the internal clock is in synchronization status Locked to sync source or Crystal mode.

To enable this functionality, Activate must be turned on and the Max change value must be set. To disable this functionality, Activate must be turned off.

Attention: don't use a too small value, because otherwise the clock controller gets instable. The smallest value suitable for synchronization via GNSS is 100.

6.6.3.2 GNSS

All pages that concern the sync source GNSS can be found under this item.

6.6.3.2.1 Status

This status page is composed of sections with detailed information about the GNSS sync source.

Reception quality

This section contains a readout for the satellites in view and for the satellites being tracked.

The satellites in view represent the number of theoretical available satellites detected by the GNSS receiver and the tracked satellites are the effective number of received satellites used for synchronization.

The reception quality of the tracked satellites is visualized with a dynamic graph and it shows the C/N0 (carrier-to-noise-density ratio) in dBHz. A low signal quality (red) is between 0-30, a sufficient one (orange) between 31-40 and a good one (green) between 41-60.

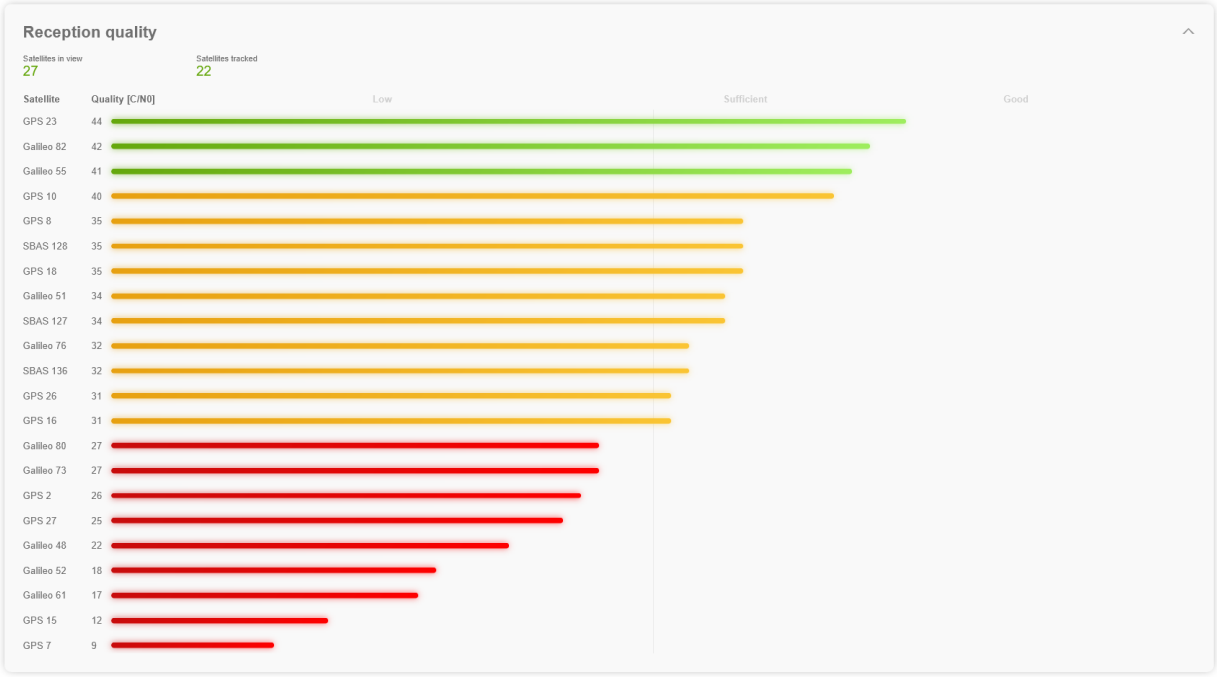


Figure 75 Example of the GNSS reception quality status section

GNSS receiver

This section consists of status outputs concerning the receiver.

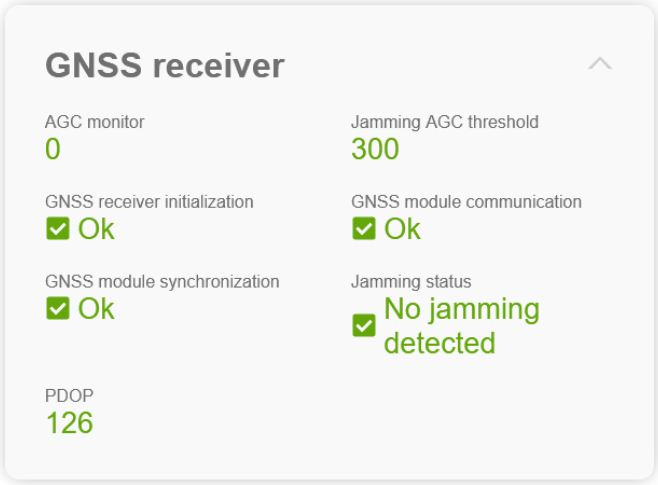


Figure 76 Example of the GNSS receiver status section

Status Label	Description
AGC monitor	Automatic gain control regulation value (0 to 8191).

Jamming AGC threshold	Threshold used for jamming detection. If the AGC monitor value is constant above this value, Jamming is indicated. The jamming AGC threshold is automatically calculated. At start up the value is 65535, what indicates, that the jamming detector has not calculated the threshold
GNSS receiver initialization	If the GNSS receiver is initialized, "Ok" is displayed, otherwise "Error" is displayed. This condition might last for max. 1 minute after particular actions.
GNSS module communication	If this error occurs even after a Power-Reset, the support team of ***hopf*** needs to be contacted for further actions.
GNSS module synchronization	If an error is indicated, the GNSS receiver requires special data from the GNSS signal for which it needs up to 13 minutes signal reception of satellites. Only then the Sync Source can be synchronized. This happens e.g., after a board reboot.
Jamming status	Initializing – The jamming AGC threshold has not been calculated yet No jamming detected – no significant jamming Jamming detected – interference visible, if GNSS firewall is enabled, the GNSS sync source will be ignored.
PDOP	Position dilution of precision (0 to 65535; smaller number means higher precision).

Antenna

Display of the actual position calculated by the GNSS receiver and the antenna short- / open-circuit detector status.

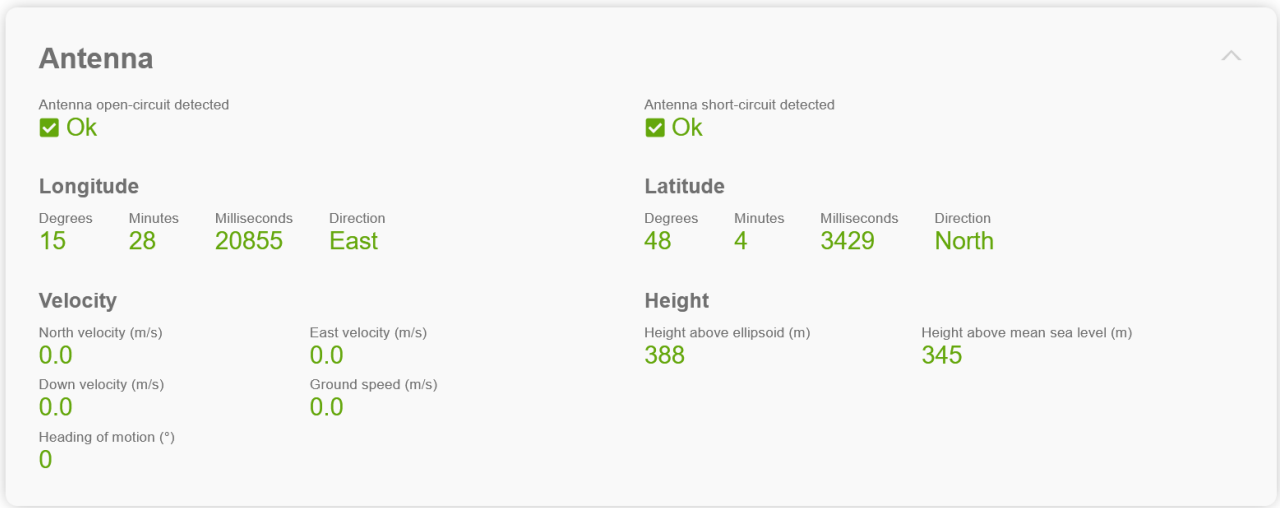


Figure 77 Example of the GNSS antenna status section

Status Label	Description
Antenna circuit-shorted detector	In case of an error the Sync Source has detected a short circuit in the antenna system. **The antenna system should be checked.**
Antenna open-circuit detector	In case of an error the Sync Source has detected an open antenna input. **The antenna system should be checked.** The antenna cable could have a break or simply not be plugged in.
Longitude / Latitude	Display of the actual position calculated by the GNSS receiver.
Velocity	Displays the actual velocity of the antenna in different formats.
Height	Displays the height of the antenna.

Security
Displays the GNSS firewall status.

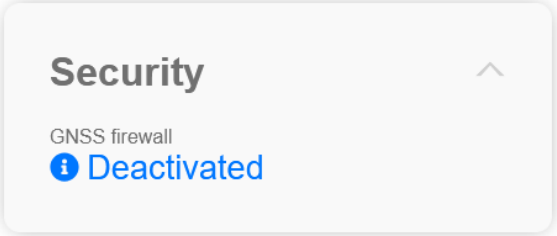
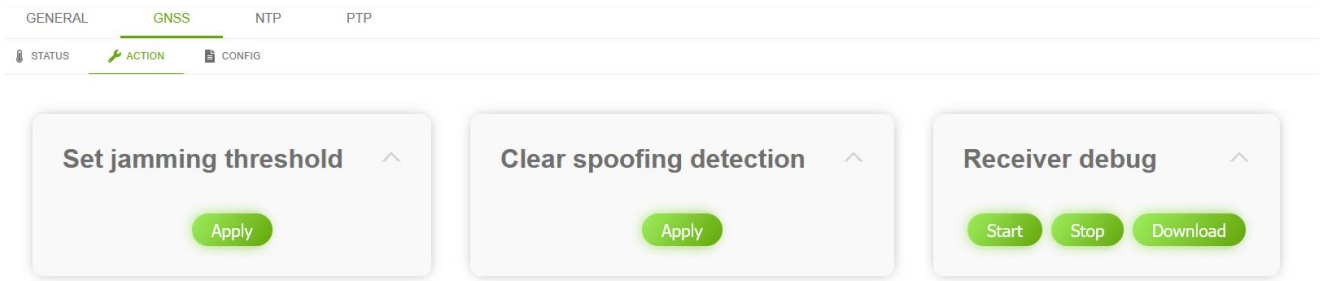


Figure 78 Example of the GNSS security status section

Status Label	Description
GNSS firewall	Deactivated – Indicates, that the GNSS firewall is disabled Initializing – Indicates, that the GNSS firewall is not fully initialized No spoofing detected – Indicates, that no spoofing has been detected Spoofing detected – Indicates, that spoofing has been detected. GNSS sync source will be ignored

6.6.3.2.2 Action

This page contains actions related to the GNSS reception.



Set jamming threshold:

The jamming detected flag can be cleared with this action, after the detection of a jamming-attack.

Clear spoofing detection:a

The spoofing detected flag can be cleared with this action, after the detection of a spoofing-attack.

Receiver debug:

This section can be used to record the communication between the processor and the GNSS receiver. Under normal operation this action is not needed, but in some support cases this action can help to analyse the problem. In those cases, the ***hopf*** support team will request the capture.
The generated file is encrypted, to prevent information leaks during the transmission of the file to the ***hopf*** support team.

To record the communication between the processor and the GNSS receiver the Start button must be clicked. This action starts the recording.

Afterwards the Stop button must be clicked, to stop the capturing.

The last step is to click the Download button, to perform the download of the encrypted record file. The download is only successful, when the recording has been stopped.

The action has a maximum size for the record file, to prevent the creation of a record that allocates the whole memory.

6.6.3.2.3 Config

On this page the configuration settings of the sync source GNSS can be changed.

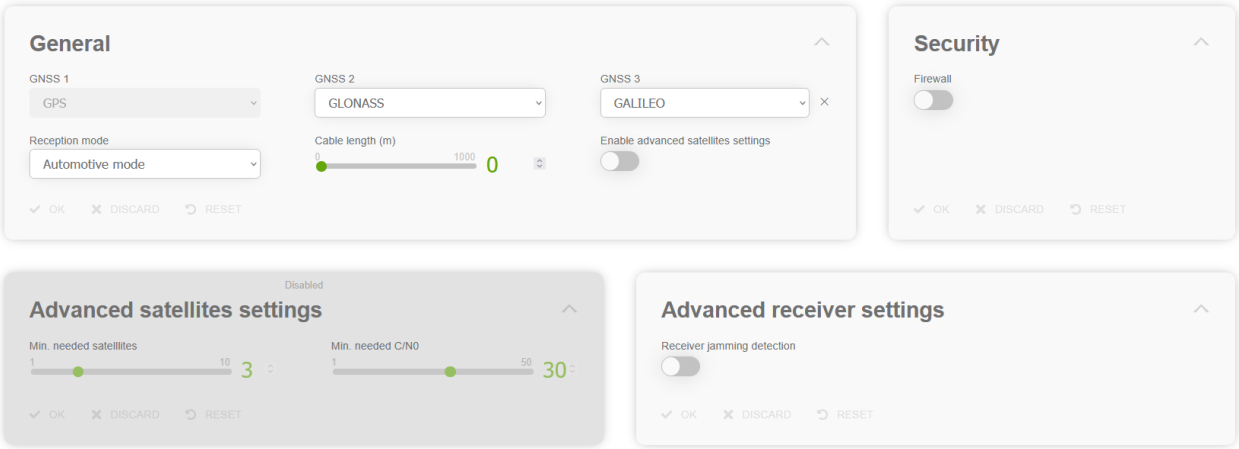


Figure 79 GNSS receiver configuration page

Input Label	**Description**
GNSS <NUMBER>	If multiple global navigation satellite systems are supported by the device, the systems to be used can be selected here. Systems that should be deactivated can be deselected with a delete button next to the drop-down selector. GNSS 1 is locked to the system "GPS".
Reception mode	Stationary mode In this mode the GNSS receiver calculates its accuracy based on a fixed position. If four or more satellites are received in this mode, the exact location is updated automatically. In this mode, a synchronization with a changing position is not possible. Automotive mode This mode allows using the device in mobile operation (except in airplanes).
Cable length	Can be used to compensate antenna cable delay. The value is in meter.
Enable advanced satellites settings	Enables / disables the Advanced satellites settings. You should only enable this feature if you are experiencing issues with your GNSS reception and the *hopf* support team advises you to do so.
Firewall	Enables / disables the GNSS firewall functionality

Min. needed satellites	The minimum number of satellites, with C/N0 greater equal the configured Min. needed C/N0 value, that are required to accept a synchronization via this GNSS channel, can be configured here.
Min. needed C/N0	The least needed C/N0 value in dBHz, that must be reached from at least Min. needed satellites to accept a synchronization via this GNSS channel, can be configured here.
Receiver jamming detection	Enables / disables the jamming detector of the GNSS receiver. The jamming detector an application level is always enabled. With this setting the jamming detector implemented in the GNSS receiver can be enabled in addition to the application level jamming detector. **Hint:** if the firewall is disabled the detection of jamming has no effect to the board operation. It will only trigger an alarm event and the status will be updated correctly. Receiver jamming detection is not supported by all receivers. On boards with a receiver that does not support this feature, the advanced receiver settings section is not shown.

Min. needed satellites and Min. needed C/N0 settings

These settings define the number of satellites with reception quality greater equal to Min. needed C/N0 value, that are needed to accept a synchronization via this GNSS channel.

This configuration is intended to prevent the synchronization during poor reception quality periods, which will introduce jitter to the internal time. If the antenna setup is according to the guidelines of ***hopf***, such a situation will not occur and the default settings (Min. needed satellites 3 and Min. needed C/N0 30), are the correct choice.

In situation where the antenna setup cannot be done according to the guidelines of ***hopf*** (e.g. in urban canyons), an optimization of these settings can help to get a good synchronization even in poor reception quality situation.

GNSS firewall

When the GNSS firewall is enabled, the corresponding board monitors and analyses the GNSS signals, to detect spoofing- and jamming-attacks. In the case of a detected spoofing- or jamming-attack, the board flags the GNSS signal as falsified, and does not use it as synchronization source. When no other synchronization source is configured, the board will go to holdover operation.

In the case of a jamming-attack the board will recognize when the jamming-attack has ended and clear the jamming detected flag. When the end of a jamming-attack is not detected correctly or the jamming-attack is detected because the GNSS antenna system setup changed, it can be cleared with the Set jamming threshold action (see 6.6.3.2.2).

In the case of a spoofing-attack, the board will not clear the spoofing detected flag automatically, a manual action is needed to trust the GNSS signal again. To clear the spoofing falsified flag, perform the Clear spoofing detection action (see 6.6.3.2.2).

6.6.3.3 NTP

All pages that concern the sync source NTP can be found under this item.

6.6.3.3.1 Status

This status page is composed of sections with detailed information about the NTP sync source.

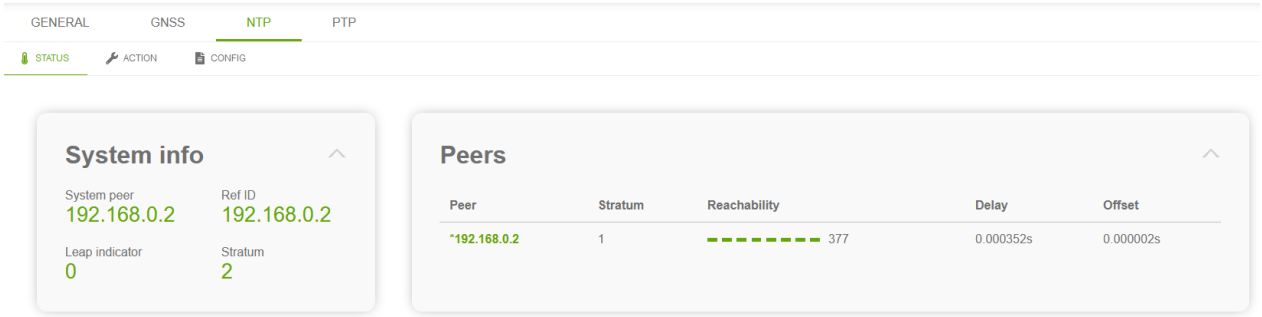


Figure 80 NTP status page example

System info

Input Label	Description
System peer	The peer the system is synced to.
Ref ID	The reference ID of the system peer
Leap indicator	0 – Time is in sync 1 – Add leap second at the end of this full hour 2 – Delete leap second at the end of this full hour 3 – Error, time invalid
Stratum	The stratum value of the system.

Peers

This section is used to track the performance of the configured NTP server/driver and the NTP algorithm itself. The information displayed is identical with the information available via NTPQ or NTPDC programs.

Each NTP server/driver that has been set up in the NTP server configuration (see 6.6.3.3.3) is displayed in the peer information.

The connection status is displayed in the reachability column (green bars indicate successful communication attempts and red ones indicate failures; the last 8 communication attempts are displayed and the number at the right side is an octal representation of those communication attempts).

6.6.3.3.2 Action

This page provides all actions related with the NTP services as synchronization source. The only supported action is a restart of the NTP service.

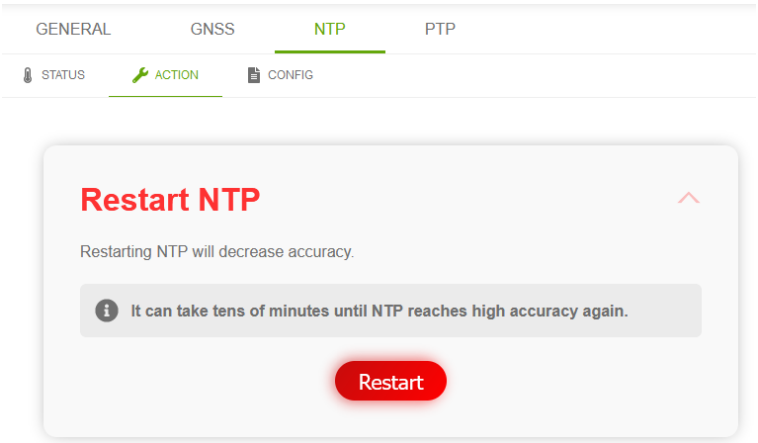


Figure 81 NTP action page

6.6.3.3.3 Config

On this page the configuration settings of the sync source NTP can be changed.

Client configuration

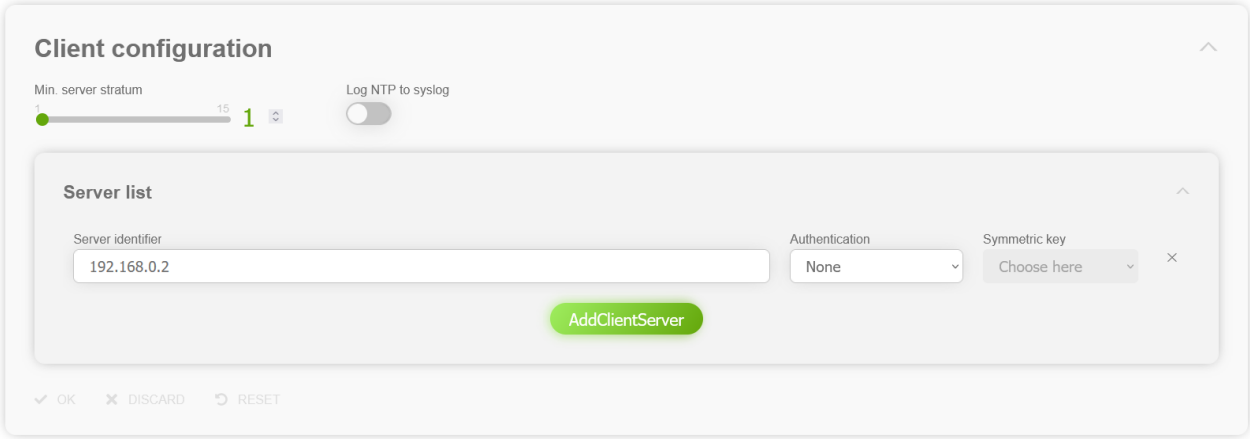


Figure 82 NTP client configuration section

Input Label	Description
Min. Server Stratum	The worst server stratum accepted to sync to is configured here. E.g., to only sync to servers with stratum 1 or 2 Min. Server Stratum must be set to 2
Log NTP to syslog	This option enables or disables Syslog messages which are generated from the NTP service. This value has no effect if Syslog is not configured (see 6.6.5.2.1).
Server Identifier	IPv4, IPv6 or hostname of the NTP server is configured here
Authentication	The authentication method can be configured here. Supported values: None RFC8915(NTS) Symmetric key Symmetric key is only available when it is configured in the following section. When Symmetric key is selected the corresponding key ID must be selected in the second drop down Due to security vulnerability Autokey is not supported anymore.

Click the AddClientServer button to add a new entry to the Server List.

Click the X at the right side of a server list entry to remove it from the list.

Symmetric keys

Symmetric key authentication has already been introduced in NTP v3, but is still supported in the new versions. The drawback of symmetric keys is that a secret key has to be exchanged in a safe way between servers and clients, while with public key authentication schemes only a public key had to be copied to clients.

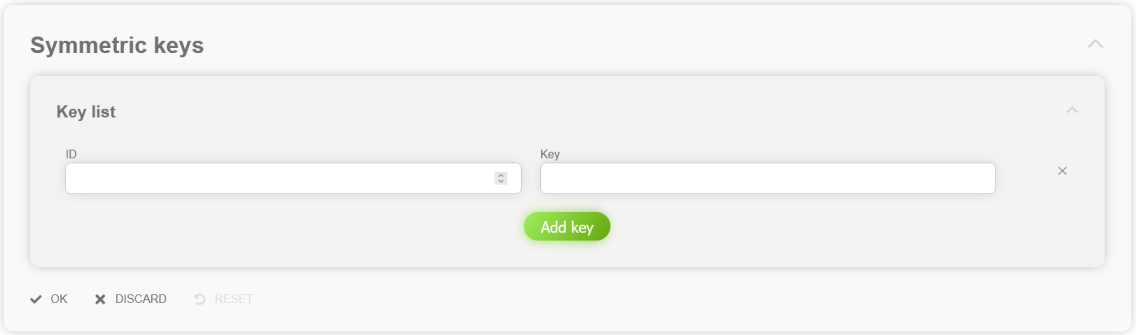


Figure 83 NTP symmetric key configuration section for sync source

Input Label	Description
ID	The key ID is used to identify the key and is in the range from 1 – 65534. This means that 65534 different keys can be defined.
Key	The key that should be used to generate the symmetric key must be specified here

Supported symmetric key formats

The keys in the symmetric keys section must be entered in the following format (no spaces are allowed, except after the [type] definition it is mandatory):
[type] [HEX:][key]

[type] … hash / cipher function that should be used. This block is optional and when omitted, the following space must also be omitted. Allowed hash / cipher functions: MD5, SHA1, SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, TIGER, WHIRLPOOL, AES128, AES256
If no type is specified MD5 is used as default.

[HEX:] … optional identifier, that the following [key] is a string of hexadecimal values. If [type] AES128 or AES256 is used [HEX:] is mandatory.

[key] … key that should be use. This block is mandatory. When [HEX:] is used only characters of the following list are allowed:
ABCDEF0123456789

If [type] AES128 is used the key string must have exactly 32 characters, if AES256 is used it must have 64 characters

Examples of valid keys:

- testkey
- test123
- MD5 testkey
- HEX:1234567890ABCDEF
- SHA1 HEX:1234567890ABCDEF
- AES128 HEX:1234567890ABCDEF1234567890ABCDEF

Examples of invalid keys:

- Test key (Test is not a supported [type] and a space is contained in the string)
- MD5 test key (the space between test and key is not allowed)
- HEX:1234567890ABCDEFG (G is not allowed for hexadecimal keys)
- AES128 HEX:1234567890ABCDEF1234567890ABCDEF1 (the key length must match 32 characters)

6.6.3.4 PTP

All pages that concern the sync source PTP can be found under this item.

6.6.3.4.1 Status

This status page is composed of sections with detailed information about the PTP sync source.

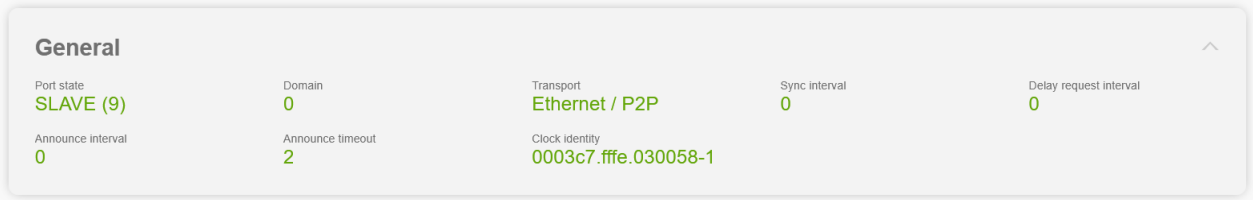


Figure 84 PTP sync source general status section

Label	Description
Port state	Port state as text and number, according to IEEE1588 standard. Important port states: FAULTY (2) – indicates a problem on the port (normally this state is active when the network port link is down). The port acts as defined for FAULTY port state in IEEE1588 standard, sending no announce and sync messages. LISTENING (4) – indicates that the port is checked for announce messages (normally this state is active after the network port link got up or after PTP has been started). The port acts as defined for LISTENING port state in IEEE1588 standard, sending no announce and sync messages.

	PASSIVE (7) – indicates that the port is in passive mode (normally this state is active when the best master clock algorithm determined that another PTP server is the best master). The port acts as defined for PASSIVE port state in IEEE1588 standard, sending no announce and sync messages. MASTER (6) – indicates that the port is in master mode (normally this state is active when no announce messages have been seen within the announce timeout for the configured domain). The port acts as defined for MASTER port state in IEEE1588 standard, sending announce and sync messages. SLAVE (9) - indicates that the port is in slave mode, it synchronizes to the PTP master. GRAND_MASTER (10) – identical to MASTER (6)
Domain	Used PTP domain Should be identical to the configured value in 6.6.3.4.2
Transport	Used PTP transport method Should be identical to the configured value in 6.6.3.4.2
Sync interval	Used PTP sync interval according Should be identical to the configured value in 6.6.3.4.2
Delay request interval	Used PTP delay request interval Should be identical to the configured value in 6.6.3.4.2
Announce interval	Used PTP announce interval Should be identical to the configured value in 6.6.3.4.2
Announce timeout	Used PTP announce timeout Should be identical to the configured value in 6.6.3.4.2
Clock identity	Clock identity received in the announce message of the PTP master

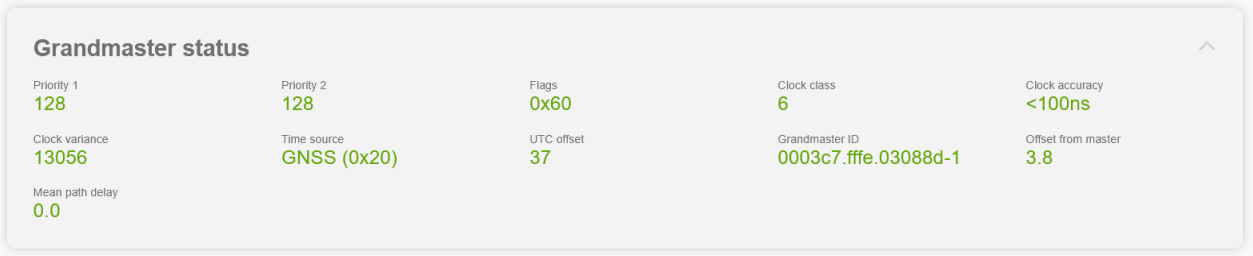


Figure 85 PTP sync source grandmaster status section

Label	**Description**
Priority 1	PTP priority 1 received from the PTP master
Priority 2	PTP priority 2 received from the PTP master
Flags	Flags value received in the announce message of the PTP master
Clock class	Clock class received in the announce message of the PTP master
Clock accuracy	Clock accuracy received in the announce message of the PTP master
Clock variance	Clock variance received in the announce message of the PTP master
Time source	Time source received in the announce message of the PTP master
UTC offset	UTC offset received in the announce message of the PTP master
Grandmaster ID	Grandmaster clock identity received in the announce message of the PTP master
Offset from master	Estimated offset between own clock and master clock
Mean path delay	Estimated mean path delay

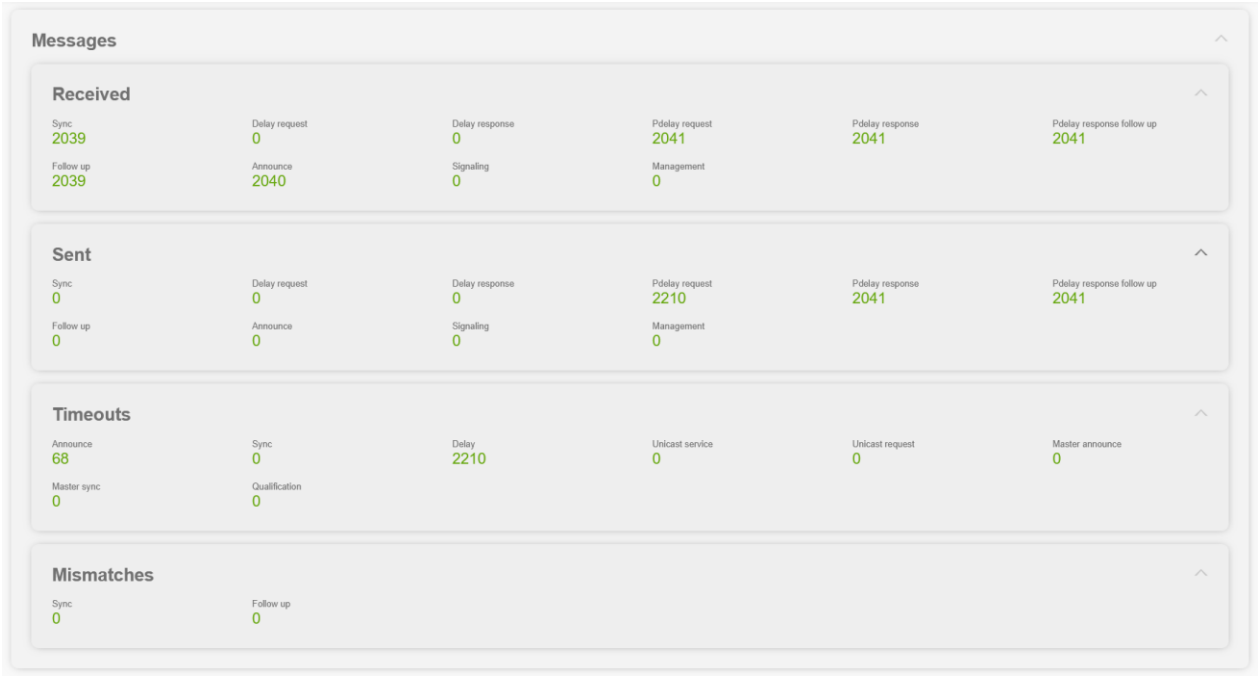


Figure 86 PTP sync source messages status section

The messages section contains counters for received and sent messages, for timeouts and mismatched packets.

6.6.3.4.2 Config

On this page the configuration settings of the sync source PTP can be changed.

Client Configuration

The minimum PTP master accuracy and clock class values needed to accept it as source, can be configured here.

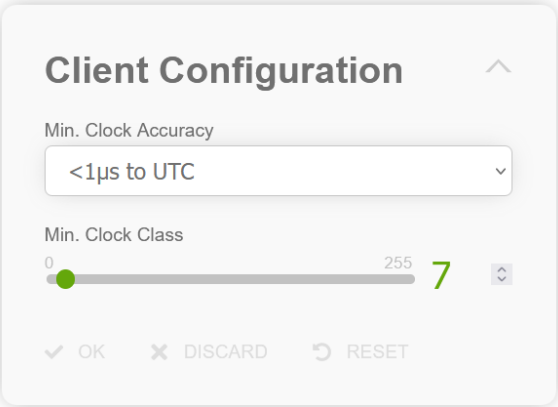


Figure 87 PTP client configuration section

Input Label	Description
Min. Clock Accuracy	Minimum clock accuracy that's needed to accept the announced PTP master as synchronization source is configured here. Supported values: <25ns to UTC <100ns to UTC <250ns to UTC <1us to UTC <2,5us to UTC <10us to UTC <25us to UTC <100us to UTC <250us to UTC <1ms to UTC <2,5ms to UTC <10ms to UTC <25ms to UTC <100ms to UTC <250ms to UTC <1s to UTC <10s to UTC >10s to UTC
Min. Clock Class	Minimum clock class that's needed to accept the announced PTP master as synchronization source is configured here. E.g., when only PTP masters with clock class 7 or smaller should be accepted 7 must be configured for Min. Clock Class

General

The basic settings for PTP base functionality are displayed under this section.

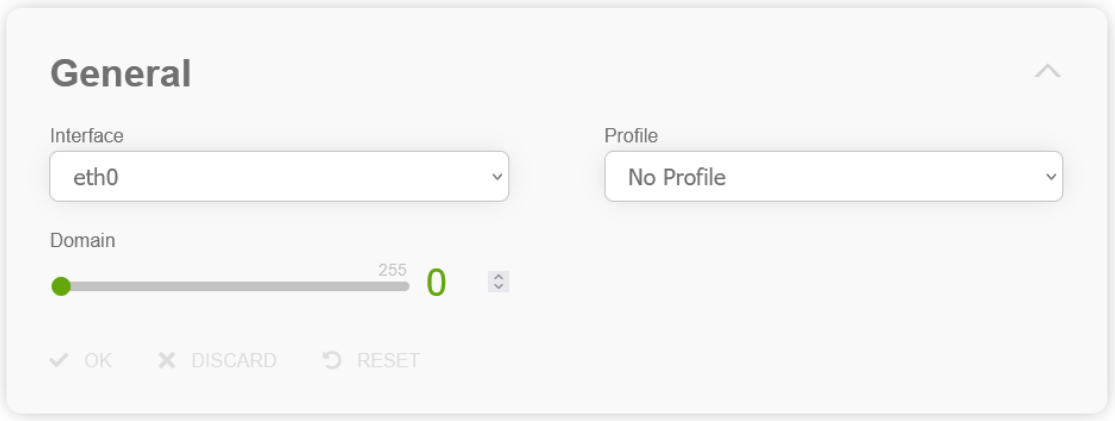


Figure 88 General PTP configuration section

Input Label	Description
Interface	Network interface on which PTP should be output
Profile	PTP profiles can be activated here. Supported PTP profiles: No Profile C37.238-2011 C37.238-2017 Power Utility Automation IEC61850-9-3-2 ITU-T G.8275.1
Domain	PTP domain that should be used

Advanced settings

The PTP transport and timeout settings are displayed under this section.

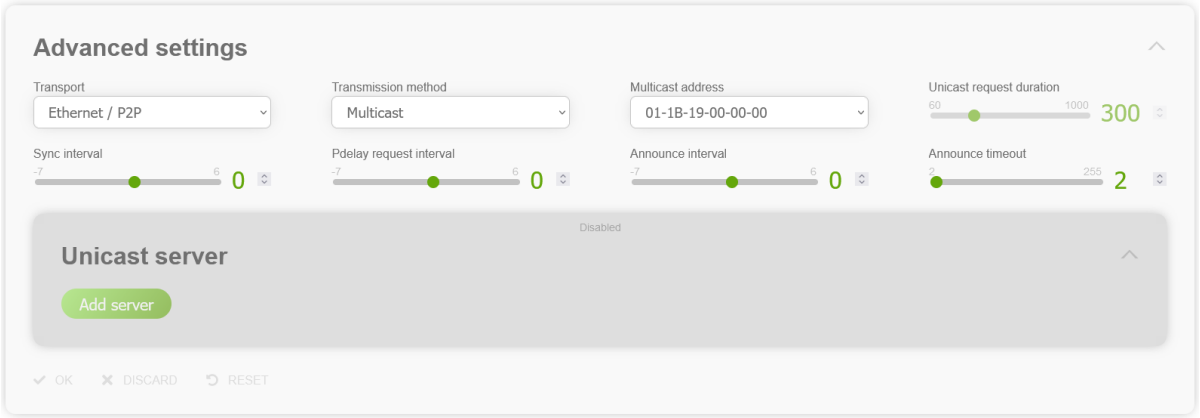


Figure 89 Advanced PTP configuration section

Input Label	Description
Transport	The transport and path delay mechanism are configured here Supported options: Ethernet / P2P Ethernet / E2E IPv4 / E2E
Transmission method	The transmission method is configured here Supported options: Multicast
Multicast address	The multicast address is configured here Supported options for ethernet transport mechanism: 01-80-C2-00-00-0E 01-1B-19-00-00-00 Supported options for IPv4 transport mechanism: 224.0.1.129
Unicast request duration	The unicast request duration is configured here (actually not used)
Sync interval	The sync message interval is configured here The interval is calculated as 2^x [sec] where x is the configured value. E.g., x = 0 results in a 1 second sync message interval
Pdelay request interval	The delay message interval is configured here The interval is calculated as 2^x [sec] where x is the configured value.

	E.g., x = 0 results in a 1 second delay message interval
Announce interval	The announce message interval is configured here The interval is calculated as 2^x [sec] where x is the configured value. E.g., x = 0 results in a 1 second announce message interval
Announce timeout	The announce timeout is configured here. The configured value is the announce timeout in seconds. E.g., configured value is 2, means that the announce timeout is 2 seconds
Unicast Server	The unicast servers are configured here (actually not used)

Some PTP profiles have fixed values for these settings, if such a profile is selected in the General section, the Advanced settings section is disabled and the values defined in the selected PTP profile are used (but they are not displayed in the Advanced settings section). An example figure is shown below.

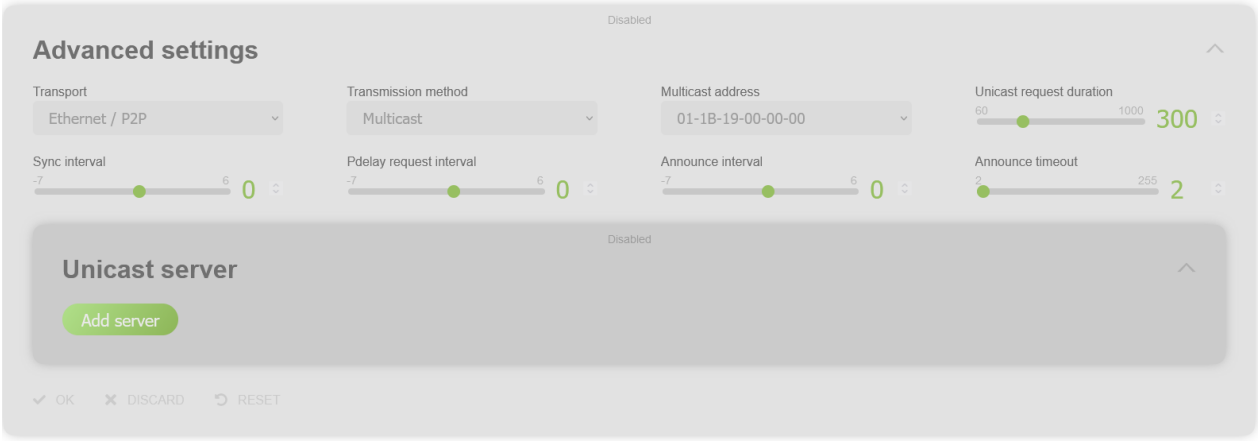


Figure 90 Disabled advanced PTP configuration section

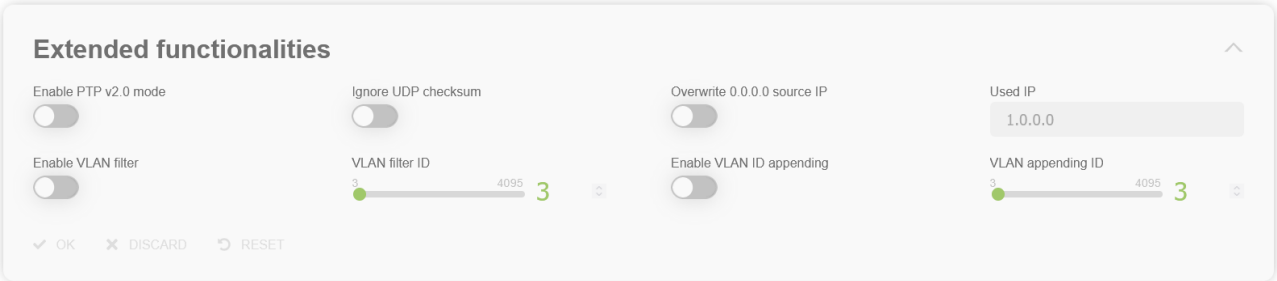


Figure 91 PTP sync source extended functionalities section

Input Label	Description
Enable PTP v2.0 mode	When enabled, the version number contained in the PTP message header is set to 2.0 and the control field is set according to table 23 of IEEE 1588-2008. When disabled, the version number contained in the PTP message header is set to 2.1 and the control field is set to 0 as defined in IEEE 1588-2019. This feature has been added, to support switches and clients, which only support IEEE 1588-2008 messages.
Ignore UDP checksum	When enabled, the software skips the validation of the UDP checksum for PTP packets sent via UDP.
Overwrite 0.0.0.0 source IP	When enabled, the software overwrites the source IP of PTP packets that are sent via UDP with source IP 0.0.0.0, with the IP address configured in Used IP. The problem with source IP 0.0.0.0 packets is, that this IP is not valid for PTP messages and those messages are dropped. When this feature is enabled the source IP of packets with 0.0.0.0 source IP is overwritten before the validation, and so they will not be dropped.
Used IP	The IP address that should be used to overwrite a 0.0.0.0 source IP should be entered here. It must be a valid IP address.
Enable VLAN filter	When enabled only PTP messages that contain the configured VLAN filter ID in the VLAN tag are processed, all other PTP messages are dropped.
VLAN filter ID	The VLAN ID to be filtered by must be set here.
Enable VLAN ID appending	When enabled a VLAN tag is appended to all PTP messages with the VLAN ID configured in VLAN appending ID
VLAN appending ID	The VLAN ID in the appended VLAN tags must be configured here.

6.6.4 Time Service

The pages under "Time Service" focus on network time services like NTP.

6.6.4.1 General

6.6.4.1.1 Status

Basic status information for all supported time services is displayed on this page. For each time service a status output is added to indicate whether the service is running.

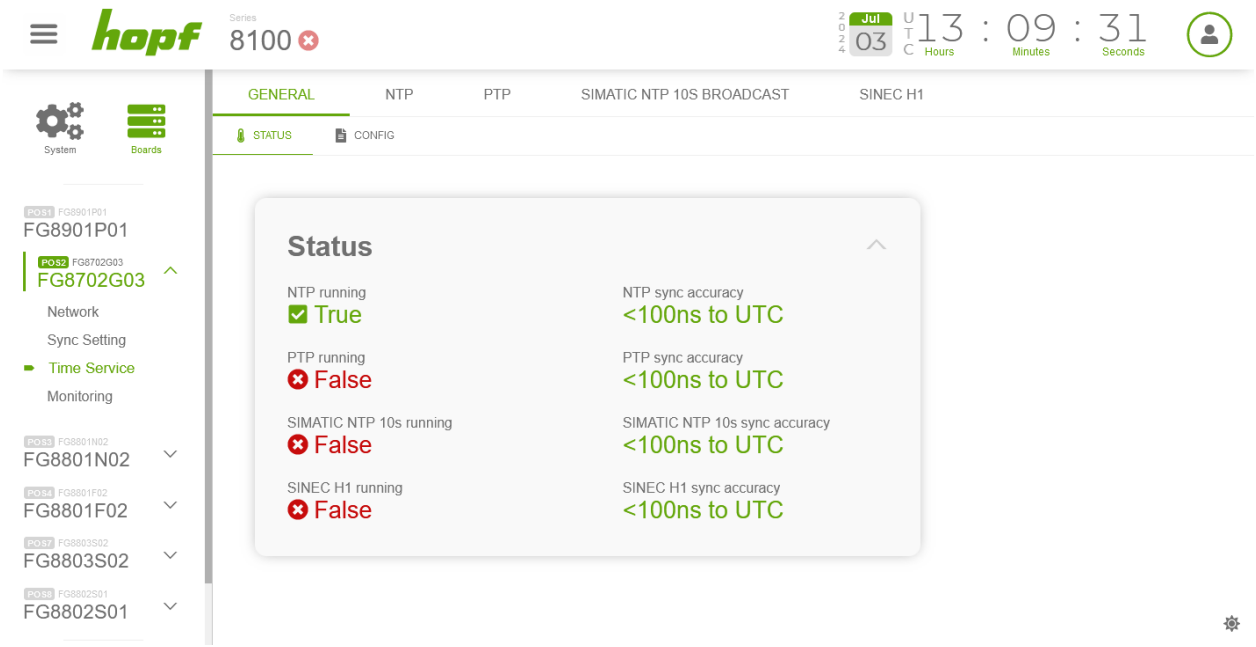


Figure 92 General time service status page example

Status Label	Description
XXX running	Indicates if the time service XXX is running (true) or not (false).
XXX sync accuracy	Time of the time service XXX is within: >= 10 ms to UTC < 10 ms to UTC < 1 ms to UTC < 100 us to UTC < 10 us to UTC < 1 us to UTC < 100 ns to UTC

6.6.4.1.2 Config

Each supported time service can be turned on or off on this config page.

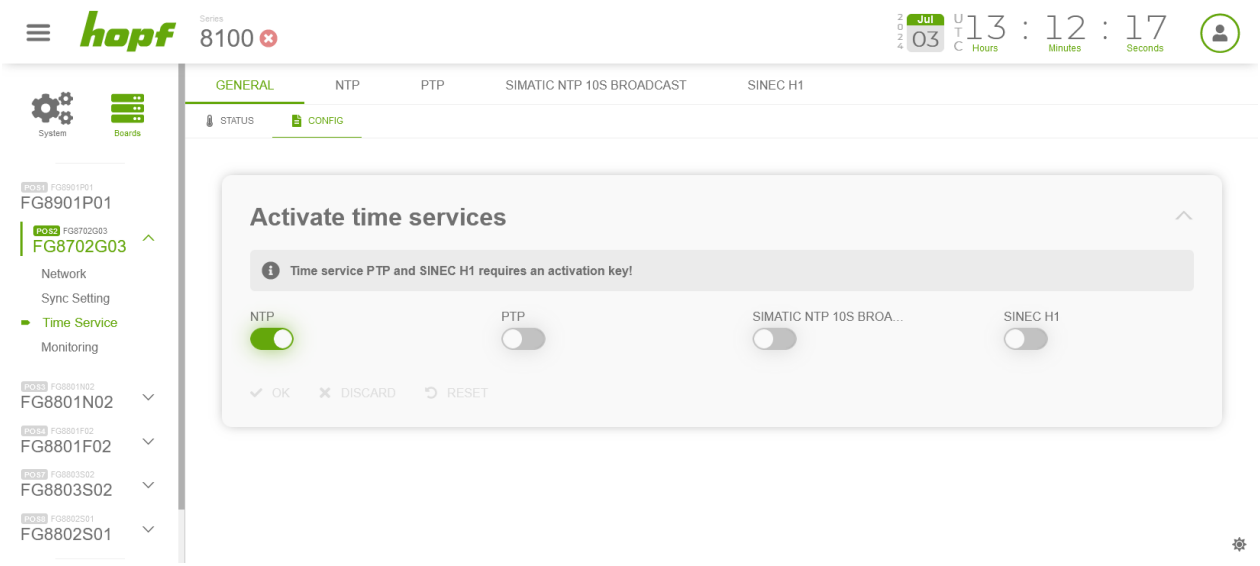


Figure 93 General time service configuration page example

6.6.4.2 NTP

All pages that concern the time service NTP can be found under this item.

6.6.4.2.1 Status

This status page consists of three sections that display status information about NTP.

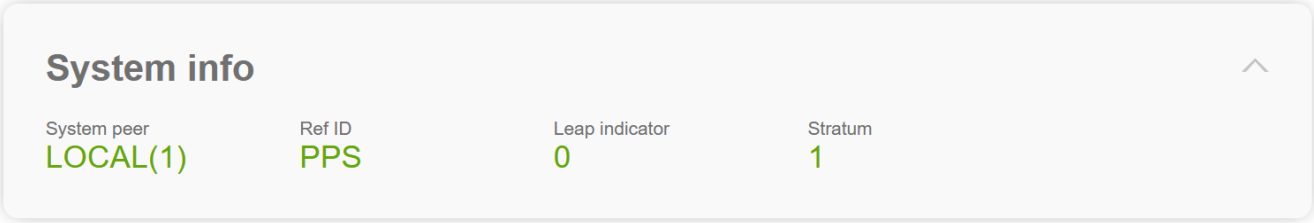


Figure 94 NTP status page example

System info

Input Label	Description
System peer	The peer the system is synced to.
Ref ID	The reference ID of the system peer

Leap indicator	0 – Time is in sync 1 – Add leap second at the end of this full hour 2 – Delete leap second at the end of this full hour 3 – Error, time invalid
Stratum	The stratum value of the system.

6.6.4.2.2 Action

This page provides sections to restart the NTP service and to upload the RFC8915 (Network Time Security) certificate.

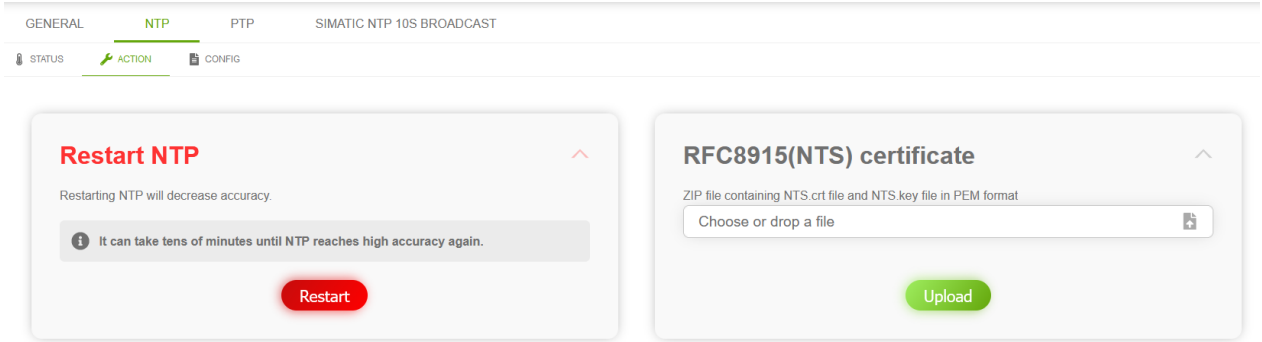


Figure 95 NTP time service action page

RFC8915(NTS) certificate format:

ECC and RSA based X509 certificates are supported.

e.g. rsa:2048, rsa:4096, prime256v1, …

The uploaded file must be a ZIP file, containing the two files NTS.crt and NTS.key.

Example content of NTS.key:

-----BEGIN PRIVATE KEY-----

MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCuXtWngcqUPrA7
f17EIBRiju97aRiaaps6K419Qc+pngY+OkqHKHcHwoCSTgjOG/pQBKGoR5OfFSi3
CSaP4QOTa4o3dZl5CW6GP4Mz4tpYulPScEebgewjTCde+rVRFbsdFNzAif6P9n+v
G7NAaXvjyMe1pi4WSriU/ziwvK5zPCudsmQxdqIdYIqL+Bw6A2lYy54wYl94jamD
qxOY2gvZWj6vNCJ+gUXjOdLjbkGlWtu9pUJnA1JR+OaLUxIrF4TLNQ4PWDeiYRBC
D4FUph4vfqJASMlyRpQmeSvSmDq5m2B7/XYBP7dkSLwlaaX2sXhe6GeK+UhNnOfw
jGJkZPRdAgMBAAECggEAdncNtvESHad9ed6uFpco4lDz2SdsxLQ648llJj1JBZbL
7QkTS0ltpEL7sOp9RvJxHF4ZKkf+vizU7Y20+jlIgaalT8qAy1+iDGkoDV9JMtDc
U/NeYwNg2BZMBVZVS1J1PmvHErRuE4bH9sLeBJvlxLrLG9lcJF79ipTfAgwehUCz
oEVq9cjt9p1/k0GGxmZM2Imv+/ILyY7K7cpLRwRxZDSwxvx6U7GSlP7R2rm5fsFL
A5+++3w1Yva34ZnK/Tprj9Ryu9XlYtHUyuvs/15VLy5oIHiMWxXtkJ3ZnqbE2lQ3
5/zRpm4GXhx0mRMQqMUqS9COYP56480avEC6u5/mwQKBgQDboVW2NtPc2//qg/UE
DuTfk0jzsCrlMw477pNrMRf8voqd+mXBwzFP7F8w30aOF9+s3qW+Lyh7EQeCVRT6

7xh8aOxjMiFcPjAle8JamJTBIdLN/UWQMurKQS6fJcFb+zBTbX3QgqrZLQX1jVWz
acwuETBqJxC0NQIy6YpnQgA2zQKBgQDLPtOwVdAzC9Q2q/MBxLxxdR3iZ/b96/8Z
tEVmrhmZiJrCrrFhhLWMa/cDf0jkdimACdKFxOzoILFkztmIcYW/IImQwO8qCp91
8dDYi19sHr56oGSz9n4UxmngqvlnqHFfyrlixOgPUn3q58TeiXs+oFXTfWuSYwnU
+FCcwMMT0QKBgQC5+iDBPiYi5CwNopWsTQxjga2JpIh+MsB/4WL1psnAHHz2jxzx
eV7dZbOph7eQBQlDsfk5VWd65o2sQG2WmzXpy1M4IC/9ky9j3itSWdfEvuZpxWjN
VUBZ6d4Xp3nXcJmYW6PpF2yioCxmpLqIRTM/YxDTIqdTYXuuLvIiw9G4lQKBgQCs
g+uTZYOPkJ7UuSdPfPqnI032e2C/L64c11OBUI4SME2MqlON/uNLCellYokwwst/
DtdPDFQ6xGVOt/UVR6bLEIc0A0/+U33+0v7+j26zi3ULCVHxH2ztnW0Jcpa4UdXK
BX1OROzk9JRE6+3DJtch1V6EYZUJcF9MEmn6Y/QxwQKBgE+C4hGDb6Gx5FODhabK
FxVGWNZiwNpHZa+LYuuZMrYbKWg38ZaroNUvBhD3A0jCMnCmo13MgeHW33WQG3+4
AKae8BUyioMXz0un4fEHppi7+PvKuBwclLKN7xCLQ/Q8qNWDncW8ec+xBdjvMxcM
jfk4BLbFKzmwDIv0qTbwQ+JF
-----END PRIVATE KEY-----

Example content of NTS.crt:

-----BEGIN CERTIFICATE-----
MIIDvzCCAqegAwIBAgIUc4+WcmTfJCCc2eiNG3pgWyCvA9UwDQYJKoZIhvcNAQEL
BQAwbzELMAkGA1UEBhMCREUxDDAKBgNVBAgMA0xVRDEMMAoGA1UEBwwDTFVEMQ0w
CwYDVQQKDARob3BmMQwwCgYDVQQLDANERVYxEzARBgNVBAMMClNlbGZTaWduZWQx
EjAQBgkqhkiG9w0BCQEWA04vQTAeFw0yNDAzMTMxNDQwMTlaFw0yNjAzMTMxNDQw
MTlaMG8xCzAJBgNVBAYTAkRFMQwwCgYDVQQIDANMVUQxDDAKBgNVBAcMA0xVRDEN
MAsGA1UECgwEaG9wZjEMMAoGA1UECwwDREVWMRMwEQYDVQQDDApTZWxmU2lnbmVk
MRIwEAYJKoZIhvcNAQkBFgNOL0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCuXtWngcqUPrA7f17EIBRiju97aRiaaps6K419Qc+pngY+OkqHKHcHwoCS
TgjOG/pQBKGoR5OfFSi3CSaP4QOTa4o3dZl5CW6GP4Mz4tpYulPScEebgewjTCde
+rVRFbsdFNzAif6P9n+vG7NAaXvjyMe1pi4WSriU/ziwvK5zPCudsmQxdqIdYIqL
+Bw6A2lYy54wYl94jamDqxOY2gvZWj6vNCJ+gUXjOdLjbkGlWtu9pUJnA1JR+OaL
UxIrF4TLNQ4PWDeiYRBCD4FUph4vfqJASMlyRpQmeSvSmDq5m2B7/XYBP7dkSLwl
aaX2sXhe6GeK+UhNnOfwjGJkZPRdAgMBAAGjUzBRMB0GA1UdDgQWBBShjoLT0duT
DMOrTLMVQURE+VzhwTAfBgNVHSMEGDAWgBShjoLT0duTDMOrTLMVQURE+VzhwTAP
BgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQAIUUJj7mFYN/v6Vl2t
7VhLGX/c0+uKDguLmTYULncJGwI7t/QOTZMDAb33cgjginZB8mNR0vtIZ3CdnqX/
gJQLmaGb/UcC/ea1WlC/+fCwWWMVAdU51k3ezsJn9TojMxVc5+cr6ZsbJN+pq86N
GNp8zNVrbABcw/KhN5FCGzlOKzBcXzQgbfJb89EmbvSAH0n88sBC/Dxgy+vnjAqE
+Hc98Nj80JDbzl6JRCB1uk5DcvVJy7LtEiHMuq4c6KuYNfzlHX3USn24+427ue2H
wf4DpYh2NDEgz76nCGkY2epL2OGlql/HgWX9EfHbeWB/a6bEpSCAGxJh1iSStkdN
y5By
-----END CERTIFICATE----

Example to generate those files with OpenSSL:

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout NTS.key -out NTS.crt

Example to generate a self-signed certificate for RFC8915 with OpenSSL, with a Subject Alternative Name (SAN) for testing:

1) Generate a file named NTS.cnf with the following content

[req]
default_bits = 2048
distinguished_name = req_distinguished_name
req_extensions = req_ext
x509_extensions = v3_req
prompt = no
[req_distinguished_name]

countryName = DE
stateOrProvinceName = N/A
localityName = N/A
organizationName = N/A
commonName = 192.168.0.1: Test certificate
[req_ext]
subjectAltName = @alt_names
[v3_req]
subjectAltName = @alt_names
[alt_names]
IP.1 = 192.168.0.1

2) Call the OpenSSL with the following statement

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout NTS.key -out NTS.crt -config NTS.cnf

3) ZIP the two generated files NTS.key and NTS.crt and upload the file to the device via RFC8915(NTS) certificate section

4) Upload the generated NTS.crt file to another device via Trusted certificate upload section (see 6.6.2.1.2). This device will now trust the certificate of the other device and will be able to use it as synchronization source when NTP is enabled as synchronization source (ATTENTION: an activation key is need to use NTP as synchronization source) and when the other device is added to the server list section. RFC8915 (NTS) is used when it is selected as authentication method and enabled on the other device (see 6.6.4.2.3).

6.6.4.2.3 Config

All configuration values related to the NTP time service can be found on this page.

Server configuration

The basic settings for NTP base functionality are displayed under this section.

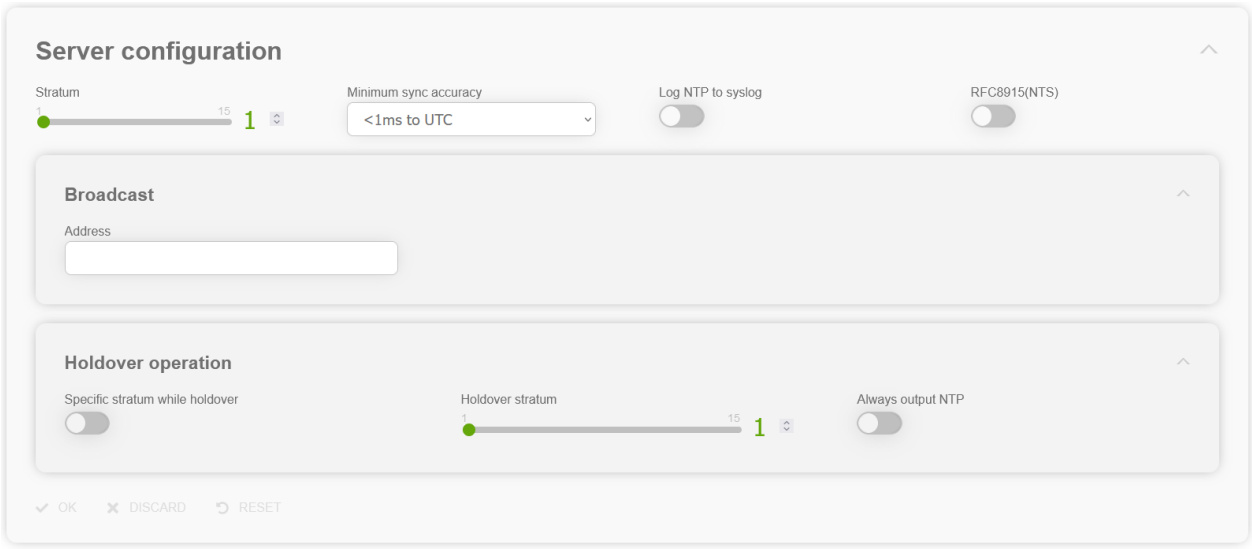


Figure 96 NTP time service general configuration section

Input Label	Description
Stratum	The stratum value of the NTP time server. Valid range 1-15. This setting allows to set a custom stratum value that can differ from the actual NTP stratum hierarchy.
Minimum sync accuracy	Minimum accuracy needed to output NTP. Selectable values: >= 10 ms to UTC < 10 ms to UTC < 1 ms to UTC < 100 us to UTC < 10 us to UTC < 1 us to UTC < 100 ns to UTC **Notice**: The accuracy under Time Service is used and not the one under Sync Setting.
Log NTP to syslog	This option enables or disables Syslog messages which are generated from the NTP service. This value has no effect if Syslog is not configured (see 6.6.5.2.1).
RFC8915(NTS)	This option enables or disables RFC8915 (Network Time Security)

Address	Address that should be used when NTP broadcast is needed
Specific stratum while holdover	With this option it is possible to use another stratum value while the device is in holdover. The used stratum value must be configured with the Holdover stratum slider.
Holdover stratum	Stratum value that should be used while the device is in holdover, when Specific stratum while holdover is enabled
Always output NTP	This option can be used to overrule the configured Minimum sync accuracy. When enabled, NTP will always be running with the configured stratum value no matter what the sync accuracy of the device is

Access restriction

One of the extended configuration options for NTP is "Access Restrictions".

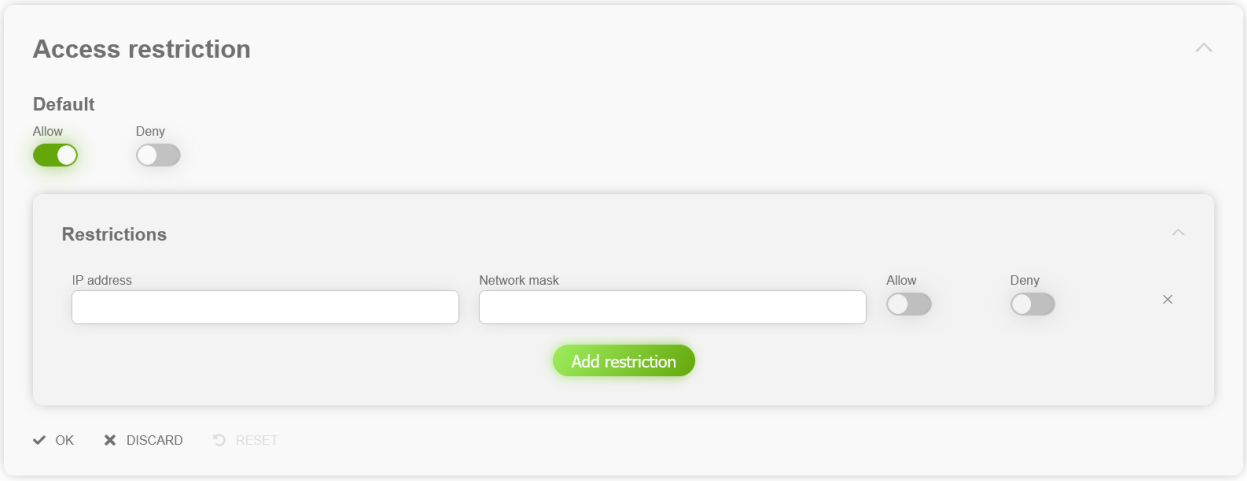


Figure 97 NTP access restrictions configuration section

Restrictions are used in order to control access to the system's NTP service.

Restrictions can be configured as white list (Default Allow disabled, Default Deny enabled and specific IP ranges with Allow enabled and Deny disabled in the Restrictions section) or as black list (Default Allow enabled, Default Deny disabled and specific IP ranges with Allow disabled and Deny enabled in the Restrictions section).

Symmetric keys

Symmetric key authentication has already been introduced in NTP v3, but is still supported in the new versions. The drawback of symmetric keys is that a secret key has to be exchanged in a safe way between servers and clients.

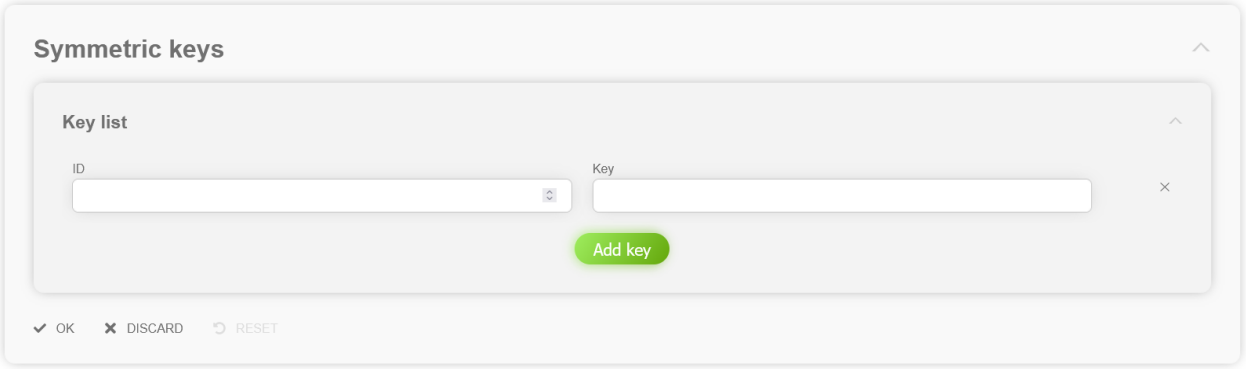


Figure 98 NTP symmetric key configuration section

Input Label	Description
ID	The key ID is used to identify the key and is in the range from 1 – 65534. This means that 65534 different keys can be defined.
Key	The key that should be used to generate the symmetric key must be specified here

Check chapter 6.6.3.3.3 for details of the key syntax.

Non-standard settings

NTP is a standard for synchronizing clocks in computer systems via packet-based communication networks. For special applications a non-standard setting can be configured. **Utilizing non-standard settings may cause time stepping!**

Figure 99 Non-standard NTP configuration section

Input Label	**Description**
Accept terms	The terms must be accepted in order to change non-standard settings.
Block output when stratum unspecified	Outputs when the stratum is unspecified (16). For example, in an error-case or at startup of the NTP service is suppressed (No answer to clients)
Timebase	For custom applications this function enables adjustment of the time base of the NTP output. Entering this function, the transmitted time protocol of the time server does not comply to the NTP standard anymore. According to the NTP standard NTP uses only the UTC time base. The following timebases can be selected: UTC – Coordinated Universal Time STD – Standard Time LOC – Local Time *Attention:* read the following block "**NTP with timebase different to UTC**" when you want to use a timebase different to UTC. This change has huge impact to the board.

NTP timebase settings	When the NTP Timebase is set to STD or LOC, the used STD and LOC timezone offset and LOC daylight saving time settings must be configured here

NTP with timebase different to UTC:

When NTP is configured with a timebase different to UTC the corresponding board changes its internal timebase from UTC to the configured timebase. That change impacts other functionalities of this board:

If this board is the management board of your device, the time displayed in the upper right corner is calculated in the following way:

- The configured timebase for NTP is treated as UTC time, configured timezone offset and daylight-saving time settings of the General device settings (6.5.1.1.3) will be added additionally
- Example: Actual UTC time is 06:40:00, NTP timebase is set to STD with +01:00:
  When the Interface timezone in General device settings is set to UTC, the displayed time is UTC 07:40:00
  When the Interface timezone in General device settings is set to STD and the corresponding timezone offset at that page is also set to +01:00, the displayed time is STD 08:40:00
  When the Interface timezone in General device settings is set to LOC and the corresponding timezone offset at that page is also set to +01:00 and it is summer time, the displayed time is LOC 09:40:00

If other time services are enabled on this board, those time services expect, that the boards timebase is UTC, but a configuration of the NTP timebase different to UTC, will force the boards timebase to something different than UTC, so those time services will output wrong time. We strongly recommend to don't enable any other time services on a board, when NTP with timebase different to UTC is used.

If the board is a time domain controller (TDC), the only allowed synchronization source is GNSS (see chapter 6.6.3.1.3). NTP and PTP are not allowed. When a configuration file with enabled PTP or NTP synchronization source and NTP time service with timebase different to UTC is uploaded, the upload fails with the following hint:

- Error occurrence: root/POSx/pages/timeService/ntp/timebase

6.6.4.3 PTP

All pages that concern the time service NTP can be found under this item.

6.6.4.3.1 Status

This status page consists of one section per network interface that outputs PTP, that displays status information about PTP.

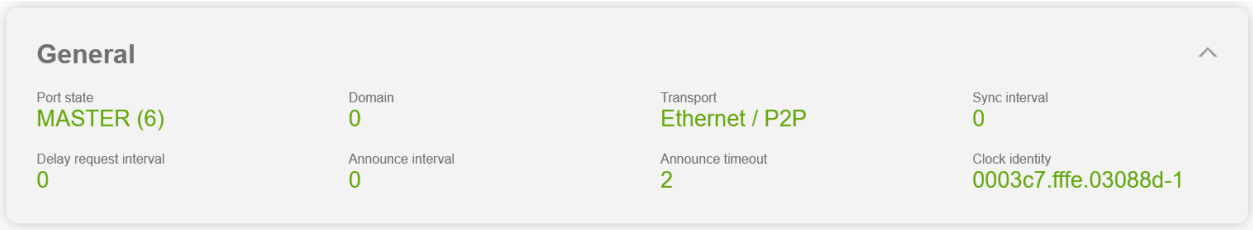


Figure 100 PTP time service general status section

Label	Description
Port state	Port state as text and number, according to IEEE1588 standard. Important port states: FAULTY (2) – indicates a problem on the port (normally this state is active when the network port link is down). The port acts as defined for FAULTY port state in IEEE1588 standard, sending no announce and sync messages. LISTENING (4) – indicates that the port is checked for announce messages (normally this state is active after the network port link got up or after PTP has been started). The port acts as defined for LISTENING port state in IEEE1588 standard, sending no announce and sync messages. PASSIVE (7) – indicates that the port is in passive mode (normally this state is active when the best master clock algorithm determined that another PTP server is the best master). The port acts as defined for PASSIVE port state in IEEE1588 standard, sending no announce and sync messages. MASTER (6) – indicates that the port is in master mode (normally this state is active when no announce messages have been seen within the announce timeout for the configured domain). The port acts as defined for MASTER port state in IEEE1588 standard, sending announce and sync messages. SLAVE (9) - indicates that the port is in slave mode, it synchronizes to the PTP master. GRAND_MASTER (10) – identical to MASTER (6)
Domain	Used PTP domain Should be identical to the configured value in 6.6.4.3.2
Transport	Used PTP transport method Should be identical to the configured value in 6.6.4.3.2

Sync interval	Used PTP sync interval Should be identical to the configured value in 6.6.4.3.2
Delay request interval	Used PTP delay request interval Should be identical to the configured value in 6.6.4.3.2
Announce interval	Used PTP announce interval Should be identical to the configured value in 6.6.4.3.2
Announce timeout	Used PTP announce timeout Should be identical to the configured value in 6.6.4.3.2
Clock identity	Clock identity used in announce messages and best master clock algorithm

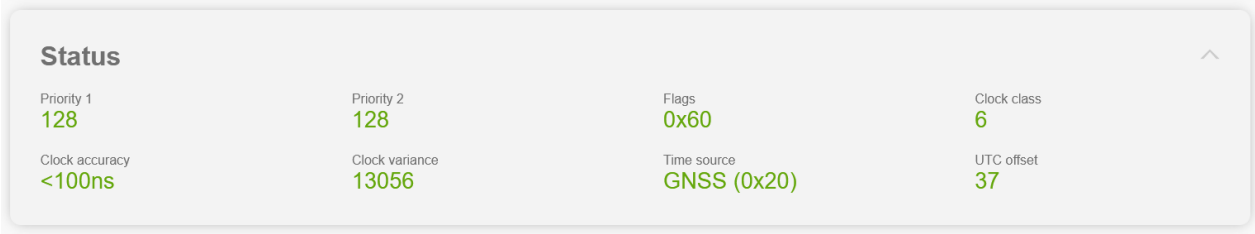


Figure 101 PTP time service status section

Label	**Description**
Priority 1	Used PTP priority 1 Should be identical to the configured value in 6.6.4.3.2
Priority 2	Used PTP priority 2 Should be identical to the configured value in 6.6.4.3.2
Flags	Flags value used in announce message Under normal condition the value is 0x1c, only during announced leap seconds the value should change to 0x1d (positive leap second) or 0x1e (negative leap second)
Clock class	Clock class used in announce messages and best master clock algorithm This value is calculated from the synchronization status and accuracy. If the synchronization status is Locked to sync source clock class will be 6
Clock accuracy	Clock accuracy used in announce messages and best master clock algorithm This value is calculated from the synchronization accuracy.
Clock variance	Clock variance used in announce messages and best master clock algorithm
Time source	Time source used in announce messages
UTC offset	UTC offset used in announce messages

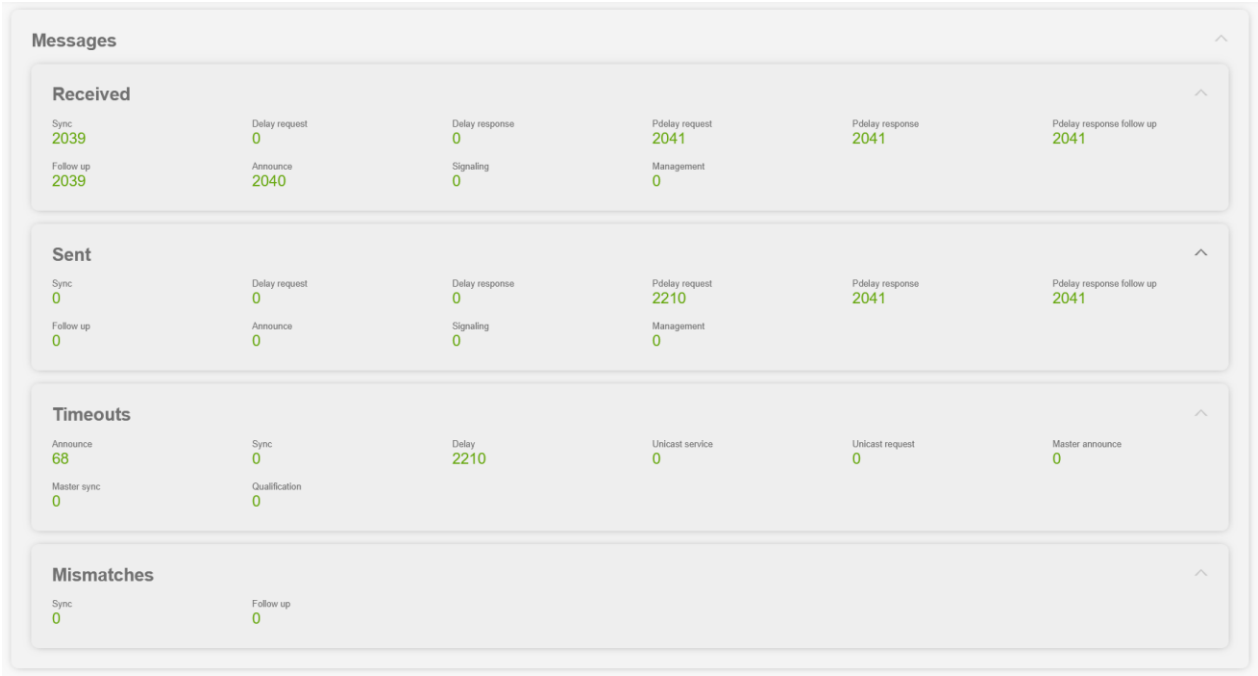


Figure 102 PTP time service messages status section

The messages section contains counters for received and sent messages, for timeouts and mismatched packets.

6.6.4.3.2 Config

All configuration values related to the PTP time service can be found on this page.

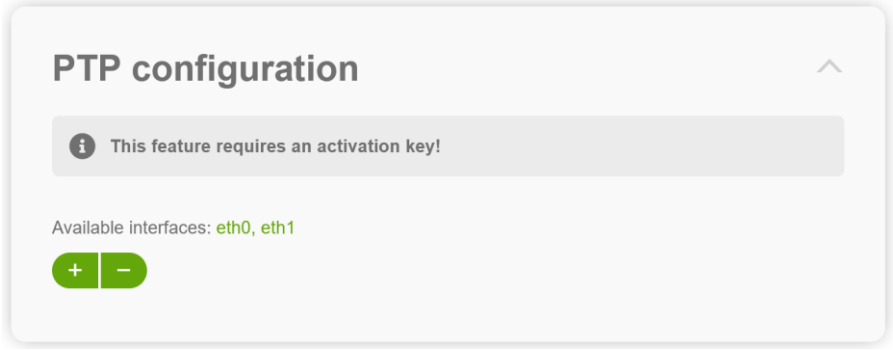


Figure 103 PTP time service section without an instance

The PTP configuration starts with adding an instance. To add an instance the plus button in the PTP configuration section must be clicked. Instances can also be removed; this can be done with a click on the minus button. A click on the minus button always removes the instance with the highest number.

When an instance is generated via the plus button an Instance section is generated.

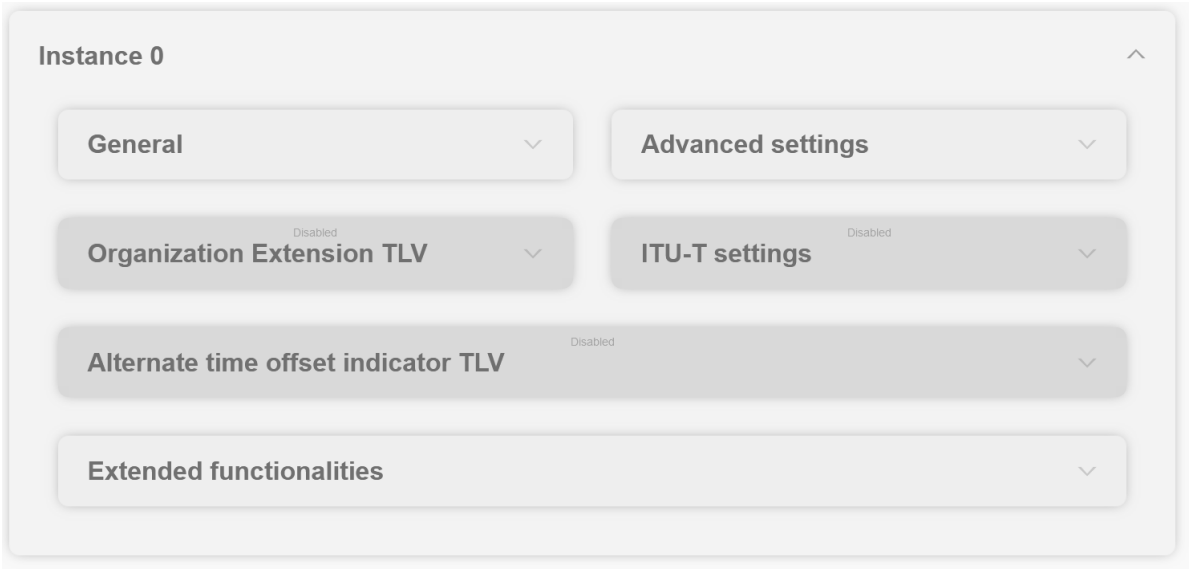


Figure 104 PTP time service instance 0 section with collapsed subsections

The above figure shows the instance section of instance 0. All subsections of instance 0 are collapsed in this figure. Those subsections and their configuration values are explained in the following paragraphs.

General

The basic settings for PTP base functionality are displayed under this section.

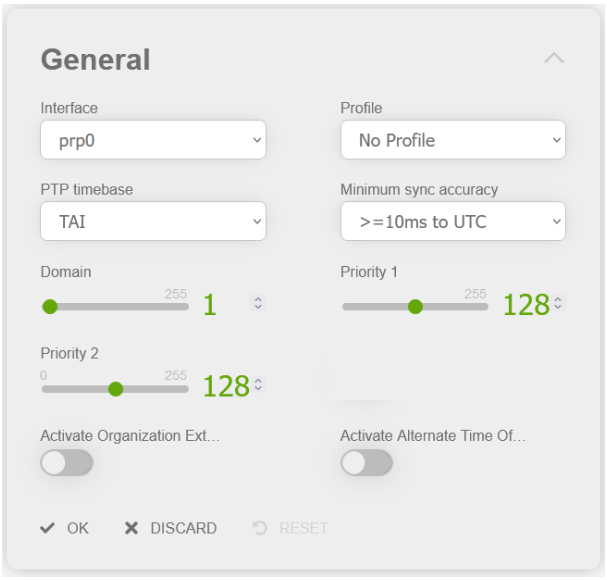


Figure 105 General PTP time service configuration section

Input Label	Description
Interface	Network interface on which PTP should be output
Profile	PTP profiles can be activated here. Supported PTP profiles:

	No Profile C37.238-2011 C37.238-2017 Power Utility Automation IEC61850-9-3-2016 ITU-T G.8275.1
PTP timezone	PTPs used timebase can be configured here Supported options: TAI UTC ARB When ARB is selected the used timebase is calculated from the configured values of the Alternate time offset indicator TLV
Minimum sync accuracy	Minimum accuracy needed to output PTP can be configured here. Supported options: >= 10 ms to UTC < 10 ms to UTC < 1 ms to UTC < 100 us to UTC < 10 us to UTC < 1 us to UTC < 100 ns to UTC **Notice**: The accuracy under Time Service is used and not the one under Sync Setting.
Domain	PTP domain that should be used
Priority 1	PTP priority 1 that should be used
Priority 2	PTP priority 2 that should be used
Activate Organization Extension TLV	Organization extension TLV can be enabled and disabled via this input
Activate Alternate Time Offset Indicator TLV	Alternate time offset indicator TLV can be enabled and disabled via this input

Advanced settings

The PTP transport and timeout settings are displayed under this section.

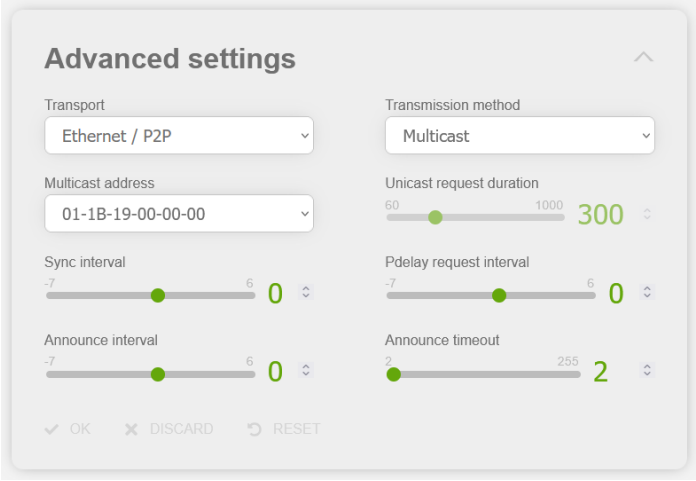


Figure 106 Advanced PTP configuration section

Input Label	Description
Transport	The transport and path delay mechanism are configured here Supported options: Ethernet / P2P Ethernet / E2E IPv4 / E2E
Transmission method	The transmission method is configured here Supported options: Multicast
Multicast address	The multicast address is configured here Supported options for ethernet transport mechanism: 01-80-C2-00-00-0E 01-1B-19-00-00-00 Supported options for IPv4 transport mechanism: 224.0.1.129
Unicast request duration	The unicast request duration is configured here (actually not used)
Sync interval	The sync message interval is configured here The interval is calculated as 2^x [sec] where x is the configured value. E.g., x = 0 results in a 1 second sync message interval

Pdelay request interval	The delay message interval is configured here The interval is calculated as 2^x [sec] where x is the configured value. E.g., x = 0 results in a 1 second delay message interval
Announce interval	The announce message interval is configured here The interval is calculated as 2^x [sec] where x is the configured value. E.g., x = 0 results in a 1 second announce message interval
Announce timeout	The announce timeout is configured here. The configured value is the announce timeout in seconds. E.g., configured value is 2, means that the announce timeout is 2 seconds

Some PTP profiles have fixed values for these settings, if such a profile is selected in the General section, the Advanced settings section is disabled and the values defined in the selected PTP profile are used (but they are not displayed in the Advanced settings section). An example figure is shown below.

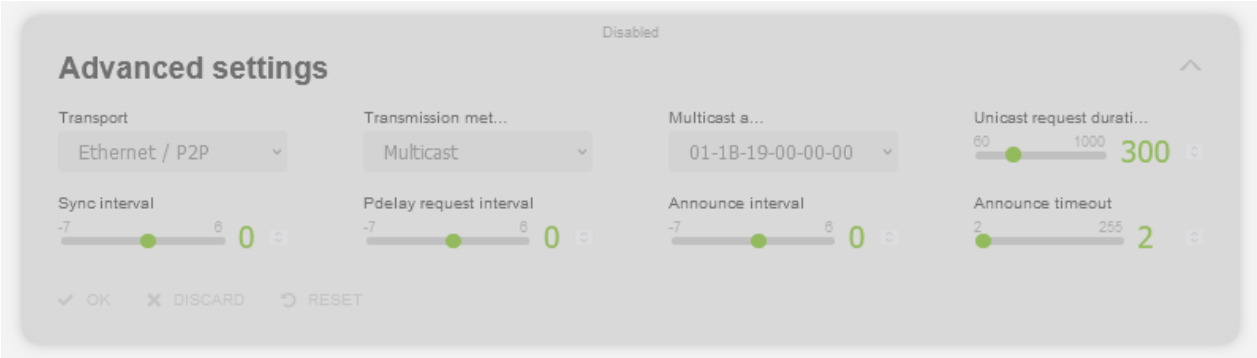


Figure 107 Disabled advanced PTP configuration section

Organization Extension TLV

The organization extension TLV settings are displayed under this section.

Figure 108 PTP organization extension TLV configuration section

Input Label	**Description**
Grandmaster ID	The grandmaster ID for the organization extension TLV can be configured here

When the organization extension TLV is disabled in the General section, the Organization Extension TLV is also disabled. An example figure is shown below.

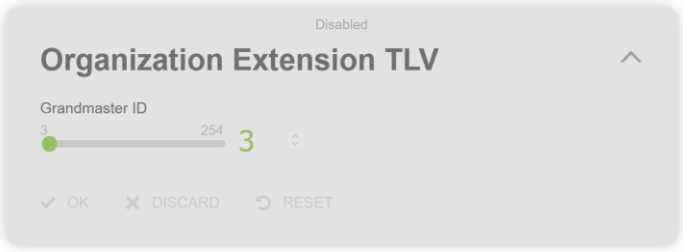


Figure 109 Disabled PTP organization extension TLV configuration section

ITU-T settings

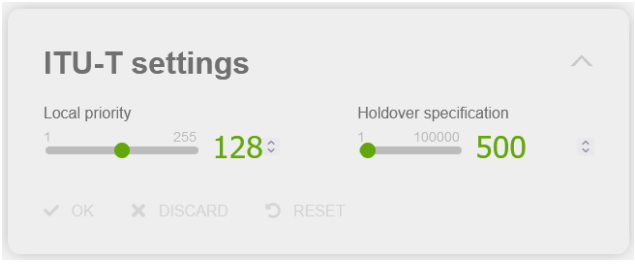


Figure 110 ITU-T settings section

Input Label	Description
Local priority	The local priority defined in the ITU-T standard G.8275.1 / 2 is configured here
Holdover specification	The holdover requirement in nanoseconds can be configured here. This value is used to calculate the correct clockClass of the server, as defined in the ITU-T standard G.8275.1 / 2

When a profile different to ITU-T G.8275.1 / 2 is used this section is disabled. An example figure is shown below.

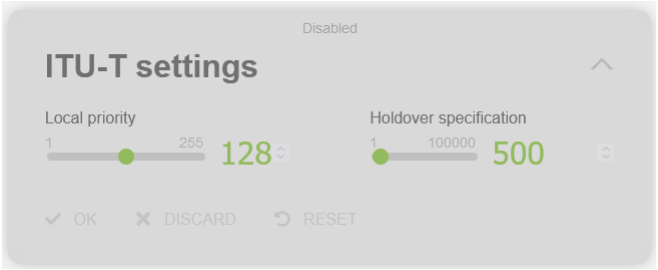


Figure 111 Disabled ITU-T settings section

Alternate time offset indicator TLV

The alternate time offset indicator TLV settings are displayed under this section.

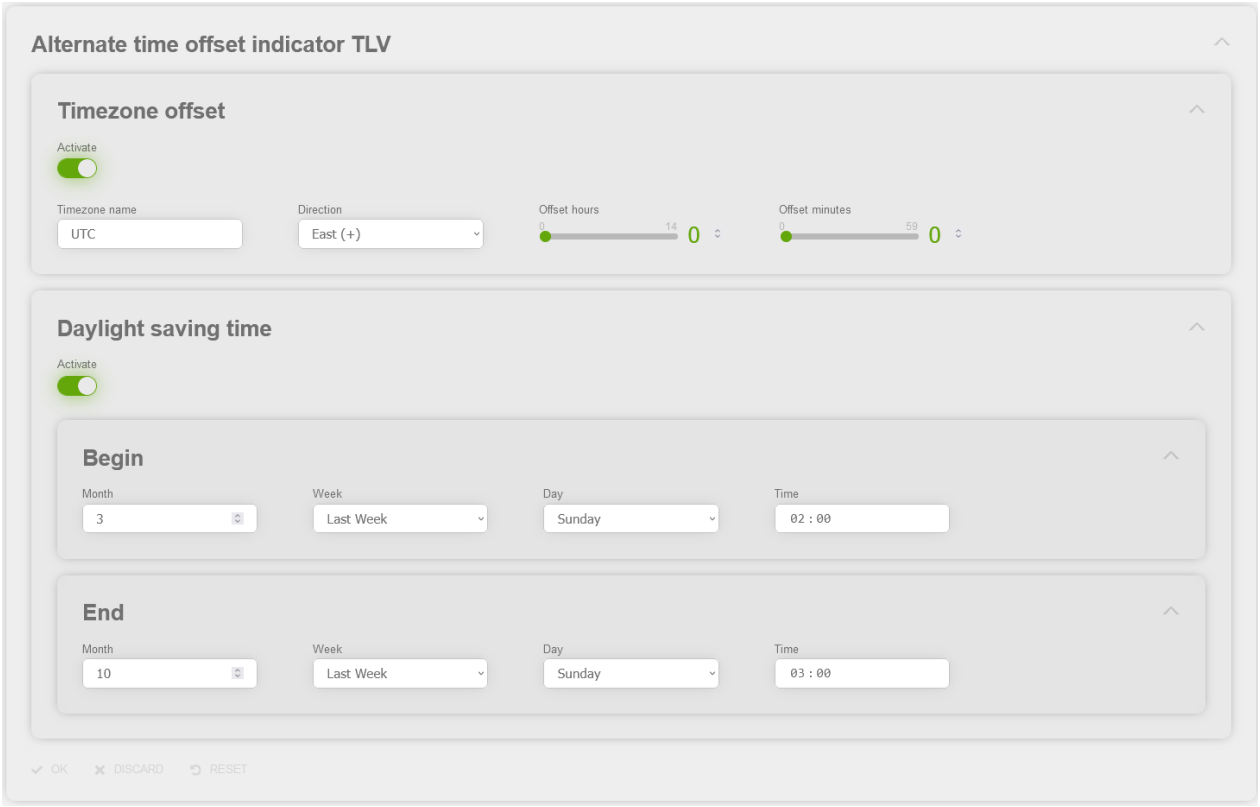


Figure 112 PTP alternate time offset indicator TLV configuration section

Input Label	Description
Timezone offset Activate	The timezone offset calculation for this PTP instance can be enabled and disabled here.
Timezone name	Timezone name that should be used in this TLV
Direction	Direction of the timezone offset used in this TLV Supported values: East (+) West (-)
Offset hours	Timezone offset hours value used in this TLV
Offset minutes	Timezone offset minutes value used in this TLV
Daylight saving time Activate	The daylight-saving time calculation for this PTP instance can be enabled and disabled here.

Month	Daylight saving time begin / end month To disable daylight saving time, begin and end month must be set to the same value
Week	Daylight saving time begin / end week Supported values: 1. Week 2. Week 3. Week 4. Week Last Week
Day	Daylight saving time begin / end day Supported values: Monday Tuesday Wednesday Thursday Friday Saturday Sunday
Time	Daylight saving time begin / end local time

Extended functionalities

Some extended functionalities for the PTP service can be configured here.

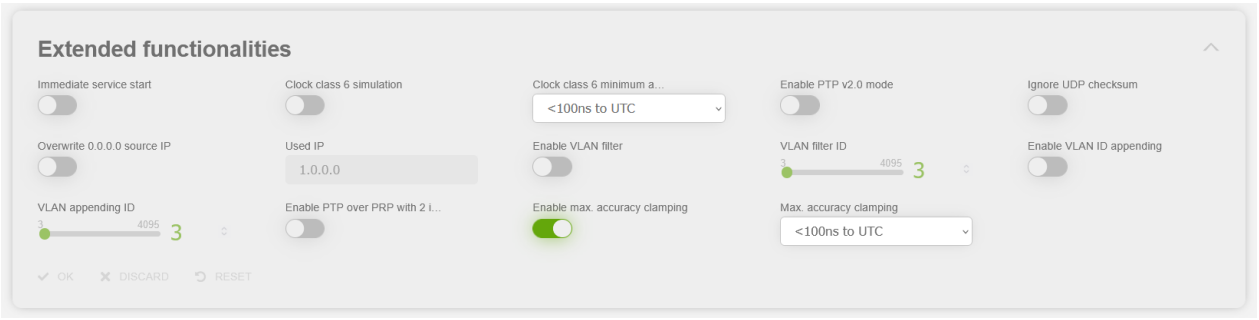


Figure 113 Example of the extended functionalities configuration of PTP

Input Label	Description
Immediate service start	If this feature is enabled the PTP service starts immediately after the boot, with clock class 187 and clock accuracy >10s, even when no valid time is known. When valid time

	is received the PTP time jumps to the received time and the clock class is calculated as defined in the standard.
Clock class 6 simulation	If this feature is enabled the PTP service simulates clock class 6, while holdover, as long as the accuracy is better than the configured value under “Clock class 6 minimum accuracy”. As long as a sync source is available or the accuracy is worse than the configured “Clock class 6 minimum accuracy”, the clock class is calculated as defined in the standard.
Clock class 6 minimum accuracy	Minimum accuracy that is needed to simulate clock class 6, when clock class 6 simulation is enabled.
Enable PTP v2.0 mode	If enabled, the version number contained in the PTP message header is set to 2.0 and the control field is set according to table 23 of IEEE 1588-2008. When disabled, the version number contained in the PTP message header is set to 2.1 and the control field is set to 0 as defined in IEEE 1588-2019. This feature has been added, to support switches and clients, which only support IEEE 1588-2008 messages.
Ignore UDP checksum	When enabled, the software skips the validation of the UDP checksum for PTP packets sent via UDP.
Overwrite 0.0.0.0 source IP	If enabled, the software overwrites the source IP of PTP packets that are sent via UDP with source IP 0.0.0.0, with the IP address configured in Used IP. The problem with source IP 0.0.0.0 packets is, that this IP is not valid for PTP messages and those messages are dropped. When this feature is enabled the source IP of packets with 0.0.0.0 source IP is overwritten before the validation, and so they will not be dropped.
Used IP	The IP address that should be used to overwrite a 0.0.0.0 source IP should be entered here. It must be a valid IP address.
Enable VLAN filter	If enabled only PTP messages that contain the configured VLAN filter ID in the VLAN tag are processed, all other PTP messages are dropped.
VLAN filter ID	The VLAN ID to be filtered by must be set here.
Enable VLAN ID appending	If enabled a VLAN tag is appended to all PTP messages with the VLAN ID configured in VLAN appending ID
VLAN appending ID	The VLAN ID in the appended VLAN tags must be configured here.
Enable PTP over PRP with 2 instances	This functionality has only an impact, if the configured interface for this PTP instance is a PRP interface. When enabled, two independent PTP instances are started to output PTP on both interfaces of the PRP interface. It follows, that PTP announce messages received on interface 1 from interface 2 (and vice versa) of the PRP interface are taken into account for the BMCA. When this functionality is not enabled, those messages are ignored for the BMCA.

	In normal PRP network setups it should never happen, that messages sent via one PRP interface are received on the other PRP interface, so this functionality will have no impact.
Enable max. accuracy clamping	If enabled the PTP service will clamp its own clock accuracy value to the selected value in the Max. accuracy clamping drop down, if the calculated accuracy is better, than the selected one. Example: if enabled and Max. accuracy clamping is set to <100ns to UTC and the calculated accuracy is <25ns to UTC, the PTP service will still use <100ns to UTC. This functionality can be used, if the time service is switching between two accuracy
Max. accuracy clamping	The accuracy level to which the PTP service should clamp its own accuracy must be selected here.

6.6.4.4 SIMATIC NTP 10s broadcast

All pages that concern the time service SIMATIC NTP 10s broadcast can be found under this item.

6.6.4.4.1 Config

All configuration values related to the SIMATIC NTP 10s broadcast time service can be found on this page.

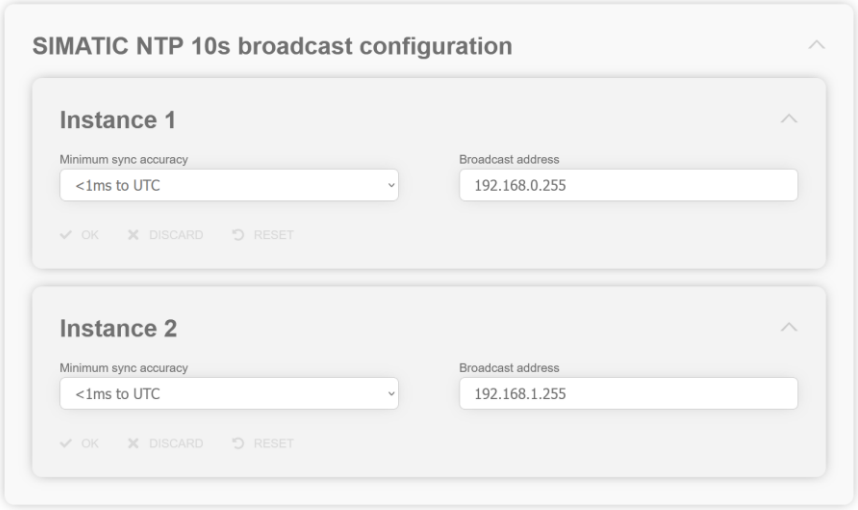


Figure 114 SIMATIC NTP 10s broadcast configuration section

Input Label	**Description**
Minimum sync accuracy	Minimum sync accuracy that's needed to send the NTP packet to the given broadcast address
Broadcast address	Broadcast address to which the NTP packets should be sent When the broadcast address is empty the SIMATIC instance is disabled

6.6.4.5 Xx

All pages that concern time services that are associated with dedicated connectors X1 to Xx, can be found under this item.

It is board depended which sections and pages are present

6.6.4.5.1 Config

All configuration values related to the connector Xx time service can be found on this page.

Depending on the device to which the page belongs, the displayed sections differ.

Config

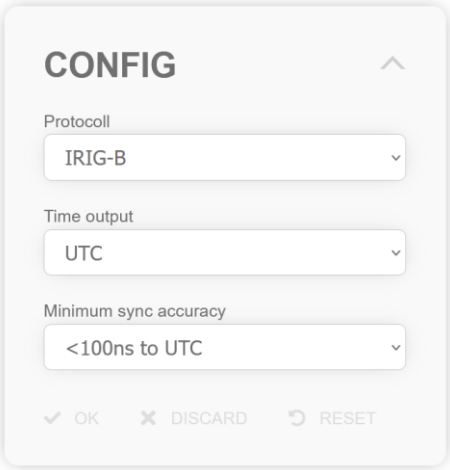


Figure 115 Xx general configuration section

Input Label	Description
Protocol	The protocol that should be output on this connector must be configured here. Supported values: IRIG-B DCF77 Cyclic Pulse This configuration value is not available for all devices
Time output	Time format used for the output. Supported values: UTC Standard time Standard time TD Local time Local time TD

Minimum sync accuracy	Minimum synchronization accuracy needed to generate the configured output signal. Supported values: >=10ms to UTC <10ms to UTC <1ms to UTC <100us to UTC <10us to UTC <1us to UTC <100ns to UTC

Difference between Time output Local time and Local time TD:

For Local time selection the local time configuration in the Timezone offset and Daylight-saving time selection on this page are used for output time calculation.

For Local time TD selection, the timezone offset and daylight-saving time configuration on the Sync Setting ➔ General ➔ Config (6.6.3.1.3) page of the time domain controller board that synchronizes the board with the Xx page are used.

Difference between Time output Standard time and Standard time TD:

For Standard time selection the timezone offset configuration in the Timezone offset selection on this page is used for output time calculation.

For Standard time TD selection, the timezone offset configuration on the Sync Setting ➔ General ➔ Config (6.6.3.1.3) page of the time domain controller board that synchronizes the board with the Xx page is used.

Timezone offset

This section is only available when Local time or Standard time is selected as Time output.

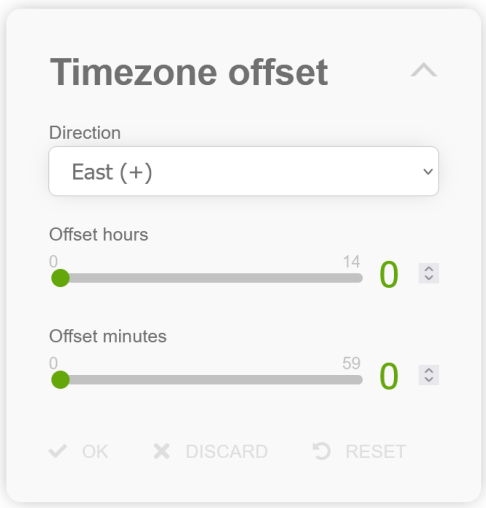


Figure 116 Timezone offset configuration section

Input Label	Description
Direction	The sign of the timezone offset value can be configured here. Supported values: East (+) West (-)
Offset hours	The hour value of the timezone offset can be configured here.
Offset minutes	The minutes value of the timezone offset can be configured here.

Daylight saving time

This section is only available when Local time is selected as Time output.

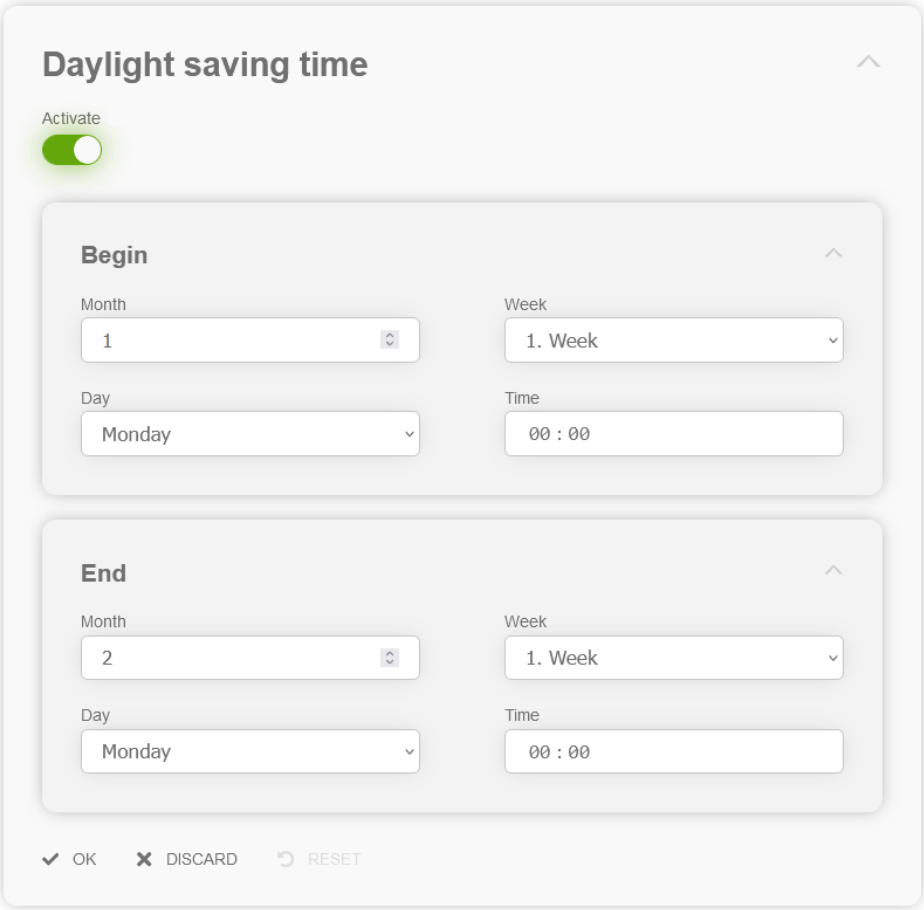


Figure 117 Daylight saving time configuration section

Input Label	Description
Activate	Enable / disable daylight saving time configuration
Month	Daylight saving time begin / end month
Week	Daylight saving time begin / end week Supported values: 1. Week 2. Week 3. Week 4. Week Last Week

Day	Daylight saving time begin / end day Supported values: Monday Tuesday Wednesday Thursday Friday Saturday Sunday
Time	Daylight saving time begin / end local time

IRIG-B Configuration

This section is only available when IRIG-G is selected as Protocol.

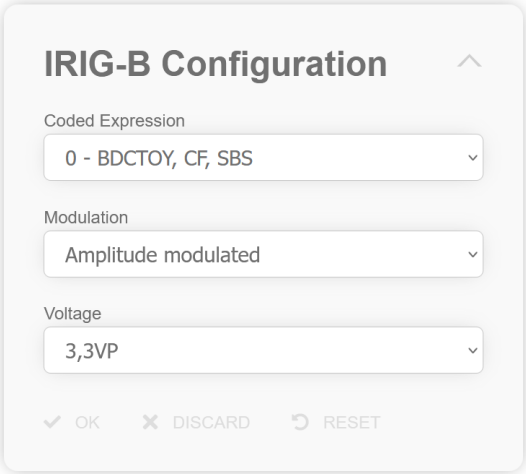


Figure 118 IRIG-G configuration section

Input Label	Description
Coded Expression	Used IRIG-B code Supported values: 0 – BCDTOY, CF, SBS 1 – BCDTOY, CF 2 – BCDTOY 3 – BCDTOY, SBS 4 – BCDTOY, BCDYEAR, CF, SBS 5 – BCDTOY, BCDYEAR, CF 6 – BCDTOY, BCDYEAR 7 – BCDTOY, BCDYEAR, SBS IEEE 1344-1995 IEEE C37.118-2005 IEEE C37.118-2011 AFNOR NF S87-500(2007)
Modulation	Used IRG-B modulation type Supported values: DCLS (not selectable for Coded Expression AFNOR NF S87-500(2007)) Amplitude modulated Manchester modulated (not selectable for Coded Expression AFNOR NF S87-500(2007))
Voltage	Used voltage for the IRIG-B output Supported values for Modulation selection DCLS and Manchester modulated: 5V 12V 24V Supported values for Modulation selection Amplitude modulated, when Coded Expression is **not** AFNOR NF S87-500(2007): 3,3VP Supported values for Modulation selection Amplitude modulated, when Coded Expression is AFNOR NF S87-500(2007): 2,14VP

Examples:

- To configure IRIG-B000 select Modulation DCLS and Coded Expression 0 – BCDTOY, CF, SBS
- To configure IRIG-B124 select Modulation Amplitude modulated and Coded Expression 4 – BCDTOY, BCDYEAR, CF, SBS
- To configure IRIG-B224 select Modulation Manchester modulated and Coded Expression 4 – BCDTOY, BCDYEAR, CF, SBS

DCF77 Configuration

This section is only available when DCF77 is selected as Protocol.

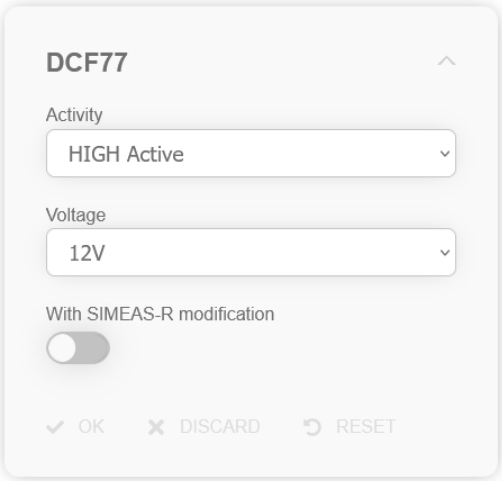


Figure 119 DCF77 configuration section

Input Label	**Description**
Activity	Configures DCF77 signal activity Supported values: HIGH Active LOW Active
Voltage	Used voltage for the DCF77 output Supported values: 5V 12V 24V
With SIMEAS-R modification	When enabled, the generated DCF77 signal is modified, to enable the synchronization of SIMEAS R systems.

Cyclic Pulse Configuration

This section is only available when Cyclic Pulse is selected as Protocol.

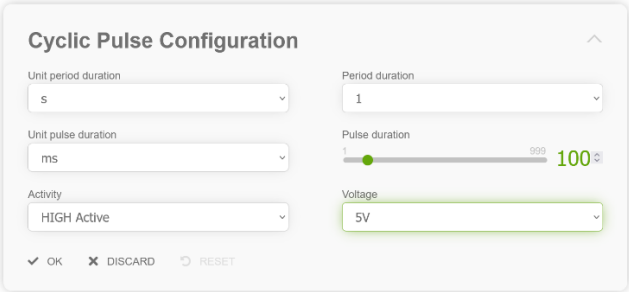


Figure 120 Cyclic pulse configuration section

Input Label	Description
Unit period duration	Unit for the period duration for the cyclic pulse Supported values: s m h
Period duration	Period duration for the cyclic pulse in selected Unit period duration unit Supported values depend on Unit period duration
Unit pulse duration	Unit for the pulse width of the cyclic pulse Supported values depend on Unit period duration
Pulse duration	Pulse width of the cyclic pulse in Unit pulse duration unit Supported values depend on Unit period duration, Period duration and Unit pulse duration
Activity	Configures the Cyclic Pulse signal activity Supported values: HIGH Active LOW Active
Voltage	Used voltage for the Cyclic Pulse output Supported values: 5V 12V 24V

Example:

The figure above shows the configuration for an 5V high active pulse per second with 100ms pulse width.

Serial Output

This section allows the configuration of a serial output.

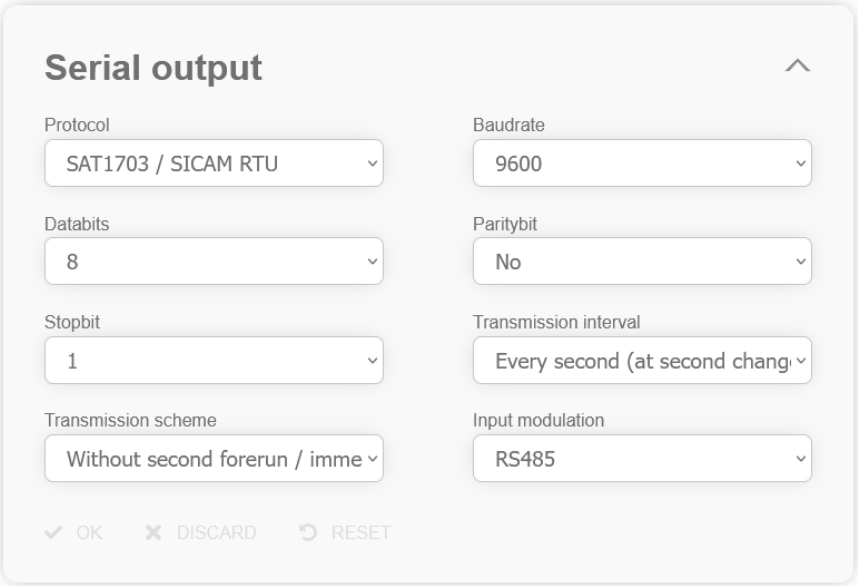


Figure 121 Serial output section

Input Label	Description
Protocol	The serial protocol that should be output can be configured here
Baudrate	The baud rate of the serial output can be configured here
Databits	The number of data bits of the serial output can be configured here
Parity	The parity of the serial output can be configured here
Stopbit	The number of stop bits of the serial output can be configured here
Transmission interval	The transmission interval of the serial output can be configured here
Transmission scheme	The transmission scheme of the serial output can be configured here
Input modulation	The used input modulation of the serial interface can be configured here

More details about the configuration of a serial output can be found in the technical documentation of the board.

PPS output

This section allows the configuration of PPS outputs on boards with serial outputs.

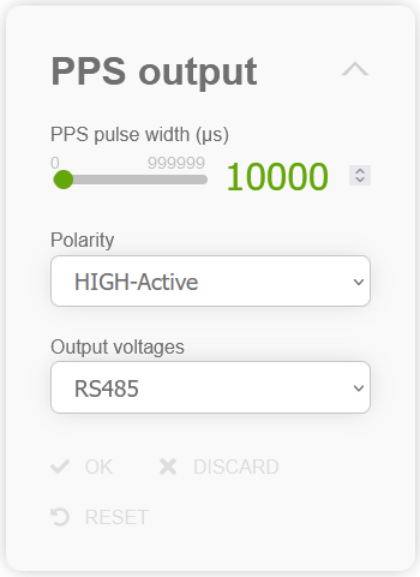


Figure 122 PPS output configuration

Input Label	Description
PPS pulse width (µs)	The pulse width of the output PPS in micro seconds
Polarity	The polarity of the PPS (high-active / low-active)
Output voltages	The output voltage of the PPS RS232 / RS485

6.6.4.6 SINEC H1

All configuration values related to the SINEC H1 time service can be found on this page.

6.6.4.6.1 Config

Figure 123 SINEC H1 section without an instace

The SINEC H1 configuration starts with adding an instance. To add an instance the plus button in the SINEC H1 section must be clicked. Instances can also be removed; this can be done with a click on the minus button. A click on the minus button always removes the instance with the highest number.

When an instance is generated via the plus button an Instance section is generated.

Figure 124 SINEC H1 time service instance 0 section with collapsed subsections

The above figure shows the instance section of instance 0. All subsections of instance 0 are collapsed in this figure. Those subsections and their configuration values are explained in the following paragraphs.

General

The basic settings of this SINEC H1 instance are configured in this subsection.

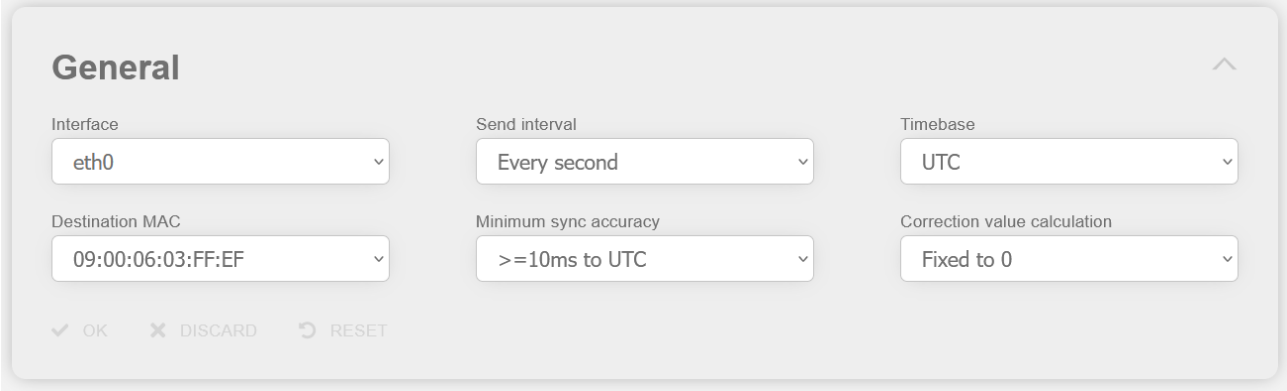


Figure 125 SINEC H1 time service instance general subsection

Input Label	**Description**
Interface	Network interface on which this SINEC H1 instance should be operated
Send interval	Send interval of this SINEC H1 instance Supported options: Every second Every 10th second Every minute
Timebase	Used timebase for this SINEC H1 instance Supported options: UTC STD LOC **Hint:** When STD is selected and daylight-saving time is enabled for this section, the daylight-saving time status is calculated for the corresponding status bit of the SINEC H1 message, but the sent time is still STD
Destination MAC	The destination MAC-address used by this SINEC H1 instance can be configured here. Supported options: 09:00:06:03:FF:EF 09:00:06:01:FF:EF FF:FF:FF:FF:FF:FF
Minimum sync accuracy	Minimum accuracy needed to output SINEC H1 via this instance Selectable values: >= 10 ms to UTC < 10 ms to UTC < 1 ms to UTC

	< 100 us to UTC < 10 us to UTC < 1 us to UTC < 100 ns to UTC **Notice**: The accuracy under Time Service is used and not the one under Sync Setting.
Correction value calculation	Defines how status byte 1 (correction value) is calculated Supported options: **Fixed to 0**: status byte 1 is set to 0 **Timezone offset**: only the value of the configured timezone offset is used for the calculation of status byte 1 **Daylight saving time**: only the DST value is used for the calculation of status byte 1 (so status byte 1 is either 0x00 or 0x08) **Timezone offset + Daylight saving time**: Timezone offset and DST are used for the calculation of status byte 1 The configured values in the sections Timezone offset and Daylight-saving time are used for the calculation. Those values are also used for the calculation of the timebase, but it is possible to configure timebase and this field independently. E.g. timebase set to UTC and correction value calculation to Timezone offset + Daylight-saving time. With this configuration the time is sent as UTC time and status byte 1 is set to the difference between local time and UTC. In this example the receiver is able to calculate local time out of the transmitted UTC time. Another example is to configure timebase to LOC and correction value calculation to Timezone offset + Daylight-saving time. With this configuration the time is sent as local time and status byte 1 is set to the difference between local time and UTC. In this example the receiver is able to calculate UTC out of the transmitted local time.

Timezone offset

The timezone offset of this SINEC H1 instance can be configured here. This section is only available, when the timebase is set to STD or LOC.

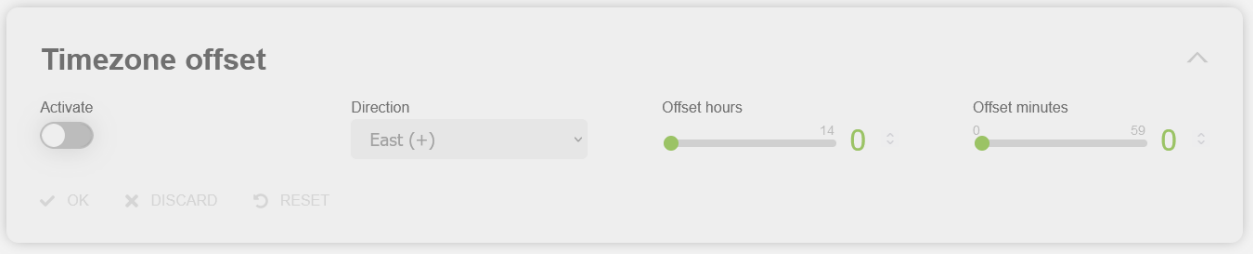


Figure 126 SINEC H1 time service instance timezone offset subsection

Input Label	Description
Activate	The timezone offset calculation for this SINEC H1 instance can be enabled here

Direction	The sign of the timezone offset value of this SINEC H1 instance can be configured here. Supported values: East (+) West (-)
Offset hours	The hour value of the timezone offset of this SINEC H1 instance can be configured here.
Offset minutes	The minutes value of the timezone offset of this SINEC H1 instance can be configured here.

Daylight saving time

The daylight-saving time settings of this SINEC H1 instance can be configured here. This section is only available, when the timebase is set to STD or LOC.

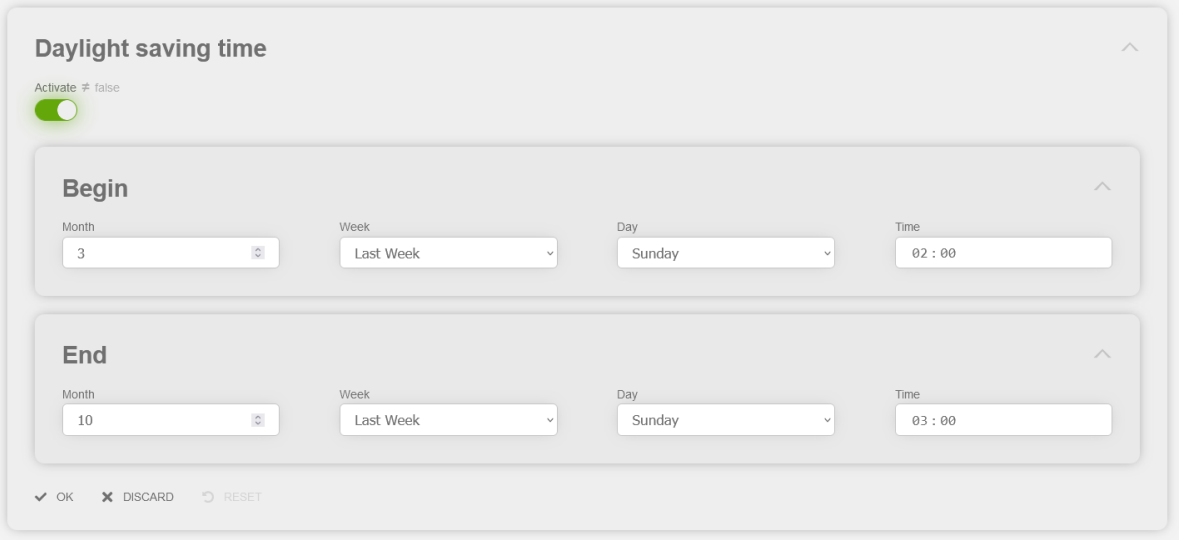


Figure 127 SINEC H1 time service instance daylight saving time offset subsection

Input Label	**Description**
Activate	Enable / disable daylight saving time configuration for this SINEC H1 instance
Month	Daylight saving time begin / end month of this SINEC H1 instance
Week	Daylight saving time begin / end week of this SINEC H1 instance Supported values: 1. Week 2. Week 3. Week

	4. Week Last Week
Day	Daylight saving time begin / end day of this SINEC H1 instance Supported values: Monday Tuesday Wednesday Thursday Friday Saturday Sunday
Time	Daylight saving time begin / end local time of this SINEC H1 instance

6.6.5 Monitoring

All settings concerning automatic information retrieval and notifications (regarding events and status of a *hopf* device) can be found under "Monitoring".

6.6.5.1 Events

6.6.5.1.1 Config

This page allows changing the event type (see 5.6) with a dropdown for certain events. Each event must have one out of the three types selected: **error**, **warn**, **info** and **ignore**. Hovering over the input label reveals the event code. Depending on the device the number of events varies.

Figure 128 Monitoring event list configuration section

6.6.5.2 Syslog

Syslog stands for System Logging Protocol and is a standard protocol used to send events to a specific server, called a Syslog server. It is primarily used to collect various device logs from several different machines in a central location for monitoring and review.

Syslog must be specified in the firewall settings (see 6.6.2.4.1) with UDP as protocol to work.

6.6.5.2.1 Config

It is necessary to enter the name or IPv4 or IPv6 address of a Syslog server in order to send an occurring event. If everything is configured correctly every event with the desired Alarm Level (or higher) is transmitted to the Syslog server.

Syslog uses Port 514.

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

Figure 129 SYSLOG configuration section without servers

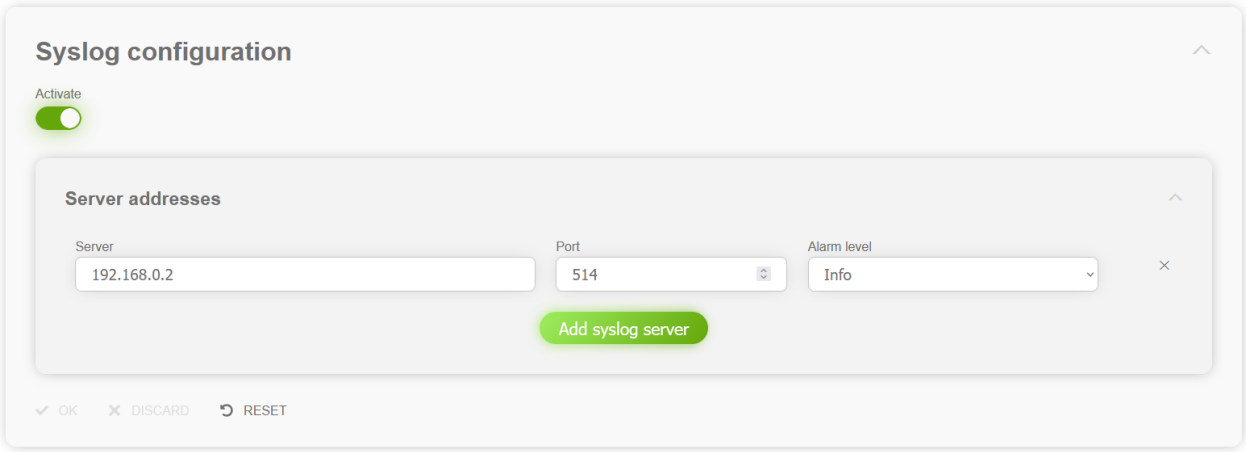


Figure 130 SYSLOG configuration section with one server

A SYSLOG server entry can be added via the "Add syslog server" button. Each server can be configured to a different alarm level. To delete a server entry the X button at the right side of that server's column must be clicked.

Input Label	Description
Activate	With this setting SYSLOG can be turned on and off.
Server	The IPv4/IPv6 address or hostname of a SYSLOG server.
Port	Configure the port on which the server listens here. The default SYSLOG port is 514
Alarm level	The alarm level defines the minimum event type that an event must have in order to be sent to the SYSLOG server. The event types info, warn and error can be selected. For more detail see 5.6.

6.6.5.3 Email

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

Email must be specified in the firewall settings (see 6.6.2.4.1) with UDP as protocol to work.

6.6.5.3.1 Config

It is possible to configure various, independent email addresses which each have different alarm levels.

An email for an occurred event will be sent automatically to the respective receiver if the event type is even or higher the selected alarm level.

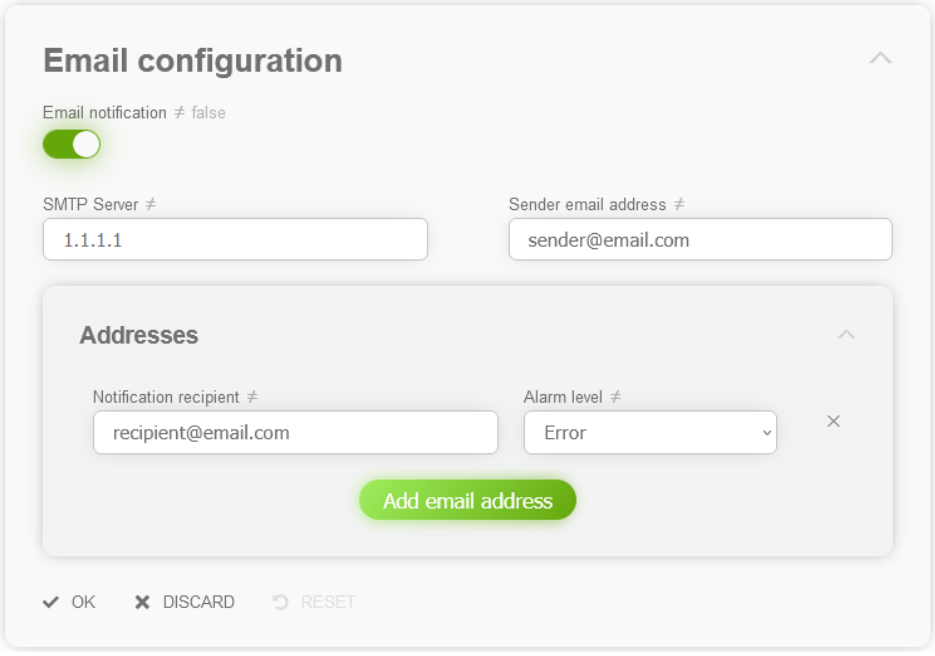


Figure 131 Email configuration section

Input Label	Description
Email notification	With this setting automatic email notification can be turned on and off.
SMTP Server	A valid IPv4/IPv6 address or hostname (SMTP server) must be entered for the purpose of correct configuration.
Sender email	Some email servers only accept messages if the sender address entered is valid (spam protection). The sender email address can be inserted in this input field.
Notification recipient	The email address of the recipient who should receive the notification can be entered here.
Alarm level	The alarm level defines the minimum event type that an event must have in order to be sent to the recipient. The event types info, warn and error can be selected. For more detail see 5.6.

6.6.5.4 SNMP

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

SNMP must be specified in the firewall settings (see 6.6.2.4.1) with UDP as protocol to work.

6.6.5.4.1 Config

On this config page SNMPv2/SNMPv3 and the SNMP traps can be configured.

General

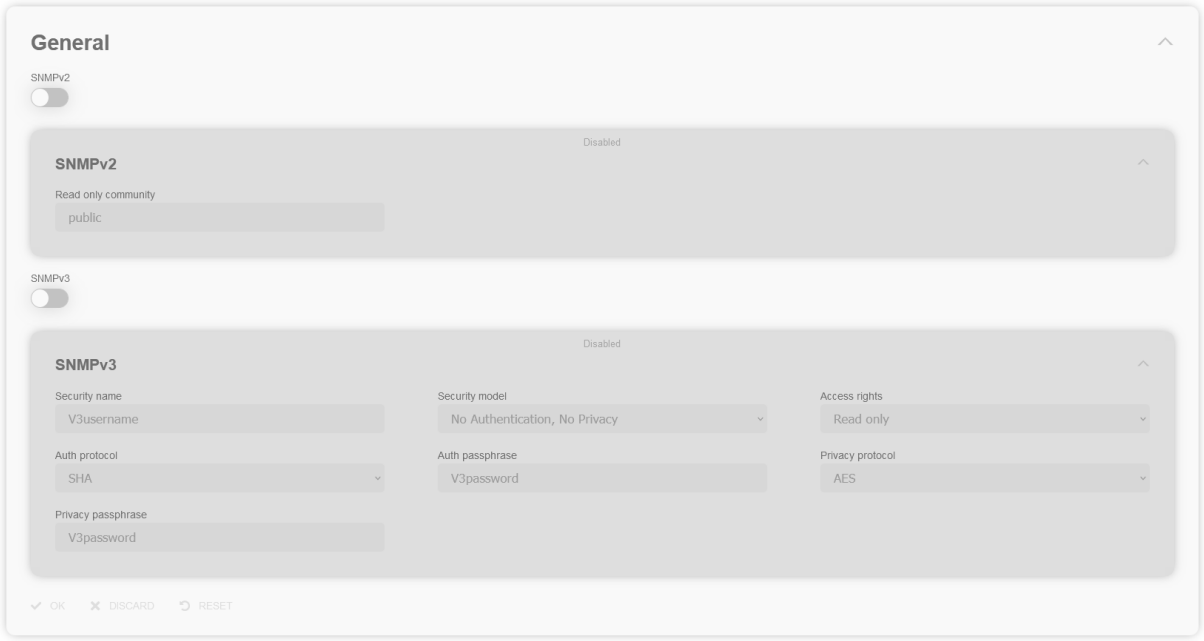


Figure 132 SNMP general section with disabled SNMPv2 and SNMPv3

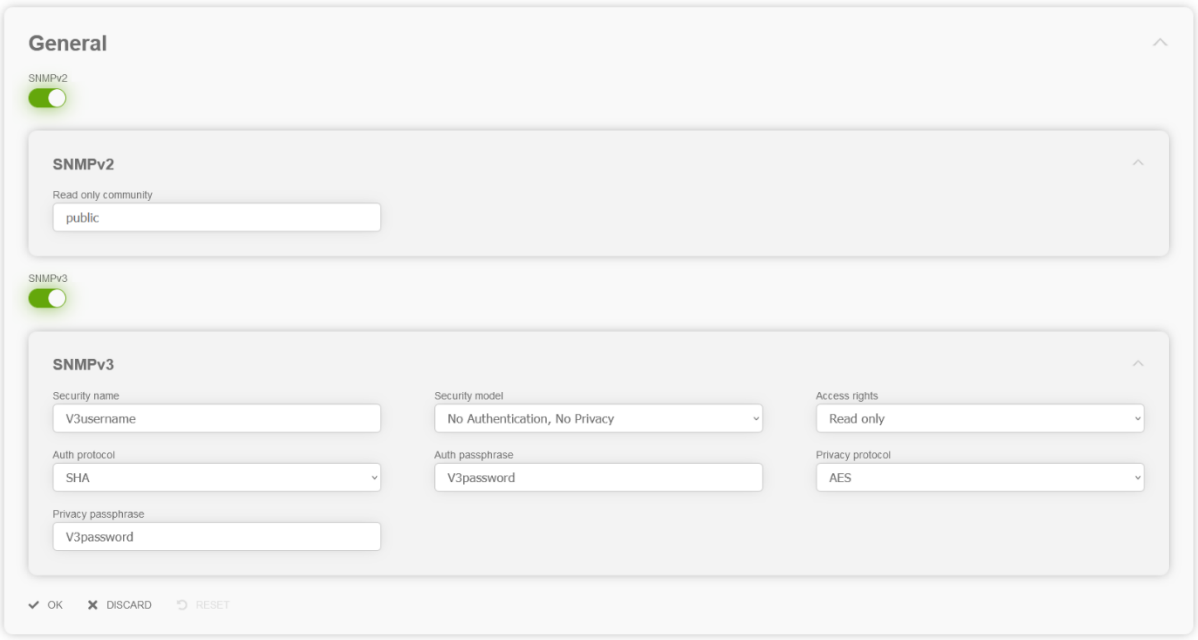


Figure 133 SNMP general section with enabled SNMPv2 and SNMPv3

Input Label	Description
SNMPv2	With this setting SNMPv2 can be turned on and off.
SNMPv3	With this setting SNMPv3 can be turned on and off.

SNMPv2

Input Label	Description
Read only community	The SNMP read only community string is like a password. It is sent along with each SNMP Get-Request and allows (or denies) read-access to the device. By default, the password is set to "public". (This is the so-called "default public community string".)

SNMPv3

Input Label	Description
Security name	The security name representing the user on whose behalf the message was received. The security name has a format that is independent of the Security model.
Security model	Security model is a security strategy used by the SNMP agent. No Authentication, No Privacy (noAuthNoPriv) – Authenticates with a username Authentication, No Privacy (authNoPriv) – Provides HMAC, MD5 or SHA algorithms for authentication Authentication & Privacy (authPriv) – The protocols used for Authentication are MD5 and SHA; for Privacy DES (Data Encryption Standard) and AES (Advanced Encryption Standard) protocols can be used.
Access rights	Defines the access rights for SNMPv3 access. Only "Read only" is supported.
Auth protocol	The auth protocol can be set to MD5 or SHA.
Auth passphrase	Authorization password of the user.
Privacy protocol	Privacy protocol type, either DES or AES.
Privacy passphrase	Decryption password that serves as the private key for encryption.

SNMP traps

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

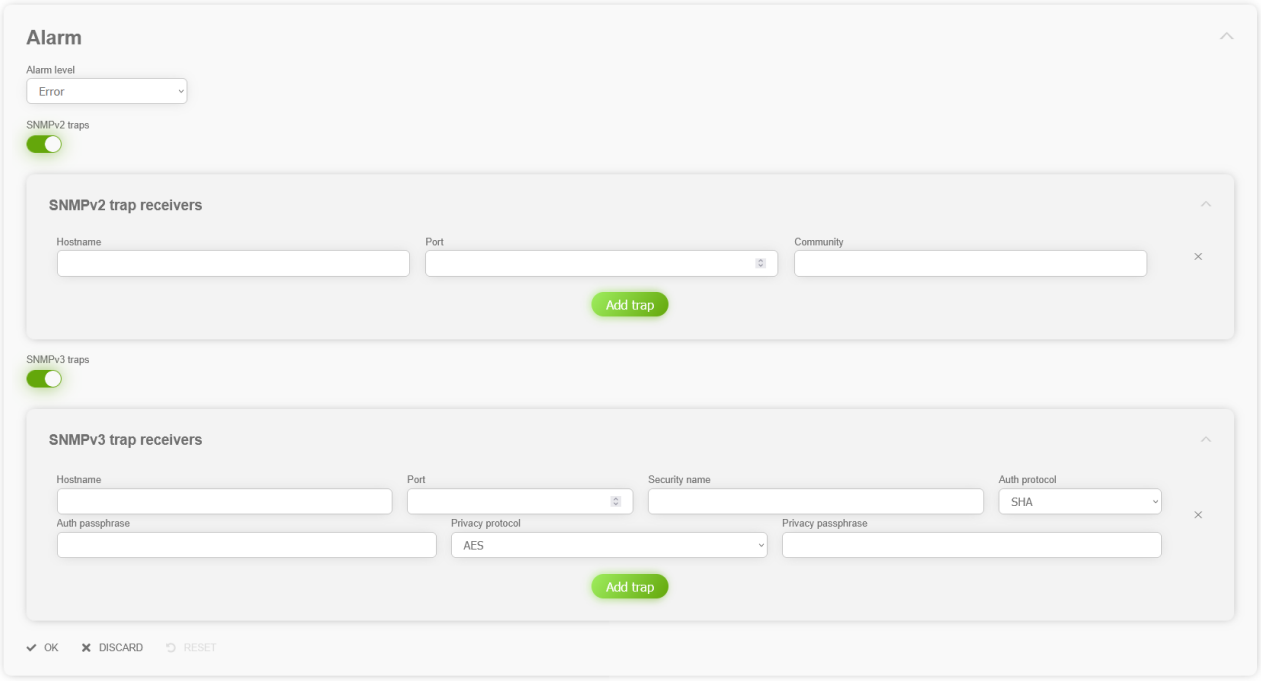


Figure 134 SNMP traps configuration section

Input Label	Description
Alarm level	The alarm level defines the minimum event type that an event must have in order to be sent to the host. The event types info, warn and error can be selected. For more detail see 5.6.
SNMPv2 traps	With this setting SNMPv2 traps can be activated.
Hostname	Specifies the name of the target host. An IPv4/IPv6 address or hostname is valid.
Port	Indicates the port on the target host for receiving trap messages.
Community	The SNMP trap community string is used when an SNMP trap is sent by a device.
SNMPv3 traps	With this setting SNMPv3 traps can be activated.
Hostname	Specifies the name of the target host. An IPv4/IPv6 address or hostname is valid.
Port	Indicates the port on the target host for receiving trap messages.

Security name	The security name representing the user on whose behalf the message was received. The security name has a format that is independent of the Security model.
Auth protocol	The auth protocol can be set to MD5 or SHA.
Auth passphrase	Authorization password of the user.
Privacy protocol	Privacy protocol type, either DES or AES.
Privacy passphrase	Decryption password that serves as the private key for encryption.

6.6.5.5 Relay

6.6.5.5.1 Config

The switchover points of the relay can be configured by the use of the components on this page.

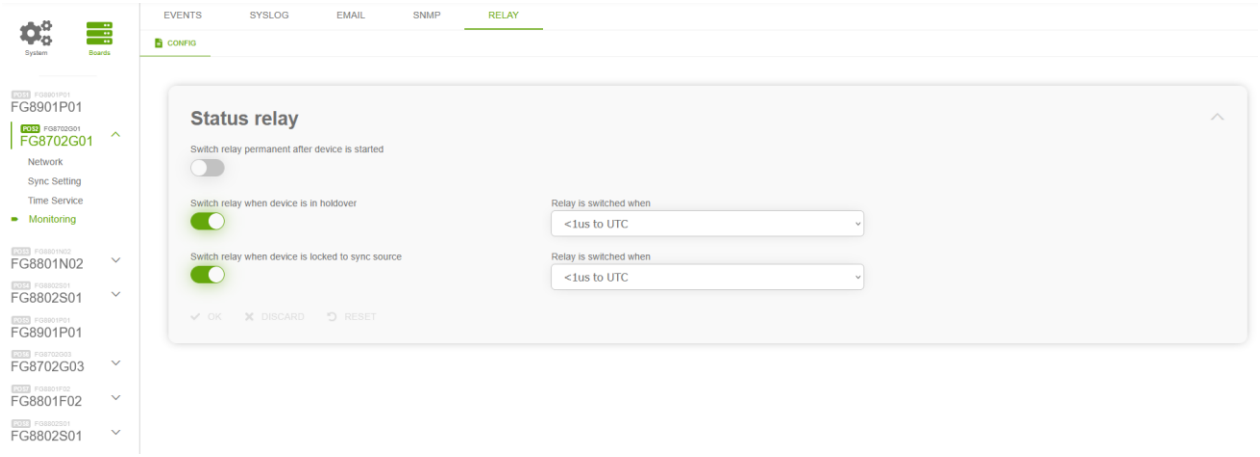


Figure 135 Synchronization status relay configuration section

If Switch relay permanent after device is started is enabled, the relay will switch through after the start-up of the board and will stay in this position until a reboot or a power-down happens. If Switch relay permanent after device is started is not enabled, the relay switches through when the total time error to UTC of this board is within the values defined in the dropdowns.

6.7 Other Pages

6.7.1 Setup wizard

After login the user is brought to the Setup wizard page until he finishes the wizard via clicking the Finish setup button. After a factory default the Setup wizard is active again.

If logged in as administrator, the Setup wizard lets you change the passwords of all local users in one step.

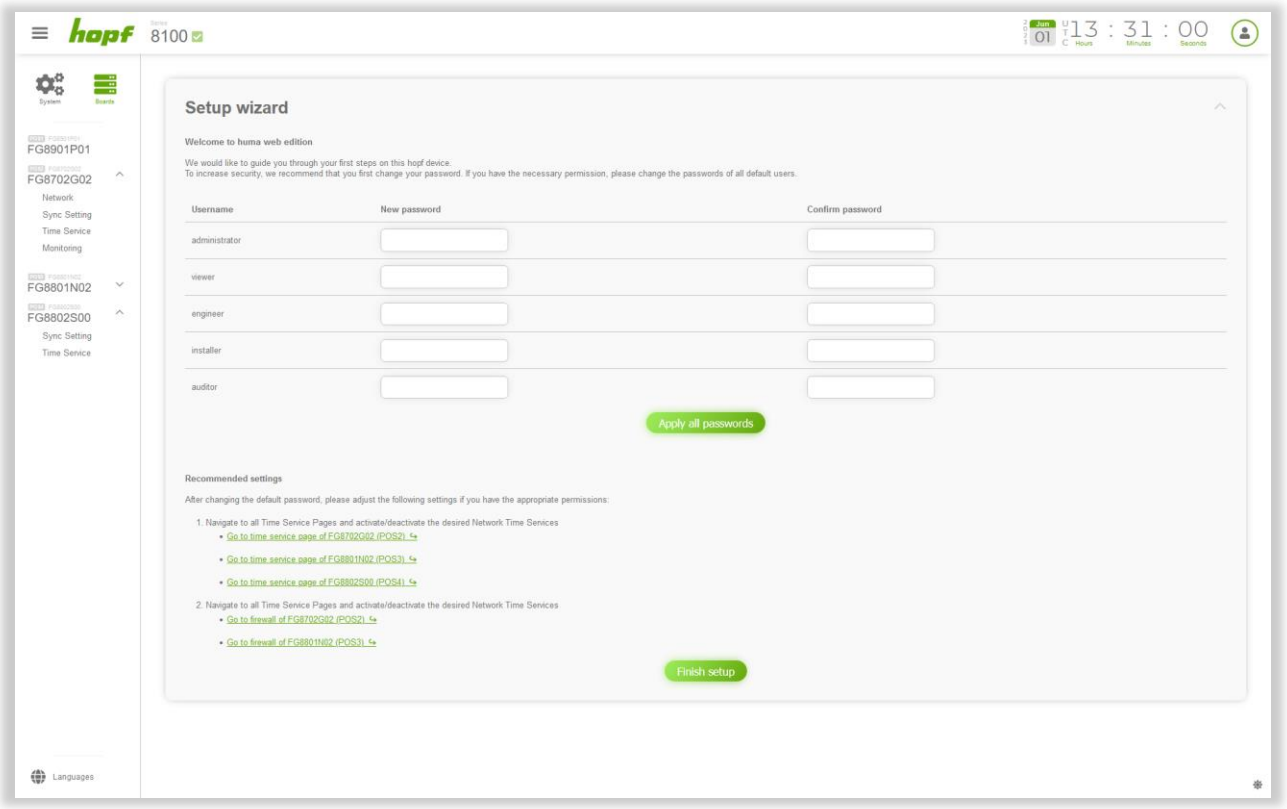


Figure 136 Administrator setup wizard page

When logged in with a local user different than administrator, the Setup wizard lets you change the password of the actual user.

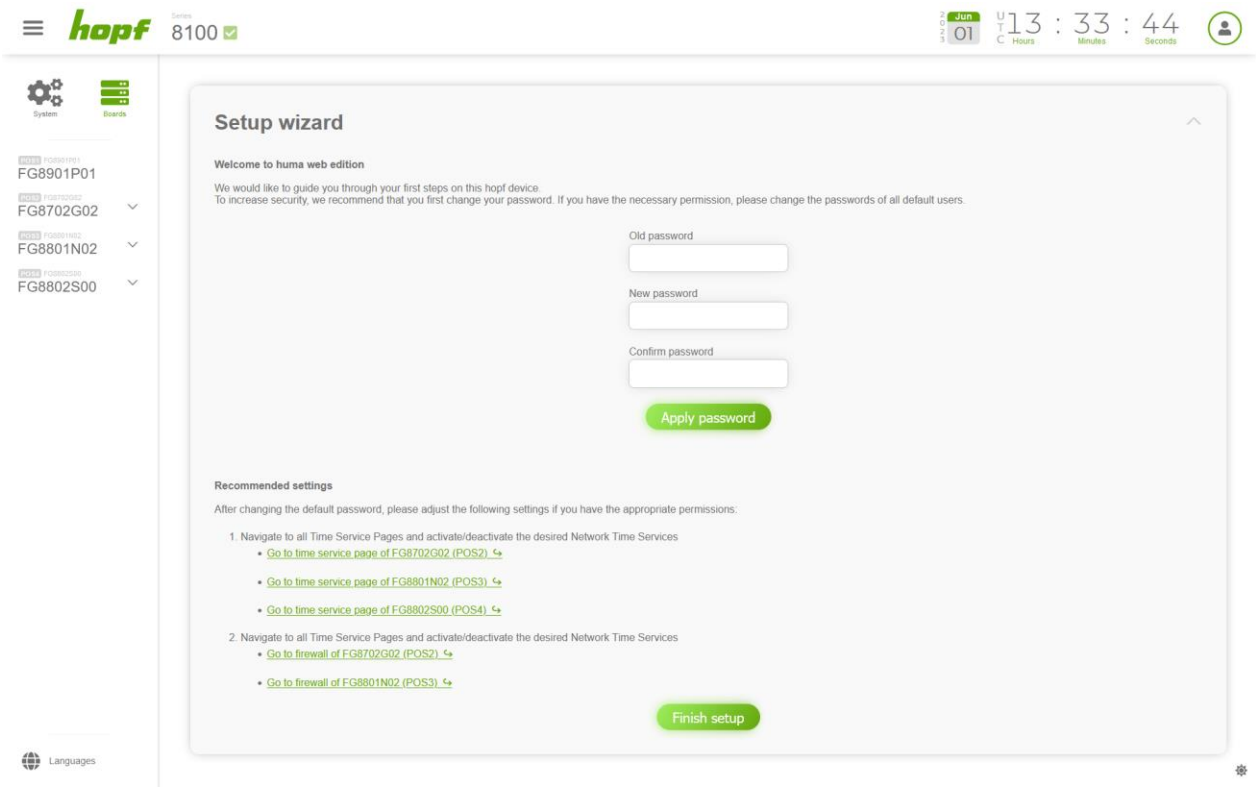


Figure 137 Non administrator setup wizard page

In both cases recommended setting changes are displayed.

Click the Finish setup button when you have finished your initial setup.

6.7.2 No Access

A user who does not have the required permission (see 6.5.4.1.1) to access a particular page (for example a status, action, or config page) encounters this page.

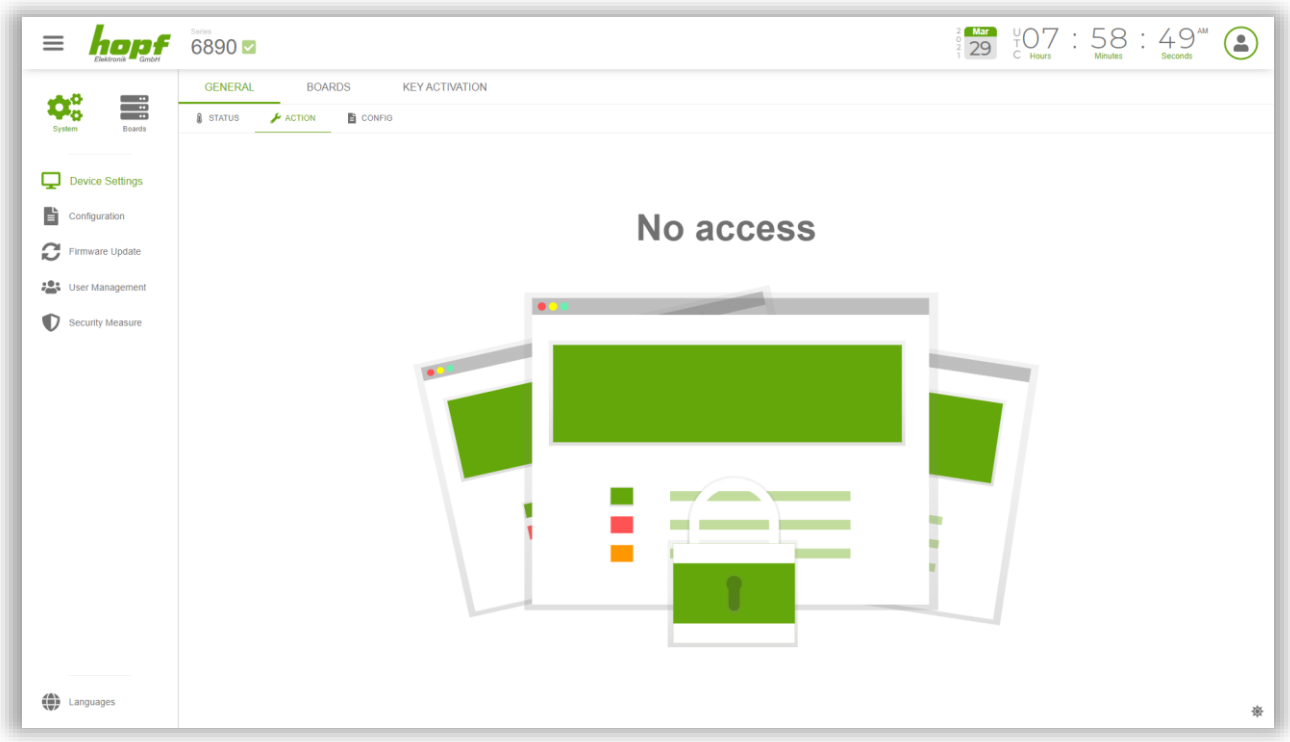


Figure 138 No access page

6.7.3 Page not found - 404

If an URL was entered in the browser address bar that does not correspond to any page existing in huma®, this page will be displayed.

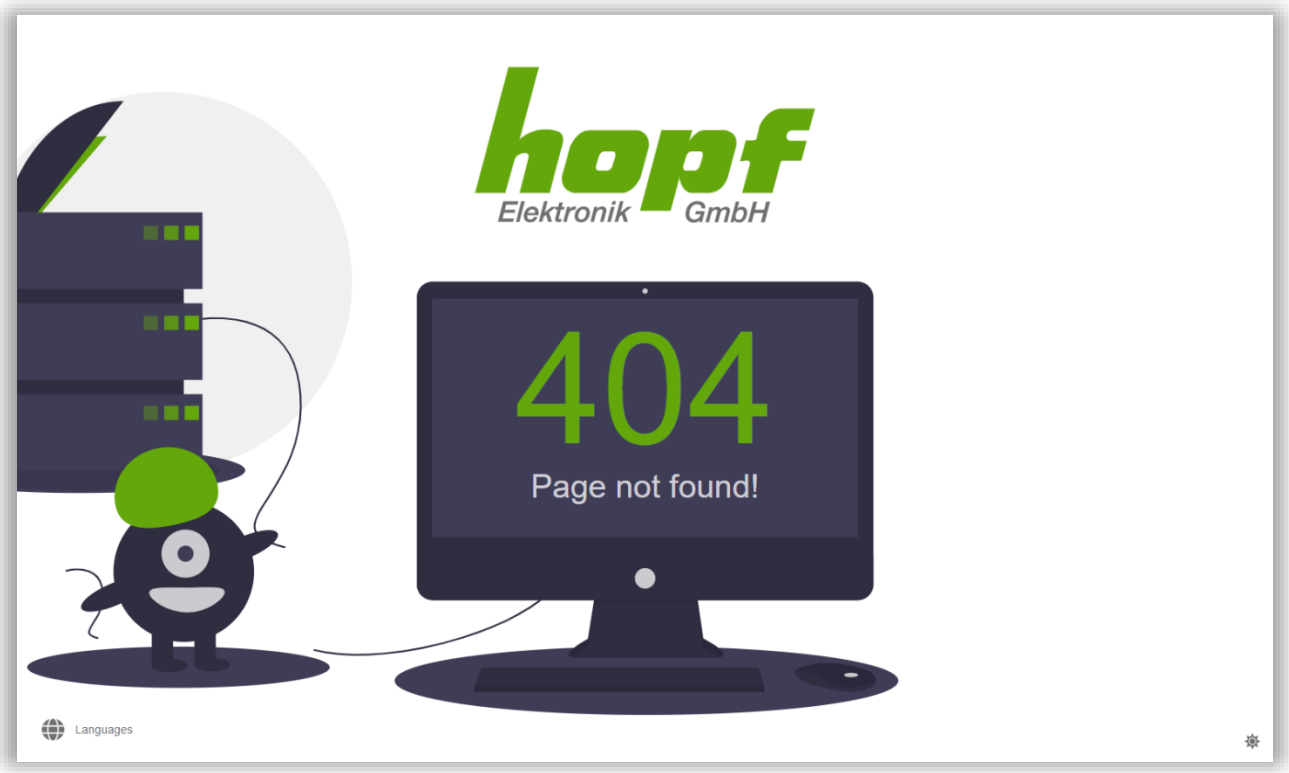


Figure 139 Page not found page