SIEMENS

SIMATIC

IOT Gateway MQTT

Operating Manual

06/2021

A5E45868122-AE

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E45868122-AE
Ⓟ 06/2021 Subject to change

Table of contents

Introduction 1

Overview

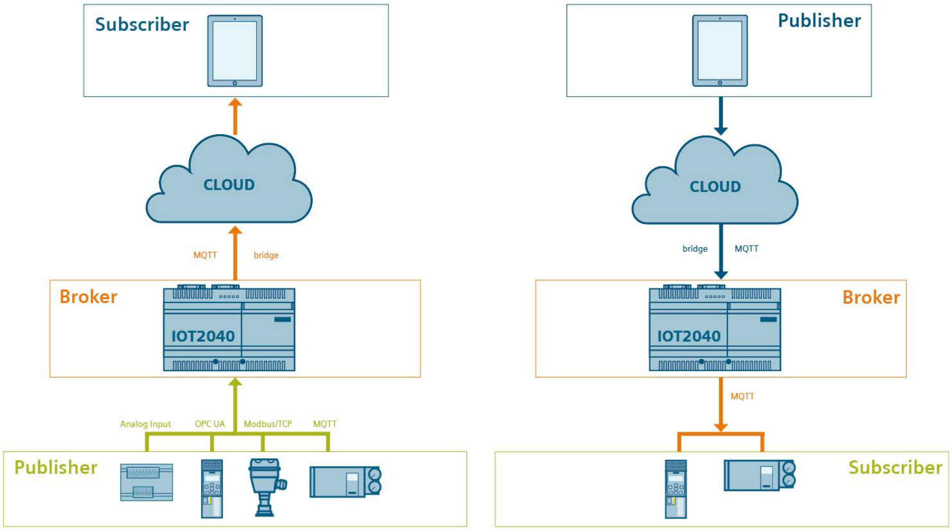
MQTT (Message Queuing Telemetry Transport) is an M2M protocol (machine-to-machine), which is used for small bandwidths and user data. MQTT enables resource-saving communication. Information about this standard can be found on the Internet: MQTT (https://mqtt.org/)

MQTT follows the rules of topic-based Publisher-Subscriber communication with the following devices:

- A **Publisher** (sender) publishes information about various topics.
- When the **Subscriber** (receiver) subscribes to a topic, it will get all the information about that topic.
- The **MQTT-Broker** mediates between Publisher and Subscriber, neither of which must know the other (IP address) nor be executed at the same time (asynchronous communication).

The SIMATIC IOT2040 hardware runs the MQTT software, which is conveniently managed via a Web interface. Hardware and software are available as "IOT Gateway MQTT" bundle, referred to hereafter as "IoT box" for short.

The documentation for the SIMATIC IOT2040 is available on the Internet: SIMATIC IOT2020, IOT2040 Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109741658)



The IoT box works as MQTT Broker:

- The MQTT devices send topics from the field level to the IoT box. The values are read cyclically from the Modbus/TCP and OPC UA devices and made available as topics. (Publisher)
- The IoT box sends these topics over the Internet to the configured cloud.
- A Subscriber can subscribe to the topics from the cloud or from the IoT box.

The Web interface of the IoT box is only accessible locally, not over the Internet.

Example of possible communication paths

Communication path Field level → Cloud:

- **MQTT device**: An MQTT sensor in the plant network acting as the Publisher sends the topic "Plant1/Machine2/Temperature sensor3/Temperature" to the IoT box. The IoT box forwards the topic to the cloud. Subscriber that have subscribed to the topic receive this message.
- **Modbus/TCP device**: The IoT box cyclically reads out a configured Register or a single bit via Modbus/TCP from the Modbus/TCP device. The IoT box "maps" the Modbus / TCP data to a topic and sends it as Publisher to the cloud. Subscriber that have subscribed to the topic receive this message.

Communication path Cloud → Field level:

- The cloud as Publisher sends a topic to the IoT box.
- If devices in the system network subscribe to the topic on the IoT box as Subscriber, they receive the corresponding data.

You can find more information on the Internet: Customer Support (https://support.industry.siemens.com/cs/ww/en/view/109761683)

General rules

All text entries such as topics, names and passwords have a maximum length of 256 characters.

OSS clearing document (Page 39) (overview of OpenSource components)

See also

Operating Instructions IOT2000 Extension Modules (https://support.industry.siemens.com/cs/ww/en/view/109745681)

Security Information 2

Industrial Security

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer’s exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under (https://www.siemens.com/industrialsecurity).

Disclaimer for third-party software updates

This product includes third-party software. Siemens AG only provides a warranty for updates/patches of the third-party software, if these have been distributed as part of a Siemens software update service contract or officially released by Siemens AG. Otherwise, updates/patches are undertaken at your own risk. You can find more information about our Software Update Service offer on the Internet at Software Update Service (https://support.industry.siemens.com/cs/ww/en/view/109759444).

Notes on protecting administrator accounts

A user with administrator privileges has extensive access and manipulation options in the system.

Therefore, ensure there are adequate safeguards for protecting the administrator accounts to prevent unauthorized changes. To do this, use secure passwords and a standard user account for normal operation. Other measures, such as the use of security policies, should be applied as needed.

Passwords

There are no preset passwords for "IoT Gateway MQTT". When the IoT box is put into operation for the first time, the user must assign an administrator password. This password provides the user with full read and write access to the IoT box. If the user accesses the IoT box without entering the password, only read access to the diagnostics is possible.

Communication via Ethernet

In Ethernet-based communication, end users themselves are responsible for the security of their data network. The proper functioning of the device cannot be guaranteed in all circumstances; targeted attacks, for example, can lead to overload of the device.

Network settings

The following table shows the network settings of the IoT box for configuration and communication:

Name	Port number	Transport protocol	Direction	Function
HTTP	80, 9001	TCP	Inbound	This service is used for the configuration of the IoT box.
MQTT	1883, 8883	TCP	Inbound, Outbound	This service is used for the MQTT communication.
Modbus/TCP	502	TCP	Inbound, Outbound	This service is used for the Modbus/TCP communication.

Start

3

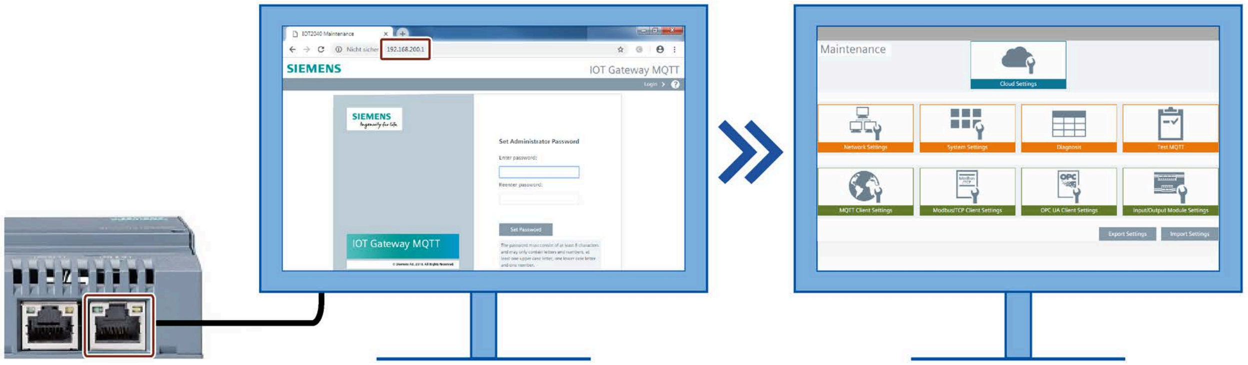
Requirements

- The IoT box is connected to the cloud via the "X1 P1 (Cloud)" interface and Internet.
- The IoT box is connected to the system network via the "X2 P1 (Bus)" interface.
- A PC with the Chrome Web browser from which you open the Web interface of the IoT box.
- The PC is connected to the same network as the IoT box.
- The Internet address of the IoT box is 192.168.200.1 (default setting).
- The network mask is set to 255.255.255.0.
- The PC is located in the same subnet the first time it is accessed.

Note

Licensing conditions

The software is stored on the SD card, which may not be removed from the IoT box for licensing reasons. The SD card is taped over with a seal and secured. **Opening the seal is considered a breach of the license agreement**.



The password must consist of at least 8 characters and may only contain letters and numbers, at least one upper case letter, one lower case letter and one number.

Call

1. Turn on the PC and the IoT box.
2. Open the Chrome Web browser on the PC.
3. Enter the IP address "192.168.200.1" as the Internet address (default setting, see Requirement).

The PC connects to the IoT box and the Web interface of the IoT box opens.

When accessing the IoT box for the first time, an administrator password must be assigned. This gives you full read and write access to the settings. With each additional opening of the Web interface, the Maintenance view is opened in read-only mode.

Reset and Reset-to-Factory

When you press the RESET button, the IoT box restarts.

To reset the box to factory settings (Reset-to-Factory), proceed as follows:

1. Press the RESET button.
2. Then press and hold the USER button. The USER LED will briefly light up orange and then flash.
3. Keep the USER button pressed until the USER LED goes out. This can take up to 20 seconds.

NOTICE

Data loss

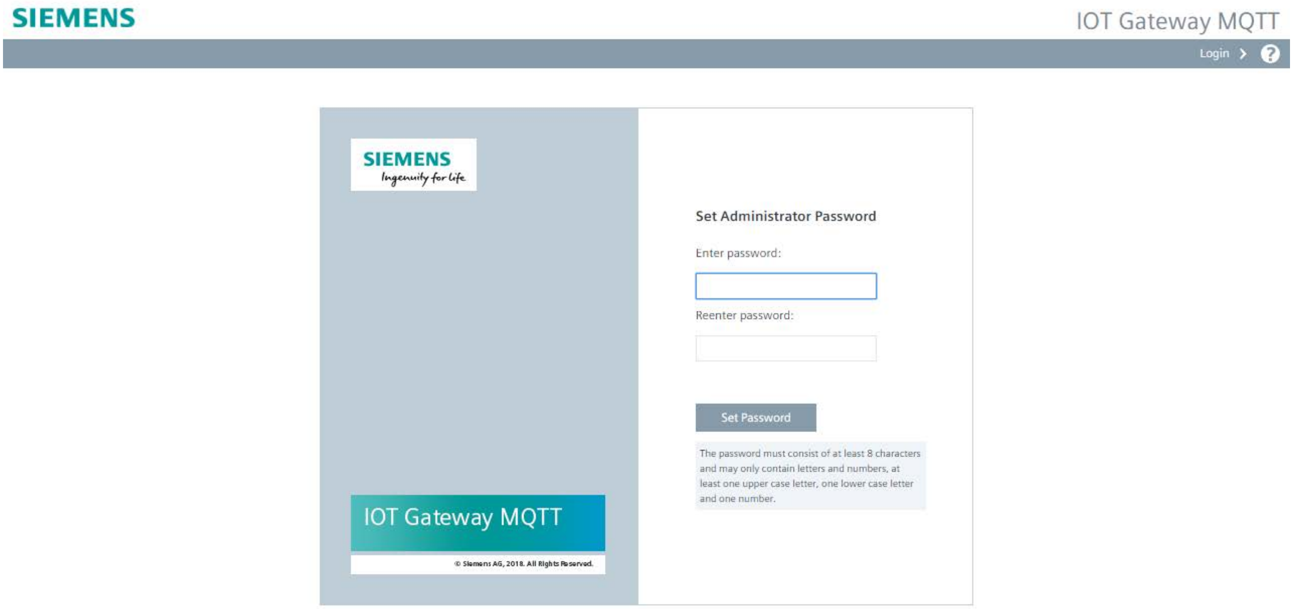
Resetting to factory settings clears all your parameter settings.

When the devices are switched off or the power supply fails, it is not ensured that the adjustable parameters are transferred correctly. This also applies to unavailability of the Internet (Denial of Service DoS), for example, due to an overload of the data network or a cyber attack.

Login

4

The following figure shows the "Login" tile:



Set Administrator Password

Enter password:

Reenter password:

The password must consist of at least 8 characters and may only contain letters and numbers, at least one upper case letter, one lower case letter and one number.

General

The login dialog appears when you access the Web interface as a user from your PC for the first time.

1. Enter a password according to the following criteria:
   - At least 8 characters long
   - Upper and lower case letters
   - At least one number
2. Close the dialog with the "Login" button.

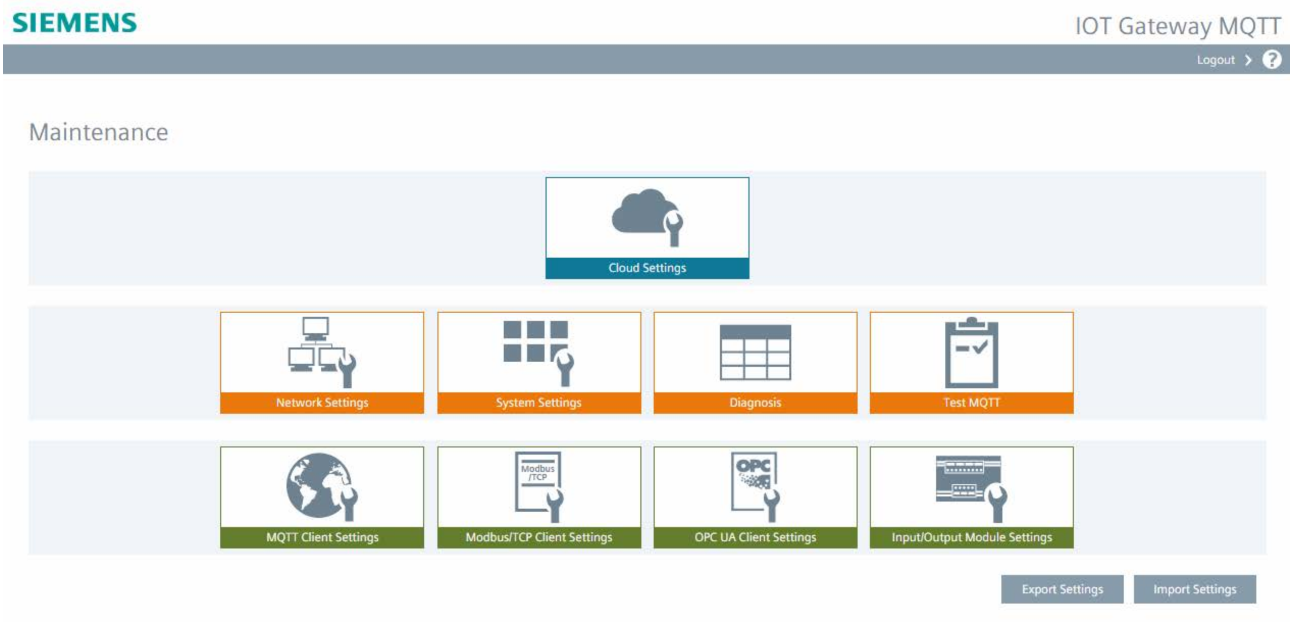
   The PC from which you access the Web interface is now registered as administrator with this password. Accordingly, you have read and write access to all adjustable parameters.

Note

Only one administrator can be logged in at the same time. If a 2nd administrator logs on/in, the 1st administrator is logged out. All other users must reload the Web interface.

Maintenance 5

The following figure shows the "Maintenance" tile:



Underlying information

- Introduction (Page 5) in MQTT
- Start (Page 9) (requirements, call, reset)
- Security Information (Page 7) Industrial Security for secure operations of devices and networks to defend from cyber threats

Basic navigation

The parameterizable areas are displayed as tiles on the "Maintenance" overview page.

- Clicking on a tile opens the corresponding page.
- "?" opens the context-sensitive dialog help.
- "Login": If Login is successful, you will receive full read and write access.

If you are not logged in, you only have read access to the diagnostics tile. All other tiles are grayed out. To get read and write access to all tiles, log in using the "Login" button at the top right.

An automatic logout occurs after 30 minutes of inactivity.

Meaning of the tiles

The displayed tiles form the "levels" of the system according to:

- The top, blue tile indicates the cloud.
- The middle, orange tiles indicate the setting options of the IoT box as MQTT Broker.
- The bottom, green tiles indicate the setting options at the field level.

Export and import of settings

With the help of the "Export Settings" and "Import Settings" buttons, you can export or import the settings via USB stick.

The settings are stored in two files in JSON format:

- syssettings.conf contains the system data
- connectivitysettings.conf contains the communication data for MQTT, Modbus/TCP and OPC UA and Input/Output Modules

To **Export**, proceed as follows:

1. Log in using the "Login" button at the top right.
2. Insert a USB stick into the IoT box.
3. Click "Export Settings". The two files referred to above and the settings made are stored on the USB stick. The certificates of the OPC UA Servers are not included in the export.
4. If necessary, you can edit these files with suitable tools. The file names must remain the same.

To **Import**, proceed as follows:

1. Log in using the "Login" button at the top right.
2. Insert the USB stick with the two files into the IoT box.
3. Click "Import Settings". The data from the conf files is imported - including the password.
4. The certificates of the OPC UA Servers are not part of the configuration data. After an import the certificates have to be loaded manually in the OPC UA tile. The certificates to be loaded are indicated by a red key behind the device.
5. The OPC UA Devices that are imported with the security policy "none" are set to the status "disable". These have to be set in the OPC UA tile to "enable" so that the data can be read.

NOTICE

Data loss during import

All existing data is overwritten during the import. If necessary, save the settings beforehand with an export.

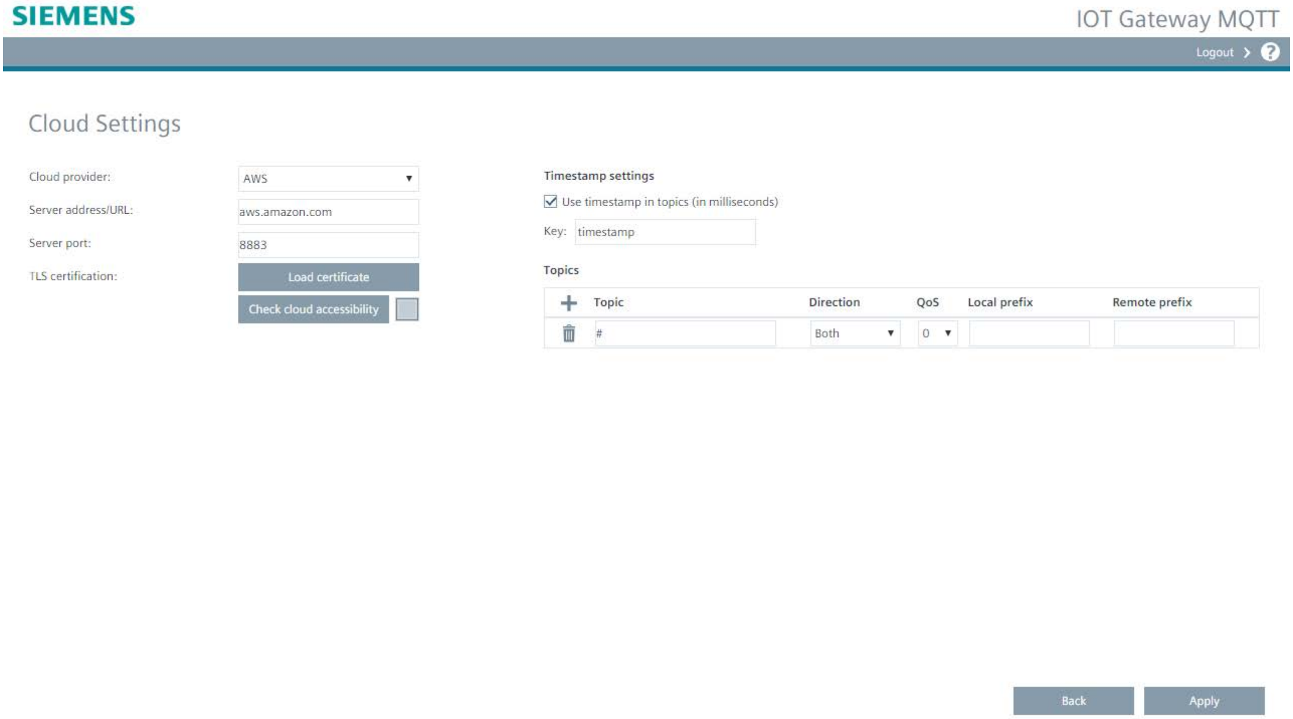
Additional information

- Meaning of User LED status indicator (Page 37)
- OpenSource components (Page 39)
- Recycling and disposal (Page 39)
- Service and support (Page 40) with support and contacts

Cloud Settings

6

The following figure shows the "Cloud Settings" tile:



Cloud Settings

Cloud provider: AWS

Server address/URL: aws.amazon.com

Server port: 8883

TLS certification:

Timestamp settings

☑ Use timestamp in topics (in milliseconds)

Key: timestamp

Topics

+	Topic	Direction	QoS	Local prefix	Remote prefix
🗑	#	Both	0		

General

The parameters of the cloud to which the topics are to be sent from the field level are set in this tile.
Cloud "None" can be selected as an alternative to cloud coupling. This enables the IOT Gateway to be operated as a Modbus/TCP server.

Cloud settings

Select your desired cloud from the drop-down menu. The two clouds "AWS" and "Azure" are already preconfigured. If a different cloud is to be used, it can be configured manually using the "Custom" entry.

Depending on the cloud used, various parameters are necessary. The following parameters are possible: "Connection name", "Server address/URL", "Serverport", "User", "Password", "Client ID", "MQTT protocol version" and "TLS version". The necessary information can be found on the page of the corresponding cloud provider.

Certificate for TLS protocol

The topics are sent to the cloud via a secure Internet connection. Therefore, it is necessary to download a corresponding certificate.

Proceed as follows:

- Download the certificate from your cloud provider to a USB stick.
- In order for the certificate to be read into the IoT box, the files must have specific names, depending on the cloud. If necessary, rename the files:
  - **AWS**:
    aws.root-CA.crt
    aws.cert.pem
    aws.private.key
  - **Azure**:
    azure.root-CA.crt
  - **Custom**: For a Custom Cloud you need to select the files that are used/required.
    custom.root-CA.crt
    custom.cert.pem
    custom.private.key
- Insert the USB stick into the IoT box.
- Click "Load certificate".

Test cloud access

The "Check cloud accessibility" button can be used to test access to the cloud. Successful access to the cloud is indicated by a green box. If access could not be successfully tested, this will be indicated by a red box.

Any errors that occur are shown in the "Diagnosis (Page 23)" tile and indicated by the user LED. An explanation of the errors can be found in section "User LED status indicator (Page 37)".

Time stamp in the topic

The "Use timestamp in topics" check box is used to select whether the current time stamp should also be sent in the topic.

If the check box is selected, the key name of the time stamp can be entered. The default name is 'timestamp'. The time is transmitted in milliseconds since January 1, 1970.

This setting is valid for the tiles "Modbus/TCP Client Settings", "OPC UA Client Settings" and "Input/Output Module Settings". If the topics of the "MQTT Client Settings" tile should contain the time stamp, this must be enabled in the respective MQTT client (Publisher).

Mapping the topics

To allow only certain topics for transfer to the cloud or from the cloud, use this table.

Use the "+" button to add a topic:

- "Topic" denotes the name of the topic, whereby the wildcards "+" and "#" are permitted
- "Direction" denotes the communication path:
  - "In": Receive from the cloud
  - "Out": Send to the cloud
  - "both": Both communication paths
- "QOS" (Quality of Service Level) indicates the degree of reliability with which a topic is transferred:
  - 0: The message is sent once (without acknowledgment of receipt).
  - 1: The message arrives at least once (with acknowledgment of receipt).
  - 2: The message arrives exactly once (with dedicated acknowledgment of receipt).

    The QOS of an incoming message can only be forwarded at the same or a lower level.

Some clouds require a specific prefix to receive the topics, e.g. "**iotgw**/mbtcp/device1/input_voltage". This list allows you to map incoming topics with a local prefix to another (remote) prefix, e.g. "**myaws**/mbtcp/device1/input_voltage":

- Wildcard "#": All topics are preset. However, you can define a specific topic in each line.
- Local Prefix: Enter the existing prefix, e.g. "iotgw/".
- Remote Prefix: Enter the destination prefix, e.g. "myaws/".

If several rules are relevant to a topic, only the first applicable rule from the list is applied.

Cloud "None"

If "None" is selected as Cloud, a Modbus/TCP server can be activated. When the server is activated, the values from the tile "Input/Output Module Settings" are stored in Modbus addresses.

- This data can be read by a Modbus/TCP client via the BUS IP address of the IoT box and port 502.
- Access of the Modbus/TCP clients to the IoT box is established via "X2 P1 (bus)".

For more information, refer to the help of the "Input/Output Module Settings" tile.

Allow all Modbus/TCP clients to connect to IOT2040 and fetch data"

With this selection, requests from all Modbus/TCP devices are permitted. At the same time, only 1 Modbus/TCP client can access the IoT box.

"Allow a specific Modbus/TCP client to connect to IOT2040 and fetch data"

Alternatively, it is possible to allow only one specified Modbus/TCP participant as client.

Note

Error

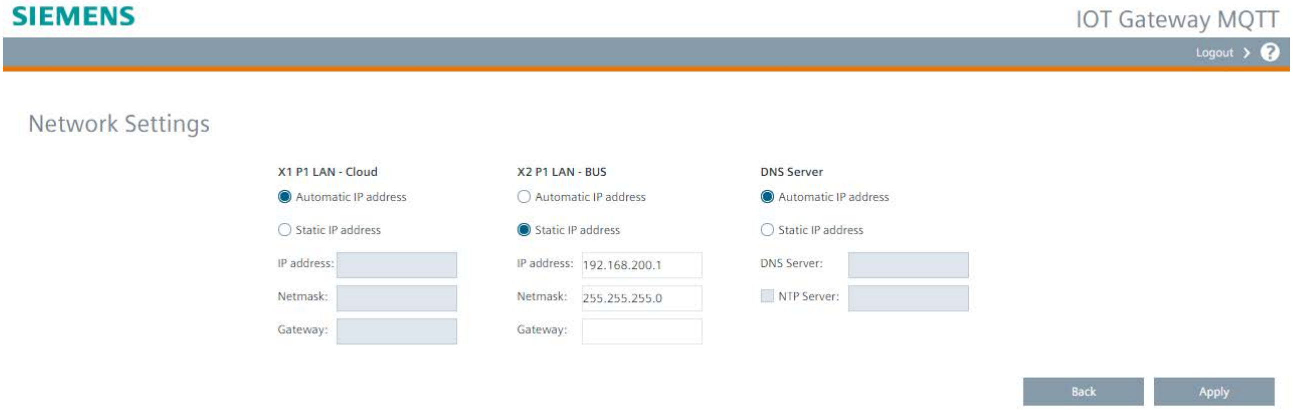
Any errors that occur are indicated by the USER LED. An explanation of the errors can be found in section "User LED status indicator (Page 37)".

Whitelisting recommended:

1. Select "Allow a specific Modbus/TCP client to connect to IOT2040 and fetch data".
2. Enter the IP address of the Modbus/TCP client to be accessed. If another Modbus/TCP client attempts to connect to the IOT2040, this is denied.

Network Settings 7

The following figure shows the "Network Settings" tile:



Network Settings

X1 P1 LAN - Cloud

● Automatic IP address

○ Static IP address

IP address:

Netmask:

Gateway:

X2 P1 LAN - BUS

○ Automatic IP address

● Static IP address

IP address: 192.168.200.1

Netmask: 255.255.255.0

Gateway:

DNS Server

● Automatic IP address

○ Static IP address

DNS Server:

□ NTP Server:

General

This tile is used to specify the settings for the network connections of the IoT box:

X1 P1 LAN - CLOUD

X1 P1 LAN CLOUD designates the interface for connection to the cloud (Internet).

"Automatic IP address" is preset for this interface, i.e. the IP address is assigned via DHCP. If required, the IP address can also be assigned statically.

X2 P1 LAN - BUS

X2 P1 LAN BUS designates the interface for the connection to the system bus.

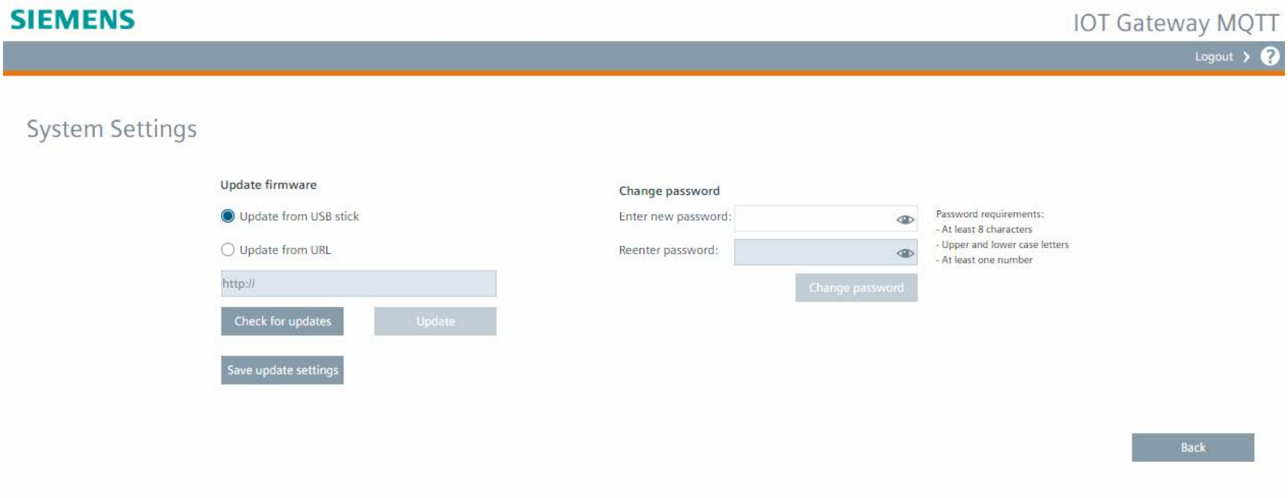
"Static IP address" is preset for this interface. In the delivery state, this address is set to 192.168.200.1. If required, the IP address can be assigned via DHCP.

DNS Server and NTP Server

It is possible to configure the DNS server automatically or dynamically. If a specific clock time is to be used, an NTP server can be configured.

8 System Settings

The following figure shows the "System Settings" tile:



Update firmware

● Update from USB stick

○ Update from URL

http://

Change password

Enter new password:

Reenter password:

Password requirements:
- At least 8 characters
- Upper and lower case letters
- At least one number

General

In the System Settings, a firmware update can be performed and the password can be changed.

Firmware update

The firmware update is possible via the USB stick or via URL. If a URL is configured or a USB flash drive is plugged, a check whether a firmware update is available is carried out when the Maintenance page is opened.

Via USB stick:

1. Select the "Update from USB-Stick" check box.
2. Insert the USB stick with the new firmware file fw.tar into the IoT box. The name of the firmware update file must not be changed.
3. Click "Check for Updates". If the test was successfully completed, the "Update" button will be activated.
4. Execute the Update by clicking "Update".

Via URL:

1. Select the "Update from URL" check box.
2. Enter the Internet address where the firmware update is available.
3. Click "Check for Updates". If the test was successfully completed, the "Update" button will be activated.
4. Execute the Update by clicking "Update".

All configured settings are retained during a firmware update. If the firmware update fails, the previous version will be executed.

The set settings can be saved by using the "Save update settings" button. After a firmware update, delete the browser cache to ensure that no obsolete data is displayed.

NOTICE

Firmware update

A version downgrade is possible, but only if the major version is not smaller.

Changing the password

To change the password, use the "Change password" button.

The password criteria are:

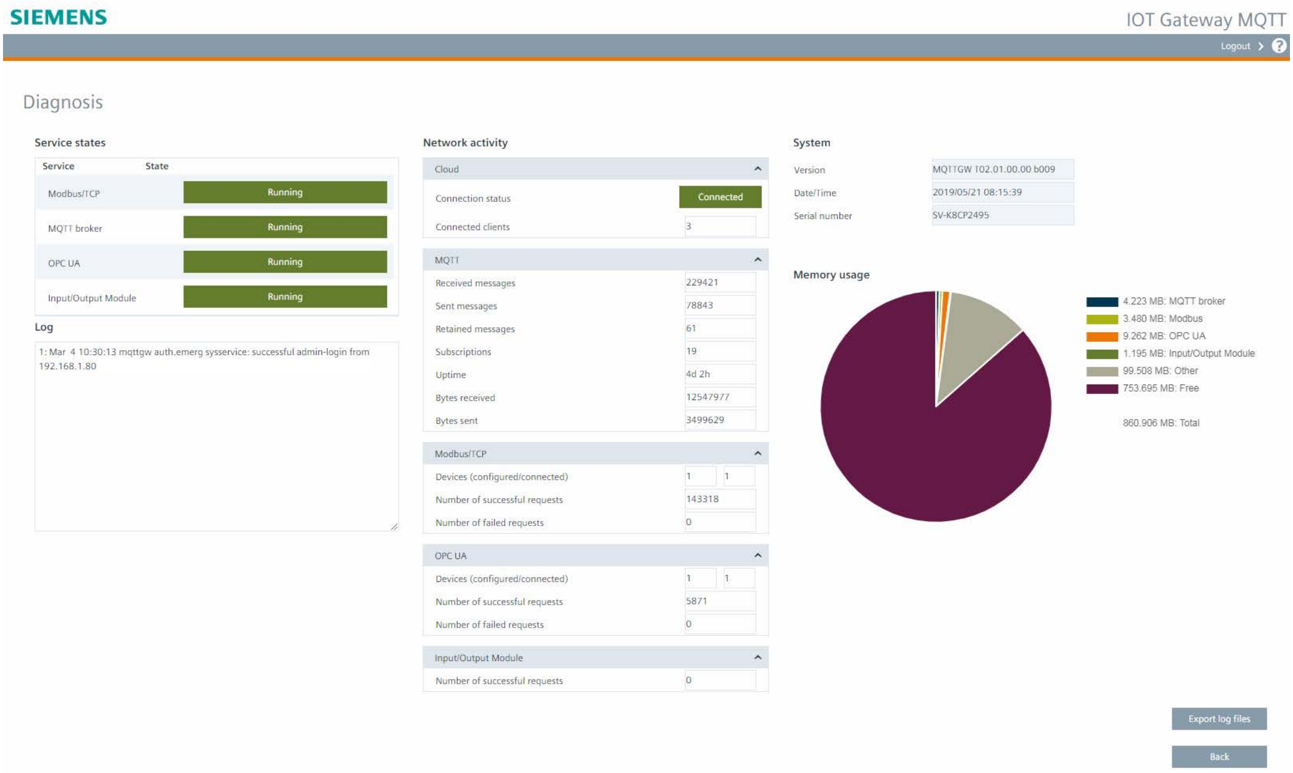
- At least 8 characters long
- Upper and lower-case letters
- At least one number

See also

Login (Page 11)

9 Diagnosis

The following figure shows the "Diagnosis" tile:



Diagnosis

Service states

Service	State
Modbus/TCP	Running
MQTT broker	Running
OPC UA	Running
Input/Output Module	Running

Log

```
1: Mar  4 10:30:13 mqttgw auth.emerg sysservice: successful admin-login from
192.168.1.80
```

Network activity

Cloud	
Connection status	Connected
Connected clients	3

MQTT	
Received messages	229421
Sent messages	78843
Retained messages	61
Subscriptions	19
Uptime	4d 2h
Bytes received	12547977
Bytes sent	3499629

Modbus/TCP		
Devices (configured/connected)	1	1
Number of successful requests	143318	
Number of failed requests	0	

OPC UA		
Devices (configured/connected)	1	1
Number of successful requests	5871	
Number of failed requests	0	

Input/Output Module	
Number of successful requests	0

System

Version	MQTTGW T02.01.00.00 b009
Date/Time	2019/05/21 08:15:39
Serial number	SV-K8CP2495

Memory usage

4.223 MB: MQTT broker
3.480 MB: Modbus
9.262 MB: OPC UA
1.195 MB: Input/Output Module
99.508 MB: Other
753.695 MB: Free

860.906 MB: Total

General

The "Diagnosis" tile displays information about the system and network activity.

"**Service states**" displays the state of the "Modbus/TCP", "MQTT Broker" and "OPC UA" and "Input/Output Modules" services.

The current diagnostic messages are shown in the "**Log**" output field.

"**Network Activity**":

- The status of the cloud connection as well as the number of
  - connected clients
  - received, sent and retained messages
  - subscriptions
  - uptime of the Mosquitto (internally used MQTT message broker) and
  - sent and the received bytes are displayed.
- If the Modbus/TCP server is activated instead of a cloud, "Connection status" indicates whether a Modbus/TCP client has connected to the IoT box. The number of
  - error-free and faulty telegrams are displayed.
- Modbus/TCP and OPC UA: The number of
  - configured and connected devices
  - error-free and faulty telegrams are displayed.
- Input/Output Modules: The number of
  - error-free telegrams are displayed.

The number of transferred messages and bytes also include the system-internal communication between the components.

The network activities can be opened and closed using the arrow.

"**System**" displays device data such as the firmware version, time stamp, serial number of the IoT box and memory usage.

Any errors that occur are indicated by the USER LED. An explanation of the errors can be found in section "User LED status indicator (Page 37)".

You can find more information on the Internet: Customer Support (https://support.industry.siemens.com/cs/ww/en/view/109761683)

Export log file

Activities and system messages are logged during runtime, for example, actions such as:

- Importing the settings
- Login via "Login"
- Error messages regarding the communication

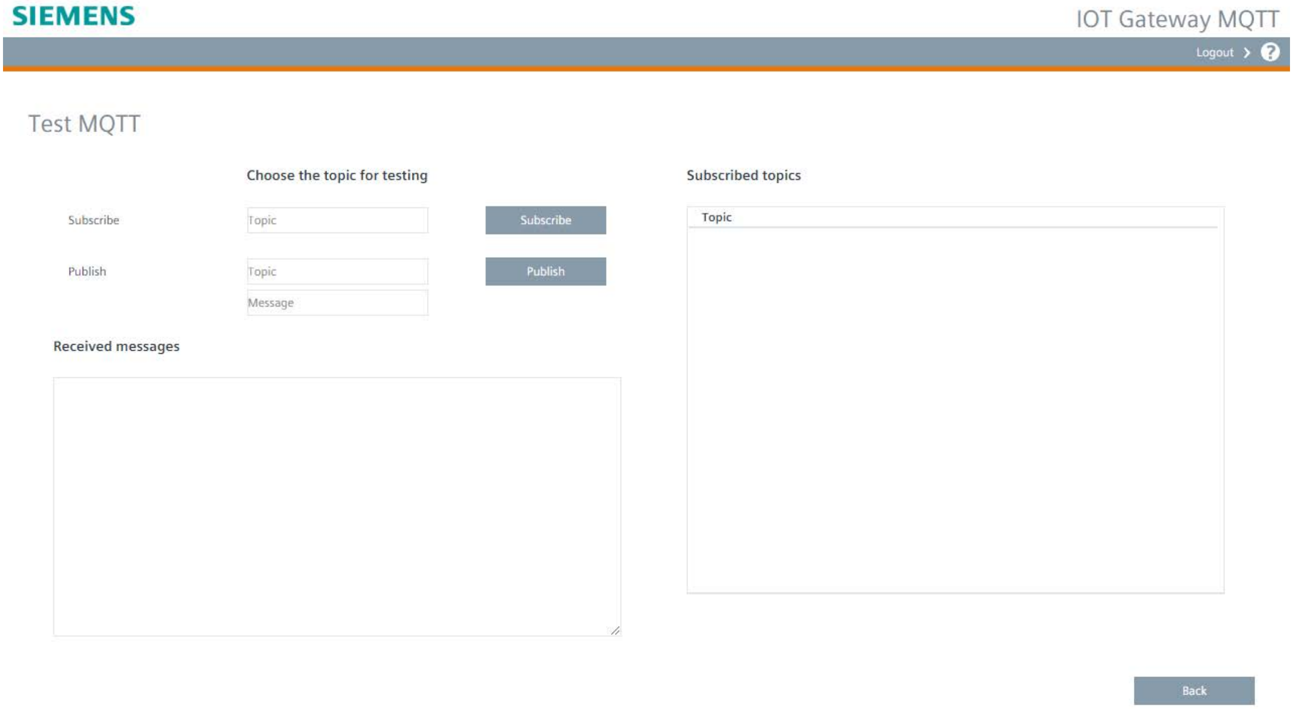
To export the log file to a plugged-in USB stick, use the "Export Log File" button. This is possible even without Login.

See also

Cloud Settings (Page 15)

10 Test MQTT

The following figure shows the "Test MQTT" tile:



General

In this tile, it is possible to test subscribing and publishing a topic using the configured "Cloud Settings".

This requires the cloud to be correctly configured and "Check accessibility" to be successfully performed. UTF-8 encoded characters can be used.

Subscribe

Enter the topic to be tested in the Subscribe field. Click "Subscribe".

If the message could be processed without errors, the entry is entered in the output field on the right. The topic can be deleted again via the recycle bin.

Publish

Enter the topic and the message to be sent in the Publish field. Click "Publish".

Result field

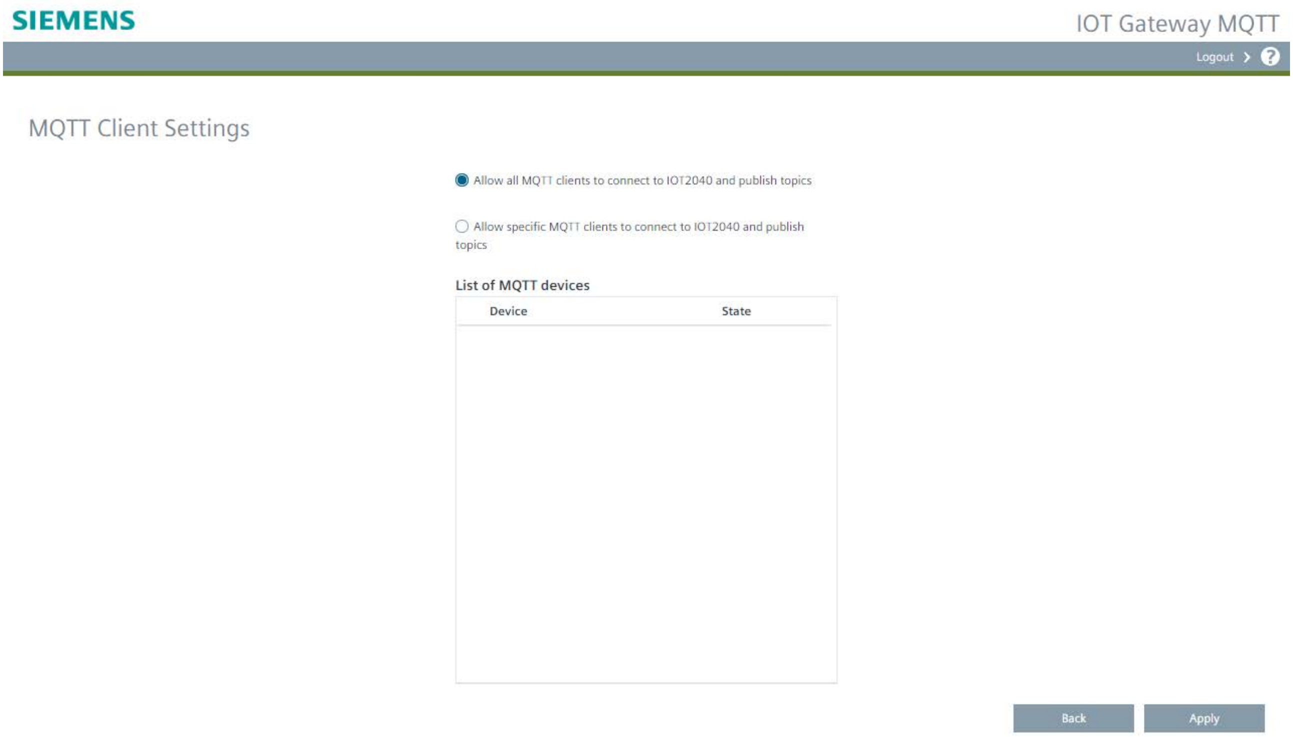
The result field displays the received messages and broker status messages.

If the direction is set to "both" in the cloud settings, two entries are displayed for each topic sent.

MQTT Client Settings

11

The following figure shows the "MQTT Client Settings" tile:



MQTT Client Settings

● Allow all MQTT clients to connect to IOT2040 and publish topics

○ Allow specific MQTT clients to connect to IOT2040 and publish topics

List of MQTT devices

Device	State

General

The MQTT devices are configured in this tile. The MQTT devices can log onto the IoT box via port 1883 as publishers and send topics unencrypted. The topics are then encrypted and forwarded to the cloud.

Project data

A maximum of 32 MQTT devices can be connected to the IoT2040 as publisher.

"Allow all MQTT clients to connect to IOT2040 and publish topics"

This selection allows all requests from MQTT devices.

"Allow specific MQTT clients to connect to IOT2040 and publish topics"

Alternatively, it is possible to allow only certain MQTT devices as Publisher. You use the "+" icon to add a new client as a Publisher. You delete the client using the "Recycle Bin" icon.

The entered device name is used as "User name", which must be unique. A password is not assigned.

The "on/off" switch can be used to deactivate a device during the commissioning phase; the device will not be processed.

- "on": MQTT device is active and can send data.
- "off": MQTT device is inactive, requests are not processed.

Note

Error

Any errors that occur are indicated by the USER LED. An explanation of the errors can be found in section "User LED status indicator (Page 37)".

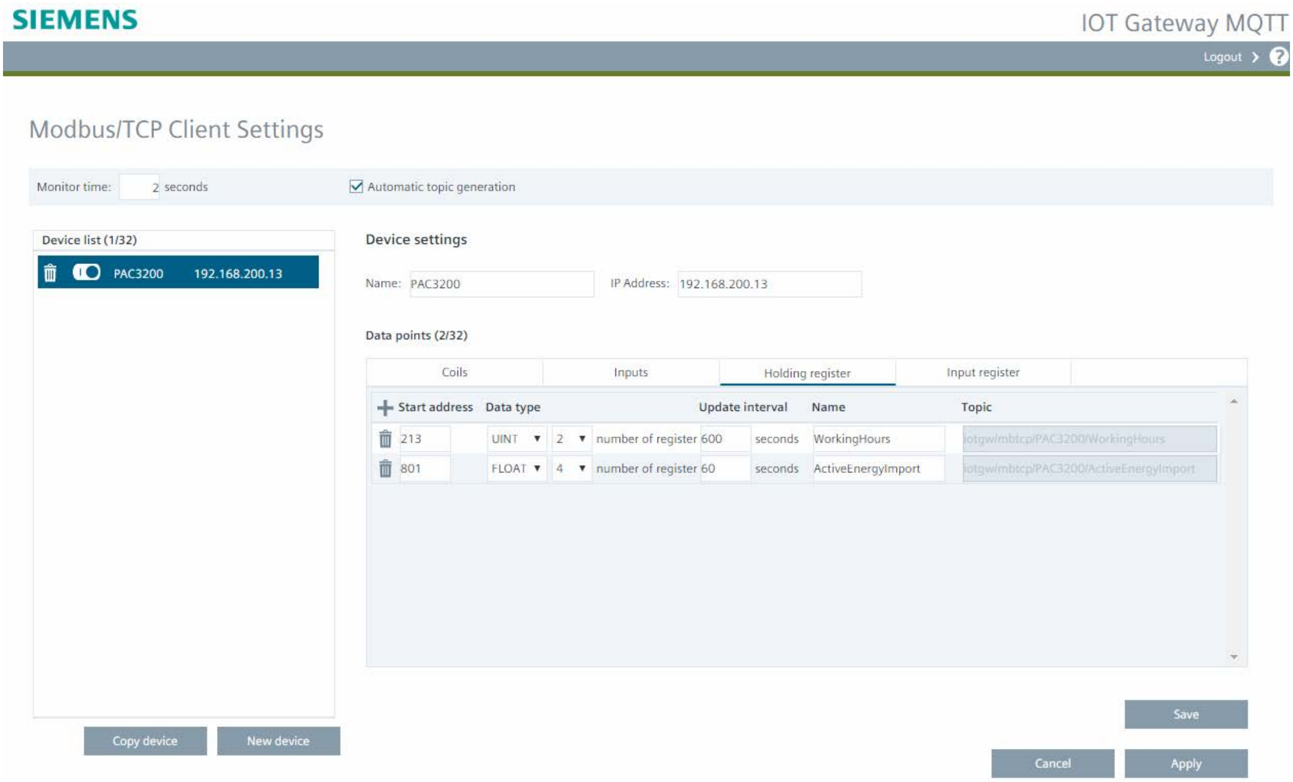
Whitelisting recommended:

1. Select "Allow specific MQTT clients to connect to IOT2040 und publish topics".
2. In the whitelist, specify the MQTT clients that can connect and submit topics using their logon names.

   Other MQTT clients not in the whitelist that attempt to connect to the IOT2040 are denied.

Modbus/TCP Client Settings 12

The following figure shows the "Modbus/TCP Client Settings" tile:



Monitor time: 2 seconds

☑ Automatic topic generation

Device list (1/32)

PAC3200 192.168.200.13

Device settings

Name: PAC3200

IP Address: 192.168.200.13

Data points (2/32)

Start address	Data type			Update interval		Name	Topic
213	UINT	2	number of register	600	seconds	WorkingHours	iotgw/mbtcp/PAC3200/WorkingHours
801	FLOAT	4	number of register	60	seconds	ActiveEnergyImport	iotgw/mbtcp/PAC3200/ActiveEnergyImport

General

This tile contains the configuration of the Modbus / TCP devices and the values to be read out from these devices. The configured values are read cyclically and sent to the cloud. Reading from the Modbus / TCP devices is unencrypted, sending of data to the cloud is encrypted. You can find the Modbus addresses and the data width (length) in your Modbus / TCP device manual.

Project data

The maximum number of configurable Modbus / TCP devices is 32. Up to 64 data points can be read per Modbus / TCP device.

Monitor time

The reading of the Modbus values is time-monitored for each device. If the configured data points cannot be read out in the monitoring time specified here, the connection to the device is terminated and re-established.

The default value amounts to 2 s. The smallest value that can be set is 1 s, the maximum value is 60 s.

Modbus / TCP devices

The "New Device" button can be used to add a Modbus/TCP device. A unique name and the IP address must be entered for the device. You delete the device using the "Recycle Bin" icon.

The Modbus addresses to be read for Coils, Inputs, Holding Register and Input Register are entered in the "Datapoints" table. You use the "+" icon to add a new Datapoint. A name must be assigned for each Datapoint. You delete the Datapoint using the "Recycle Bin" icon.

The possible settings regarding addresses, data types and lengths are listed in the following table:

Modbus area	Start address	Data types	Length
Coils / Inputs	0-65535	BOOL	1 bit
		BLOCK	1 - 2000 bits
Holding Register / Input Register	0-65535	INT	1 Register (16 bits)
			2 Register (32 bits)
			4 Register (64 bits)
		UINT	1 Register (16 bits)
			2 Register (32 bits)
		FLOAT	2 Register (32 bits)
			4 Register (64 bits)
		BLOCK	1 - 125 Register

"Update Interval" indicates the interval in seconds at which the value is to be read from the device. The default value amounts to 60 s. The smallest value that can be set is 1 s, the maximum value is 4294967 s.

If a Modbus / TCP device is not to be processed during commissioning, this can be deactivated using the "on/off" switch.

Automatic topic generation

The values read from the Modbus / TCP devices are sent as topics to the cloud. The topic name required for this is automatically formed from a prefix, the device name and the datapoint name with the "automatic topic generation" check box selected. If the topic name is to be assigned manually, clear the check box. Spaces are not permitted in the topic name.

You can use the "Save" button to save the parameter assignment for a Modbus/TCP client.

Note

Error

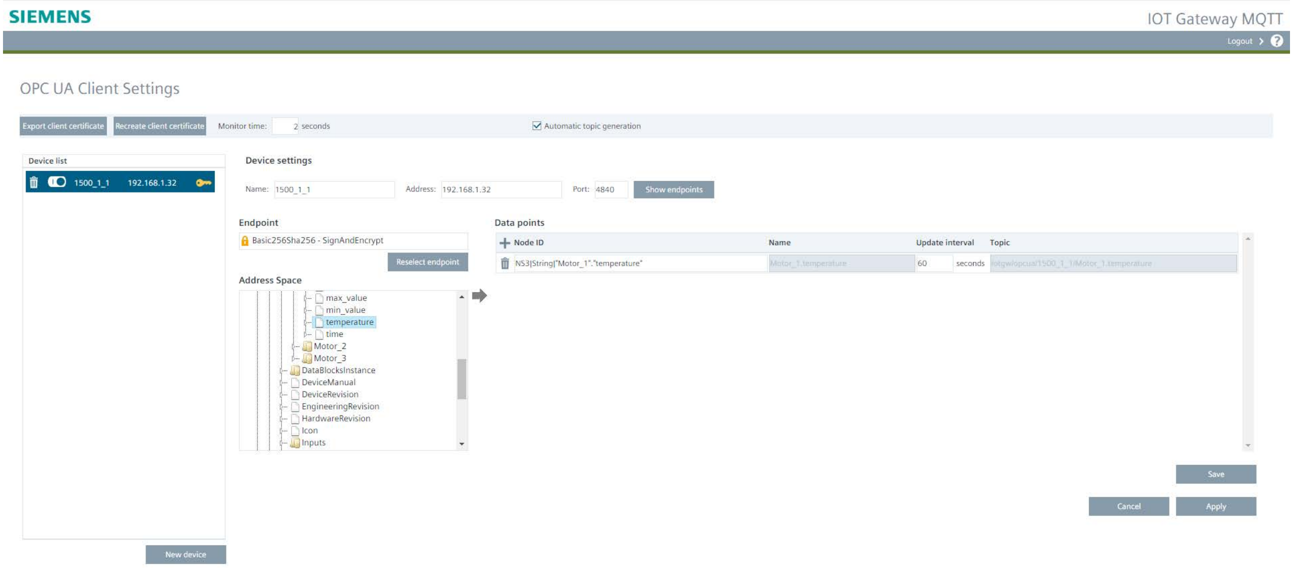
Any errors that occur are indicated by the USER LED. An explanation of the errors can be found in section "User LED status indicator (Page 37)".

Modbus / TCP protocol

Modbus/TCP handling was implemented according to the "MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1b, December 28, 2006".

13 OPC UA Client Settings

The following figure shows the "OPC UA Client Settings" tile:



Monitor time: 2 seconds

☑ Automatic topic generation

Device list

1500_1_1 192.168.1.32

Device settings

Name: 1500_1_1 Address: 192.168.1.32 Port: 4840

Endpoint

Basic256Sha256 - SignAndEncrypt

Address Space

- max_value
- min_value
- temperature
- time
- Motor_2
- Motor_3
- DataBlocksInstance
- DeviceManual
- DeviceRevision
- EngineeringRevision
- HardwareRevision
- Icon
- Inputs

Data points

Node ID	Name	Update interval	Topic
NS3|String|"Motor_1"."temperature"	Motor_1.temperature	60 seconds	iotgw/opcua/1500_1_1/Motor_1.temperature

General

In this tile the configuration of the OPC UA devices and the values to be read out from these devices is carried out. The configured values are read cyclically and sent to the cloud.

Project data

The maximum number of configurable OPC UA devices is 32. Up to 64 data points can be read per OPC UA device.

Client certificate

When delivered from the factory, an OPC UA Client certificate is issued for the IoT2040. This is valid until a reset-to-factory is carried out or the "Recreate client certificate" is pressed. A reset-to-factory and the "Recreate client certificate" button generate a new client certificate.

The certificate can be written to the plugged USB flash drive by using the "Export Client Certificate" button.

Monitor time

The reading of the values is time-monitored for each device. If the configured data points cannot be read out in the monitoring time specified here, the connection to the device is terminated and re-established.

The default value is 2 s. The smallest value that can be set is 1 s, the maximum value is 60 s.

Procedure "Configuring a device"

1. You use the "New device" button to add a new OPC UA- device to the "Device list".

   You use the "on/off" switch to deactivate an OPC UA device that is then not processed during commissioning. You delete a device by using the "Recycle Bin" icon.

2. Under "Device settings", assign a name that is unique in the IOT gateway and the IP address or symbolic name that can be used for addressing via OPC UA and the port number.

3. Click "Show endpoints".

   The existing OPC UA end points of the device are displayed in the "Endpoint" list. If the OPC UA Server cannot be accessed, continue with Item 8.

4. Select the desired end point and click the "Select endpoint" button.

   A dialog is displayed with the transferred certificate of the OPC UA device or, respectively, a note if no protection level has been selected.

   Note: Unencrypted communication

   If the end point "None" is selected for an OPC UA Server, communication is carried out unencrypted.

5. Confirm the certificate or, respectively, the note in the dialog. In the case of a successful exchange of certificates a yellow key is displayed at the device (see the section "Certificate / key display").

   A directory tree is displayed under "Address Space".

6. Navigate through the tree and select the desired data point.

7. Transfer the selected data point to the "Data points" list by using the arrow to the right.

   Alternatively drag-and-drop the selected data point into the "Data points" list.

8. You can also use the "+" icon to add data points manually to the list. You delete the data point by using the "Recycle Bin" icon.

9. Enter the interval in seconds at which the value is to be read from the device in the "Update interval" field. The default value amounts to 60 s. The smallest value that can be set is 1 s, the maximum value is 4294967 s.

The "Reselect endpoint" button can be used to deselect the end point currently selected and select a different end point from the list.

Automatic topic generation

The values read from the OPC UA devices are sent as topics to the Cloud. The topic name required for this is automatically formed from a prefix, the device name and the data point name with the "Automatic topic generation" check box selected. If the topic name is to be assigned manually, clear the check box. Spaces are not permitted in the topic name.

You can use the "Save" button to save the parameter assignment for an OPC UA Client.

Certificate / key display

A yellow key shows that a certificate has been loaded for the device. A red key shows that the certificate has to be loaded. If no key is displayed, communication is carried out unencrypted.

During an import of the configuration the certificates are not included in the import. In order to make fault-free communication possible, the certificate has to be loaded by clicking the red key. In order to update an existing certificate, click the yellow key.

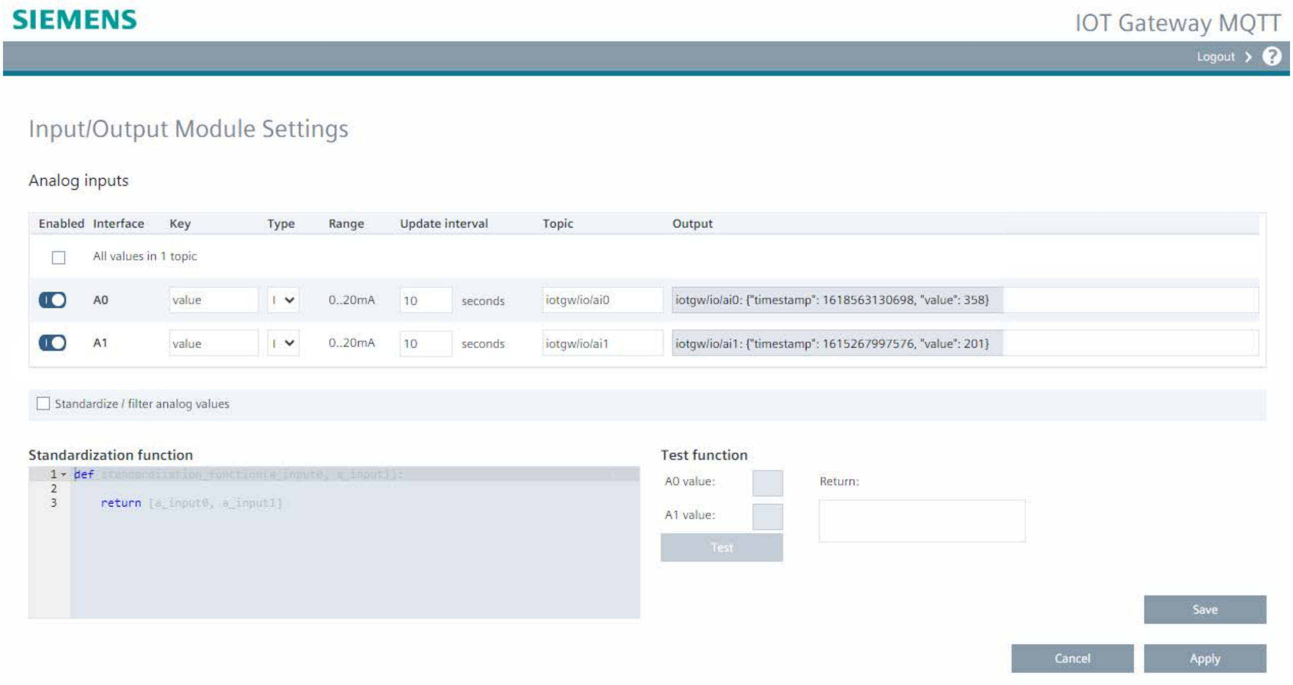
Note: Error

Any errors that occur are indicated by the USER LED. An explanation of the errors can be found in section "User LED status indicator (Page 37)".

Input/output module settings

14

The following figure shows the "Input/Output Module Settings" tile:



Input/Output Module Settings

Analog inputs

Enabled	Interface	Key	Type	Range	Update interval		Topic	Output
☐	All values in 1 topic							
●	A0	value	I	0..20mA	10	seconds	iotgw/io/ai0	iotgw/io/ai0: {"timestamp": 1618563130698, "value": 358}
●	A1	value	I	0..20mA	10	seconds	iotgw/io/ai1	iotgw/io/ai1: {"timestamp": 1615267997576, "value": 201}

☐ Standardize / filter analog values

Standardization function

```
def standardization_function(a_input0, a_input1):

    return [a_input0, a_input1]
```

Test function

A0 value:

A1 value:

Return:

General

An additional hardware module is required to use this tile. The order number of this "Input/Output Module" is 6ES7647-0KA01-0AA2. The documentation is available on the Internet: Operating Instructions IOT2000 Extension Modules (https://support.industry.siemens.com/cs/ww/en/view/109745681)

If the hardware module is inserted, the analog inputs A0 and A1 of the input/output module can be configured. The values are read cyclically and sent to the cloud.

In addition, it is possible to store the values in Modbus addresses, see "Cloud - None" in the "Cloud Settings" tile.

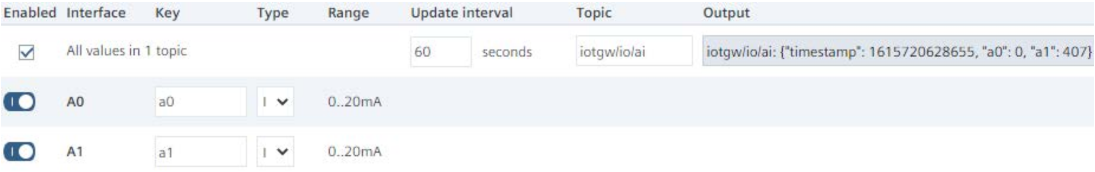
Analog inputs A0 and A1:

The "on/off" switch is used to deactivate an analog input (for example, during commissioning), which is then not processed.

The "Type" selection box determines whether the value is read as a voltage value or current value.

Enter the interval in seconds at which the analog value is to be read in the "Update interval" field. The default value is 60 s. The smallest value that can be set is 0.1 s, the maximum value is 4294967 s.

By selecting the "**All values in 1 topic**" check box, all enabled analog values are written to one topic. If the check box is cleared, the analog values are written individually in topics. If the time stamp has been activated in the cloud settings, the time stamp is saved in the topic in addition to the analog value(s).



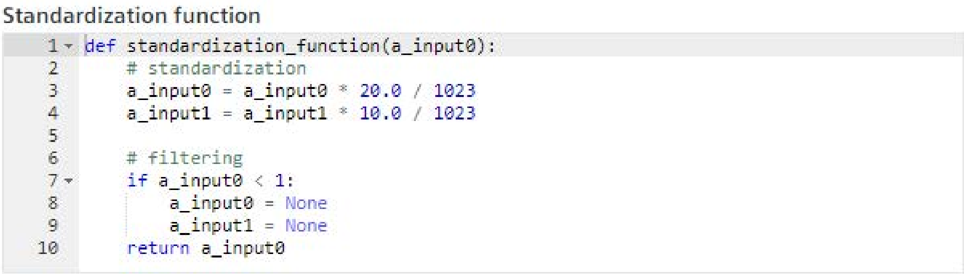
Enabled	Interface	Key	Type	Range	Update interval		Topic	Output
☑	All values in 1 topic				60	seconds	iotgw/io/ai	iotgw/io/ai: {"timestamp": 1615720628655, "a0": 0, "a1": 407}
●	A0	a0	I	0..20mA				
●	A1	a1	I	0..20mA				

If the check box "**Standardize / filter analog values**" is not selected, the read raw values are sent to the cloud as topics. If the check box is selected, the calculated/filtered values are transferred to the cloud as topics. The required topic name is automatically formed from a prefix and the analog input. The topic name can be changed, but spaces are not permitted in the topic name.

Standardization / filter anlaog values

It is possible to normalize and/or filter the read raw values via the "Standardize / filter analog values" check box. If the check box is selected, the update time of A0 is used for both inputs and the code field is enabled. The function is programmed in Python.

Example for a normalization / filtering

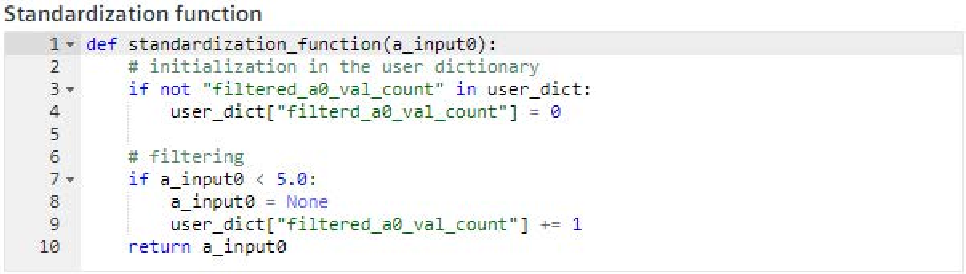


Standardization function

```
def standardization_function(a_input0):
    # standardization
    a_input0 = a_input0 * 20.0 / 1023
    a_input1 = a_input1 * 10.0 / 1023

    # filtering
    if a_input0 < 1:
        a_input0 = None
        a_input1 = None
    return a_input0
```

Additional functions

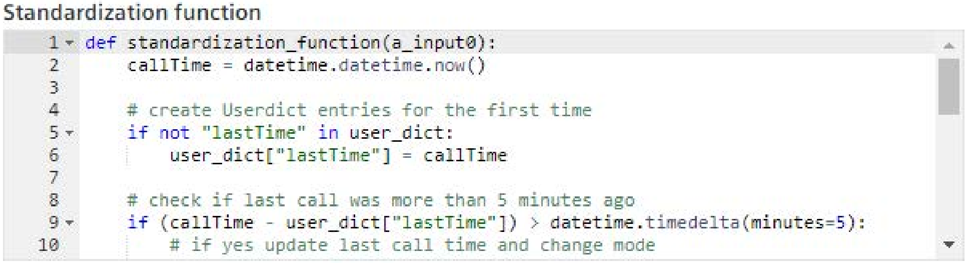
- The use of user-specific tags is possible via the dictionary `user_dict`.



Standardization function

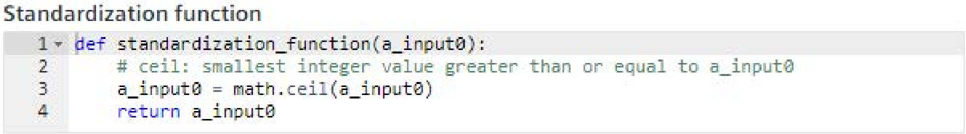
```
def standardization_function(a_input0):
    # initialization in the user dictionary
    if not "filtered_a0_val_count" in user_dict:
        user_dict["filterd_a0_val_count"] = 0

    # filtering
    if a_input0 < 5.0:
        a_input0 = None
        user_dict["filtered_a0_val_count"] += 1
    return a_input0
```

- The libraries `datetime` and `math` are integrated and can be used. The import of additional libraries is not possible.



Standardization function

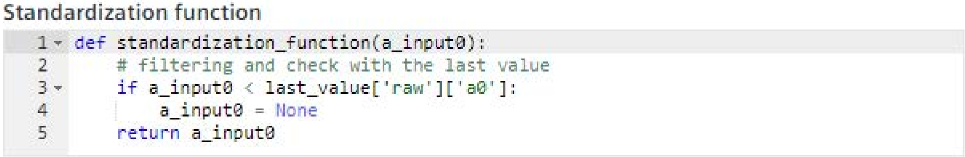
```
def standardization_function(a_input0):
    callTime = datetime.datetime.now()

    # create Userdict entries for the first time
    if not "lastTime" in user_dict:
        user_dict["lastTime"] = callTime

    # check if last call was more than 5 minutes ago
    if (callTime - user_dict["lastTime"]) > datetime.timedelta(minutes=5):
        # if yes update last call time and change mode
```



Standardization function

```
def standardization_function(a_input0):
    # ceil: smallest integer value greater than or equal to a_input0
    a_input0 = math.ceil(a_input0)
    return a_input0
```

- The **last raw values** can be accessed via `last_value['raw']['a0']` and `last_value['raw']['a1']`.



Standardization function

```
def standardization_function(a_input0):
    # filtering and check with the last value
    if a_input0 < last_value['raw']['a0']:
        a_input0 = None
    return a_input0
```

- Accordingly, access to the **last normalized values** is established via `last_value['normalized']['a0']`, `last_value['normalized']['a1']`.

Setting the "None" keyword for one or both analog values causes filtering:

- In this case, the values are not passed to the cloud or to the Modbus/TCP registers.
- This reduces the number of bytes transferred and decreases data traffic.

You can use the test function to check the programmed function. Enter test values for A0 and A1 and press the "Test" button. The calculated values are displayed in the output field. It is possible to enter integers for testing.

"Cloud Settings" - Cloud "None"

If "None" is selected as cloud in the "Cloud Settings", a Modbus/TCP server can be activated. When the server is activated, the analog inputs are stored in Modbus addresses. The current time stamp is stored in Holding Registers 0-3, the analog value 0 in Holding Registers 4 and 5 and the analog value 1 in Holding Registers 6 and 7. If normalization/filtering is activated, the calculated/filtered values are stored in the respective registers.

This data can be read by a Modbus/TCP client via the BUS IP address of the IoT box and port 502.

- individual: 0 to 3, 4 and 5, 6 and 7 or
- shared: 0 to 7

You can use the "Save" button to save the parameter assignment for the analog inputs.

Note

Error

Any errors that occur are indicated by the USER LED. An explanation of the errors can be found in section "User LED status indicator (Page 37)".

15 User LED status indicator

Status	Description
GREEN	Access to the cloud is successful.
GREEN "blinking"	Access to the cloud is running.
RED "flashing"	Access to the cloud has failed.
ORANGE "blinking"	The USB stick is in operation: • The USB stick is active. • Network diagnostics is running. • The configuration file is read.
	A firmware update is being executed.
RED "blinking"	The USB stick has an error: • Read error: The USB memory is damaged. • The configuration file is invalid: damaged, unreadable or configured for another system. • Write error: The USB stick is write-protected or the USB memory is full.
	The IoT box may lose data: • The data transfer is too slow. • The data from the Modbus device could not be received in the configured cycle time. • Errors while publishing information about the MQTT broker.
ORANGE	No connection to the cloud: • The network cable is missing or damaged. • The Ethernet port on the IoT box is defective. • The firewall of the IoT box blocks the connection. • The server is offline. • An addressed server can not be accessed. • Network problems of the provider. • Insufficient access rights.
	No connection to bus / data. • A problem with the network connection of your device. • The network cable is unplugged or damaged. • At least one Modbus device is not connected.
RED	Error during firmware update.
	Fatal system error: Contact Product Support.
OFF	The device is offline: not configured.

Technical support A

A.1 OpenSource components

The software contains open source components. The following information provides an overview of them.

See also

OSS clearing document (https://support.industry.siemens.com/cs/ww/en/view/109761683)

A.2 Recycling and disposal

Legal statement regarding disposal of old devices

European law forbids disposal of electrical and electronic devices in household waste.

- Do **not** dispose the device or its replacement and expansion components in household waste and **not** at public waste disposal points.
- For environmentally compatible recycling and disposal of the device and its components, contact a certified disposal company for electronic waste or your Siemens contact (product return (https://support.industry.siemens.com/cs/ww/en/view/109479891)).

Observe the following:

- Country-specific regulations
- Local legal requirements
- Special information regarding the German Battery Ordinance

See also

WEEE (Page 39)

A.3 WEEE

WEEE Directive

The device is low-emission, recyclable and meets the requirements of the WEEE Directive 2012/19/EU on the disposal of waste electrical and electronic equipment. Siemens AG is registered with Stiftung EAR, WEEE-Reg. No. DE 23691322.

A.4 Service and support

You can find additional information and support for the products described on the Internet at the following addresses:

- Technical support (https://support.industry.siemens.com/cs/us/en/)
- Support request form (https://www.siemens.com/automation/support-request)
- After Sales Information System SIMATIC IPC/PG (https://www.siemens.com/asis)
- SIMATIC Documentation Collection (https://www.siemens.com/simatic-tech-doku-portal)
- Your local representative (https://www.automation.siemens.com/aspa_app)
- Training center (https://siemens.com/sitrain)
- Industry Mall (https://mall.industry.siemens.com)

When contacting your local representative or Technical Support, please have the following information at hand:

- MLFB of the device
- BIOS version for industrial PC or image version of the device
- Other installed hardware
- Other installed software

Current documentation

Always use the current documentation available for your product. You can find the latest edition of this manual and other important documents by entering the article number of your device on the Internet (https://support.industry.siemens.com/cs/us/en/). If necessary, filter the comments for the entry type "Manual".

Tools & downloads

Please check regularly if updates and hotfixes are available for download to your device. The download area is available on the Internet at the following link:

After Sales Information System SIMATIC IPC/PG (https://www.siemens.com/asis)

See also

TIA Selection Tool (https://www.siemens.com/tia-selection-tool)