

## User Guide

# Gateway (edgeGate, uaGate SI, uaGate MB and uaGate 840D)



## Disclaimer of liability

The information contained in these instructions corresponds to the technical status at the time of printing of it and is passed on with the best of our knowledge. Softing does not warrant that this document is error free. The information in these instructions is in no event a basis for warranty claims or contractual agreements concerning the described products, and may especially not be deemed as warranty concerning the quality and durability pursuant to Sec. 443 German Civil Code. We reserve the right to make any alterations or improvements to these instructions without prior notice. The actual design of products may deviate from the information contained in the instructions if technical alterations and product improvements so require.


## OpenSource


To comply with international software licensing terms, we offer the source files of open source software used in our products. For details see <https://opensource.softing.com/>

If you are interested in our source modifications and sources used, please contact: [info@softing.com](mailto:info@softing.com)

## Softing Industrial Automation GmbH

Richard-Reitzner-Allee 6  
85540 Haar / Germany  
<https://industrial.softing.com>

 + 49 89 4 56 56-340

 [info.automation@softing.com](mailto:info.automation@softing.com)  
[support.automation@softing.com](mailto:support.automation@softing.com)

 <https://industrial.softing.com/services/product-support.html>



Scan the QR code to find the latest documentation on the product web page under Downloads.

# Table of Contents

<b>Chapter 1</b>	<b>Introduction.....</b>	<b>5</b>
1.1	About this product.....	5
1.2	System requirements.....	5
1.3	Safety Precautions.....	6
1.4	Feedback to Softing.....	6
<b>Chapter 2</b>	<b>Setting Up the Device.....</b>	<b>7</b>
2.1	Mounting and Dismounting.....	7
2.2	Connecting the Power Supply.....	8
2.3	Configuration and Login.....	9
2.4	Inserting a micro SD Card.....	11
2.5	Connecting to the Network.....	12
2.6	Powering up the Device.....	13
2.7	Resetting the Device.....	13
<b>Chapter 3</b>	<b>Information.....</b>	<b>14</b>
3.1	Gateway Status.....	14
3.2	Help & Support.....	14
3.3	Version.....	15
3.4	Licence Agreements.....	15
<b>Chapter 4</b>	<b>IT Settings.....</b>	<b>16</b>
4.1	IT Network Configuration.....	16
4.2	OPC UA Server.....	17
4.2.1	Generate Server Certificate.....	17
4.2.2	OPC UA Security.....	19
4.2.3	OPC UA Authentication.....	19
4.2.4	Manage Client Certificates.....	20
4.3	MQTT Broker Configuration.....	21
4.3.1	MQTT Topic Settings.....	22
4.3.2	MQTT Topic Selection.....	25
4.3.3	MQTT Security Settings.....	26
4.3.4	MQTT Client Certificate.....	27
4.3.5	MQTT Last Will Settings.....	28
4.3.6	MQTT Cloud Sample Configurations.....	28
<b>Chapter 5</b>	<b>Machine Settings.....</b>	<b>29</b>
5.1	Machine Network.....	29
5.2	PLC Connection.....	30
5.2.1	Siemens S7 Settings.....	31
5.2.1.1	Symbol Import.....	32

5.2.2	Siemens S7-2 Settings .....	33
5.2.2.1	Filtering the Address Space of a Siemens PLC with Optimized Blocks .....	33
5.2.3	Modbus Settings .....	34
5.2.3.1	Symbol Import .....	36
	Modbus Item Syntax.....	37
5.2.4	SINUMERIK 840D Settings .....	42
5.2.4.1	Symbol Import NCK.....	43
5.3	Symbol View.....	43
<b>Chapter 6</b>	<b>Service Settings.....</b>	<b>44</b>
6.1	Time Settings.....	44
6.2	Reset .....	44
6.3	Firmware Update.....	45
6.4	Backup and Restore.....	45
6.5	User Password.....	46
6.6	micro SD Card.....	47
6.7	Support .....	47
<b>Chapter 7</b>	<b>LED Status Indicators.....</b>	<b>48</b>
<b>Chapter 8</b>	<b>Technical Data.....</b>	<b>49</b>
<b>Chapter 9</b>	<b>Declarations of Conformity.....</b>	<b>50</b>



# 1 Introduction

## 1.1 About this product

The Gateway has been designed to integrate OPC UA Server functionality in new and existing plants for easy and secure data connectivity with higher-level management systems, such as ERP, MES or SCADA. The MQTT Publisher functionality allows integrating controller data into IoT Cloud applications.

Softing offers a variety of stand-alone gateway solutions.

For more details see <https://industrial.softing.com/products/gateways.html>.



### Note

Faultless and safe operation of the product requires proper transport, proper storage and installation, and expert operation and maintenance in accordance with the manual.



### Note

If the notes stated in this document are not observed or in case of inappropriate handling of the device, our liability is waived. In addition, the warranty on devices and spare parts does no longer apply.

For information about safety aspects refer to section [Safety Precautions](#)<sup>6</sup>.

## 1.2 System requirements

### Hardware

- PC
- Ethernet switch (optional)

### Supported Browsers

- Mozilla Firefox, version 38 or higher
- Google Chrome, version 10.0 or higher
- Microsoft Edge HTML, version 17.17134 or higher

### 1.3 Safety Precautions



#### CAUTION

This product contains a lithium backup battery. The lithium content is less than 1 g. The battery has been successfully tested by the manufacturer in accordance with the "Manual of Tests and Criteria" of the United Nations (UN), Part III: Classification procedures, test methods and criteria, sub-section 38.3.

If the product is handled properly, this battery does not need to be replaced during the lifetime of the product. Therefore, opening the product is unnecessary and not permitted. The product must only be operated within the specified temperature range. Do not expose to heat above this temperature range and keep away from open fire. Store in a dry place. Improper handling of lithium batteries can cause the batteries to ignite or explode and pose a burn hazard to users.



#### CAUTION

During operation, the device's surface will be heated up. Avoid direct contact. When servicing, turn off the power supply and wait until surface has cooled down.



#### Note

Do not open the housing of the Gateway. It does not contain any parts that need to be maintained or repaired. In the event of a fault or defect, remove the device and return it to the vendor. Opening the device will void the warranty!

### 1.4 Feedback to Softing

Softing likes to encourage you to provide feedback and comments to help us improve the documentation.

Please send your comments to the e-mail address [support.automation@softing.com](mailto:support.automation@softing.com). If you have a PDF copy of this document available, please add your comments and suggestions to the PDF file using the editing tool in Adobe Reader and send it to Softing.

Please ensure to include the following information in your feedback communication:

- Document title
- Document version (as shown on cover page)
- Page

## 2 Setting Up the Device

### 2.1 Mounting and Dismounting



#### Note

Make sure the Gateway is mounted in a manner that the power supply disconnecting device or interrupt facility can always be reached easily.



#### Note

Depending on the installation position, the maximum ambient operating temperature may differ. Refer to [Technical Data](#)<sup>49)</sup> for detailed information.

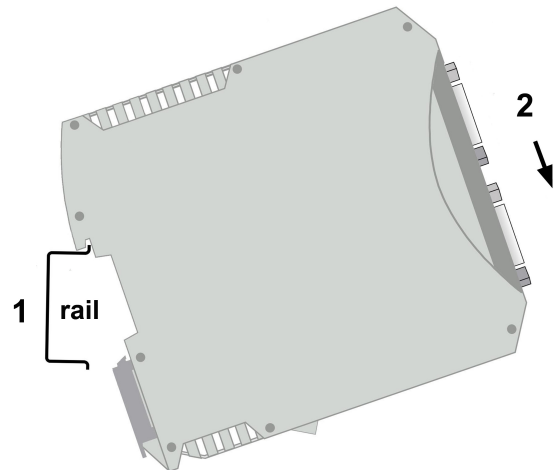


#### Installation and inspection

Installation and inspection must be carried out by qualified personnel only (personnel qualified according to the German standard TRBS 1203 or similar (Technical Regulations for Operational Safety). The definition of terms can be found in IEC 60079-17.

#### Mounting

1. Hook the upper notch of the cut-out on the back of the Gateway into a 35 mm DIN rail.
2. Press the Gateway down towards the rail until it slides into place over the lip of the locking bar.

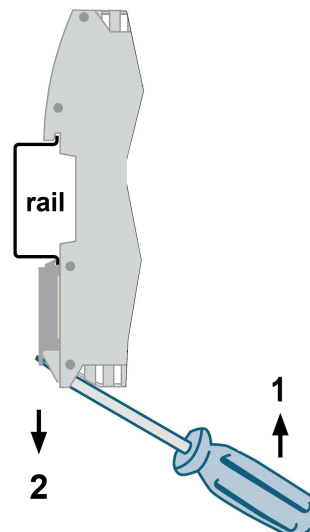


#### Note

Do not put stress on the device by bending or torsion.

#### Dismounting

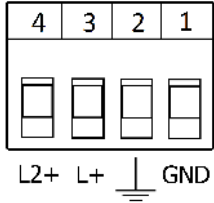

1. Slide a screwdriver diagonally under the housing into the locking bar.
2. Lever the screwdriver upwards, pull the locking bar downwards - without tilting the screwdriver - and move the gateway upwards off the rail.



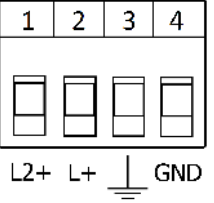

## 2.2 Connecting the Power Supply

The supply voltage (18 VDC ... 32 VDC) is connected by a 4-pole terminal block. The power supply is connected to the plug connector via flexible wires with a cross section of 0.75 to 1.5 mm<sup>2</sup>. The ground connection wire must have a cross section of 1.5 mm<sup>2</sup>.

### Wiring diagram for hardware, version 1.01 and lower

4 3 2 1	Pin	Signal	Description
	4	L2+	Redundant positive supply voltage
	3	L+	Positive supply voltage
	2		Functional Earth
	1	GND	Ground

### Wiring diagram for hardware, version 1.02 and higher

1 2 3 4	Pin	Signal	Description
	1	L2+	Redundant positive supply voltage
	2	L+	Positive supply voltage
	3		Functional Earth
	4	GND	Ground



#### CAUTION


The Functional Earth (FE) connection of the device has to be connected at low inductance with the Protective Earth (PE) of the system.

## 2.3 Configuration and Login

### IP address information

- The default IP address for the Ethernet interface in the machine floor LAN is *192.168.1.111* (see device label).
- The IP address of the web server in the common LAN is configured per default via DHCP. Depending on the configuration of your local DHCP and DNS servers, it is possible to reach the device by this host name in your network.
- The Gateway supports the network connection protocol UPnP (*Universal Plug And Play*) for Windows 10. The operating systems MAC, Linux and Android use Avahi/Zeroconf, the *Zero Configuration* network implementation protocol which identifies the gateway as an HTTPs server.

### How to establish an IP connection to the web server of the Gateway

Your network has a DHCP and DNS server	Your network does <u>not</u> have a DHCP and DNS server
<ol style="list-style-type: none"> <li>1. Connect the upper Ethernet socket (<b>IT</b>) to your network.</li> <li>2. Read the last 4 digits/letters of the Gateway serial number (in the lower left part of the label). The host name of the device is <i>uaGate / edgeGate</i> followed by the last 4 digits/letters of the serial number. For example, if the serial number is <i>123456789ab</i>, the host name is <b><i>uagate89ab</i></b> or <b><i>edgagate89ab</i></b>.</li> <li>3. Open your browser and enter the address <i>http://&lt;hostname&gt;</i> respectively <i>https://&lt;hostname&gt;</i>. (*)</li> <li>4. The login window appears.</li> </ol>	<ol style="list-style-type: none"> <li>1. Connect the lower Ethernet socket (<b>MACHINE</b>) directly to a laptop.           <div style="text-align: center;">  </div> </li> <li>2. Set the laptop IP address to <i>192.168.1.1/24</i></li> <li>3. Open your browser and enter the address <i>http://192.168.1.111</i> respectively <i>https://192.168.1.111</i> (*)</li> <li>4. The login window appears.</li> </ol>

- (\*) The Gateway supports the HTTPs protocol, which provides a secure and encrypted transfer of sensitive data such as passwords so the data cannot be read by another network user. In addition, HTTPs uses a certificate to identify the server. At Softing, we use the OPC UA Server certificate that has been generated before the last reboot.

### Login

Login with the respective login name and password. The following standard logins and passwords are available:

Role	Login name	Password
<i>Administrator</i>	administrator	administrator
<i>IT Responsible</i>	itadmin	itadmin
<i>Service Engineer</i>	mfadmin	mfadmin



**Note**

We highly recommend to change the standard password(s) to a secure password after you logged in for the first time. Refer to [User Password](#)<sup>46</sup> for more information.

For an overview of which task can be performed by which role refer to [User role and related tasks](#)<sup>47</sup>

## 2.4 Inserting a micro SD Card

On the bottom of the device you find a slot for a micro SD card. You can save your gateway configuration data to a storage card and reload it from here in case your device settings have been accidentally corrupted.



### Note

The micro SD card is not included in the delivery. When selecting a micro SD card bear in mind the range of the operating temperature of the Gateway. The storage capacity of the micro SD card may not exceed 32 GB.

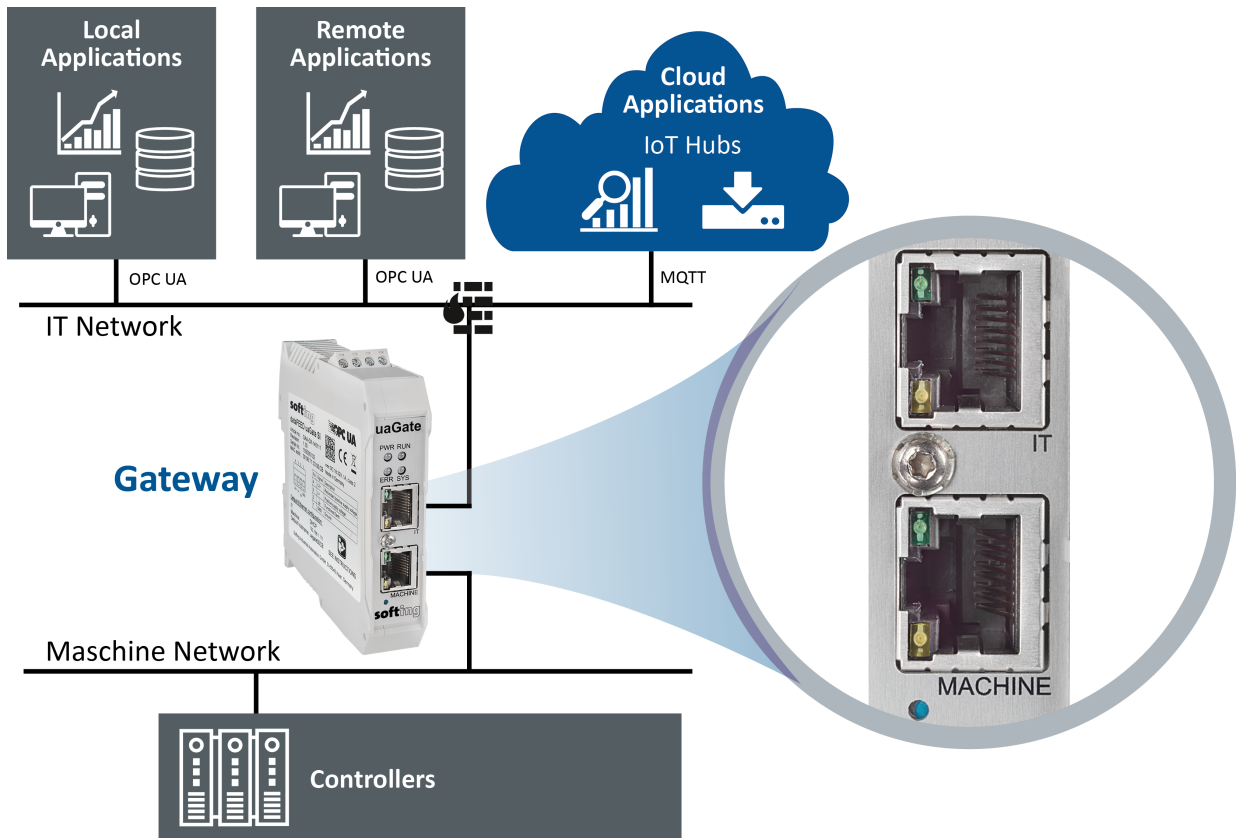


1. Remove the card slot cover on the bottom of the device.
2. Insert the micro SD card carefully into the slot until the card clicks into place.
3. Place the cover back on the housing.
4. Open the user interface of the gateway and check if the micro SD card is recognized by the device (see [Configuration and Login](#)<sup>(9)</sup>).
5. Start **Information / Gateway Status / Hardware Status**.  
The page will show you if the micro SD card is recognized in the file system and how much of the storage memory is available.

## 2.5 Connecting to the Network

The Gateway is equipped with two 10/100 Base-T Ethernet interface receptacle (RJ45). The ports correspond to the IEEE 802.3.

- **IT**  
for connecting to the IT network (upper part of diagram)
- **MACHINE**  
for connecting to the machine network



### Two different logical network connections

Both network connections (ports) have their own network segment. Thus make sure that IP addresses used differ depending on the network segment.

#### Example

Subnet mask:	255.255.255.0
IP address 1:	192.168.1.1
IP address 2:	192.168.2.1

#### Common network

If there is only one (logical) network, than it is recommended to connect only the IT Ethernet interface with this network. In this case the Ethernet interface of the machine side should be disabled by assigning the IP address 0.0.0.0 and the subnetmask 0.0.0.0 to it (see [Machine Network](#)<sup>29</sup>).



## 2.6 Powering up the Device

Turn on the power supply. The boot process takes a few seconds.

For an indication of proper operation of the Gateway refer to [LED Status Indicators](#)<sup>48</sup>.

## 2.7 Resetting the Device

If the Gateway cannot be reached e.g. due to an error in the configuration, use the reset button at the lower front side of the device. This will reset the Gateway to the factory settings.



### Reset the configuration to factory defaults

1. Disconnect the Gateway from the power supply.
2. Re-connect it to the power supply and hold down the reset button until the LEDs **SYS**, **RUN** and **ERR** light up red for about one second.



#### Hint

To prevent the device from accidental configuration reset, the reset button is only active for a short period during reboot.

## 3 Information

In the **Information** web server view you will find general device status information plus further information related to the following topics:

[Gateway Status](#) <sup>(14)</sup>

[Help & Support](#) <sup>(14)</sup>

[Version](#) <sup>(15)</sup>

[Licence Agreements](#) <sup>(15)</sup>

### 3.1 Gateway Status

The **Gateway Status** view provides the following information:

#### **General Status**

- **Operating Status**  
Status of the main application  
The following states can be shown: "*Main application running*" and "*Main application not running*".
- **System Uptime**  
Time elapsed since the last reboot or "*Power Cycle*".
- **Connection to Machine**  
The status of the connection between the device and the controller, as configured in the **Machine Settings** web server view (see [Machine Network](#) <sup>(29)</sup>). If the connection has been successfully established, the status "OK" is shown.

#### **Hardware Status**

- **Temperature**  
Device temperature in °C
- **Memory Load**  
Percentage of RAM usage
- **Flash Memory Load**  
Percentage of usage of the internal flash file system
- **micro SD Card Load**  
Mount state of the micro SD card respectively the percentage of usage of the corresponding flash file system.

#### **MQTT Connection Status**

MQTT connection status and additional information regarding the connection, if available.

### 3.2 Help & Support

The **Help & Support** view provides the following information:

- Link to the Gateway documentation
- Support e-mail address
- Softing contact information

### 3.3 Version

The *Version* view provides the following information:

- Serial Number
- Firmware Version
- Kernel Version
- Hardware Version
- Order Number

### 3.4 Licence Agreements

The *License Agreement* view provides links to

- List of public domain software and their license information
- Package copyright information

A detailed list of used licenses can be found at

<http://opensource.softing.com/IA/dataFEEDUAGateway/V1.75/>.

## 4 IT Settings

In the *IT Settings* web server view you configure the part of the device which connects with the common network. Especially the OPC UA Server provided by the device should be available in the common network.

- [IT Network Configuration](#) <sup>16</sup>
- [OPC UA Server](#) <sup>17</sup>
- [MQTT Broker Configuration](#) <sup>21</sup>

### 4.1 IT Network Configuration

The *IT Network Configuration* view provides the means to configure the various network settings of the IT Ethernet interface.

- **MAC**  
MAC address of the Ethernet interface (read only)
- **Host**  
Host name used for registration by the DHCP server  
Depending on the configuration of your local DHCP and DNS servers it is possible to reach the device by this host name in your network.
- **IPv4 Address**  
IPv4 address of the Ethernet interface  
If DHCP is disabled, a static IP address can be assigned.
- **Subnet Mask**  
Network mask of the IPv4 address in decimal dotted notation, e.g. *255.255.255.0*
- **Default Gateway**  
Default router address to be used in the common network
- **Obtain an IP Address from a DHCP Server**  
If enabled, the device should obtain network settings by DHCP for the IT Ethernet interface. If disabled, static settings are used (see above).  
By default network setting by the DHCP server is enabled.
- **DNS Address**  
IP address of the Domain Name Server to be used by the Gateway  
This setting might be overwritten by the DHCP server.
- **IPv6**  
(Read-only) IPv6 address(es) of the IT Ethernet interface, as assigned by *IPv6 autoconf*.  
The *IPv6* information is only shown, if the used network is configured to use IPv6. Up to 16 IPv6 addresses can be assigned to the IT Ethernet interface.



#### Note

If you re-configure the IP settings of the Ethernet interface used for configuration, you need to re-connect afterwards using the new configured IP address.

#### Saving and applying settings

1. Click the **Save** button to save your settings.  
A hint will appear reminding you that the application of some other settings is pending:

Pending settings. Click here to apply all settings!

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

## 4.2 OPC UA Server

The **OPC UA Server** view provides the means to configure the OPC UA Server of the device. This page provides the following information:

- **Endpoint URI**  
OPC UA endpoint URI  
Endpoint URI using different formats (host name, IP address, IPv4, IPv6), depending on used network configuration  
The string is read-only. For easy configuration of your OPC UA Client copy this URI and paste it into the appropriate field of your OPC UA Client configuration.  
See [IT Network Configuration](#)<sup>(16)</sup> for additional information regarding the shown IPv6 information
- **Port**  
Port number of internal OPC UA Server  
The allowed range for the port number setting is 1024 ... 65535. The default value is 4840.

### 4.2.1 Generate Server Certificate

The **Generate Server Certificate** view deals with the details of the OPC UA Server certificate in the Gateway.

#### Certificate details

The user entries in the input fields Country code (two letters), **Location, State, Organization, Department, Common name, E-mail address** and **Validity period of certificate that is generated (days)** are used to create a certificate for the OPC UA Server.

The input field **Validity period of certificate that is generated (days)** allows you to determine the duration for which the generated certificate is valid. The validity period starts with the current system time and ends after the number of days given in this field . Make sure you have configured the system time correctly before generating the OPC UA Server certificate (refer to [Time Settings](#)<sup>(44)</sup> for details).

The default setting of this field is not derived from the current certificate.

Click the **Generate Server Certificate** button to create a new self-signed OPC UA Server certificate in the Gateway.

#### CA signed Certificate

It is also possible for network administrators to use their own certificate authority for signing the generated OPC UA server certificate.

To do so, download the certificate request file using the **OPC-UA-Certificate\_req.pem** button and send it to your certificate authority to generate the signed certificate file. Afterwards upload this certificate file into the device using the **Upload CA signed server certificate** file dialog.

### Download Server Certificate

The certificate can be downloaded from the device in *PEM* or *DER* format using the ***OPC-UA-certificate.pem*** respectively ***OPC-UA-certificate.der*** buttons.



#### **Note**

The certificate generated here is also valid for the web server. The web server will use the newly generated certificate after the next reboot.

## 4.2.2 OPC UA Security

The **OPC UA Security** view supports the configuration of the OPC UA transport layer for access by OPC UA Clients.

### Security Mode

The following security mode options are supported:

- **sign**  
Messages are signed digitally to protect against manipulation.
- **sign & encrypt**  
Messages are signed digitally to protect against manipulation and encrypted.
- **none**  
Messages are not signed digitally and encrypted.

### Security Policy

If the security modes **sign** or **sign & encrypt** has been selected as least one of the following security policies has to be selected.

- **Basic128Rsa15**  
Support of medium message security  
The OPC UA Client certificate needs to be trusted (see [Manage Client Certificates](#)<sup>(20)</sup>).
- **Basic256**  
Support of high message security  
The OPC UA Client certificate needs to be trusted (see [Manage Client Certificates](#)<sup>(20)</sup>).
- **Basic256Sha256**  
Support of very high message security  
The OPC UA Client certificate needs to be trusted (see [Manage Client Certificates](#)<sup>(20)</sup>).



#### Note

The **Basic256Sha256** security policy can only be set, if the certificate has been generated with firmware version V1.40 or higher.

## 4.2.3 OPC UA Authentication

The **OPC UA Authentication** view allows to select the authentication settings of the OPC UA Server of the Gateway.

The following authentication policies are supported:

- **Certificate policy**  
OPC UA Clients that are authenticated by a trusted certificate may access data of the OPC UA Server.  
(see [Manage Client Certificates](#)<sup>(20)</sup>)
- **Anonymous policy**  
Each OPC UA Client may access data of the OPC UA Server.
- **User Name Policy**  
OPC UA Clients that are authenticated by a valid user name and password may access data of the OPC UA Server.

#### 4.2.4 Manage Client Certificates

The **Manage Client Certificates** view supports the management of existing certificates, the upload of new certificates and the display of certificate properties in a table.

For a certificate of an OPC UA Client to become trusted (from view of the OPC UA Server in the Gateway) the following conditions need to be fulfilled:

1. The certificate is digitally signed and the whole chain of certificates used for signing is available to the Gateway. It is either stored in the **CA** (Certificate Authority) folder or in the **Trusted certificates** folder (see below).
2. The certificate is stored in the Gateway. Self-signed certificates need to be stored in the **Trusted certificates** folder to become trusted. This classification stays valid unless a certificate is declared not trusted.
3. In addition, it is checked for user authentication that the certificate is not stored in the **Rejected certificates** folder in the Gateway.

##### Upload new certificate

To ease certificate management, the OPC UA Server in the Gateway stores each new client certificate in the **New certificates** folder using the binary *DER* format. Additional *DER* format certificates can be uploaded in the Gateway using the **Browse...** button.

##### Declare a certificate trusted

To declare a certificate trusted, move it into the **Trusted certificates** folder. To do so, select the certificate and click the **Move to trusted folder** (👉) button.



##### Note

Check the certificate's fingerprint to make sure you declare the correct certificate trusted.

##### Declare a certificate not trusted

To exclude a certificate from being trusted, remove it from the **Trusted certificates** folder. To do so, select the certificate and delete it by clicking the **Delete certificate** (🗑️) button or move it to the **Rejected** folder by clicking the **Move to rejected folder** (👎) button.



##### Note

If the certificate is deleted, it may reappear in the **New certificates** folder, if the certificate owner tries to re-connect.

##### Manage certificate authorities certificates

The certificates of certificate authorities (CA) are certificates that are required to verify that (not self-signed) certificates in the **Trusted Certificates** folder are valid. These certificates are uploaded in the Gateway as follows:

1. Upload the *DER* format certificate into the **New certificates** folder (see above).
2. Select the uploaded certificate and click the **Move to certificate authority (CA)** (👇) button to move it to the **CA** folder.



## 4.3 MQTT Broker Configuration

### MQTT Introduction

The MQTT protocol knows the following peers:

#### 1. MQTT Broker

The MQTT Broker is the central instance in an MQTT network. The other participants establish each a TCP or SLL/TLS connection to the broker. Depending on the MQTT Broker configuration an authentication with user name and passwords or an SSL certificate is required. The MQTT Broker receives data from MQTT Publishers. If an individual publisher does not have the required write permissions, the corresponding data is discarded by the broker. Otherwise the broker provides the data to all MQTT Subscribers that have subscribed to this data.

#### 2. MQTT Publisher

The MQTT Publisher creates the MQTT address space (topics) and fills this space with content (data). The MQTT Publisher sends this data to the MQTT Broker. This is exactly the functionality of the MQTT Publisher module implemented in the Gateway.

#### 3. MQTT Subscriber

The MQTT Subscribers subscribe to MQTT Topics. For defining the subscribed topics the subscriber may use the wild card characters *+* and *#*. This means that an MQTT Subscriber using the character *#* for a topic subscription subscribes to all data from a broker.

The data format is not specified by the MQTT protocol specification but can be specified by the respective MQTT Publisher. The Gateway MQTT Publisher module uses strings as data format.

The **MQTT Broker Configuration** view allows to configure all settings for the connection to the MQTT Broker.

The following settings are provided:

- **MQTT Broker URI**

The broker URI defines the MQTT Broker to be used by the Gateway.

It is composed of the transport protocol, the Fully Qualified Domain Name (FQDN), consisting of the host name and the domain name (see [https://en.wikipedia.org/wiki/Fully\\_qualified\\_domain\\_name](https://en.wikipedia.org/wiki/Fully_qualified_domain_name) for details), and optionally the port number.

The following transport protocols are supported:

- **tcp://**  
MQTT uses plain TCP. Often MQTT Brokers offer this service at port 1883.
- **ssl://**  
MQTT uses SSL or TLS security upon TCP. Often MQTT Brokers offer this service at port 8883.

The **Hostname** is defined by the Fully Qualified Domain Name. Optionally it can be replaced by the corresponding IPv4 or IPv6 address. (IPv6 addresses are identified by square-brackets).

- **Client ID**

The client ID defined the identifier of the Gateway.

The IDs of the various MQTT clients have to be unique for the respective MQTT Broker. If two MQTT clients are using an identical ID, the connections of theses clients to the MQTT Broker are disconnected. For an individual client, e.g. the Gateway, there is no way to find out whether a specific client ID is already used by another client or not.

The MQTT Broker configuration allows to determine specific client IDs, identifying the individual clients to which a connection is accepted.

- **Clean Session**  
Some MQTT Brokers require the clean session flag for connecting. Use this check box to enable this feature.
- **Authentication**  
Depending on the MQTT Broker configuration the Gateway may need to authenticate itself as an MQTT Client using its user name and password. In this case select the radio button **Username and password** otherwise select the radio button **anonymous**. If user name and password authentication is selected the user name and password have to be defined in the appropriate input fields. If necessary, define the corresponding certificate files for this connection at [MQTT Client Certificate](#)<sup>(27)</sup>.
- **Enable MQTT**  
This flag specifies whether the MQTT connection will be activated or not.

### Saving and applying settings

1. Click the **Save** button to save your settings.  
A hint will appear reminding you that the application of some other settings is pending:

A green rectangular notification box with white text that reads: "Pending settings. Click here to apply all settings!"

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

### 4.3.1 MQTT Topic Settings

The **MQTT Topic Settings** view allows to configure the settings of the topics to be published to the MQTT Broker.

#### MQTT Topic Configuration

The following settings are provided:

- **MQTT Root Topic (Topic Prefix)**  
The specified root topic is added as a prefix to all MQTT Topic names which are going to be published.  
If this setting is not empty, than a trailing slash (/) is inserted between the root topic and the automatically generated topic name.
- **Hierarchy**  
The following hierarchy options are supported:
  - **Full PLC hierarchy**  
The hierarchy of PLC symbols is translated into a corresponding MQTT hierarchy below the Root Topic.
  - **Flattened PLC hierarchy**  
The PLC symbols are flattened into just one MQTT hierarchical level below the Root Topic.
  - **Suppressed PLC symbols**  
The PLC symbol names are not used in the MQTT Topic namespace.  
Use this setting, if the MQTT Broker allows only to publish to one single MQTT Topic name.

- **MQTT Suffix Topic**  
The specified suffix topic is appended at the end to each MQTT Topic which is going to be published.  
Depending on the requirements of your MQTT Broker and your application, you may need to begin the suffix topic with a leading slash (/).
- **MQTT QoS**  
The following MQTT QoS options are available:
  - **Level 0**  
An MQTT message is published with the safety of the current TCP connection.
  - **Level 1**  
An MQTT message is repeated in the next TCP connection, if the delivery of the message in the current TCP connection fails.
  - **Level 2**  
The MQTT protocol uses the confirmation of confirmations to ensure that a message is delivered exactly once.
- **Enable MQTT Retain**  
By setting the Retain flag the MQTT Broker is instructed to save the most recent data value for the topic. Depending on the configuration the broker saves the data into the RAM or persistently into the file system/data base.  
Data values without Retain flag are only transferred from the MQTT Broker to those MQTT Subscribers that are registered at the broker and have subscribed to the appropriate topic in the moment when sending the data to the broker.  
This check box allows to specify whether the MQTT Publisher module sets the Retain flag for the respective topic or not.
- **Publish only on value change**  
If this setting is activate, a data value is only published to the MQTT Broker, if the value has changed and the minimum publishing interval (see below) has expired.
- **Group several PLC values into one MQTT message**  
To reduce the amount of MQTT messages, it is possible to transmit several PLC values into one MQTT message.  
This option automatically sets the hierarchy setting to **Suppressed PLC symbols**.
- **Maximum Number of PLC values per MQTT message**  
If you have activated message grouping, you can define the maximum number of PLC values here.  
It is possible to group up to 10 PLC values into one MQTT message.
- **Minimum publishing interval [s]**  
The same topic is not published with a faster interval than this setting (in seconds).  
This setting protect MQTT Broker and MQTT Subscribers from a flooding by too many publish messages for an individual topic. If the polling interval (see [Siemens Settings](#)<sup>31</sup> or [Modbus Settings](#)<sup>34</sup>) is larger than this setting, the defined polling interval overrules this setting.
- **Publish Format**  
The user could define the format string of the data to publish  
The following keywords (use capital letters) will be replaced with the corresponding data:
  - **@VALUE@**  
The value of the PLC item
  - **@TIME@**  
The timestamp of the PLC item
  - **@QUALITY@**  
The quality attribute of the PLC item

- **@ITEM@**  
The symbolic name of the PLC source item

### PLC Value marker

If you have enabled the grouping of messages, you may specify the **Begin**, **Separator** and **End** marker in these input fields.

### Saving and applying settings

1. Click the **Save** button to save your settings.  
A hint will appear reminding you that the application of some other settings is pending:

A green rectangular hint box with white text that reads: "Pending settings. Click here to apply all settings!"

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

### 4.3.2 MQTT Topic Selection

A PLC project typically contains many PLC items. Generally, only a small subset of these items are relevant for publishing via the MQTT protocol.

Due to performance reasons, only activate those items which are important to you.

The **MQTT Topic Selection** view allows to select the PLC items which are published to the MQTT Broker. For performing this selection the available PLC address space is displayed in a hierarchical order.

Only scalar items are available for publishing.

#### Activation and deactivation of items

- Activate or deactivate an individual item for publishing by selecting or deselecting the corresponding checkbox of the item.
- By selecting or deselecting the checkbox of a parent node in the hierarchical tree view, all child nodes are activated or deactivated together with the parent node.

#### Saving and applying settings

1. Click the **Save** button to save your settings.

A hint will appear reminding you that the application of some other settings is pending:

A green rectangular notification box with white text that reads: "Pending settings. Click here to apply all settings!"

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

### 4.3.3 MQTT Security Settings

Certificate usage for the MQTT protocol is similar to HTTPS. The client verifies the identity of the server by evaluating the certificate provided by the server. Therefore the client in advance needs to know the complete chain of the server certificates to trust.

If a certificate chain file has been located in the **Trusted Certificates** folder before connection establishment, then the Gateway verifies the identity of the MQTT Broker using this certificate chain. If the MQTT Broker fails to proof its identity with the provided certificate, then the MQTT connection will not be completely established. If there is no certificate stored in the **Trusted Certificates** folder, then the verification of the MQTT Broker identity is disabled.

For the Gateway the **MQTT Security Settings** view allows to manage existing certificates, to upload new certificates and to display certificate properties in a table.

#### Upload new certificate

To ease certificate management, the MQTT Publisher in the Gateway stores each new client certificate in the **New Certificates** folder using the *PEM* format. Additional *PEM* format certificates can be uploaded in the Gateway using the **Browse...** button.

*PEM* format certificate files may contain more than one certificate. For the MQTT protocol the complete chain of trusted certificates is expected in the *PEM* file.

#### Download a certificate chain from the server

By using the **Get certificate from server** (📄) button, the Gateway uses the *openssl* command to fetch the whole certificate chain from the server into the **New Certificates** folder.



#### Note

The *openssl* command only is available for IPv4 connections.

#### Declare a certificate trusted

To declare a certificate trusted, move it into the **Trusted Certificates** folder. To do so, select the certificate and click the **Move to trusted folder** (✔) button.

Only one trusted certificate is allowed to be stored in the **Trusted Certificates** folder.



#### Note

Check the certificate's fingerprint to make sure you declare the correct certificate trusted.

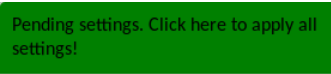
### 4.3.4 MQTT Client Certificate

The **MQTT Client Certificate** view allows to select the client certificate which is used to authenticate the MQTT Client at the MQTT Broker.

For defining the certificate the following input opportunities are supported:

1. The *PEM* format file containing the public certificate chain of the client. It may also include the private key of the client, which may be encrypted optionally.  
The client certificate file can be selected using the **Browse...** button.
2. If not included in the certificate file above (see issue 1.), the *PEM* format file containing the private key of the client has to be defined.  
The file including the private key can be selected using the **Browse...** button.
3. Definition of the password to load the private key of the client, if it is included in the files described above in an encrypted way.
4. Activation of MQTT Client certificate usage

#### Saving and applying settings

1. Click the **Save** button to save your settings.  
A hint will appear reminding you that the application of some other settings is pending:  

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

### 4.3.5 MQTT Last Will Settings

When establishing a connection, MQTT Clients, e.g. the Gateway MQTT Publisher module, can transfer an MQTT Topic name and a message to the MQTT Broker. If the MQTT Broker detects that the connection to the client does not exist any longer (e.g. because a network switch has failed) the MQTT Broker publishes this message within the topic.

The **MQTT Last Will Settings** view allows to define the *Last Will and Testament* settings for the MQTT connection:

- **Topic name**  
The topic name field includes the complete name of the Last Will topic including all hierarchy levels. The individual hierarchy levels have to be separated by the / character.
- **Testament**  
The testament field defines the message to be published by the MQTT Broker as testament.
- **Enable MQTT Retain**  
By setting the Retain flag the MQTT Broker is instructed to save the most recent data value for the topic. Depending on the configuration the broker saves the data into the RAM or persistently into the file system/data base.  
Data values without Retain flag are only transferred from the MQTT Broker to those MQTT Subscribers that are registered at the broker and have subscribed to the appropriate topic in the moment when sending the data to the broker.
- **Enable Last Will Option**  
This check box allows to specify whether the *Last Will and Testament* MQTT connection options are used or not.  
If they are used, additional configuration fields are available.

#### Saving and applying settings

1. Click the **Save** button to save your settings.  
A hint will appear reminding you that the application of some other settings is pending:

A green rectangular notification box with white text that reads: "Pending settings. Click here to apply all settings!"

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

### 4.3.6 MQTT Cloud Sample Configurations

The given websites provide examples how to configure the Gateway to use it with the MQTT Broker of a specific cloud provider.

- IBM Watson / Bluemix  
Link: <https://developer.ibm.com/recipes/tutorials/send-plc-data-via-softing-datafeed-edgate-or-uagate-to-watson-iot/>
- Microsoft Azure IoT-Hub  
Link: [https://github.com/SoftingIndustrial/azure-iot-device-ecosystem/blob/master/get\\_started/embedded-linux-softing-uagate-c.md](https://github.com/SoftingIndustrial/azure-iot-device-ecosystem/blob/master/get_started/embedded-linux-softing-uagate-c.md)



## 5 Machine Settings

The **Machine Settings** view allows to configure the part of the device, which is connected with the machine network. It is expected that the PLC is part of the machine network.

However, it may be likely that there is only one network. In this case, connect only one Ethernet interface of the device with your network.

### 5.1 Machine Network

The **Machine Network** view allows to configure the network settings of the Ethernet Interface of the machine network.

The following settings are available:

#### Machine Network Interface

- **MAC**  
MAC address of the Ethernet interface (read only)
- **IPv4 Address**  
IPv4 address of the Ethernet interface  
Assigning the IPv4 address *0.0.0.0* deactivates the interface (for IPv4 communication).
- **Subnet Mask**  
Network mask of the IPv4 address in decimal dotted notation, e.g. *255.255.255.0*
- **IPv6**  
(Read-only) IPv6 address(es) of the machine network Ethernet interface, as assigned by *IPv6 autoconf*.  
The **IPv6** information is only shown, if the used network is configured to use IPv6. Up to 16 IPv6 addresses can be assigned to the Ethernet interface of the machine network.



#### Note

If you re-configure the IP settings of the Ethernet interface used for configuration, you need to re-connect afterwards using the new configured IP address.

#### Saving and applying settings

1. Click the **Save** button to save your settings.  
A hint will appear reminding you that the application of some other settings is pending:

Pending settings. Click here to apply all settings!

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

## 5.2 PLC Connection

The **PLC Connection** view allows to add new controller connections, to configure these connections and to delete connections. This page also shows all configured PLC connections and their status.

**edgeGate** supports up to 5 PLC connections (SIMATIC S7 and/or Modbus TCP controllers).

**uaGate SI** allows to setup a connection to one SIMATIC S7-300/400/1200/1500 or SIMATIC S7-1200/1500 PLC with optimized data access.

**uaGate MB** allows to setup a connection to one Modbus TCP controller.

**uaGate 840D** supports the connection to one SINUMERIK 840D.

### Adding a Connection

Depending on the current gateway device, the configuration page for a [Siemens S7 connection](#)<sup>(31)</sup>, [Siemens S7-2 connection](#)<sup>(33)</sup>, [Modbus connection](#)<sup>(34)</sup> or a [SINUMERIK 840D connection](#)<sup>(42)</sup> is shown when clicking the **Add** button.

When working with **edgeGate** there is a chance to connect to a SIMATIC S7 PLC or to a Modbus TCP controller by selecting the appropriate controller type in the **PLC Type** dropdown list.

When working with **uaGate SI** there is a chance to connect to a SIMATIC S7 PLC or to a SIMATIC S7-1200/1500 PLC by selecting the appropriate controller type in the **PLC Type** dropdown list.

A connection name only can be chosen when adding a PLC connection.



#### Note

If the maximum number of the supported PLC connections of the Gateway already has been reached there is no chance to add further connections to the Gateway.

By clicking the **Save** button the connection configuration is stored in the device using the assigned connection name.

### Modifying a Connection

To modify the configuration of an existing PLC connection, select the line of the connection to be modified and click the **Modify** button. Depending on the current gateway device this will open the configuration page for a [Siemens S7 connection](#)<sup>(31)</sup>, [Siemens S7-2 connection](#)<sup>(33)</sup>, [Modbus connection](#)<sup>(34)</sup> or the [SINUMERIK 840D connection](#)<sup>(42)</sup>.

### Controller Symbol Import

It is possible to import symbols from the PLC project for a defined connection configuration. To do so, first select the connection for which you want to import symbols and then click the **Symbol Import** button. This will open the page for [Siemens S7 Symbol Import](#)<sup>(32)</sup>, [Siemens S7-2 address-space filter](#)<sup>(33)</sup>, [Modbus Symbol Import](#)<sup>(36)</sup> or [SINUMERIK 840D Symbol Import](#)<sup>(43)</sup>.

### Deleting a connection

To delete a PLC connection, first select the connection to be deleted and click the **Delete** button.

### 5.2.1 Siemens S7 Settings

The **Siemens Settings** view allows to configure the IP address and the type of the Siemens PLC.



**Note**

This description only applies to the **edgeGate** and **uaGate SI** products!

The following settings are available:

**Machine Access**

- **Connection Name**  
Connection name to be used  
Special characters are not supported.
- **IPv4 Address**  
IPv4 address of the PLC to which a connection should be established
- **PLC Type**  
The type of the SIMATIC S7 PLC to be connected  
Possible values are: *S7 300/400* and *S7 1200/1500*.
- **Polling interval [ms]**  
Time in milliseconds between individual read requests to the PLC  
This setting is used to limit the traffic between the device and the PLC. The polling interval also defines the lower limit of the OPC UA sampling interval. This value has to be greater or equal to 50 ms.

In special cases it might be necessary to configure the TSAP settings to allow a connection to your S7. Deactivate the **Default TSAP-Settings** checkbox for doing so.

- **TSAP Own**  
The TSAP to be used as own address  
By default this value is configured by your choice of the PLC type in the machine network part of the web page.
- **TSAP Destination**  
The TSAP to be used as foreign address  
By default this value is configured by your choice of the PLC type in the machine network part of the web page.

**Saving and applying settings**

1. Click the **Save** button to save your settings.  
A hint will appear reminding you that the application of some other settings is pending:

Pending settings. Click here to apply all settings!

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

### 5.2.1.1 Symbol Import

**Note**

This description only applies to the *edgeGate*, *uaGate SI* and *uaGate 840D* products!

The symbolic names of the SIMATIC S7 data have to be provided in an *SDFI* file.

You can generate the *SDFI* file using the Softing **dataFEED Exporter** tool. This tool uses **STEP 7** or **TIA Portal** project files as input and allows you to select a S7 PLC to generate the *SDFI* file containing the symbol definition.

Proceed as follows to convert and import symbol files:

1. Download [dataFEED Exporter](#) to that PC where the PLC configuration software (**STEP 7** or **TIA Portal** V13/V14/V15/V16/V17/V18) is installed.
2. Start the installation process and follow the instructions of the installation wizard.
3. Run **dataFEED Exporter** from the standard location (*Start/All Programs/Softing/dataFEED Exporter/dataFEED Exporter*) or from your specific installation location.
4. Follow the **dataFEED Exporter** instructions to load and convert your **STEP 7** or **TIA Portal** symbol files.
5. Save the converted *SDFI* file at your PC.
6. Go back to the Gateway and click the **Browse...** button in the **Select File** section. Select your previously converted *SDFI* file.
7. Click the **Import** button to import the *SDFI* file into the Gateway.  
The imported symbols will replace the already existing symbols. A maximum number of 20,000 nodes (\*) can be generated during the import process.

(\*) Each Data Point, Tag, Variable, Symbol is considered as an OPC UA Node. The system automatically creates additional OPC UA Nodes to generate the OPC UA Address Space structure.

**Note**

Depending on the number of symbols within the file, the import and internal processing may take some time.

The import of symbolic names containing the special character period (.) is not supported.

The Gateway is able to process OPC UA subscriptions of up to 2,500 items of data type *Byte* using a polling interval of 200 ms.

## 5.2.2 Siemens S7-2 Settings

In the *Siemens Settings* view you can configure the IP address of a S7-1200 or S7-1500 series PLC.



### Note

This description only applies to the *uaGate SI* product!

The following settings are available:

#### Machine Access

- **Connection Name**  
Connection name to be used  
Special characters are not supported.
- **IPv4 Address**  
IPv4 address of the PLC to which a connection should be established
- **Expertsetting**  
Change the expertsettings only if this is explicitly recommended by the Softing-Support.

#### Saving and applying settings

1. Click the **Save** button to save your settings.  
A hint will appear reminding you that the application of some other settings is pending:

Pending settings. Click here to apply all settings!

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

### 5.2.2.1 Filtering the Address Space of a Siemens PLC with Optimized Blocks



### Note

This description only applies to the *uaGate SI* product!

Without filtering the complete available address space of a S7-1200/S7-1500 PLC with optimized blocks is available for the OPC UA and MQTT data exchange using *uaGate SI*. However it is possible to filter the address space thus to restrict the visible variables.

For doing so select the previously established connection to a S7-1200/S7-1500 PLC with optimized blocks and click the **Symbol Import** button. In a next step it is possible to flip open the complete available address space in the **Address Space** view and to select the individual variables to be accessed via OPC UA and MQTT respectively to de-select these again.

If a specific variable in the controller's address space is selected its **Node ID**, **Node Class**, **Browse Name**, **Display Name** and **Description** is shown in the **Properties** view

If full access to the whole PLC address space should be provided, then it is recommended to delete any filter settings in advance.

#### Saving and applying settings

1. Click the **Save** button to save and apply your settings.

### 5.2.3 Modbus Settings

The Modbus Settings view allows to configure the IP address as well as details of the Modbus controller to be connected.

**Note**

This description only applies to the *edgeGate* and *uaGate MB* products!

**Note**

The *edgeGate* product allows to define more than one Modbus connection.

The following settings are available:

**Machine Access**

- **Connection Name**  
Connection name to be used  
Special characters are not supported.
- **IPv4 Address**  
IPv4 address of the PLC to which a connection should be established
- **Port**  
Port number of the PLC to which a connection should be established
- **Unit-Id**  
Slave Address of the PLC to which a connection should be established
- **Polling interval [ms]**  
Time in milliseconds between individual read requests to the PLC  
This setting is used to limit the traffic between the device and the PLC. The polling interval also defines the lower limit of the OPC UA sampling interval. This value has to be greater or equal to 50 ms.
- **Start Address**  
Start address setting for address association  
Some Modbus controllers start address association for connected devices at 0, other start at 1.
  - **Start Address 0**  
Radio button for setting the start address to begin at 0 for the Modbus controller
  - **Start Address 1**  
Radio button for setting the start address to begin at 1 for the Modbus controller
- **Swap Setting**  
Setting for sequence of data within frames
  - **Byte Swap**  
Check box for swapping Bytes within a Word (16 bits)
  - **Word Swap**  
Check box for swapping Words within a Double Word (32 bits)
  - **Dword Swap**  
Check box for swapping Double Words within a Double Float (64 bits)
- **Functioncode Setting**  
Setting of function codes for writing of data
  - **Write Single Register**  
Check box for using Modbus function code *Write Single Register 06* instead of function code *Write Multiple Registers 16* for writing of values

- **Write Single Coil**  
Check box for using Modbus function code *Write Single Coil 05* instead of function code *Write Multiple Coils 15* for writing of values

### Saving and applying settings

1. Click the **Save** button to save your settings.  
A hint will appear reminding you that the application of some other settings is pending:

Pending settings. Click here to apply all settings!

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

#### 5.2.3.1 Symbol Import



##### Note

This description only applies to the *edgeGate* and *uaGate MB* products!



##### Note

The symbolic names for Modbus items have to be provided in an ASCII text file. The file is built up by lines, each defining a symbol name and the corresponding Modbus item. The line starts with the symbolic name, followed by the equal sign = and the Modbus item definition. Hierarchy levels can be defined using the dot ..

Example of a Modbus symbol file:

```
MO_0=RX12288.0
MO_1=RX12288.1
MO_2=RX12288.2
M1_0=RX12289.0
M2_0=RX12290.0
Number_of_Jobs=RI12288
```

The **Symbol Import** view allows to import the symbolic names for a connected Modbus PLC.



##### Note

For importing a Modbus symbol file properly the corresponding Modbus connection has to be configured in a first step (see [Modbus Settings](#)<sup>34</sup>).

1. Click the **Browse...** button in the **Select File** section. Select the symbol file to be imported.
2. Click the **Import** button to load the symbol file into the Gateway.  
The imported symbols will replace the already existing symbols.



## 5.2.3.1.1 Modbus Item Syntax

**Note**

This description only applies to the *edgeGate* and *uaGate MB* products!

**Modbus Item Syntax**

- The Modbus item syntax has the following structure:  
`[Group.]<Area><DataType><StartAddress>[.ArraySize][Suffix]`
- For Modbus items of data type *BOOL* the bit number has to be provided as well:  
`[Group.]<Area><DataType><StartAddress><.Bitnumber>[.ArraySize][Suffix]`
- If *UnitID individual with item syntax* has been selected for the connection, the following syntax is required:  
`[UnitID.][Group.]<Area><DataType><StartAddress><.Bitnumber>[.ArraySize][Suffix]`

Legend:

<> = mandatory component of Modbus item

[ ] = optional component of Modbus item

**[Group.]**

Operand ranges can be combined to groups.

If *UnitID individual with item syntax* has been selected in the range 0 - 65535, the range is reduced to 0 - 255.

Gaps in the periphery can be skipped by building different groups. The gap is then not called upon.

Simply place the group name in front of the item name and separate both by a dot  
 (*GroupName.ItemName*).

The group name is made up by *G* and the number.

Example:

- G1.40001
- G2.R2
- G3.S20.30

**[UnitID.]**

The UnitID for this item is specified by the item syntax. Simply place the UnitID name in front of the item name (*UnitIDName.ItemName*).

The UnitID name is made up by *Id* and the number.

If a Group is specified, the range of the Group number is reduced to 0 - 255.

If the UnitID is missing in the item syntax, the parametrized UnitID is transferred to the PLC.

Example:

- Id1.40001
- Id2.R2
- Id3.S20.30
- Id1.G2.R3    UnitID + Group

<Area>

	Syntax Abbreviation	Number	Orientation*	Access Rights
Discrete Inputs	I E DI DE	1xxxxx	BIT	read
Discrete Outputs	A O Q DA DO DQ	0xxxxx	BIT	read / write
Input Register	ER IR	3xxxxx	WORD	read
Register (Holding Register)	R HR	4xxxxx	WORD	read / write
Discrete Inputs Octal **	J	-	BIT	read
Discrete Outputs Octal **	P	-	BIT	read / write

\* BIT-oriented means that one bit is addressed per physical address. WORD-oriented means that one word (16 bits) is addressed per physical address.

\*\* Input of the start address is octal, which means that the number 8 and 9 are invalid characters. The address is managed internally by decimal point and must be considered for logger and status.

Discrete inputs and outputs are assigned 1 bit in the PLC. During reading and writing they are processed as an 8 bit value. **This means that reading and writing of single bits is not supported.**

The ranges can be addresses using the above character strings or a number. For example, a discrete input can be addressed both by *E* and the number *1*.

## &lt;DataType&gt;

	Syntax	Syntax R	Syntax E / A	Syntax ER	With Array	Meaningful Suffixes
<b>BIT</b> <b>VT_BOOL</b>	<b>X</b>	RX5.2 HRX5.2 4X5.2	E255 I255 DE255 DI255 125543	----	----	----
<b>INT ****</b> <b>VT_I2</b> (signed)	<b>None</b> <b>I</b>	R50 HR50 400050 RI50 HRI50 4I50	----	ER120 IR120 3I2034 ERI120 IRI120 3I12034	R50.2 HR50.2 400050.2 ER120.2 IR120.2 3I2034.2	BCD BA
<b>WORD ****</b> <b>VT_UI2</b> (unsigned)	<b>W</b>	RW50 HRW50 4W50	----	ERW120 IRW120 3W12034	RW50.2 HRW50.2 4W00050.2 ERW120.2 IRW120.2 3W12034.2	BCD BA
<b>DOUBLE INT ****</b> <b>VT_I4</b> (signed)	<b>D</b> <b>DI</b>	RD50 HRD50 4D50 RDI50 HRDI50 4DI50	----	ERD120 IRD120 3D12034 ERDI120 IRDI120 3DI12034	RD50.2 HRD50.2 4D00050.2 ERD120.2 IRD120.2 3D12034.2	BCD BA
<b>DOUBLE WORD ****</b> <b>VT_UI4</b> (unsigned)	<b>DW</b>	RDW50 HRDW50 4DW50	----	ERDW120 IRDW120 3DW12034	RDW50.3 HRDW50.3 4DW50.3 ERDW120.3 IRDW120.3 3DW12034.3	BCD BA
<b>REAL</b> <b>VT_R4</b>	<b>R</b>	RR5	----	ERR5	RR5.3 ERR5.2	----
<b>DOUBLE</b> <b>VT_R8</b>	<b>RD</b>	RRD5	----	ERRD5	RRD5.10	----
<b>STRING</b> <b>VT_BSTR</b>	<b>S</b>	RS5.4	----	ERS5.4	----	----

\* if *only standard types* has been selected as data types (server settings)

\*\* if *also unsigned* has been selected as data types (server settings)

\*\*\* with suffix *WDT (Wago Date and Time)* 4 registers (8 bytes) are read

\*\*\*\* It depends on the manufacturer which byte is given as first or second of the Word / Double Word. It is possible to create two connections: (1) One for Word /Double Word access and possibly the *Word Swap* option (depending on the Double Word implementation of the Modbus terminal). (2) One for Byte access and the *Byte Swap* option.

**<StartAddress>**

The start address defines the point at which reading and writing starts.

Example:

- ER120: Input Register 120

If the start address is a specific bit, the bit number is also required.

**<.BitNumber>**

The bit number must be provided whenever the data type is BOOL.

Example:

- HRX5.2: bit 2 of Holding Register 5

**[.ArraySize]**

Arrays merge several units of one data type.

Example:

- HRD50.3

**[Strings]**

For a Modbus controller to support strings we interpret consecutive Modbus registers as a character string with 8 bit ASCII coding.

For string both bytes of the 16 bit registers are used.

Example:

- RS100.8 allows an interpretation of Modbus registers 100 to 108 as a string of 8 character of 8 bits each.

**[Suffix]**

By using a suffix a value can be presented in another format.

Suffix	Syntax	Use	Area	Data type	Comments
BitArray	BA		No. of bits:		
		Byte	Size in bytes times 8	BOOLEAN	With the <i>BA</i> suffix, the data saved in the PLC is shown as an array of bits.
		Word	Size in words times 16	BOOLEAN	
		Int	Size in Int times 16	BOOLEAN	
		DWord	Size in DWord times 32	BOOLEAN	
Dint	Size in Dint times 32	BOOLEAN			

BCD	BCD	Byte	Byte:	0 to 99	SHORT	With the <i>BCD</i> suffix, the data saved in the PLC is shown as non-signed, binary-coded values. For example, the decimal value 65535 is shown as 9999.
		Word	Word:	0 to 9999	SHORT	
		Int	Int:	0 to 9999		
		DWord	DWord:	0 to 9999999		
		Dint	Dint:	0 to 9999999		

## 5.2.4 SINUMERIK 840D Settings

The **Siemens Settings** view allows to configure a SINUMERIK 840D connection.



### Note

This description only applies to the **uaGate 840D** product!

The following settings are available:

### Machine Access

A SINUMERIK 840D connection is defined by the following settings:

- **Connection Name**  
Connection name to be used  
Special characters are not supported.
- **IPv4 Address**  
IPv4 address of the SINUMERIK 840D to which the connection should be established
- **Enabled connection types**  
Using the **NCK** and **PLC** check boxes the connection to the NCK and the PLC part of the SINUMERIK 840D can be enabled or disabled.
- **NCK TSAP Selection**  
A set of predefined destination TSAPs (Sinumerik 840D SL NCK, user-defined) for the NCK connection. Default is **Sinumerik 840D SL NCK**. With the selection **user-defined** the input field **NCK TSAP Destination** becomes available.
- **NCK TSAP Destination**  
Input field for a user-defined destination NCK TSAP.
- **PLC TSAP Selection**  
A set of predefined destination TSAPs (Sinumerik 840D SL PLC, S7 300/400, S7 1200/1500, user-defined) for the PLC connection. Default is **Sinumerik 840D SL PLC**. With the selection **user-defined** the input field **PLC TSAP Destination** becomes available.
- **PLC TSAP Destination**  
Input field for a user-defined destination PLC TSAP.
- **Enable Alarms**  
This enables the sending of alarm messages from the Sinumerik to the **uaGate 840D**. For some versions of the Sinumerik 840D PL this could lead to problems.
- **Enable Tooling**  
This adds tooling related entries to the OPC UA address space.
- **Expertsetting**  
Change the expertsettings only if this is explicitly recommended by the Softing-Support.
- **Forbid write to device component**  
With this settings you are able to adjust the write access to the PLC and NCK components of the Sinumerik 840D. In case you allow the write access to the PLC, this only applies to the items which have also write permission in the SDFI-file. In case you allow write access to thr NCK, this only applies to the variables which are writable by the Sinumerik 840D.  
**Warning: Write access to the Sinumerik 840D might be dangerous. Enable write access only if you could ensure to write only to items which are safe to change!**

### Saving and applying settings

1. Click the **Save** button to save your settings.  
A hint will appear reminding you that the application of some other settings is pending:

Pending settings. Click here to apply all settings!

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

#### 5.2.4.1 Symbol Import NCK



##### Note

This description only applies to the *uaGate 840D* product!

A default symbol file is already included in *uaGate 840D*. It is activated once a connection has been configured.

By importing an *AWL* format symbol file the namespace can be changed.

1. Click the **Browse...** button in the **Select File** section and select the *AWL* file to be imported
2. Click the **Import** button to import the *AWL* file into *uaGate 840D*. The imported symbols will replace the already existing symbols.



##### Note

An **alarm** symbol is automatically added at the root level of the namespace. It is used to display NCK alarms.

If the imported symbol file also contains an **alarm** symbol this is overwritten by the automatically generated **alarm** symbol.

## 5.3 Symbol View

This page displays either the filtered namespace of the configured PLC or the namespace of the imported symbol file(s) in a hierarchical view.

## 6 Service Settings

The **Service Settings** view allows to configure common Gateway settings.

These settings are described in the following sections:

- [Time Settings](#) <sup>44</sup>
- [Reset](#) <sup>44</sup>
- [Firmware Update](#) <sup>45</sup>
- [Backup and Restore](#) <sup>45</sup>
- [User Password](#) <sup>46</sup>
- [micro SD Card](#) <sup>47</sup>
- [Support](#) <sup>47</sup>

### 6.1 Time Settings

The **Time Settings** view allows to configure the Gateway system time.

Local time is not supported by the Gateway. All time entries have to be entered as *UTC* time.

The system time can be synchronized by NTPv4 [RFC 5905], either from an NTP server within your LAN network or from some Internet NTP server (e.g. 0.pool.ntp.org). In the later case you need to ensure that the UDP port 123 is not blocked by a firewall.

To enable the NTP usage, activate the **Obtain time automatically** checkbox and enter the IP address or the host and domain name of the NTP server into the **NTP Server Address** input field.

With NTP is enabled on the Gateway other devices in your network can access the Gateway as NTP server.

#### Saving and applying settings

1. Click the **Save** button to save your settings.  
A hint will appear reminding you that the application of some other settings is pending:

A green rectangular notification box with white text that reads: "Pending settings. Click here to apply all settings!"

2. Click at this link. Your settings will be applied.  
Depending on the number of modified settings this process may take some time before being completed.
3. A message in the upper window part will inform you about the successful modification(s).

### 6.2 Reset

The **Reset** view resets different Gateway aspects.

#### Gateway restart



- Click the **Reboot** button in the **Hardware reboot** section to perform a Gateway hardware reboot. The hardware reboot also causes all new configurations to be taken on.

#### Reset configuration to default values

- Select the **IT Settings** checkbox, if the Gateway configuration of the IT network needs to be reset.
- Select the **Machine Settings** checkbox, if the Gateway configuration of the Machine network needs to be reset.
- Click the **Reset configuration to default values** button to reset the selected part(s) of the configuration to the firmware default values.

## 6.3 Firmware Update

The **Firmware Update** view allows to update the Gateway firmware.

#### Firmware Update

1. Click the **Browse...** button in the **Update Firmware From File** section to select the provided firmware image file and click the **Open** button  
Uploading the firmware file takes some time.
2. After the file has been uploaded completely, the firmware image will automatically be decompressed.  
During decompression the **SYS** LED is permanently shown green.
3. In a next step the firmware image file is verified.  
During verification the **SYS** LED is blinking green.
4. Once the verification has been performed successfully the Gateway reboots finalizing the firmware update.  
During the Gateway reboot the **SYS** LED is blinking red.  
If an error is detected during firmware update (e.g. if a wrong firmware image file has been selected) the firmware update is aborted and the **ERR** LED is permanently shown red.  
For LED details see [LED Status Indicators](#)<sup>48</sup>.

## 6.4 Backup and Restore

The **Backup and Restore** view allows to store and restore the device configuration either to/from a file on your computer or the Gateway micro SD card.

#### Backup Restore - File

- Click the **Browse...** button in the **Load configuration from file** section to select a previously stored configuration file on your computer and to load it into the Gateway.
- Click the **Backup** button in the **Save configuration in file** section to save the current configuration into a backup file on your computer.

#### Backup Restore - SD card

- Click the **Restore** button in the **Restore Configuration from SD card** section to load the configuration file previously stored on the micro SD card into the Gateway.
- Click the **Save** button in the **Save Configuration on SD card** section to save the current configuration on the micro SD card.
- Click the **Browse** button in the **SD-Card Content** section to view the actual contents of the micro SD card.

**Note**

If you modify the IP settings of the interface that you use for configuration, you need to re-connect to this interface afterwards using the new IP address setting.

**Note**

When restoring the configuration only that part editable by the currently logged-in user (*Administrator*, *IT Responsible* or *Service Engineer*) is included.

Thus, only users working as *Administrator* are capable to restore the complete configuration.

**Exception:**

Users working as *Service Engineer* are also allowed to restore the symbols in the MQTT Topic Selection from IT Settings, because these symbols are derived from the Machine Settings Symbol Import.

Independent on the currently logged-in user, backup always stores the complete Gateway configuration.

## 6.5 User Password

The **User Password** view allows to change the Gateway password(s) depending on the current role: While a user logged-in as *Administrator* can change all individual Gateway passwords, the user *IT Responsible* only can modify the *IT Responsible* password and the user *Service Engineer* only can modify the *Service Engineer* password.

**Change Password - administrator****Change Password - itadmin****Change Password - madmin**

Follow the steps to change the user password for the different user roles. The individual passwords, which can be changed depend on the current role.

1. Enter the current password into the entry field of the **Current Password** section.  
The entry of the current password is only required, if the password to be changed refers to the role of the current user is logged-in to.
2. Enter the new password into the entry field of the **New Password** section.
3. Confirm the entered new password by re-typing the new password into entry field of the **Confirm Password** section.
4. Click **Save** button to save the edited password changes.

**Note**

The new password is active immediately after clicking the **Save** button. Once the browser loads a page that accesses dynamical data, a new login is required.

### User roles and related tasks

Task	Administrator (administrator)	IT Responsible (itadmin)	Service Engineer (mfadmin)
Modify configuration and update firmware, change password of other roles than <i>Administrator</i>	<input checked="" type="checkbox"/>		
Modify <a href="#">IT Settings</a> <sup>(16)</sup> and <a href="#">Time Settings</a> <sup>(44)</sup>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Modify <a href="#">Machine Settings</a> <sup>(29)</sup> and <a href="#">Time Settings</a> <sup>(44)</sup>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>



#### Note

Be careful when modifying the *Administrator* password.

If you forget the *Administrator* password, you can reset the device to factory settings (including the *Administrator* password), however the configuration data will be lost by this step (see [Device reset button](#))<sup>(13)</sup>.

## 6.6 micro SD Card

The *SD-Card* view provides micro SD card related information and options.

- **SD Card Load**  
Shows, if a micro SD card is available and the percentage of the micro SD card memory used. The information *not mounted* indicates that the micro SD card is not recognized or available.
- Click the **Browse** button in the **SD-Card Content** section to show the content of the micro SD card.
- Click the **Remove** button in the **Prepare save removal of SD-Card** section to unmount the file system of the micro SD card, so it can be safely removed from the Gateway.

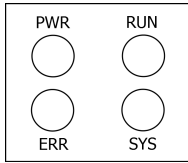
## 6.7 Support

The **Support** page provides means to access additional information in case of problems.

- Click the **Start** button in the **Capture network traffic** section to start logging the network traffic on all Ethernet interfaces of the Gateway.  
Once the **Start** button has been clicked, the network traffic is recorded in a cyclic list of capture files. Recording stops upon device restart.  
The capture files are stored on the micro SD card. Thus, this feature only is available, if a writeable micro SD card has been inserted in the Gateway with at least 8 GB of free space.
- Click the **Stop** button in the **Capture network traffic** section to stop logging the network traffic.
- Click the **Browse** button in the **Capture files** section to access the previously recorded network capture files.  
The files are suitable to be viewed using the free and open-source *Wireshark* packet analyzer tool (see [www.wireshark.org](http://www.wireshark.org)).
- Click the **Browse** buttons in the Log files section to access the log files of the Gateway.

## 7 LED Status Indicators

Gateway is equipped with four LEDs on its front side:



- PWR**                      **Power Supply**  
(permanently green if the 24 VDC power supply is OK)
- RUN**                      **Running**
- ERR**                      **Error**
- SYS**                      **System**

The LEDs may be on permanently or flash in different colors and frequencies. We use the following symbols:

Symbol	Color	Lighting
	None	Off
	Red	Permanent
	Green	Permanent
	Red	Flashing
	Green	Flashing

### Meaning of the LEDs

<b>RUN</b>		Permanently green while the OPC UA endpoint has been opened and the device is fully functional and the web server is available.
		Flashing green while the OPC UA namespace is built up (evaluating symbols etc.)
<b>SYS</b>		Permanently green while the firmware image is unzipped.
		Flashing green while the consistency of the image is checked and the kernel is exchanged.
		Flashing red while the firmware is replaced with the firmware image content. (During this time the device is not fully operational.)
<b>ERR</b>		Permanently red if the OPC UA endpoint could not be opened or an error during firmware update occurred.
		Flashing green while the configuration has pending changes.



#### Note

If you reset the device using the reset button on the front plate or by clicking the reboot button in *Service Settings* → *Reset* → *Gateway Restart* in the web server interface, the LEDs are shortly switched off.

## 8 Technical Data

Power supply	18 VDC ... 32 VDC; SELV/PELV supply mandatory Typical input current is 200 mA; maximum is 1 A (considering the rush-in current at switch-on).
Ethernet	2x IEEE 802.3 100BASE-TX/10BASE-T (independent interfaces)
Operating temperature, horizontal DIN rail installation	-40 °C ... +50 °C (0 mm minimum distance) -40 °C ... +55 °C (22.5 mm minimum distance)
Operating temperature, vertical DIN rail installation	-40 °C ... +35 °C (0 mm minimum distance) -40 °C ... +40 °C (22.5 mm minimum distance)
Storage temperature	-40 °C ... +85 °C
Relative humidity	10 % ... 95 % (non-condensing)
Altitude	Must not exceed 2,000 m
Location	Indoor use only; no direct sunlight
Dimensions (H x W x D)	100 mm x 22.5 mm x 105 mm
Mounting	35 mm DIN Rail
Ingress protection	IP20
Weight	about 0.2 kg
IT network / cloud connection	OPC UA (Server, 20,000 OPC UA Nodes(*) in total), MQTT (Publisher, up to 1,000 topics)
Industrial network connectivity	OPC UA, controllers (Siemens SIMATIC S7-300/400/1200/1500, Modbus TCP-compatible controllers, Siemens SINUMERIK 840D Solution Line)
Supported development tools	SIMATIC Step 7, TIA Portal, Siemens NCVar Selector

(\*) Each Data Point, Tag, Variable, Symbol is considered as an OPC UA Node. The system automatically creates additional OPC UA Nodes to generate the OPC UA Address Space structure.

## 9 Declarations of Conformity

This device is compliant with EC directive 2014/30/EG for "Electromagnetic Compatibility" (EMC) and meets the following harmonized standards:

- EN 55011 Industrial, scientific and medical (ISM) devices - radio disturbance - limits and methods of measurement
- EN 61000-6-4 Electromagnetic compatibility (EMC); Part 6-4: generic standard – emission for industrial environments
- EN 61000-6-2 Electromagnetic compatibility (EMC); Part 6-2: generic standard - immunity for industrial environments



### Note

To fulfill the EMC requirements, the other components of your installation (DC adapter, Industrial Ethernet devices, etc.) also have to meet the EMC requirements. A shielded cable must be used. In addition, the cable shield must be grounded properly.



### CAUTION

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures!



### CE

For this device a Declaration of Conformity in compliance with the CE standard has been made.

It can be requested from Softing Industrial Automation GmbH.



### ROHS

This device is ROHS compliant.



### FCC

This device has been tested and found to comply with the limits for a Class A digital device, under part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.



### VCCI

This Class A device conforms to the regulations of Voluntary Control Council for Interference (VCCI) by Information Technology Equipment.



### WEEE

Electrical and electronic equipment must be disposed of separately from normal waste at the end of its operational lifetime. Packaging material and worn components shall be disposed of according to the regulations applicable in the country of installation.

**REACH**

**REACH**


For this device a Statement in compliance with the European Union Directive "REACH" N°1907/2006 has been made.

It can be requested from Softing Industrial Automation GmbH.

**Softing Industrial Automation GmbH**

Richard-Reitzner-Allee 6  
85540 Haar / Germany  
<https://industrial.softing.com>

 + 49 89 45 656-340

 [info.automation@softing.com](mailto:info.automation@softing.com)

