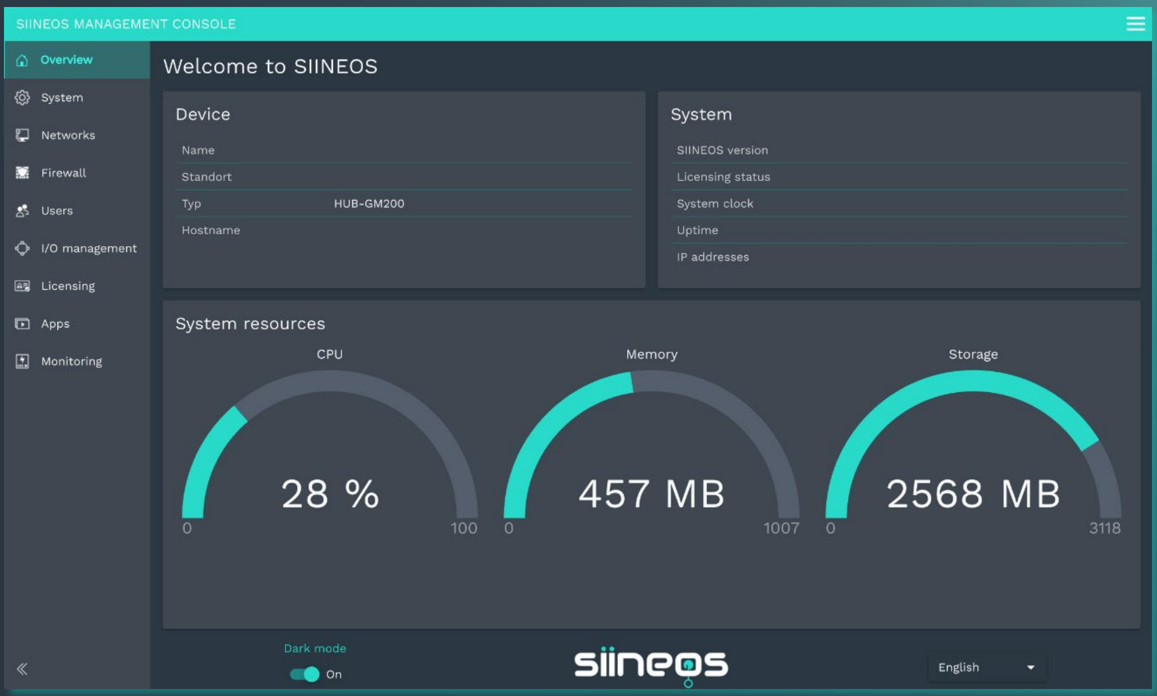


SIINEOS MANAGEMENT CONSOLE

Welcome to SIINEOS

Device

Name	
Standort	
Typ	HUB-GM200
Hostname	

System

SIINEOS version
Licensing status
System clock
Uptime
IP addresses

System resources

Dark mode: On

English

USER MANUAL

Software SIINEOS

Software version 2.8.1.

Release date 2024-07-12

Table of contents

1 Legal notice

Warning concept

This manual contains information that you must observe for your personal safety and to prevent damage to property. Warnings are presented in decreasing order of hazard level as follows:

⚠ **DANGER**

Indicates a direct hazard for humans. Irreversible injuries or death will result if not observed.

⚠ **WARNING**

Indicates a recognizable hazard for humans. Irreversible injuries or death may result if not observed.

⚠ **CAUTION**

Indicates a recognizable hazard for humans or possible damage to property. May lead to reversible injuries or damage to property if not observed.

ATTENTION

Information on potential damage to property. May cause damage to property if not observed.

NOTE: Under “Note”, you will find tips, recommendations, and useful information on specific actions and facts.

If several hazard levels occur, the warning for the highest level is always used. If the triangle warning against personal injury is used in a warning, then a warning against property damage can also be added to the same warning notice.

Qualified personnel

The product associated with this documentation may only be handled by personnel qualified for the respective task. Furthermore, the product may only be handled in compliance with the associated documentation and the safety and warning instructions contained therein. Due to their training and experience, qualified personnel are equipped to recognize and avoid potential hazards when handling these products.

Basic knowledge required

Knowledge of personal computers, operating systems, and programming is a prerequisite. General knowledge in the field of automation technology is recommended.

Safety instructions

Before commissioning the product, be sure to read the safety regulations carefully and observe the corresponding information in the manual. Always keep the User Manual within reach.

Intended use

in.hub products may only be used for the applications specified in the corresponding technical documentation.

If third-party products and components are used, they must be recommended or approved by in.hub.

Proper storage, setting up, assembly, installation, commissioning, operation, and maintenance are essential for the correct and safe operation of the product.

The permissible environmental conditions must be complied with. Information in the associated documentation must be observed.

Trademarks

All names marked with the symbol “®” are registered trademarks. Other names in this document may be trademarks whose use by third parties for their own purposes may infringe on the rights of the owners.

Disclaimer

The content of this publication has been checked for conformity with the hardware described. Nevertheless, discrepancies cannot be ruled out, so we do not assume any liability for its completeness and correctness. The information in this publication is reviewed on a regular basis. Any corrections needed will be included in the subsequent editions.

2 General information

This User Manual contains all the information you need to configure and set up your gateway with SIINEOS.

This manual is intended for system administrators who are commissioning a gateway or an add-on module and connecting it to other units (automation systems, mobile terminals, personal computers, etc.), as well as for service and maintenance technicians who are installing extensions or performing error analyses.

2.1 Scope of delivery

1 x SIINEOS operating system

1 × User Manual SIINEOS (PDF)

2.2 Network security

Please keep in mind that the product does not encrypt communication within the internal network. Therefore, protect your network against unauthorized access from outside! The integration into a network with Internet access must be carried out with special care. For this, it is essential to talk with your system administrator in advance.

2.3 Service and support

If you have any questions about specific use cases or about technical parameters, please contact us.

Community:	https://community.inhub.de/
Email:	service@inhub.de
Phone:	+49 371 335 655 00 (Technical Sales Staff)

These details will connect you with the appropriate contact.

3 Product information

SIINEOS is a Linux-based operating system and IoT platform specifically designed to meet the requirements of data security and continuity for operating procedures in the industrial sector.

It supports all common interfaces and fieldbus protocols for the direct connection of sensors, controllers, and other peripheral devices.

Furthermore, SIINEOS supports easy data acquisition, data preprocessing, and data connection to third-party systems, thus reducing the complexity of IoT and digitalization projects and making it easier to start working with them.

Extensive documentation on SIINEOS and a user-friendly software development kit make it possible to use all the potential of our industrial gateways quickly and efficiently. Regular software updates keep you up to date.

3.1 Software architecture

SIINEOS comprises four levels:

- Boot level
- System level
- In.Core framework

  Collection of software building blocks that can be used to quickly create both simple and complex IoT and IIoT applications.

- Application level with the In.Core apps.

  These consist of generic and parent objects and can be easily configured and combined using the QML language. Each In.Core module can be imported individually and contains the actual function objects.

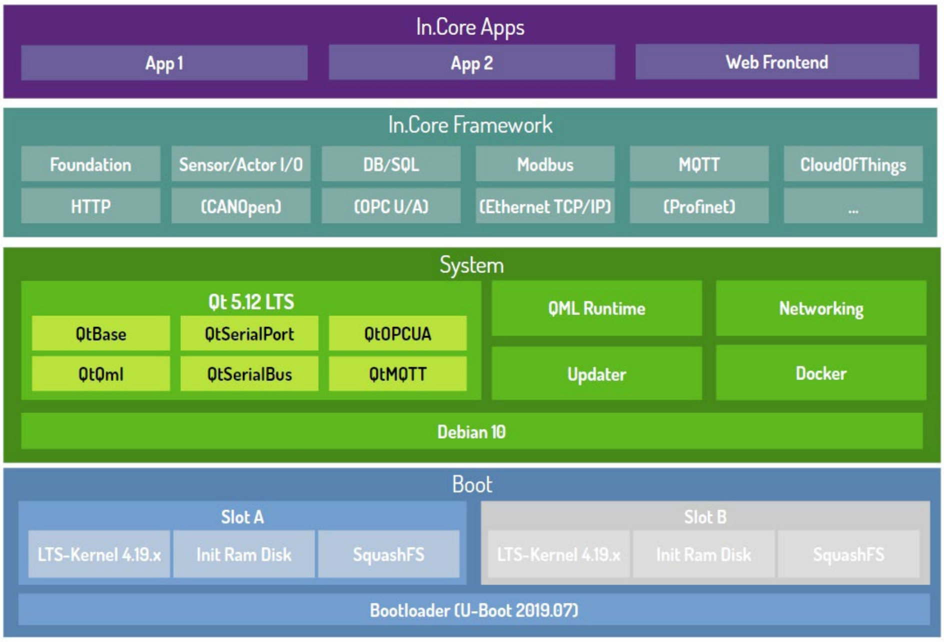


Fig. 1: SIINEOS software architecture

4 Setting up the working environment with SIINEOS

In this section, you will find detailed step-by-step instructions for configuring SIINEOS and setting up your working environment.

In short, you can also get help via tooltips in the SIINEOS UI when you move the mouse over a button or an input field.

You can also download all current technical documents, as well as software packages, tutorials, and installation instructions from the in.hub download portal:

https://download.inhub.de/

4.1 Preparing the IT infrastructure in your own company network

1. Ensure that the following ports are enabled by the system to enable communication between the devices and applications:

Ports	Access to SMAC
1989	SMAC interface (for https access)
1988	SMAC interface (for http access)
443	HTTPS
80	HTTP

Ports	Access to device services and apps
4840	OPC UA
3000	Grafana
1883	MQTT
502	Modbus TCP

2. If you want to encrypt communication with the gateway using TLS certificates, create a security certificate via the Certification Authority (CA) of your organization.

   You can upload this certificate together with the private key in SIINEOS, see Optional: Configuring TLS-Certificates, page 17.

4.2 Logging in to SIINEOS

NOTE: The latest versions of **Firefox, Edge** or **Chrome** browsers are recommended for SIINEOS. Using other or older browsers may cause compatibility issues.

NOTE: Make sure that the gateway is connected to the PC.

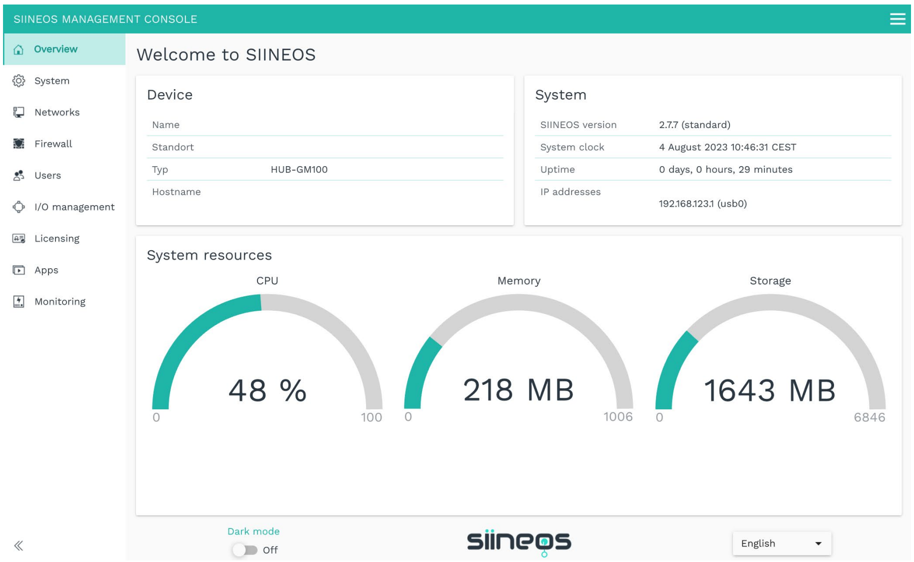
When you log in to SIINEOS for the first time

1. Enter the following address in your browser:

   http://192.168.123.1/smac

2. Log in with the initial user data (**hubadmin/hubadmin**).

   The SIINEOS management console opens.



Device

Name	
Standort	
Typ	HUB-GM100
Hostname	

System

SIINEOS version	2.7.7 (standard)
System clock	4 August 2023 10:46:31 CEST
Uptime	0 days, 0 hours, 29 minutes
IP addresses	192.168.123.1 (usb0)

Fig. 2: Home page of SIINEOS (example)

On the start page, you will now see information about your system, e.g., the current SIINEOS version, name of the device, location, type, system resources, etc.

3. Select the **Users** page and change the password of the **hubadmin** user. See the section Managing user accounts, page 34.

If you have already set up SIINEOS

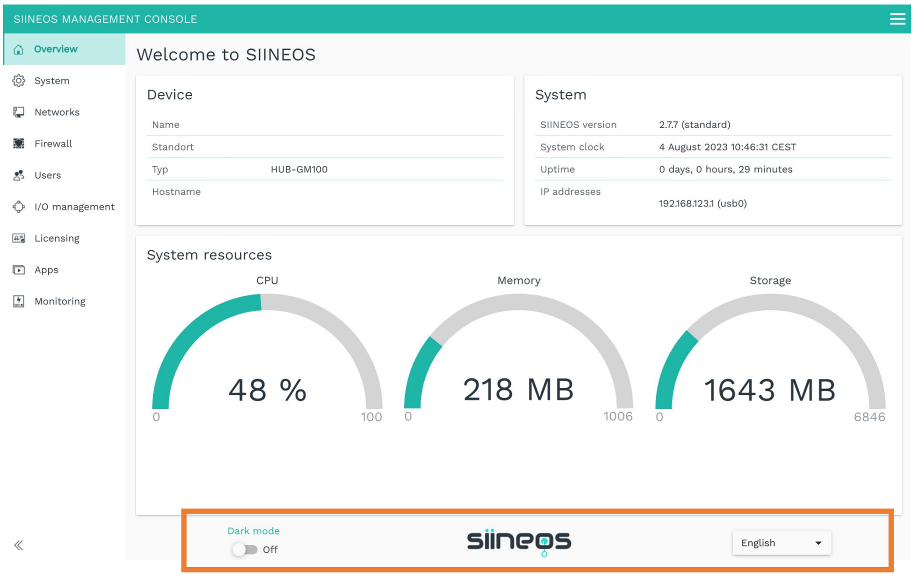
1. In your browser, enter the individual IP address you configured. See the section Setting up Ethernet 1 and Ethernet 2, page 19.

2. Log in with your user data and click **Log in**.

   The SIINEOS management console opens.

4.3 Setting the color mode and language

1. Open the SIINEOS home page by selecting the **Overview** page on the left.



SIINEOS MANAGEMENT CONSOLE

Welcome to SIINEOS

Device

Name	
Standort	
Typ	HUB-GM100
Hostname	

System

SIINEOS version	2.7.7 (standard)
System clock	4 August 2023 10:46:31 CEST
Uptime	0 days, 0 hours, 29 minutes
IP addresses	192.168.123.1 (usb0)

System resources

CPU	Memory	Storage
48 % (0–100)	218 MB (0–1006)	1643 MB (0–6846)

Dark mode: Off — English

Fig. 3: “Overview” page with color mode and language settings (example)

2. By default, the dark mode is selected for the screen display. To switch to the light screen mode, set the **Dark mode** slider to **Off**.
3. To change the language, open the drop-down list.

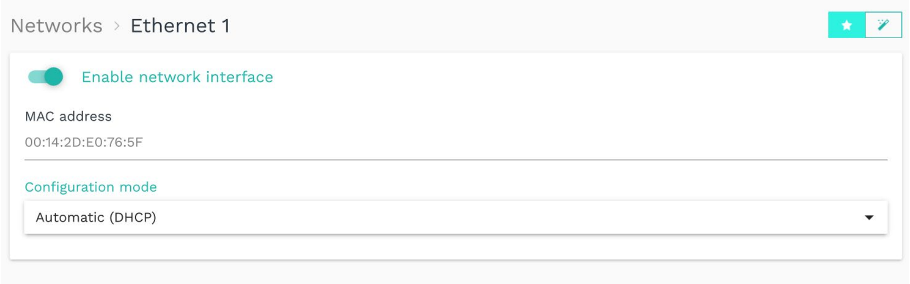
   German and **English** are available.

4.4 Viewing mode: Default and Advanced

You can only make configurations in SIINEOS with the system administrator role.

Within this role, there are two viewing modes with which you can display additional settings on some pages. You will find the two buttons for switching at the top right.

- **Standard** mode is activated when SIINEOS is started. Only the parameters and setting options that are sufficient for most applications are displayed. This makes the configuration clearer for you.



Networks › Ethernet 1

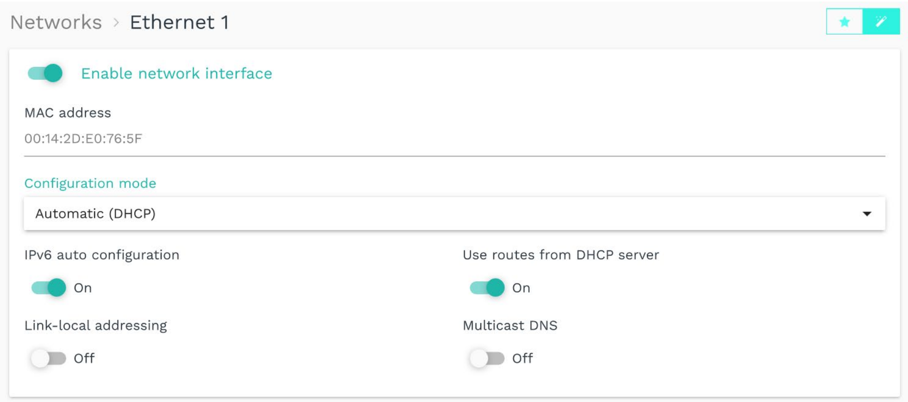
Enable network interface

MAC address: 00:14:2D:E0:76:5F

Configuration mode: Automatic (DHCP)

Abb. 4: Viewing mode “Standard“ using the example of the network settings

- If you switch to **Advanced** mode, you will be shown additional parameters and setting options that cover special cases. Here you can define every detail of your configuration yourself.



Enable network interface

MAC address
00:14:2D:E0:76:5F

Configuration mode
Automatic (DHCP)

IPv6 auto configuration: On

Use routes from DHCP server: On

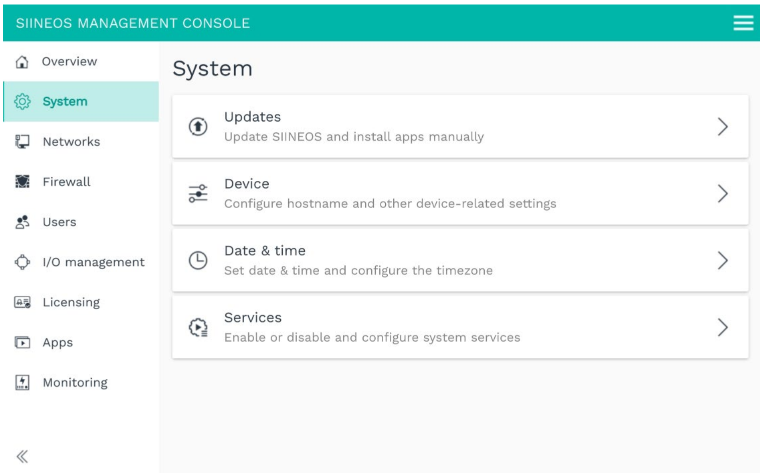
Link-local addressing: Off

Multicast DNS: Off

Abb. 5: Viewing mode “Advanced“ using the example of the network settings

4.5 Configuring the system

On the **System** page, you can enter or configure the following system settings and information:



System

Updates
Update SIINEOS and install apps manually

Device
Configure hostname and other device-related settings

Date & time
Set date & time and configure the timezone

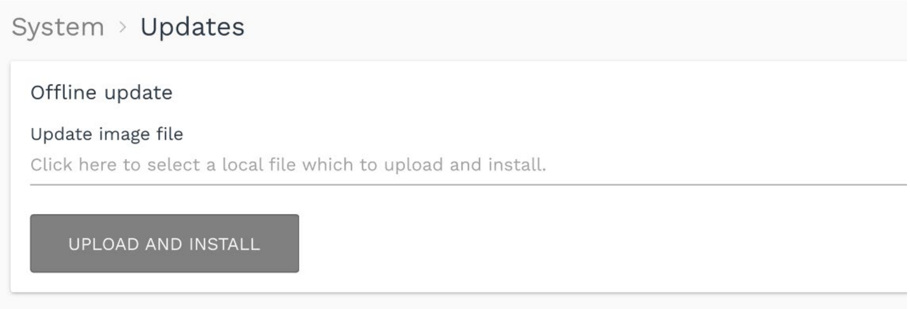
Services
Enable or disable and configure system services

Fig. 6: “System” page

4.5.1 Uploading SIINEOS updates and application software packages (apps)

You can only upload updates on the **System** page if you have a valid SIINEOS license.

If the license has expired, you will be informed that you cannot make any updates.



System › Updates

Offline update

Update image file

Click here to select a local file which to upload and install.

Fig. 7: System > Updates

Update SIINEOS

NOTE: As soon as a SIINEOS update is available, in.hub provides the software package. Therefore, check the in.hub download portal regularly to see if new updates are available: https://download.inhub.de/

1. Go to the https://download.inhub.de/siineos/ page and select the current SIINEOS version and package.

   Two variants are available: the complete software package and a light variant with no Docker container and with a smaller file size.
2. When the download is complete, go to the **System** page in SIINEOS and select **Updates.**
3. Click in the **Update image file** input field and select the software bundle from your local file store.
4. Click **Upload and install**.

   The installation runs automatically.

   After successful installation, you will be asked if you want to restart the gateway.
5. Click **Yes**.
6. After restarting, check on the **Overview** page that the new version of SIINEOS is displayed.
7. If the version has not been updated, proceed as follows:
   - First, clear your browser cache and refresh the page in your browser.
   - If that doesn't work:

     Disconnect the gateway from the power supply and reconnect it after a few seconds.
   - Start SIINEOS and check the version number.

Install app updates

1. On the **System** page, click **Updates.**
2. Click in the **Update image file** input field and select the software bundle provided by in.hub in `*.raucb` format from your local file store.
3. Click **Upload and install**.

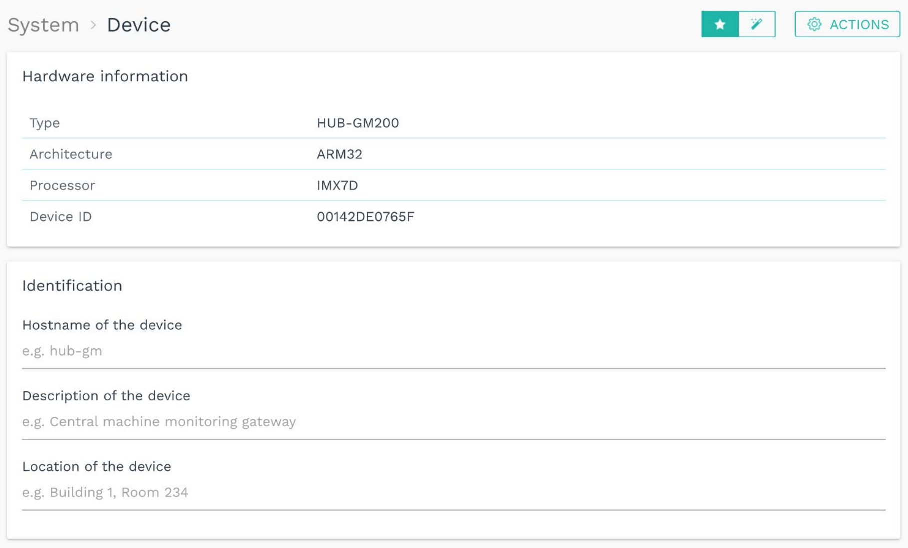
   The installation runs automatically.

   You will then be prompted to restart the gateway.
4. Click **No**.

   You do not need to restart the gateway when uploading apps.

4.5.2 Making device settings

1. On the **System** page, click **Device.**



Hardware information

Type	HUB-GM200
Architecture	ARM32
Processor	IMX7D
Device ID	00142DE0765F

Identification

Hostname of the device
e.g. hub-gm

Description of the device
e.g. Central machine monitoring gateway

Location of the device
e.g. Building 1, Room 234

Fig. 8: System > Device (example)

In the **Hardware information** section, you will find details about your gateway, such as the device ID or the installed processor.

2. Make the following entries in the input fields:
   - **Host name of the device**: Enter a name to uniquely identify the device in the network.
   - **Description of the device**: Enter what the device is used for.
   - **Location of the device**: Enter the physical location of the device so that you can quickly find the control cabinet and device if necessary.
3. The following functions are available in **Advanced** viewing mode:
   - **Log debug messages**

     Messages from the SIINEOS management service are logged in the system journal, which help in.hub with troubleshooting.

- **Log trace messages**

  Activate this function if detailed calls of system functions and the parameters used are to be logged in the system journal.

NOTES: Do not activate these functions in productive operation, as otherwise performance losses are to be expected.

On the **Monitoring** page under **Journal**, you can view the debug and trace messages and download them using a button.

Please note that the messages are only saved temporarily and will be lost after a restart. You should save them regularly.

4. When you have completed the input, click **Save & close**.

4.5.3 Locating the gateway in the control cabinet

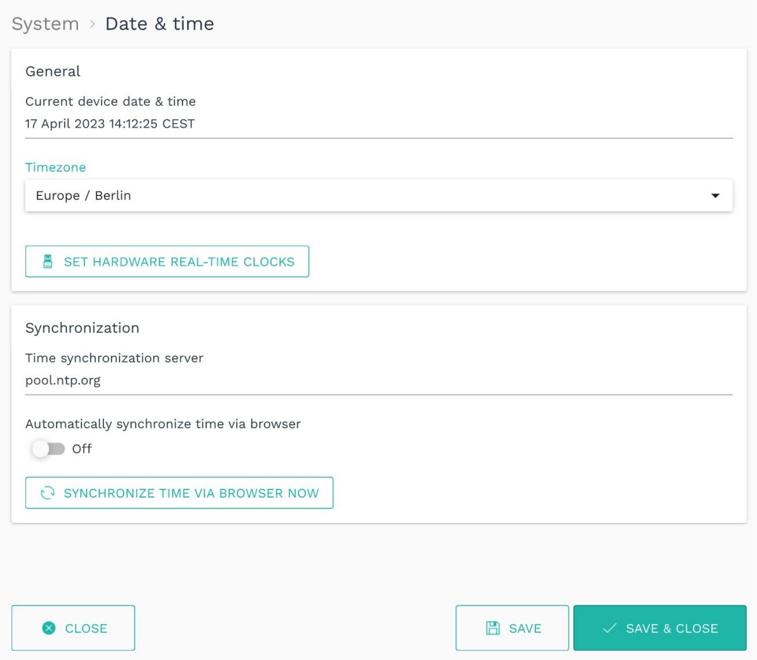
To keep track of which device you are currently making settings on when using several gateways, there is the function **Identify via LEDs** in SIINEOS.

1. On the **System** page, click **Device**.
2. Click the **Actions** button and select **Identify via LEDs**.

   On the gateway you are currently on, the device identification LED on the front panel will start flashing red and green alternately for 10 seconds.

4.5.4 Setting the date and time

1. On the **System** page, click **Date & time**.



System › Date & time

General

Current device date & time
17 April 2023 14:12:25 CEST

Timezone
Europe / Berlin

Synchronization

Time synchronization server
pool.ntp.org

Automatically synchronize time via browser
Off

SET HARDWARE REAL-TIME CLOCKS
SYNCHRONIZE TIME VIA BROWSER NOW
CLOSE
SAVE
SAVE & CLOSE

Fig. 9: System > Date & time (example)

The current system time of the gateway is displayed under **General**. When logging in for the first time, the UTC time is displayed.

2. Select the **time zone** where your gateway is located.

3. Optional: If you are using a HUB-MRT100 or a HUB-RT100, you can write the gateway's system time to the real-time clock on the USB stick by clicking **Set hardware real-time clocks**.

   See also Optional: Calibrating the HUB-MRT100 / HUB-RT100, page 15.

4. If you want to obtain the system time of your gateway from a central NTP server, enter the server address under **Time synchronization server**.

5. If you want to synchronize the system time of your gateway with the system time of your browser, set the **Automatically synchronize time via browser** slider to **On**.

6. Click **Synchronize time via browser now** to synchronize the date settings for the gateway with your computer.

   If the gateway has been switched off and you are not using an external real-time clock for the time, this setting will be lost. You must then synchronize again with the browser. The time zone is kept.

7. When you have completed the input, click **Save & close**.

NOTE: If you enter an NTP server for the synchronization of the time on this page, it will automatically be adopted in the configuration of the **Wi-Fi** and **Ethernet** networks. However, if an address is already entered there, it will not be overwritten. You should therefore check your entries for the NTP server.

4.5.5 Optional: Calibrating the HUB-MRT100 / HUB-RT100

HUB-MRT100 is a USB stick that stores the system time on the one hand and process data on the other, so that this information is not lost in the event of a power failure.
HUB-RT100 only stores the system time.

If you use one of the two real-time clocks, a calibration function is available in SIINEOS. This allows you to transfer and save the system time of the gateway to the stick.

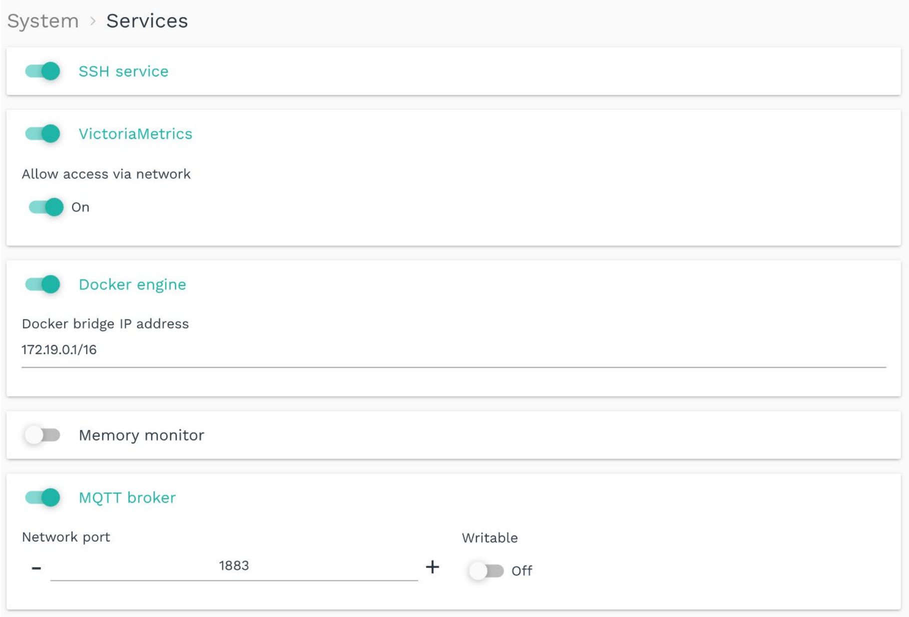
1. Plug the HUB-MRT100 or HUB-RT100 into a USB port on your gateway.

   If there is not enough space in the control cabinet, you can also use a USB extension cable or a USB HUB.

   As soon as the stick is plugged in, the LED in the stick lights up, indicating that the external real-time clock is working.
2. In SIINEOS navigate to **System > Date & Time**.
3. First click **Synchronize time via browser now** to ensure that the gateway time is in sync with the computer.
4. Now click **Set hardware real-time clocks** to transfer the system time to the external real-time clock.
5. Leave the stick permanently plugged into the device so that the gateway can always get the time from the HUB-MRT100 or the HUB-RT100 if the power supply is interrupted.

4.5.6 Configuring system services

1. On the **System** page, click **Services**.
2. Activate the slider for the service you want to use. If there are further setting options, the entry expands.



System › Services

SSH service

VictoriaMetrics

Allow access via network

On

Docker engine

Docker bridge IP address

172.19.0.1/16

Memory monitor

MQTT broker

Network port

- 1883 +

Writable

Off

Fig. 10: System > Services (example)

3. Make the following entries in the input fields and with the sliders:

SSH service	If you want to access the gateway with an SSH client, set the slider to **On**. The SSH service allows direct access to the system and data, as well as troubleshooting. In conjunction with the OpenVPN client, a gateway can also be accessed from outside the local network.
VictoriaMetrics	If you want to use the local VictoriaMetrics time series database to record I/O signal values, set the slider to **On**. Set the **Allow access via network** slider to **On** if the VictoriaMetrics service is to be publicly accessible via the network.
Docker-Engine	Set the slider to **On** if you want the Docker Engine to start automatically at system startup. If you are using your own Docker container with the "Always" restart policy, activate the autostart of the Docker Engine here. If you are using an app in SIINEOS that uses the Docker engine anyway, such as Grafana, you can leave this slider deactivated. Here you can enter a different IP address for the Dockerbridge if the default IP address is already used in the company.

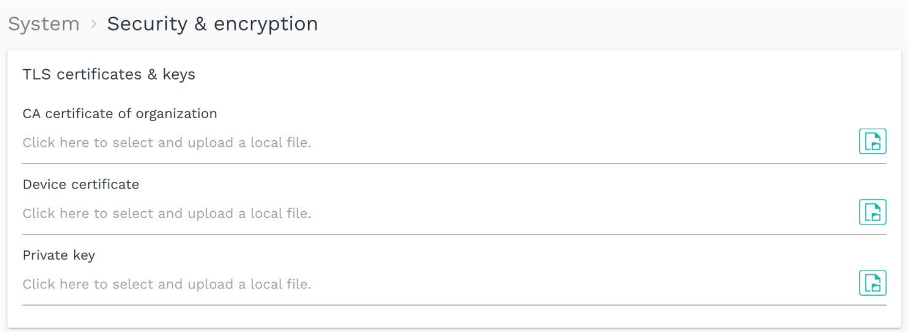
Memory monitor	Set the slider to **On** to automatically restart the gateway when memory is insufficient.
MQTT broker	Set the slider to **On** to publish the local system bus via an MQTT broker. Change the default **Network port** if necessary. If external clients are to publish messages on the bus, set the **Writable** slider to **Off**.

4. When you have completed the input, click **Save & close**.

4.5.7 Optional: Configuring TLS-Certificates

If you want to communicate with the gateway in encrypted form (https), you can upload the necessary security certificates on this page.

1. On the **System** page, click on Security & encryption.



System > Security & encryption

TLS certificates & keys

CA certificate of organization

Click here to select and upload a local file.

Device certificate

Click here to select and upload a local file.

Private key

Click here to select and upload a local file.

Fig. 11: System > Security & encryption

2. Ff the gateway is to communicate with other devices and services in encrypted form (e.g. MQTT), click on **CA certificate of organization** to upload the CA certificate.

   With this CA certificate, the gateway can check whether the certificates of the devices and services of your organization are valid. If this validity check fails, no encrypted connection can be established.

3. Click on **Device certificate** to upload the security certificate created by your organization for this device.

4. Click on **Private key** to upload the corresponding key for this device.

4.6 Restarting, shutting down, or logging off

1. In the SIINEOS management console, click the button in the upper right corner ☰.

   A menu opens.

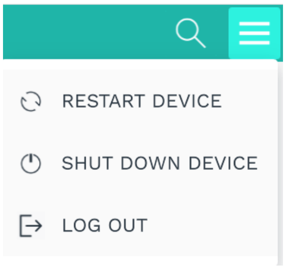


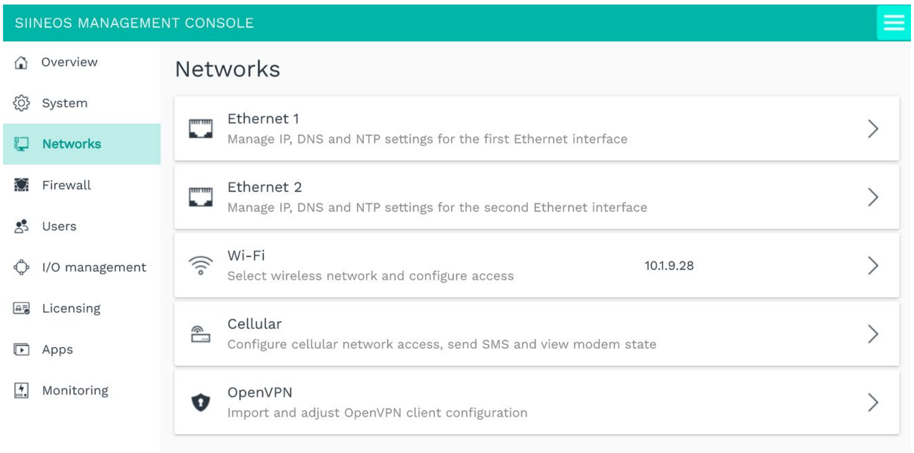
Fig. 12: Menu with actions for the current session

2. Select the action you want to perform:

Restart device	A system message is displayed asking if you really want to restart the gateway. 1. Confirm with **Yes**. After the restart, the login window is displayed again.	Possible reasons for a restart: - When the system stops responding - If you have postponed the restart after an update, for example, and want to do it later - If the new version is not displayed after an SIINEOS software update
Shut down device	A system message is displayed asking if you really want to shut down the gateway. 1. Confirm with **Yes**. All apps and SIINEOS will shut down safely and still-opened/buffered data will be stored. **NOTE**: After shutdown, you can only connect to the gateway using the micro-USB cable and the IP address http://192.168.123.1/smac.	Possible reasons for a shutdown: - If you want to prepare maintenance work on the power supply - If you want to shut down cleanly at the end of a demonstration and avoid data loss due to abrupt shutdown during a write operation.
Log out	You log out of the system and allow another user to log in.	Possible reasons for logging off: - Shift change

4.7 Configuring networks

On the **Networks** page, you can configure the following connections:



SIINEOS MANAGEMENT CONSOLE

Networks

Ethernet 1
Manage IP, DNS and NTP settings for the first Ethernet interface

Ethernet 2
Manage IP, DNS and NTP settings for the second Ethernet interface

Wi-Fi
Select wireless network and configure access
10.1.9.28

Cellular
Configure cellular network access, send SMS and view modem state

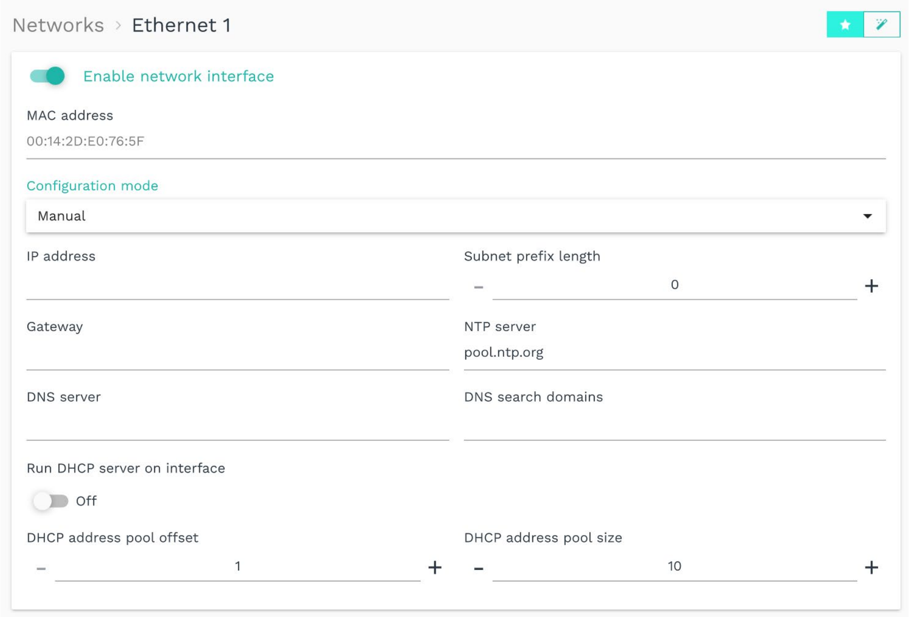
OpenVPN
Import and adjust OpenVPN client configuration

Fig. 13: “Networks” page (example)

4.7.1 Setting up Ethernet 1 and Ethernet 2

On the **Ethernet 1** and **Ethernet 2** pages, you can activate/deactivate the first and second Ethernet interface of your gateway and enter the respective network parameters.

RECOMMENDATION: We recommend **Ethernet 1** for gateway communication in a company network and **Ethernet 2** for gateway communication in an isolated machine network.



Networks › Ethernet 1

Enable network interface

MAC address
00:14:2D:E0:76:5F

Configuration mode
Manual

IP address

Subnet prefix length
– 0 +

Gateway

NTP server
pool.ntp.org

DNS server

DNS search domains

Run DHCP server on interface
Off

DHCP address pool offset
– 1 +

DHCP address pool size
– 10 +

Fig. 14: Networks > Ethernet 1 > Configuration mode “Manual” (viewing mode “Standard”)

1. On the **Networks** page, select **Ethernet 1** or **Ethernet 2.**
2. To enable the interface, set the **Enable network interface** slider to **On.**

   The MAC address printed on the gateway housing is displayed.
3. To automatically obtain all network parameters via a DHCP server, select **Automatic (DHCP)** from the **Configuration mode** drop-down list.

   In **Standard** viewing mode, you do not need to make any entries.

   In **Advanced** viewing mode, you can refine the network configuration.

IPv6 auto configuration	By default, the slider is set to **On**, which means that in addition to the IPv4 address, an IPv6 address is also automatically configured using IPv6 router advertisements from the network and the DHCPv6 client is started.
Use routes from DHCP server	By default, the slider is set to **On** if the routes/gateways, it receives from the DHCP server, are to be registered in the system. Set the slider to **Off** if you only want to access the local network via this interface and access the Internet via another interface if necessary.
Link-local addressing (optional)	Set the slider to **On** if you need a link-local address for local communication within the network segment. The gateway generates the link-local address automatically, so that communication in the same network segment is possible without DHCP or static IP address.
Multicast DNS (optional)	Set the slider to **On** if all nodes in the network are to be addressed directly instead of a query to a DNS server. Gateways are then accessible in the network at **<hostname>.local**. The host name can be found in SIINEOS on the **System > Device** page.

4. To configure the network parameters manually, select **Manual** from the **Configuration mode** drop-down list.
5. Fill in the input fields:

   HINT: For several parameters where you can make multiple entries, e.g. for the DNS server, separate them with a space, not a comma.

IP address	Enter the required IPv4 or IPv6 address of the gateway to be assigned to the Ethernet 1 or Ethernet 2 interface.
Subnet prefix length	Enter the subnet prefix length of the IPv4 or IPv6 address. For IPv4 addresses, the value **24** is typically entered here for networks with subnet mask **255.255.255.0** or the value **16** for networks with subnet mask **255.255.0.0.**
Gateway	Enter the IP address of the gateway.
NTP server (optional)	Enter the IP address or computer name of the time server from which the gateway should obtain its system time.
DNS server	Enter the IP address of the DNS server through which names of computers in the network / on the Internet are to be resolved.

DNS search domains (optional)	Enter the internal DNS domain of your company network, e.g., **lan.mycompany.com**.
Run DHCP server on interface	**NOTE**: We recommend using this function only for a direct one-to-one connection between the gateway and a sensor, a PLC, an add-on module, or a TBEN module. A larger network with multiple machines requires a central IT infrastructure. Set the **Run DHCP server on interface** slider to **On** if you want the gateway to assume the role of DHCP server and assign IP addresses to the connected devices in the isolated machine network.
DHCP address pool offset	Specify which IP addresses are to be assigned for the connected peripheral device. Example: You enter a "12". Starting from the parameter entered under **IP address,** the number after the last dot is replaced by "12", e.g., 10.1.9.**12** If this IP address is already assigned, the device may not be accessible on the network. Change your entries if necessary.
DHCP address pool size	Specify the maximum number of peripherals that can be included in the network. The recommended value is 1. **RECOMMENDATION**: Restart the connected peripheral device so that it can send its requests to the gateway. Only then will the IP address be assigned.
Link-local addressing (only in Advanced viewing mode)	Set the slider to **On** if you need a link-local address for local communication within the network segment. The gateway generates the link-local address automatically, so that communication in the same network segment is possible without DHCP or static IP address.
Multicast DNS (only in Advanced viewing mode)	Set the slider to **On** if all nodes in the network are to be addressed directly instead of a query to a DNS server. Gateways are then accessible in the network at **<hostname>.local**. The host name can be found in SIINEOS on the **System > Device** page.

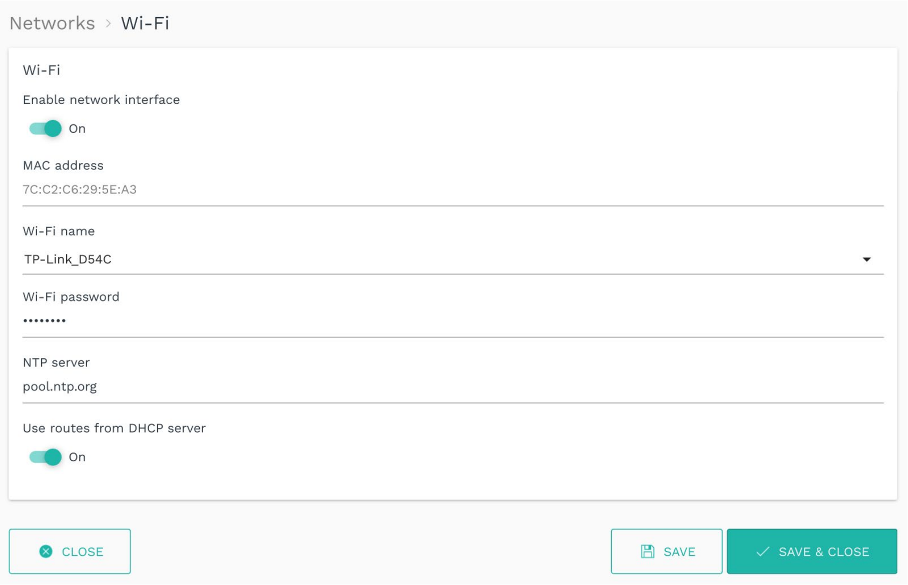
6. Click **Save & close** to save your entries.

   This takes you back to the **Networks** page.

4.7.2 Setting up Wi-Fi

If a WLAN stick is plugged in, you can configure the WLAN connection on this page.

If the network interface is not used, you cannot make any entries.



Networks > Wi-Fi

Wi-Fi

Enable network interface: On

MAC address: 7C:C2:C6:29:5E:A3

Wi-Fi name: TP-Link_D54C

Wi-Fi password: ••••••••

NTP server: pool.ntp.org

Use routes from DHCP server: On

Fig. 15: Networks > Wi-Fi

1. If you want to connect to a wireless network, set the **Enable network interface** slider to **On**.

   The MAC address, which is also printed on the gateway housing, is displayed.

2. Enter the name and password of the wireless network you want to connect to.

3. Optional: Enter the IP address of an NTP server from which the gateway should obtain its system time.

4. Optional: Set the **Use routes from DHCP server** slider to **Off** to access only the local network through this interface and access the Internet through another interface if necessary.

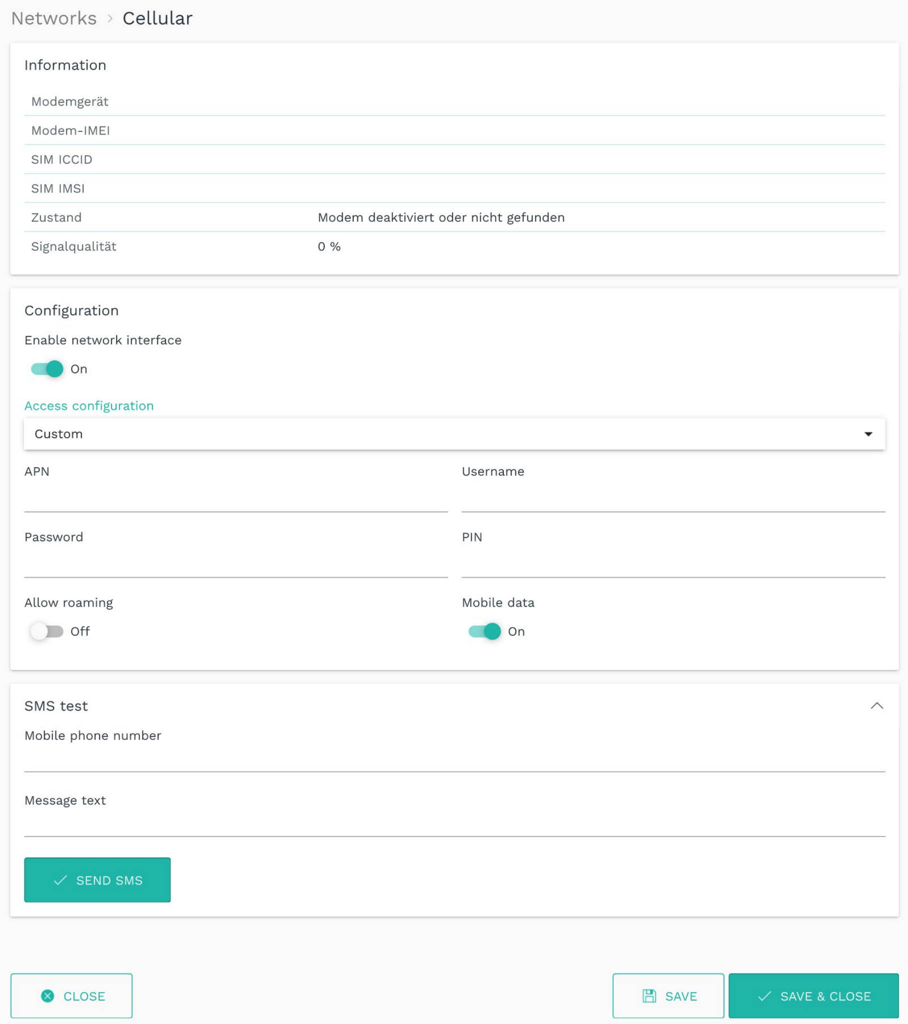
5. Click **Save & close** to save your entries.

   This takes you back to the **Networks** page.

4.7.3 Setting up the mobile connection

The in.hub LTE stick can be connected via an USB interface to establish Internet access in environments without a network. This access can be used, for example, to connect the gateway to a cloud or to access the gateway remotely via the VPN tunnel.

If the network interface is not used, you cannot make any entries.



Networks > Cellular

Information

Modemgerät	
Modem-IMEI	
SIM ICCID	
SIM IMSI	
Zustand	Modem deaktiviert oder nicht gefunden
Signalqualität	0 %

Configuration

Enable network interface: On

Access configuration: Custom

APN

Username

Password

PIN

Allow roaming: Off

Mobile data: On

SMS test

Mobile phone number

Message text

Fig. 16: Networks > Cellular > Access configuration “Custom” (example)

1. If you want to use the in.hub LTE stick as a network interface, set the **Enable network interface** slider to **On**.
2. In the **Access configuration** drop-down list, select a predefined SIM card / cellphone provider(s) or **Custom**.
3. If you have selected **Custom**, make the following entries:

APN	Access point (access point name) Enter the address of the access point you received from your cellphone operator to establish communication between the terminal device and the cellular network.
Username	If the network provider has specified a username in addition to the APN, enter it here.

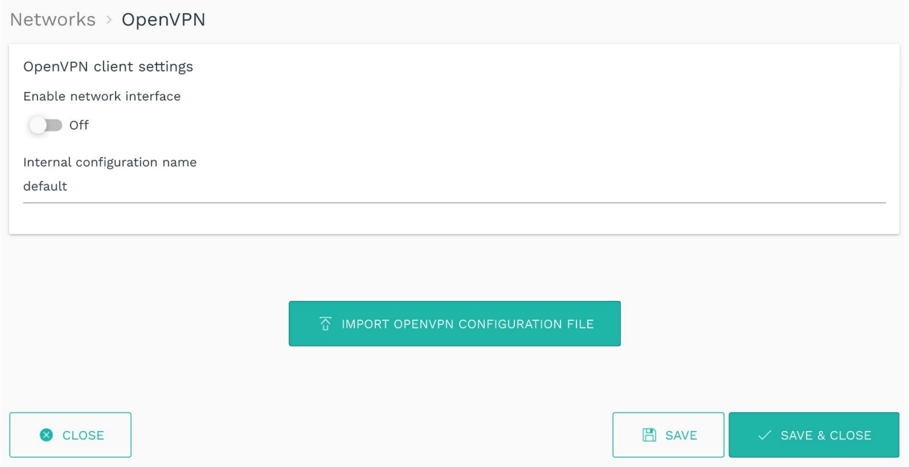
Password	If the network provider has specified a password in addition to the APN, enter it here.
PIN	Enter the PIN of the SIM card. **NOTE**: Make sure you enter the correct PIN for the SIM card inserted, otherwise the card will be blocked after three unsuccessful attempts.
Allow roaming	If you want to allow roaming, set the slider to **On**. **NOTE:** If you have a SIM card with roaming service, you can enable this feature to dial into non-provider networks when needed.
Mobile data	By default, this function is turned on. If you only want to use the in.hub LTE stick to send SMS messages, set the slider to **Off**.

4. To check whether your entries are correct, enter a message text and the cellphone number of the terminal under **SMS test** and click **Send SMS.**
5. If no SMS arrives, check if the signal quality is sufficient.
6. Click **Save & close** to save your entries.

   This takes you back to the **Networks** page.

4.7.4 Setting up OpenVPN

If the gateway is to use a VPN tunnel to your company network, you can import the OpenVPN client configuration here and adjust the name. This requires that an OpenVPN server to be running in the company headquarters.



Networks › OpenVPN

OpenVPN client settings

Enable network interface

Off

Internal configuration name

default

Fig. 17: Networks > OpenVPN

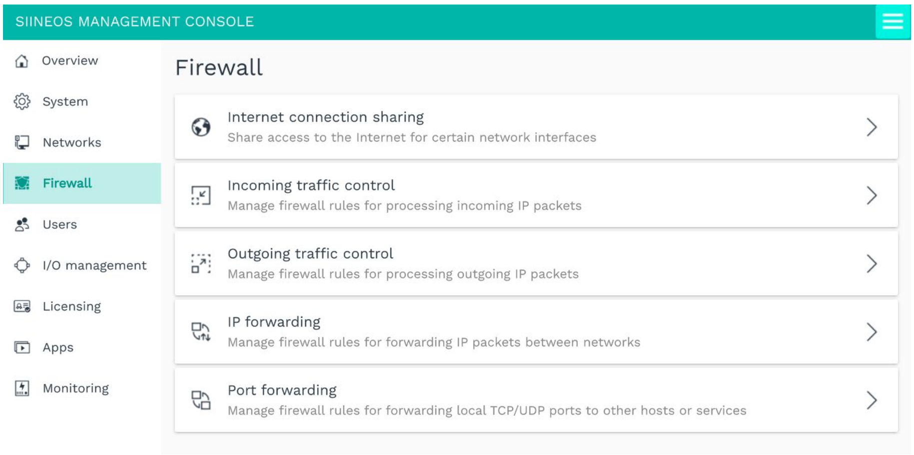
1. If you want to use OpenVPN, set the **Enable network interface** slider to **On**.
2. Click **Import OpenVPN configuration file** to select the configuration file from your local file directory.
3. Enter the file name (without file extension) in the **Internal configuration name** field.
4. Click **Save & close to** save your entries.

   This takes you back to the **Networks** page.

4.8 Configuring the firewall

> **RECOMMENDATION:** When adjusting or configuring the device-internal firewall, always connect your computer via the micro-USB port on the front of the gateway if possible and open the SIINEOS management console via the USB network address http://192.168.123.1.
>
> This will prevent you from losing access to the gateway over the network due to an incompletely or incorrectly configured firewall rule.

On the **Firewall** page, you can configure the gateway's built-in network firewall, defining rules that determine how the gateway communicates on the network and how it handles network traffic received. The following functions are available:



Firewall

Internet connection sharing
Share access to the Internet for certain network interfaces

Incoming traffic control
Manage firewall rules for processing incoming IP packets

Outgoing traffic control
Manage firewall rules for processing outgoing IP packets

IP forwarding
Manage firewall rules for forwarding IP packets between networks

Port forwarding
Manage firewall rules for forwarding local TCP/UDP ports to other hosts or services

Fig. 18: "Firewall" page

In principle, you can use the device-internal firewall as part of your company's own security concept, but you do not have to. The configuration of the firewall is optional. A firewall is particularly useful when devices or the network in which one of the communicating devices is located are accessed from outside.

So, first you specify whether the traffic passing through the gateway should be processed or not.

- If you don't need this feature, just skip the **Firewall** page.
- If you do, then you can follow the blacklisting approach that SIINEOS uses by default, i.e., any traffic that is not explicitly forbidden is allowed.

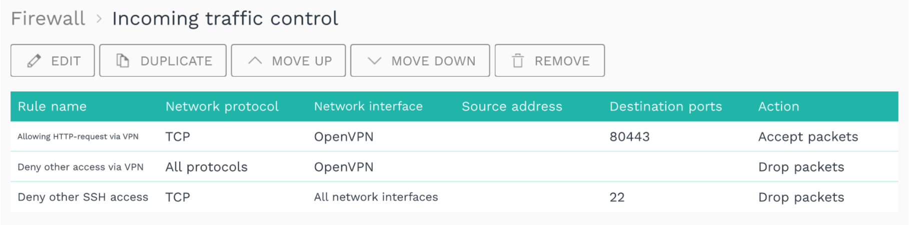
  Or you can take the whitelisting approach, which means that any traffic that is not explicitly allowed is forbidden.

ATTENTION

If you have made changes to the firewall configuration, restart the device so that all settings for Docker-based apps such as Grafana or NodeRED are applied correctly. Otherwise, access to these apps and communication between these apps and your network or the Internet may be restricted.

Notes on incoming and outgoing network traffic

All rules you create are processed for each incoming data package in sequence—from top to bottom in the list. At the point where all the criteria of a rule apply to a data packet, rule processing is concluded with the selected action. No further rules are processed.



Rule name	Network protocol	Network interface	Source address	Destination ports	Action
Allowing HTTP-request via VPN	TCP	OpenVPN		80443	Accept packets
Deny other access via VPN	All protocols	OpenVPN			Drop packets
Deny other SSH access	TCP	All network interfaces		22	Drop packets

Fig. 19: Example of a rules list for incoming network traffic

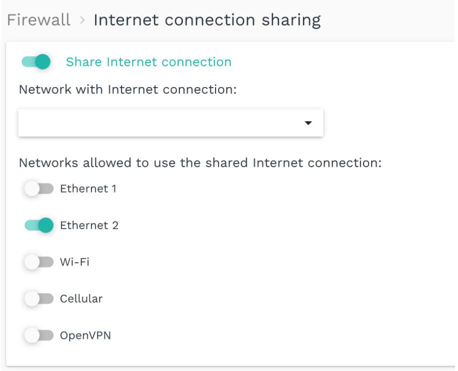
You can change the order of the rules using the **Move up** or **Move down** buttons.

RECOMMENDATION: Create all positive rules first. It must be defined very specifically which access should be allowed by whom. It is useful to have a rule at the end of the list where no conditions are set. You can then only select in the **Actions** drop-down whether the gateway ignores the request from the network (**Drop packet**) or whether the gateway actively rejects the request (**Reject packet**).

4.8.1 Sharing Internet connections

In this window, you define the networks that the devices (e.g. machines) connected in this network are allowed to use to access the Internet via the gateway.

1. On the **Firewall** page, select **Share Internet connection**.



● Share Internet connection

Network with Internet connection:

Networks allowed to use the shared Internet connection:

○ Ethernet 1

● Ethernet 2

○ Wi-Fi

○ Cellular

○ OpenVPN

Fig. 20: Firewall > Internet connection sharing (example)

2. Activate the **Share Internet connection** slider.
3. In the **Network with Internet connection** drop-down list, select the network that the gateway uses to access the Internet.
4. Activate the slider of the network that is allowed to use the shared Internet connection.
5. Click **Save & close**.

   This takes you back to the **Firewall** page.

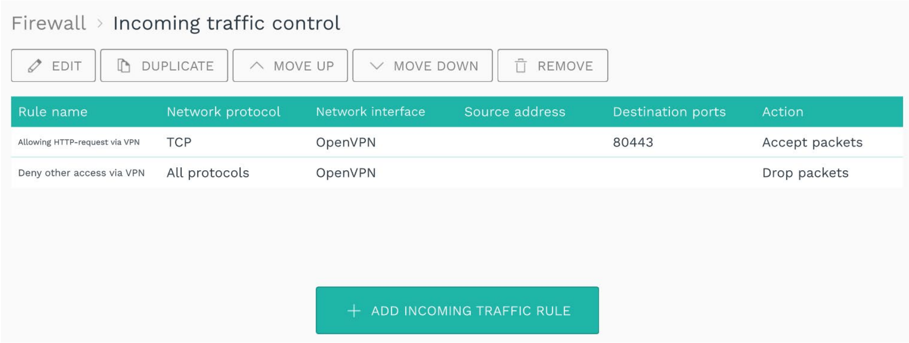
4.8.2 Controlling incoming network traffic

In this window, you define firewall rules that determine how incoming IP packets are handled by SIINEOS.

By default, all incoming packets are allowed, so the respective network services of the gateway (e.g., SSH, MQTT, SMAC) are accessible from all networks.

So, if you want to restrict access from certain source addresses, you can define rules here.

1. On the **Firewall** page, select **Incoming traffic control**.


Firewall › Incoming traffic control
EDIT
DUPLICATE
MOVE UP
MOVE DOWN
REMOVE
ADD INCOMING TRAFFIC RULE

Rule name	Network protocol	Network interface	Source address	Destination ports	Action
Allowing HTTP-request via VPN	TCP	OpenVPN		80443	Accept packets
Deny other access via VPN	All protocols	OpenVPN			Drop packets

Fig. 21: Firewall > Incoming traffic control (example)

2. To add a new rule, click **Add incoming traffic rule**.

   The setup wizard opens to guide you through creating the rule. In the following, confirm each entry either with **Next** or by pressing **Enter**.

3. Under **Rule name,** enter a name.

4. Select the **Network protocol** for network packets for which this rule applies.

   Select **All protocols** if you want the rule to apply to all network protocols.

5. Select the **Input interface** through which the data packet must arrive for the rule to apply.

   Select **All network interfaces** if the packet can arrive via any interface for the rule to apply.

6. Enter a **Source address** if you want the rule to apply only to packets sent from specific hosts or networks.

   Enter the network address of an entire network (e.g. 192.168.5.0/24) or of a specific machine (e.g. 192.168.5.140).

   If you leave the field empty, the rule will be applied to any source address.

7. Under **Destination ports**, you can restrict access to specific TCP/UDP ports of the gateway.

   Enter the port numbers, separated by spaces, to which access is to be controlled by this rule.

   If you leave the field empty, access to all TCP/UDP ports will be allowed or denied (depending on the action selected in the next step).

8. Under **Action,** select from the drop-down list what to do with the network packets that match all the criteria of the rule.
   - **No action**: The rule is switched to inactive, i.e., the process advances to the next rule.
   - **Accept packets**: The request is allowed, and the packets are allowed to arrive.
   - **Drop packets**: The request is not allowed, and the packet is discarded, i.e., effectively ignored. No response is returned.
   - **Reject packets**: The request is actively rejected and answered. A reject packet is returned to the sender so that the connection setup fails.
9. When you have made all the entries, click **Finish**.

   This takes you back to the list of all rules.
10. If you want to edit a rule, select the rule and click **Edit** or double-click.

    A page opens, where you can see and edit all the settings for the rule in one view.

    To save your changes, click **Save & close**.
11. If you want to duplicate a rule, select the rule, and click **Duplicate**.

    This takes you back to the setup wizard, where you can customize the rule.
12. If you want to remove a rule, select the rule, and click **Remove**.
13. If you want to change the order in which the rules are run, select a rule and click **Move up** or **Move down.**

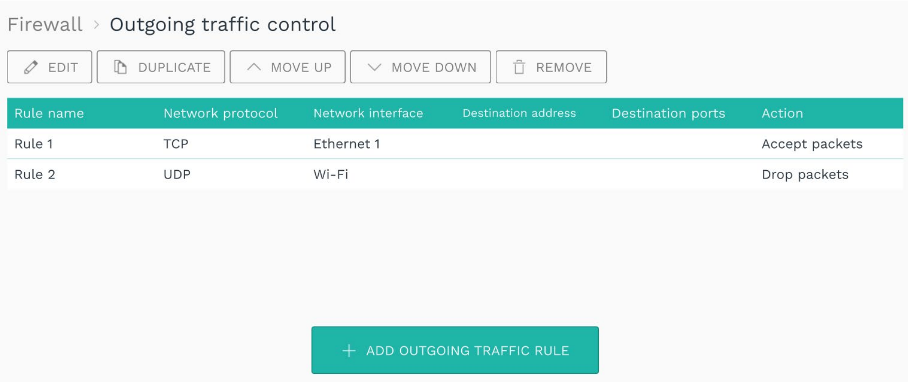
4.8.3 Controlling outgoing network traffic

In this window, you can define firewall rules that determine how outgoing IP packets are handled by SIINEOS.

By default, all outgoing packets are allowed, so the gateway has unrestricted access to all reachable networks, as well as the Internet, if applicable.

If you want to prevent access to certain destination addresses, you can define rules here.

1. On the **Firewall** page, select **Outgoing traffic control**.


Firewall > Outgoing traffic control
EDIT
DUPLICATE
MOVE UP
MOVE DOWN
REMOVE
ADD OUTGOING TRAFFIC RULE

Rule name	Network protocol	Network interface	Destination address	Destination ports	Action
Rule 1	TCP	Ethernet 1			Accept packets
Rule 2	UDP	Wi-Fi			Drop packets

Fig. 22: Firewall > Outgoing traffic control (example)

2. To add a new rule, click **Add outgoing traffic rule**.

   The setup wizard opens to guide you through creating the rule. In the following, confirm each entry either with **Next** or by pressing **Enter**.

3. Under **Rule name,** enter a name.

4. Select the **Network protocol** for the network packets to which this rule should apply.

   Select **All protocols** if you want the rule to apply to all network protocols.

5. Select the **Output interface** through which the packet will be sent (based on the network configuration/routing table).

   Select **All network interfaces** if the packet can originate from any interface for the rule to apply.

6. Enter a **Destination address** if you want the rule to apply only to packets sent to specific recipients (hosts/networks).

   Enter the network address of an entire network (e.g. 192.168.5.0/24) or of a specific machine (e.g. 192.168.5.140).

   If you leave the field empty, the rule will be applied to all recipients (hosts/networks).

7. Under **Destination ports**, you restrict access from the gateway to specific TCP/UDP ports of the destination computer/network.

   Now enter the port numbers, separated by spaces, to which access is to be controlled by this rule.

   If you leave the field empty, access to all TCP/UDP ports will be allowed or denied (depending on the action selected).

8. Under **Action,** select from the drop-down list what to do with the network packets to which this rule applies:
   - **No action**: The rule is switched to inactive, i.e. the process advances to the next rule.
   - **Accept packets**: The packet may be sent over the corresponding network interface.
   - **Drop packages**: The packet is not sent but discarded. The sending application does not receive any information that the packet was not sent.
   - **Reject packets**: The packet will not be sent, and the sending application will be informed that the network packet could not be / has not been sent.
9. When you have made all the entries, click **Finish**.

   This takes you back to the list with all the rules.
10. If you want to edit a rule, select the rule, and click **Edit** or double-click.

    A page opens, where you can see and edit all the settings for the rule in one view.

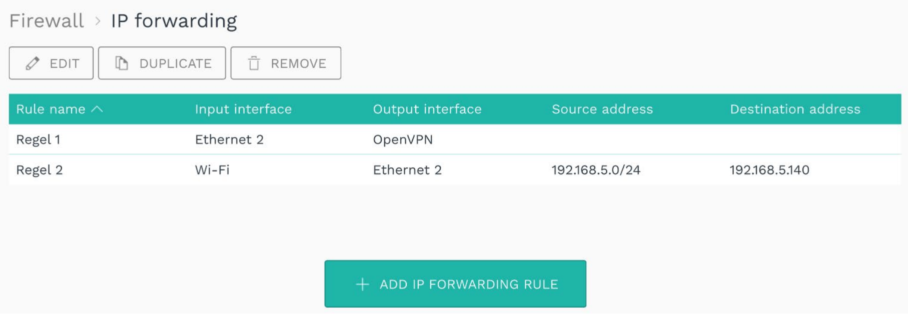
    To save your changes, click **Save & close**.
11. If you want to duplicate a rule, select the rule and click **Duplicate**.

    This takes you back to the setup wizard, where you can customize the rule.
12. If you want to remove a rule, select the rule and click **Remove**.
13. If you want to change the order in which the rules are run, select the rule and click **Move up** or **Move down.**

4.8.4 Setting and editing rules for IP forwarding

In this window, you can define rules for direct forwarding of data packets, for example, if you want to access a machine connected to the gateway via VPN.

1. On the **Firewall** page, select **IP forwarding.**



Rule name ^	Input interface	Output interface	Source address	Destination address
Regel 1	Ethernet 2	OpenVPN		
Regel 2	Wi-Fi	Ethernet 2	192.168.5.0/24	192.168.5.140

Fig. 23: Firewall > IP forwarding (example)

2. To add a new rule, click **Add IP forwarding rule**.

   The setup wizard opens to guide you through creating the rule. In the following, confirm each entry either with **Next** or by pressing **Enter**.

3. Under **Rule name,** enter a name.

4. From the drop-down list, select the **Input interface** from which to forward traffic.

5. From the drop-down list, select the **Output interface** (destination) to which the traffic is to be forwarded.

6. If traffic should only take place with a certain host or in a limited network, you can now enter the **Source address** and then the **Destination address.**

   Enter the network address of an entire network (e.g. 192.168.5.0/24) or of a specific machine (e.g. 192.168.5.140).

   If you do not enter anything, the traffic will not be restricted.

7. When you have made all the entries, click **Finish**.

   This takes you back to the list with all forwarding rules.

8. If you want to edit a rule, select the rule and click **Edit** or double-click.

   A page opens, where you can see all the settings for the rule and edit them in one view.

   To save your changes, click **Save & close**.

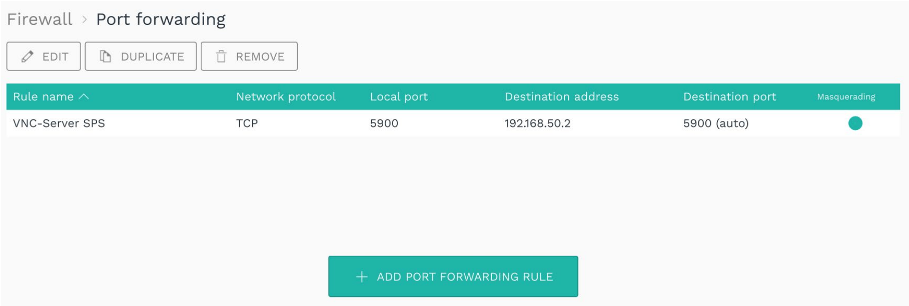
9. If you want to duplicate a rule, select the rule and click **Duplicate**.

   This takes you back to the setup wizard where you can customize the rule.

10. If you want to remove a rule, select the rule and click **Remove**.

4.8.5 Configuring port forwarding

1. On the **Firewall** page, select **Port forwarding.**



Rule name	Network protocol	Local port	Destination address	Destination port	Masquerading
VNC-Server SPS	TCP	5900	192.168.50.2	5900 (auto)	●

Fig. 24: Firewall > Port forwarding (example)

2. To add a new rule, click **Add port forwarding rule**.

   The setup wizard opens to guide you through creating the rule. In the following, confirm each entry either with **Next** or by pressing **Enter**.

3. Under **Rule name,** enter a name.
4. Select the **Network protocol** for network packets for which the port forwarding rule should apply.
5. Under **Local port,** enter the number of the local port to be forwarded.
6. Under **Destination address,** enter the IP address of the host to which the traffic should be forwarded.
7. If you want to forward the traffic to another port instead of a local port, specify the required port number under **Destination port.**

   If you do not enter anything, the local port is used.

8. Under **Masquerading**, the slider is automatically set to **On**. This means, that for all forwarded packets the source address is replaced by the IP address of the gateway.

   This is always necessary if no direct IP routing between sender and destination host is possible. This address translation ensures that replies from the destination host are correctly returned to the original sender. In most cases where port forwarding is desired, masquerading is also necessary for communication to work as desired.

   If you do not want this, set the slider to **Off**.

9. When you have made all the entries, click **Finish**.

   This takes you back to the list with all port forwarding rules.

10. If you want to edit a rule, select the rule and click **Edit** or double-click.

    A page opens, where you can see all the settings for the rule and edit them in one view.

    To save your changes, click **Save & close**.

11. If you want to duplicate a rule, select the rule and click **Duplicate**.

    This takes you back to the setup wizard, where you can customize the rule.

12. If you want to remove a rule, select the rule and click **Remove**.

4.9 User management

The following three user roles are provided in the SIINEOS user administration:

- **System administrator**

  Can log into SIINEOS and configure the system, activate apps, and open them in SIINEOS so that app users can access them.

  For the first login to SIINEOS, a user account (**hubadmin/hubadmin**) with the role **System administrator** is created. You should change the preset password after logging in.

- **App administrator**

  Can log into the administration interface of an app (e.g. MADOW) and configure it.

  For the initial login to the **InGraf** app, a user account (**ingrafadmin**/**ingrafadmin**) with the **App administrator** role is created.

  For the initial login to the **MADOW** app, a user account (**madowadmin**/**madowadmin**) with the **App administrator** role is also created.

  You should change the preset passwords after logging in.

- **App user**

  Can log into protected areas of an app where sensitive information is displayed, for example.

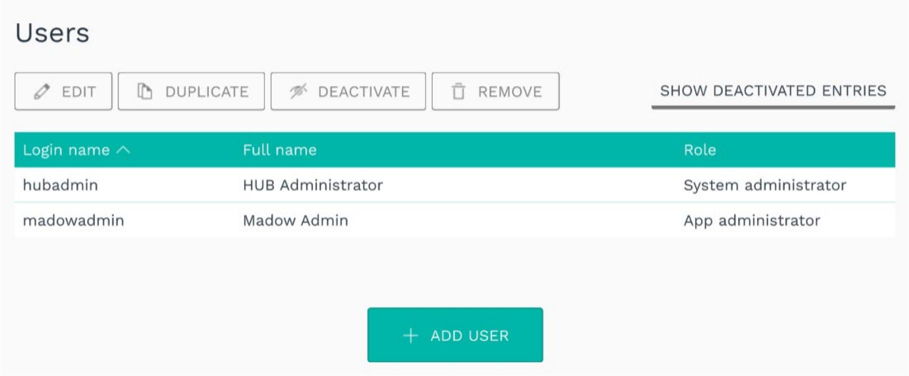
All other user accounts are created and managed by you as the system administrator. For apps, the two user roles **App administrator** and **App user** are available.

Some areas in the apps require no authentication. For example, a machine operator can connect directly to MADOW via the corresponding web address and view downtimes without having to log in.

4.9.1 Managing user accounts

On the **Users** page you can add user profiles, assign one of the predefined roles to users and edit, deactivate, or remove profiles.

> **NOTE:** You cannot deactivate or remove the preconfigured **System administrator** role.



Login name ^	Full name	Role
hubadmin	HUB Administrator	System administrator
madowadmin	Madow Admin	App administrator

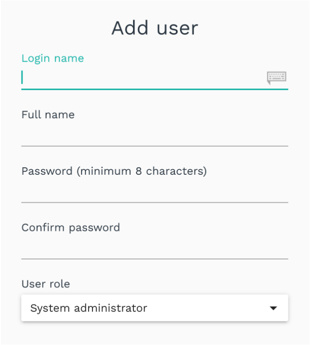
Fig. 25: “Users” page (example)

1. On the **Users** page, click **Add User** to create a new user.

   -or-

   Select an existing user and click **Duplicate**.

   The **Add user** dialog box opens.

   Add user

   Login name

   Full name

   Password (minimum 8 characters)

   Confirm password

   User role: System administrator

   Fig. 26: Users > Add user (example)

2. Enter the **Login name**, **Full name,** and a **Password**.

   The password must have of at least 8 characters.

3. In the drop-down list, assign a **User role** to the user.
4. When you have completed the input, click **Save & close**.

   The user is created and appears in the list.

5. To edit a user, select the corresponding line in the list and click **Edit**.

   The same window opens as when creating a user. Here, you can change all the details and/or assign a different user role.

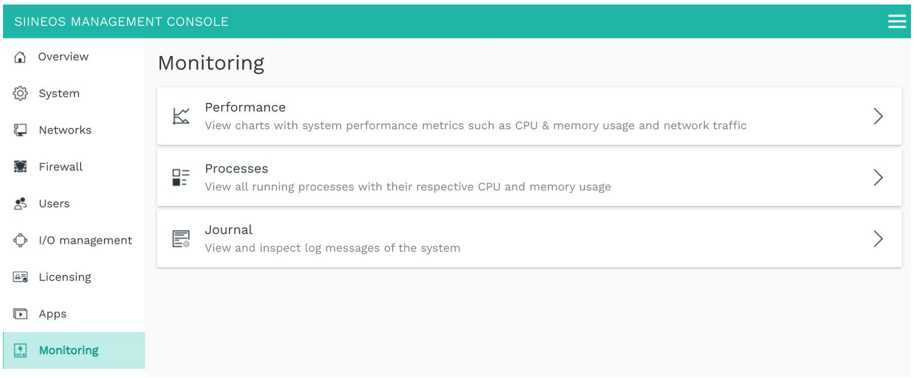
6. If you want to remove a user, select the user and click **Remove**.

7. To deactivate a user, e.g., because the user is absent for a prolonged period, select the corresponding line in the list and click **Deactivate**.
8. To restore a deactivated user, click the **Show deactivated entries** filter, select a user and click **Activate**.

> **TIP:** If there are many entries, you can search within the list. To do this, click on the icon with the magnifying glass at the top right and enter the username you are looking for.
>
> 🔍

4.10 Monitoring system

On the **Monitoring** page, you can monitor the utilization of the processor and the network interfaces, as well as the data traffic of your gateway live. The page is primarily used for diagnostic purposes.



Monitoring

Performance
View charts with system performance metrics such as CPU & memory usage and network traffic

Processes
View all running processes with their respective CPU and memory usage

Journal
View and inspect log messages of the system

Abb. 27: “Monitoring“ page

You can access the following information via this page:

- **Performance**: Check whether, for example, data is being sent or received via the correct network interface or how the CPU and RAM are being used

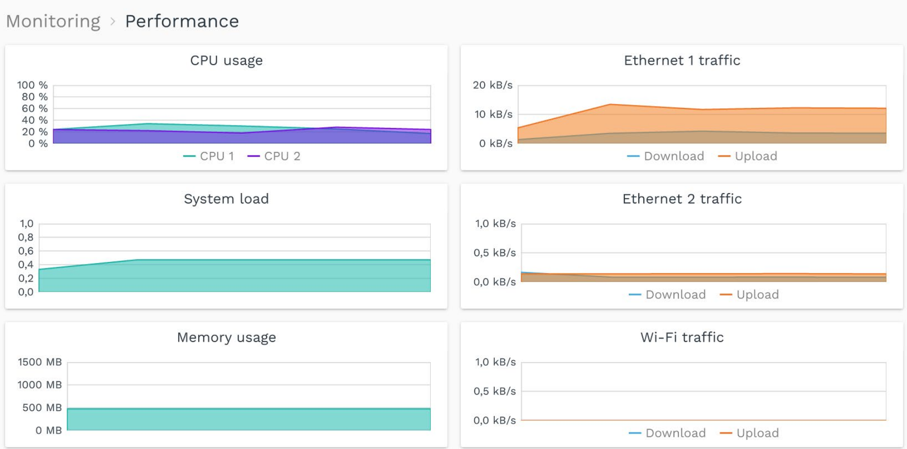
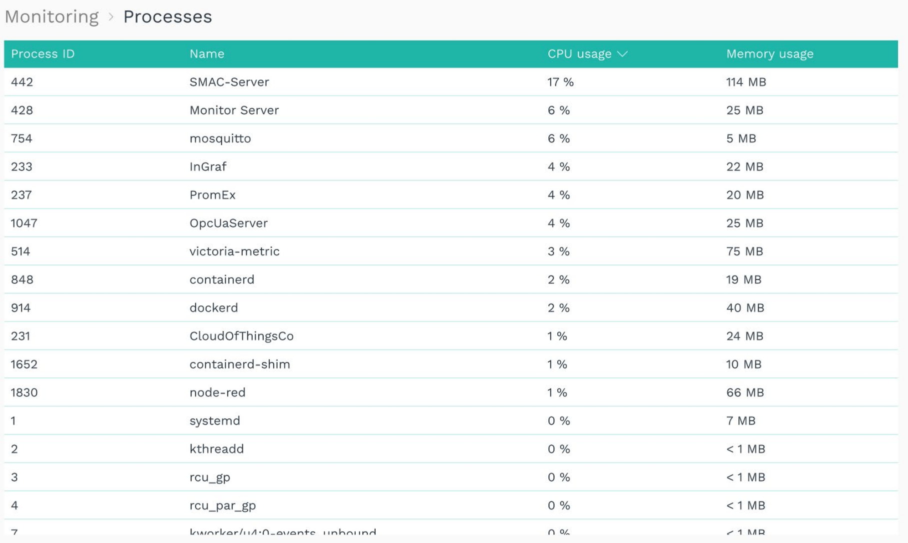


Fig. 28: “Monitoring” page > Performance (example)

- **Processes**: Check whether the system is fully started, which apps are active and what CPU load they are working with.

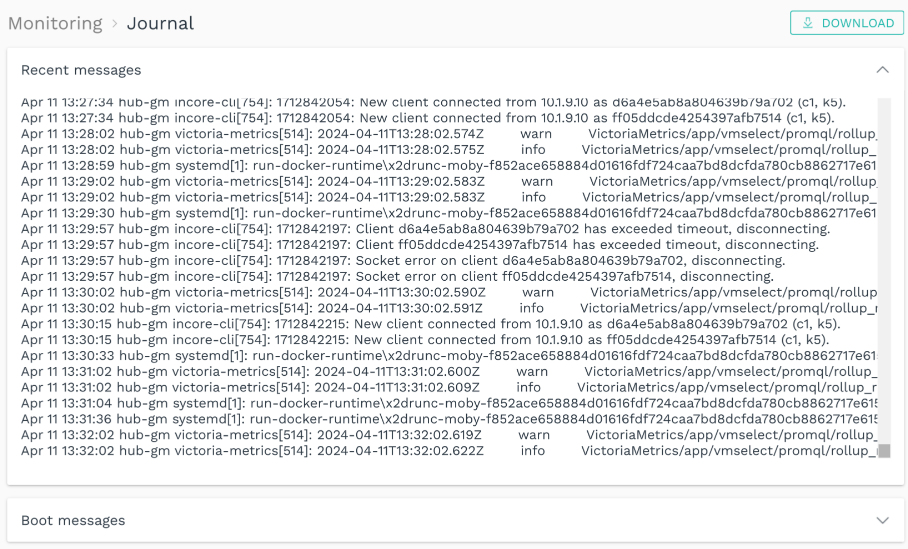


Monitoring › Processes

Process ID	Name	CPU usage	Memory usage
442	SMAC-Server	17 %	114 MB
428	Monitor Server	6 %	25 MB
754	mosquitto	6 %	5 MB
233	InGraf	4 %	22 MB
237	PromEx	4 %	20 MB
1047	OpcUaServer	4 %	25 MB
514	victoria-metric	3 %	75 MB
848	containerd	2 %	19 MB
914	dockerd	2 %	40 MB
231	CloudOfThingsCo	1 %	24 MB
1652	containerd-shim	1 %	10 MB
1830	node-red	1 %	66 MB
1	systemd	0 %	7 MB
2	kthreadd	0 %	< 1 MB
3	rcu_gp	0 %	< 1 MB
4	rcu_par_gp	0 %	< 1 MB
7	kworker/u4:0-events_unbound	0 %	< 1 MB

Fig. 29: “Monitoring” page > Processes (example)

- **Journal**: Read the SIINEOS log files. A distinction is made between **Boot messages** and **Recent messages**. Click on the small arrow on the right to open or close the list of log files.



Monitoring › Journal

Recent messages

```
Apr 11 13:27:34 hub-gm incore-cli[754]: 1712842054: New client connected from 10.1.9.10 as d6a4e5ab8a804639b79a702 (c1, k5).
Apr 11 13:27:34 hub-gm incore-cli[754]: 1712842054: New client connected from 10.1.9.10 as ff05ddcde4254397afb7514 (c1, k5).
Apr 11 13:28:02 hub-gm victoria-metrics[514]: 2024-04-11T13:28:02.574Z       warn       VictoriaMetrics/app/vmselect/promql/rollup_
Apr 11 13:28:02 hub-gm victoria-metrics[514]: 2024-04-11T13:28:02.575Z       info       VictoriaMetrics/app/vmselect/promql/rollup_
Apr 11 13:28:59 hub-gm systemd[1]: run-docker-runtime\x2drunc-moby-f852ace658884d01616fdf724caa7bd8dcfda780cb8862717e61
Apr 11 13:29:02 hub-gm victoria-metrics[514]: 2024-04-11T13:29:02.583Z       warn       VictoriaMetrics/app/vmselect/promql/rollup_
Apr 11 13:29:02 hub-gm victoria-metrics[514]: 2024-04-11T13:29:02.583Z       info       VictoriaMetrics/app/vmselect/promql/rollup_
Apr 11 13:29:30 hub-gm systemd[1]: run-docker-runtime\x2drunc-moby-f852ace658884d01616fdf724caa7bd8dcfda780cb8862717e61
Apr 11 13:29:57 hub-gm incore-cli[754]: 1712842197: Client d6a4e5ab8a804639b79a702 has exceeded timeout, disconnecting.
Apr 11 13:29:57 hub-gm incore-cli[754]: 1712842197: Client ff05ddcde4254397afb7514 has exceeded timeout, disconnecting.
Apr 11 13:29:57 hub-gm incore-cli[754]: 1712842197: Socket error on client d6a4e5ab8a804639b79a702, disconnecting.
Apr 11 13:29:57 hub-gm incore-cli[754]: 1712842197: Socket error on client ff05ddcde4254397afb7514, disconnecting.
Apr 11 13:30:02 hub-gm victoria-metrics[514]: 2024-04-11T13:30:02.590Z       warn       VictoriaMetrics/app/vmselect/promql/rollup
Apr 11 13:30:02 hub-gm victoria-metrics[514]: 2024-04-11T13:30:02.591Z       info       VictoriaMetrics/app/vmselect/promql/rollup_r
Apr 11 13:30:15 hub-gm incore-cli[754]: 1712842215: New client connected from 10.1.9.10 as d6a4e5ab8a804639b79a702 (c1, k5).
Apr 11 13:30:15 hub-gm incore-cli[754]: 1712842215: New client connected from 10.1.9.10 as ff05ddcde4254397afb7514 (c1, k5).
Apr 11 13:30:33 hub-gm systemd[1]: run-docker-runtime\x2drunc-moby-f852ace658884d01616fdf724caa7bd8dcfda780cb8862717e61
Apr 11 13:31:02 hub-gm victoria-metrics[514]: 2024-04-11T13:31:02.600Z       warn       VictoriaMetrics/app/vmselect/promql/rollup_
Apr 11 13:31:02 hub-gm victoria-metrics[514]: 2024-04-11T13:31:02.609Z       info       VictoriaMetrics/app/vmselect/promql/rollup_r
Apr 11 13:31:04 hub-gm systemd[1]: run-docker-runtime\x2drunc-moby-f852ace658884d01616fdf724caa7bd8dcfda780cb8862717e615
Apr 11 13:31:36 hub-gm systemd[1]: run-docker-runtime\x2drunc-moby-f852ace658884d01616fdf724caa7bd8dcfda780cb8862717e615
Apr 11 13:32:02 hub-gm victoria-metrics[514]: 2024-04-11T13:32:02.619Z       warn       VictoriaMetrics/app/vmselect/promql/rollup_
Apr 11 13:32:02 hub-gm victoria-metrics[514]: 2024-04-11T13:32:02.622Z       info       VictoriaMetrics/app/vmselect/promql/rollup_r
```

Boot messages

Fig. 30: “Monitoring” page > Journal (example)

Click **Download** to download debug and trace messages as a TXT file. You can download the **Recent messages** and **Boot messages** separately. You can send these to us for diagnostic purposes by arrangement.

4.11 Opening and managing apps

On the **Apps** page you will find various software tools that you can access directly. The apps shown in the following image are pre-installed.

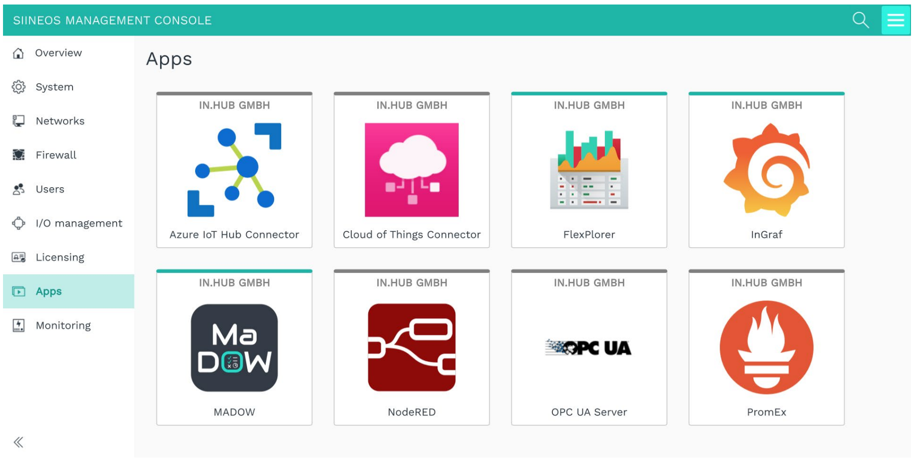


Fig. 31: "Apps" page

1. Open the required app by clicking on the tile.

   An overview opens, where you can find information about the application, as well as a description of the app and how it works.

2. Two additional buttons are displayed in the **Advanced** viewing mode:

   ○ **Log debug messages**

   Messages from the SIINEOS management service are logged in the system journal, which help in.hub with troubleshooting.

   ○ **Log trace messages**

   Activate this function if detailed calls of system functions and the parameters used by the respective app are to be logged.

   NOTE: Do not activate this function in productive operation, as otherwise performance losses are to be expected.

   On the **Monitoring** page under **Journal**, you can view the debug and trace messages and download them using a button.

   Please note that the messages are only saved temporarily and are lost after a restart. You should therefore save them in good time

3. To start the app, click **Enable app**.

4. To view or change the settings for the app, click **Manage app**.

   You can find out how to manage the connection between the apps and SIINEOS in chapter Managing the apps, page 88.

5. Once the app is activated, click **Open app**.

   The app will now open in a new window or tab, depending on your browser settings.

   If it is an external app, e.g., Grafana, you will now be forwarded to the login page. Make sure that you have a user account.

TIP: If there are many entries, you can also search specifically for an app. To do this, click on the icon with the magnifying glass at the top right and enter the name of the app or the manufacturer.

🔍

4.12 Managing SIINEOS licenses

With every new in.hub device you purchase, you automatically receive a SIINEOS license for 3 years. During the license period, you can update SIINEOS as often as you like and install the latest version on the device.

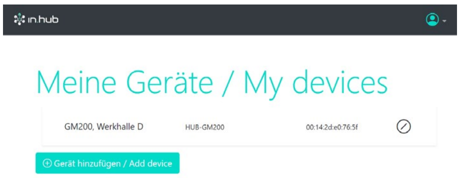
As soon as the license period has expired, you can either continue working with the currently installed SIINEOS version or you can purchase another license from in.hub to benefit from the further development and product improvement of SIINEOS.

4.12.1 Requesting a voucher and activating the software license

1. Contact in.hub either by e-mail or telephone and let us know for which term you would like to purchase the license.

   You will then receive a voucher with which you can activate a software license.

2. Navigate to the website https://apps.inhub.de/ and register or log in if you are already registered.



in.hub

Meine Geräte / My devices

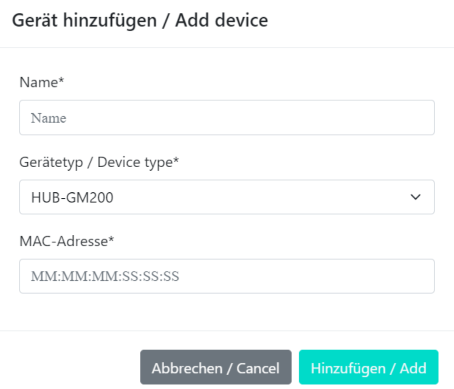
GM200, Werkhalle D HUB-GM200 00:14:2d:e0:76:5f

Fig. 32: My devices (example)

3. If you want to activate a license for a new device, click **Add device**.

   -or-

   If you want to extend the license for a device that has already been created, click on the relevant device under **My devices**.



Gerät hinzufügen / Add device

Name*

Name

Gerätetyp / Device type*

HUB-GM200

MAC-Adresse*

MM:MM:MM:SS:SS:SS

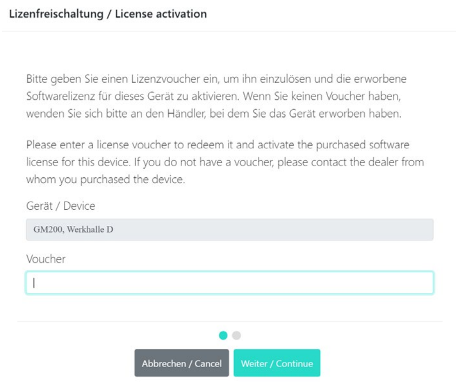
Fig. 33: Add device

4. Enter the **Name** of the device, select the **Device type** and enter the **MAC-Address** of the device.

   These can be found under **SIINEOS > Networks > Ethernet 1**.

5. Click **Add**.

   The **License activation** window opens:



Lizenzfreischaltung / License activation

Bitte geben Sie einen Lizenzvoucher ein, um ihn einzulösen und die erworbene Softwarelizenz für dieses Gerät zu aktivieren. Wenn Sie keinen Voucher haben, wenden Sie sich bitte an den Händler, bei dem Sie das Gerät erworben haben.

Please enter a license voucher to redeem it and activate the purchased software license for this device. If you do not have a voucher, please contact the dealer from whom you purchased the device.

Gerät / Device: GM200, Werkhalle D

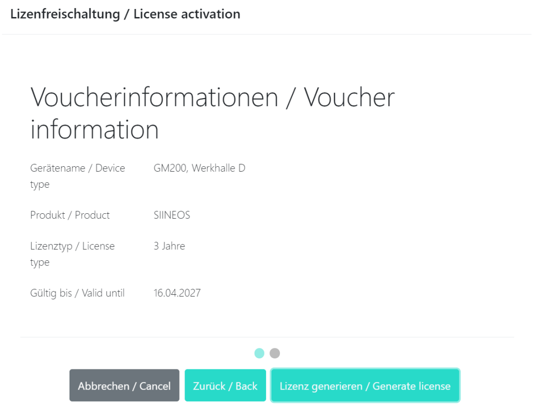
Voucher: |

Fig. 34: License activation

6. Copy the name of the voucher you received from in.hub into the **Voucher** field.

7. Click **Continue**.

   All voucher information is displayed:



Lizenzfreischaltung / License activation

Voucherinformationen / Voucher information

Gerätename / Device type	GM200, Werkhalle D
Produkt / Product	SIINEOS
Lizenztyp / License type	3 Jahre
Gültig bis / Valid until	16.04.2027

Fig. 35: Voucher information

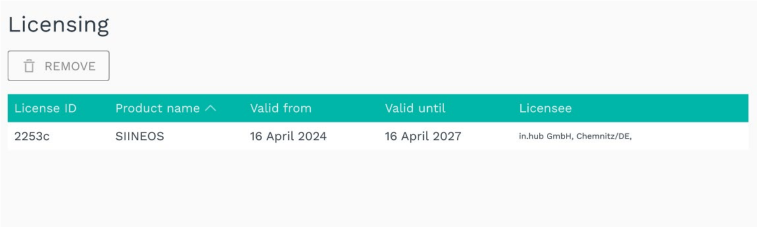
8. Check the details, especially the validity and the license type (i.e. whether the requested license term matches the term specified here).

9. If the information is correct, click **Generate license**.

10. The license file is downloaded automatically.

4.12.2 Adding licenses in SIINEOS

In SIINEOS, on the **Licensing** page, you will find all in.hub software licenses that you have purchased.



Licensing

License ID	Product name ^	Valid from	Valid until	Licensee
2253c	SIINEOS	16 April 2024	16 April 2027	in.hub GmbH, Chemnitz/DE,

Fig. 36: “Licensing“ page (example)

1. Click **Add license**.
2. Select the license file that you received from in.hub from your file directory and click **OK**.

   The license is added to the list.
3. To remove a license, e.g. because it has become invalid, select the license ID and click **Remove**.

   The license file itself is not deleted, but only removed from the list.
4. Only now can you install a new SIINEOS software bundle on the **System > Updates** page.

5 I/O management

You can connect a variety of external peripheral devices to an in.hub gateway, such as sensors, Modbus Clients, or even other in.hub gateways and add-on modules.

The interfaces and signals of the peripheral devices are configured and set up by you, so that measured values are output according to your requirements.

On the **I/O management** page, you can perform the following tasks:

- Create I/O units, manage them, and configure their interfaces.

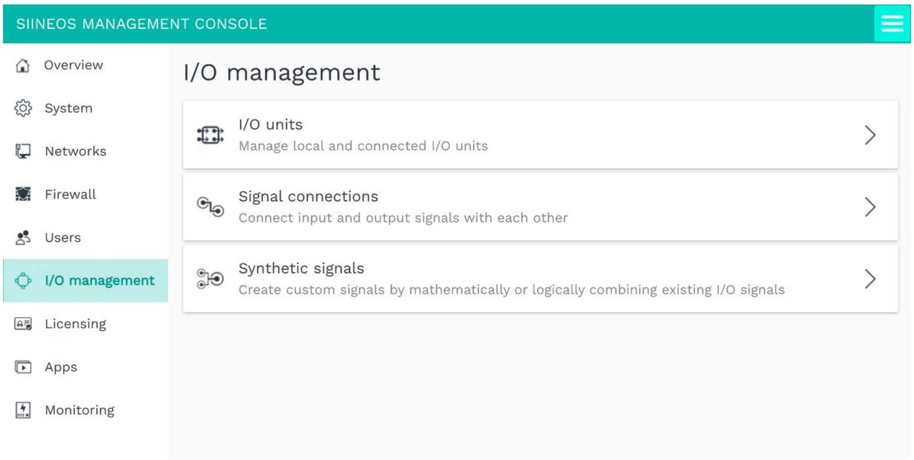
  Creating I/O units, page 48

- Link input and output signals to trigger actions when signal values or measured values fall outside a defined range.

  Configuring signal connections, page 83

- Connect signals from different I/O units to create new, synthetic signals.

  Creating synthetic signals, page 84



SIINEOS MANAGEMENT CONSOLE

I/O management

I/O units
Manage local and connected I/O units

Signal connections
Connect input and output signals with each other

Synthetic signals
Create custom signals by mathematically or logically combining existing I/O signals

Fig. 37: "I/O management" page

> **TIP:** Regularly check the in.hub community at https://community.inhub.de/. There you will find workflows, answers to tricky use cases or helpful tips about SIINEOS in practice. Or ask questions yourself if you need help setting up.

5.1 Working with I/O management

When you use I/O management to create devices or clients or to configure signals and/or signal connections, there are several functions that can support you in your daily work. These include, for example, sorting and filtering of long lists or saving and reusing settings that you have made for a specific I/O unit. The following section will introduce you to these tools.

5.1.1 Filtering I/O units

If there are a large number of devices on the **I/O units** page, it may be helpful to filter them. You have the following filters available:

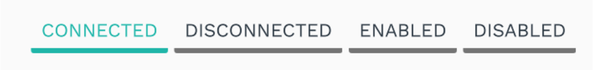


Fig. 38: Filter criteria (the "Connected" filter is currently applied)

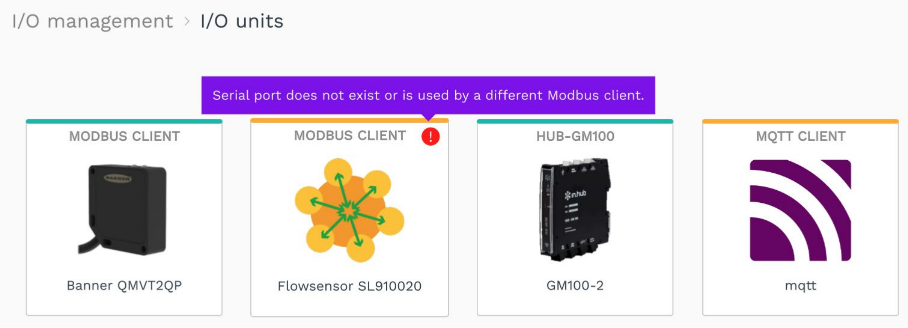
The following rules apply to the filtering of entries:

- An I/O device can either be connected **or** disconnected, i.e., the device is physically connected, or the underlying network connection is established (e.g., to the MQTT broker or to the OPC UA server).
- An I/O unit can either be enabled **or** disabled. This is done in the general settings of each unit.
- For example, an I/O unit may be disconnected but still enabled, or connected but still disabled, etc.

  Exception: For I/O units based on network connections, "connected" and "disabled" are mutually exclusive. Here, the "connected" state is the only way to determine whether the connection parameters are correct, and a connection is possible.

Reading information

- Move the mouse over a tile. Further information about the created I/O unit is displayed.
- In case of error messages, a character is displayed in the upper right corner. In the tooltip you will find more information about this error message.



Serial port does not exist or is used by a different Modbus client.

Abb. 39: Error message at I/O unit "Modbus Client" (example)

Setting filters

1. On the **I/O management** page, click a filter in the upper right corner to apply it.

   The filter changes its color to turquoise.

2. Click the filter again to deselect it.

   The filter changes its color to gray.

5.1.2 Using the menu „Actions“

If you edit entries in the I/O management, you can use the **Actions** menu in the **Add I/O unit** and **Synthetic signals** windows. This allows you to save the entries with the settings you have made in order to use them again elsewhere, or you can load entries that have already been saved onto the current device.

1. Open a I/O unit and click the **Actions** button.

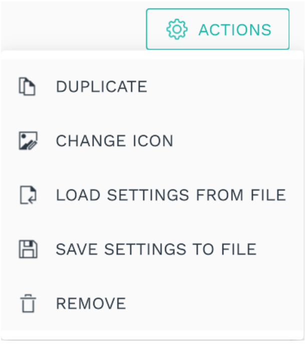


Fig. 40: “Actions” menu

-or-

Open the list with the synthetic signals and click the **Actions** button.

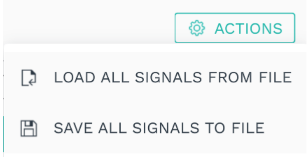


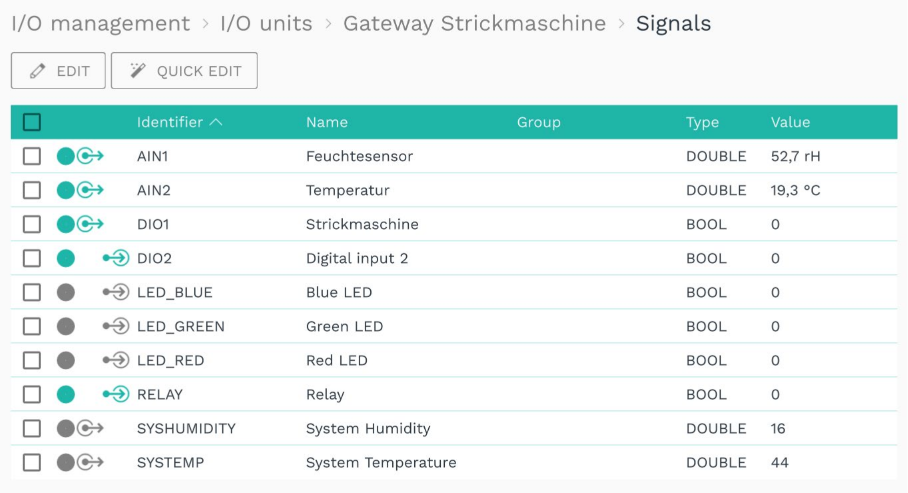
Abb. 41: Synthetic signales > “Actions“ menu

2. Now select the required action for the I/O unit or the synthetic signal:

Duplicate	A tile is created on the **I/O unit** page and identified by the suffix **(copy).** You can now edit this I/O unit as you wish.
Change icon (Picture of an I/O unit)	A dialog is displayed where you can upload the new image. 1. Click in the **Image file** input field and select from your local data directory the new image in PNG format and with max. 128 KB file size. 2. Click **Upload and update**. 3. If you want to restore the original image, click **Reset to default**. 4. Confirm with **OK**. The image is now replaced.
Load settings from file	This allows you to apply settings that have already saved to the open I/O unit. Your local data directory opens. 1. Select the file with the settings to upload.
Save settings to file	Depending on your system, a file save dialog will open or the file will be automatically downloaded to your download folder.
Remove	1. Confirm with **Yes**. The unit is then removed.
Load all signals from file	This allows you to load all signals into the list that you have already saved. Your local data directory opens. 1. Select the JSON file with the settings to upload it.
Save all signals to file	All synthetic signals including their settings are saved in a JSON file and downloaded immediately.

5.1.3 Sorting lists and reading information

You can quickly and easily sort lists and read various information about signals, signal connections, or synthetic signals directly in the list view.



I/O management › I/O units › Gateway Strickmaschine › Signals

□		Identifier ^	Name	Group	Type	Value
□	● ↦	AIN1	Feuchtesensor		DOUBLE	52,7 rH
□	● ↦	AIN2	Temperatur		DOUBLE	19,3 °C
□	● ↦	DIO1	Strickmaschine		BOOL	0
□	● ⇥	DIO2	Digital input 2		BOOL	0
□	● ⇥	LED_BLUE	Blue LED		BOOL	0
□	● ⇥	LED_GREEN	Green LED		BOOL	0
□	● ⇥	LED_RED	Red LED		BOOL	0
□	● ⇥	RELAY	Relay		BOOL	0
□	● ↦	SYSHUMIDITY	System Humidity		DOUBLE	16
□	● ↦	SYSTEMP	System Temperature		DOUBLE	44

Fig. 42: List view of the signals from the HUB-GM100 (example)

1. Open an I/O unit and go to the overview of signals.

   -or-

   On the **I/O management** page, click **Signal connections.**

   -or-

   On the **I/O management** page, click **Synthetic signals.**

   A list view is displayed showing all signals or connections.

2. To sort, click in the header of a column.

   You can sort alphabetically forward (A-Z) or alphabetically backward (Z-A).

3. To get information on the states of a signal or a signal connection, pay attention to the following icons:

   ☑ Only for signals: Entry is selected for the **Remove** and **Quick edit** function

   ● Signal or signal connection is activated

   ● Signal or signal connection is deactivated

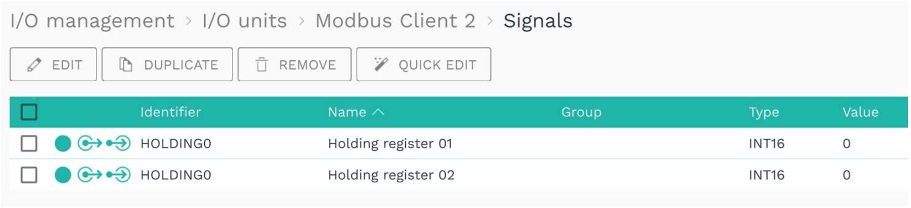
   ⇥ Only for signals: Signal is being written to the I/O unit (e.g., to a relay)

   ↦ Only for signals: Signal is being read from the I/O unit (e.g., from a sensor at an analog input)

> **NOTE:** The icons may vary depending on the task you have selected on the **I/O management** page.

5.1.4 Editing, duplicating, or removing list entries

For editing signals, signal connections, or synthetic signals, various buttons are available in each list view.



□		Identifier	Name ^	Group	Type	Value
□	●	HOLDING0	Holding register 01		INT16	0
□	●	HOLDING0	Holding register 02		INT16	0

Fig. 43: List view with buttons for editing (example)

NOTE: The buttons for the signals may vary depending on the I/O unit selected. If a button is not displayed in a list view, this function is not available for the selected I/O unit.

1. Open an I/O unit and go to the overview of signals.

   -or-

   On the **I/O management** page, click **Signal connections.**

   -or-

   On the **I/O management** page, click **Synthetic signals.**

   A list view is displayed showing all signals or connections.

2. Select one of the following buttons:

Edit	1. Select an entry and click **Edit**. -or- Double-click the entry you want to edit. You will return either to the setup wizard or to the Signal settings.
Duplicate	1. Select a list entry and click **Duplicate**. A copy of the signal or signal connection will be created, which you can edit as usual. **NOTE**: This button is not displayed for I/O units that have fixed preconfigured signals or channels.
Remove	1. Select the signal via the checkbox. -or- Select the signal connection. 2. Click **Remove**. A message will be displayed asking if you really want to delete the entry. 3. Confirm with **Yes**.

Edit signal properties (Only in Synthetic signals)	1. Select a synthetic signal from the list and click **Edit signal properties**. A window will open where you will find three tabs. 2. In the **Signal settings** tab, activate and configure the synthetic signal. 3. In the **Signal processing** tab, you can define how the signal value should be processed. For more details, see Configuring signal-processing steps, page 75. 4. Click **Save**. 5. In the **Measurement modelling** tab, you define how the measured values are to be displayed. For more details, see Configuring measurement modelling, page 81. 6. Finally, click **Save & close**.
Reset (Only in Synthetic signals)	Resets an applied counter (**Infinite counter** or **Resettable counter**). 1. Select a synthetic signal and click **Reset**. The counter is reset.
Quick edit (Only under I/O unit > Signals)	1. If you want to edit several signals at the same time, select the signals via the checkbox and then click **Quick edit**. 2. Select one of the five actions to be applied to all selected signals: ○ **Enable/Disable**: Enable or disable multiple signals at once ○ **Group**: Assign a common group name ○ **Data series set**: All synthetic signals including their Assign a common name for the data series set. This will display all signals with the same data series set in FlexPlorer under Live diagrams in a common diagram, so that the signal values of different devices/sensors can be compared directly in live operation. ○ **Sampling interval**: Set the sampling interval ○ **Recording settings**: Specify whether you want to record the signal values in the VictoriaMetrics database and at what time interval [s] this should take place. ○ **Decimals**: Set the number of decimal places ○ **Unit**: Set a unit A dialog window opens. 3. Enter the parameter required by the selected quick tool (e.g., the group name or number of decimal places). 4. Click **Save & close**.

5.1.5 Searching for entries

The search function is available for all list views of the SIINEOS management console. In the **I/O management,** you can use it to search through I/O units, signals, signal connections, and synthetic signals.

1. Just start typing.

   Your input is directly transferred to the search field in the upper right corner and the hits are dynamically displayed in the list.

sensor

   You can enter upper- or lower-case letters and numbers.

   The search runs through all the entries you have made in the settings, for example, also device addresses.

5.2 Creating I/O units

If you have selected **I/O units** on the **I/O management** page, you can now set up your peripheral devices. Each device has individual settings and parameters, so the following sections describe how to set up each I/O unit separately.

On the in.hub download portal you will also find the operating manuals of in.hub's own devices for further information: https://download.inhub.de/

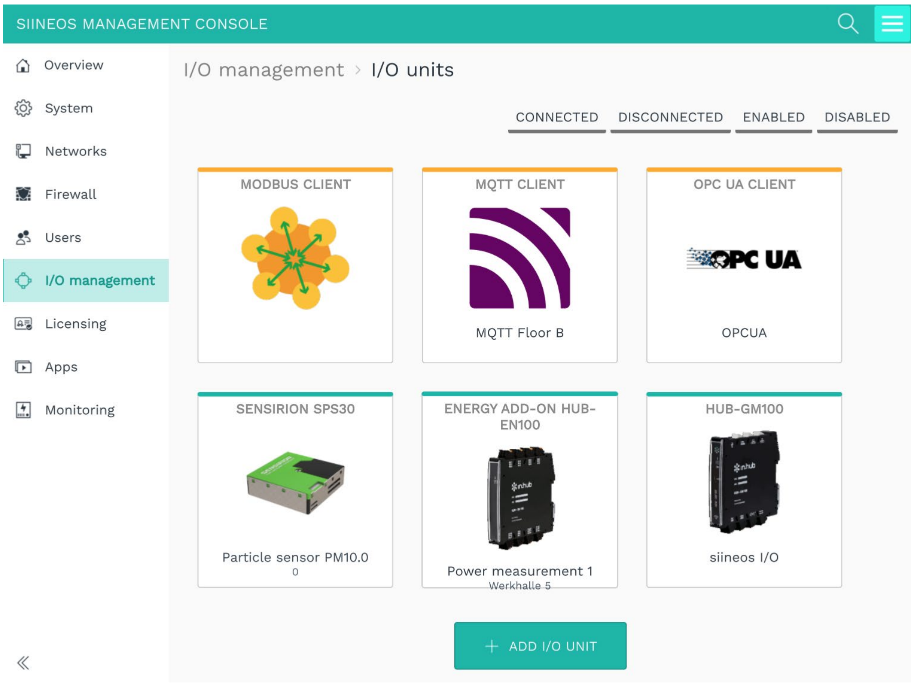


Fig. 44: I/O management > I/O units (example)

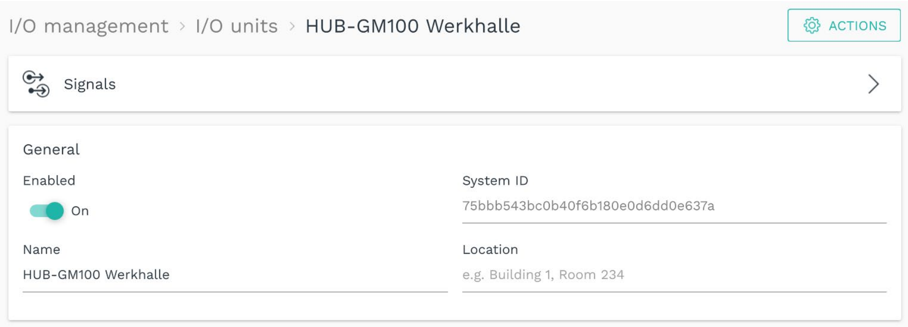
5.2.1 Adding a HUB-GM100

NOTE: This I/O unit refers to the local gateway you are currently using and allows you to access signals at the local interfaces.

1. On the home page of **I/O management,** select **I/O units.**
2. Click **Add I/O unit**.
3. Select **HUB-GM100** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.



I/O management › I/O units › HUB-GM100 Werkhalle

General

Enabled: On

System ID: 75bbb543bc0b40f6b180e0d6dd0e637a

Name: HUB-GM100 Werkhalle

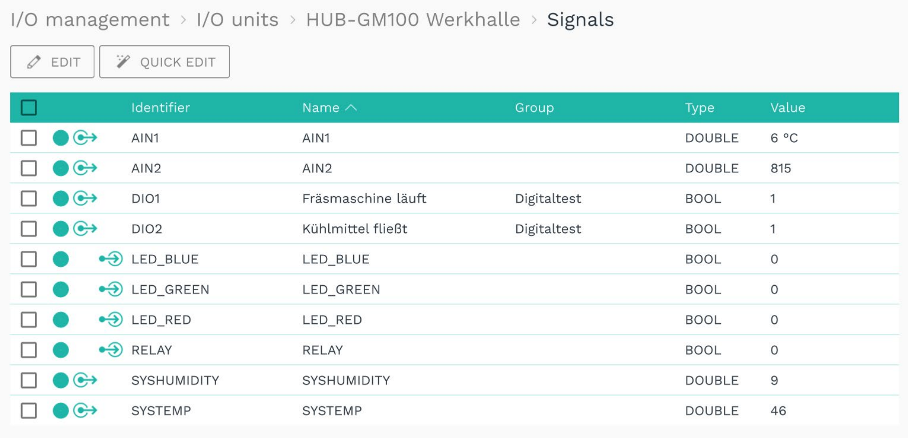
Location: e.g. Building 1, Room 234

Fig. 45: Device settings for the HUB-GM100 (example)

The new I/O unit is automatically enabled. If you only want to use it later, you have to set the **Enabled** slider to **Off**.

6. Optional: Enter the **Location**.
7. Click **Signals**.

   The signals for all interfaces and internal sensors are already created.



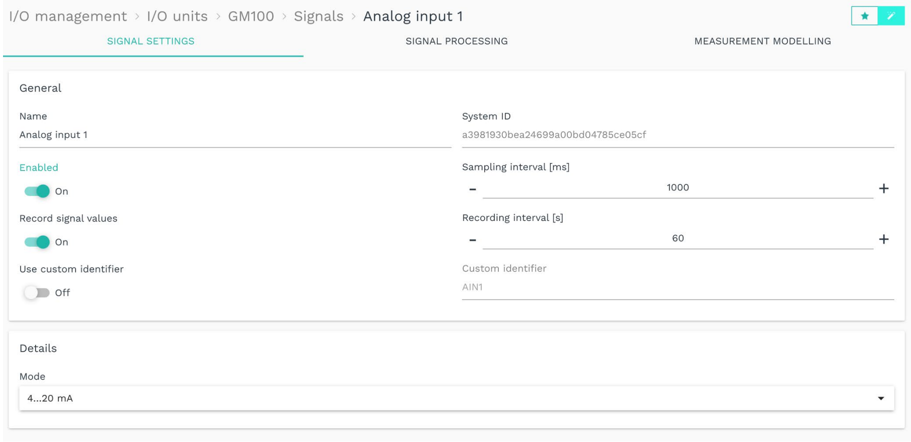
I/O management › I/O units › HUB-GM100 Werkhalle › Signals

☐		Identifier	Name	Group	Type	Value
☐	●	AIN1	AIN1		DOUBLE	6 °C
☐	●	AIN2	AIN2		DOUBLE	815
☐	●	DIO1	Fräsmaschine läuft	Digitaltest	BOOL	1
☐	●	DIO2	Kühlmittel fließt	Digitaltest	BOOL	1
☐	●	LED_BLUE	LED_BLUE		BOOL	0
☐	●	LED_GREEN	LED_GREEN		BOOL	0
☐	●	LED_RED	LED_RED		BOOL	0
☐	●	RELAY	RELAY		BOOL	0
☐	●	SYSHUMIDITY	SYSHUMIDITY		DOUBLE	9
☐	●	SYSTEMP	SYSTEMP		DOUBLE	46

Fig. 46: Signals for the HUB-GM100 (example)

8. Select the signal you want to configure.

   A window opens, where you will find three tabs.


I/O management › I/O units › GM100 › Signals › Analog input 1
SIGNAL SETTINGS
SIGNAL PROCESSING
MEASUREMENT MODELLING

General

Name: Analog input 1

System ID: a3981930bea24699a00bd04785ce05cf

Enabled: On

Sampling interval [ms]: 1000

Record signal values: On

Recording interval [s]: 60

Use custom identifier: Off

Custom identifier: AIN1

Details

Mode: 4...20 mA

Abb. 47: Tab card “Signal settings“ in the “Advanced” viewing mode

9. In the **Signal settings** tab, activate and configure the interface.
   - Optional: Change the name of the interface.
   - Set the slider to **On**.
   - In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).
   - Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
   - Enter the desired time interval for the recording in the **Recording interval** field (in milliseconds).
10. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.
11. Depending on the selected signal type, further inputs are necessary:

AIN (analog input)	**Mode** Select the analog interface type for the connected sensor. The options are 0...5 V / 0...10 V / 0...20 V / 4...20 mA
DIO (digital input/output)	**Mode** Specify whether this interface is to act as an input or output. ○ You have selected **Input**: To count how many times the signal value has changed from 0 to 1, set the slider **Count rising edges** to **On**. To count how many times the signal value has changed from 1 to 0, set the slider **Count falling edges** to **On**. ○ You have selected **Output**: Under **Default state** set the slider to **On**, if a positive voltage is to be output at the digital input.

LED	**Default state** Set whether the LED should be off or on in the default state.
Relay	**Default state** Set whether the relay should be off or on in the default state.

12. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.

13. Click **Save**.

14. In the **Measurement modelling** tab, you can define how the measured values are to be displayed.

    For more information, see Configuring measurement modelling, page 81.

15. Finally, click **Save & close**.

5.2.2 Adding a HUB-GM200

> **NOTE:** This I/O unit refers to the local gateway you are currently using and allows you to access signals at the local interfaces.

1. On the home page of **I/O management,** select **I/O units.**

2. Click **Add I/O unit**.

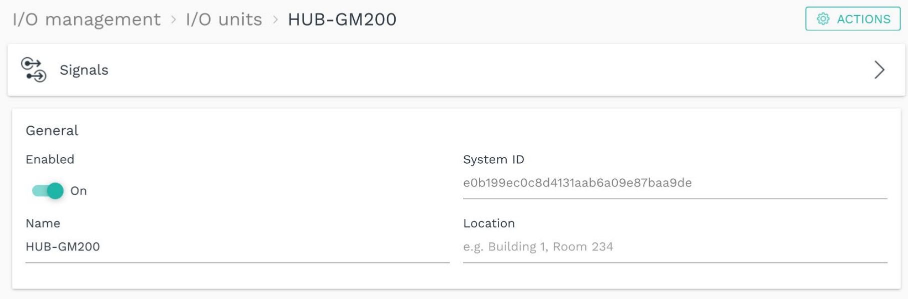
3. Select **HUB-GM200** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.

4. Enter the **Name** for the I/O unit.

5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.



General

Enabled: On

System ID: e0b199ec0c8d4131aab6a09e87baa9de

Name: HUB-GM200

Location: e.g. Building 1, Room 234

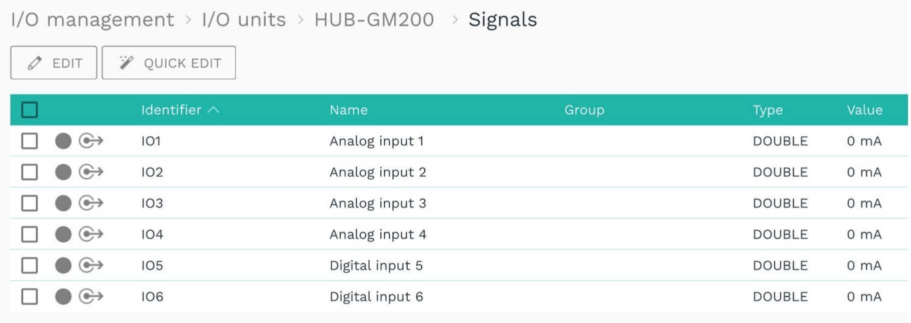
Fig. 48: Device settings for the HUB-GM200 (example)

The new I/O unit is automatically enabled. If you only want to use it later, you have to set the **Enabled** slider to **Off**.

6. Optional: Enter the **Location**.

7. Click **Signals**.

   The signals for all interfaces are already created.



I/O management › I/O units › HUB-GM200 › Signals

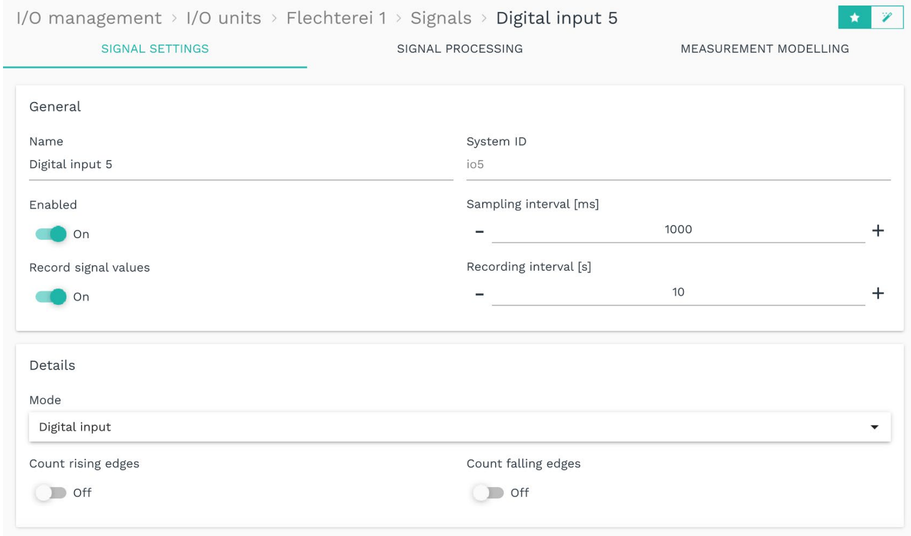
EDIT | QUICK EDIT

□		Identifier	Name	Group	Type	Value
□	●	IO1	Analog input 1		DOUBLE	0 mA
□	●	IO2	Analog input 2		DOUBLE	0 mA
□	●	IO3	Analog input 3		DOUBLE	0 mA
□	●	IO4	Analog input 4		DOUBLE	0 mA
□	●	IO5	Digital input 5		DOUBLE	0 mA
□	●	IO6	Digital input 6		DOUBLE	0 mA

Fig. 49: Signals for the HUB-GM200 (example)

8. Select the signal you want to configure.

   A window opens, where you will find three tabs.



I/O management › I/O units › Flechterei 1 › Signals › Digital input 5

SIGNAL SETTINGS | SIGNAL PROCESSING | MEASUREMENT MODELLING

General

Name: Digital input 5

System ID: io5

Enabled: On

Sampling interval [ms]: 1000

Record signal values: On

Recording interval [s]: 10

Details

Mode: Digital input

Count rising edges: Off

Count falling edges: Off

Fig. 50: Signals for the HUB-GM200 (example)

9. In the **Signal settings** tab, activate and configure the interface.
   - Optional: Change the name of the interface.
   - Set the **Enabled** slider to **On**.
   - In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).
   - Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
   - Enter the desired time interval for the recording in the **Recording interval** field (in seconds).
10. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.

11. In the **Details** area, you specify whether this interface is to function as an **Analog input 4...20 mA**, **Analog input 0...10 V**, **Digital input** or **Digital output**.
12. Depending on the selected signal type, further inputs are necessary:
    - If **Digital input** is selected:

      To count how often the signal value has changed from 0 to 1, set the **Count rising edges** slider to **On**.

      To count how often the signal value has changed from 1 to 0, set the **Count falling edges** slider to **On**.
    - If **Digital output** is selected:

      Specify whether the default state should be off or on.
13. For all input signals you can define how the signal value should be processed in the **Signal processing** tab.

    For more information, see Configuring signal-processing steps, page 75.
14. Click **Save**.
15. In the **Measurement modelling** tab, you can define how the measured values are to be displayed.

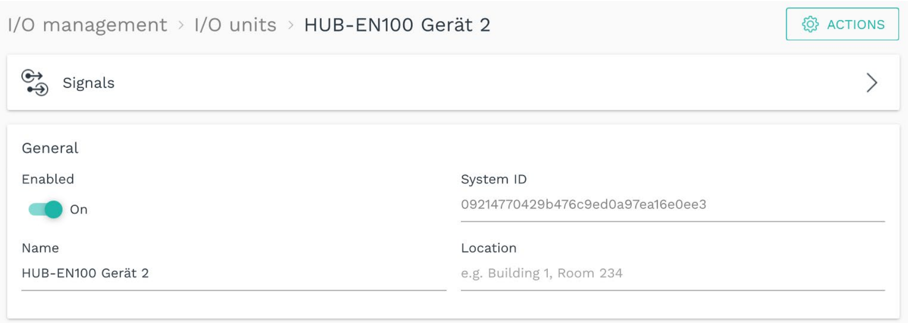
    For more information, see Configuring measurement modelling, page 81.
16. Finally, click **Save & close**.

5.2.3 Adding a HUB-EN100 energy add-on module

1. On the home page of **I/O management,** select **I/O units.**
2. Click **Add I/O unit**.
3. Select **Energy Add-On HUB-EN100** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.



Enabled: On

System ID: 09214770429b476c9ed0a97ea16e0ee3

Name: HUB-EN100 Gerät 2

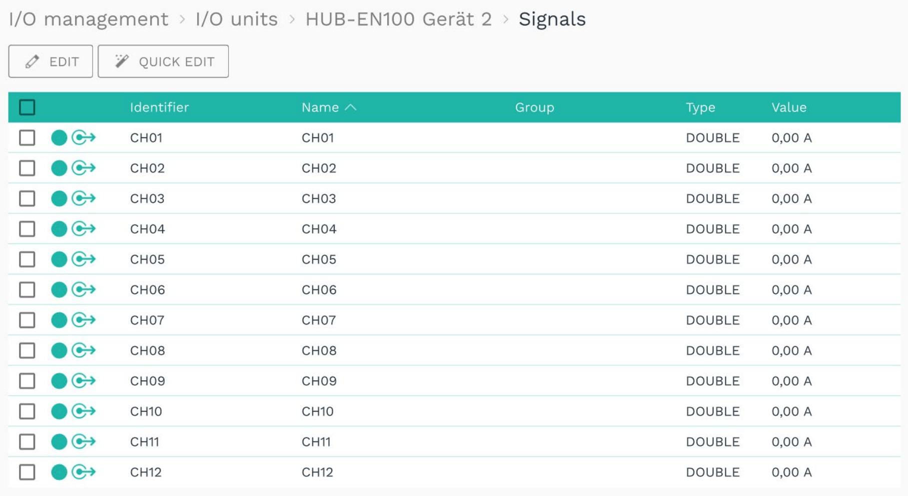
Location: e.g. Building 1, Room 234

Fig. 51: Device settings for the HUB-EN100 (example)

The new I/O unit is automatically enabled. If you only want to use it later, you have to set the **Enabled** slider to **Off**.

6. Optional: Enter the **Location.**
7. Click **Signals**.

   The signals for all channels of the HUB-EN100 are already created.



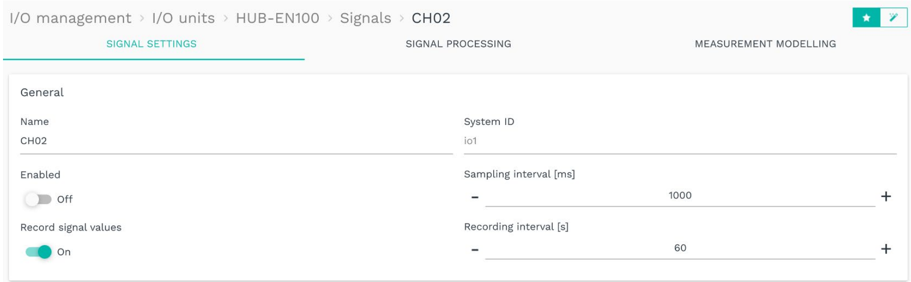
I/O management › I/O units › HUB-EN100 Gerät 2 › Signals

☐		Identifier	Name	Group	Type	Value
☐	●	CH01	CH01		DOUBLE	0,00 A
☐	●	CH02	CH02		DOUBLE	0,00 A
☐	●	CH03	CH03		DOUBLE	0,00 A
☐	●	CH04	CH04		DOUBLE	0,00 A
☐	●	CH05	CH05		DOUBLE	0,00 A
☐	●	CH06	CH06		DOUBLE	0,00 A
☐	●	CH07	CH07		DOUBLE	0,00 A
☐	●	CH08	CH08		DOUBLE	0,00 A
☐	●	CH09	CH09		DOUBLE	0,00 A
☐	●	CH10	CH10		DOUBLE	0,00 A
☐	●	CH11	CH11		DOUBLE	0,00 A
☐	●	CH12	CH12		DOUBLE	0,00 A

Fig. 52: Signals for the HUB-EN100 (example)

8. Select the signal you want to configure.

   A window opens, where you will find three tabs.



I/O management › I/O units › HUB-EN100 › Signals › CH02

General

Name: CH02

System ID: io1

Enabled: Off

Sampling interval [ms]: – 1000 +

Record signal values: On

Recording interval [s]: – 60 +

Fig. 53: “Signal settings” tab for the HUB-EN100

9. In the **Signal settings** tab, activate and configure the interface.
   - Optional: Change the name of the interface.
   - Set the slider to **On**.
   - In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).
   - Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
   - Enter the desired time interval for the recording in the **Recording interval** field (in seconds).
10. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.

11. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.

12. Click **Save**.

13. In the **Measurement modelling** tab, you define how the measured values are to be displayed.

    For more information, see Configuring measurement modelling, page 81.

14. Finally, click **Save & close**.

5.2.4 Adding the HUB-VM102 vibration module

1. On the home page of **I/O management,** select **I/O units.**

2. Click **Add I/O unit**.

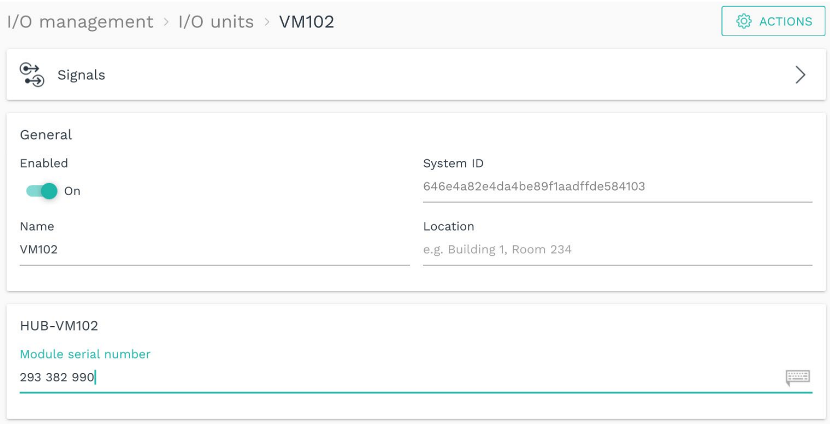
3. Select **HUB-VM102** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.

4. Enter the **Name** for the I/O unit.

5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.



Enabled: On

System ID: 646e4a82e4da4be89f1aadffde584103

Name: VM102

Location: e.g. Building 1, Room 234

Module serial number: 293 382 990

Fig. 54: Device settings for the HUB-VM102 (example)

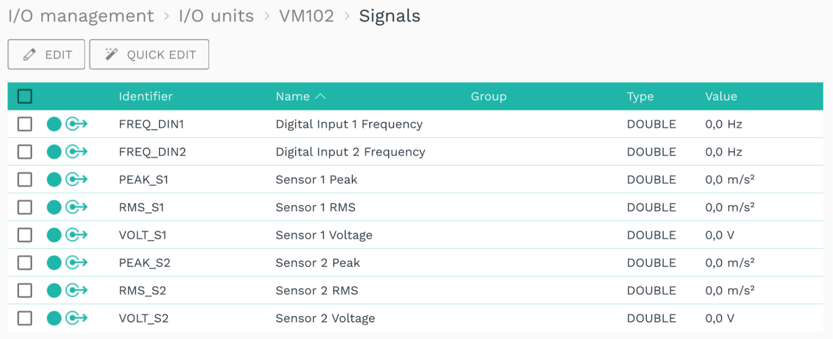
The new I/O unit is automatically enabled. If you only want to use it later, set the slider to **Off**.

6. Optional: Enter the **Location.**

7. Under **Module serial number**, enter the S/N number that can be found on the housing of the HUB-VM102.

8. Click **Signals**.

   The signals for all channels of the HUB-VM102 are already created.



I/O management › I/O units › VM102 › Signals

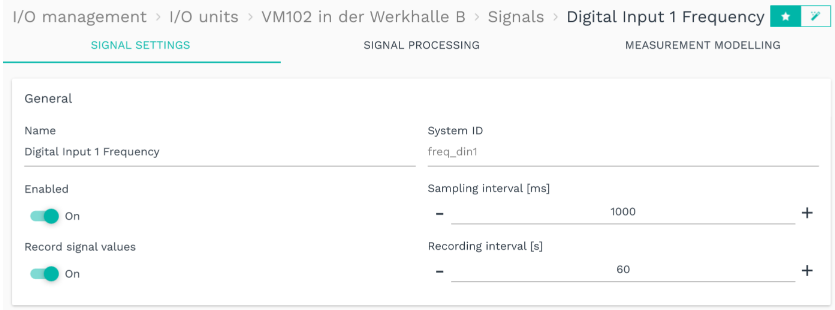
EDIT QUICK EDIT

□		Identifier	Name	Group	Type	Value
□	●	FREQ_DIN1	Digital Input 1 Frequency		DOUBLE	0,0 Hz
□	●	FREQ_DIN2	Digital Input 2 Frequency		DOUBLE	0,0 Hz
□	●	PEAK_S1	Sensor 1 Peak		DOUBLE	0,0 m/s²
□	●	RMS_S1	Sensor 1 RMS		DOUBLE	0,0 m/s²
□	●	VOLT_S1	Sensor 1 Voltage		DOUBLE	0,0 V
□	●	PEAK_S2	Sensor 2 Peak		DOUBLE	0,0 m/s²
□	●	RMS_S2	Sensor 2 RMS		DOUBLE	0,0 m/s²
□	●	VOLT_S2	Sensor 2 Voltage		DOUBLE	0,0 V

Fig. 55: Signals for the HUB-VM102 (example)

9. Select the signal you want to configure.

   A window opens, where you will find three tabs.



I/O management › I/O units › VM102 in der Werkhalle B › Signals › Digital Input 1 Frequency

SIGNAL SETTINGS SIGNAL PROCESSING MEASUREMENT MODELLING

General

Name: Digital Input 1 Frequency

System ID: freq_din1

Enabled: On

Sampling interval [ms]: 1000

Record signal values: On

Recording interval [s]: 60

Fig. 56: “Signal settings” tab for the HUB-VM102

10. In the **Signal settings** tab, activate and configure the interface.
    - Optional: Change the name of the interface.
    - Set the **Enabled** slider to **On**.
    - In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).
    - Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
    - Enter the desired time interval for the recording in the **Recording interval** field (in seconds).
11. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.
12. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.
13. Click **Save**.
14. In the **Measurement modelling** tab, you define how the measured values are to be displayed.

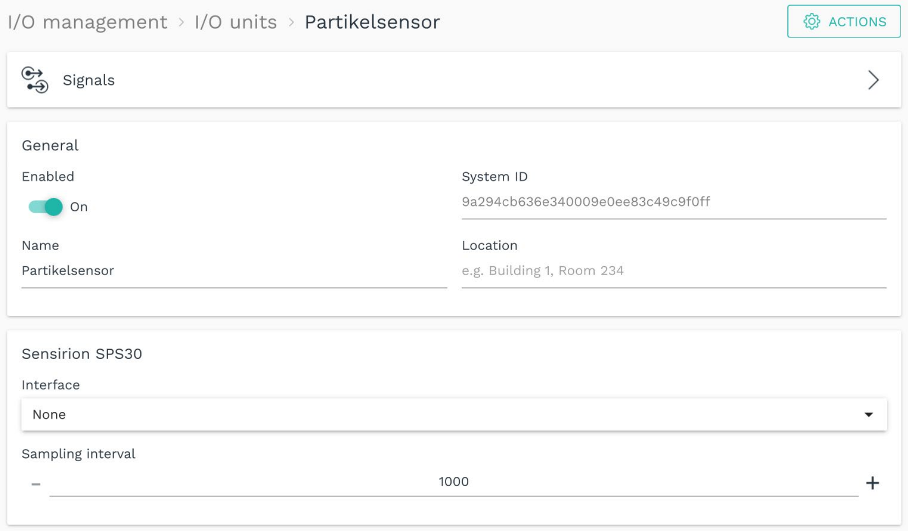
    For more information, see Configuring measurement modelling, page 81.
15. Finally, click **Save & close**.

5.2.5 Adding a Sensirion SPS30 particle sensor

1. On the **I/O management** page, select **I/O units.**
2. Click **Add I/O unit**.
3. Select **Sensirion SPS30** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.



I/O management › I/O units › Partikelsensor

General

Enabled: On

System ID: 9a294cb636e340009e0ee83c49c9f0ff

Name: Partikelsensor

Location: e.g. Building 1, Room 234

Sensirion SPS30

Interface: None

Sampling interval: 1000

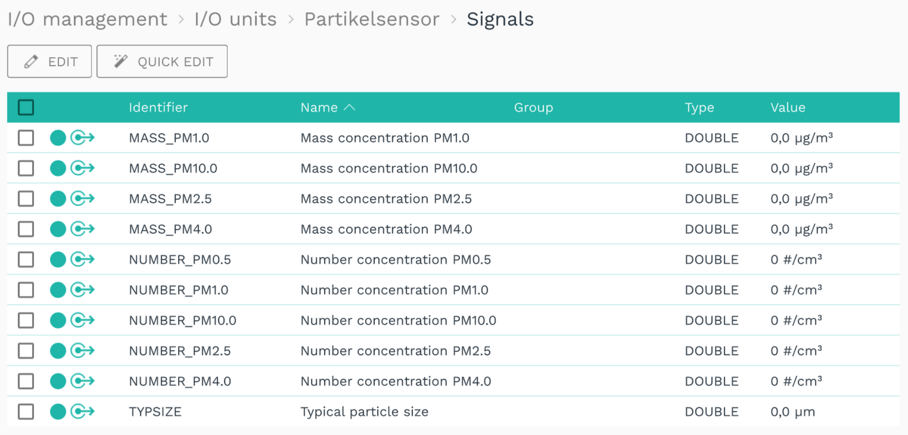
Fig. 57: Device settings for the Sensirion SPS30 particle sensor (example)

   The new I/O unit is automatically enabled. If you only want to use it later, set the **Enabled** slider to **Off**.
6. Optional: Enter the **Location**.
7. In the **Interface** drop-down list, select the sensor you want to add.

   NOTE: This list is only filled in if you also have sensors connected. If multiple sensors are connected, e.g., via a USB hub, then the sensors are numbered in sequence as they are plugged in to the USB hub.
8. In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).

9. Click **Signals**.

   The signals for all measured values of the particle sensor are already created.



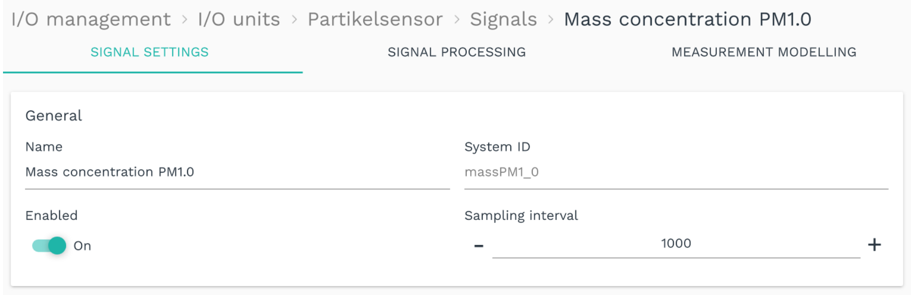
I/O management › I/O units › Partikelsensor › Signals

☐		Identifier	Name	Group	Type	Value
☐	●	MASS_PM1.0	Mass concentration PM1.0		DOUBLE	0,0 µg/m³
☐	●	MASS_PM10.0	Mass concentration PM10.0		DOUBLE	0,0 µg/m³
☐	●	MASS_PM2.5	Mass concentration PM2.5		DOUBLE	0,0 µg/m³
☐	●	MASS_PM4.0	Mass concentration PM4.0		DOUBLE	0,0 µg/m³
☐	●	NUMBER_PM0.5	Number concentration PM0.5		DOUBLE	0 #/cm³
☐	●	NUMBER_PM1.0	Number concentration PM1.0		DOUBLE	0 #/cm³
☐	●	NUMBER_PM10.0	Number concentration PM10.0		DOUBLE	0 #/cm³
☐	●	NUMBER_PM2.5	Number concentration PM2.5		DOUBLE	0 #/cm³
☐	●	NUMBER_PM4.0	Number concentration PM4.0		DOUBLE	0 #/cm³
☐	●	TYPSIZE	Typical particle size		DOUBLE	0,0 µm

Fig. 58: Signals for the Sensirion SPS30 particle sensor (example)

10. Select the signal you want to configure.

    A window opens, where you will find three tabs.



I/O management › I/O units › Partikelsensor › Signals › Mass concentration PM1.0

General

Name: Mass concentration PM1.0

System ID: massPM1_0

Enabled: On

Sampling interval: – 1000 +

Fig. 59: “Signal settings” tab for the Sensirion SPS30

11. In the **Signal settings** tab, activate and configure the interface.
    - Optional: Change the name of the interface.
    - Set the slider to **On**.
    - In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).
    - Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
    - Enter the desired time interval for the recording in the **Recording interval** field (in seconds).
12. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.
13. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.
14. Click **Save**.

15. In the **Measurement modelling** tab, you define how the measured values are to be displayed.

    For more information, see Configuring measurement modelling, page 81.

16. Finally, click **Save & close**.

5.2.6 Adding a Modbus RTU Modbus client

1. On the **I/O management** page, select **I/O units.**

   Before you create a new Modbus client of the **Modbus RTU** type, please check whether a Modbus RTU client already exists.

   Several Modbus clients (RTU) can be created for both the built-in RS485 interface and the backplane bus via the I/O management to communicate with several Modbus devices on the same bus. It is important that the settings of the Modbus RTU clients are identical except for the Modbus ID.

   If an RS485 or RS232 converter is connected via the external USB interface, several Modbus RTU clients cannot access it at the same time. If you still want to communicate with several devices via this bus, only one I/O unit may be created. In this case, the respective Modbus ID must be set accordingly in the Modbus registers.

2. Click **Add I/O unit**.

3. Select **Modbus client** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.

4. Enter the **Name** for the I/O unit.

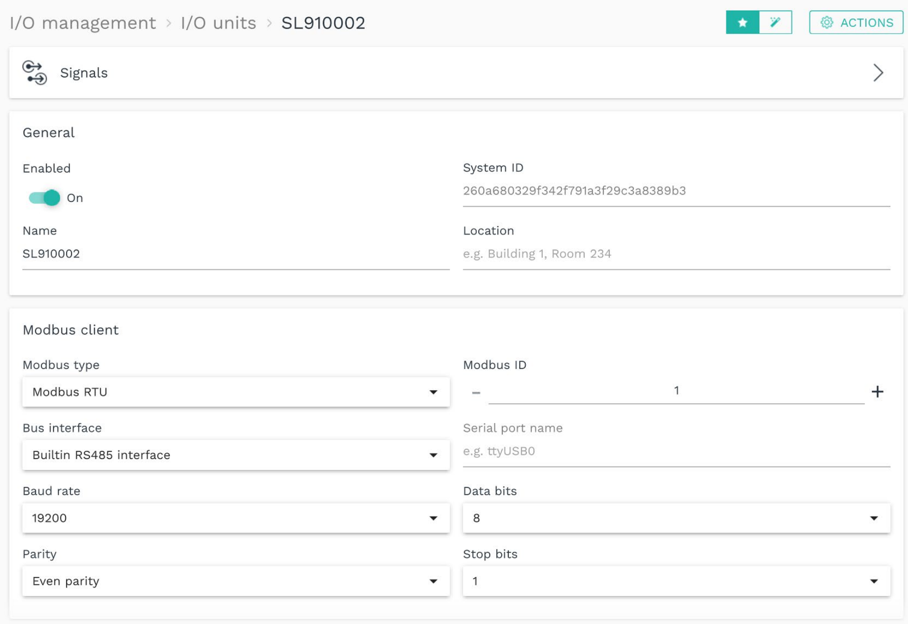
5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.

   The new I/O unit is automatically enabled. If you only want to use it later, set the **Enabled** slider to **Off**.

6. Optional: Enter the **Location**.

7. Under **Modbus type** select **Modbus RTU.**



I/O management › I/O units › SL910002

General

Enabled: On

System ID: 260a680329f342f791a3f29c3a8389b3

Name: SL910002

Location: e.g. Building 1, Room 234

Modbus client

Modbus type: Modbus RTU

Modbus ID: – 1 +

Bus interface: Builtin RS485 interface

Serial port name: e.g. ttyUSB0

Baud rate: 19200

Data bits: 8

Parity: Even parity

Stop bits: 1

Fig. 60: Device settings for the Modbus client type RTU in “Standard” viewing mode (example)

8. In the **Modbus client** area, you now make the following settings.

   ○ Under **Modbus ID**, enter the ID of the device you wish to communicate with.

   ○ Fill in all other input fields, such as **Baud rate** or **Parity**, according to the documentation of the connected device.

   ○ The corresponding **Bus interface** must be selected for communication with the Modbus device; in most cases, this will be the **Builtin RS485 interface**. For I/O modules (such as the HUB-IO100 or the HUB-EN200), select **Backplane bus**. A **Serial interface** is required if an RS485 or RS232 converter is connected via the external USB interface.

     Note: When using the serial interfaces, you must specify the **Name of the serial interface**. This depends on the device and may need to be determined via SSH. Usually "ttyUSB0" or in some cases "ttyACM0" is used.

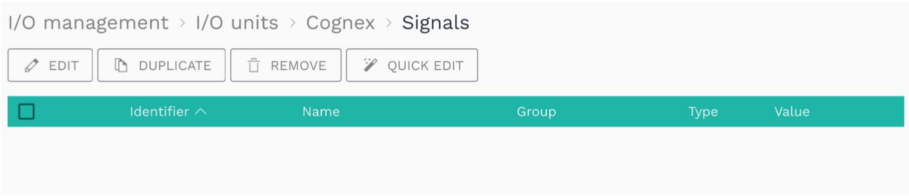
   ○ In the **Advanced** viewing mode, you can make additional fine adjustments if timing and performance problems occur during Modbus communication.

     In the **Request timeout [ms]** field, define the number of milliseconds after which a request is resent or discarded without a response.

     In the **Request retry count** field, enter how often a request should be sent if no response is received. After the number of attempts entered, the request is finally canceled.

     In the **Request queue size limit** field, enter the maximum number of requests to be included in the queue. If the value is set too low (lower than the number of Modbus registers), individual requests may never be sent to the bus. If the value is too high (significantly higher than the number of Modbus registers), the bus will be overloaded and the processing of requests will be delayed

9. Click **Signals**.

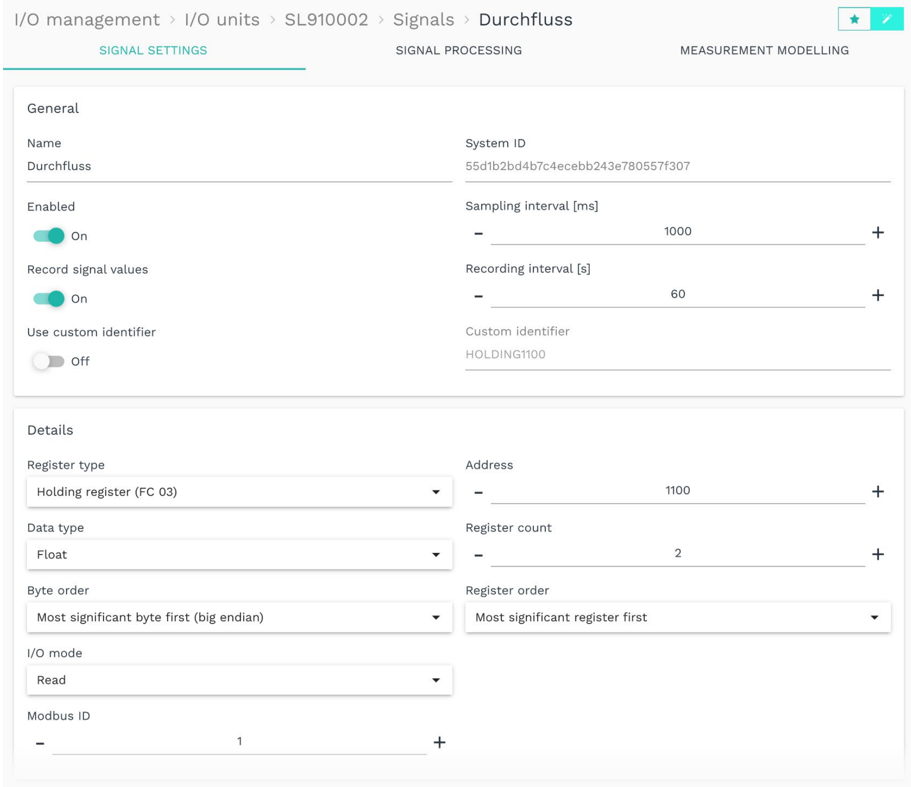


☐	Identifier ^	Name	Group	Type	Value

Fig. 61: Initially, no signals are predefined for the Modbus client

10. Click **Add I/O signal**.

A window opens, where you will find three tabs.


I/O management > I/O units > SL910002 > Signals > Durchfluss
SIGNAL SETTINGS
SIGNAL PROCESSING
MEASUREMENT MODELLING

General

Name: Durchfluss

System ID: 55d1b2bd4b7c4ecebb243e780557f307

Enabled: On

Sampling interval [ms]: 1000

Record signal values: On

Recording interval [s]: 60

Use custom identifier: Off

Custom identifier: HOLDING1100

Details

Register type: Holding register (FC 03)

Address: 1100

Data type: Float

Register count: 2

Byte order: Most significant byte first (big endian)

Register order: Most significant register first

I/O mode: Read

Modbus ID: 1

Fig. 62: "Signal settings" tab for the Modbus client in "Advanced" viewing mode

11. In the **Signal settings** tab, activate and configure the signal.

- Optional: Change the name of the signal.
- Set the **Enabled** slider to **On**.
- In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).

  NOTE: If you have selected the **I/O mode** "Write", no sampling takes place, and the sampling interval is ignored. Instead, the default value is written at startup and at each change. If the register is connected to a source signal via signal connection, the register is written with each change of the source signal.
- Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
- Enter the desired time interval for the recording in the **Recording interval** field (in seconds).

12. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.
13. Further entries are necessary in the **Details** area.
    - Depending on the selected register type, different entries can be made as to whether to read from the register or whether and what is to be written to the register. Please also refer to the tooltips.
    - If it is not possible to use several Modbus RTU clients (with different Modbus IDs) on the same bus interface (RS485/RS232 converter via USB), the respective ID of the device to be addressed can be specified instead. This ignores the global setting of the **Modbus client** I/O unit (see point 8) and instead uses the Modbus ID entered here for this register. Modbus ID entered here is used for this register instead.
    - Otherwise, leave the default value (**0**).
    - Fill in all other input fields according to the documentation of the connected device.
14. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.
15. Click **Save**.
16. In the **Measurement modelling** tab, you define how the measured values are to be displayed.

    For more information, see Configuring measurement modelling, page 81.
17. Finally, click **Save & close**.

5.2.7 Adding a Modbus TCP Modbus client

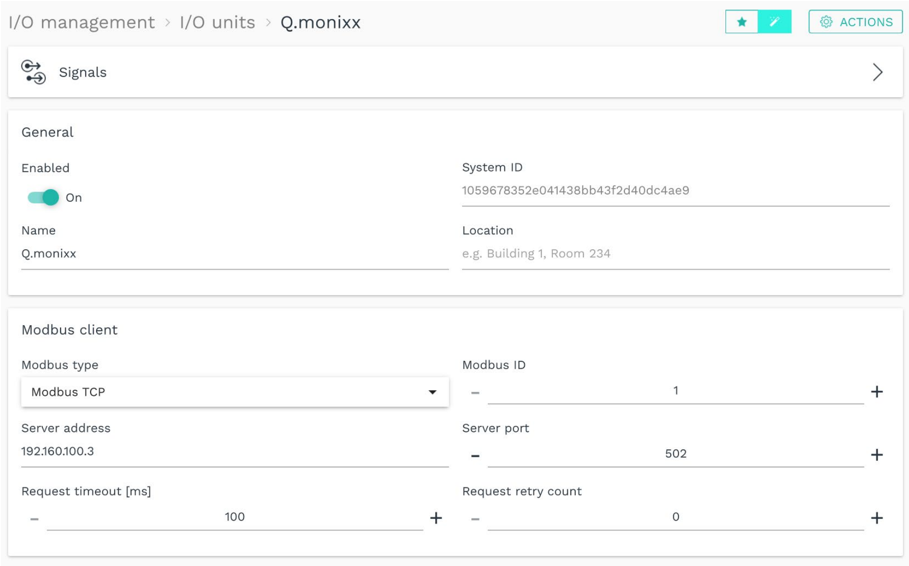
1. On the **I/O management** page, select **I/O units.**
2. Click **Add I/O unit**.
3. Select **Modbus client** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.

   The new I/O unit is automatically enabled. If you only want to use it later, set the slider to **Off**.
6. Optional: Enter the **Location**.

7. Under **Modbus type** select **Modbus TCP.**



Enabled: On

System ID: 1059678352e041438bb43f2d40dc4ae9

Name: Q.monixx

Location: e.g. Building 1, Room 234

Modbus type: Modbus TCP

Modbus ID: 1

Server address: 192.160.100.3

Server port: 502

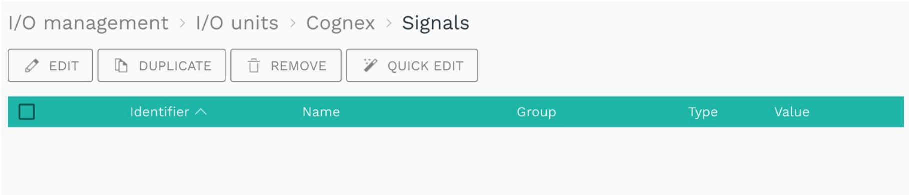
Request timeout [ms]: 100

Request retry count: 0

Fig. 63: Device settings for the Modbus client type TCP in “Advanced” viewing mode (example)

8. Enter the Modbus ID of the device you want to communicate with.
9. Enter the **Server address** and the **Server port** of the Modbus TCP server.
10. In the **Advanced** viewing mode, you can also define in the **Request timeout [ms]** field after how many milliseconds a request is resent without a response.

    In the **Request retry count** field, enter how often a request should be sent if no response is received. The request is then finally canceled after the entered attempts.
11. Click **Signals**.

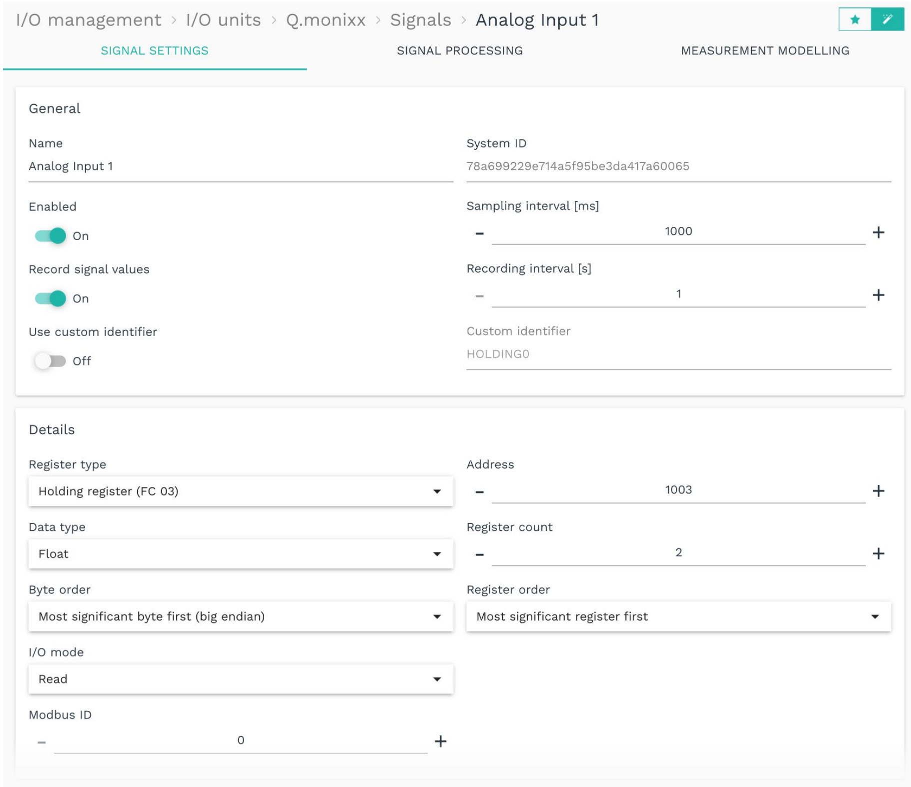


☐	Identifier ^	Name	Group	Type	Value

Fig. 64: Initially, no signals are predefined for the Modbus client

12. Click **Add I/O signal**.

    A window opens, where you will find three tabs.


I/O management › I/O units › Q.monixx › Signals › Analog Input 1
SIGNAL SETTINGS
SIGNAL PROCESSING
MEASUREMENT MODELLING

General

Name: Analog Input 1

System ID: 78a699229e714a5f95be3da417a60065

Enabled: On

Sampling interval [ms]: 1000

Record signal values: On

Recording interval [s]: 1

Use custom identifier: Off

Custom identifier: HOLDING0

Details

Register type: Holding register (FC 03)

Address: 1003

Data type: Float

Register count: 2

Byte order: Most significant byte first (big endian)

Register order: Most significant register first

I/O mode: Read

Modbus ID: 0

Fig. 65: “Signal settings” tab for the Modbus client in the “Advanced” viewing mode

13. In the **Signal settings** tab, activate and configure the signal.
    - Optional: Change the name of the signal.
    - Set the slider to **On**.
    - In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).

      NOTE: If you have selected the **I/O mode** "Write", no sampling takes place, and the sampling interval is ignored. Instead, the default value is written at startup and at each change. If the register is connected to a source signal via signal connection, the register is written with each change of the source signal.
    - Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
    - Enter the desired time interval for the recording in the **Recording interval** field (in seconds).
14. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.
15. Further entries are necessary in the **Details** area.
    - Depending on the selected register type, different entries can be made as to whether to read from the register or whether and what is to be written to the register. Please also refer to the tooltips.
    - Fill in all other input fields according to the documentation of the connected device.

16. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.

17. Click **Save**.

18. In the **Measurement modelling** tab, you define how the measured values are to be displayed.

    For more information, see Configuring measurement modelling, page 81.

19. Finally, click **Save & close.**

5.2.8 Adding an MQTT client

1. On the **I/O management** page, select **I/O units.**

2. Click **Add I/O unit**.

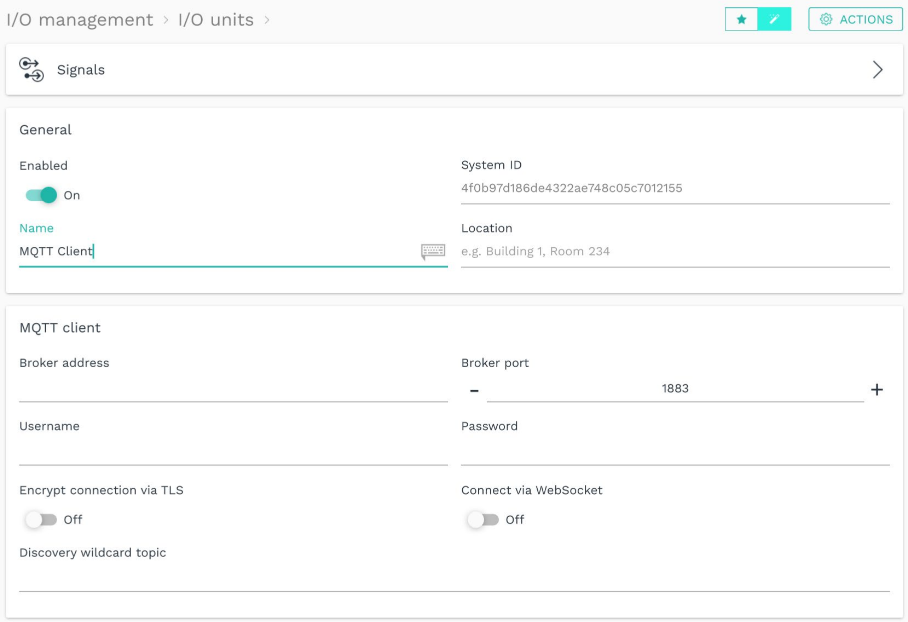
3. Select **MQTT client** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.

4. Enter the **Name** for the I/O unit.

5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.



General

Enabled: On

System ID: 4f0b97d186de4322ae748c05c7012155

Name: MQTT Client

Location: e.g. Building 1, Room 234

MQTT client

Broker address:

Broker port: 1883

Username:

Password:

Encrypt connection via TLS: Off

Connect via WebSocket: Off

Discovery wildcard topic:

Fig. 66: Device settings for the MQTT client in the “Advanced” viewing mode

   The new I/O unit is automatically enabled. If you only want to use it later, set the **Enabled** slider to **Off**.

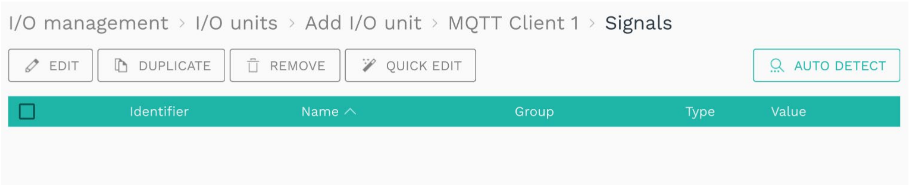
6. Optional: Enter the **Location**.

7. Under **MQTT Client**, enter the **Broker address**, **Broker port**, and optionally the **Discovery wildcard topic.**

   NOTE: These parameters must be known to you from your MQTT network.

- If authentication is required for the connection to the broker, you must enter the corresponding **Username** and **Password**.
- If you want to encrypt MQTT, set the **Encrypt connection via TLS** slider to **On**. If the connection is established with a broker in the internal network, the certificate of the organization CA must be stored under **System > Security & encryption**.
- In **Advanced** viewing mode, set the Connect via WebSocket slider to On if the MQTT broker only offers a connection via WebSockets.

8. Click **Save**.
9. Click **Signals**.


I/O management › I/O units › Add I/O unit › MQTT Client 1 › Signals

□	Identifier	Name ^	Group	Type	Value

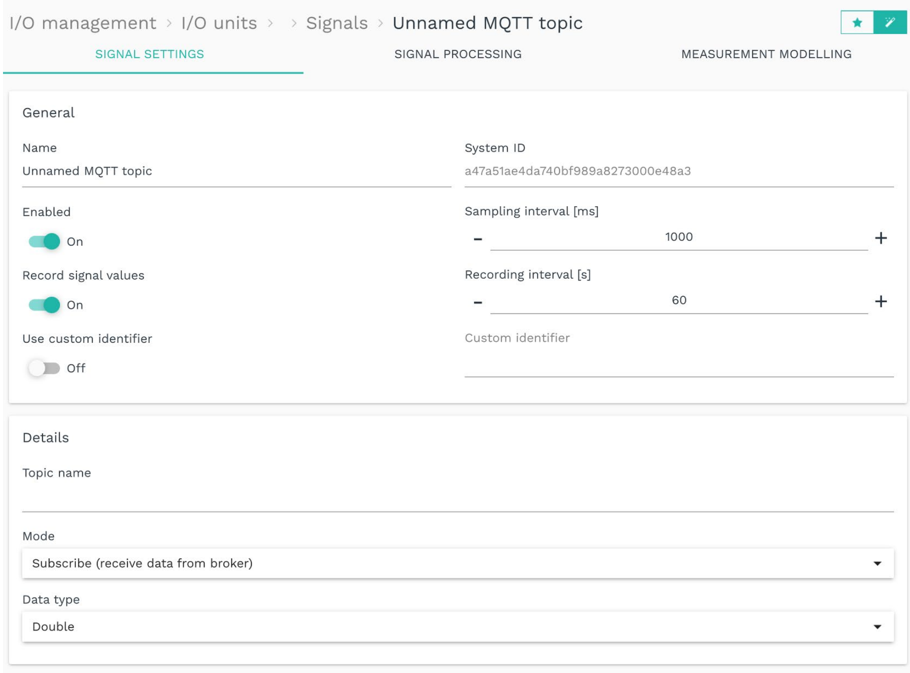
Fig. 67: Initially, no signals are predefined for the MQTT client

10. Click **Add I/O signal**.

    -or-

    Click **Auto detect** to add as signals all topics published on the MQTT broker that match the discovery wildcard topic as signals.

    When you add a new signal, a window opens, where you will find three tabs.


I/O management › I/O units › › Signals › Unnamed MQTT topic

General

Name: Unnamed MQTT topic

System ID: a47a51ae4da740bf989a8273000e48a3

Enabled: On

Sampling interval [ms]: – 1000 +

Record signal values: On

Recording interval [s]: – 60 +

Use custom identifier: Off

Custom identifier

Details

Topic name

Mode: Subscribe (receive data from broker)

Data type: Double

Fig. 68: “Signal settings” tab for the MQTT Client in “Advanced” viewing mode

11. In the **Signal settings** tab, activate and configure the signal.
    - Enter the name of the signal.
    - Set the **Enabled** slider to **On**.

- In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).
- Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
- Enter the desired time interval for the recording in the **Recording interval** field (in seconds).

12. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.
13. In the **Details** area, you can enter additional parameters:
    - Enter a **Topic name**.
    - In the **Mode** drop-down list, select whether you want to receive data from the broker via the MQTT client (**Subscribe**) or send data to the broker (**Publish**).
    - In the **Data type** drop-down list, select how the data in the MQTT topic should be interpreted.

      Double is selected by default, i.e. the MQTT data is interpreted as floating point numbers with double precision.

      If the data in the MQTT topic is available as a JSON string, select the **JSON data** entry. Only then can you enter the key name containing the numerical value to be used in the **JSON data key** field.
    - In **Publish** mode, set the **Publish as retained message** slider. In this case, the broker sends the last value published via this topic to all newly added clients.

    NOTE: These parameters must be known to you from your MQTT network.
14. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.
15. Click **Save**.
16. In the **Measurement modelling** tab, you define how the measured values are to be displayed.

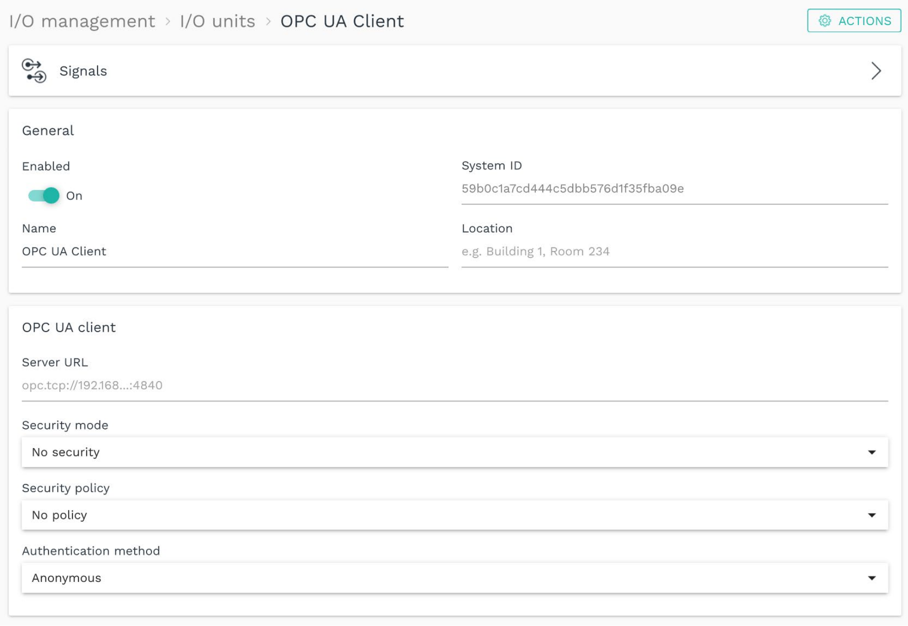
    For more information, see Configuring measurement modelling, page 81.
17. Finally, click **Save & close**.

5.2.9 Adding an OPC UA client

1. On the **I/O management** page, select **I/O units.**
2. Click **Add I/O unit**.
3. Select **OPC UA Client** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.



General

Enabled: On

System ID: 59b0c1a7cd444c5dbb576d1f35fba09e

Name: OPC UA Client

Location: e.g. Building 1, Room 234

OPC UA client

Server URL: opc.tcp://192.168...:4840

Security mode: No security

Security policy: No policy

Authentication method: Anonymous

Fig. 69: Device settings for the OPC UA client (example)

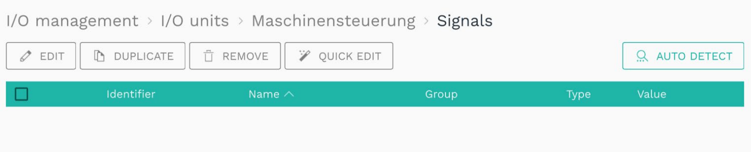
The new I/O unit is automatically enabled. If you only want to use it later, set the **Enabled** slider to **Off**.

6. Optional: Enter the **Location**.
7. Under **OPC UA client** make the following settings:
   - **Server URL**
   - Under **Security mode**, specify whether messages between the gateway and OPC UA server should only be signed or encrypted and signed.
   - Under **Security policy**, select which encryption algorithm is to be used for the security modes.

     If no encryption algorithm is to be used, select **No policy**. If you do, you can upload the respective server and client certificate as a file and enter the private key.
   - If authentication is required on the OPC UA server, select the **Authentication method** "Username and password" and specify the user data. If no authentication is required, select "Anonymous".

NOTE: These parameters must be known from your OPC UA server (e.g., the PLC configuration).

8. Click **Save**.
9. Select **Signals**.

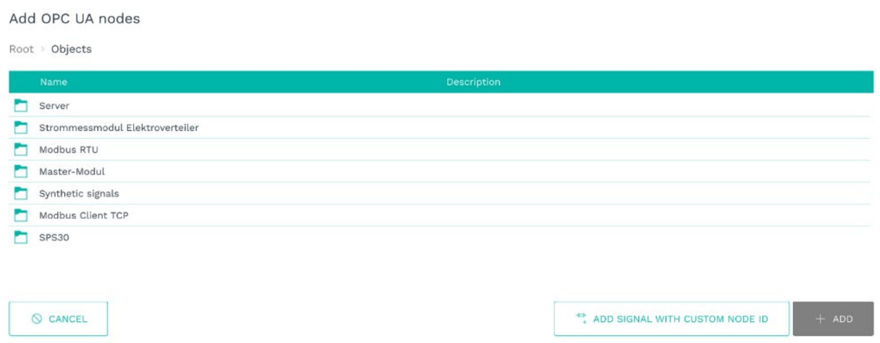


□	Identifier	Name ^	Group	Type	Value

Fig. 70: Initially, no signals are predefined for the OPC UA client

10. Click **Add I/O signal**.

    A new window opens in which you can select an existing object from the OPC UA node:


Add OPC UA nodes

Name	Description
Server	
Strommessmodul Elektroverteiler	
Modbus RTU	
Master-Modul	
Synthetic signals	
Modbus Client TCP	
SPS30	

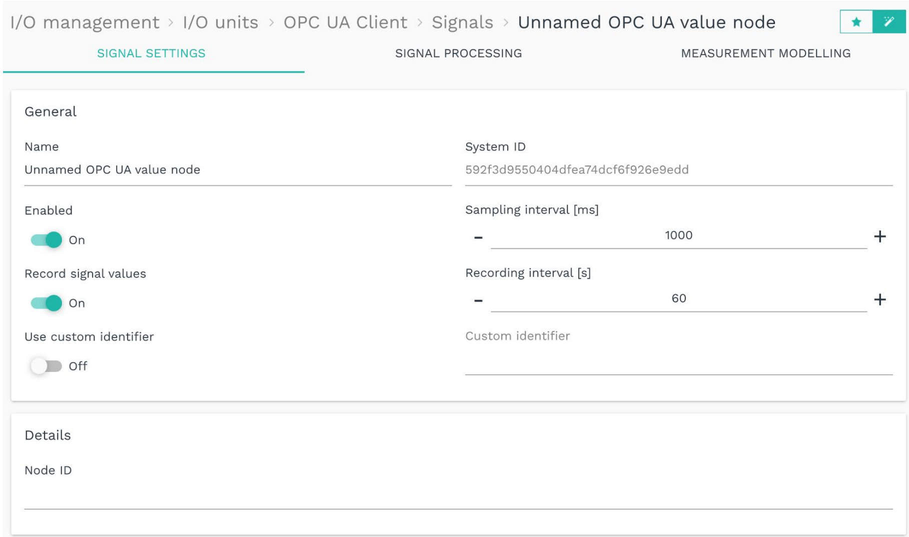
Fig. 71: “Add OPC UA nodes” window (Example)

11. Select a node object and click **Add**.

    -or

    If you want to create a new signal, click on **Add signal with custom node ID**.

    A window opens, where you will find three tabs.


I/O management › I/O units › OPC UA Client › Signals › Unnamed OPC UA value node
SIGNAL SETTINGS
SIGNAL PROCESSING
MEASUREMENT MODELLING

General

Name: Unnamed OPC UA value node

System ID: 592f3d9550404dfea74dcf6f926e9edd

Enabled: On

Sampling interval [ms]: – 1000 +

Record signal values: On

Recording interval [s]: – 60 +

Use custom identifier: Off

Custom identifier

Details

Node ID

Fig. 72: “Signal settings” tab of the OPC UA client

12. In the **Signal settings** tab, activate and configure the signal.
    - Enter the name of the signal.
    - Set the slider to **On**.
    - In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).
    - Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
    - Enter the desired time interval for the recording in the **Recording interval** field (in seconds).
13. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.
14. In the **Details** area, enter the **Node ID.**

    NOTE: This parameter must be known to you from your OPC UA server (e.g., the PLC configuration).

    If the signal was automatically detected, the field **Node ID** is filled in. If not, specify the full node ID, e.g. “ns=2;s=Machine”.
15. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.
16. Click **Save**.
17. In the **Measurement modelling** tab, you define how the measured values are to be displayed.

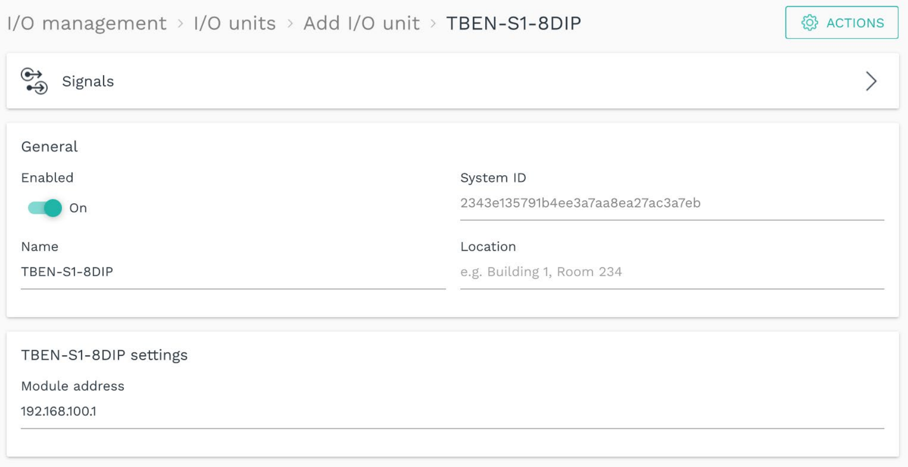
    For more information, see Configuring measurement modelling, page 81.
18. Finally, click **Save & close**.

5.2.10 Adding a TBEN-S1-8DIP module

1. On the **I/O management** page, select **I/O units.**
2. Click **Add I/O unit**.
3. Select **TBEN-S1-8DIP** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.



I/O management › I/O units › Add I/O unit › TBEN-S1-8DIP

ACTIONS

Signals

General

Enabled: On

System ID: 2343e135791b4ee3a7aa8ea27ac3a7eb

Name: TBEN-S1-8DIP

Location: e.g. Building 1, Room 234

TBEN-S1-8DIP settings

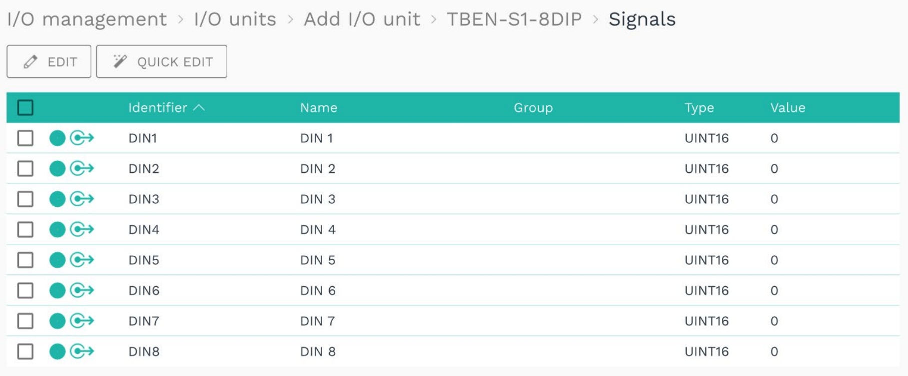
Module address: 192.168.100.1

Fig. 73: Device settings for the TBEN-S1-8DIP module (example)

The new I/O unit is automatically enabled. If you only want to use it later, set the **Enabled** slider to **Off**.

6. Optional: Enter the **Location**.
7. In the **Module address** input field, enter the host name or the IP address of the TBEN module to which a connection is to be established.
8. Click **Save**.
9. Select **Signals**.

   The signals for all digital inputs of the TBEN module are already created.



I/O management › I/O units › Add I/O unit › TBEN-S1-8DIP › Signals

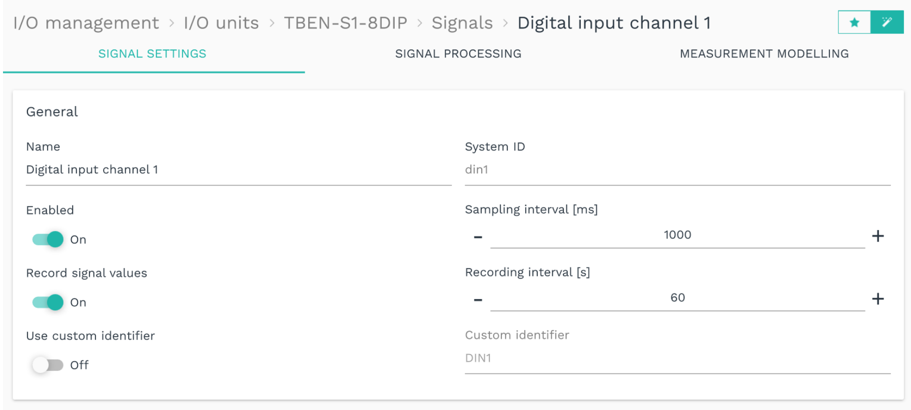
EDIT QUICK EDIT

□		Identifier	Name	Group	Type	Value
□	●	DIN1	DIN 1		UINT16	0
□	●	DIN2	DIN 2		UINT16	0
□	●	DIN3	DIN 3		UINT16	0
□	●	DIN4	DIN 4		UINT16	0
□	●	DIN5	DIN 5		UINT16	0
□	●	DIN6	DIN 6		UINT16	0
□	●	DIN7	DIN 7		UINT16	0
□	●	DIN8	DIN 8		UINT16	0

Fig. 74: Signals for the TBEN-S1-8DIP module

10. Select the signal you want to configure.

    A window opens, where you will find three tabs.



I/O management › I/O units › TBEN-S1-8DIP › Signals › Digital input channel 1

SIGNAL SETTINGS | SIGNAL PROCESSING | MEASUREMENT MODELLING

General

Name: Digital input channel 1

System ID: din1

Enabled: On

Sampling interval [ms]: 1000

Record signal values: On

Recording interval [s]: 60

Use custom identifier: Off

Custom identifier: DIN1

Fig. 75: “Signal settings” tab for the TBEN-S1-8DIP module

11. In the **Signal settings** tab, activate and configure the signal.
    - Enter the name of the signal.
    - Set the slider to **On**.
    - In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).
    - Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
    - Enter the desired time interval for the recording in the **Recording interval** field (in seconds).
12. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.
13. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.
14. Click **Save**.
15. In the **Measurement modelling** tab, you define how the measured values are to be displayed.

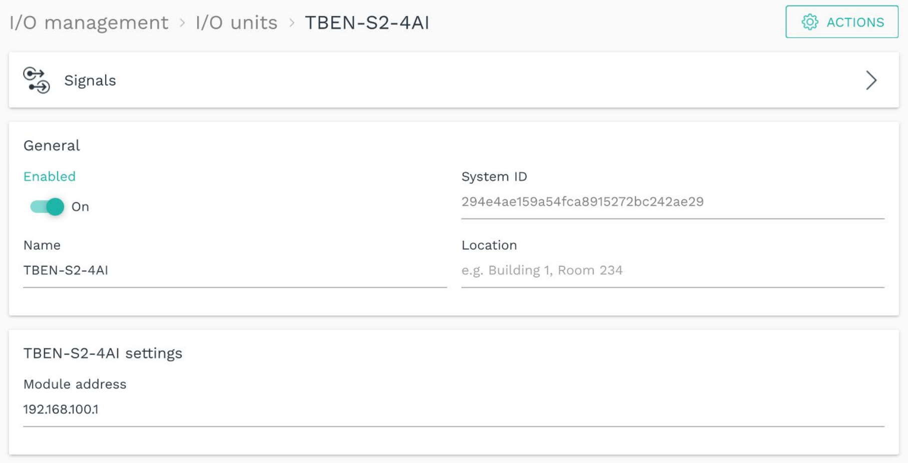
    For more information, see Configuring measurement modelling, page 81.
16. Finally, click **Save & close**.

5.2.11 Adding a TBEN-S2-4AI module

1. On the home page of **I/O management,** select **I/O units.**
2. Click **Add I/O unit**.
3. Select **TBEN-S2-4AI** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.


I/O management › I/O units › TBEN-S2-4AI

General

Enabled: On

System ID: 294e4ae159a54fca8915272bc242ae29

Name: TBEN-S2-4AI

Location: e.g. Building 1, Room 234

TBEN-S2-4AI settings

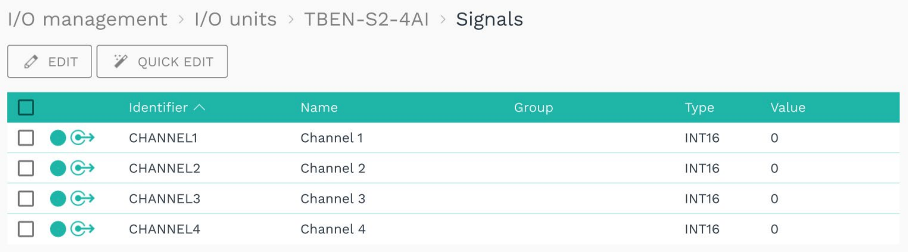
Module address: 192.168.100.1

Fig. 76: Device settings for the TBEN-S2-4AI module (example)

   The new I/O unit is automatically enabled. If you only want to use it later, set the **Enabled** slider to **Off**.

6. Optional: Enter the **Location**.
7. Enter in the input field **Module address** the host name or the IP address of the TBEN module to which a connection is to be established.
8. Click **Save**.
9. Select **Signals**.

   The signals for all analog input channels are already applied.

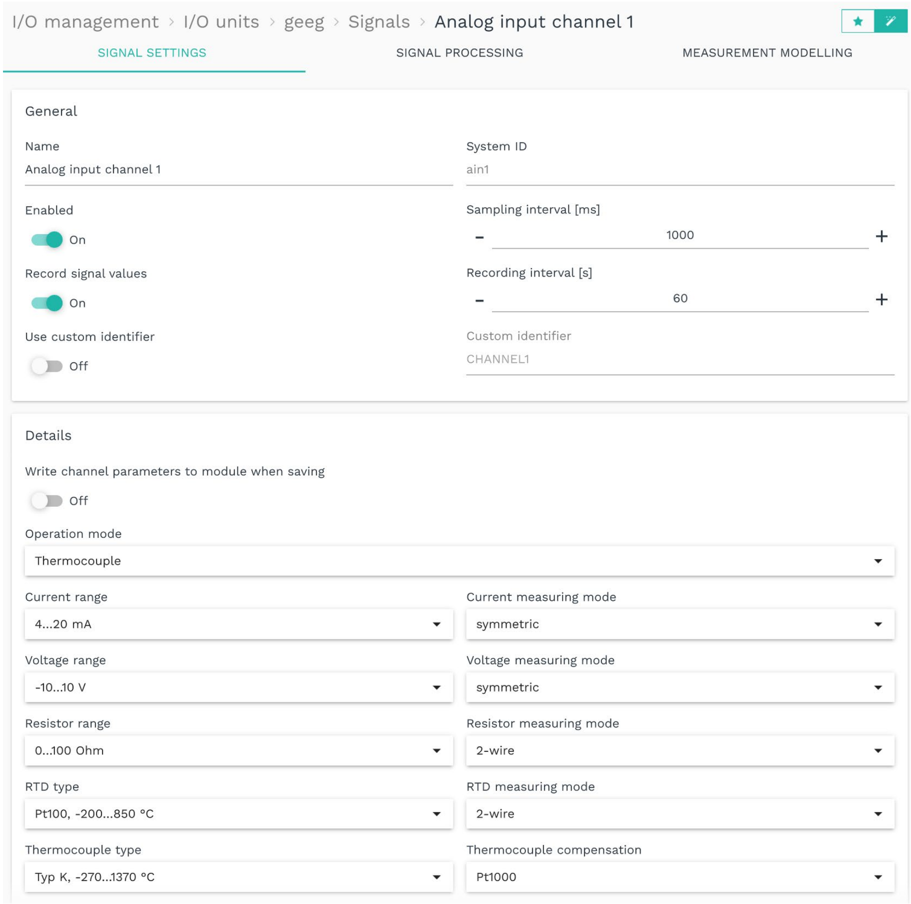

I/O management › I/O units › TBEN-S2-4AI › Signals

□	Identifier	Name	Group	Type	Value
□	CHANNEL1	Channel 1		INT16	0
□	CHANNEL2	Channel 2		INT16	0
□	CHANNEL3	Channel 3		INT16	0
□	CHANNEL4	Channel 4		INT16	0

Fig. 77: Signals for the TBEN-S2-4AI module

10. Select the signal you want to configure.

    A window opens, where you will find three tabs.


I/O management › I/O units › geeg › Signals › Analog input channel 1
SIGNAL SETTINGS
SIGNAL PROCESSING
MEASUREMENT MODELLING

General

Name: Analog input channel 1

System ID: ain1

Enabled: On

Sampling interval [ms]: 1000

Record signal values: On

Recording interval [s]: 60

Use custom identifier: Off

Custom identifier: CHANNEL1

Details

Write channel parameters to module when saving: Off

Operation mode: Thermocouple

Current range: 4...20 mA

Current measuring mode: symmetric

Voltage range: -10...10 V

Voltage measuring mode: symmetric

Resistor range: 0...100 Ohm

Resistor measuring mode: 2-wire

RTD type: Pt100, -200...850 °C

RTD measuring mode: 2-wire

Thermocouple type: Typ K, -270...1370 °C

Thermocouple compensation: Pt1000

Fig. 78: “Signal settings” tab for the TBEN-S2-4AI module in “Advanced” viewing mode

11. In the **Signal settings** tab, activate and configure the signal.
    - Enter the name of the signal.
    - Set the slider to **On**.
    - In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).
    - Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
    - Enter the desired time interval for the recording in the **Recording interval** field (in seconds).
12. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.
13. The **Details** area displays the parameters that are read in by the connected TBEN-S2-4AI module.

    NOTE: Only make changes if you are sure that they will not damage the module.

    By activating the **Write channel parameters to module when saving** slider, you confirm that the settings read in and possibly changed are correct and should really be written back to the module. The changes only become effective if you click **Save** afterwards.

14. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.

15. Click **Save**.

16. In the **Measurement modelling** tab, you define how the measured values are to be displayed.

    For more information, see Configuring measurement modelling, page 81.

17. Finally, click **Save & close**.

5.2.12 Adding a S7-PLC-Client

Adding an S7 PLC client is mandatory if you want to connect the device to a Siemens S7 controller.

1. On the home page of **I/O management,** select **I/O units.**

2. Click **Add I/O unit**.

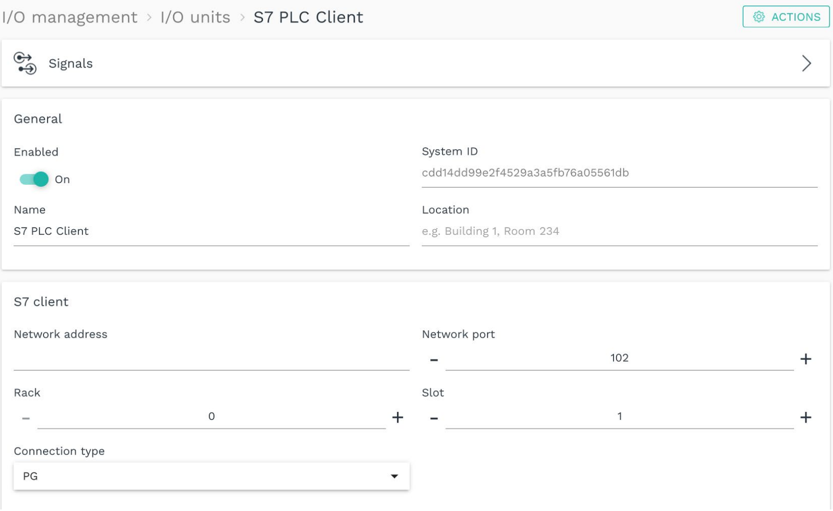
3. Select **S7- PLC Client** as the type.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.

4. Enter the **Name** for the I/O unit.

5. Click **Finish** to add the I/O unit.

   A page opens, where you can now make the settings for the unit.



General

Enabled: On

System ID: cdd14dd99e2f4529a3a5fb76a05561db

Name: S7 PLC Client

Location: e.g. Building 1, Room 234

S7 client

Network address:

Network port: 102

Rack: 0

Slot: 1

Connection type: PG

Fig. 79: Device settings for the S7 PLC client

The new I/O unit is automatically enabled. If you only want to use it later, set the **Enabled** slider to **Off**.

6. Optional: Enter the **Location**.

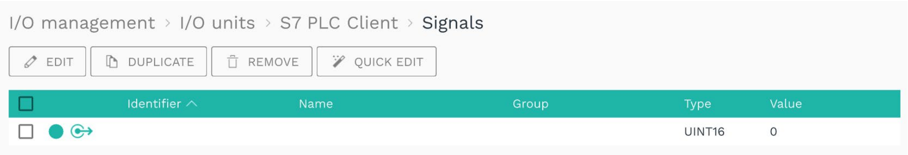
7. You can make the following settings in the **S7 client** area:

   - **Network address**: Enter the host name or IP address of the SIEMENS controller with which a connection is to be established.
   - **Network port**: Enter the port under which the Siemens S7 controller can be reached. Generally, the default value "102" does not need to be changed.

- **Rack** and **Slot**: Specify the position of the CPU module in the control unit. Depending on the control unit model, the CPU module may also be located in slot "0" or "2".
- **Connection type**: Select the mode with which the connection is to be established. The default value **PG** (programming device) only needs to be changed to **OP** (operating mode for HMI panels) or S7-**Basic** (fall-back) in exceptional cases.

8. Click **Save**.
9. Select **Signals**.

   The signals for all analog input channels are already applied.

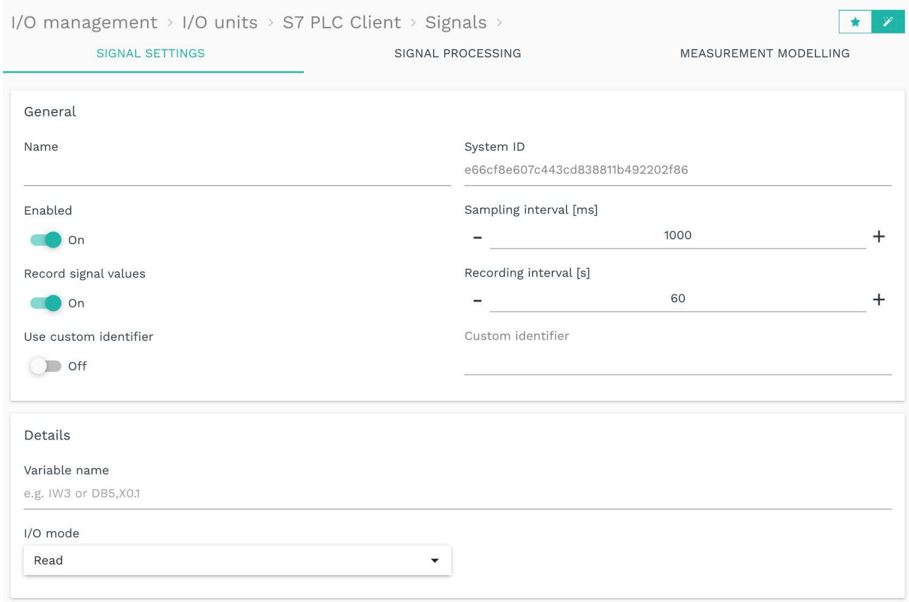


□	Identifier	Name	Group	Type	Value
□	●			UINT16	0

Fig. 80: Initially, no signals are predefined for the S7 PLC client

10. Click **Add I/O signal**.

    A window opens, where you will find three tabs.



General

Name:

System ID: e66cf8e607c443cd838811b492202f86

Enabled: On

Sampling interval [ms]: 1000

Record signal values: On

Recording interval [s]: 60

Use custom identifier: Off

Custom identifier:

Details

Variable name: e.g. IW3 or DB5,X0.1

I/O mode: Read

Fig. 81: “Signal settings” tab for the S7 PLC client in “Advanced” viewing mode

11. In the **Signal settings** tab, activate and configure the signal.
    - Enter the name of the signal.
    - Set the **Enabled** slider to **On**.
    - In the **Sampling interval** field, specify the intervals at which the signal is to be sampled (in milliseconds).

      NOTE: If you have selected the **I/O mode** "Write", no sampling takes place, and the sampling interval is ignored
    - Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.

  - Enter the desired time interval for the recording in the **Recording interval** field (in seconds).

12. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.
    - **Custom identifier**: Enter your own identifier name.

13. Enter further parameters in the **Details** area:
    - **Variable name**: The S7 variable name encodes which address is to be accessed with which data type in which area of the S7. There are different variable areas: Data block, digital inputs and outputs or memory or flags. You can find information on this in the PLC manufacturer's interface description or variable list.

      If you have problems with the connection to the S7 PLC, please also note the following information: https://flows.nodered.org/node/node-red-contrib-s7#variable-addressing.
    - **I/O mode**: Select whether a data value/date is to be read from the control unit (**Read**) or written to the control unit (**Write**).

14. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.

15. Click **Save**.

16. In the **Measurement modelling** tab, you define how the measured values are to be displayed.

    For more information, see Configuring measurement modelling, page 81.

17. Finally, click **Save & close**.

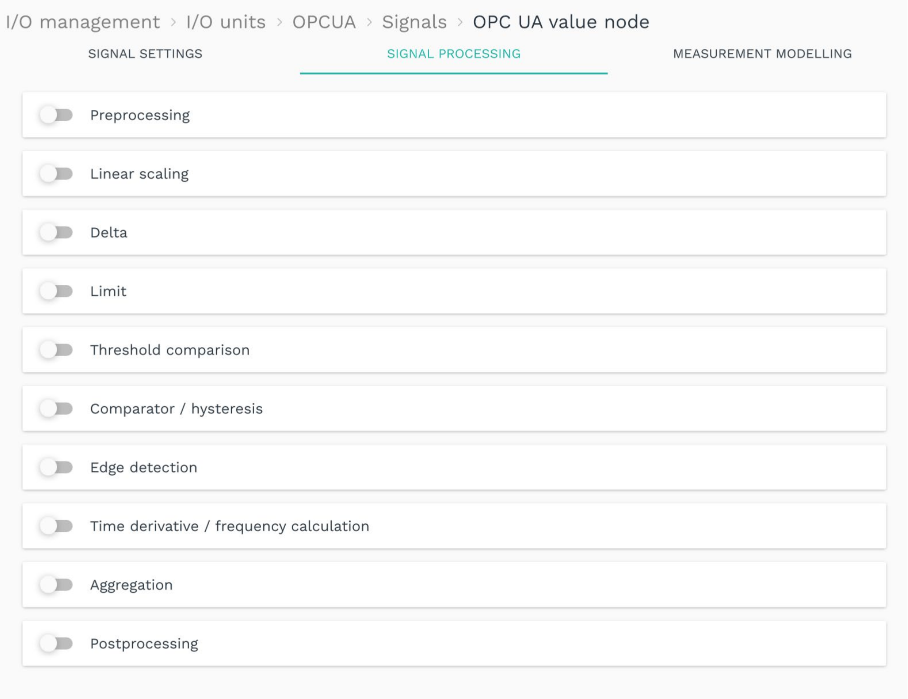
5.2.13 Configuring signal-processing steps

> **HINWEIS:** SIINEOS uses the expr-eval library as of version 2.7.4. This provides the following mathematical functions:
>
> https://github.com/in-hub/expr-eval#expression-syntax
>
> This can lead to incorrect results or signal processing steps that do not function properly for signals that have already been configured. Therefore, check the mathematical functions of your existing signal processing steps.

For all I/O units and interfaces, the steps with which signal values can be processed can be selected on the **Signal processing** tab.

The processing functions are processed by SIINEOS in the order in which they appear on the tab, so if you have activated **Preprocessing** and **Threshold comparison**, preprocessing is calculated first, and the threshold comparison is then carried out with this value.

The signal-processing steps are optional. You do not have to process your signal values: you can have them output unprocessed if this is sufficient.



I/O management › I/O units › OPCUA › Signals › OPC UA value node

Fig. 82: “Signal processing” tab

1. Use the slider to activate the required step of the signal processing.

   The input area opens.

   The following processing functions are available:

Preprocessing	With this function, the signal value can be preprocessed via a mathematical expression. The signal value is available in the variable “x” and can be combined with any arithmetic operators (+ – * / % **) and constants. For example, a fixed value (offset) can be subtracted or added. SIINEOS uses the expr-eval library for the calculation. With this, the following mathematical functions can now be applied: https://github.com/in-hub/expr-eval#expression-syntax Examples of mathematical expressions: x - 2 (x - 4) * 0.7 sin(x * PI / 180) max(x, 10) abs(x)
Linear scaling	This function applies a simple linear function to the input value. While it is basically also possible to create a linear function using the parameters (slope/coefficient and constant) given in the previous function as a mathematical expression (e.g. x * 5 + 7), this function allows the simple input of 2 input and output values. These values are often known from the data sheets especially for analog sensors.

	Example: A temperature sensor can have a value range of -20 °C to +80 °C at a 4 … 20 mA interface. In this case, the value **4** would be entered at **X1** and the value **20** at **X2,** as well as the value **-20** at **Y1** and the value **80** at **Y2.**
Delta	The function compares the current signal value with the previously measured signal value. You have several options via the drop-down list how the delta should be calculated: • Absolute difference to the previous value • Relative changes to the previous value • Relative changes to the previous value in %. • If the value changes from a numeric value that is considered positive to a numeric value that is considered negative (or vice versa), -1 (or +1) is output. This can be used to detect anomalies, for example.
Limit	The function sets lower and upper limits for the signal value downwards and/or upwards, i.e., if the signal is falling below the minimum value, the gateway supplies this minimum value as the signal value. If the signal value is above the maximum value, this value is used as the signal value.
Threshold comparison	The function converts the signal value into a logical 0 or 1 value, depending on how the signal value relates to the threshold value. Example: If the **Signal is above** mode is selected and a threshold value of **10** is set, the output of the device is 1 as long as the signal value is greater than 10. If it falls below, the output is 0.
Comparator/ hysteresis	The function compares the input value with a lower and upper threshold value and delivers the associated output value depending on the result. With this behavior, a two-point control or hysteresis is achieved. In addition, the course over time can be included by setting the minimum undercut and minimum overshoot duration to a value greater than 0 ms. For the output signal to assume the upper output value, the input signal must be continuously above the upper threshold for a certain number of milliseconds. Similarly, the output signal is only reset to the lower output value if the value has fallen below the lower threshold value for longer than x milliseconds.
Edge detection	If (especially digital) signals are to be used for counting, the rising and/or falling edges can be counted. A counter is then used as the output value, which increases each time the input signal changes from 0 to 1 (rising edge) or from 1 to 0 (falling edge). Analog signals can also be converted into digital signals using upstream functions such as threshold value comparison, e.g.,

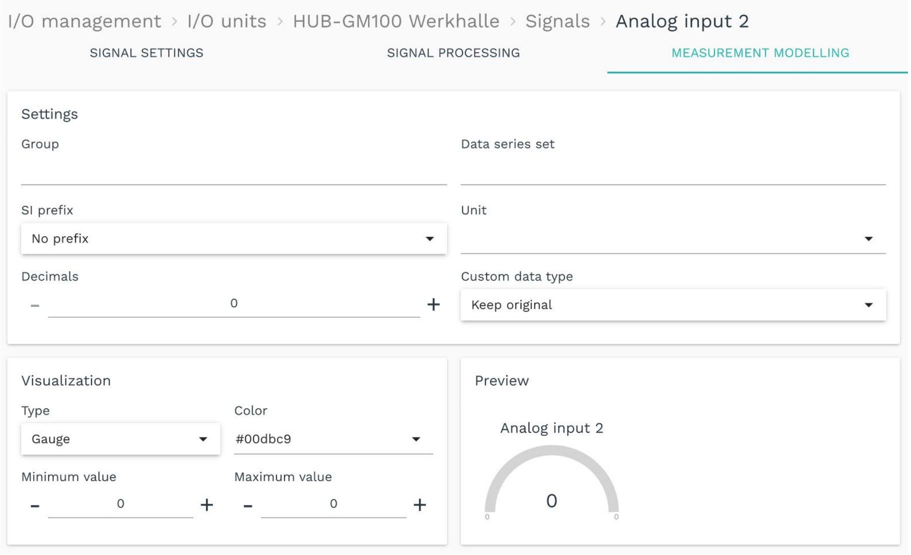
	by using the value 1 (rising edge) as input for edge detection when a threshold value is exceeded and thus automatically using the value 0 as input when the value falls below the threshold value.
Time derivative / frequency calculation	This function determines the number of changes from 0 to non-0 (e.g. to 1 or any other level). As the result, it delivers not the original signal value, but the number per unit time or the frequency. This can, for example, be used to create a piece counter, so that the signal processing no longer delivers the digital input, but the number of parts produced per second/minute/hour. Ideally, this function is combined with an averaging directly afterwards, because otherwise the value can fluctuate wildly, especially at the beginning.
Aggregation	If several signal values are to be combined in time, the **Aggregation** function can be activated. Here, either a specific value (e.g. the largest or smallest), the sum of all values, or the average value is determined and output based on the values received over a specific duration (aggregation interval). You can also specify whether the aggregated value should be calculated every time it is sampled (continuously) or only periodically at the end of the aggregation interval (periodically).
Postprocessing	After the input signal has been processed by one or more functions, it can be post-processed analogously to the preprocessing function, so the accuracy can be adjusted by rounding or similar, for example. The format and syntax of the mathematical expression correspond to those of the **Preprocessing** function.

2. Fill in the input fields of the signal-processing steps you want to apply.
3. Click **Save** and continue to the **Measurement modelling** tab.

5.2.14 Configuring measurement modelling

For all I/O units and interfaces, the same parameters can be configured on the **Measurement modelling** tab to display measured values.

NOTE: This configuration is optional, but you can only display your data in the **FlexPlorer** app if this tab is filled in. For example, you should enter the number of decimal places, because otherwise measured values always appear without decimal places by default, and therefore also in the apps that transfer the values to the cloud or write them to Grafana.



I/O management › I/O units › HUB-GM100 Werkhalle › Signals › Analog input 2

SIGNAL SETTINGS | SIGNAL PROCESSING | MEASUREMENT MODELLING

Settings

Group:

Data series set:

SI prefix: No prefix

Unit:

Decimals: 0

Custom data type: Keep original

Visualization

Type: Gauge

Color: #00dbc9

Minimum value: 0

Maximum value: 0

Preview

Analog input 2

0

Fig. 83: “Measurement modelling” tab

1. Select the following parameters as required or enter the appropriate values:

Group	If a name is entered, this only affects the view in the FlexPlorer app. For all interfaces with the same group name, the preview views (sensibly of the same type, e.g., gauge) are lined up side by side in FlexPlorer, so that measured values from various devices/sensors can be compared.
Data series set	All signals with the same data series set are displayed in FlexPlorer in a common diagram under Live Diagrams, so that the signal values from various devices/sensors can be compared directly in live operation.
SI prefix	Depending on the value range of the signal, it may be useful to select a suitable SI prefix for the unit, e.g., giga, mega, kilo, etc.
Unit	Select the physical unit that the value should be given.
Decimals	Enter the number of decimal places to be displayed.

Custom data type	Select a data type and overwrite the original data type of a signal. This is useful, for example, when calculating a float value from a Modbus UINT16 register or a digital input with a truth value (Boolean).
Minimum value	Enter the value to be used as minimum in the visualization element (e.g. a gauge). This can be the smallest measurable value of the connected device, but it does not have to be.
Maximum value	Enter the value to be used as the maximum in the visualization element (e.g. a gauge). This can be the largest measurable value of the connected device, but it does not have to be.
Type	Select the type of visualization that best fits the output values. **Gauge**, **counter**, **LED** or **no visualization** are available.
Color	Select a color for the display of the measured values.

2. Click **Save & close** to finish the input.

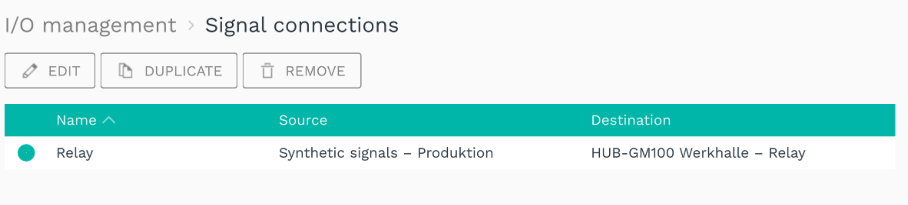
5.3 Configuring signal connections

If you want to control and write output signals depending on input signals, you can configure and use signal connections.

With signal connections, you can trigger actions that control the switching of an alarm by a relay, for example, or you can forward sensor values to a Modbus-connected controller.

> **NOTE**: In the signal connections setup wizard, readable input signals to the I/O units are displayed only if they have been activated with the slider in **Signal settings**.

1. On the **I/O management** page, select the **Signal connections** function.



	Name ^	Source	Destination
●	Relay	Synthetic signals – Produktion	HUB-GM100 Werkhalle – Relay

Fig. 84: Examples for signal connections (initially, no synthetic signals are predefined)

2. To create a new signal connection, click **Add signal connection**.

   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.

3. Enter the **Connection name.**

   The connection is automatically enabled. If you want to disable it temporarily or permanently, you can deactivate the connection.

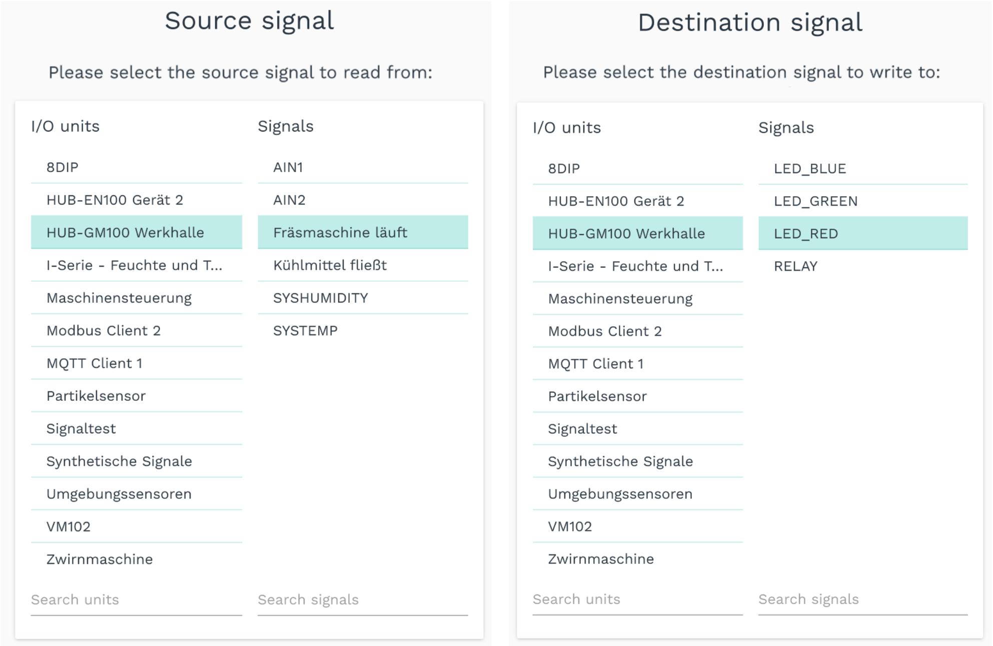
4. Under **Source signal**, select the I/O unit and the associated signal to be read from, e.g., a particle sensor.

5. Under **Signal processing**, you can optionally process or modify the just-selected source signal before it is written to the destination signal, e.g., 0 and 1 in case of a threshold exceedance.

   NOTE: The source signal itself is not changed: this step refers exclusively to the calculation of the target signal. The signal processing of the source signal, as you know it from the I/O units, still takes place independently.

6. Under **Destination signal**, you select the I/O unit and the associated signal to which the value is forwarded. This can be e.g., the HUB-GM100 with a relay that signals a stop to the machine when a threshold value is exceeded.

The signal connection could now look like this, for example:



Source signal

Please select the source signal to read from:

I/O units

- 8DIP
- HUB-EN100 Gerät 2
- HUB-GM100 Werkhalle
- I-Serie - Feuchte und T...
- Maschinensteuerung
- Modbus Client 2
- MQTT Client 1
- Partikelsensor
- Signaltest
- Synthetische Signale
- Umgebungssensoren
- VM102
- Zwirnmaschine

Search units

Signals

- AIN1
- AIN2
- Fräsmaschine läuft
- Kühlmittel fließt
- SYSHUMIDITY
- SYSTEMP

Search signals

Destination signal

Please select the destination signal to write to:

I/O units

- 8DIP
- HUB-EN100 Gerät 2
- HUB-GM100 Werkhalle
- I-Serie - Feuchte und T...
- Maschinensteuerung
- Modbus Client 2
- MQTT Client 1
- Partikelsensor
- Signaltest
- Synthetische Signale
- Umgebungssensoren
- VM102
- Zwirnmaschine

Search units

Signals

- LED_BLUE
- LED_GREEN
- LED_RED
- RELAY

Search signals

Fig. 85: I/O management > Signal connections > Edit signal connection (example)
Example: The milling machine is connected to the digital input (DIO1) of the HUB-GM100. The red LED of the HUB-GM100 is to light up when a threshold value is exceeded. Enter this threshold value directly after the source signal (see step 5).

7. Where there are extensive entries, you can search for units or signals by entering at least one digit or letter in the search field below the selection lists.
8. When you have finished typing, click **Save & close**.

5.4 Creating synthetic signals

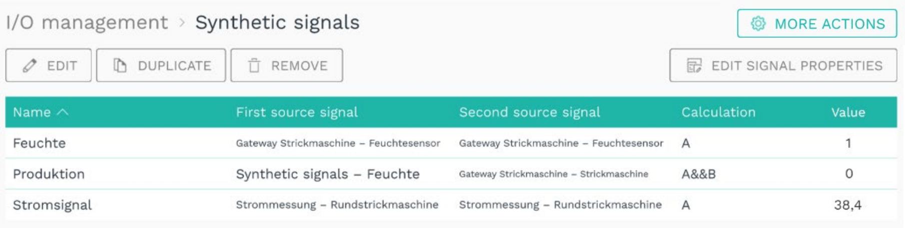
With this function you can logically link signals from sensors or from bus protocols, for example, and thus create new signals. This is particularly useful in combination with software applications that can evaluate machine statuses, such as MADOW.

Case study 1: You can, for example, link two signals—“milling machine running” (signal 1) and “coolant flowing” (signal 2)—with each other using “AND”, and define that a machine is only recognized as running if signal 1 AND signal 2 are true/active/set or have the logical value 1. A standstill is thus detected as soon as one of the two signals no longer has the logical value 1.

Case study 2: With logical/binary signals, an alarm can be triggered as soon as at least one of 2 measured values from a particle sensor for different particle sizes is above a limit value.

NOTE: In the signal connections setup wizard, readable input signals to the I/O units are only displayed if they have been activated with the slider in the signal settings.

1. On the **I/O management** page, select the **Synthetic signals** function.



Name	First source signal	Second source signal	Calculation	Value
Feuchte	Gateway Strickmaschine – Feuchtesensor	Gateway Strickmaschine – Feuchtesensor	A	1
Produktion	Synthetic signals – Feuchte	Gateway Strickmaschine – Strickmaschine	A&&B	0
Stromsignal	Strommessung – Rundstrickmaschine	Strommessung – Rundstrickmaschine	A	38,4

Fig. 86: Example of synthetic signals (initially, no synthetic signals are predefined)

2. To create a new signal, click **Add synthetic signal**.

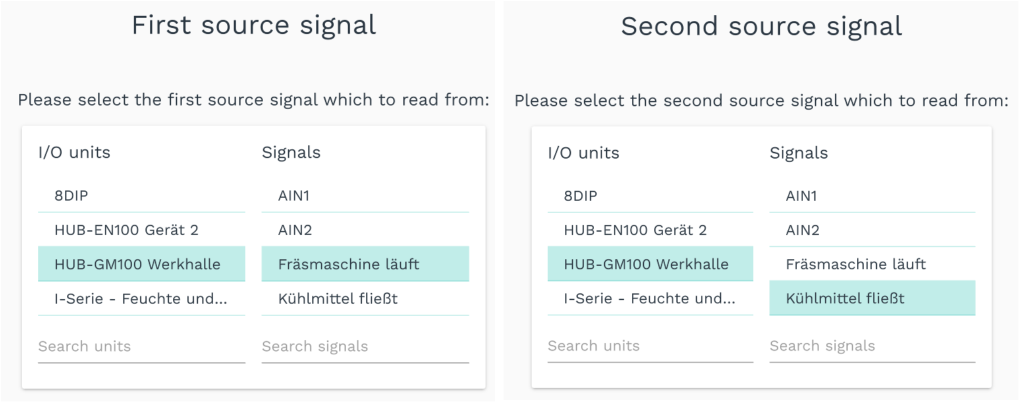
   The setup wizard opens to guide you through the creation process. In the following, confirm each entry either with **Next** or by pressing **Enter**.

3. Enter the **Signal name.**

4. Under **First source signal,** select the I/O unit and the first signal to be read from, e.g., the digital input DIO1 (“Milling machine running”).

5. Under **Second source signal**, select the I/O unit and the second signal to be read from, e.g., digital input DIO2 (“Coolant flowing”).

   The synthetic signal could now look like the following, for example:



First source signal

Please select the first source signal which to read from:

I/O units	Signals
8DIP	AIN1
HUB-EN100 Gerät 2	AIN2
HUB-GM100 Werkhalle	Fräsmaschine läuft
I-Serie - Feuchte und...	Kühlmittel fließt

Second source signal

Please select the second source signal which to read from:

I/O units	Signals
8DIP	AIN1
HUB-EN100 Gerät 2	AIN2
HUB-GM100 Werkhalle	Fräsmaschine läuft
I-Serie - Feuchte und...	Kühlmittel fließt

Fig. 87: I/O management > Synthetic signals > Edit synthetic signal (example)
Example: If the signal value of digital input 1 (DIO1) detects that the “milling machine is running” and the signal value of digital input 2 (DIO2) detects that the “coolant is flowing”, then the synthetic signal added here is generated, which outputs a machine state (however is is defined).

6. Where there are extensive entries, you can search for units or signals by entering at least one digit or letter in the search field below the selection lists.

7. Now select one of the mathematical operations or logics to be used to calculate the synthetic signal from the two source signals.

   - **Sum up values**: The values of both source signals are added together.
   - **Subtract values**: The values of both source signals are subtracted.
   - **Multiplicate values**: The values of both source signals are multiplied.
   - **Divide values**: The values of both source signals are divided.
   - **Logical AND operation**: Combines both source signals with an “AND”, i.e., both signal values must be non-0 for the synthetic signal also to have the logical value 1.

- **Logical OR operation**: Links both source signals with an “OR”, i.e., at least one signal value must be non-0 for the synthetic signal also to have the logical value 1.
- **RS flip-flop**: You can use this function to model an RS flip-flop in which the output is controlled by the signals S (set) and R (reset). The signal S sets the output to 1 until the output is reset to 0 via the signal R.

  The two inputs S (set) and R (reset) correspond to the first and second source signals. If a source signal has a value greater than 0, it is interpreted as a logical 1, i.e. the flip-flop is set or reset.

  During the setup process, the RS flip-flop can be reset to the value 0 at any time using the **Reset** button.
- **Infinite counter**: Increases by the difference between the previous and current value of the source signal. The counter value is retained even when the device is restarted and can be reset to 0 with the Reset button in the signal overview if required.

  HINT: As the second source signal is ignored, it makes sense to select the same signal as the first source signal.
- **Resettable counter**: Works like the endless counter with the difference that the second signal resets the counter if this value is not equal to 0. The counter value is retained even if the device is restarted and can be reset to 0 using the Reset button in the signal overview if required.

  HINT: The counter values are saved in the background every 10 seconds.
- **Custom mathematical or logical expression**: Enter a mathematical formula according to the syntax of the expr-eval library (https://github.com/oat-sa/expr-eval#expression-syntax) to calculate the value of the synthetic signal from the source signals 1 and 2.

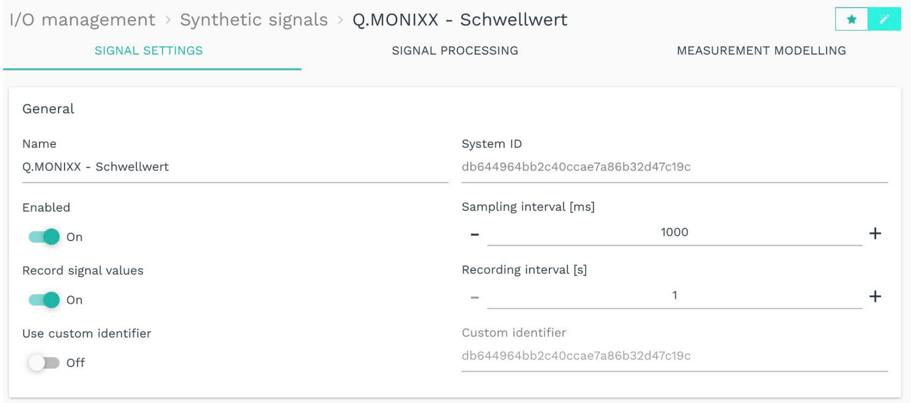
  Examples of inputs:

A >= 1 or B >= 2	Result = 1, if A ≥ 1 OR B ≥ 2; otherwise, result = 0
A > 0.5 and B < 10	Result = 1, if A > 0.5 AND B < 10; otherwise, result = 0
max(A, B)	The larger of the two signals is the result
A^B	Result = A to the B-th power

8. When you have finished typing, click **Finish**.
9. To save all signals in one file (e.g. to reuse them on another device) or if you want to transfer synthetic signals from another device to the present one, click **Actions** and select the corresponding menu item.
10. To reset dynamic features such as endless counters or RS flip-flop, which are retained even when the device is restarted, to 0, click on the **Reset** button. This is useful, for example, after setting up and testing a synthetic signal.

11. You can deactivate, make settings, process and model the synthetic signal in the same way as all other signals. To do this, select the signal and click on **Edit signal properties** or double-click on the signal.

    A window opens in which you will find three tabs.



I/O management › Synthetic signals › Q.MONIXX - Schwellwert

SIGNAL SETTINGS | SIGNAL PROCESSING | MEASUREMENT MODELLING

General

Name: Q.MONIXX - Schwellwert

System ID: db644964bb2c40ccae7a86b32d47c19c

Enabled: On

Sampling interval [ms]: 1000

Record signal values: On

Recording interval [s]: 1

Use custom identifier: Off

Custom identifier: db644964bb2c40ccae7a86b32d47c19c

Fig. 88: “Signal settings” tab for the selected synthetic signal in “Advanced” viewing mode

12. In the **Signal settings** tab, activate and configure the signal.
    - Optional: Change the name of the signal if necessary.
    - Optional: Set the slider to **Off** if you do not want to use the signal at this time.
    - In the **Sampling Interval** field, specify the intervals at which calculations are to be made from the source signals (in milliseconds).

      RECOMMENDATION: The synthetic signal is not automatically recalculated as soon as one of the source signals changes, but only as often as specified by the sampling interval. We recommend choosing a very short sampling interval (e.g., set it to the minimum of 50 ms), so that the synthetic signal is updated with only very little delay.
    - Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
    - Enter the desired time interval for the recording in the **Recording interval** field (in seconds).
13. Two additional settings are available in the **Advanced** viewing mode:
    - **Use custom identifier**: Set the slider to **On** if you want to enter your own identifier name.

      Custom identifier: Enter your own identifier name.
14. In the **Signal processing** tab, you can define how the signal value should be processed.

    For more information, see Configuring signal-processing steps, page 75.
15. Click **Save**.
16. In the **Measurement modelling** tab, you define how the measured values are to be displayed.

    For more information, see Configuring measurement modelling, page 81.
17. Finally, click **Save & close**.

6 Managing the apps

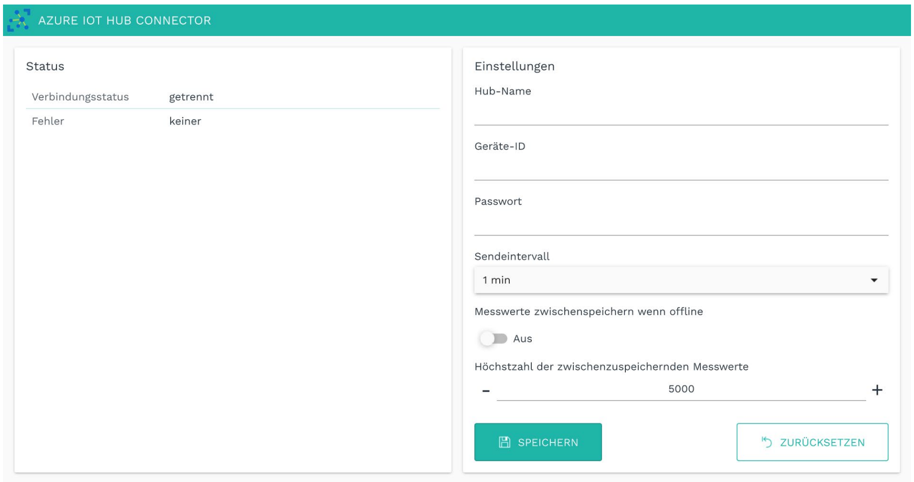
The following chapter provides you with an overview of the apps pre-installed in SIINEOS and how you can manage and configure them.

6.1 Azure IoT Hub Connector

With the **Azure IoT Hub Connector** app, you can establish a communication channel between an IoT device (e.g. the HUB-GM200) and the Microsoft IoT platform.

You must have previously purchased access to Microsoft's IoT platform from Microsoft. in.hub only establishes the connection with which you can send data directly to Azure.

To configure the **Azure IoT Hub Connector,** you have the following input fields available:



AZURE IOT HUB CONNECTOR

Status

Verbindungsstatus	getrennt
Fehler	keiner

Einstellungen

Hub-Name

Geräte-ID

Passwort

Sendeintervall: 1 min

Messwerte zwischenspeichern wenn offline: Aus

Höchstzahl der zwischenzuspeichernden Messwerte: 5000

Fig. 89: Settings for the "Azure IoT Hub Connector" app

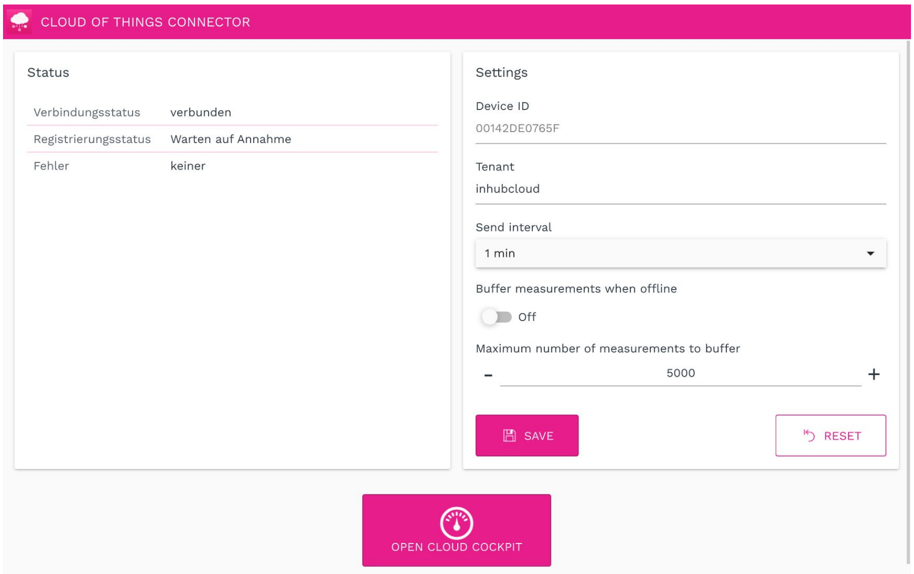
1. Enter the following details and then click **Save.**

Hub name	Enter the name of the device whose data you want to send to the Azure IoT platform.
Device ID	Enter the device ID of the device whose data you want to send to the Azure IoT platform. You can find this ID in your Azure IoT Hub administration interface.
password	Enter the password. You can find the password in your Azure IoT Hub administration interface.
Transmission interval	From the drop-down list, select the time interval at which the data should be sent from the IoT device to Azure.
Cache measured values when offline	Switch the slider to **On** if you want the data to be saved as soon as the gateway is offline and you temporarily have no Internet access to the device (e.g. due to a mobile phone fault or network maintenance work).
Maximum number of measured values to be buffered	Specify the maximum number of measured values to be stored temporarily.

6.2 Cloud of Things Connector

With the **Cloud of Things Connector** app, you can establish a communication channel between an IoT device (e.g. the HUB-GM200) and the Telekom IoT platform.

You must have previously purchased access to the IoT platform from Deutsche Telekom. in.hub only establishes the connection with which you can send data directly to the Telekom cloud.



Status

Verbindungsstatus	verbunden
Registrierungsstatus	Warten auf Annahme
Fehler	keiner

Settings

Device ID
00142DE0765F

Tenant
inhubcloud

Send interval
1 min

Buffer measurements when offline
Off

Maximum number of measurements to buffer
5000

Fig. 90: Overview in the Cloud of Things Connector

1. In the **Status** area, you can view the following information about the status of the connection to the Telekom Cloud:

Connection status	Connection status between the app and the Telekom Cloud
Registration status	Status of registration in the Telekom Cloud
Error	If a connection error occurs, the reason is displayed in this field

2. The following input fields are available in the **Settings** area to configure the **Cloud of Things Connector**:

Device ID	Display of the device ID
Tenant	Enter the name of the (logical) unit under which all associated users and data are summarized and managed. If you have purchased cloud access via in.hub, you must enter the company account, in this case "inhubcloud". This field is pre-filled by default. If you want to use your own Telekom Cloud, you can also enter your own company account in this field.
Send interval	Select the time interval at which data is to be sent from SIINEOS to the Telekom Cloud.

Buffer measurements when offline	Switch the slider to **On** if the measured values are to be saved temporarily when the connection is interrupted.
Maximum number of measurements to buffer	Enter the maximum number of measured values to be stored temporarily.

3. Click **Save**.
4. Click **Open Cloud Cockpit.**

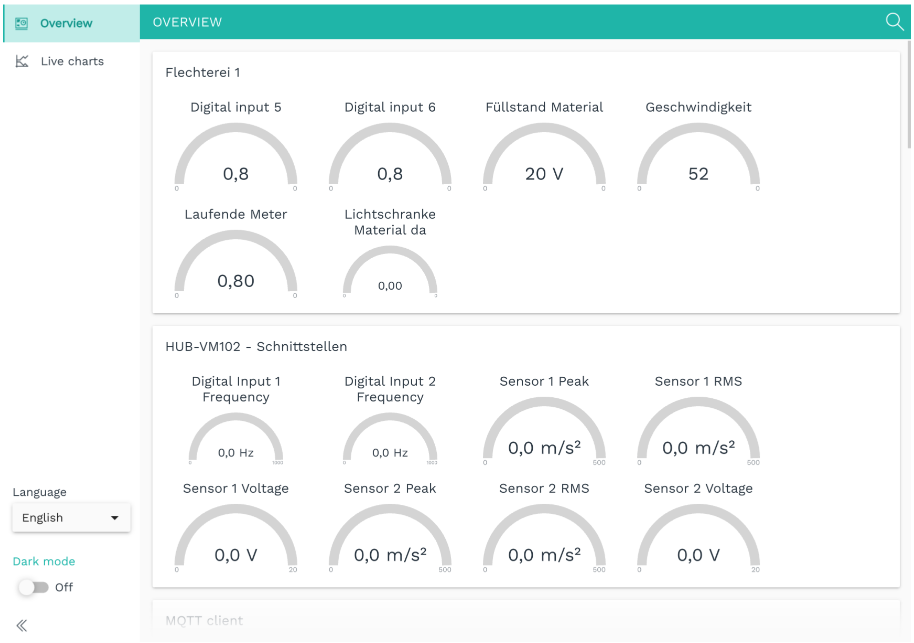
   The Telekom Cloud opens, where you can log in with your individual user data.

6.3 FlexPlorer

The **FlexPlorer** app is in.hub's own visualization tool that displays the data that arrives and is processed in SIINEOS in dashboards. FlexPlorer is not as extensively configurable as Grafana but provides a good initial overview of all active signals from the devices connected to the gateway. You do not need an additional user account for FlexPlorer.

You can switch between two views in FlexPlorer: **Overview** and **Live charts**.

On the **Overview** page, you can see the information from the measured value modeling for each activated I/O unit with the configured signals in a graphical representation:



Language: English

Dark mode: Off

Fig. 91: Overview in FlexPlorer

You can monitor the measured value progression live on the **Live charts** page:

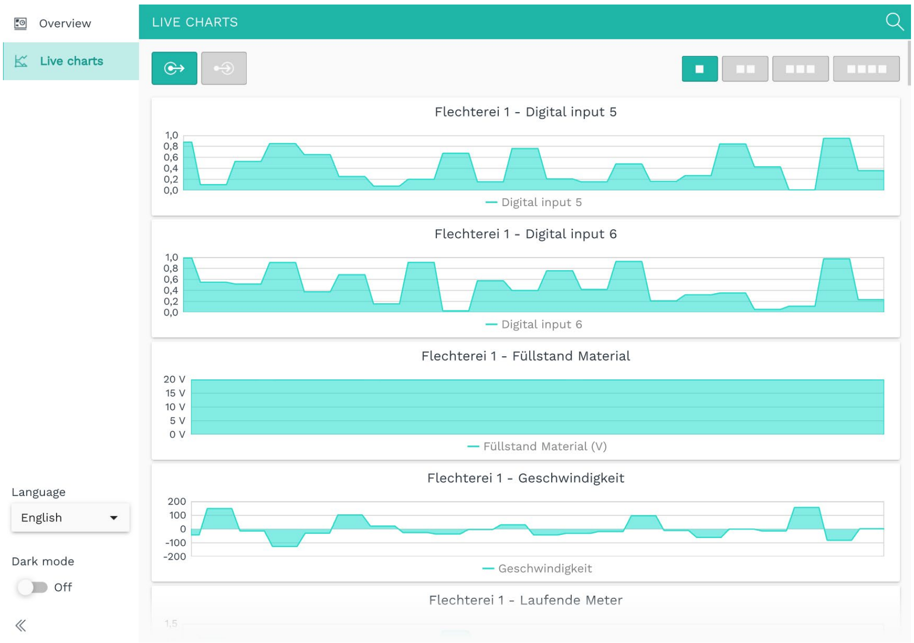


Fig. 92: Live diagrams in FlexPlorer

You can customize the view of the live diagrams using various buttons:

- Specify whether the live diagrams should be displayed in a 1, 2, 3 or 4 column layout.
- Select whether only readable, only writable or all signals should be displayed.

6.4 InGraf

The **InGraf** app integrates the cross-platform open-source application **Grafana** and provides access to visualize and display data from all I/O units and signals from SIINEOS.

Grafana accesses two databases: **VictoriaMetrics** and **Prometheus**. As of the current version, VictoriaMetrics runs in the background by default.

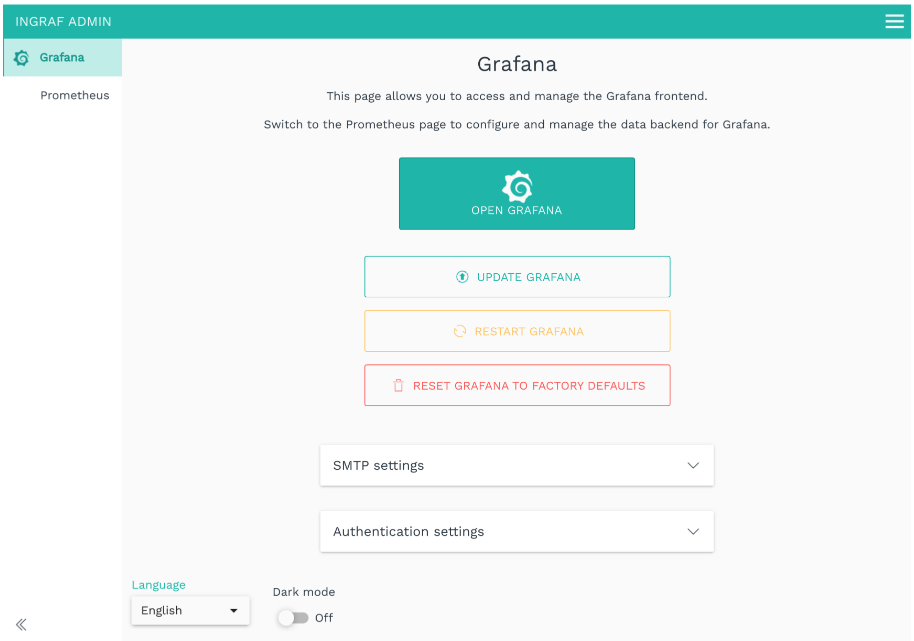
If you update to SIINEOS 2.8.0., nothing will change for you: your data will be saved both in VictoriaMetrics and in Prometheus. For performance reasons, however, we recommend transferring the data from Prometheus and deactivating Prometheus.

If you set up a new device with SIINEOS version 2.8.0, your data will only be saved with VictoriaMetrics.

In addition to managing the app, you can also configure and manage the Prometheus database in the **InGraf** app.

> **NOTE ON USER ADMINISTRATION:**
>
> To manage the **InGraf** app, a separate user role, the application administrator, is created with the initial user data **ingrafadmin/ingrafadmin**.
>
> See also chapter User management, page 33.
>
> The initial user data **admin/admin** is defined for access to Grafana**.** Log in and then change the access data.

Configure Grafana connection



Grafana

This page allows you to access and manage the Grafana frontend.

Switch to the Prometheus page to configure and manage the data backend for Grafana.

Fig. 93: Settings for the Grafana front end

1. Use the following buttons as required:

Open Grafana	Click the button to open Grafana in a new window. Have your user data ready and log in.
Update Grafana	Click the button if you want to update your Grafana version to the latest version. Your dashboards remain in place.
Restart Grafana	If Grafana does not respond or react, restart the program.
Reset Grafana to factory defaults	Click the button if you want to reset all your settings in Grafana. This also means that individually created dashboards are lost.

2. To activate alarms, you must first configure the SMTP mail server. You have the following input fields for this:

SMTP activated	Set the slider to **On** if you want Grafana to send via your SMTP server. Grafana cannot send e-mails without SMTP server configuration, so that e.g. the alerting function cannot be used.
SMTP server	Enter the name of your mail server.
SMTP port	Enter the port of your mail server.
SMTP user	In order for Grafana to log on to your SMTP server, the data of an e-mail account is required. Ask your system administrator for the access data that Grafana should use to send e-mails.
SMTP password	

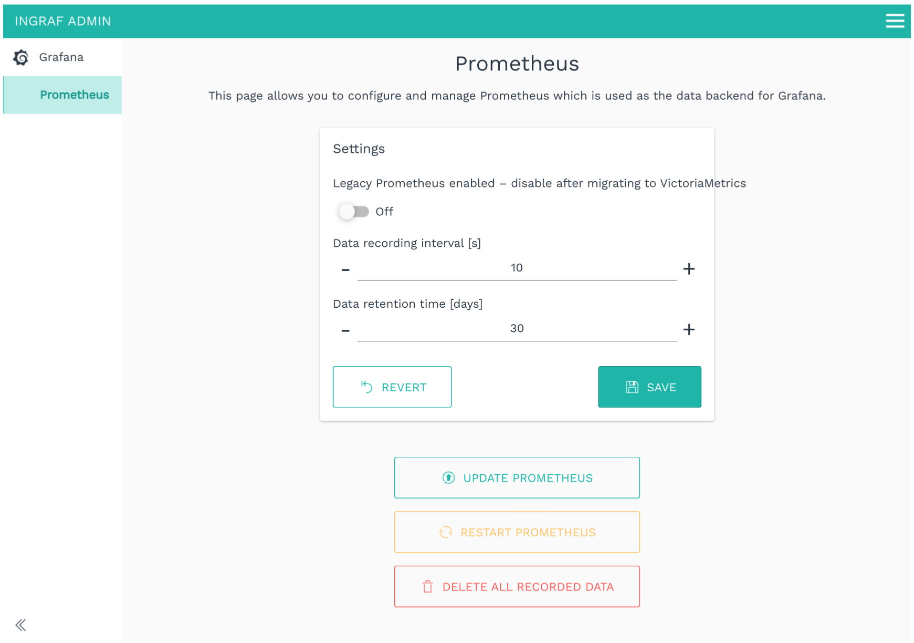
Sender address	Enter an e-mail address that will appear as the sender in the e-mails e-mails that Grafana sends. You configure the target addresses individually in Grafana, as different recipients are also possible for different alarms, for example.
Sender name	Enter a name under which Grafana should appear as the sender in your mailbox.

3. You can make the authentication settings for Grafana with the following settings:

Allow anonymous access	Set the slider to **On** if dashboards should also be visible in Grafana without prior login.
User role for anonymous access	In the drop-down list, you can select which Grafana user role is used for anonymous access. **Viewer**, **Editor** and **Administrator** are available.

4. Click **Save**.

Configuring the Prometheus database



Prometheus

This page allows you to configure and manage Prometheus which is used as the data backend for Grafana.

Settings

Legacy Prometheus enabled – disable after migrating to VictoriaMetrics

Off

Data recording interval [s]

10

Data retention time [days]

30

Fig. 94: Settings for the Grafana backend with the Prometheus database

1. Use the following input fields to configure the connection between SIINEOS and the Prometheus database:

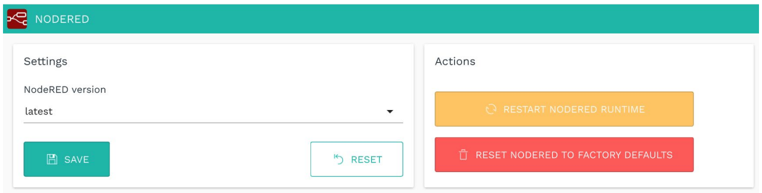
Legacy Prometheus enabled - disable after migrating to VictoriaMetrics	If you have migrated your data to VictoriaMetrics after the SIINEOS update, we recommend setting the slider to Off to improve performance and save system resources.
Data recording interval [s]	Enter a time period in seconds after which the data should be recorded.
Data retention time [days]	Enter the number of days the data will be kept before it is deleted.

2. Use the following buttons as required:

Update Prometheus	Click the button if you want to update the version of Prometheus to the latest version. Your data is retained.
Restart Prometheus	If Grafana does not provide/display valid data or e.g. an empty list appears during signal selection, you must restart Prometheus.
Delete all recorded data	Click the button if you want to delete all the data saved in the database.

6.5 NodeRED

With the **NodeRED** open source application, you can connect hardware, software, interfaces and services with each other via graphical programming using the modular principle. When this app is activated, the NodeRED Docker container is downloaded and executed. All further activities are your responsibility.



NODERED

Settings

NodeRED version: latest

Fig. 95: Settings for the "NodeRed" app

1. In the **Settings** area, select the NodeRED version you want to use.

   If there is an Internet connection, the set version is automatically downloaded and used.

   If you are working offline with the gateway, you can download the latest version of NodeRED from the in.hub download portal at https://download.inhub.de/docker/ and install it in **SIINEOS > System > Updates.** Select **latest** from the list.

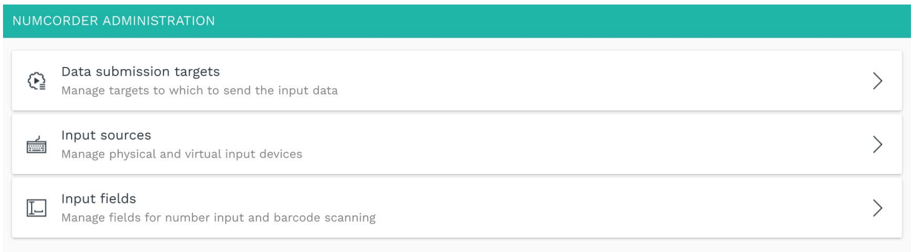
2. You can perform the following actions in the **Actions** area:

Restart the NodeRed runtime	If a message appears when you open the **NodeRED** app stating that the page cannot be reached, you must restart the app.
Reset NodeRed to factory defaults	Everything that you have set up, programmed or installed in **NodeRED** yourself is reset with this button.

6.7 NumCorder

You can use the **NumCorder** app to scan barcodes or enter serial numbers. This allows you to make any type of entry and freely configure input fields.

If you click on the **Manage app** button, you have the following options for configuring the NumCorder:



NUMCORDER ADMINISTRATION

Data submission targets
Manage targets to which to send the input data

Input sources
Manage physical and virtual input devices

Input fields
Manage fields for number input and barcode scanning

Fig. 96: Administration for the “NumCorder” app

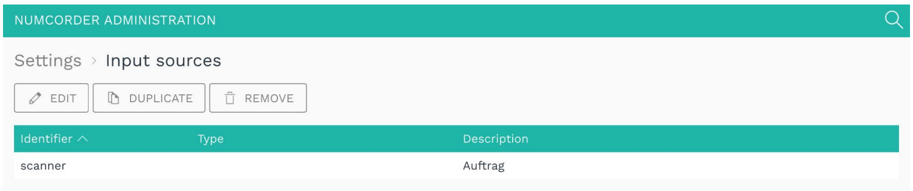
Manage data submission targets

1. Activate the data transmission destination in which your input is to be saved via NumCorder and configure the associated parameters:

Built-in VictoriaMetrics database	Set the **Save field values as labels** slider to **On** if not only numbers but also input values containing letters and special characters are to be saved. The field value is then not stored in the metric value itself, but in the label of the metric.
HTTP API	Enter the **API endpoint URL** to which the data is to be sent. Select the **HTTP method** to be used to send the data from the drop-down list. In the **Data format** drop-down list, you can also specify the format of the data transmission - as a **JSON object** or as **comma-separated values**.
MQTT	Enter all connection details such as the **MQTT broker address** and the **MQTT broker port**, **Username** and P**assword** to send the NumCorder data via the MQTT protocol. You can encrypt this **connection via TLS** (organization CA must be uploaded). Communication via **WebSockets** can also be activated if the broker only allows WebSocket connections. To do this, set the respective slider to **On**. In the **Data format** drop-down menu, you can also specify the format of the data transmission - as a JSON object in a topic or as field values in a subtopic. Set the **Publish retained messages** slider to **On** if you want the broker to send the last value published via this topic to all new clients. In the **Topic name** field, enter the topic name under which the data is to be published.

Manage input sources

Here you can configure the physical and/or virtual input devices that can be used to capture input.



Identifier	Type	Description
scanner		Auftrag

Fig. 97: Create and manage input sources

1. Click on **Add input source**.

   The setup wizard opens to guide you through the creation process. Confirm each entry with **Next** or press **Enter**.

2. Enter the **Identifier** (name) of the input source, e.g. "barcode scanner".

   Only lower case is allowed without spaces and special characters.

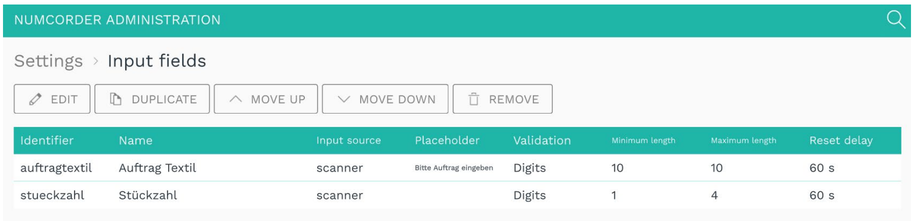
3. Select the **Type** of input source.

   You can choose from the preconfigured input sources.

4. Optional: Enter a **Description** for the input device.

5. Click on **Finish**.

Manage input fields



Identifier	Name	Input source	Placeholder	Validation	Minimum length	Maximum length	Reset delay
auftragtextil	Auftrag Textil	scanner	Bitte Auftrag eingeben	Digits	10	10	60 s
stueckzahl	Stückzahl	scanner		Digits	1	4	60 s

Fig. 98: Create and manage input fields

1. Click on **Add input field**.

   The setup wizard opens to guide you through the creation process. Confirm each entry with **Next** or press **Enter**.

2. Enter the **Identifier** (name) of the input field, e.g. "delivery bill".

   Only lower case is allowed without spaces and special characters.

3. Enter the **Name** that is displayed next to the input field.

4. Select the **Input source** from the drop-down list.

   The input sources that you have created yourself are displayed.

5. Optional: Enter a **Placeholder** text that will be displayed in the input field if it is empty.

6. Under **Input validation,** you can specify which characters should be allowed for input.

7. Set the **Minimum input length** of the characters.

   By default, 10 characters are entered.

8. Set the **Maximum input length** of the characters.

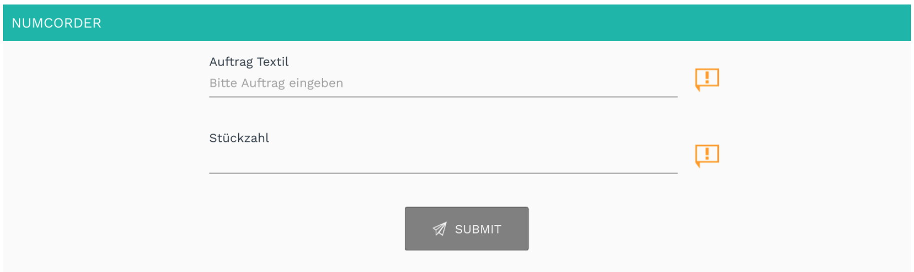
   By default, 10 characters are entered.

9. Under **Reset delay**, you can specify when the input field is automatically cleared again after inactivity and you have to restart the input.

   The default setting is 60 seconds.

10. Click on **Finish**.

    As soon as you open the **NumCorder** app, the defined input field appears.



Auftrag Textil
Bitte Auftrag eingeben

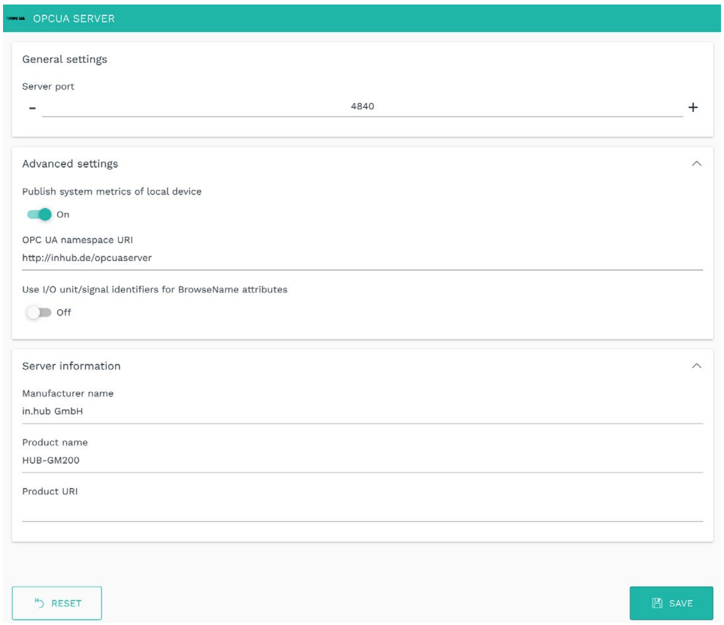
Stückzahl

Fig. 99: Input fields (example)

6.8 OPC UA Server

With the **OPC UA Server** app, you can implement the platform independent OPC UA standard and make the data of all I/O units and I/O signals available to the outside world via the standardized OPC UA interface.

If, for example, you want to connect two in.hub gateways with each other via OPC UA, you can activate the **OPC UA Server** app on one device (so that this device acts as a server) and set up the OPC UA client on the other device.



General settings

Server port
4840

Advanced settings

Publish system metrics of local device
On

OPC UA namespace URI
http://inhub.de/opcuaserver

Use I/O unit/signal identifiers for BrowseName attributes
Off

Server information

Manufacturer name
in.hub GmbH

Product name
HUB-GM200

Product URI

Fig. 100: Settings for the "OPCUA Server" app (example)

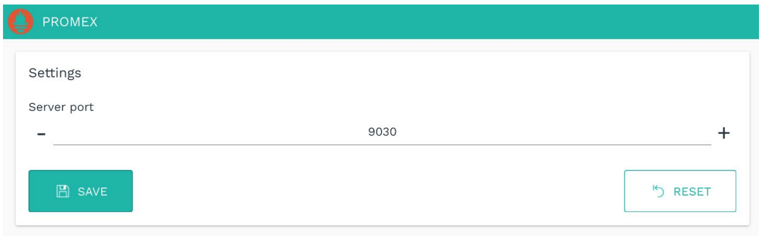
The following input fields are available for configuring the OPC UA server:

General settings	Enter the **Server port** on which the OPC UA server should be accessible.
Advanced settings	• Set the **Publish system metrics of the local device** slider to **On** to publish the system metrics CPU load, CPU usage, memory usage and data storage usage/utilization via OPC/UA in addition to the I/O units. This makes it easy to monitor the gateway remotely. • Enter the **OPC UA namespace URI** that identifies the data schema for this OPC UA server. • Set the **Use I/O unit/signal identifiers for BrowserName attributes** slider to **On** (recommended) to use the respective OPC UA node ID string instead of the configured names of I/O units and I/O signals for the respective browse name attribute of the OPC UA object. The node ID string is a unique identifier that represents the path to the OPC UA node, e.g. "s=GM200Werkhalle.AIN1".
Server information	Enter additional information about the server, such as **Manufacturer name**, **Product name**, and **Product URI**.

6.9 PromEx

The **PromEx** app provides an HTTP interface, a so-called Prometheus Exporter, which can be used to retrieve the current values of all I/O signals from an external Prometheus database.
I/O signals can be retrieved.

When you open the administration of the app, you can only enter the port via which the HTTP interface can communicate with the Prometheus database and vice versa.



PROMEX

Settings

Server port: 9030

Fig. 101: Settings for the “PromEx” app (example)

6.10 TOSIBOX® Lock for Container

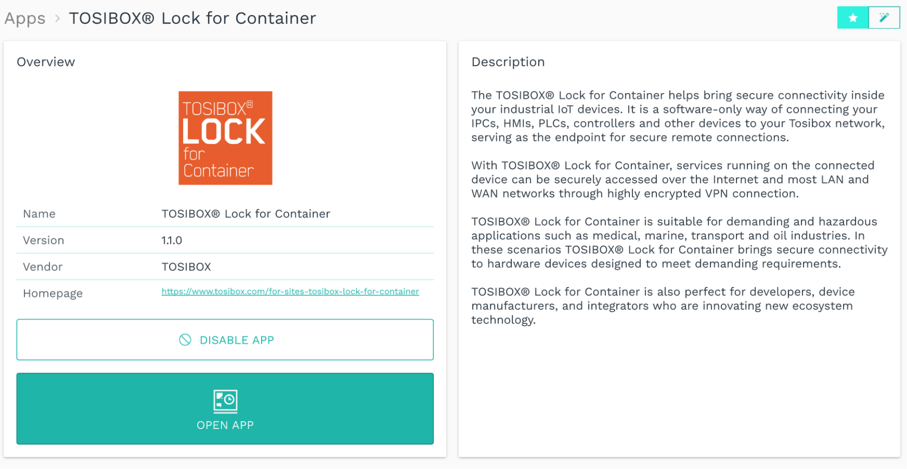
TOSIBOX® Lock for Container provides secure connections within your industrial IoT devices. It is a software-only solution that allows you to connect your IPCs, HMIs, PLCs, controllers and other devices to your Tosibox® network and serves as an endpoint for secure remote connections.

With TOSIBOX® Lock for Container, services running on the connected device can be securely accessed over the Internet and most LAN and WAN networks via a highly encrypted VPN connection. The app does not limit the number of services or devices that can be managed. You can connect any service via any protocol between any devices.

NOTE:

No administration is required for the **TOSIBOX® Lock for Container** app. You can open the app directly, but you will need the access data you received with the software. After you have activated the app, please restart the device.

If connection problems occur after deactivating and reactivating the app, you should restart the device so that all services and settings work correctly.



Apps › TOSIBOX® Lock for Container

Overview

Name	TOSIBOX® Lock for Container
Version	1.1.0
Vendor	TOSIBOX
Homepage	https://www.tosibox.com/for-sites-tosibox-lock-for-container

Description

The TOSIBOX® Lock for Container helps bring secure connectivity inside your industrial IoT devices. It is a software-only way of connecting your IPCs, HMIs, PLCs, controllers and other devices to your Tosibox network, serving as the endpoint for secure remote connections.

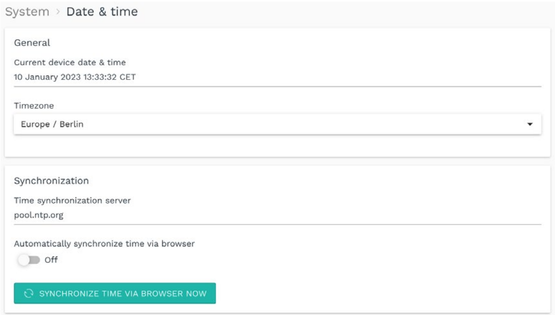
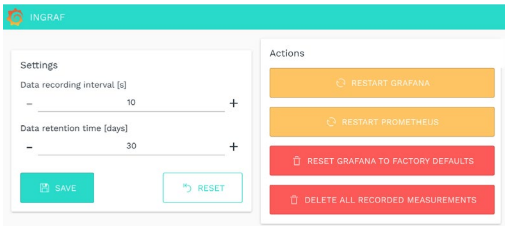
With TOSIBOX® Lock for Container, services running on the connected device can be securely accessed over the Internet and most LAN and WAN networks through highly encrypted VPN connection.

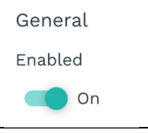
TOSIBOX® Lock for Container is suitable for demanding and hazardous applications such as medical, marine, transport and oil industries. In these scenarios TOSIBOX® Lock for Container brings secure connectivity to hardware devices designed to meet demanding requirements.

TOSIBOX® Lock for Container is also perfect for developers, device manufacturers, and integrators who are innovating new ecosystem technology.

Fig. 102: Settings for the “TOSIBOX® Lock for Container” app

7 Troubleshooting

Problem	Possible cause	Remedy
Grafana Data is not arriving in the app. Visualization is not possible.	In SIINEOS, the time has not been synchronized with the browser. -or- The gateway was briefly without power, and the time setting was lost.	1. In SIINEOS, select the **System** page and go to the **Date & time** section.  System › Date & time General Current device date & time: 10 January 2023 13:33:32 CET Timezone: Europe / Berlin Synchronization Time synchronization server: pool.ntp.org Automatically synchronize time via browser: Off 2. Click **Synchronize time via browser now** to synchronize the date settings for the gateway with your computer. If the gateway power supply is cut off, this setting is lost. You will then have to resynchronize with the browser.
	The database has broken down due to the loss of voltage during writing.	1. In SIINEOS, select the **Apps** page and open the **InGraf** app. 2. Click **Manage app**.  INGRAF Settings Data recording interval [s]: 10 Data retention time [days]: 30 Actions SAVE RESET RESTART GRAFANA RESTART PROMETHEUS RESET GRAFANA TO FACTORY DEFAULTS DELETE ALL RECORDED MEASUREMENTS 3. Click the **Delete all recorded measurements** action to completely reset the database.
The gateway no longer responds, e.g. during the update process. The gateway cannot be put into operation even by switching it off and on (disconnect power supply and reconnect).	–	Disconnect and connect the gateway from/with the power supply three times in a row. The LEDs on the front panel must have lit up for at least 5 seconds between the three processes. After 3 unsuccessful boot attempts, the device switches to another boot slot and boots with the usually older version installed in this boot slot. 4. All settings are retained.

Problem	Possible cause	Remedy
Signal connections Required I/O unit or signal is not displayed	The I/O unit or signal has not been activated.	1. In SIINEOS, select the **I/O management** page and open the I/O unit or signal you are looking for. 2. In the device settings for the I/O unit or in the signal settings for the signal, set the slider to **On**.  General Enabled On
Update You have uploaded a SIINEOS update, and the new software version is not displayed.	Browser cache still contains an old version of the web interface. -or- Gateway is no longer responding.	1. First, clear your browser cache and refresh the page in your browser. 2. If this does not work: Switch off the power to the gateway and switch it on again after a few seconds. Then restart SIINEOS and check the version number on the **Overview** page.
Connection problems An error message occurs when trying to open the address http://192.168.123.1/smac	A proxy server is specified for this IP address in the SIINEOS network settings. -or- The firewall of the local PC (Windows firewall) or the firewall of the company network prevents access to the gateway or parts of the interface.	1. First check if the gateway is plugged in via USB cable and flashing. 2. In the proxy server settings for the system or the browser, you or your administrator must make sure that no proxy server is used for the IP address 192.168.123.1, so that the browser accesses the connected gateway directly. Either temporarily disable the use of the proxy server or add an appropriate exception rule for the above IP address.
Upload of the license file fails	The system time of your device is not synchronized with the current time.	3. In SIINEOS, navigate to **System > Date & time** und select your correct time zone. 4. Click **Save**.

Problem	Possible cause	Remedy
Connection problems You can no longer reach the gateway on the network, or a system service is not responding.	A firewall rule in SIINEOS is preventing traffic to and from the gateway.	1. Go to the **Firewall** page and check which action is selected in the rules for both incoming and outgoing network traffic. 2. Select the **Accept packet** action to allow the data exchange.
Connection problems The gateway is located in an isolated machine network and you cannot reach it in this network.	If the network is secured by its own firewall, the ports for communication with the gateway may not be enabled.	Make sure that the following ports are enabled in your local system firewall settings to access the gateway: • HTTP port: 80 • HTTPS port: 443 • SIINEOS system bus (MQTT): 1988
Connection problems An add-on module is connected to the network via Ethernet and you cannot reach it on the network.	You have assigned the device an IP address that lies in the range between 192.168.123.**1** and 192.168.123.**254**. This network address range is already used for the direct USB connection.	Assign a new IP address that is outside the range already assigned.
Network problems / Connection problems The gateway is connected to the network via Ethernet and you cannot reach it on the network.	The gateway has been configured automatically or manually with an IP address that is in the range **172.17.0.0/16** and **172.18.0.0/16**. This address range is used by default by the Docker service for the Docker networks.	Configure an IP address from a different IP address range for the Docker service. To do this, enter an IP address including subnet prefix from a non-used IP address range under **System > Services > Docker Engine > IP address of the Docker bridge**.
Signals from the Modbus RTU device do not arrive. The Modbus RTU device is connected, but signals are not arriving at the gateway.	The pins of the RS485 socket of the gateway and the corresponding pins on the Modbus RTU device are not connected correctly.	Check the RS485 socket on the in.hub gateway to ensure that: • + is connected to bus line A • - is connected to bus line B **NOTE**: In some cases, manufacturers A and B have different names. Therefore, compare the signs of the bus cable in the manufacturer's data sheet with our connections and swap the pairing if necessary.

Problem	Possible cause	Remedy
App does not have access to the Internet You can no longer open or restart an app.	Docker-based apps are temporarily unable to connect to the Internet after changes in firewall rules.	Restart the gateway. The firewall is reconfigured in interaction with the Docker service.
The results of the signal processing are 0 or incorrect. You have entered mathematical expressions in the **Signal Processing** tab that cannot be evaluated by the expr-eval library without errors.	Since SIINEOS version 2.7.4, mathematical expressions are calculated with an improved method for signal processing as well as for user-defined calculations of synthetic signals. Instead of internal functions with ECMAScript syntax, the more powerful expr-eval library is used. Existing formulas may have to be adapted with it.	Navigate to the **Signal Processing** tab and rearrange your mathematical formulas according to the specifications of the expr-eval library: https://github.com/in-hub/expr-eval#expression-syntax

8 Further information

8.1 OPTIONAL: Programming your own software applications (apps)

NOTE: in.hub provides the building blocks for programming your own app, the programming itself is carried out by the customer's own software developer.

1. On your PC, go to the in.hub download section at https://download.inhub.de/ and select **InCore downloads > InCore SDK installer** to download the software development kit (In.Core Framework).
2. To install and set up the software development kit and some necessary applications, please follow the instructions at https://download.inhub.de/incore/ **> InCore install guide.**
3. Once installation and setup are complete, you can program the user software according to your in-house requirements.

   Please refer to the developer documentation. It provides user-ready software blocks to quickly build the IoT/IIoT application: https://incore.readthedocs.io/en/latest/
4. Store the finished software bundle locally on your PC in `*.raucb` format.
5. Upload the software application to SIINEOS.

in.hub GmbH
Technologie-Campus 1
DE-09126 Chemnitz

+49 371 335 655 00
info@inhub.de