



SIINEOS 2.9.4

User Manual

Document version 1.0 | Publication date:
29. August 2025

Table of Contents

Legal information	4
1. General information	6
1.1. Scope of delivery	6
1.2. Other applicable documents	6
1.3. Network security	6
2. General product information	7
2.1. Software architecture	7
3. Setting up the working environment with SIINEOS	8
3.1. Preparing the IT infrastructure in your own company network	8
3.2. Logging on to SIINEOS	8
3.2.1. When logging on to SIINEOS for the first time	9
3.2.2. If you have already set up SIINEOS	9
3.3. Setting the colour mode and language	10
3.4. Viewing mode: Standard and Advanced	10
3.5. Configuring the system	11
3.5.1. Installing SIINEOS updates	11
3.5.2. Installing app updates	12
3.5.3. Configuring device settings	13
3.5.4. Locating the gateway in the control cabinet	14
3.5.5. Setting the date and time	14
3.5.6. Optional: Calibrating the HUB-MRT100/HUB-RT100	15
3.5.7. Configuring system services	15
3.5.8. Optional: Configuring TLS certificates	17
3.5.9. Setting up mail servers for notifications	17
3.6. Restarting the gateway, shutting down and logging out	19
3.7. Configuring networks	20
3.7.1. Setting up Ethernet 1 and Ethernet 2	20
3.7.2. Setting up Wi-Fi	23
3.7.3. Setting up a mobile connection	24
3.7.4. Setting up OpenVPN	25
3.8. Configuring the firewall	26
3.8.1. Sharing Internet connections	27
3.8.2. Controlling incoming traffic	28
3.8.3. Controlling outgoing traffic	29
3.8.4. Defining and editing rules for IP forwarding	30
3.8.5. Configuring port forwarding	31
3.9. User administration	32
3.9.1. Managing user accounts	33
3.10. Creating and configuring alert signals, destinations and rules	34
3.10.1. Creating alert signals	35
3.10.2. Managing alert destinations	36
3.10.3. Adding an alert rule	38
3.11. Monitoring the system	40
3.11.1. Storage maintenance	42
3.12. Opening and managing apps	43
3.13. Managing licences	44
3.13.1. Requesting a voucher and activating a software licence	44

3.13.2. Adding a licence file to SIINEOS	46
4. I/O management	48
4.1. Working with I/O management	49
4.1.1. Filtering I/O units and reading information	49
4.1.2. Using the “Actions” menu	50
4.1.3. Sorting lists and reading information	51
4.1.4. Editing, duplicating or removing list entries	52
4.1.5. Searching for entries	54
4.2. Creating I/O units	54
4.2.1. Adding a HUB-GM100	55
4.2.2. Adding a HUB-GM200	57
4.2.3. Adding a HUB-EN100 module for energy monitoring	60
4.2.4. Establishing communication with the HUB-VM102 via a network	61
4.2.5. Adding a Sensirion SPS30 particle sensor	64
4.2.6. Adding a Modbus client of the RTU type	66
4.2.7. Adding a Modbus client of the TCP type	70
4.2.8. Adding an MQTT client	72
4.2.9. Adding an OPC UA client	76
4.2.10. Adding a TBEN-S1-8DIP module	79
4.2.11. Adding a TBEN-S2-4AI module	81
4.2.12. Adding an S7 PLC client	84
4.2.13. Adding a ControlPlex® CPC12 bus controller	86
4.3. Signal processing	89
4.3.1. Signal processing functions	90
4.3.2. Configuring the signal processing steps	92
4.4. Measurement modelling	93
4.5. Configuring signal connections	95
4.6. Creating synthetic signals	97
4.7. Configure I/O endpoints	100
4.7.1. Modbus server	100
4.8. Export time series database	102
5. Managing apps	105
5.1. Azure IoT Hub Connector	105
5.2. Cloud of Things Connector	106
5.3. FlexPlover	107
5.4. InGraf	108
5.4.1. Configuring the Grafana connection	109
5.5. NodeRED	111
5.6. NumCorder	111
5.6.1. Configuring data submission targets	112
5.6.2. Configuring input sources	113
5.6.3. Creating input fields	113
5.7. OPC UA Server	114
5.8. SIGNAL4	116
5.9. PromEx	117
5.10. TOSIBOX® Lock for Container	117
6. Troubleshooting	119

Legal information

Safety information

This documentation contains information that you must observe for your personal safety and to prevent material damage. Read the safety information carefully and always keep this documentation within easy reach.

The safety information is presented in descending order of hazard level as follows:

**DANGER**

Indicates an immediate hazard to humans. Failure to comply will lead to irreversible injuries or death.

**WARNING**

Indicates an identifiable hazard to humans. Failure to comply may lead to irreversible injuries or death.

**CAUTION**

Indicates an identifiable hazard to humans or potential material damage. Failure to comply may lead to reversible injuries or material damage.

**ATTENTION**

This gives you information that may lead to material damage if not complied with.

**NOTE**

A note gives you useful information on specific actions and issues.

**TIP**

A tip gives you tips, tricks or recommendations from in.hub that have proven to be helpful in handling the products.

Qualified personnel

The product associated with this documentation may only be handled by personnel qualified for the respective task. The device may only be installed, commissioned and operated in compliance with the associated documentation and the safety information contained therein.

Based on their training and experience, qualified personnel are able to recognize risks and avoid potential hazards when handling these products.

Knowledge of PCs, operating systems and web applications is a prerequisite. General knowledge in the field of automation technology is recommended.

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, set-up, assembly, installation, commissioning, operation and maintenance are essential for the correct and safe operation of the products.

The permissible ambient conditions must be complied with. Instructions in the associated documentation must be followed.

Brands

All designations marked with the “®” symbol are registered trademarks. The other designations in this document may be trademarks whose use by third parties for their own purposes may infringe the rights of the owner.

Disclaimer

in.hub accepts no liability for product malfunctions resulting from improper handling, mechanical damage, incorrect application and improper use.

The contents of this document have been checked for conformity with the product described. However, deviations cannot be ruled out, so that we cannot guarantee complete conformity. The information in this publication is regularly reviewed. Necessary corrections are included in subsequent editions.

1. General information

This document contains all the information you need to commission and use the device/software.

The document is intended for service technicians, system administrators and installers who connect the product with other units, configure it and commission it.

1.1. Scope of delivery

1 × SIINEOS

1× User Manual as a PDF

1.2. Other applicable documents

In addition to this document, please observe the following documents. You can find these in the in.hub download portal at <https://download.inhub.de/>:

- Operating Instructions for the gateway or module on which SIINEOS is installed

1.3. Network security

Please bear in mind that the product does not communicate in encrypted form within the internal network. Therefore, protect your network from unauthorized access from outside! Any integration into a network with Internet access must be undertaken with great caution. It is imperative to speak with your system administrator in advance.

2. General product information

SIINEOS is a Linux-based operating system and IoT platform that is specifically tailored to meet the high requirements for data security and continuity of operations 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 enables simple data acquisition, data preprocessing and data connection to third-party systems, making it easier to get started and reducing the complexity of IoT and digitalization projects.

Comprehensive documentation on SIINEOS and a user-friendly software development kit (SDK) help you realise all the possibilities of our industrial gateways quickly and efficiently. Regular software updates continually ensure that the system is always up to date.

2.1. Software architecture

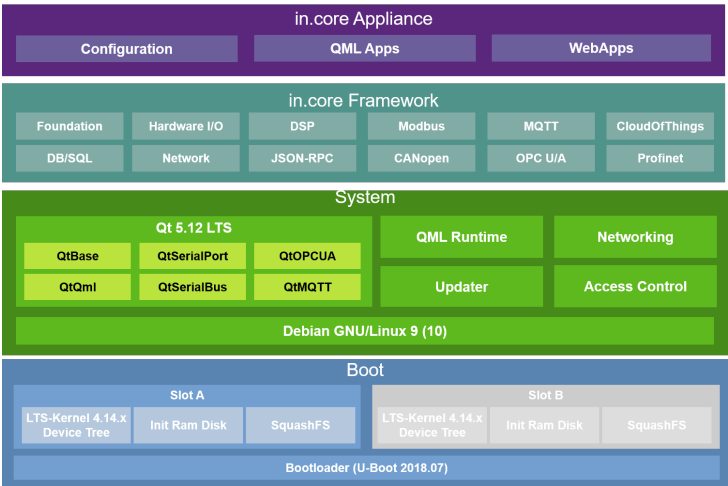
SIINEOS comprises four levels:

- Boot level
- System level
- In.Core framework

This is a collection of software modules that can be used to quickly create both simple and complex IoT and Industrial Internet of Things (IIoT) applications.

- Application level with the In.Core apps

These consist of generic and higher-level objects and can be easily configured and combined using QML (Qt Modelling Language). Each InCore module can be imported individually and contains the actual function objects.



SIINEOS software architecture

3. Setting up the working environment with SIINEOS

This chapter gives you detailed step-by-step instructions for configuring SIINEOS and setting up your working environment.

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

You can also download all the latest technical documents, software packages, tutorials and installation instructions from the in.hub download portal: <https://download.inhub.de/>

3.1. Preparing the IT infrastructure in your own company network

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

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

TCP ports	Access to device services and apps
502	Modbus TCP I/O endpoint
1880	Node-RED app
1883	MQTT broker If no direct access to the MQTT broker is required (System > Services > MQTT broker is deactivated), you do not need to unlock this port.
3000	If the in.hub device is to be accessed via the InGraf (Grafana) app
4840	If the in.hub device is to be accessed via the OPC UA Server app

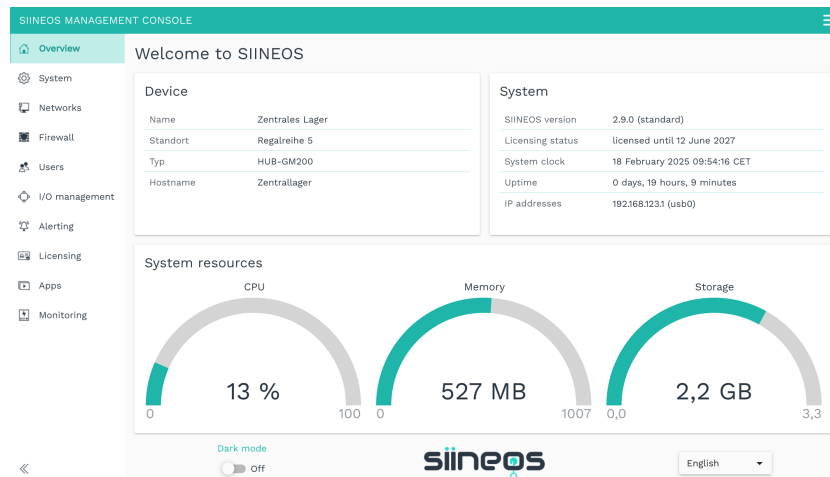
2. If you want to encrypt communication with the gateway by using TLS certificates, create a security certificate via your organisation's Certification Authority (CA).
You can upload this certificate together with the private key in SIINEOS, see [Optional: Configuring TLS certificates \[17\]](#).

3.2. Logging on to SIINEOS

We recommend that you use the latest versions of the **Firefox**, **Edge** or **Chrome** browsers for SIINEOS. Compatibility problems may occur with other or older browsers.

3.2.1. When logging on to SIINEOS for the first time

1. Connect the gateway or module to your PC using a micro USB cable (USB port on the front of the device).
2. Enter the following address in your browser:
<http://192.168.123.1>
3. Log on with the initial user data (**hubadmin/hubadmin**).
The SIINEOS Management Console opens.



SIINEOS start page (example)

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

4. Select the **Users** page and change the password for the user **hubadmin**.
See the chapter [Managing user accounts \[33\]](#).

3.2.2. If you have already set up SIINEOS

1. In your browser, enter the individual IP network address that you have configured.
See the chapter [Setting up Ethernet 1 and Ethernet 2 \[20\]](#).
2. Log on with your user data and click on **Log in**.
The SIINEOS Management Console opens.

3.3. Setting the colour mode and language

1. Go to the SIINEOS start page by selecting the **Overview** page on the left.



“Overview” page with colour mode and language setting (example)

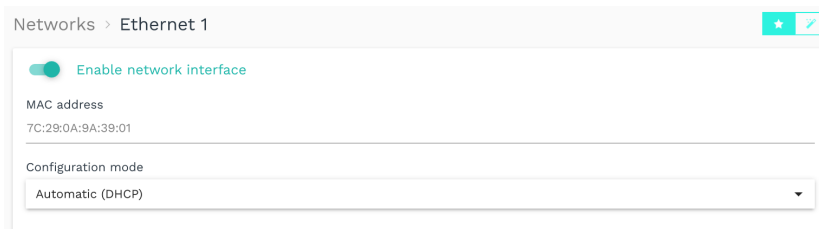
2. The dark mode for the screen display is selected by default. To switch to the bright screen mode, set the **Dark mode** slider to **Off**.
3. To change the language, open the drop-down list.
German and **English** are available.

3.4. Viewing mode: Standard and Advanced

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

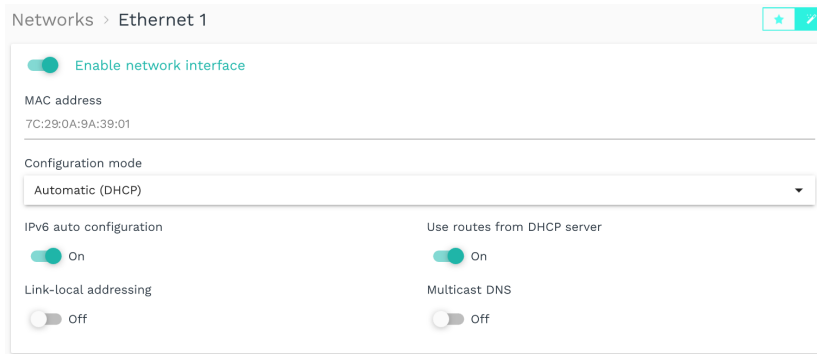
There are two viewing modes in this role, allowing you to display additional settings on some pages. You will find the two buttons for switching at top right.

- **Standard** mode is enabled when you start SIINEOS. You are only shown the parameters and setting options that are sufficient for most applications. This makes configuration easier for you.



“Standard” viewing mode, network settings example

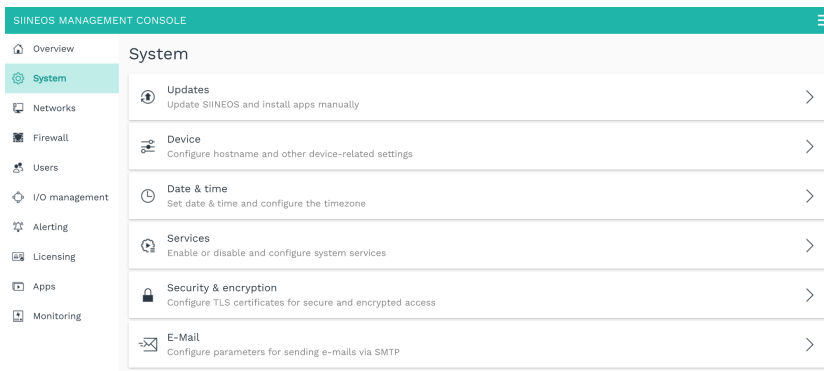
- If you switch to **Advanced** mode, you will be shown further parameters and setting options that cover special cases. Here, you can define every detail of your configuration yourself.



“Advanced” viewing mode, network settings example

3.5. Configuring the system

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



“System” page

3.5.1. Installing SIINEOS updates



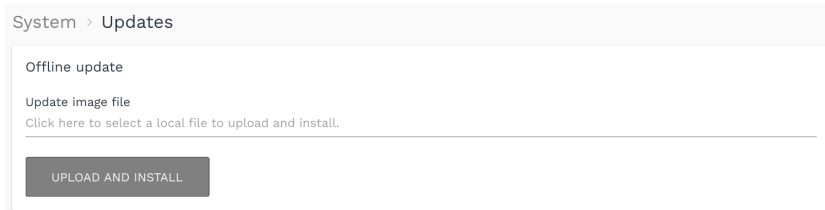
NOTE

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

If the licence has expired, you will be informed that you cannot import any updates.

[Managing SIINEOS licences \[44\]](#)

- Go to the download portal at <https://download.inhub.de/siineos/> and select the required SIINEOS package.
Two variants are available:
 - The complete software package for the gateways and modules, such as the HUB-GM200 or the HUB-EN200
 - SIINEOS Light without Docker containers with a smaller file size for the HUB-IO100
- When the download is complete, go to the **System** page in SIINEOS and select **Updates**.

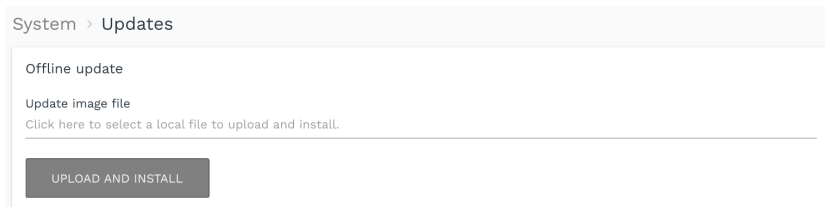


System > Updates

3. Click in the **Update image file** input field and select the software package provided by in.hub in *.raucb format from your local file-storage location.
4. Click on **Upload and install.**
The installation will proceed automatically and takes about 1 minute. After a successful installation, you will be asked whether you want to restart the gateway.
5. Click on **Yes.**
6. After restarting, check that the new version of SIINEOS is displayed on the **Overview** page.
7. If the version has not been updated, proceed as follows:
 - a. First delete your browser cache and refresh the page in your browser.
 - b. If that doesn't work, switch off the power to the gateway and switch it on again after a few seconds.
 - c. Start SIINEOS and check the version number.

3.5.2. Installing app updates

1. On the **System** page, click on **Updates.**



System > Updates

2. Click in the **Update image file** input field and select the software package provided by in.hub in *.raucb format from your local file-storage location.
3. Click on **Upload and install.**
Installation will proceed automatically.
After a successful installation, you will be asked whether you want to restart the gateway.
4. Click on **No.**
You do not need to restart the gateway when uploading apps.

3.5.3. Configuring device settings

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

System > Device ★ ✎ ⚙️ ACTIONS

Hardware information

Typ	HUB-GM200
Architektur	ARM32
Prozessor	IMX7D
Geräte-ID	00142DE082EB

Identification

Hostname of the device
Zentrallager

Description of the device
Zentrales Lager

Location of the device
Regalreihe 5

Communication LED

Red
Disabled

Green
RS485 interface

Debugging

Log debug messages
☐ Off

Log trace messages
☐ Off

Logging filter rules

System > Device, “Advanced” viewing mode (example)

The **Hardware information** section shows the details of your gateway, such as the device ID and the installed processor.

2. Enter the following information in the input fields:
 - a. **Hostname of the device:** Enter a name to uniquely identify the device in the network.
 - b. **Description of the device:** Enter what the device is used for.
 - c. **Location of the device:** Enter the physical location of the device so that you can quickly locate the control cabinet and device if necessary.
 - d. Under **Communication LED**, you can configure LED 2 on the front of the device. It is a bicolour LED, so you can assign the colours red and/or green to the activity of the interface(s).
3. Additional settings are available in **Advanced** viewing mode:
 - **Log debug messages:** Messages from the SIINEOS management service are logged in the system journal to 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.
 - **Logging filter rules:** This field is reserved for in.hub for support purposes and for troubleshooting.

**NOTE**

Do not use these functions during production – performance could be impaired.

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

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

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

3.5.4. Locating the gateway in the control cabinet

To keep track of which device you are currently configuring when using multiple gateways, SIINEOS offers the **Identify via LEDs** function.

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

The LED for device identification on the front of the gateway on which you are currently located starts to flash alternately red and green for 10 seconds.

3.5.5. Setting the date and time

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

System > Date & time

General

Current device date & time
11 July 2024 13:13:55 CEST

Timezone
Europe / Berlin

SET HARDWARE REAL-TIME CLOCKS

Synchronization

Time synchronization server
pool.ntp.org

Automatically synchronize time via browser
☐ Off

SYNCHRONIZE TIME VIA BROWSER NOW

System > Date & time (example)

The gateway's current system time is displayed under **General**. (When you log on for the first time, the UTC time is still displayed by default.)

2. Select the **Timezone** in which your gateway is located.
3. Optional: If you are using a HUB-MRT100 or a HUB-RT100, you can write the system time of the gateway to the real-time clock of the USB stick by clicking on **Set hardware real-time clocks**.

See also [Optional: Calibrating the HUB-MRT100/HUB-RT100 \[15\]](#).

4. If you want to obtain the system time for 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 on **Synchronize time via browser now** to synchronize the gateway's date settings with your computer.
If the gateway's power is disconnected and you are not using an external real-time clock for the time, this setting will be lost. You will then have to synchronize with the browser again. The time zone is retained.
7. When you have completed the entry, click on **Save & close**.

**NOTE**

If you enter an NTP server for synchronizing the time on this page, this is also be automatically transferred to the **Wi-Fi** and **Ethernet** network configurations. However, if an address is already entered there, it will not be overwritten. You should therefore check your entries for the NTP server.

3.5.6. Optional: Calibrating the HUB-MRT100/HUB-RT100

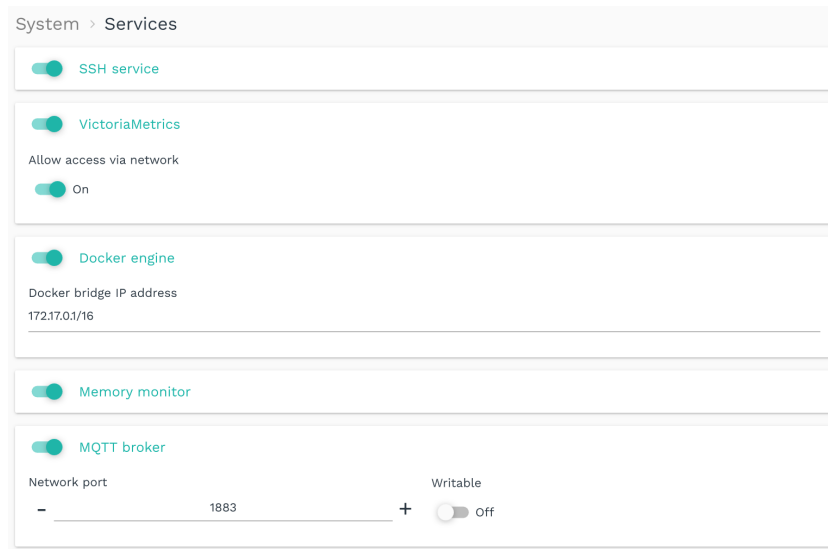
The HUB-MRT100 is a USB stick that stores both the system clock time and process data so that this information is not lost in the event of a power failure. The HUB-RT100 only saves the system clock time.

If you are using one of the two real-time clocks, a calibration function is available in SIINEOS. In order to transfer the system time of the gateway to the stick and save it there, proceed as follows:

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

3.5.7. Configuring system services

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



System > Services

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 enables direct access to the system and data, as well as troubleshooting. In conjunction with the OpenVPN client, a gateway outside the local network can also be accessed.
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 you want the VictoriaMetrics service 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 use your own Docker container with the “Always” restart policy, activate the Docker engine autostart here. If you are using an app in SIINEOS that uses the Docker engine anyway, such as Grafana, you can leave this slider off. You can enter a different IP address for the Docker bridge here if the default IP address is already in use in the company.
Memory monitor	Set the slider to On to restart the gateway automatically if the RAM is no longer sufficient.
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.

- When you have completed the entry, click on **Save & close**.

3.5.8. Optional: Configuring TLS certificates

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

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



System > Security & encryption

- If the gateway is to communicate with other devices and services in encrypted form (e.g., MQTT), click on **CA certificate of the organization** to upload the CA certificate. With this CA certificate, the gateway can check whether the certificates of your organization's devices and services are valid. If this validity check fails, no encrypted connection can be established.
- Click on **Device certificate** to upload the security certificate for this device created by your organization.
- Click on **Private key** to upload the associated key for this device.

3.5.9. Setting up mail servers for notifications



NOTE

Emails can only be sent using a mailbox that supports SMTP. To do this, in your mailbox, you must activate the setting that allows POP3, IMAP or SMTP. This may be different in each email programme.

If necessary, ask your IT service, which can help you configure your mailbox or set up an SMTP-enabled mail account.

- On the **System** page, click on **E-mail**.

System > E-Mail

☒ Send e-mails via SMTP

Server address
smtp.strato.de

Server port
- 465 +

Encryption mode
SSL

Authentication method
LOGIN

Username
alerts@inhub.de

Password
.....

Sender e-mail address
alerts@inhub.de

Sender name
Zentrallager

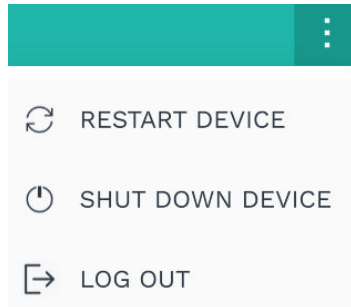
 SEND TEST E-MAIL

System > E-mail (example)

2. Enter the **server address** and **server port** of your mail server.
3. Select the **Encryption mode** to be used for communication with the e-mail/SMTP server. **SSL**, **TLS** and **No encryption** are available.
4. Select the **Authentication method**. **PLAIN**, **LOGIN** and **CRAM-MD5** are available.
5. Enter the **Username** and **Password** you use to log on to the mail server.
6. Enter the **Sender e-mail address** with which the notifications, alarms or e-mails should be provided.
7. Now enter the **Sender name**.
8. To test whether all entries are correct, click on **Send test e-mail** and check whether the test e-mail has arrived.
9. When you have completed the entry, click on **Save & close**.

3.6. Restarting the gateway, shutting down and logging out

1. In the SIINEOS Management Console, click on  at top right.
A menu will open.



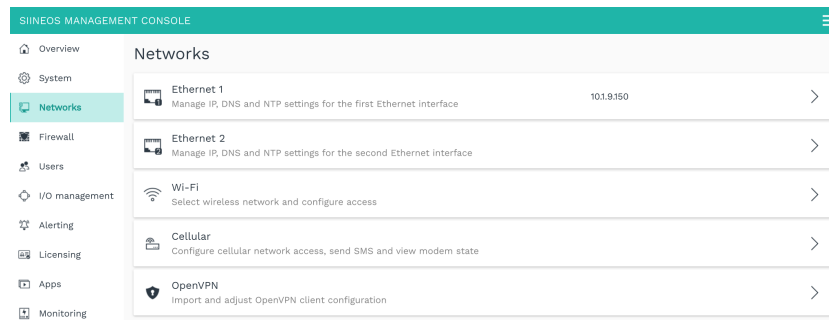
Menu with actions for the current session

2. Select the action you want to perform:

Restart device	A system message is displayed asking whether you really want to restart the gateway. 1. Confirm with Yes. After restarting, the login window will be displayed again.	Possible reasons for restarting: • If the system is no longer responding • If you have postponed the restart after an update, for example, and want to catch up later • If the new version is not displayed after a SIINEOS software update
Shut down device	A system message is displayed asking whether you really want to shut down the gateway. 1. Confirm with Yes.	Possible reasons for shutting down: • If you want to prepare for 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 an abrupt switch-off during a write process.
Log out	You log out of the system and allow another user to log on.	Possible reasons for logging out: • Shift change

3.7. Configuring networks

You can configure the following connections on the **Networks** page:



“Networks” page (example)

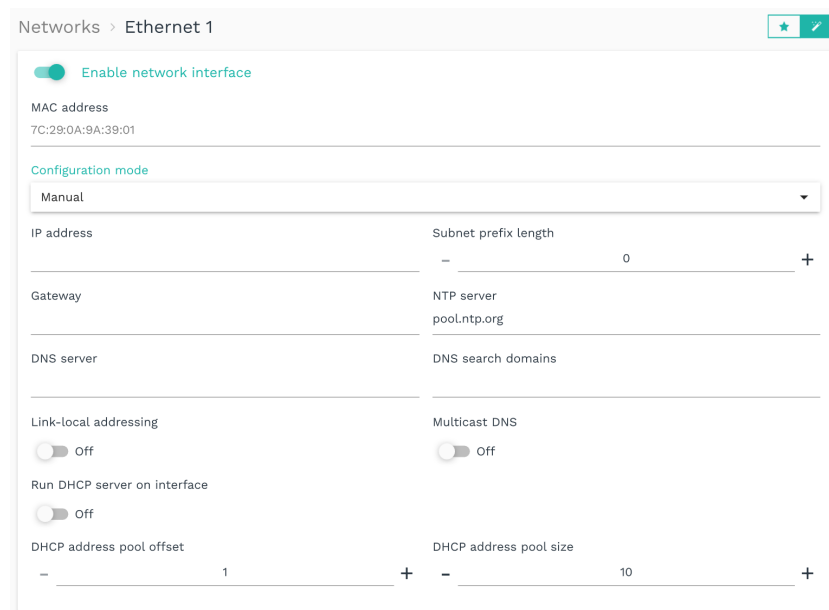
3.7.1. Setting up Ethernet 1 and Ethernet 2

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



RECOMMENDATION

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



Networks > Ethernet 1 > Configuration mode “Manual” (viewing mode “Advanced”)

1. On the **Networks** page, select **Ethernet 1** or **Ethernet 2**.
2. To activate the interface, set the **Enable network interface** slider to **On**.
The MAC address printed on the housing of the gateway is displayed.
3. To automatically obtain all network parameters via a DHCP server, leave the default setting **Automatic (DHCP)** selected in the **Configuration mode** drop-down list.

You do not need to make any other entries in the **Standard** viewing mode.

You can refine the network configuration in the **Advanced** viewing mode:

IPv6 autoconfiguration	By default, the slider is set to On , i.e. 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 received 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	The slider is set to On by default. The gateway generates the link-local address automatically, so that communication within the same network segment is possible without DHCP or a static IP address. If you do not require a link-local address for local communication within the network segment, deactivate the function.
Multicast DNS	The slider is set to On by default. Instead of a request being sent to a DNS server, all subscribers in the network are addressed directly. Gateways can then be accessed in the network at <hostname>.local. You can find the hostname in SIINEOS on the System > Device page.

- To configure the network parameters manually, select **Manual** from the **Configuration mode** drop-down list.
- Complete the input fields.

NOTE: For some parameters where you can make multiple entries, as in the case of the DNS server, separate them with a space, not a comma.

IP address	Enter the gateway IPv4 or IPv6 address to be assigned to the Ethernet 1 or Ethernet 2 interface, respectively. The address ranges 172.17.0.0/16 and 172.18.0.0/16 are reserved for the internal Docker network and can be changed in System > Services if required.
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 the subnet mask 255.255.255.0 or the value 16 for networks with the subnet mask 255.255.0.0 .
Gateway	Enter the IP address of the gateway.
NTP server (optional)	Enter the IP address or the computer name of the time server from which the gateway is to obtain its system time.

DNS server	Enter the IP address of the DNS server used to resolve the names of computers in the network / on the Internet.
DNS search domains (optional)	Enter the internal DNS domain for your company network, e.g. <code>lan.mycompany.com</code> .
Run DHCP server on interface	Set the Run DHCP server on interface slider to On if the gateway is to take over the role of the DHCP server and assign IP addresses to the devices connected in the isolated machine network. RECOMMENDATION: Only use this function for a direct 1:1 connection between the gateway and a sensor, a PLC, an add-on module or a TBEN module. In a larger network with several machines, a central IT infrastructure is necessary.
DHCP address pool offset	Specify which IP addresses are to be assigned for the connected peripheral device. For example: You enter a "12". Starting with the parameter entered under IP address , the number after the last point 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 peripheral devices 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)	The slider is set to On by default. The gateway generates the link-local address automatically, so that communication within the same network segment is possible without DHCP or a static IP address. If you do not require a link-local address for local communication within the network segment, deactivate the function.
Multicast DNS (only in Advanced viewing mode)	The slider is set to On by default. Instead of a request being sent to a DNS server, all subscribers in the network are addressed directly. Gateways can then be accessed in the network at <code><hostname>.local</code> . You can find the hostname in SIINEOS on the System > Device page.

6. If you have selected **None** in **Configuration mode**, the gateway is still accessible via a link-local IP address or using the name announced via multicast DNS (e.g. `hub-gm.local`) – but only locally and not across network boundaries.
You can change this setting in the **Advanced** viewing mode:

Link-local addressing (only in Advanced viewing mode)	The slider is set to On by default. The gateway generates the link-local address automatically, so that communication within the same network segment is possible without DHCP or a static IP address. If you do not require a link-local address for local communication within the network segment, deactivate the function.
Multicast DNS (only in Advanced viewing mode)	The slider is set to On by default. Instead of a request being sent to a DNS server, all subscribers in the network are addressed directly. Gateways can then be accessed in the network at <hostname>.local. You can find the hostname in SIINEOS on the System > Device page.

- Finally, click on **Save & close**.
This will take you back to the **Networks** page.

3.7.2. Setting up Wi-Fi

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

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

Networks > Wi-Fi

☒ Enable network interface

MAC address
A8:42:A1:58:CA:03

Wi-Fi name

Wi-Fi password

NTP server
pool.ntp.org

Use routes from DHCP server
☒ On

Networks > Wi-Fi

- If you want to connect to a Wi-Fi network, set the **Enable network interface** slider to **On**.
The MAC address, which is also printed on the housing of the gateway, will be displayed.
- Enter the name and password of the Wi-Fi you want to connect to.
- Optional: Enter the IP address of an NTP server from which the gateway is to obtain its system time.
- Optional: Set the **Use routes from DHCP server** slider to **Off** to only access the local network via this interface and access the Internet via another interface if necessary.
- Finally, click on **Save & close**.
This will take you back to the **Networks** page.

3.7.3. Setting up a mobile connection

The in.hub LTE stick can be connected via a USB interface to access the Internet in environments without a network. The gateway can use this access to connect to a cloud, for example, or the gateway can be accessed remotely via the VPN (Virtual Private Network) tunnel.

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

Networks > Cellular > Access configuration “Custom” (in “Standard” viewing mode)

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 / mobile network provider or **Custom**.
3. If you have selected **Custom**, enter the following information:

APN	Access point name Enter the access point address you received from your mobile network provider to establish communication between the terminal device and the mobile 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 for the SIM card. Make sure to use the correct PIN for the SIM card used. Otherwise, the card will be blocked after three unsuccessful attempts.
Allow roaming	If you want to allow roaming, set the slider to On . If you have a SIM card with roaming service, you can enable this function to dial into third-party-provider networks if required.
Mobile data	This function is switched on by default. If you only want to use the in.hub LTE stick to send text messages, set the slider to Off .

- To check whether your entries are correct, enter a message text and the mobile number of the terminal device under **SMS test** and click on **Send SMS**.
- If no SMS arrives, check whether the signal quality is adequate.
- Finally, click on **Save & close**.
This will take you back to the **Networks** page.

3.7.4. Setting up OpenVPN

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

Networks > OpenVPN

- If you want to use an OpenVPN, set the **Enable network interface** slider to **On**.
- Click on **Import OpenVPN configuration file** to select the configuration file from your local file directory.
- Enter the file name (without file extension) in the **Internal configuration name** input field.
- Finally, click on **Save & close**.
This will take you back to the **Networks** page.

3.8. Configuring the firewall

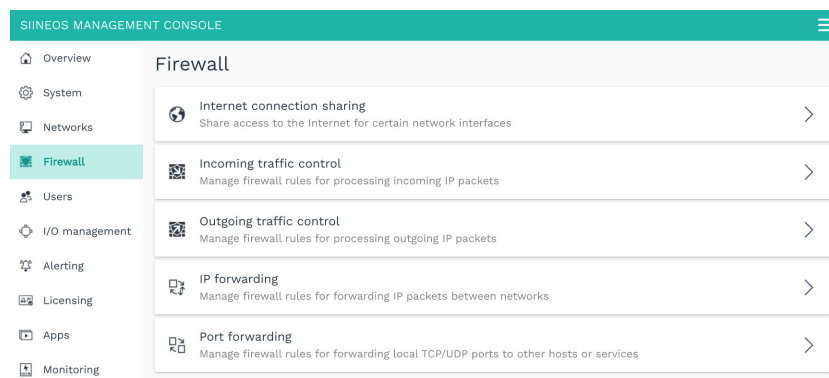


RECOMMENDATION

When customizing or configuring the device's internal firewall, if possible, connect your computer via the micro USB port on the front of the gateway and open the SIINEOS Management Console via the USB network address <http://192.168.123.1>.

This prevents you from losing access to the gateway via the network due to an incomplete or incorrectly configured firewall rule.

On the **Firewall** page, you can configure the gateway's integrated network firewall and define rules that determine how the gateway communicates in the network and how it handles the network traffic it receives. The following functions are available:



“Firewall” page

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

You first specify whether data traffic passing through the gateway is to be processed or not.

- If you do not need this function, simply skip the **Firewall** page.
- If you do, you can follow the blacklisting approach that SIINEOS uses by default, whereby any data traffic that is not explicitly prohibited is allowed.

Alternatively, you can follow the whitelisting approach, whereby any data traffic that is not explicitly permitted is not allowed.



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 limited.

Notes on incoming and outgoing network traffic: All rules that you create are processed in sequence for each incoming data packet – from top to bottom in the list. At the point when all criteria of a rule are met by a data packet, rule processing is completed with the specified action. No further rules are processed.

Firewall > Incoming traffic control

Rule name	Network protocol	Network interface	Source address	Destination ports	Action
HTTP-Anfragen über VPN erlauben	TCP	OpenVPN		443	Accept packets
Sonstigen Zugriff über VPN verbieten	All protocols	OpenVPN			Drop packets
SSH-Zugriff von Admin-PC erlauben	TCP	Ethernet 1	192.400.532	22	Accept packets
Sonstigen SSH-Zugriff verbieten	TCP	All network interfaces		22	No action

Example of a list of rules for incoming network traffic

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



TIP

Create all positive rules first. In doing so, it must be very specifically defined which access is to be authorized by whom. At the end of the list, it is useful to have a rule in which no conditions are set. You can then only select in the **Actions** drop-down list whether the gateway ignores requests from the network (Drop packets) or actively rejects such requests (Reject packets).

3.8.1. Sharing Internet connections

In this window, you define the networks through which the devices connected to this network (e.g. machines) are authorized to access the Internet via the gateway.

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

Firewall > Internet connection sharing

☒ Share Internet connection

Network with Internet connection:

Ethernet 1

Networks allowed to use the shared Internet connection:

☒ Ethernet 1

☐ Ethernet 2

☐ Wi-Fi

☐ Cellular

☐ OpenVPN

Firewall > Internet connection sharing

2. Enable the **Share Internet connection** slider.
3. In the **Network with Internet connection** drop-down list, select the network through which the gateway accesses the Internet.
4. Enable the slider for the network that is allowed to use the shared Internet connection.
5. Click on **Save & close**.
This will take you back to the **Firewall** page.

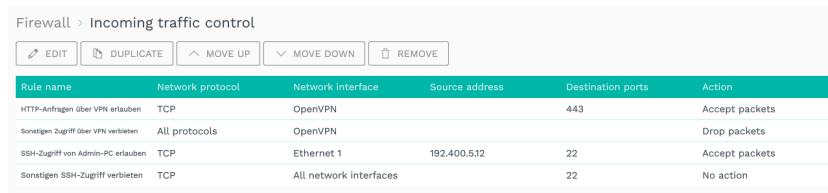
3.8.2. Controlling incoming traffic

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

All incoming packets are allowed by default, so that the respective network services of the gateway (e.g. SSH, MQTT, SMAC) can be accessed from all networks.

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

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



The screenshot shows the 'Firewall > Incoming traffic control' interface. At the top, there are buttons for 'EDIT', 'DUPLICATE', 'MOVE UP', 'MOVE DOWN', and 'REMOVE'. Below these is a table with the following data:

Rule name	Network protocol	Network interface	Source address	Destination ports	Action
HTTP-Anfragen über VPN erlauben	TCP	OpenVPN		443	Accept packets
Sonstigen Zugriff über VPN verbieten	All protocols	OpenVPN			Drop packets
SSH-Zugriff von Admin-PC erlauben	TCP	Ethernet 1	192.400.532	22	Accept packets
Sonstigen SSH-Zugriff verbieten	TCP	All network interfaces		22	No action

Firewall > Incoming traffic control (example)

2. To add a new rule, click on **Add incoming traffic rule**.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
3. Enter a name under **Rule name**.
4. Select the **Network protocol** for network packets to 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 through any interface for the rule to apply.
6. Enter a **Source address** if the rule should only apply 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 certain TCP/UDP ports of the gateway.
Then 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 is allowed or denied (depending on the action selected in the next step).
8. Under **Action**, select from the drop-down list what should happen to network packets that meet all the criteria of the rule.
 - **No action:** The rule is disabled, i.e. the process continues with the next rule.
 - **Accept packets:** The request is authorized and the packets are allowed to arrive.
 - **Drop packets:** The request is not authorized and the packet is dropped, i.e. effectively ignored. No answer is returned.

- **Reject packets:** The request is actively rejected and answered. A reject packet is sent back to the sender, so that establishing the connection fails.
- Once you have made all the entries, click on **Finish**.
This will take you back to the list with all the rules.
 - If you want to edit a rule, select it and click on **Edit** or double-click.
A page opens where you can see and edit all the rule settings at a glance.
To save your changes, click on **Save & close**.
 - If you want to duplicate a rule, select it and click on **Duplicate**.
This will take you back to the setup wizard, where you can customise the rule.
 - If you want to remove a rule, select it and click on **Remove**.
 - If you want to change the order in which the rules are applied, select the rule and click on **Move up** or **Move down**.

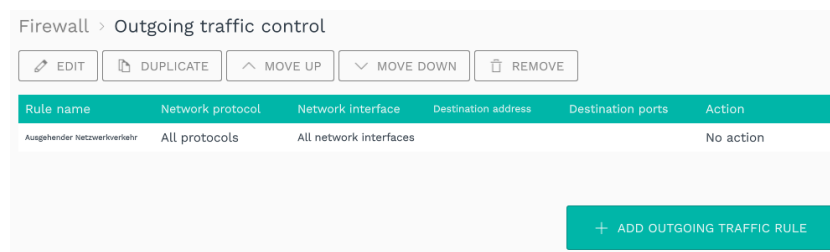
3.8.3. Controlling outgoing traffic

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

All outgoing packets are allowed by default, so the gateway can access all accessible networks and, if applicable, the Internet without restriction.

You can define rules here to block access to certain destination addresses.

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



Firewall > Outgoing traffic control (example)

- To add a new rule, click on **Add outgoing traffic rule**.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
- Enter a name under **Rule name**.
- Select the **Network protocol** for network packets to which this rule applies.
Select **All protocols** if you want the rule to apply to all network protocols.
- 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 be sent through any interface for the rule to apply.
- Enter a **Destination address** if the rule should only apply 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 can restrict access from the gateway to certain TCP/UDP ports of the target computer/network.

Then 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 is allowed or denied (depending on the action selected).

8. Under **Action**, select from the drop-down list what should happen to network packets that meet all the criteria of the rule.

- **No action:** The rule is disabled, i.e. the process continues with the next rule.
- **Accept packets:** The packet may be sent via the corresponding network interface.
- **Drop packets:** The packet is not sent, but dropped (discarded). The sending application receives no information that the packet has not been sent.
- **Reject packets:** The packet is not sent and the sending application is informed that the network packet could not be sent / was not sent.

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

This will take you back to the list with all the rules.

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

A page opens where you can see and edit all the rule settings at a glance.

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

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

This will take you back to the setup wizard, where you can customise the rule.

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

13. If you want to change the order in which the rules are applied, select the rule and click on **Move up** or **Move down**.

3.8.4. Defining and editing rules for IP forwarding

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

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

Firewall > IP forwarding

EDIT DUPLICATE REMOVE

Rule name ^	Input interface	Output interface	Source address	Destination address
Tosibox 1	All network interfaces	All network interfaces	10.10.206.0/24	
Tosibox 2	All network interfaces	All network interfaces		10.10.206.0/24

+ ADD IP FORWARDING RULE

Firewall > IP forwarding (example)

- To add a new rule, click on **Add IP forwarding rule**.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
- Enter a **name**.
- From the drop-down list, select the **Input interface** from which the data traffic is to be forwarded.
- From the drop-down list, select the **Output interface** (destination) to which the data traffic is to be forwarded.
- To limit data traffic only to a specific host or a defined 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, data traffic will not be restricted.
- When you have completed the entry, click on **Save & close**.
This will take you back to the list with all forwarding rules.
- If you want to edit a rule, select it and click on **Edit** or double-click.
A page opens where you can see and edit all the rule settings at a glance.
To save your changes, click on **Save & close**.
- If you want to duplicate a rule, select it and click on **Duplicate**.
This will take you back to the setup wizard, where you can customise the rule.
- If you want to remove a rule, select it and click on **Remove**.

3.8.5. Configuring port forwarding

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

Firewall > Port forwarding

EDIT DUPLICATE REMOVE

Rule name ^	Network protocol	Local port	Destination address	Destination port	Masking
VNC-Server SPS	TCP	58	10.5.8.12	58 (auto)	●

+ ADD PORT FORWARDING RULE

Firewall > Port forwarding (example)

2. To add a new rule, click on **Add port forwarding rule**.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
3. Enter a name under **Rule name**.
4. Select the **Network protocol** for network packets to which the port forwarding rule is to be applied.
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 data traffic is to be forwarded.
7. If you do not want to forward data traffic to a local port but to another port, enter the desired port number under **Destination port**.
If you do not enter anything, the local port will be used.
8. Under **Masquerading**, the slider is automatically set to **On**. This means that the source address is replaced by the gateway's IP address for all forwarded packets.
This is always necessary if direct IP routing between the sender and target host is not possible. This address translation ensures that replies from the target host are correctly returned to the original sender. In the most cases where port forwarding is required, masquerading is also necessary for communication to function as desired.
If you do not want this to happen, set the slider to **Off**.
9. Once you have made all the entries, click on **Finish**.
This will take you back to the list with all forwarding rules.
10. If you want to edit a rule, select it and click on **Edit** or double-click.
A page opens where you can see and edit all the rule settings at a glance.
To save your changes, click on **Save & close**.
11. If you want to duplicate a rule, select it and click on **Duplicate**.
This will take you back to the setup wizard, where you can customise the rule.
12. If you want to remove a rule, select it and click on **Remove**.

3.9. User administration

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

- **System administrator**

This role can log on to SIINEOS and configure the system, activate apps and open them in SIINEOS so that app users can access them.

When logging on to SIINEOS for the first time, a user account (**hubadmin/hubadmin**) is created with the role of **System administrator**. You should change the preset password after logging on.

- **App administrator**

This role can log on to the administration interface of an app (e.g. MADOW) and configure it.

When logging on to the **InGraf** app for the first time, a user account (**ingrafadmin/ingrafadmin**) is created with the role of **App administrator**.

Likewise, when logging on to the MADOW app for the first time, a user account (**madowadmin/madowadmin**) is created with the role of **App administrator**.

You should change the preset passwords after logging on.

- **App user**

This role can log on to protected areas of an app where, for example, sensitive information is displayed.

All other user accounts are created and managed by you as the system administrator. The two user roles **App administrator** and **App user** are available for Apps.

No authentication is required for some areas in apps. For example, a machine operator can connect directly to MADOW via the appropriate web address and view downtimes without having to log on.

Also, not every app has rights management. The **Grafana** and **NodeRED** apps only establish the connection to the external applications, for which you need your own accounts.

3.9.1. Managing user accounts

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



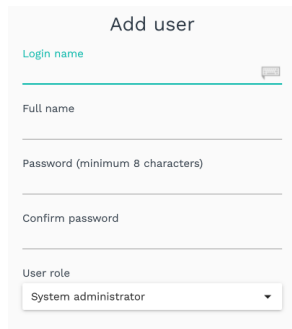
NOTE

You can neither deactivate nor remove the preconfigured **System administrator** role.

Users		
EDIT DUPLICATE DEACTIVATE REMOVE		
SHOW DEACTIVATED ENTRIES		
Login name ^	Full name	Role
hubadmin	HUB Administrator	System administrator
hubuser1	Hannes Mustermann (Maschineneinrichter)	App user
ingrafadmin	InGraf Administrator	App administrator
madowadmin	MADOW Administrator	App administrator
+ ADD USER		

“Users” page (example)

1. On the **Users** page, click **Add user** to create a new user;
– or –
select an existing user and click on **Duplicate**.



Users > Add user

2. Enter the **Login name**, the **Full name** and a **Password**.
The password must consist of at least 8 characters.
3. Assign a **User role** to the user in the drop-down list.
4. When you have completed the entry, click on **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 on **Edit**.
The same window opens as when creating a user. Here you can change all details and/or assign a different user role.
6. If you want to remove a user, select them and click on **Remove**.
7. To deactivate a user, e.g. because the user is absent for a longer period of time, select the corresponding line in the list and click on **Deactivate**.
8. To restore a deactivated user, click on the **Show deactivated entries** filter, select a user and click on **Activate**.



TIP

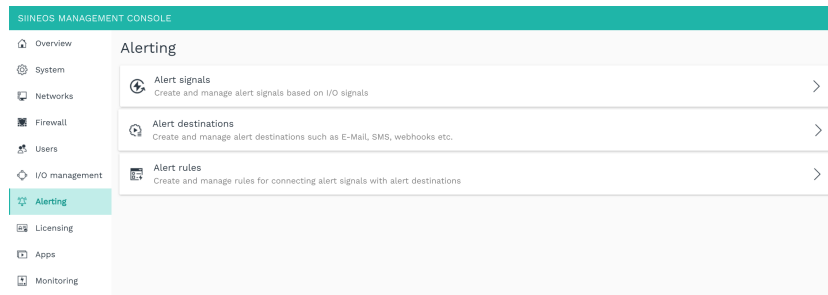
For many entries, you can search within the list. Click on the magnifying glass at top right  and enter the username you are looking for.

3.10. Creating and configuring alert signals, destinations and rules

On the **Alerting** page, you can cause an alert signal to be triggered when a state you have defined is entered, see [Creating alert signals \[35\]](#).

You can forward this in various ways, for example by e-mail, SMS or webhook, see [Managing alert destinations \[36\]](#).

In addition, you can define alert rules that continuously process the alert signals and forward their statuses to the alert destinations, see [Adding an alert rule \[38\]](#).



“Alerting” page

3.10.1. Creating alert signals

1. On the start page of **Alerting**, select **Alert signals**.

If alert signals have already been created, they will be displayed in a list.

Alerting > Alert signals

SHOW DEACTIVATED ENTRIES

Name	Source	Evaluation mode	Severity	Category	State	Last change
Feuchtealarm	GM200-Zentrallager – Feuchte	Compare with thresholds	High / critical	Melden	✗	Tue Feb 18 13:58:07 2020 UTC+0100
Partikelmessung PM2.5	Sensiron SPMS30 – Mass concentration PM2.5	Map binary input value	Medium / warning	Bar	✓	Tue Feb 18 13:58:48 2020 UTC+0100
ZL Strom	GM200-Zentrallager – Roboterstrom	Map binary input value	Low / info	Foo	✓	Tue Feb 18 13:58:48 2020 UTC+0100

List with examples of alert signals

2. To create a new alert signal, click on **Add alert signal**.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
3. Enter the **Name** for the alert signal.
4. Under **Source**, select the I/O signal for which an alarm state is to be defined.
5. Under **Evaluation mode**, you can define how the source signal is to be evaluated. The following options are available:
 - a. **Use binary input value:** The source signal represents the status of the alert signal as a binary value. This mode is, for example, well suited for a light barrier or if the input signal is a digital signal (an error or a condition) from a PLC.
 - b. **Compare with thresholds:** The source signal must be within certain limits in order to remain in the OK state. This mode is, for example, well suited for process-related values such as humidity, speed, current, etc.
 - c. **Follow counter:** The source signal is a counter that must increase steadily in order to remain in the OK state. This mode is well suited for piece counters, energy meters, metre counters, etc.
 - d. **Follow cycles:** The incoming signal follows a cycle. The signal remains in the OK state only if the duration between two pulses does not exceed a specified time. This mode is, for example, well suited for processes and production cycles – as soon as the next pulse arrives late or not at all, the machine stops and the alarm is triggered.
6. Depending on which evaluation mode you have selected in the previous step, you can now configure what is an OK state and what is an alert state.

- a. After selecting **Use binary input value**, you can define under **Polarity** whether 0 is the OK state and 1 is the alert state or 0 is the alert state and 1 is the OK state.
 - b. After selecting **Compare with thresholds**, you can define when the signal value should become an alert when it reaches one or more **Thresholds** you have set.
 - c. After selecting **Follow counter**, you can enter the **Step size** by which the counter must be increased regularly to keep the alert signal in the OK state.
 - d. After selecting **Follow cycles**, you can enter the **Thresholds** that the signal value must exceed in order to detect a pulse.
7. If you have selected **Follow counter** or **Follow cycles**, an additional page will be displayed. Here you can enter the **Cycle time** in milliseconds, i.e. define the time between two pulses or counters.
 8. Under **State transition delays**, you can enter the time that should still elapse until the alert or OK state is entered.

This is useful if outliers such as temperature or current peaks are to be ignored so that fewer messages are sent when the measured values or signal values vary around a limit range.
 9. Under **Severity**, select how critical the alert signal is.
 10. Optional: Under **Category**, assign a name if you want to assign this alert signal to a category.

The category is stored as meta information and can be used as a variable in the alert destinations. For example, the variable is used by the **SIGNL4** app, where the category is important basic information.
 11. Once you have made all the entries, click on **Finish**.

You return to the list with all alert signals.
 12. If you want to edit an alert signal, select it and click on **Edit** or double-click.

This will take you back to the setup wizard.
 13. If you want to duplicate an alert signal, select it and click on **Duplicate**.

This will take you back to the setup wizard.
 14. If you want to deactivate an entry because you want to perform a test run on your production line, for example, select the entry and click on **Deactivate**.

The entry is now only visible if you click on **Show deactivated entries**.
If you want to reactivate the entry, select it and click on **Activate**.
 15. If you want to remove an alert signal, select it and click on **Remove**.

3.10.2. Managing alert destinations

1. On the start page of **Alerting**, select **Alert destinations**.

If alert destinations have already been created, they will be displayed in a list.

Alerting > Alert destinations

[EDIT](#)
[DUPLICATE](#)
[DEACTIVATE](#)
[REMOVE](#)
[SHOW DEACTIVATED ENTRIES](#)

Name ^	Type	Details
E-Mail an Max Mustermann	E-Mail	max.mustermann@inhub.de
SMS an Betriebsleitung	SMS	016897788596

List with examples of alert destinations

- To add a new alert destination, click on **Add alert destination**.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
- Enter the **Name** for the alert destination.
- Under **Type**, you can select the desired type of alert destination. The following options are available:
 - E-mail**
 - SMS**
 - Webhook**
 - VictoriaMetrics**
 - I/O signal**
 - MQTT**
 - App**
- Depending on which type you have selected in the previous step, you can now specify the way in which the alert destination processes and forwards the alert signals under **Details**.
TIP: Placeholders are available for free-text fields. They are displayed when clicking in the input field or on the **Placeholder variables** icon.
 - After selecting **E-mail**, you can enter the e-mail addresses of the recipients, the subject and the text.
 - After selecting **SMS**, you can enter the telephone numbers of the recipients and the message text.
 - After selecting **Webhook**, you can enter the URL, the HTTP method and the data for the body of the HTTP request.
 - After selecting **VictoriaMetrics**, you can enter the metric name.
 - After selecting **I/O signal**, you can select the I/O signal from the existing I/O units into which the alert state is to be written, e.g. an LED or a digital output.
 - After selecting **MQTT**, you can enter the MQTT broker address, MQTT broker port, topic name and topic data. In addition, you can select whether the published data is to be kept on the MQTT broker, so that later-connecting MQTT clients still receive this data.
 - After selecting **App**, you can select the alert-processing app **SIGNAL4** to which the notification is to be forwarded. The app must be installed in SIINEOS.

6. Once you have made all the entries, click on **Finish**.
You return to the list with all alert destinations.
7. If you want to edit an alert destination, select it and click on **Edit** or double-click.
This will take you back to the setup wizard.
8. If you want to duplicate an alert destination, select it and click on **Duplicate**.
This will take you back to the setup wizard.
9. If you want to deactivate an entry, select the entry and click on **Deactivate**. This may become necessary if, for example, the alert destination is not currently available and/or alert messages that are sent too frequently during set-up are to be temporarily muted.
The entry is now only visible if you click on **Show deactivated entries**.
If you want to reactivate the entry, select it and click on **Activate**.
10. If you want to remove an alert destination, select it and click on **Remove**.

3.10.3. Adding an alert rule

1. On the start page of **Alerting**, select **Alert rules**.
If alert rules have already been created, they will be displayed in a list.

Alerting > Alert rules

[SHOW DEACTIVATED ENTRIES](#)

Name	Alert signals	Alert destinations	Details	Last trigger
E-Mails für kritische Alarme versenden	All alert signals	SMS an Betriebsleitung	ⓘ	Mon Jan 27 11:31:20 2025 UTC+01:00
Schwellwertüberschreitung in Datenbank schreiben	All alert signals	In Datenbank schreiben	ⓘ	Mon Jan 27 11:31:20 2025 UTC+01:00

List with examples of alert rules

In the **Details** column, the most important parameters of the alert (trigger, repetition, severity levels) are summarized in a tooltip.

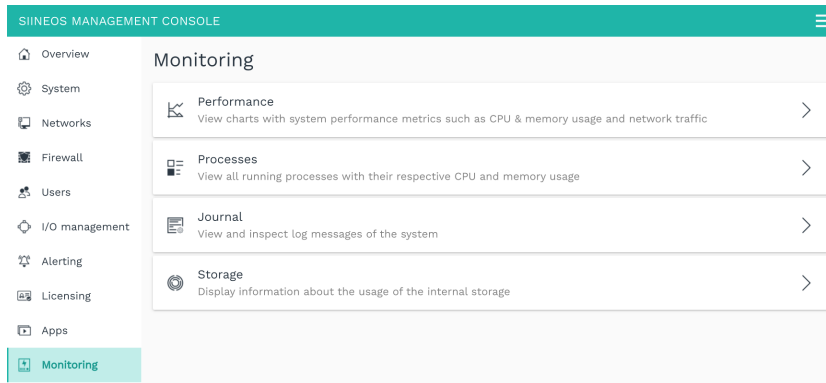
2. To create a new alert rule, click on **Add alert rule**.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
3. Enter the **Name** for the alert rule.
4. Under **Alert signals**, leave the slider set to **On** if all alert signals are to be evaluated by this rule;
– or –
set the slider to **Off** and select individual alert signals to be evaluated by this rule.
5. Under **Trigger**, set the **Alert** slider to **On** so that the alert rule is applied when the alert signal changes to or remains in the alert state;
– or –
set the **OK** slider to **On** if the alert rule is applied as soon as the alert signal returns to or continues in the OK state.
6. Optional: Under **Repetition**, you can specify whether the rule sends alert messages via the alert destinations periodically with the alert signals in an unchanged state and, if so, how long the repetition interval should be.

If you do not specify an interval, the rule will only ever be applied if the state changes.

7. Under **Severity levels**, select which severity level of an alert signal is to be included in the alert rule.
8. Under **Destinations**, you can select the alert destinations via which (alert) messages are to be sent when the selected alert signals are in the configured states.
9. Once you have made all the entries, click on **Finish**.
You return to the list with all alert rules.
10. If you want to edit an alert rule, select it and click on **Edit** or double-click.
This will take you back to the setup wizard.
11. If you want to duplicate an alert rule, select it and click on **Duplicate**.
This will take you back to the setup wizard.
12. If you want to deactivate an entry, for example, because you want to temporarily suspend alert forwarding to your alert destination, select the entry and click on **Deactivate**.
The entry is now only visible if you click on **Show deactivated entries**.
If you want to reactivate the entry, select it and click on **Activate**.
13. If you want to remove an alert rule, select it and click on **Remove**.

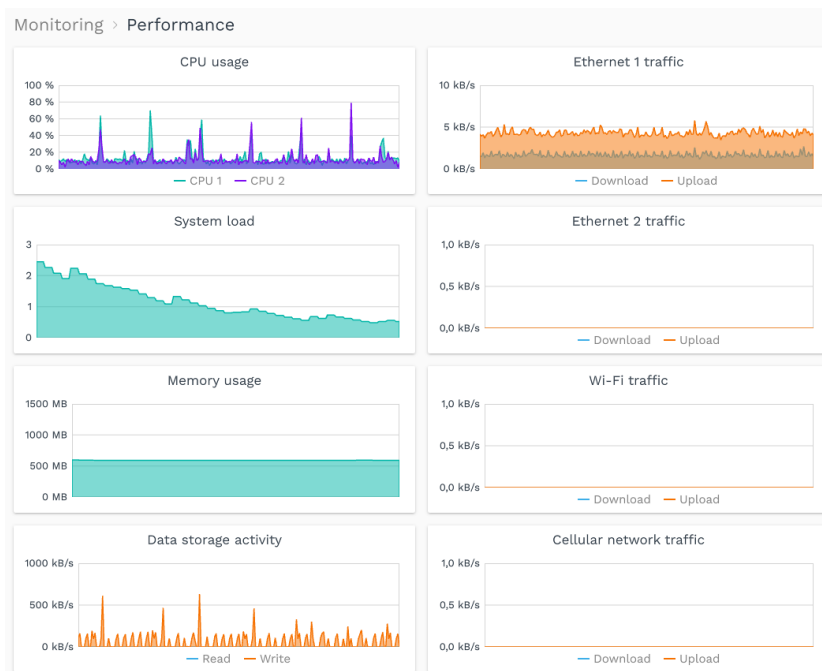
3.11. Monitoring the system

Various functions for device monitoring and diagnostic purposes are available on the **Monitoring** page:



“Monitoring” page

- **Performance:** Check the utilization of the processor and RAM live, as well as the activity of the storage and the network interfaces of your gateway.



Monitoring > Performance (example)

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

Monitoring > Processes

Process ID	Name	CPU usage ▾	Memory usage
373	SMAC-Server	13 %	72 MB
485	victoria-metric	2 %	77 MB
22502	mosquitto	2 %	6 MB
299	Monitor Server	1 %	26 MB
7237	InGraf	1 %	22 MB
22819	OpcUaServer	1 %	26 MB
1	systemd	0 %	7 MB
2	kthreadd	0 %	< 1 MB
3	rcu_gp	0 %	< 1 MB
4	rcu_par_gp	0 %	< 1 MB
8	mm_percpu_wq	0 %	< 1 MB
9	ksoftirqd/0	0 %	< 1 MB
10	rcu_sched	0 %	< 1 MB
11	migration/0	0 %	< 1 MB
12	cpuhp/0	0 %	< 1 MB
13	cpuhp/1	0 %	< 1 MB
14	migration/1	0 %	< 1 MB
15	ksoftirqd/1	0 %	< 1 MB

Monitoring > Processes (example)

- **Journal:** Gain insight into the primary log files of SIINEOS, which contain important messages, especially error messages, for ongoing operations. In case of problems with SIINEOS, you can check whether any relevant error messages have been logged here.

Monitoring > Journal

[Download](#)

Recent messages

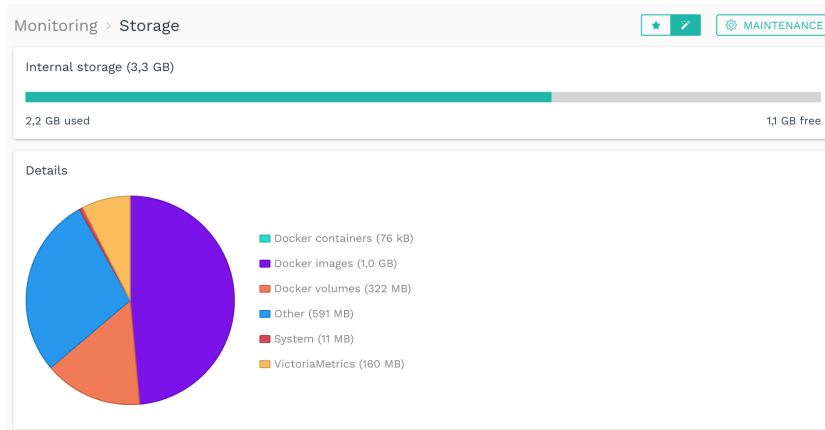
Boot messages

```
-- Journal begins at Thu 2024-07-11 11:56:38 UTC, ends at Thu 2024-07-11 11:56:58 UTC. --
Jul 11 11:56:38 hub-gm kernel: Booting Linux on physical CPU 0x0
Jul 11 11:56:38 hub-gm kernel: Linux version 5.4.279-gm200+ (root@runner-n8pqbiw-project-14-concurrent-0) (gcc version 8.
Jul 11 11:56:38 hub-gm kernel: CPU: ARMv7 Processor [410fc075] revision 5 (ARMv7), cr=10c5387d
Jul 11 11:56:38 hub-gm kernel: CPU: div instructions available: patching division code
Jul 11 11:56:38 hub-gm kernel: CPU: PIPT / VIPT nonaliasing data cache, VIPT aliasing instruction cache
Jul 11 11:56:38 hub-gm kernel: OF: fdt: Machine model: in.hub HUB-GM200
Jul 11 11:56:38 hub-gm kernel: Memory policy: Data cache writealloc
Jul 11 11:56:38 hub-gm kernel: On node 0 totalpages: 262144
Jul 11 11:56:38 hub-gm kernel: Normal zone: 1728 pages used for memmap
Jul 11 11:56:38 hub-gm kernel: Normal zone: 0 pages reserved
Jul 11 11:56:38 hub-gm kernel: Normal zone: 196608 pages, LIFO batch:63
Jul 11 11:56:38 hub-gm kernel: HighMem zone: 65536 pages, LIFO batch:15
Jul 11 11:56:38 hub-gm kernel: psci: probing for conduit method from DT.
Jul 11 11:56:38 hub-gm kernel: psci: PSCTv1.0 detected in firmware.
Jul 11 11:56:38 hub-gm kernel: psci: Using standard PSCI v0.2 function IDs
Jul 11 11:56:38 hub-gm kernel: psci: Trusted OS migration not required
Jul 11 11:56:38 hub-gm kernel: psci: SMC Calling Convention v1.0
Jul 11 11:56:38 hub-gm kernel: percpu: Embedded 15 pages/cpu s30668 r8192 d22580 u61440
Jul 11 11:56:38 hub-gm kernel: pcpu-alloc: s30668 r8192 d22580 u61440 alloc=15*4096
Jul 11 11:56:38 hub-gm kernel: pcpu-alloc: [0] 0 [0] 1
Jul 11 11:56:38 hub-gm kernel: Built 1 zonelists, mobility grouping on. Total pages: 260416
Jul 11 11:56:38 hub-gm kernel: Kernel command line: rauc.slot=A boot=/dev/mmcblk0p2 root=/dev/mmcblk0p3 quiet console=
Jul 11 11:56:38 hub-gm kernel: Dentry cache hash table entries: 131072 (order: 7, 524288 bytes, linear)
Jul 11 11:56:38 hub-gm kernel: Inode-cache hash table entries: 65536 (order: 6, 262144 bytes, linear)
Jul 11 11:56:38 hub-gm kernel: mem auto-init: stack:off, heap alloc:off, heap free:off
Jul 11 11:56:38 hub-gm kernel: Memory: 1029684K/1048576K available (6144K kernel code, 189K rwdata, 800K rodata, 1024K init
Jul 11 11:56:38 hub-gm kernel: SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=2, Nodes=1
Jul 11 11:56:38 hub-gm kernel: rcu: Hierarchical RCU implementation.
Jul 11 11:56:38 hub-gm kernel: rcu: RCU calculated value of scheduler-enlistment delay is 100 jiffies.
Jul 11 11:56:38 hub-gm kernel: NR_IRQS: 16, nr_irqs: 16, preallocated irq: 16
Jul 11 11:56:38 hub-gm kernel: GIC: Using split EOI/Deactivate mode
Jul 11 11:56:38 hub-gm kernel: arch_timer: cp15 timer(s) running at 8.00MHz (phys).
```

Monitoring > Journal (example)

Click **Download** to save the displayed messages as a TXT file.

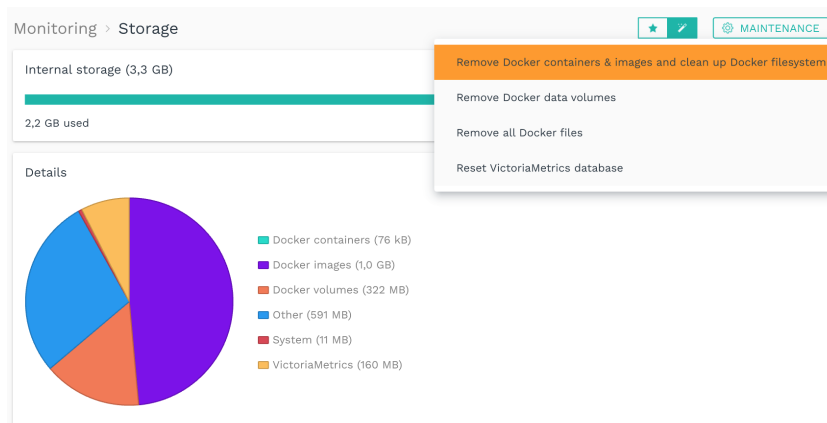
- **Storage:** Get an overview of the utilization of the internal storage as well as a breakdown into individual parts/components/areas and perform maintenance on the storage.



Monitoring > Storage, in “Advanced” viewing mode (example)

3.11.1. Storage maintenance

1. On the **Monitoring > Storage** page, switch to the **Advanced** viewing mode.
2. Click on the **Maintenance** button.



Functions for storage maintenance (first entry selected)

The following maintenance options are available:

- a. **Remove Docker containers and images and clean up Docker file system:** All settings and data such as the Grafana dashboards or the Node-RED flows are retained. All Docker containers are removed and then have to be reinstalled.
 - b. **Remove Docker data volume:** All settings and data such as the Grafana dashboards or the Node-RED flows are deleted from the containers (reset to factory defaults). All Docker containers will be retained.
 - c. **Remove all Docker files:** All settings and data, as well as the Docker containers, will be removed. The Docker containers then have to be reinstalled.
 - d. **Reset VictoriaMetrics database:** The database memory is cleared.
3. Confirm your selection with **Yes**;
– or –

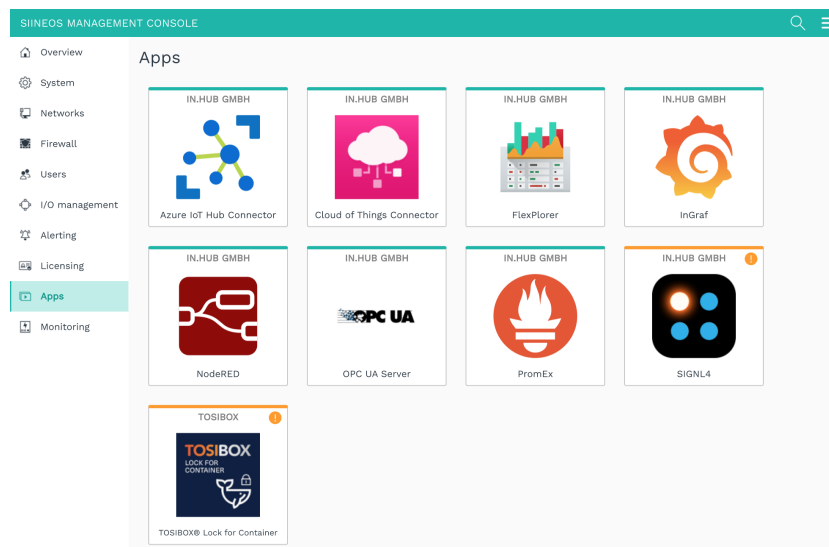
click on **No** if you want to reconsider your selection.

- If you want to see a detailed view of how the storage is composed, click on a colour field in the pie chart.

3.12. Opening and managing apps

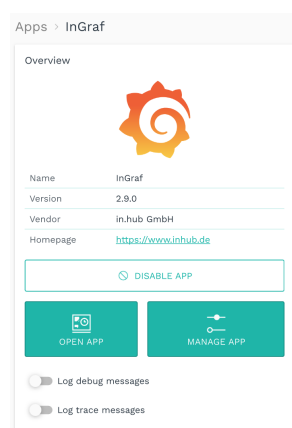
On the **Apps** page, you will find various applications that you can use to set up communication interfaces, data visualization or cloud connections, for example. How many apps are displayed on this page depends on which licences you have purchased.

Apps that do not have a valid licence or whose licence has expired are identified in the view (orange bar and exclamation mark).



“Apps” page (example)

- Open the desired app by clicking on the tile.
A window opens from which you can activate, open and manage the app.



- Additional settings are available in **Advanced** viewing mode:
 - Log debug messages:** Messages from the SIINEOS management service are logged in the system journal to help in.hub with troubleshooting.

- **Log trace messages:** Activate this function if detailed calls of system functions and the parameters used by the various apps are to be logged.

**NOTE**

Do not use these functions during production – performance could be impaired.

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

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

3. To start an app, click on **Enable app**.
4. To view or change app settings, click on **Manage app**.
Learn how to manage and configure apps in the chapter [Managing apps \[105\]](#).
5. Once the app has been activated, click on **Open app**.
The app will then open in a new window or tab (depending on browser settings).
If it is an external app, such as Grafana, you will be taken to the login page. Make sure that you have created a user account beforehand.

**TIP**

For many entries, you can search within the list. Click on the magnifying glass at top right  and enter the username you are looking for.

3.13. Managing licences

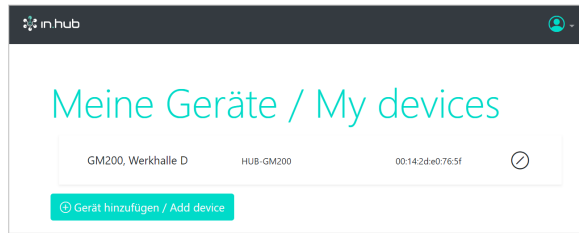
With every new SIINEOS-enabled in.hub device you purchase, you will automatically receive a SIINEOS licence for 3 years. You can update SIINEOS as often as you like during the licence period and install the latest version on the device.

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

If you need an app licence or want to extend one, please refer to the relevant User Manual.

3.13.1. Requesting a voucher and activating a software licence

1. Please contact service@inhub.de and let us know the term for which you would like to purchase the licence.
SIINEOS licences can be purchased for 1 year or 3 years.
You can activate the software licence with the voucher you receive from us.
2. Navigate to the website <https://apps.inhub.de/> and register or log on if you are already registered.



My devices (example)

3. If you want to extend a software licence, click on the device on which the software licence is to be renewed under **My devices**;
– or –
if you want to activate the software licence for a new device, click on **Add device**.

Gerät hinzufügen / Add device

Name*

Gerätetyp / Device type*

HUB-GM200
▼

MAC-Adresse*

Abbrechen / Cancel

Hinzufügen / Add

Add device

4. Enter the **Name** of the device, select the **Device Type** and enter the MAC address of the device.
The MAC address can be found via **SIINEOS > Networks > Ethernet 1**.
NOTE: Only the MAC address of Ethernet 1 is recognized and accepted.
5. Click on **Add**.
The **License activation** page opens:

Lizenfreischaltung / 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

Abbrechen / Cancel Weiter / Continue

License activation

6. Copy the name of the voucher you received from in.hub into the **Voucher** field.
7. Click on **Next**.
The information stored in the voucher, such as the term, product and validity, etc., will be displayed.

Lizenfreischaltung / 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

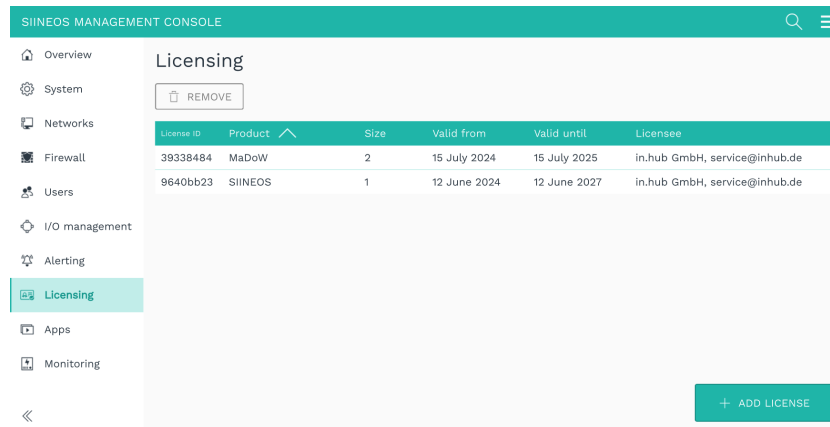
Abbrechen / Cancel Zurück / Back Lizenz generieren / Generate license

Voucher information (example: Activation of a SIINEOS licence valid for 3 years)

8. Check the details, especially whether the requested licence term matches the term specified here.
9. If the details are correct, click on Generate license.
The licence file is downloaded automatically.

3.13.2. Adding a licence file to SIINEOS

1. In SIINEOS, navigate to **Licensing**.
In the list, you will find all software licences that you have purchased and uploaded.



“Licensing” page (example)

2. Click on **Add license**.
3. Select the licence file from your file directory and click on **OK**.
The licence is added to the list. From that point on, you can implement updates again or return to using a blocked app.
4. To remove a licence again – because it has become invalid, for example – select the licence ID and click on **Remove**.
This will not delete the licence file itself, but only remove it from the list.



NOTE

Make sure that the system time of your device is correctly set and/or synchronized. Otherwise, the licence-file upload may fail.

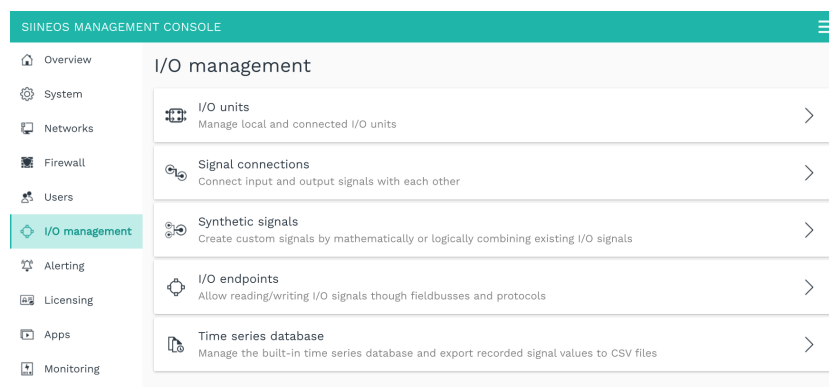
4. I/O management

You can connect a variety of external peripheral devices to one in.hub gateway, such as sensors, Modbus clients or other in.hub modules.

You configure the interfaces and signals from the peripheral devices so that measurements are output according to your requirements.

You can perform the following tasks on the **I/O management** page:

- Create I/O units, manage them and configure their interfaces.
[Creating I/O units \[54\]](#)
- Connect input and output signals with each other to trigger actions when signal values or measurements fall outside a defined range.
[Configuring signal connections \[95\]](#)
- Combine signals from the I/O units with each other to generate new, synthetic signals.
[Creating synthetic signals \[97\]](#)
- Allow the reading and/or writing of I/O signals via fieldbuses and protocols
[Configure I/O endpoints \[100\]](#)
- Manage the built-in time series database and export the recorded signal values as a CSV file
[Export time series database \[102\]](#)



“I/O management” page



TIP

Visit the in.hub community regularly at <https://community.inhub.de>. There, you will find workflows, answers regarding tricky SIINEOS use cases and helpful practical tips. Or you can ask your own questions if you need help setting up.

4.1. Working with I/O management

If you use I/O management to create devices or clients and/or to configure signals and/or signal connections, there are a number of functions that can support you in your daily work. These include, for example, the sorting and filtering of long lists or the saving and reuse of settings that you have made for a specific I/O unit. These tools are presented in the next chapter.

4.1.1. Filtering I/O units and reading information

If a large number of devices appears on the **I/O units** page, it can be helpful to filter them. The following filters are available:



Filter criteria (the “Connected” filter is currently applied)

The following rules apply to the filtering of entries:

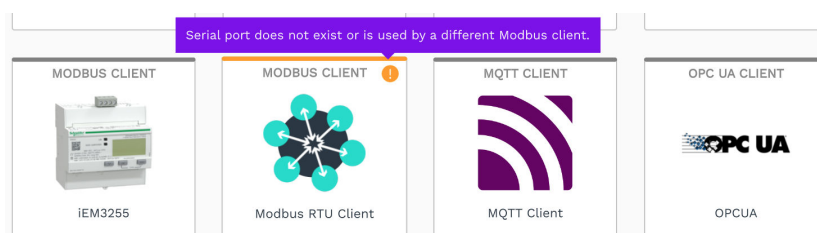
- An I/O unit can either be connected – i.e. the device is physically connected or the underlying network connection is established (e.g. to the MQTT broker or OPC UA server) – or disconnected.
- An I/O unit can either be enabled or disabled. This is done in the general settings for the unit.
- For example,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

Setting filters

1. On the **I/O management** start page, click a filter in the upper right corner to apply it. The filter changes its colour to turquoise.
2. Click on the filter again to deselect it. The filter changes its colour to grey.

Reading information

- Move the mouse over a tile. Further information on the I/O unit created is displayed.
- In cases of error messages, a symbol is displayed in the upper right corner. You can find more information about this error message in the tooltip.

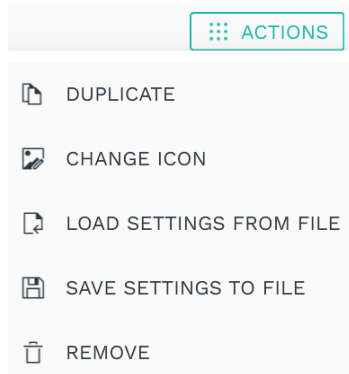


Error message for the “Modbus client” I/O unit (example)

4.1.2. Using the “Actions” menu

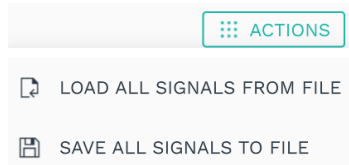
In I/O management, the **Actions** menu is also available for the device settings of the I/O units and for synthetic signals. This allows you to save the settings you have made so that you can reuse them elsewhere or you can import entries that have already been saved to the current device.

1. Open an I/O unit and click on **Actions**;



– or –

open the list of synthetic signals and click on **Actions**.



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 labelled with the suffix “copy”. You can now edit this I/O unit according to your requirements.
Change icon (image for an I/O unit)	A dialogue will appear, in which you can upload the new image. 1. Click in the Image file input field and select the new image in PNG format with a maximum file size of 128 kB from your local data directory. 2. Click on Upload and update. 3. If you want to restore the original image, click on Reset to default. 4. Confirm with OK. The image will then have been replaced.
Load settings from file	This allows you to apply already-saved settings to the I/O unit. Your local data directory will open.

	1. Select the JSON file with the settings to upload it.
Save settings to file	Depending on your system, a file storage dialogue will open or the JSON file will be automatically downloaded to your download folder.
Remove	1. Confirm with Yes . The unit has now been removed.
Load all signals from file	This allows you to load all previously saved signals into the list. Your local data directory will open. 1. Select the JSON file with the settings to upload it.
Save all signals to file	All synthetic signals and their settings are saved in a JSON file and downloaded immediately.

4.1.3. Sorting lists and reading information

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

I/O management > I/O units > GM200-Zentrallager > Signals

EDIT QUICK EDIT

☐	Identifier ^	Name	Group	Type	Value
☐	IO1	Digital Input 1		BOOL	1,0
☐	IO2	Temperatur Lagerplatz 5		DOUBLE	-20,0 °C
☐	IO3	Vibration		DOUBLE	8106,00 Hz
☐	IO4	Energie		DOUBLE	4494 W
☐	IO5	io5		BOOL	0
☐	IO6	io6		BOOL	0
☐	LED_GREEN	Green LED		BOOL	0
☐	LED_RED	Red LED		BOOL	0

List view of HUB-GM200 signals (example)

1. Open an I/O unit and go to the overview of signals;
– or –
on the **I/O management** start page, click on **Signal connections**;
– or –
on the **I/O management** start page, click on **Synthetic signals**.
A list view will be displayed showing all signals or connections.
2. To sort them, click on the header of a table column.
You can sort alphabetically forwards (A–Z) or alphabetically backwards (Z–A).
3. You can get information about the statuses of a signal or signal connection by noting the following icons:



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

-  Signal / signal connection is activated
-  Signal / 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 connected to an analogue input)



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

4.1.4. Editing, duplicating or removing list entries

Various buttons are available in each list view for editing signals, signal connections and synthetic signals.

I/O management > I/O units > TBEN-Modul S2-4AI > Signals

EDIT QUICK EDIT

☐	Identifier ^	Name	Group	Type	Value
☐	 	CHANNEL1	Analog input channel 1	INT16	0
☐	 	CHANNEL2	Analog input channel 2	INT16	0
☐	 	CHANNEL3	Analog input channel 3	INT16	0
☐	 	CHANNEL4	Analog input channel 4	INT16	0

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** start page, click on **Signal connections**;
– or –
on the **I/O management** start page, click on **Synthetic signals**.
A list view will be displayed showing all signals or connections.

2. Select one of the following buttons:

Edit	1. Select an entry and click on Edit ; – or – double-click on the entry you want to edit.
-------------	--

	This will either take you back to the setup wizard or to the signal settings.
Duplicate	1. Select a list entry and click on 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 permanently preconfigured signals or channels.
Remove	1. Select the signal using the checkbox; – or – select the signal connection. 2. Click on Remove. A message will be displayed asking whether 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 on Edit signal properties. A window opens in which you will find three tabs. 2. Enable and configure the synthetic signal on the Signal settings tab. 3. On the Signal processing tab, you can specify how the signal value is to be processed. You can find out more at Configuring the signal processing steps [92]. 4. Click on Save. 5. On the Measurement modelling tab, you specify how the measurements are to be visualized. You can find out more at Measurement modelling [93]. 6. Finally, click on Save & close.
Reset (only in “Synthetic signals”)	Resets an applied counter (Infinite counter or Resettable counter). 1. Select a synthetic signal and click on Reset. The counter will be reset.
Quick edit (only in “I/O unit > Signals”)	1. If you want to edit several signals at the same time, select the signals using the checkbox and then click on Quick edit. 2. Select one of the four actions to be applied to all selected signals: • Enable/disable: Enable or disable several signals at once.

	• Group: Assign a common group name. • Data series set: Assign a common name for the data series set. This means that all signals with the same data series set are displayed in FlexPlover under Live charts in a common chart, so that the signal values from different devices/sensors can be compared directly in live operation. • Sampling interval: Specify 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: Specify the number of decimal places. • Unit: Specify the unit. A dialogue window will open. 3. Enter the parameter required by the selected quick tool (e.g. the group name or number of decimal places). 4. Finally, click on Save & close.
--	--

4.1.5. Searching for entries

The search function is available in all list views. In **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 will be transferred directly into the search field at top right and the hits will be displayed dynamically in the list.



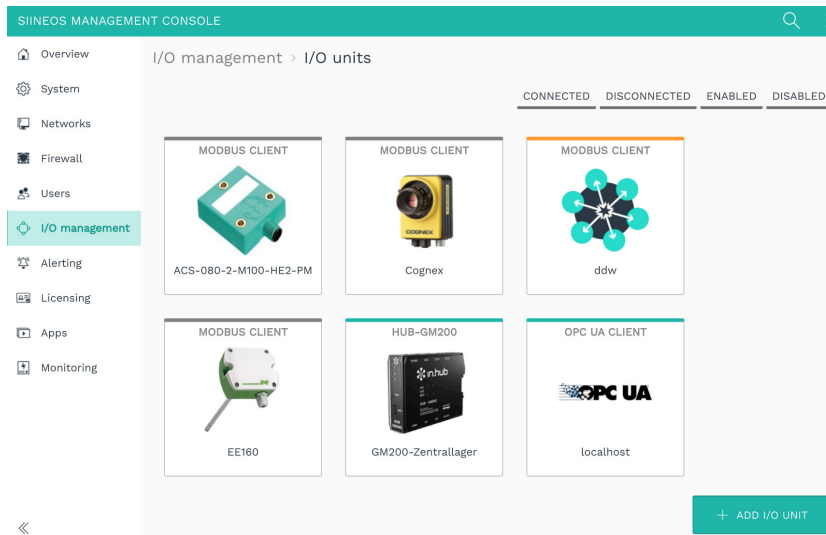
You can enter upper- or lower-case letters and numbers.

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

4.2. Creating I/O units

If you have selected the **I/O units** option on the **I/O management** page, you can now set up your peripheral devices. Each device has its own settings and parameters, which is why the following chapters describe how to set up each I/O unit separately.

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



I/O management > I/O units (example)

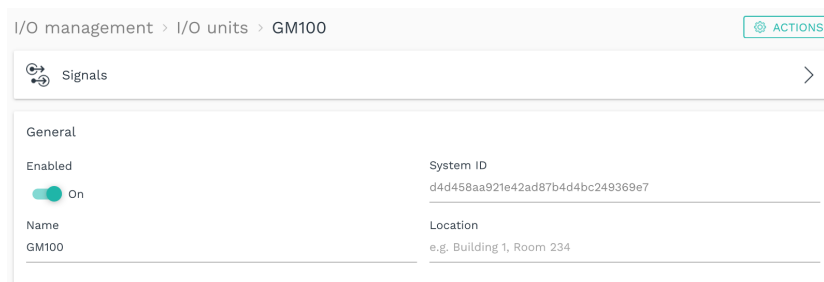
4.2.1. Adding a HUB-GM100



NOTE

This I/O unit refers to the local gateway on which you are currently located and allows you to access signals on the local interfaces.

1. On the **I/O management** start page, select **I/O units**.
2. Click on **Add I/O unit**.
3. Select **HUB-GM100** as the type.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click on **Finish** to add the I/O unit.
A page will open where you can configure the settings for the unit.



Device settings for the HUB-GM100 (example)

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

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

7. Click on **Signals**.

The signals for all channels of the HUB-GM100 have already been created.

I/O management > I/O units > GM100 > Signals

[EDIT](#) [QUICK EDIT](#)

☐	Identifier ^	Name	Group	Type	Value
☐	AIN1	Analog input 1		DOUBLE	0 mA
☐	AIN2	Analog input 2		DOUBLE	0 mA
☐	DIO1	Drehzahlsensor		BOOL	3
☐	DIO2	Ausgang		BOOL	1
☐	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	0 %
☐	SYSTEMP	System Temperature		DOUBLE	0 °C

Signals for the HUB-GM100 (example)

8. Select the signal you want to configure.

A window opens in which 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: ☐ Off Sampling interval [ms]: 1000

Record signal values: ☒ On Recording interval [s]: 60

Use custom identifier: ☐ Off Custom identifier: AIN1

Details

Mode: 4...20 mA

“Signal settings” tab in “Advanced” viewing mode

9. Enable and configure the interface on the **Signal settings** tab.

- Optional: Change the name of the interface.
- Set the **Enabled** slider to **On**.
- In the **Sampling interval** field, specify the interval 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.
- In the **Recording interval** field, enter the desired time interval for the recording (in seconds).

10. Additional settings are available in **Advanced** viewing mode:

- Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.

b. **Custom identifier:** Enter your own identifier name.

11. Depending on the type of signal selected, further entries may be necessary:

AIN (analogue input)	Under Mode , select the type of analogue interface for the connected sensor. Available options: 0–5 V / 0–10 V / 0–20 V / 4–20 mA.
DIO (digital input/output)	Under Mode , specify whether that interface is to function as an input or output. - You have selected Input: To continuously 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. - You have selected Output: Under Default state, set the slider to On if a positive voltage is to be output at the digital output.
LED	Specify whether the LED should be switched off or on in the Default state .
Relay	Specify whether the relay should be switched off or on in the Default state .

12. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).

13. Click on **Save**.

14. On the **Measurement modelling** tab, you specify how the measurements are to be visualized.

You can find out more at [Measurement modelling \[93\]](#).

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

4.2.2. Adding a HUB-GM200



NOTE

This I/O unit refers to the local gateway on which you are currently located and allows you to access signals on the local interfaces.

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

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

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

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

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

- Click on **Finish** to add the I/O unit.

A page will open where you can configure the settings for the unit.

I/O management > I/O units > GM200-Zentrallager ACTIONS

Signals >

General

Enabled	System ID
☒ On	6b862d3e74064a28b46727a082e8876e
Name	Location
GM200-Zentrallager	e.g. Building 1, Room 234

Device settings for the HUB-GM200 (example)

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

- Optional: Enter the **Location**.

- Click on **Signals**.

The signals for all channels of the HUB-GM200 have already been created.

I/O management > I/O units > GM200-Zentrallager > Signals

EDIT QUICK EDIT

☐	Identifier	Name	Group	Type	Value
☐	BP_POWER_SUPPLY	Backplane bus power supply		BOOL	1
☐	IO1	Stückzahlzähler		BOOL	0,0
☐	IO2	Feuchte		BOOL	43,4
☐	IO3	Vibration		BOOL	1,00
☐	IO4	Roboterstrom		DOUBLE	262 kWh
☐	IO5	Spannungsversorgung EE150		BOOL	1
☐	IO6	Io6		BOOL	1
☐	LED_GREEN	Red LED		BOOL	0
☐	LED_RED	Green LED		BOOL	0
☐	RS485_POWER_SUPPLY	RS485 power supply		BOOL	0

Signals for the HUB-GM200 (example)

- Select the signal you want to configure.

A window opens in which you will find three tabs.

I/O management > I/O units > GM200-Zentrallager > Signals > Temperatur Lagerplatz 5 ★ ✎

SIGNAL SETTINGS **SIGNAL PROCESSING** **MEASUREMENT MODELLING**

General

Name	System ID
Temperatur Lagerplatz 5	io2
Enabled	Sampling interval [ms]
☒ On	- 1000 +
Record signal values	Recording interval [s]
☒ On	- 60 +

Details

Mode

Analog input 4...20 mA

“Signal settings” tab (example)

9. Enable and configure the interface on the **Signal settings** tab.
 - a. Optional: Change the name of the interface.
 - b. Set the **Enabled** slider to **On**.
 - c. In the **Sampling interval** field, specify the interval at which the signal is to be sampled (in milliseconds).
 - d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).
10. Additional settings are available in **Advanced** viewing mode:
 - a. **Use custom identifiers**: Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier**: Enter your own identifier name.
 - c. **Calibrate to 0 mA** button: Calibrate the analogue input so that the current analogue value is 0 mA.
 - d. **Reset calibration** button: This resets the calibration of the analogue input to 0 mA.
11. Depending on the type of signal and mode selected, further entries may be necessary under **Details**:

Selection as an Analogue input	Under Mode , select the type of analogue interface for the connected sensor. Available options: 0–10 V and 4–20 mA .
Selection as a Digital input	To continuously 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 .
Selection as a Digital output	Under Default state , select which voltage should be output at the interface. Available options are Off (0 V) and On (24 V) .
LED	Specify whether the LED should be switched off or on in the Default state .
Power supply	Specify whether the power supply via the backplane bus or the RS485 interface should be switched on or off in the Default state .

12. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
13. Click on **Save**.
14. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).

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

4.2.3. Adding a HUB-EN100 module for energy monitoring

- 1. On the **I/O management** start page, select **I/O units**.
- 2. Click on **Add I/O unit**.
- 3. Select **HUB-EN100** as the type.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
- 4. Enter the **Name** for the I/O unit.
- 5. Click on **Finish** to add the I/O unit.
A page will open where you can configure the settings for the unit.

I/O management > I/O units > HUB-EN100 Strommessung ACTIONS

Signals >

General

Enabled

On

System ID

c49ecd5a0b164ef5979c34b9b51cd61d

Name

HUB-EN100 Strommessung

Location

e.g. Building 1, Room 234

Communication settings

Backplane bus address

- 1 +

Device settings for the HUB-EN100 (example)

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

- 6. Optional: Enter the **Location**.
- 7. Click on **Signals**.
The signals for all channels of the HUB-EN100 have already been created.

I/O management > I/O units > HUB-EN100 Strommessung > Signals

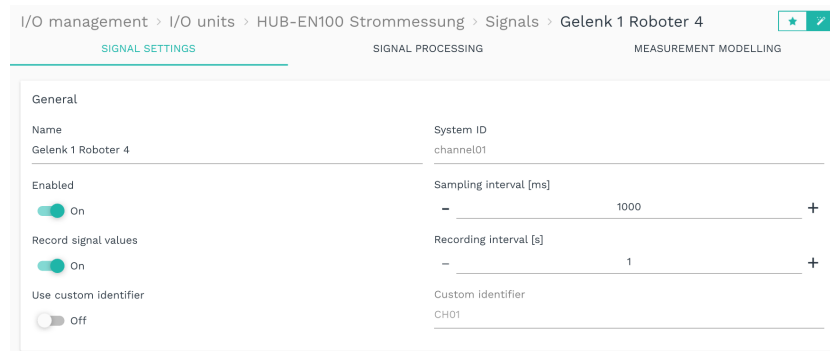
EDIT QUICK EDIT

☐	Identifier ^	Name	Group	Type	Value
☐	CH01	Gelenk 1 Roboter 4		DOUBLE	9,38 A
☐	CH02	Gelenk 2 Roboter 4		DOUBLE	1,00 A
☐	CH03	Channel 03		DOUBLE	0,00 A
☐	CH04	Channel 04		DOUBLE	0,00 A
☐	CH05	Channel 05		DOUBLE	0,00 A
☐	CH06	Channel 06		DOUBLE	0,00 A
☐	CH07	Channel 07		DOUBLE	0,00 A
☐	CH08	Channel 08		DOUBLE	0,00 A
☐	CH09	Channel 09		DOUBLE	0,00 A
☐	CH10	Channel 10		DOUBLE	0,00 A
☐	CH11	Channel 11		DOUBLE	0,00 A
☐	CH12	Channel 12		DOUBLE	0,00 A

Signals for the HUB-EN100 (example)

8. Select the signal you want to configure.

A window opens in which you will find three tabs.



“Signal settings” tab in “Advanced” viewing mode

9. Enable and configure the interface on the **Signal settings** tab.
 - a. Optional: Change the name of the interface.
 - b. Set the **Enabled** slider to **On**.
 - c. In the **Sampling interval** field, specify the interval at which the signal is to be sampled (in milliseconds).
 - d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).
10. Additional settings are available in **Advanced** viewing mode:
 - a. **Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier:** Enter your own identifier name.
11. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
12. Click on **Save**.
13. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).
14. Finally, click on **Save & close**.

4.2.4. Establishing communication with the HUB-VM102 via a network

The procedure described here applies if you integrate a HUB-VM102 via network (LAN). For data communication via the backplane bus, please create a Modbus client of the RTU type as usual, see [Adding a Modbus client of the RTU type \[66\]](#).

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

2. Click on **Add I/O unit**.
3. Select **HUB-VM102** as the type.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click on **Finish** to add the I/O unit.
A page will open where you can configure the settings for the unit.

Device settings for the HUB-VM102 in “Advanced” viewing mode (example)

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

6. Optional: Enter the **Location**.
7. Enter the IP address of the HUB-VM102.
Each HUB-VM102 has a factory-set IP address **192.168.1.200**, which is always the same.
8. If you want to use more than one HUB-VM102 in the network, you must change the IP address(-es) of the other devices.
To do this, open the I/O units one after the other and give each HUB-VM102 a different IP address:
 - a. Switch to **Advanced** viewing mode.
 - b. Click on the **Change VM102 network settings** button.

- c. Enter a **New IP address**, a **New subnet mask** and a **New gateway address** and confirm with **OK**.
The new **Subnet mask** and **Gateway address** will be displayed in the device settings of the HUB-VM102 for your information.
- d. In the **Request timeout [ms]** field, define after how many milliseconds without a response a request should be resent or discarded.
- e. In the **Request retry count** field, enter how often a request should be sent if no response is received. After the entered number of attempts, the request is finally cancelled.

9. Click on **Signals**.

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

I/O management > I/O units > HUB-VM102 in.hub Fabrik > 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
☐	PEAK_S2	Sensor 2 Peak		DOUBLE	0,0 m/s²
☐	RMS_S1	Sensor 1 RMS		DOUBLE	0,0 m/s²
☐	RMS_S2	Sensor 2 RMS		DOUBLE	0,0 m/s²
☐	VOLT_S1	Sensor 1 Voltage		DOUBLE	0,0 V
☐	VOLT_S2	Sensor 2 Voltage		DOUBLE	0,0 V

Signals for the HUB-VM102 (example)

10. Select the signal you want to configure.

A window opens in which you will find three tabs.

I/O management > I/O units > HUB-VM102 in.hub Fabrik > Signals > Digital Input 1 Frequency

SIGNAL SETTINGS | SIGNAL PROCESSING | MEASUREMENT MODELLING

General

Name
Digital Input 1 Frequency

Enabled
☒ On

Record signal values
☒ On

Use custom identifier
☐ Off

System ID
freq_din1

Sampling interval [ms]
- 1000 +

Recording interval [s]
- 60 +

Custom identifier
FREQ_DIN1

“Signal settings” tab in “Advanced” viewing mode

11. Enable and configure the interface on the **Signal settings** tab.
 - a. Optional: Change the name of the interface.
 - b. Set the **Enabled** slider to **On**.
 - c. In the **Sampling interval** field, specify the interval at which the signal is to be sampled (in milliseconds).
 - d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).

12. Additional settings are available in **Advanced** viewing mode:
 - a. **Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier:** Enter your own identifier name.
13. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
14. Click on **Save**.
15. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).
16. Finally, click on **Save & close**.

4.2.5. Adding a Sensirion SPS30 particle sensor

1. On the **I/O management** start page, select **I/O units**.
2. Click on **Add I/O unit**.
3. Select **Sensirion SPS30** as the type.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click on **Finish** to add the I/O unit.
A page will open where you can configure the settings for the unit.

I/O management > I/O units > Partikelsensor ACTIONS

Signals >

General

Enabled System ID
☐ Off ba8845888fad4ecb8af3a1db63d8baf1

Name Location
 Partikelsensor e.g. Building 1, Room 234

Sensirion SPS30

Interface
 None

Sampling interval
 — 1000 +

Device settings for the Sensirion SPS30 particle sensor (example)

The newly added I/O unit is automatically enabled. If you 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 out if you have also connected sensors. If several sensors are connected – via a USB hub, for example – they will be numbered in the sequence of their being connected to the USB hub.

8. In the **Sampling interval** field, specify the interval at which the signal is to be sampled (in milliseconds).

9. Click on **Signals**.

The signals for all measurements of the particle sensor have already been created.

I/O management > I/O units > Partikelsensor > Signals

EDIT QUICK EDIT

☐	Identifier ^	Name	Group	Type	Value
☐	MASS_PM1.0	Mass concentration PM1.0		DOUBLE	0,000 µg/m³
☐	MASS_PM10.0	Mass concentration PM10.0		DOUBLE	0,000 µg/m³
☐	MASS_PM2.5	Mass concentration PM2.5		DOUBLE	0,000 µg/m³
☐	MASS_PM4.0	Mass concentration PM4.0		DOUBLE	0,000 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
☐	TYPESIZE	Typical particle size		DOUBLE	0,0 µm

Signals for the Sensirion SPS30 particle sensor

10. Select the signal you want to configure.

A window opens in which you will find three tabs.

I/O management > I/O units > Partikelsensor > Signals > Mass concentration PM4.0

SIGNAL SETTINGS SIGNAL PROCESSING MEASUREMENT MODELLING

General

Name
Mass concentration PM4.0

System ID
massPM4_0

Enabled
☒ On

Record signal values
☒ On

Use custom identifier
☐ Off

Sampling interval [ms]
- 1000 +

Recording interval [s]
- 60 +

Custom identifier
MASS_PM4.0

“Signal settings” tab in “Advanced” viewing mode

11. Enable and configure the interface on the **Signal settings** tab.
 - a. Optional: Change the name of the interface.
 - b. Set the **Enabled** slider to **On**.
 - c. In the **Sampling interval** field, specify the interval at which the signal is to be sampled (in milliseconds).
 - d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).

12. Additional settings are available in **Advanced** viewing mode:
 - a. **Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier:** Enter your own identifier name.
13. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
14. Click on **Save**.
15. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).
16. Finally, click on **Save & close**.

4.2.6. Adding a Modbus client of the RTU type

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

Multiple Modbus clients (RTUs) can be created for both the built-in RS485 interface and the backplane bus via I/O management in order to communicate with multiple Modbus devices on the same bus.

IMPORTANT TO KNOW: The activated client with the lowest Modbus ID takes over the communication for all Modbus clients working on the same bus. If the client with the lowest Modbus ID is deactivated, the client with the next higher ID is used, etc. The settings therefore do not have to be synchronous, but should be, so that when the primary Modbus client is deactivated, the communication continues to work and the next higher Modbus client can take over.

If an RS485 or RS232 converter is connected via the external USB interface, more than one Modbus RTU client 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 appropriate Modbus ID must be set accordingly in the Modbus registers.

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

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

A page will open where you can configure the settings for the unit. The newly added I/O unit is automatically enabled. If you want to use it later, set the **Enabled** slider to **Off**.

Device settings for the Modbus RTU client in “Advanced” viewing mode (example)

6. Optional: Enter the **Location**.
 7. You can make further entries in the **Modbus client** section:
 - a. **Modbus type**: Select the **Modbus RTU** entry.
 - b. Under **Modbus ID**, enter the backplane bus ID, which is made up of the last three digits of the serial number of the in.hub device with which you want to communicate.
 The range defined by in.hub for the Modbus ID is between 1 and 100. Therefore, an ID cannot be 0 and cannot be greater than 100.
Example: The serial number is **13197240900021**. The backplane bus ID would be **21**.
 - c. The appropriate **Bus interface** must be selected for communication with the Modbus device; in most cases, this will be the **Built-in RS485 interface**. For I/O modules (such as the HUB-IO100 or HUB-EN200), select **Backplane bus**. A **Serial interface** is then required if an RS485 or RS232 converter is connected via the external USB interface.
-  **NOTE**
 When using serial interfaces, you must specify the **Serial port name**. This depends on the device and may need to be determined via SSH. Usually “ttyUSB0” is used, or in some cases “ttyACM0”.
- d. Complete all other input fields, such as **Baud rate** or **Parity**, according to the documentation of the connected device.
 8. If you want to use an already-created Modbus device profile to save time during setup, for example, click on **Import Modbus device profile** and select the file from your file directory.
 9. Additional settings are available in **Advanced** viewing mode:

- a. In the **Request timeout [ms]** field, define after how many milliseconds without a response a request should be resent or discarded.
 - b. In the **Request retry count** field, enter how often a request should be sent if no response is received. After the entered number of attempts, the request is finally cancelled.
 - c. 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 not 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.
 - d. In the **Waiting time between messages [ms]** field, specify how many milliseconds should be waited between two consecutive Modbus messages. The default setting is **-1**, i.e. the waiting time between messages is calculated automatically based on the baud rate.
10. Click on **Save**.
 11. Click on **Signals**.

I/O management > I/O units > iEM3255 via Modbus RTU > Signals

EDIT DUPLICATE REMOVE QUICK EDIT

☐	Identifier ^	Name	Group	Type	Value
☐	HOLDING0	Holding register		UINT16	0
☐	HOLDING2402	Z-Axis RMS Velocity (mm/sec) 10Hz - 1kHz		UINT16	0,00 mm/s
☐	HOLDING2403	xy-Axis RMS Velocity (mm/sec)		UINT16	0,00 mm/s

Signals for the Modbus RTU client (initially, no signals are predefined)

12. Click on **Add I/O unit**.
- A window opens in which you will find three tabs.

I/O management > I/O units > iEM3255 via Modbus RTU > Signals > Holding register

SIGNAL SETTINGS SIGNAL PROCESSING MEASUREMENT MODELLING

General

Name: Holding register

System ID: 51b5eb8305304a368536f543c05c95a4

Enabled: ☒ On

Sampling interval [ms]: 1000

Record signal values: ☒ On

Recording interval [s]: 60

Use custom identifier: ☐ Off

Custom identifier: HOLDING0

Details

Register type: Holding register (FC 03)

Address: 0

Data type: Unsigned 16 bit integer

Register count: 1

Byte order: Most significant byte first (big endian)

Register order: Most significant register first

I/O mode: Read

Modbus ID: 0

“Signal settings” tab in “Advanced” viewing mode

13. Enable and configure the interface on the **Signal settings** tab.
 - a. Optional: Change the name of the interface.
 - b. Set the **Enabled** slider to **On**.
 - c. In the **Sampling interval** field, specify the interval 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 output value** is written on starting up and each time a change is made. If the register is connected to a source signal via a signal connection, the register is written each time the source signal changes.

 - d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).
14. Additional settings are available in **Advanced** viewing mode:
 - a. **Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier:** Enter your own identifier name.
15. Further entries are required in the **Details** section.
 - a. Depending on the selected register type, different entries can be made as to whether to read from the register or whether and what should be written to the register. Please also note the tooltips.
 - b. 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 means that the global setting of the Modbus Client (see point 8) is ignored and the Modbus ID entered here is used for this register instead (point to point). Otherwise, leave the default value (**0**).
 - c. Complete all other parameters according to the documentation of the connected device.
16. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
17. Click on **Save**.
18. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).
19. Finally, click on **Save & close**.

4.2.7. Adding a Modbus client of the TCP type

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

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

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

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

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

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

A page will open where you can configure the settings for the unit.

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

The screenshot shows the configuration page for a Modbus TCP client. The breadcrumb navigation at the top reads 'I/O management > I/O units > Modbus TCP'. There are icons for a star, a pencil, and an 'ACTIONS' button. Below the navigation bar is a 'Signals' section with a right arrow. The main configuration area is divided into three sections: 'General', 'Modbus client', and 'TCP packet flow optimization'. In the 'General' section, the 'Enabled' toggle is 'On', the 'System ID' is '50a237459eba4f82ba9191c5ffe5d04', the 'Name' is 'Modbus TCP', and the 'Location' is 'e.g. Building 1, Room 234'. In the 'Modbus client' section, the 'Modbus type' is 'Modbus TCP', the 'Modbus ID' is '1', and the 'Server port' is '502'. In the 'TCP packet flow optimization' section, the 'Request timeout [ms]' is '100' and the 'Request retry count' is '0'. There is an 'IMPORT MODBUS DEVICE PROFILE' button at the bottom.

Device settings for the Modbus TCP client in “Advanced” viewing mode (example)

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

7. You can make further entries in the **Modbus client** section:

a. **Modbus type:** Select the **Modbus TCP** entry.

b. Under **Modbus ID**, enter the backplane bus ID, which is made up of the last three digits of the serial number of the in.hub device with which you want to communicate.

The range defined by in.hub for the Modbus ID is between 1 and 100. Therefore, an ID cannot be 0 and cannot be greater than 100.

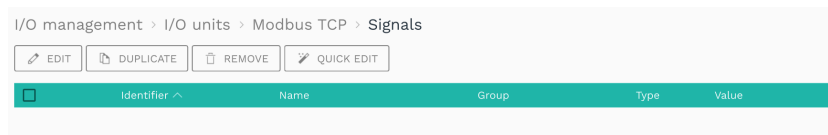
Example: The serial number is **13197240900021**. The backplane bus ID would be **21**.

c. Enter the **Server address** and **Server port** of the Modbus TCP server.

d. Under **TCP packet flow optimization**, you can select the sequence and compilation for sending Modbus queries. **High efficiency** is selected by default, i.e. the sending of requests and their combination into larger TCP packets take place in parallel.

TIP: In the event of communication issues with the Modbus device, you can try switching to either **Low latency** as the next-best option or **Half-duplex** as the slowest option (with the best compatibility).

8. If you want to use an already-created Modbus device profile to save time during setup, for example, click on **Import Modbus device profile** and select the file from your file directory.
9. Additional settings are available in **Advanced** viewing mode:
 - a. In the **Request timeout [ms]** field, define after how many milliseconds without a response a request should be resent or discarded.
 - b. In the **Request retry count** field, enter how often a request should be sent if no response is received. After the entered number of attempts, the request is finally cancelled.
10. Click on **Save**.
11. Click on **Signals**.



Initially, no signals are predefined.

12. Click on **Add I/O unit**.
A window opens in which you will find three tabs.

“Signal settings” tab in “Advanced” viewing mode

13. Enable and configure the interface on the **Signal settings** tab.
 - a. Optional: Change the name of the interface.

- b. Set the **Enabled** slider to **On**.
- c. In the **Sampling interval** field, specify the interval 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 output value** is written on starting up and each time a change is made. If the register is connected to a source signal via a signal connection, the register is written each time the source signal changes.

- d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).
14. Additional settings are available in **Advanced** viewing mode:
- a. **Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier:** Enter your own identifier name.
15. Further entries are required in the **Details** section.
- a. Depending on the selected register type, different entries can be made as to whether to read from the register or whether and what should be written to the register. Please also note the tooltips.
 - b. Complete all other parameters according to the documentation of the connected device.
16. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
17. Click on **Save**.
18. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).
19. Finally, click on **Save & close**.

4.2.8. Adding an MQTT client

1. On the **I/O management** start page, select **I/O units**.
2. Click on **Add I/O unit**.
3. Select **MQTT client** as the type.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
4. Enter the **Name** for the I/O unit.

- Click on **Finish** to add the I/O unit.

A page will open where you can configure the settings for the unit.

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

The screenshot shows the 'MQTT-Client' configuration page. At the top, there's a breadcrumb 'I/O management > I/O units > MQTT-Client' and an 'ACTIONS' button. Below is a 'Signals' section with a right arrow. The main configuration is divided into two sections: 'General' and 'MQTT client'.

General section:

- Enabled:** A toggle switch is set to 'On'.
- System ID:** 99fe1d94d6854af282137e4c5693ba51
- Name:** MQTT-Client
- Location:** e.g. Building 1, Room 234

MQTT client section:

- Broker address:** localhost
- Broker port:** 1988
- Username:** (empty field)
- Password:** (empty field)
- Client ID:** hub-gm200-00142de082eb
- Protocol version:** 3.1.1 (selected from a dropdown)
- Encrypt connection via TLS:** A toggle switch is set to 'Off'.
- Connect via WebSocket:** A toggle switch is set to 'On'.
- Connection keepalive interval [s]:** 30

Device settings for the MQTT client in “Advanced” viewing mode (example)

- Optional: Enter the **Location**.
- You can make further entries in the **MQTT client** section:
 - Enter the **broker address** and **broker port**.
NOTE: These parameters must be known to you from your MQTT network.
 - If authentication is required to connect 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's CA must be stored under **System > Security & encryption**.
 - Optional: In Client ID, you can specify a name that the client uses to log in to the MQTT broker.
 - In **Connection keepalive interval**, you can enter how often the MQTT client sends so-called keepalive messages to the MQTT broker to inform it that the client is still active and the network connection is OK. If the MQTT broker does not receive any messages within the interval, it closes the connection to the MQTT client.
 - In the **Protocol version** drop-down list, you can select the MQTT version to be used for communication.
- Additional settings are available in **Advanced** viewing mode:
 - Set the **Connect via WebSocket** slider to **On** if the MQTT broker only offers a connection via WebSockets.
 - Connection keepalive interval [s]:** Enter the interval, in seconds, after which a ping is used to check whether the connection has been established. If the broker does not respond, the connection is terminated and the MQTT client attempts to re-es-

establish the connection. This function is used to actively recognize a connection interruption.

9. Click on **Save**.

10. Click on **Signals**.

Initially, no signals are predefined.

11. Click on **Add I/O signal**.

A new window opens, in which you can select an existing object from the MQTT topics.

NOTE: Only topics published with retain flags or topics received since dialogue openings are displayed. Sporadically updated topics may not appear here, and the topic must be added with a **custom topic name**, i.e. the topic name must be known and manually entered.

Add MQTT topics

Root

Search topics

Name
☐ alerting
☐ apps
☐ device
☐ iounits
☐ licensing
☐ system
☐ vm102
☐ vmsys

Only topics with retained or recently published values are displayed here. If the desired topic is not shown, please use the button below to add a signal with a custom topic name.

“Add MQTT topics” window (example)

12. Select an MQTT topic and click on **Add**.

– or –

if you would like to create a new topic, click on **Add signal with custom topic name**.

A window opens in which you will find three tabs.

I/O management > I/O units > MQTT-Client > Signals > Unnamed MQTT topic

SIGNAL SETTINGS SIGNAL PROCESSING MEASUREMENT MODELLING

General

Name: Unnamed MQTT topic System ID: 91e5b63654f64764bba5c86a838884b

Enabled: ☒ On Sampling interval [ms]: 1000

Record signal values: ☒ On Recording interval [s]: 60

Details

Topic name: _____

Mode:
Subscribe (receive data from broker)

Data type:
Double

“Signal settings” tab in “Standard” viewing mode

13. Enable and configure the interface on the **Signal settings** tab.
 - a. Optional: Change the name of the interface.
 - b. Set the **Enabled** slider to **On**.
 - c. In the **Sampling interval** field, specify the interval at which the signal is to be sampled (in milliseconds).
 - d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).
14. Additional settings are available in **Advanced** viewing mode:
 - a. **Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier:** Enter your own identifier name.
15. Further entries are required in the **Details** section.
 - a. assign a **Topic name**.
 - b. In the **Mode** drop-down list, select whether you want to receive data from the broker (**Subscribe**) or send data to the broker (**Publish**) via the MQTT broker.
 - c. 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 is present in the MQTT topic 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.
 When selecting the **Boolean** data type, the topic value “true” or “false” becomes “1” or “0” in the signal.
 - d. 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.

16. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
17. Click on **Save**.
18. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).
19. Finally, click on **Save & close**.

4.2.9. Adding an OPC UA client

**TIP**

The community page at <https://community.inhub.de/> contains a sample workflow for how to connect two gateways using OPC UA.

1. On the **I/O management** start page, select **I/O units**.
2. Click on **Add I/O unit**.
3. Select **OPC UA client** as the type.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click on **Finish** to add the I/O unit.
A page will open where you can configure the settings for the unit.
The newly added I/O unit is automatically enabled. If you want to use it later, set the **Enabled** slider to **Off**.

I/O management > I/O units > OPCUA ACTIONS

Signals

General

Enabled

On

System ID

70fd92329dad42bfae3b6572d0801eb0

Name

OPCUA

Location

e.g. Building 1, Room 234

Basic settings

Security & encryption

Authentication

Server URL

opc.tcp://101.9.151:4840

Device settings for the OPC UA client (example)

6. Optional: Enter the **Location**.
7. You can enter the **Server URL** in the **Basic settings**.
8. You can make the following settings under **Security & encryption**:

- a. Under **Security mode**, you first specify whether messages between the gateway and OPC UA server should be unsecured, only signed or encrypted and signed.
- b. Then, under **Security policy**, select which encryption algorithm should be used. If you are unsure, you can start with the Basic algorithm and, if necessary, try whether the server also supports the two other, more modern encryption algorithms.
- c. If a security mode and a security policy are selected, you have further input fields:

Set the **Verify server certificate** slider to **On** if the server uses a specific certificate that “proves” the authenticity of the server. You must upload this certificate under **CA or server certificate** so that the clients cannot connect to any server. Alternatively, the certificate of the certification authority (CA) can be uploaded if the server certificate was issued by a CA.

The **Use trusted client certificate** slider is set to **On** by default. Depending on the server’s security settings, the server checks the authenticity of client certificates for connection encryption to prevent unknown clients from communicating with the server. To do this, a **Client certificate** must be uploaded and the **Private key** entered.

If the slider is deactivated, the internal default certificate of SIINEOS is automatically used. Therefore, only deactivate this function if the server accepts any self-signed client certificate.

NOTE: The settings on the OPC UA server are decisive. First, check the security level specified by the server before making any changes here.

9. You can select the following authentication methods under **Authentication**:
 - a. **Anonymous:** No authentication is required.
 - b. **Username and password:** On the OPC UA server, it is specified that authentication via user data is required. Enter the user data.
 - c. **Client certificate with private key:** On the OPC UA server, it is specified that a client-certified connection is to be used. The client certificate that you have uploaded under **Security & encryption** is used for authentication.
Use a separate client certificate for authentication: If a different client certificate is used, set the slider to **On**, upload the **Client certificate** and enter the **Private key**.
10. Click on **Save**.
11. Click on **Signals**.

I/O management > I/O units > OPCUA > Signals

 EDIT

 DUPLICATE

 REMOVE

 QUICK EDIT

☐	Identifier ▾	Name	Group	Type	Value
☐	 ns=2;s=StrommessmodulElektroverteller.CH01	Channel 01			0
☐	 ns=2;s=SPS30.NUMBER_PM0_5	Number concentration PM0.5			0
☐	 ns=2;s=Master_ModuLAIN1	Analog input 1			0

Signals for the OPC UA client (initially, no signals are predefined)

12. Click on **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

Root > Objects

Q Search nodes

☐	System name ^	Display name
☐	GM200-Zentrallager	GM200-Zentrallager
☐	MQTT-Client	MQTT-Client
☐	OPC UA Client	OPC UA Client
☐	Oliver	Oliver
☐	QE-POWER-T-PLUS-Lite-Version	QE-POWER-T-PLUS-Lite-Version
☐	Sensirion SPS30	Sensirion SPS30
☐	Server	Server
☐	Synthetic signals	Synthetic signals

CANCEL
ADD SIGNAL WITH CUSTOM NODE ID
+ ADD

“Add OPC UA node” window (example)

13. Select a node object and click on **Add**;

– or –

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

A window opens in which you will find three tabs.

I/O management > I/O units > OPC UA Client > Signals > Feuchte

SIGNAL SETTINGS SIGNAL PROCESSING MEASUREMENT MODELLING

General

Name: Feuchte System ID: 5f5441599f59439a988a756abcedfcb7

Enabled: ☒ On Sampling interval [ms]: 1000

Record signal values: ☒ On Recording interval [s]: 60

Use custom identifier: ☐ Off Custom identifier: ns=2;s=IO100.AIN2

Details

Node ID: ns=2;s=IO100.AIN2

Array index: -1

Timestamp source: Local device

“Signal settings” tab in “Advanced” viewing mode

14. Enable and configure the interface on the **Signal settings** tab.
- Optional: Change the name of the interface.
 - Set the **Enabled** slider to **On**.
 - In the **Sampling interval** field, specify the interval 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.
 - In the **Recording interval** field, enter the desired time interval for the recording (in seconds).

15. In the **Details** section, enter the **Node ID**.

**NOTE**

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

If an existing I/O signal has been recognized automatically, this field is filled in. If not, enter the complete node ID, e.g. “ns=2;s=Machine”.

16. Additional settings are available in **Advanced** viewing mode:
- Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.
 - Custom identifier:** Enter your own identifier name.
 - Array index:** If the object node contains a one-dimensional array, you can specify the index (starting at 0) of the element that is to be read as the signal value. For a non-array, the default value **-1** is entered.
 - Timestamp source:** Select the timestamp source that the signal uses for its own timestamp.

Local device: Timestamp of the local system of the time when the device received the value from the OPC UA server

Server timestamp: Timestamp of the time at which the OPC UA server obtained the value from its own data source

Value source timestamp: Timestamp of the data source of the OPC UA server, provided that the data source also provides a timestamp in addition to the actual value. This timestamp can be identical to the timestamp of the OPC UA server. However, it can also be the time of a measurement if, for example, a PLC connected via OPC UA or a device has read an input/register/variable.
17. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
18. Click on **Save**.
19. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).
20. Finally, click on **Save & close**.

4.2.10. Adding a TBEN-S1-8DIP module

- On the **I/O management** start page, select **I/O units**.
- Click on **Add I/O unit**.
- Select **TBEN-S1-8DIP** as the type.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
- Enter the **Name** for the I/O unit.

- Click on **Finish** to add the I/O unit.

A page will open where you can configure the settings for the unit.

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

I/O management > I/O units > TBEN-Modul S1-8DIP ACTIONS

Signals >

General
 Enabled
☐ Off

System ID
 fc32fc538fef4855b35c12c4ce2169a7

Name
 TBEN-Modul S1-8DIP

Location
 e.g. Building 1, Room 234

TBEN-S1-8DIP settings
 Module address
 192.168.100.1

Device settings for the TBEN-S1-8DIP module (example)

- Optional: Enter the **Location**.
- In the **Module address** input field, enter the hostname and IP address of the TBEN module with which a connection is to be established.
- Click on **Save**.
- Click on **Signals**.

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

I/O management > I/O units > TBEN-Modul S1-8DIP > Signals

EDIT QUICK EDIT

☐	Identifier ^	Name	Group	Type	Value
☐	DIN1	Digital input channel 1		UINT16	0
☐	DIN2	Digital input channel 2		UINT16	0
☐	DIN3	Digital input channel 3		UINT16	0
☐	DIN4	Digital input channel 4		UINT16	0
☐	DIN5	Digital input channel 5		UINT16	0
☐	DIN6	Digital input channel 6		UINT16	0
☐	DIN7	Digital input channel 7		UINT16	0
☐	DIN8	Digital input channel 8		UINT16	0

Signals for the TBEN-S1-8DIP module (initially, no signals are predefined)

- Select the signal you want to configure.
- A window opens in which you will find three tabs.

I/O management > I/O units > TBEN-Modul S1-8DIP > Signals > Digital input channel 1 ★ ✎

SIGNAL SETTINGS SIGNAL PROCESSING MEASUREMENT MODELLING

General
 Name
 Digital input channel 1

System ID
 din1

Enabled
☒ On

Record signal values
☒ On

Use custom identifier
☐ Off

Sampling interval [ms]
 - 1000 +

Recording interval [s]
 - 60 +

Custom identifier
 DIN1

“Signal settings” tab in “Advanced” viewing mode

- Enable and configure the interface on the **Signal settings** tab.

- a. Optional: Change the name of the interface.
 - b. Set the **Enabled** slider to **On**.
 - c. In the **Sampling interval** field, specify the interval at which the signal is to be sampled (in milliseconds).
 - d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).
12. Additional settings are available in **Advanced** viewing mode:
- a. **Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier:** Enter your own identifier name.
13. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
14. Click on **Save**.
15. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).
16. Finally, click on **Save & close**.

4.2.11. Adding a TBEN-S2-4AI module

1. On the **I/O management** start page, select **I/O units**.
2. Click on **Add I/O unit**.
3. Select **TBEN-S2-4AI** as the type.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click on **Finish** to add the I/O unit.
A page will open where you can configure the settings for the unit.
The newly added I/O unit is automatically enabled. If you want to use it later, set the **Enabled** slider to **Off**.

I/O management > I/O units > TBEN-Modul S2-4AI

ACTIONS

Signals

>

General

Enabled

Off

System ID

fc32fc536fef4855b35c12c4ce2159a7

Name

TBEN-Modul S2-4AI

Location

e.g. Building 1, Room 234

TBEN-S2-4AI settings

Module address

192.168.100.1

Device settings for the TBEN-S2-4AI module (example)

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

The signals for all analogue input channels have already been created.

I/O management > I/O units > TBEN-Modul S2-4AI > Signals

EDIT

QUICK EDIT

☐	Identifier ^	Name	Group	Type	Value
☐	CHANNEL1	Analog input channel 1		INT16	0
☐	CHANNEL2	Analog input channel 2		INT16	0
☐	CHANNEL3	Analog input channel 3		INT16	0
☐	CHANNEL4	Analog input channel 4		INT16	0

Signals for the TBEN-S2-4AI module

10. Select the signal you want to configure.
- A window opens in which you will find three tabs.

I/O management > I/O units > TBEN-Modul S2-4AI > 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

“Signal settings” tab in “Advanced” viewing mode

11. Enable and configure the interface on the **Signal settings** tab.
 - a. Optional: Change the name of the interface.
 - b. Set the **Enabled** slider to **On**.
 - c. In the **Sampling interval** field, specify the interval at which the signal is to be sampled (in milliseconds).
 - d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).
12. Additional settings are available in **Advanced** viewing mode:
 - a. **Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier:** Enter your own identifier name.
13. The **Details** section shows the parameters read in from 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 in fact be written back to the module. The changes will only take effect if you then click on **Save**.

14. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
15. Click on **Save**.
16. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).
17. Finally, click on **Save & close**.

4.2.12. Adding an S7 PLC client

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

1. On the **I/O management** start page, select **I/O units**.
2. Click on **Add I/O unit**.
3. Select **S7 PLC client** as the type.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
4. Enter the **Name** for the I/O unit.
5. Click on **Finish** to add the I/O unit.
A page will open where you can configure the settings for the unit.
The newly added I/O unit is automatically enabled. If you want to use it later, set the **Enabled** slider to **Off**.

I/O management > I/O units > S7 PLC Client

Signals

General

Enabled: ☒ On

Name: S7 PLC Client

System ID: f6b9108bc2ab47e7bb0501ceb4ddf80a

Location: e.g. Building 1, Room 234

S7 client

Network address: _____ Network port: _____ 102

Rack: _____ Slot: _____ 1

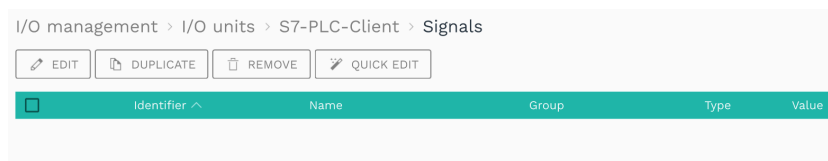
Connection type: PG Byte order: Most significant byte first (big endian)

If you encounter problems connecting to the S7 PLC or with reading out variables, please follow the instructions at [S7 client connection instructions](#), especially the S7 1200/1500 notes and screenshots below.

Device settings for the S7 PLC client in “Advanced” viewing mode

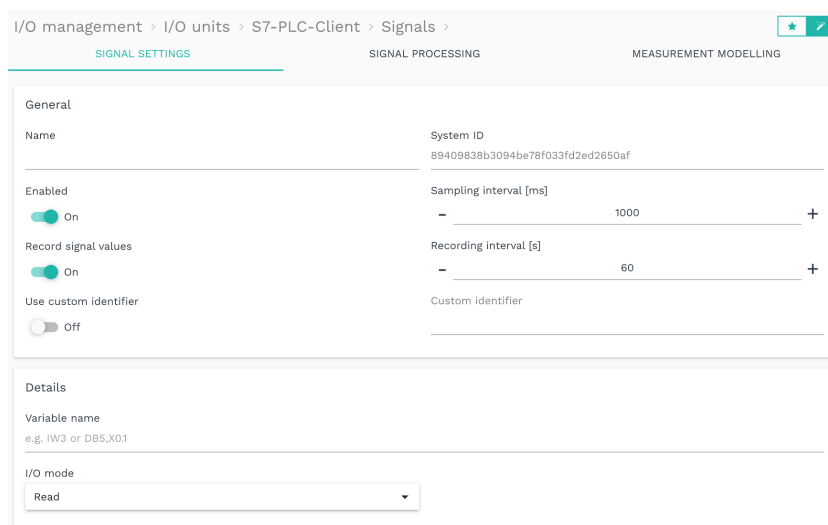
6. Optional: Enter the **Location**.
7. You can configure the following settings in the **S7 client** section:
 - a. **Network address:** Enter the hostname or IP address of the SIEMENS controller to which a connection is to be established.

- b. **Network port:** Enter the port through which the Siemens S7 controller can be accessed. As a rule, the default value “102” does not need to be changed.
 - c. **Rack** and **Slot:** Specify the position of the CPU module in the controller. Depending on the controller model, the CPU can also be located in slot “0” or “2”.
 - d. **Connection type:** Select the mode to be used for establishing the connection. The default value **PG** (programming device) only needs to be changed to **OP** (operating mode for HMI panels) or **Basic** (fallback) in exceptional cases.
 - e. **Byte order:** Specify the byte order in which the PLC stores its data in the memory – whether with the **Most significant byte first (big endian)** or the **Least significant byte first (little endian)**. Change this setting if you notice that the data is implausible.
8. Additional settings are available in **Advanced** viewing mode:
 - a. **Local TSAP** and **Remote TSAP:** If you have problems with the connection despite changing the rack and slot settings, these two parameters can be adjusted accordingly. Please contact the support team at in.hub and only make changes after consultation.
 9. Click on **Save**.
 10. Click on **Signals**.



Signals for the S7 PLC client (initially, no signals are predefined)

11. Click on **Add I/O unit**.
A window opens in which you will find three tabs.



“Signal settings” tab in “Advanced” viewing mode

12. Enable and configure the interface on the **Signal settings** tab.

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

NOTE
If you have selected **I/O mode** “Write”, no sampling takes place and the sampling interval is ignored.
- d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).
13. Additional settings are available in **Advanced** viewing mode:
 - a. **Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier:** Enter your own identifier name.
 14. Further entries are required in the **Details** section.
 - a. **Variable name:** The S7 variable name encodes which address is to be accessed with which data type in which section of the S7. There are different variable areas: Data block, digital inputs/outputs or memory/flags. For more information, see the PLC manufacturer’s interface description or list of variables.
In case of 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>.
 - b. **I/O mode:** Select whether a data value / date is to be read from the controller (**Read**) or written to the controller (**Write**).
 15. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
 16. Click on **Save**.
 17. On the **Measurement modelling** tab, you specify how the measurements are to be visualized.
You can find out more at [Measurement modelling \[93\]](#).
 18. Finally, click on **Save & close**.

4.2.13. Adding a ControlPlex® CPC12 bus controller

1. On the **I/O management** start page, select **I/O units**.
2. Click on **Add I/O unit**.
3. Select **ControlPlex® CPC12** as the type.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.

4. Enter the **Name** for the I/O unit.
5. Click on **Finish** to add the I/O unit.

A page will open where you can configure the settings for the unit.

I/O management > I/O units > ControlPlex ACTIONS

Signals >

General

Enabled

☒ On

System ID

ecac79f4f2fe49b1824ebf466890f001

Name

ControlPlex

Location

e.g. Building 1, Room 234

Communication settings

Device address

Device settings for the ControlPlex® CPC12 (example)

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

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

The signals for all channels of the ControlPlex® CPC12 have already been created.

I/O management > I/O units > ControlPlex > Signals

EDIT QUICK EDIT

☐	Identifier	Name	Group	Type	Value
☐	CURRENT_CH01	Channel 01 Current		DOUBLE	0,00 A
☐	CURRENT_CH02	Channel 02 Current		DOUBLE	0,00 A
☐	CURRENT_CH03	Channel 03 Current		DOUBLE	0,00 A
☐	CURRENT_CH04	Channel 04 Current		DOUBLE	0,00 A
☐	CURRENT_CH05	Channel 05 Current		DOUBLE	0,00 A
☐	CURRENT_CH06	Channel 06 Current		DOUBLE	0,00 A
☐	CURRENT_CH07	Channel 07 Current		DOUBLE	0,00 A
☐	CURRENT_CH08	Channel 08 Current		DOUBLE	0,00 A
☐	CURRENT_CH09	Channel 09 Current		DOUBLE	0,00 A
☐	CURRENT_CH10	Channel 10 Current		DOUBLE	0,00 A
☐	CURRENT_CH11	Channel 11 Current		DOUBLE	0,00 A
☐	CURRENT_CH12	Channel 12 Current		DOUBLE	0,00 A
☐	CURRENT_CH13	Channel 13 Current		DOUBLE	0,00 A
☐	CURRENT_CH14	Channel 14 Current		DOUBLE	0,00 A

Signals for the ControlPlex® CPC12 (example)

8. Select the signal you want to configure.
A window opens in which you will find three tabs.
9. Enable and configure the interface on the **Signal settings** tab.
 - a. Optional: Change the name of the interface.
 - b. Set the **Enabled** slider to **On**.
 - c. In the **Sampling interval** field, specify the interval at which the signal is to be sampled (in milliseconds).

- d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).
10. Additional settings are available in **Advanced** viewing mode:
 - a. **Use custom identifiers**: Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier**: Enter your own identifier name.
 11. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
 12. Click on **Save**.
 13. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).
 14. Finally, click on **Save & close**.

4.3. Signal processing



NOTE

SIINEOS version 2.7.4. and later use the `expr-eval` library. The following mathematical functions are thus available:

<https://github.com/in-hub/expr-eval#expression-syntax>

This can lead to incorrect results or improperly functioning signal-processing steps for signals that have already been configured. You should therefore check the mathematical functions of your existing signal-processing steps.

In the **Signal processing** tab, you can convert the input values using mathematical functions if you require a physical quantity or a process variable instead of the raw values. SIINEOS processes the processing functions in the order in which they appear in the tab. For example, if you have activated **preprocessing** and **threshold comparison**, then **preprocessing** is calculated first and then the **threshold comparison** is performed using that value.

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



NOTE

If you require more than one formula, e.g. for **preprocessing** for your signal processing, you must create a synthetic signal. There, you can enter the first formula in the **Signal Processing** tab when creating it, and then enter the second formula in the signal settings for the synthetic signal. See also [Creating synthetic signals \[97\]](#).

SIGNAL SETTINGS	SIGNAL PROCESSING	MEASUREMENT MODELLING
☐ Preprocessing		
☐ Linear scaling		
☐ Delta		
☐ Limit		
☐ Threshold comparison		
☐ Comparator / hysteresis		
☐ Edge detection		
☐ Time derivative / frequency calculation		
☐ Aggregation		
☐ Postprocessing		

“Signal processing” tab

4.3.1. Signal processing functions

Function	Explanation
Preprocessing	This function can be used to preprocess the signal value using 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. Examples of mathematical expressions: • $x - 2$ • $(x - 4) * 0.7$ • $\sin(x * \text{PI} / 180)$ • $\max(x, 10)$ • $\text{abs}(x)$
Linear scaling	This function is used to apply a simple linear function to the input value. While in principle it is also possible to implement a linear function as a mathematical expression (e.g. $x * 5 + 7$) using the given parameters (slope/coefficient and constant) in the previous function, this function allows the simple input of 2 input and output values. These values are often known from data sheets, especially for analogue sensors. <i>For example:</i> A temperature sensor on a 4–20 mA interface can have a value range from –20°C to +80°C. In this case, you would enter the values 4 for X1 and 20 for X2, as well as the values –20 for Y1 and 80 for Y2.
Delta	This function compares the current signal value with the previously measured signal value. There are various options in the drop-down list for 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 % • Leading sign difference to the previous value: If the value changes from a positive numerical value to a negative numerical value (or vice versa), –1 (or +1) is output. This can be used to detect anomalies, for example.
Limit	This function imposes lower and/or upper limits on the signal value, so if the signal falls below the minimum value, the gateway delivers the minimum value as the signal value. If the signal value is above the maximum value, this maximum value is used as the signal value.

Function	Explanation
Threshold comparison	This function converts the signal value into a logical value of 0 or 1, depending on how the signal value relates to the threshold value. <i>Example:</i> If the Signal is above mode is selected and a threshold value of 10 is set, the output from the device is 1 as long as the signal value is greater than 10. If it falls below this, the output is 0.
Comparator/hysteresis	The function compares the input value with lower and upper thresholds and returns the appropriate output value depending on the result. This behaviour is used to implement two-point control or hysteresis. Additionally, the progression over time can be included by setting the minimum undershoot and minimum overshoot duration to a value >0 ms. For the output signal to assume the upper output value, the input signal must be continuously above the upper threshold value for a certain number of milliseconds. Similarly, the output signal is only reset to the lower output value once the value falls below the lower threshold 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). Analogue signals can also be converted into digital signals with the help of upstream functions such as threshold comparison, e.g. by using the value 1 (rising edge) as the input for edge detection when a threshold value is exceeded and thus automatically using the value 0 when the value falls below it.
Time derivative / frequency calculation	The function determines the number of changes from 0 to non-0 (e.g. to 1 or any other level). The result is then no longer the original signal value, but the number per time unit or the frequency. This function can be used to implement a piece counter, for example, so that signal processing no longer outputs the digital input, but the number of parts produced per second/minute/hour. If necessary, this function can be combined with averaging directly afterwards, as the value can fluctuate greatly, especially at the beginning. To do this, go to the Aggregation step and select the Average value entry under Aggregation type.
Aggregation	If several signal values are to be summarized over time (also known as aggregation), the Aggregation function can be activated.

Function	Explanation
	With this, either a specific value (e.g. the largest or smallest), the sum of all values or the average value is determined from values that are received over a certain duration (Aggregation interval) and delivered as an output (Aggregation type). You can also specify whether the aggregate value is to be calculated at every sampling point (continuously) or only regularly at the end of the aggregation interval (periodically).
Postprocessing	Once the input signal has been processed by one or more functions, it can be postprocessed in the same way as by the preprocessing function, e.g. the accuracy can be adjusted by rounding or similar. The format and syntax of the mathematical expression correspond to those of the Preprocessing function.

4.3.2. Configuring the signal processing steps

1. Use the slider to activate the desired signal processing step.
The input section opens.
2. Complete the input fields for the signal processing steps you want to apply.
3. Click on **Save** and continue to the **Measurement modelling** tab.

4.4. Measurement modelling

The **Measurement modelling** tab allows you to configure the same parameters for all I/O units and interfaces in order to display measurements.



NOTE
This configuration is optional. However, you can only visualize your data in the **FlexPlorer** app if this tab is filled out. For example, you should enter the number of decimal places, as otherwise measurements will always appear without decimal places by default, including in the apps that transfer the values to the cloud or write them to Grafana, for example.

I/O management > I/O units > GM200-Zentrallager > Signals > Digital Input 1

SIGNAL SETTINGS SIGNAL PROCESSING MEASUREMENT MODELLING

Settings

Group

SI prefix

No prefix

Decimals

1

Data series set

Unit

Custom data type

Keep original

Visualization

Type

Gauge

Minimum value

0

Color

#00dbc9

Maximum value

0

Preview

Digital Input 1

1,0

CLOSE

SAVE

SAVE & CLOSE

“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 previews (preferably of the same type, e.g. Gauge) are lined up next to each other in FlexPlorer , so that measurements from different devices/sensors can be compared with each other.
Data series set	All signals with the same data series set are displayed in FlexPlorer under Live charts in a common chart, so that the signal values from different 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: G (giga, 10 ⁹), M (mega, 10 ⁶), k (kilo, 10 ³), h (hecto, 10 ²), d (deci, 10 ⁻¹), c (centi, 10 ⁻²), m (milli, 10 ⁻³), µ (micro, 10 ⁻⁶), n (nano, 10 ⁻⁹), p (pico, 10 ⁻¹²)

Unit	Select the physical unit to be assigned to the value.
Decimal places	Enter the number of decimal places to be displayed.
Custom data type	Select a data type and overwrite the original data type for a signal. This is useful, for example, when calculating a float value from a Modbus UINT16 register or a digital input with a true/false value (Boolean).
Minimum value	Enter the value to be used as the minimum in the visualization element (e.g. a gauge). This may be the smallest measurable value for the connected device, but 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 may be the largest measurable value for the connected device, but does not have to be.
Type	Select the type of visualization that best matches the output values. Available options are Gauge , Counter , LED or No visualization .
Colour	Select a colour for displaying measurements.

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

4.5. Configuring signal connections

If you want to control and/or 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

Readable input signals for the I/O units are only displayed in the signal connection setup wizard if they have previously been activated in the signal settings using the slider.

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

I/O management > Signal connections

EDIT DUPLICATE REMOVE

Name ^	Source	Destination
Milling machine & LED red	GM200-Zentrallager – Digital Input 1	GM200-Zentrallager – Red LED
Partikelmessung 1.0 PM - LED	Partikelsensor – Mass concentration PM1.0	GM200-Zentrallager – Green LED

Example for signal connections (initially, no signal connections are predefined)

2. To create a new signal connection, click on **Add signal connection**.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
3. Enter the **Connection name**.
The connection is enabled automatically. If you want to deactivate it temporarily or permanently, you can disable the connection.
4. Under **Source signal**, select the I/O unit and the associated signal to be read from, e.g. the digital input of the HUB-GM200 in the central warehouse.
5. Under **Signal processing**, you can optionally process or modify the source signal you have just selected before it is written to the destination signal, e.g. “0” and “1” if a threshold is exceeded.
NOTE: This does not change the source signal itself; rather, this step relates exclusively to the calculation of the destination signal. Signal processing of the source signal, as you know from the I/O units, continues independently of this.
6. Under **Destination signal**, select the I/O unit and the associated signal to which the value is to be forwarded. This can be, for example, the HUB-GM200 with an LED that lights up when a threshold value is exceeded.

The signal connection could now look as follows, for example:

Source signal

Please select the source signal to read from:

I/O units

ACS-080-2-M100-HE2-PM
GETT
GM200-Zentrallager
HUB-GM200 in.hub Fabrik
HUB-VM102 in.hub Fabrik
IEM3255 via Modbus RTU
IEM3255 via Modbus RTU
Modbus TCP
MQTT Client
Numcoder
OPCUA
Partikelsensor
ST-PLC-Client
Synthetic signals
TBEN-Modul S2-4AI
TBEN-Modul S2-4AI
VM102

Search units

Signals

Mass concentration PM1.0
Mass concentration PM10.0
Mass concentration PM2.5
Mass concentration PM4.0
Number concentration PM0.5
Number concentration PM1.0
Number concentration PM10.0
Number concentration PM2.5
Number concentration PM4.0
Typical particle size

Search signals

Destination signal

Please select the destination signal to write to:

I/O units

ACS-080-2-M100-HE2-PM
GETT
GM200-Zentrallager
HUB-GM200 in.hub Fabrik
HUB-VM102 in.hub Fabrik
IEM3255 via Modbus RTU
IEM3255 via Modbus RTU
Modbus TCP
MQTT Client
Numcoder
OPCUA
Partikelsensor
ST-PLC-Client
Synthetic signals
TBEN-Modul S2-4AI
TBEN-Modul S2-4AI
VM102

Search units

Signals

Green LED
Red LED

Search signals

I/O management > Signal connections > Edit signal connection (example)

Example: A particle sensor is connected to digital input 1 of the HUB-GM200. The green LED of the HUB-GM200 is to light up if the PM1.0 particle concentration is undershot or exceeded.

- 7. For large entries, you can search for units or signals by entering at least one number or letter in the search field below the selection lists.
- 8. When you have completed the input, click on **Save & close**.

4.6. Creating synthetic signals

You can use this function to logically link signals, e.g. from sensors or bus protocols, and thus generate new signals. This is particularly interesting in combination with software applications with which machine statuses can be analysed, e.g. with MADOW.

Case study 1: For example, you can link two signals – “Milling machine running” (signal 1) and “Coolant flowing” (signal 2) – together 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”. On this basis, downtime is recognized 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 two measurements from a particle sensor for different particle sizes is above a limit value.



NOTE

Readable input signals for the I/O units are only displayed in the signal connection setup wizard if they have been activated in the signal settings using the slider.

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

I/O management › Synthetic signals ACTIONS

EDIT DUPLICATE REMOVE RESET EDIT SIGNAL PROPERTIES

Name ^	First source signal	Second source signal	Calculation	Value
Kilo	Numcoder – kilogramm	Numcoder – kilogramm	A	0
Schwellwert	IEM3255 via Modbus RTU – Temperatur	GM200-Zentrallager – Digital Input 1	A+B	1
Taktzahl	GM200-Zentrallager – Digital Input 1	OPCUA – Channel 01	A+B*3	1
Lieferschein	Numcoder – Lieferschein	Numcoder – Lieferschein	A	0

Example for synthetic signals (initially, no synthetic signals are predefined)

2. To create a new signal, click on **Add synthetic signal**.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **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. a temperature sensor.
5. Under **Second source signal**, select the I/O unit and the second signal to be read from, e.g. digital input DIO1.
The synthetic signal could now look as follows, for example:

Source signal

Please select the source signal to read from:

I/O units	Signals
ACS-080-2-M100-HE2-PM	Mass concentration PM1.0
GETT	Mass concentration PM10.0
GM200-Zentrallager	Mass concentration PM2.5
HUB-GM200 in.hub Fabrik	Mass concentration PM4.0
HUB-VM102 in.hub Fabrik	Number concentration PM0.5
IM3255 via Modbus RTU	Number concentration PM1.0
IM3255 via Modbus RTU	Number concentration PM10.0
Modbus TCP	Number concentration PM2.5
MQTT Client	Number concentration PM4.0
Numcoder	Typical particle size
OPCUA	
Partikelsensor	
ST-PLC-Client	
Synthetic signals	
TBEN-Modul S2-4AI	
TBEN-Modul S2-4AI	
VM102	

Search units Search signals

Destination signal

Please select the destination signal to write to:

I/O units	Signals
ACS-080-2-M100-HE2-PM	Green LED
GETT	Red LED
GM200-Zentrallager	
HUB-GM200 in.hub Fabrik	
HUB-VM102 in.hub Fabrik	
IM3255 via Modbus RTU	
IM3255 via Modbus RTU	
Modbus TCP	
MQTT Client	
Numcoder	
OPCUA	
Partikelsensor	
ST-PLC-Client	
Synthetic signals	
TBEN-Modul S2-4AI	
TBEN-Modul S2-4AI	
VM102	

Search units Search signals

I/O management > Synthetic signals > Edit synthetic signal (example)

If the signal value of digital input 1 (DIO1) outputs that the “milling machine is running” and the signal value of digital input 2 (DIO2) outputs that the “coolant is flowing”, then the synthetic signal added here is generated, which outputs a machine status (however defined).

- For large entries, you can search for units or signals by entering at least one number or letter in the search field below the selection lists.
- Now, under **Calculation**, select one of the mathematical operations or logics with which the synthetic signal is to be calculated from the two source signals.

Add values	The values of the two source signals are added together.
Subtract values	The values of the two source signals are subtracted.
Multiply values	The values of the two source signals are multiplied.
Divide values	The values of the two source signals are divided.
Logical AND operation	The two source signals are linked with an “AND”, i.e. both signal values must be non-zero for the synthetic signal also to have the logical value “1”.
Logical OR operation	The two source signals are linked with an “OR”, i.e. at least one signal value must be non-zero for the synthetic signal also to have the logical value “1”.
RS flip-flop	This function allows you to model an RS flip-flop, whereby the output is controlled by the R (reset) and S (set) signals. The S signal sets the output to 1 until the output is reset to 0 by the R signal. The two inputs – S (set) and R (reset) – correspond to the first and second source signals. If a source signal has a value >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 if required using the Reset button in the signal overview. Note: As the second source signal is ignored, it makes sense to select the same signal as for the first source signal.
Resettable counter	Increases by the difference between the previous and current value of the source signal. If the second signal briefly (or for longer) assumes a value not equal to 0, the counter is reset.
Custom mathematical or logical expression	Enter a mathematical formula in accordance with 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 source signals 1 and 2. Examples for the input: • $A \geq 1$ or $B \geq 2$: Result = 1 if $A \geq 1$ OR $B \geq 2$, otherwise the result = 0 • $A > 0.5$ and $B < 10$: Result = 1 if $A > 0.5$ AND $B < 10$, otherwise the result = 0 • $\max(A, B)$: The larger of the two signals is the result • A^B: Result = A to the power of B

- When you have completed the input, click on **Finish**.
- To save all signals in a file (to reuse them on another device, for example) or if you want to transfer synthetic signals from another device to the current one, click on **Actions** and select the corresponding menu item.
- To reset dynamic features – such as infinite counters or RS flip-flops, 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.
- Like all other signals, you can disable the synthetic signal, make settings, process and model it. 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 > Schwellwert

SIGNAL SETTINGS SIGNAL PROCESSING MEASUREMENT MODELLING

General

Name
Schwellwert

System ID
663c7090e6ab43c5a5ccc0c0de199fc4

Enabled
☒ On

Record signal values
☒ On

Use custom identifier
☐ Off

Sampling interval [ms]
- 1000 +

Recording interval [s]
- 60 +

Custom identifier
663c7090e6ab43c5a5ccc0c0de199fc4

Signal settings of the selected synthetic signal in “Advanced” viewing mode

12. Enable and configure the synthetic signal on the **Signal settings** tab.
 - a. Optional: Change the name of the synthetic signal if necessary.
 - b. Optional: Set the slider to **Off** if you do not want to use the synthetic signal at the moment.
 - c. In the **Sampling interval** field, specify the interval at which the signal is to be sampled (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 setting the sampling interval very low (e.g., to the minimum of 50 ms) so that the synthetic signal is updated with very little delay.

- d. Set the **Record signal values** slider to **On** if the values are to be recorded in the local VictoriaMetrics database.
 - e. In the **Recording interval** field, enter the desired time interval for the recording (in seconds).
13. Additional settings are available in **Advanced** viewing mode:
 - a. **Use custom identifiers:** Set the slider to **On** if you want to enter your own identifier name.
 - b. **Custom identifier:** Enter your own identifier name.
14. On the **Signal processing** tab, you can specify how the signal value is to be processed. You can find out more at [Configuring the signal processing steps \[92\]](#).
15. Click on **Save**.
16. On the **Measurement modelling** tab, you specify how the measurements are to be visualized. You can find out more at [Measurement modelling \[93\]](#).
17. Finally, click on **Save & close**.

4.7. Configure I/O endpoints

You can use this function to configure that I/O signals may be written or read via fieldbuses and protocols. These are called I/O endpoints. An endpoint can be both a device and a protocol.

4.7.1. Modbus server

Make I/O signals available via Modbus TCP (network) or RTU (backplane bus) so that these signals can be read or written by the connected devices.

1. On the **I/O management** start page, select **I/O endpoints > Modbus server**.

I/O management > I/O endpoints > Modbus server

☒ **Modbus TCP**

Network address: 0.0.0.0 Network port: 502

☒ **Modbus RTU**

Bus interface: Built-in RS485 interface Serial port name: e.g. ttyUSB0

Baud rate: 500000 Data bits: 6

Parity: Even parity Stop bits: 1

Modbus ID: 1

Registers

EDIT DUPLICATE REMOVE **+ ADD REGISTER**

Register type	Register address	Data type	Connected I/O signal	I/O mode	Signal value
Coil (FC 01)	222	Double	GM200-Zentrallager – Spannungsversorgung EE150	↔	1

I/O endpoints > Modbus server

2. If you would like to “enable” I/O signals via Modbus TCP, set the **Modbus TCP** slider to **On**.
Enter the **Network address** and the **Network port** of the endpoint that is to have access to the I/O signal.
If the field **Network address** contains “0.0.0.0”, this means that access is obtained via all local IPs/devices, e.g. via Ethernet 1, 2, Wi-Fi, USB, etc. If you do not want to allow this, limit access by entering only the IP address of the allowed device.
3. If you want to “enable” I/O signals via Modbus RTU, set the **Modbus RTU** slider to **On**.
 - a. The appropriate **Bus interface** must be selected for communication with the Modbus device; in most cases, this will be the **Built-in RS485 interface**.
For I/O modules (such as the HUB-IO100 or HUB-EN200), select **Backplane bus**.
A **Serial interface** is then required if an RS485 or RS232 converter is connected via the external USB interface.
When using serial interfaces, you must specify the **Serial port name**. This depends on the device and may need to be determined via SSH. Usually “ttyUSB0” is used, or in some cases “ttyACM0”.
 - b. Complete all other input fields, such as **Baud rate** or **Parity**, according to the documentation of the connected device.
 - c. Enter the **Modbus ID** of the device you wish to communicate with.
4. Under **Registers**, you can create the Modbus registers that are to read or write the I/O signal.
 - a. Click on **Add register**.
 - b. **Register type**: Select the register type.
 - c. **Register address**: Enter the desired address of the register.

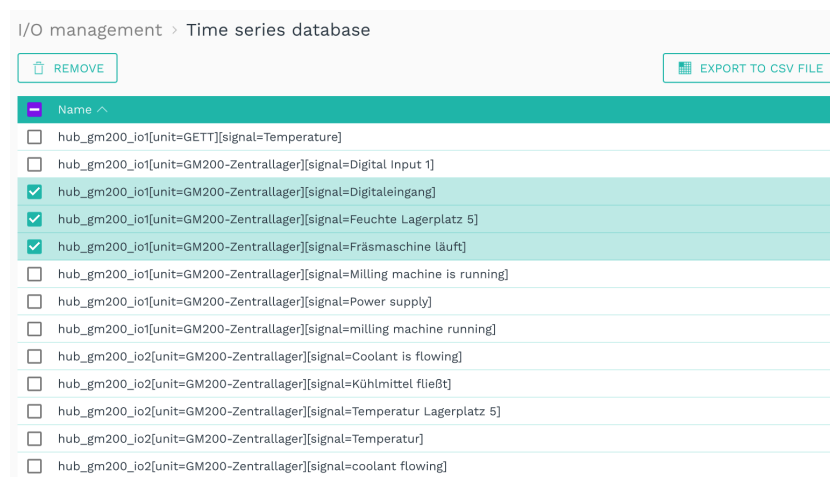
- d. **Data type:** Select the data type for the register.
- e. **Connected I/O signal:** Select the signal to be read or written.
- f. **I/O mode:** Select whether the I/O signal value is to be read and made available in the register or whether the register value is to be read and written to the I/O signal.
- g. Click on **Finish**.
In the **Register** list, you will find all entries, which you can **Edit**, **Duplicate** or **Remove** as usual.

5. Finally, click on **Save & close**.

4.8. Export time series database

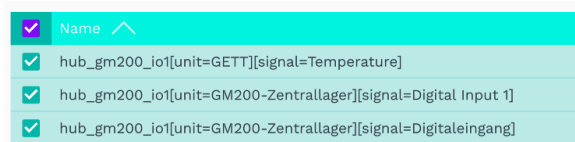
This function allows you to export or delete the recorded measurements from the time series database (VictoriaMetrics). This can be useful, for example, if you want to start productive operation and tidy up test data.

1. On the **I/O management** start page, select **Time series database**.



I/O management > Time series database

2. Select all database entries by activating the checkbox in the header;



– or –

Just start typing.

Your input will be transferred directly into the search field at top right and the hits will be displayed dynamically in the list.



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

you can then select the filtered hits again using the checkbox in the header.

3. To export the selected data, click on **Export to CSV file**.

A window opens in which you can make detailed settings for the CSV export.

“CSV export” dialogue window (example)

4. Make the following entries in the **CSV export** dialogue window:
 - a. By default, the period of one month is entered retroactively.
If you want to adjust this period, enter a new **Start date** and **End date**.
 - b. In the **Interval** drop-down list, you specify the intervals at which the entries are to be exported.
 - c. Under **Decimal separator**, specify whether the decimal place should be a point or a comma.
 - d. Under **Aggregation**, you can output additional columns for each measurement series, in which either the **Minimum**, **Maximum**, **Average**, **Sum** or **Number** of values within an interval are listed.
 - e. In the **Date/time format** drop-down list, you can select the format in which the date and time of the database entry is to be displayed in the CSV file.

Timestamp: A timestamp is set for each entry.

Local date + time (2 columns): The date and time are converted into the time zone that you have specified under **SIINEOS > System > Date & time** and are output in the format YYYY-MM-DD and hh:mm:ss.

UTC date + time (2 columns): The UTC date and UTC time are output in the format YYYY-MM-DD and hh:mm:ss.

ISO string: Date and time in a machine-readable character format

Localized string: Detailed date with day of the week and month written out in full. The format depends on the language environment.



TIP

The smaller the interval and/or the longer the time period, the more data has to be written and the longer the process takes.

If the recording interval of the signal is greater than the interval entered here, the same value is output for each time unit. This increases the size of the CSV file and therefore also the duration of the download.

5. Click on **Start export**.

Depending on the selected interval, period and selected summaries, this may take a few minutes.

6. To save data in a file, select individual or all data and click on **Export to CSV file**.
7. To delete data from the time series database, select individual or all data and click **Remove**.

5. Managing apps

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

5.1. Azure IoT Hub Connector

The **Azure IoT Hub Connector** app allows you to establish a communication channel between an IoT device (e.g. the HUB-GM200) and Microsoft's 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.

The following input fields are available for configuring the Azure IoT Hub Connector:

Settings for the “Azure IoT Hub Connector” app

1. Enter the following details, then click on **Save**:
 - a. **Hub name:** Enter the name of the device from which you want to send data to the Azure IoT platform.
 - b. **Device ID:** Enter the device ID of the device whose data you would like to send to the Azure IoT platform. You can find this ID in your Azure IoT hub management interface.
 - c. **Password:** Enter the password. You can find the password in your Azure IoT hub management interface.
 - d. **Send interval:** From the drop-down list, select the time interval at which the data should be sent from the IoT device to Azure.
 - e. **Buffer measurements 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 mobile-phone interference or network maintenance work).
 - f. **Maximum number of measurements to buffer:** Specify the maximum number of measurements to be buffered.

5.2. Cloud of Things Connector

The **Cloud of Things Connector** app allows you to establish a communication channel between an IoT device (e.g. the HUB-GM200) and Telekom's IoT platform.

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

Settings for the “Cloud of Things Connector” app

- In the **Status** section, 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
- The following input fields for configuring the Cloud of Things Connector are available in the Settings area:
 - Device ID:** Display of the device ID.
 - Tenant:** Enter the name of the (logical) unit under which all associated users and data are to be summarized and administered.
If you have purchased cloud access via in.hub, you must enter the company account, in this case “inhubcloud”. This field is prefilled 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 measurements are to be buffered in the event of a connection being interrupted.
 - Maximum number of measurements to buffer:** Enter the maximum number of measurements to be buffered.
- Click on **Save**.

4. Click on **Open Cloud Cockpit**.

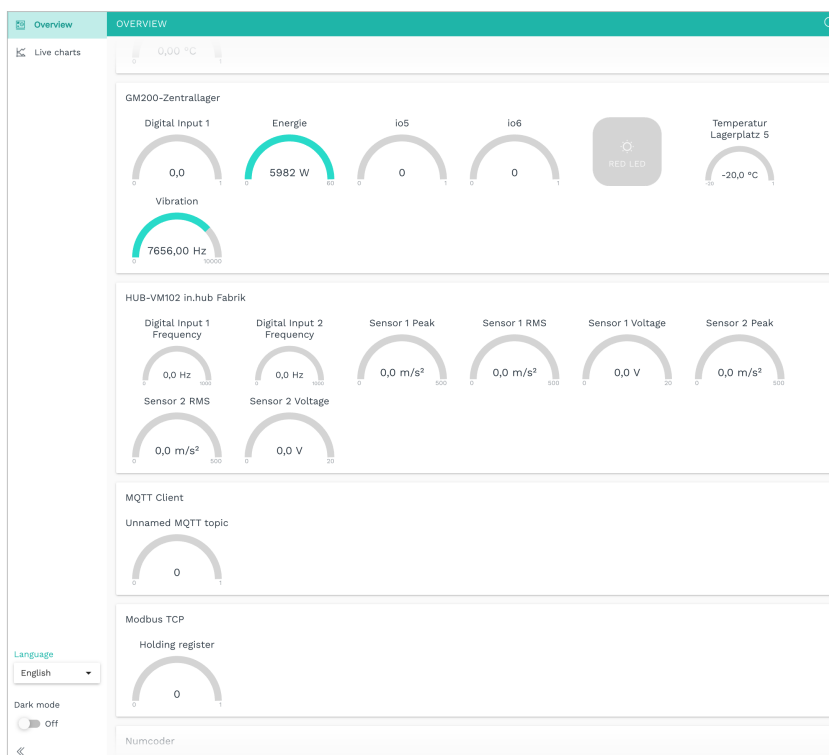
The Telekom Cloud opens, where you can log on with your individual user data.

5.3. FlexPlorer

in.hub's own visualization tool **FlexPlorer** 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.

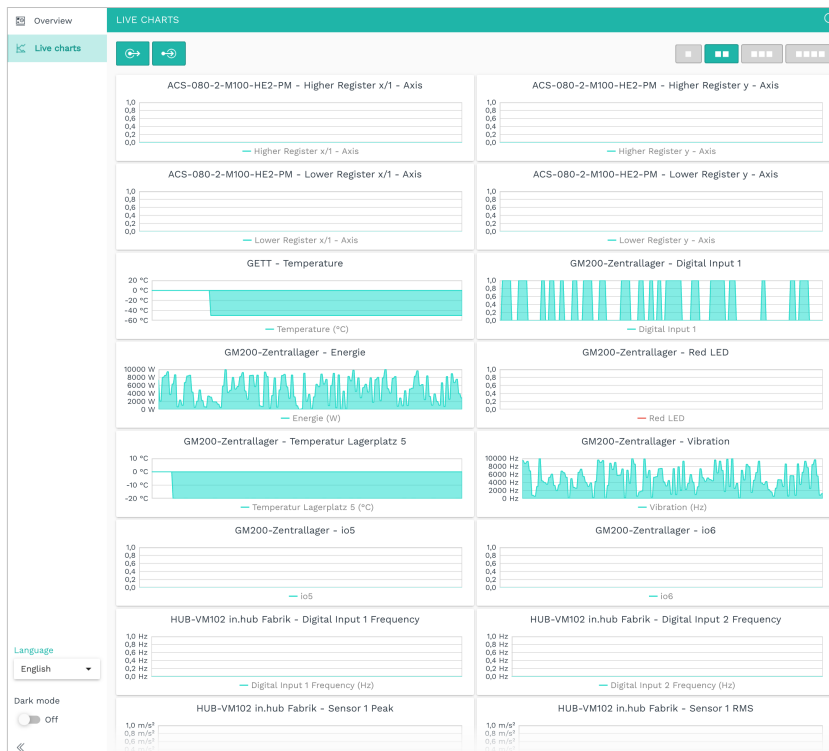
You can switch between two views in FlexPlorer: **Overview** and **Live charts**.

On the **Overview** page, you can see the signals of each activated I/O unit in a graphical representation. The display is based on your entries in the **Measurement modelling** tab.



Overview in FlexPlorer

You can monitor the progression of measurements live on the **Live charts** page:



Live charts in FlexPlorer

You can customise the view of the live charts using various buttons:

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

5.4. InGraf

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

Grafana accesses the built-in **VictoriaMetrics** database.

If you are updating from SIINEOS 2.8.0 and above to the current version, please ensure that the data source in Grafana is switched to VictoriaMetrics.

If you are updating from SIINEOS 2.7.7 and below to the current version, some settings are necessary. Please contact us beforehand at service@inhub.de.



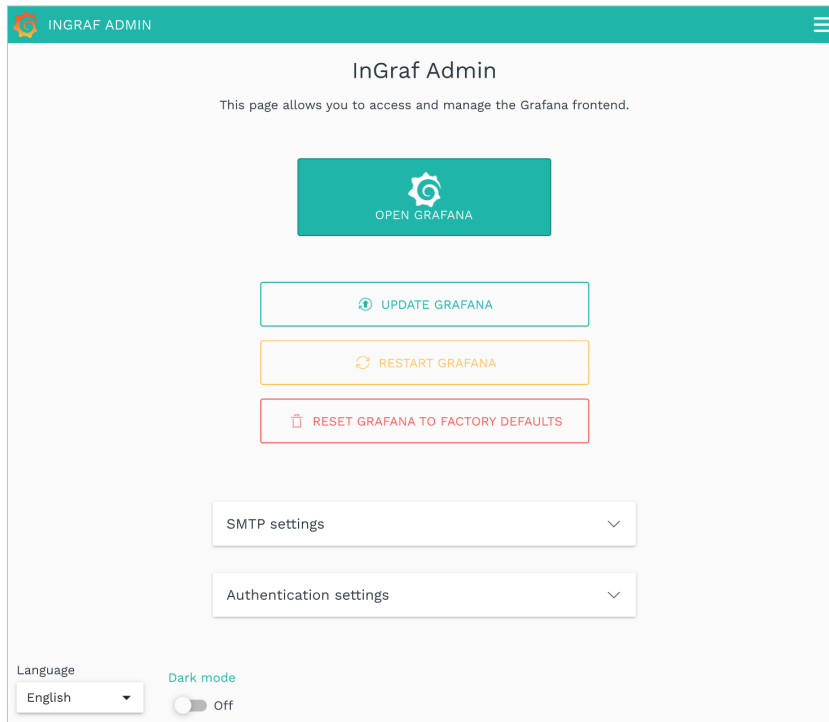
NOTE

To manage the **InGraf** app, a separate user role – the app administrator – is created with the initial user data: **ingrafadmin/ingrafadmin**.

See also [User administration \[32\]](#).

The initial user data **admin/admin** is defined for access to **Grafana**. Log on and then change your access data.

5.4.1. Configuring the Grafana connection



Settings for the Grafana front end

1. Use the following buttons as required:
 - a. **Open Grafana:** Opens Grafana in a new window. Have your user data ready and log on.
 - b. **Update Grafana:** Updates your Grafana version to the latest version. Your dashboards will remain unaffected.
 - c. **Restart Grafana:** Restarts Grafana in case the programme fails to reply or respond.
 - d. **Reset Grafana to factory defaults:** Resets all your settings in Grafana.



ATTENTION

With this, all dashboards, alarm configurations and other settings will be lost. This does not affect the data recorded in VictoriaMetrics.

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

The screenshot shows the 'SMTP settings' window. It contains the following fields and controls:

- SMTP enabled:** A toggle switch set to 'On'.
- SMTP server:** A text input field.
- SMTP port:** A numeric input field with a value of 25 and minus/plus buttons.
- SMTP user:** A text input field.
- SMTP password:** A text input field.
- Sender address:** A text input field with the example 'e.g. admin@mycompany.com'.
- Sender name:** A text input field with the example 'InGraf'.
- Buttons:** 'REVERT' and 'SAVE' buttons at the bottom.

- a. **SMTP enabled:** Set the slider to **On** if you want Grafana to send via your SMTP server.
Grafana cannot send e-mails without a SMTP server configuration, so the alerting function cannot be used, for example.
 - b. **SMTP server:** Enter the name of your e-mail server.
 - c. **SMTP port:** Enter the port for your e-mail server.
 - d. **SMTP user** and **SMTP password:** In order for Grafana to log on to your SMTP server, the details of an e-mail account are required. Ask your system administrator for the access data that Grafana is to use to send e-mails.
 - e. **Sender address:** Enter the e-mail address that appears as the sender in the e-mails that Grafana sends. You configure the destination addresses individually in Grafana, as different recipients are also possible for different alarms, for example.
 - f. **Sender name:** Enter a name under which Grafana should appear in your mailbox as the sender.
3. You can configure the authentication settings for Grafana with the following settings:

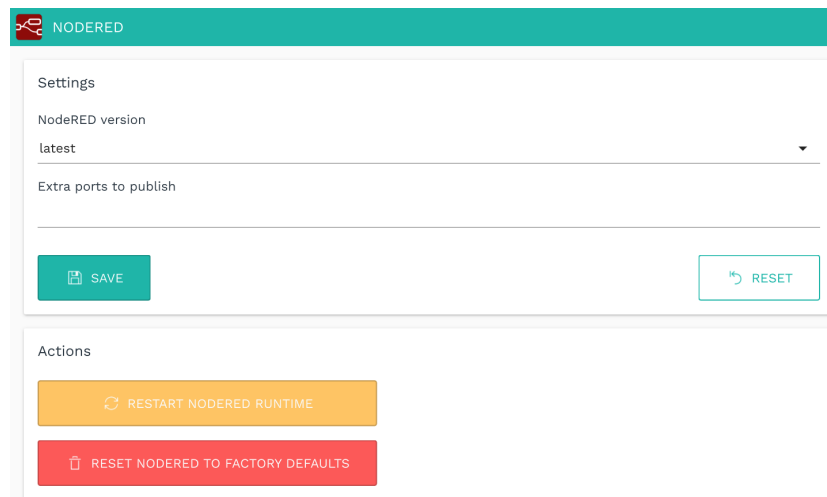
The screenshot shows the 'Authentication settings' window. It contains the following fields and controls:

- Allow anonymous access:** A toggle switch set to 'On'.
- User role for anonymous access:** A drop-down menu with 'Administrator' selected.
- Buttons:** 'REVERT' and 'SAVE' buttons at the bottom.

- a. **Allow anonymous access:** Set the slider to **On** if you want dashboards to be visible in Grafana even without prior login.
 - b. **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 on **Save**.

5.5. NodeRED

The **NodeRED** open-source application allows you to connect hardware, software, interfaces and services via graphical programming according to the modular principle. When this app is activated, the NodeRED Docker container is downloaded and executed. All further activities are your responsibility.



Settings for the Node-RED app

1. In the **Settings** section, select the Node-RED version you want to use.
If an Internet connection is established, the selected version will be automatically downloaded and used.
If you are working offline with the gateway, you can download the latest version of Node-RED 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. **Additional ports to be published:** If you use Node-RED to provide other services and interfaces, you can enter the ports here to allow access to these services and interfaces from other devices and machines.
3. You can perform the following actions in the **Actions** section:
 - a. **Restart NodeRed runtime:** If a message appears when you open the **NodeRED** app stating that the page cannot be accessed, you need to restart the app.
 - b. **Reset NodeRED to factory defaults:** Everything that you have set up, programmed or installed in **NodeRED** yourself is reset with this button.

5.6. NumCorder

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

If you click on the **Manage app** button, you have various options for configuring NumCorder: These are presented below.

Once you have finished configuring all input parameters, you can click on **Open app**. However, please check beforehand that NumCorder has also been activated (via the **Activate app** button).

5.6.1. Configuring data submission targets

You can submit the entered data either to the VictoriaMetrics database, to an HTTP API or to an MQTT interface. To do this, activate the corresponding slider.

NUMCORDER ADMINISTRATION

Settings > Data submission targets

Built-in VictoriaMetrics database

Save field values as labels

On

HTTP API

API endpoint URL

HTTP method: POST

Data format: JSON object

MQTT

MQTT broker address: localhost

MQTT broker port: 1883

Username:

Password:

Encrypt connection via TLS: Off

Connect via WebSocket: Off

Data format: Field values in subtopics

Publish retained messages: On

Topic name: inhub/numcorder/fields

Settings for data submission targets (example)

1. If you have selected **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.
Then the field value is not stored in the metric value itself, but in the label of the metric and the query must be adjusted accordingly, e.g. in Grafana.
2. If you have selected **HTTP API**:
Enter the URL of the API endpoint to which the data is to be sent.
From the drop-down list, select the **HTTP method** to be used to send data.
In the **Data format** drop-down list, you can also specify whether the data should be sent/transmitted as a **JSON object** or as **Comma-separated values**.
3. If you have selected **MQTT**:
Enter all connection details, such as the **MQTT broker address** and the **MQTT broker port**, **Username** and **Password** 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 whether the data should be published as a **JSON object** or as **Field values in subtopics**.
Set the **Publish retained messages** slider to **On** if you want the broker to send the last value published regarding this topic to all new clients.
In the **Topic name** field, enter the topic name under which the data is to be published.

4. Finish your entry with **Save & close**.

5.6.2. Configuring input sources

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

Identifier	Type	Description
barcodescanner	auftragsdaten	
input	Lokale Benutzereingabe	
virtuelletastatur		

Creating and administering input sources

1. Click on **Add input source**.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
2. Enter the **Identifier** of the input source, e.g. “barcodescanner”.
Only lower-case letters without spaces or special characters are permitted.
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**.

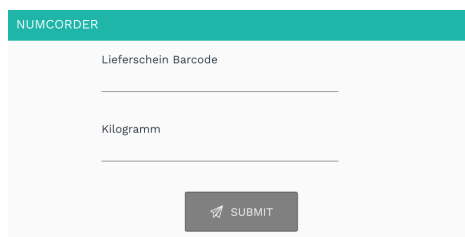
5.6.3. Creating input fields

Identifier	Name	Input source	Placeholder	Validation	Minimum length	Maximum length	Reset delay	Retain
lieferchein	Lieferschein Barcode	barcodescanner		Any characters	10	10	60 s	
kilogramm	Kilogramm	virtuelletastatur		Any characters	4	4	60 s	

Creating and administering input fields (example)

1. Click on **Add input field**.
The setup wizard opens to guide you through the rule creation process. In the following, confirm each entry with **Next** or press **Enter**.
2. Enter the **Identifier** of the input field, e.g. “deliverynote”.
Only lower-case letters without spaces or special characters are permitted.

3. Enter the **Name** to be 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** to be displayed in the input field if empty.
6. Under **Input validation**, you can specify which characters are to be allowed for input.
7. Specify the **Minimum length** in terms of characters.
The default setting is 10 characters.
If a field does not have to be filled in, 0 can also be specified as the minimum input length.
8. Specify the **Maximum length** in terms of characters.
The default setting is 10 characters.
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. Set the slider under **Retain after sending** to **On** if you want the input field to retain its value after it has been sent.
11. Click on **Finish**.
As soon as you open the **NumCorder** app, the defined input field appears.



The screenshot shows the NUMCORDER app interface. It has a teal header with the text 'NUMCORDER'. Below the header, there are two input fields. The first field is labeled 'Lieferschein Barcode' and the second field is labeled 'Kilogramm'. Below these fields is a grey button with a white arrow icon and the text 'SUBMIT'.

Input fields (example)

12. All input fields that you have created are also displayed when you open the app and must be filled in to send the data to the data submission targets.
If you want to remove a field again, select it in the list and click on **Remove**.
13. If you want to adjust the order of the input fields, select a field in the list and click on **Move up** or **Move down**.
The order of the list is also the order for entry.

5.7. OPC UA Server

The **OPC UA Server** app allows you to implement the platform-independent OPC UA standard and make the data of all I/O units and I/O signals available externally via the standardized OPC UA interface.

For example, if 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 (this will make this device act as a server) and set up the OPC UA client on the other device.

OPCUA SERVER

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

Settings for the OPC UA Server app (example)

These fields are available for configuring OPC UA Server:

Server port	This is where you enter the Server port on which the OPC UA server is to be accessible.
Advanced settings	- Set the Publish system metrics of local device slider to On to publish the system metrics CPU load, CPU usage, RAM utilization and data storage usage/utilization via OPC/UA in addition to the I/O units. This makes it easy to monitor the gateway by remote access. - Enter the OPC UA namespace URI that identifies the data schema for this OPC UA Server. - Set the Use I/O unit/signal identifier for BrowseName 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 BrowseName 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 the Manufacturer name , Product name and Product URI .

5.8. SIGNAL4

The SIGNAL4 **app** establishes a connection to the SIGNAL4 cloud so that alerts can be forwarded directly to it.

SIGNAL4 Administration

Team secret

●●●●●●●●

CHECK AND SAVE TEAM SECRET

Heartbeat

Heartbeat enabled (needs "Optimize" package)

☒ On

Heartbeat ID

Interval [s]

- 30 +

Keyword

REVERT

SAVE

Status LED control

Indicate working heartbeat to SIGNAL4 via:

No LED ▼

REVERT

SAVE

Administration for the SIGNAL4 connector

The following input fields are available for forwarding alerts to the SIGNAL4 cloud:

Team secret	Enter your Team Secret. You can find Team Secret in your SIGNAL4 profile. Use the Check and save Team Secret button to check whether Team Secret is valid. This button is only activated if a key has been entered in the input field.
Heartbeat NOTE: To activate the heartbeat function, you need the "Optimize" package from SIGNAL4.	Heartbeat enabled: Set the slider to On if you want your device to send a continuous signal to the SIGNAL4 cloud. Heartbeat ID: Enter the Heartbeat ID that is associated with the integration of your SIGNAL4 cloud. To do this, log onto the SIGNAL4 cloud with your account.

	Interval [s]: Enter the time interval for sending alerts from the in.hub device to the SIGNAL4 cloud. TIP: If, for example, the setting made in the SIGNAL4 cloud is 5 minutes, you should enter half that time here to compensate for any delays in the network. Keyword: Optionally enter, for example, the name of the in.hub device from which the heartbeat is sent. This input field is only used to identify the device.
Status LED control	The following options are available in the drop-down list: • No LED: The heartbeat is not visualised. There is no visual indication that the alerts are being transmitted to the SIGNAL4 cloud. • Red LED: The red LED of LED 3 (status LED) on the front of the device is used for visualisation. • Green LED: The green LED of LED 3 (status LED) on the front of the device is used for visualisation.

**TIP**

For a description of how to set up the heartbeat in the SIGNAL4 cloud, see the SIGNAL4 documentation at <https://docs.signal4.com/integrations/heartbeat-monitoring/heartbeat-monitoring.html>.

5.9. 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.

When you open the app’s administration, you can only enter the port under which the exporter is available and/or under which Prometheus can retrieve the data from the device.

Settings for the PromEx app (example)

5.10. TOSIBOX® Lock for Container

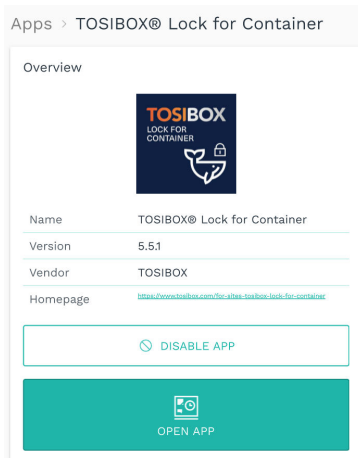
TOSIBOX® Lock for Container ensures secure connections within your industrial IoT devices. It is a software-only solution that allows you to connect your IPCs, HMIs, PLCs, controllers and other devices to your TOSIBOX® network and acts as an endpoint for secure remote connections.

With TOSIBOX® Lock for Container, services running on the connected device can be securely accessed over the Internet and most LAN and Wi-Fi networks via a highly encrypted VPN connection. The app does not restrict the number of services or devices that can be administered. You can connect any service between any devices via any protocol.

**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.

If you have experienced connection problems after disabling and re-enabling the app, you should restart the device to ensure that all services and settings work correctly.



Settings for the TOSIBOX® Lock for Container app

6. 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 in.hub device's power supply was briefly disconnected and the time setting was lost.	1. In SIINEOS, select the System page and go to the Date & time section. 2. Click on Synchronize time via browser now to synchronize the device's date settings with your computer. If the device's power supply is disconnected, this setting is lost. You will then have to synchronize with the browser again.
	The database was corrupted due to a sudden loss of power (at the device) while writing.	1. In SIINEOS, select the Monitoring page and select Data storage. 2. Activate the Advanced viewing mode and click on the Maintenance button. 3. In the drop-down list, select Reset VictoriaMetrics database to completely reset the database.
The in.hub device is no longer responding, e.g. during the updating process. The device cannot be started up even by switching it off and on (disconnecting and reconnecting the power supply).	–	Disconnect and connect the device's power supply three times in succession. In between, the LEDs on the front must have lit up for at least 5 seconds. After 3 unsuccessful boot attempts, the device switches to another boot slot and starts with the usually older version installed in that boot slot. All settings are retained.
Signal connections The required I/O unit or required 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 of the I/O unit or in the Signal settings of the signal, set the slider to On.

Problem	Possible cause	Remedy
		General Enabled 
Update You have uploaded a SIINEOS update and the new software version is not being displayed.	The browser cache still contains an old version of the web interface; – or – the in.hub device is no longer responding.	1. First delete your browser cache and refresh the page in your browser. 2. If that doesn't work: Switch off the power to the in.hub device 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 opening the address http://192.168.123.1.	A proxy server is configured in the browser or system settings in the network settings of your local PC; – or – the firewall of the local PC (Windows firewall) or the firewall of the company network is preventing access to the in.hub device or parts of the interface.	1. First, check whether the in.hub device is connected via USB cable and is flashing. Make sure that it is a USB cable that also supports a data connection. 2. In the proxy-server settings of the system or browser, you or your administrator must ensure that no proxy server is being used for the IP address 192.168.123.1 so that the browser accesses the connected in.hub device directly. Either temporarily disable the use of the proxy server or add the appropriate exception rule for the above-mentioned IP address; – or – make sure that the following ports are enabled in the settings of your local system firewall to allow access to the in.hub device. Preparing the IT infrastructure in your own company network [8]
Connection problems	A firewall rule in SIINEOS is preventing data traffic to and from the SIINEOS device.	1. Go to the Firewall page and check which action is selected in the rules for both incoming and outgoing network traffic.

Problem	Possible cause	Remedy
You can no longer access the in.hub device in the network or a system service is not responding.		2. Select the Accept packet action to allow the data exchange.
Connection problems The in.hub device is located in an isolated machine network and you cannot reach it in this network.	The communication between the machine network and the general company network is controlled by a firewall and only access to defined ports of certain in.hub devices is allowed.	Make sure, or get the system administrator to make sure, that the network firewall allows access to the in.hub device via the appropriate ports. Preparing the IT infrastructure in your own company network [8]
Connection problems An I/O module is integrated into the network via Ethernet and you are unable to access it in the network.	You have assigned the in.hub device an IP address 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 in.hub device is integrated into the network via Ethernet and you are unable to access it in the network.	The device has been automatically or manually configured with an IP address that is in the range 172.17.0.0/16 and 172.18.0.0/16 . The Docker service uses this address range by default 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 an unused IP address range under System > Services > Docker engine > Docker bridge IP address .
Signals from the Modbus RTU device are not arriving The Modbus RTU device is connected, but signals are not arriving at the in.hub device.	The pins of the in.hub device's RS485 socket and the corresponding pins on the Modbus RTU device are not correctly connected.	Check the RS485 socket on the in.hub device to ensure that: • + is connected to bus line A • – is connected to bus line B Note: Occasionally, manufacturers name A and B differently. For this reason, compare the signs of the bus line in the manufacturer's data sheet with our connections and, if necessary, swap the pairing.

Problem	Possible cause	Remedy
Docker-based apps, such as Grafana, Node-RED or Tosi-box, do not start or cannot be opened.	The in.hub device itself has no Internet access – either intentionally to seal off the machine network or unintentionally due to a configuration error. You have three options for troubleshooting.	Fix possible configuration errors: Either allow the firewall on the network to grant access to the Internet by opening TCP ports 80 and/or 443; – or – check the Wi-Fi configuration on the in.hub device yourself; – or – check that the address of the Gateway and, if applicable, the DNS server are entered correctly under Networks > Ethernet 1 (or 2) in the Manual configuration mode.
		Reinstall the Docker container: 1. Download the appropriate Docker container bundle for offline installation from the in.hub download portal. https://download.inhub.de/docker/ 2. Install the bundle under System > Updates.
		Reset the Docker service: 1. Under Monitoring > Storage, click on the Advanced viewing mode and then on the Maintenance button. 2. First, select Remove Docker containers and images and clean up Docker file system: – or – if that doesn't work: Click on Remove all Docker files and reinstall the Docker containers. 3. Then restart the in.hub device. The apps will re-initialize. 4. If the initialization did not work, download the Docker container bundle for offline installation via the in.hub download portal: https://download.inhub.de/docker/

Problem	Possible cause	Remedy
		and install the bundle under System > Updates .
No further plug-ins can be installed within Grafana and Node-RED.	Docker-based apps are temporarily unable to establish an Internet connection after changes to the firewall rules.	Restart the in.hub device. The firewall is reconfigured together with the Docker service.
The internal memory is full and offline bundles can no longer be installed (e.g. if Grafana or Node-RED is updated manually).	Previous updates of Docker containers that were incomplete or incorrect; – or – Docker containers (In-Graf, Tosibox, Node-RED) that have not been shut down cleanly due to sudden voltage loss; – or – log files from the Docker containers have become too large over time (especially Node-RED).	- Under Monitoring > Storage, click on the Advanced viewing mode and then on the Maintenance button. - Select Remove Docker containers and images and clean up Docker file system: - Confirm the Docker cleanup with Yes.
Communication problems with the Modbus TCP connection	Under certain circumstances, a very simple TCP/IP network stack and/or Modbus protocol stack, especially on microcontroller-based devices, may only be able to receive and answer individual requests. If several requests arrive in succession or bundled in a TCP packet, the device may not be able to handle the requests and may go into an error state.	- Navigate to I/O management > I/O units and open the Modbus TCP client where the transmission problems are occurring. High efficiency is set by default under TCP packet flow optimization. Therefore, switch to either Low latency or Half-duplex to simplify the sequence and compilation of Modbus queries. - Save the change and check whether communication now works.

Problem	Possible cause	Remedy
The results of signal processing are 0 or incorrect. You have entered mathematical expressions on the Signal processing tab that cannot be evaluated correctly by the expr-eval library.	Since SIINEOS version 2.7.4, mathematical expressions have been calculated using an improved method for both signal processing and custom 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 accordingly.	Navigate to the Signal processing tab and convert your mathematical formulae according to the specifications of the expr-eval library: https://github.com/in-hub/expr-eval#expression-syntax

This document is available in electronic form in the download portal of in.hub. Printed versions or copies not explicitly provided by in.hub are deemed uncontrolled.

The original language of this document is German.

Made in Germany.

Service & Support: service@inhub.de | <https://community.inhub.de/>

in.hub Download portal: <https://download.inhub.de/>



in.hub GmbH
Technologie-Campus 1
DE-09126 Chemnitz

+49 371 335 655 00
info@inhub.de