

## Benutzerhandbuch

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



Version: EN-011923-1.75

© Softing Industrial Automation GmbH



## Haftungsausschluss

Die in dieser Anleitung gemachten Angaben entsprechen dem Stand der Technik zum Zeitpunkt der Drucklegung und werden nach bestem Wissen weitergegeben. Garantieansprüche auf Grund der in dieser Anleitung gemachten Angaben, insbesondere eine Beschaffenheits- und Haltbarkeitsgarantie gemäß § 443 BGB, werden von uns nicht übernommen. Wir behalten uns vor, Verbesserungen, Ergänzungen und neue Erkenntnisse ohne Vorankündigung in diese Anleitung neu aufzunehmen. Die tatsächliche Ausführung von Produkten kann gegenüber den in der Anleitung gemachten Angaben abweichen, falls technische Änderungen infolge von Produktverbesserungen dies notwendig machen. Nachdruck und Vervielfältigung sowie die Übernahme in elektronischer Form, auch auszugsweise, sind nicht zulässig.


## OpenSource


Um den internationalen Software-Lizenzbedingungen zu entsprechen, bieten wir die Quelldateien der in unseren Produkten verwendeten Open-Source-Software an. Nähere Hinweise finden Sie unter: <http://opensource.softing.com/>


Sollten Sie an unseren Quellcodemodifikationen und den verwendeten Quellen interessiert sind, wenden Sie sich bitte an: [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/de/services/produktsupport.html>



Scannen Sie den QR-Code, um die neueste Dokumentation von der Produkt-Website unter Downloads herunterzuladen.

# Table of Contents

<b>Chapter 1</b>	<b>Einführung .....</b>	<b>5</b>
1.1	Über dieses Produkt.....	5
1.2	Systemanforderungen.....	5
1.3	Sicherheitshinweise.....	6
1.4	Rückmeldung an Softing.....	6
<b>Chapter 2</b>	<b>Einrichtung des Geräts .....</b>	<b>7</b>
2.1	Montage und Demontage.....	7
2.2	Spannungsversorgung anschließen.....	8
2.3	Konfiguration und Anmeldung.....	9
2.4	micro SD-Karte einsetzen.....	11
2.5	Mit dem Netz verbinden.....	12
2.6	Das Gerät einschalten.....	13
2.7	Das Gerät zurücksetzen.....	13
<b>Chapter 3</b>	<b>Information .....</b>	<b>14</b>
3.1	Gateway-Status.....	14
3.2	Hilfe und Support.....	14
3.3	Version .....	15
3.4	Lizenzvereinbarungen.....	15
<b>Chapter 4</b>	<b>IT-Einstellungen .....</b>	<b>16</b>
4.1	IT-Netzwerkconfiguration.....	16
4.2	OPC UA-Server.....	17
4.2.1	Serverzertifikat erzeugen .....	18
4.2.2	OPC UA-Sicherheit .....	19
4.2.3	OPC UA-Authentifizierung .....	19
4.2.4	Client-Zertifikate verwalten .....	21
4.3	MQTT Broker-Konfiguration.....	23
4.3.1	MQTT Topic-Einstellungen .....	24
4.3.2	MQTT Topic-Auswahl .....	27
4.3.3	MQTT Sicherheits-Einstellungen .....	29
4.3.4	MQTT Client-Zertifikat .....	30
4.3.5	MQTT Last Will-Einstellungen .....	30
4.3.6	MQTT Cloud-Beispielkonfigurationen .....	31
<b>Chapter 5</b>	<b>Maschinen-Einstellungen .....</b>	<b>32</b>
5.1	Maschinennetz.....	32
5.2	SPS-Verbindung.....	33
5.2.1	Siemens S7-Einstellungen .....	35
5.2.1.1	Symbol-Import .....	36

5.2.2	Siemens S7-2 Einstellungen .....	37
5.2.2.1	Adressraum einer Siemens-SPS mit optimierten Bausteinen einschränken.....	37
5.2.3	Modbus-Einstellungen .....	39
5.2.3.1	Symbol-Import .....	40
	Modbus Item Syntax.....	42
5.2.4	SINUMERIK 840D-Einstellungen .....	46
5.2.4.1	Symbol-Import NCK.....	47
5.3	Symbol-Ansicht.....	47
<b>Chapter 6</b>	<b>Service-Einstellungen .....</b>	<b>48</b>
6.1	Zeiteinstellungen.....	48
6.2	Zurücksetzen.....	48
6.3	Firmware-Update.....	49
6.4	Sichern und wiederherstellen.....	50
6.5	Benutzerpasswort.....	51
6.6	micro SD-Karte .....	52
6.7	Support .....	52
<b>Chapter 7</b>	<b>LED-Statusanzeigen .....</b>	<b>53</b>
<b>Chapter 8</b>	<b>Technische Daten .....</b>	<b>54</b>
<b>Chapter 9</b>	<b>Herstellererklärung.....</b>	<b>55</b>



# 1 Einführung

## 1.1 Über dieses Produkt

Das dataFEED Gateway integriert OPC UA-Server-Funktionalität in neue und bestehende Anlagen und bietet eine einfache und sichere Datenanbindung an übergeordnete Management-Systeme wie ERP-, MES- oder SCADA-Systeme. Die MQTT Publisher-Funktionalität erlaubt die direkte Einbindung von Steuerungsdaten in IoT-Cloud-Anwendungen.

Das Produktangebot von Softing umfasst verschiedene Gateway-Lösungen. Weitere Details dazu finden Sie unter <https://industrial.softing.com/de/produkte/gateways/>.



### Hinweis

Eine fehlerfreie und sichere Funktionsweise setzt sachgemäßen Transport, sachgemäße Lagerung und Installation sowie fachkundige Bedienung und Wartung in Übereinstimmung mit diesem Handbuch voraus.



### Hinweis

Bei Nichteinhaltung der in diesem Dokument gegebenen Hinweise oder im Fall unsachgemäßer Handhabung entfällt unsere Haftung. Außerdem entfällt in diesen Fällen unsere Garantie auf Geräte und Ersatzteile.

Mehr Information zu Sicherheitsaspekten finden Sie im Abschnitt [Sicherheitshinweise](#)<sup>6</sup>.

## 1.2 Systemanforderungen

### Hardware

- PC
- Ethernet-Switch (optional)

### Unterstützte Browser

- Mozilla Firefox, Version 38 oder höher
- Google Chrome, Version 10.0 oder höher
- Microsoft Edge HTML, Version 17.17134 oder höher

## 1.3 Sicherheitshinweise



### VORSICHT

Dieses Gerät enthält eine Lithium-Pufferbatterie. Der Lithium-Gehalt beträgt weniger als 1 g. Ein Test gemäß dem "Manual of Tests and Criteria" der Vereinten Nationen (UN), Part III: Classification procedures, test methods and criteria, sub-section 38.3, wurde vom Hersteller erfolgreich durchgeführt.

Bei bestimmungsgemäßem Gebrauch des Geräts ist kein Wechsel dieser Batterie während der Produktlebenszeit notwendig. Ein Öffnen des Gerätes ist deshalb nicht notwendig und nicht zulässig. Das Gerät darf nur im angegebenen Temperaturbereich betrieben werden. Es darf keinesfalls darüber hinaus erhitzt werden oder in offene Flammen geworfen werden. Das Gerät ist trocken zu lagern. Bei unsachgemäßem Gebrauch können Lithium-Batterien sich entzünden oder explodieren und es besteht Verbrennungsgefahr.



### VORSICHT

Im Betrieb heizt sich die Geräteoberfläche auf. Vermeiden Sie direkten Kontakt. Bei Wartungsarbeiten schalten Sie die Spannungsversorgung ab und warten Sie, bis sich die Oberfläche abgekühlt hat.



### Hinweis

Öffnen Sie das Gehäuse des dataFEED Gateway nicht. Es enthält keinerlei Teile, die gewartet oder repariert werden müssen. Bei Defekt oder im Fehlerfall bauen Sie das Gerät ab und senden Sie es an Ihren Lieferanten. Ein Öffnen des Geräts führt zum Garantieverlust!

## 1.4 Rückmeldung an Softing

Softing bittet Sie um Ihre Rückmeldung für eine Verbesserung dieser Anleitung.

Bitte senden Sie Ihre Kommentare an die E-Mail-Adresse [support.automation@softing.com](mailto:support.automation@softing.com). Sollte Ihnen die Anleitung als PDF-Datei vorliegen, können Sie Ihre Kommentare und Vorschläge mit Hilfe der Anmerkungswerkzeuge in Adobe Reader gerne direkt in die PDF-Datei einfügen und uns zusenden.

Bitte stellen Sie sicher, dass folgende Information in Ihrer Rückmeldung enthalten ist:

- Titel der Anleitung
- Dokumentenversion (wie auf dem Deckblatt angegeben)
- Seite

## 2 Einrichtung des Geräts

### 2.1 Montage und Demontage



#### Hinweis

Stellen Sie sicher, dass das dataFEED Gateway so angebracht ist, dass die Netztrenneinrichtung jederzeit leicht erreicht werden kann.



#### Hinweis

Die maximal erlaubte Betriebstemperatur unterscheidet sich in Abhängigkeit von der Installationsrichtung. Mehr dazu finden Sie in [Technische Daten](#) <sup>54</sup>.

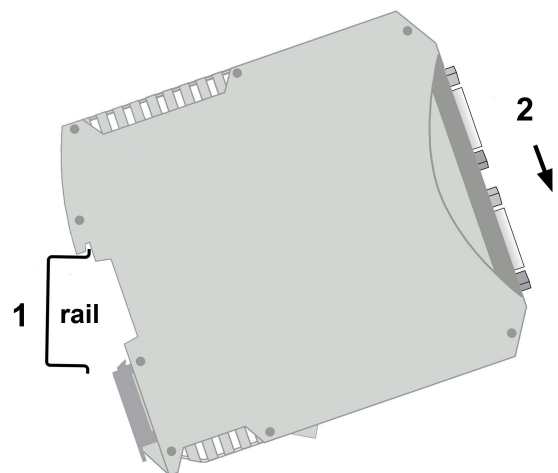


#### Installation und Wartung

Installations- und Wartungsaufgaben dürfen nur von qualifiziertem Personal (qualifiziert gemäß TRBS 1203 oder vergleichbar) ausgeführt werden! Die Begriffsdefinitionen finden Sie in IEC 60079-17.

#### Montage

1. Hängen Sie das dataFEED Gateway rückseitig mit der oberen Aussparungen auf eine Hutschiene (35 mm).
2. Drücken Sie das dataFEED Gateway nach unten bis die Verriegelung des Geräts in der Schiene einrastet.

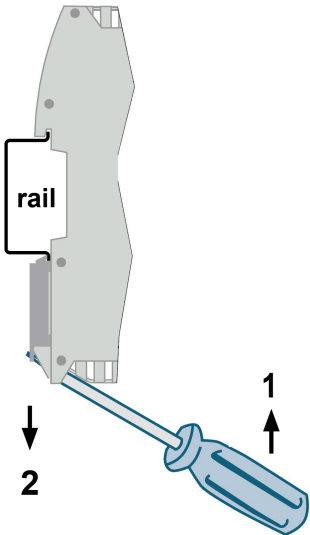


#### Hinweis

Bringen Sie keine Belastung durch Drehen oder Biegen auf das Gerät.

#### Demontage

- 1. Schieben Sie einen Schraubendreher diagonal unter das Gehäuse in die Verriegelung.
- 2. Heben Sie den Schraubendreher nach oben, die Verriegelung nach unten - ohne den Schraubendreher zu verkannten - und klappen Sie das Gerät nach oben.



2.2 Spannungsversorgung anschließen

Die Versorgungsspannung (18 VDC ... 32 VDC) erfolgt über eine 4-polige Anschlussklemme. Die Spannungsversorgung erfolgt am Steckverbinder mit flexiblen Drähten, die einen Querschnitt von 0,75 bis 1,5 mm<sup>2</sup> haben. Das Erdungskabel muss einen Querschnitt von 1,5 mm<sup>2</sup> haben.

Schaltbild für Hardware, Version 1.01 und niedriger

4 3 2 1	Pol	Signal	Beschreibung
	4	L2+	Redundante, positive Versorgungsspannung
	3	L+	Positive Versorgungsspannung
	2		Funktionserde
	1	GND	Masse

Schaltbild für Hardware, Version 1.02 und höher

1 2 3 4	Pol	Signal	Beschreibung
	1	L2+	Redundante, positive Versorgungsspannung
	2	L+	Positive Versorgungsspannung
	3		Funktionserde
	4	GND	Masse



VORSICHT


Die Funktionserde (FE) des Geräts muss niederohmig mit der Schutz Erde (PE) des Systems verbunden werden.

## 2.3 Konfiguration und Anmeldung

### IP-Adressinformation

- Die voreingestellte IP-Adresse der Ethernet-Schnittstelle im Maschinen-LAN ist **192.168.1.111** (siehe Geräteaufkleber).
- Die IP-Adresse des Webserver im LAN wird standardmäßig über DHCP konfiguriert. Je nach Konfiguration Ihrer lokalen DHCP- und DNS-Server können Sie das Gerät über diesen Hostnamen in Ihrem Netz erreichen.
- Unter Windows 10 unterstützt das dataFEED Gateway die Netzadressierung UPnP (*Universal Plug And Play*). Für die Betriebssysteme MAC, Linux und Android wird Avahi, die *Zero Configuration*-Netzimplementierung (Zeroconf), unterstützt, mit der sich das Gateway als HTTPs-Server lokalisieren lässt.

### Elne IP-Verbindung zum Webserver des dataFEED Gateway herstellen

Ihr Netz verfügt über einen DHCP- und DNS-Server	Ihr Netz verfügt über <u>keinen</u> DHCP- und DNS-Server
<ol style="list-style-type: none"> <li>Verbinden Sie den oberen Ethernet-Anschluss (<b>IT</b>) mit Ihrem Netz.</li> <li>Lesen Sie die letzten vier Ziffern/Buchstaben der dataFEED Gateway-Seriennummer. Der Hostname des Geräts ist <code>&lt;%HOSTNAME%&gt;</code>, gefolgt von den letzten vier Ziffern/Buchstaben der Seriennummer. Lautet die Seriennummer beispielsweise <b>123456789ab</b>, so ergibt sich daraus der Hostname <b>uagate89ab</b> bzw. <b>edgegate89ab</b></li> <li>Öffnen Sie Ihren Browser und geben Sie die Adresse <code>http://&lt;hostname&gt;</code> bzw. <code>https://&lt;hostname&gt;</code> ein. (*)</li> <li>Das Anmeldefenster erscheint.</li> </ol>	<ol style="list-style-type: none"> <li>Schließen Sie den unteren Ethernet-Anschluss (<b>MACHINE</b>) an einen Laptop an.  </li> <li>Stellen Sie die Laptop-IP-Adresse auf <b>192.168.1.1/24</b></li> <li>Öffnen Sie Ihren Browser und geben Sie die Adresse <code>http://192.168.1.111</code> bzw. <code>https://192.168.1.111</code> ein. (*)</li> <li>Das Anmeldefenster erscheint.</li> </ol>

- (\*) Das dataFEED Gateway unterstützt HTTPs. Damit ist Ihr Datentransfer verschlüsselt und sensible Daten wie Passwörter können nicht von anderen Netzteilnehmern gelesen werden. Zusätzlich verifiziert der HTTPs-Server seine Identität, indem er ein Zertifikat verwendet. Wir verwenden dazu das OPC UA-Serverzertifikat, dass vor dem letzten Neustart generiert wurde.

### Anmelden

Melden Sie sich mit dem zugehörigen Anmeldenamen und Passwort an. Folgende Standardnamen und -passwörter sind vergeben:

Rolle	Anmeldename	Passwort
<i>Administrator</i>	administrator	administrator
<i>IT-Administrator</i>	itadmin	itadmin
<i>Service- oder Wartungstechniker</i>	mfadmin	mfadmin



### **Hinweis**

Wir empfehlen dringend, die Standardpasswörter nach dem ersten Anmelden durch neue, sichere Passwörter zu ersetzen. Mehr dazu finden Sie in [Benutzerpasswort](#)<sup>51</sup>.

Eine Übersicht, welche Aufgabe von welcher Rolle ausgeführt werden kann finden Sie in [Benutzerrolle und zugehörige Aufgaben](#)<sup>51</sup>.

## 2.4 micro SD-Karte einsetzen

Auf der Unterseite des Gerätes befindet sich ein Steckplatz für eine micro SD-Karte. Sie können diesen Steckplatz verwenden, um beispielsweise Ihre Gateway-Konfiguration auf einer micro SD-Karte zu speichern und diese im Falle einer fehlerhaften Konfiguration von hier neu zu laden.



### Hinweis

Die micro SD-Karte ist nicht Teil des Lieferumfangs. Achten Sie bei der Wahl der micro SD-Karte auf den Temperaturbereich, in dem dataFEED Gateway eingesetzt wird. Die micro SD-Karte darf maximal eine Speicherkapazität von 32 GB besitzen.

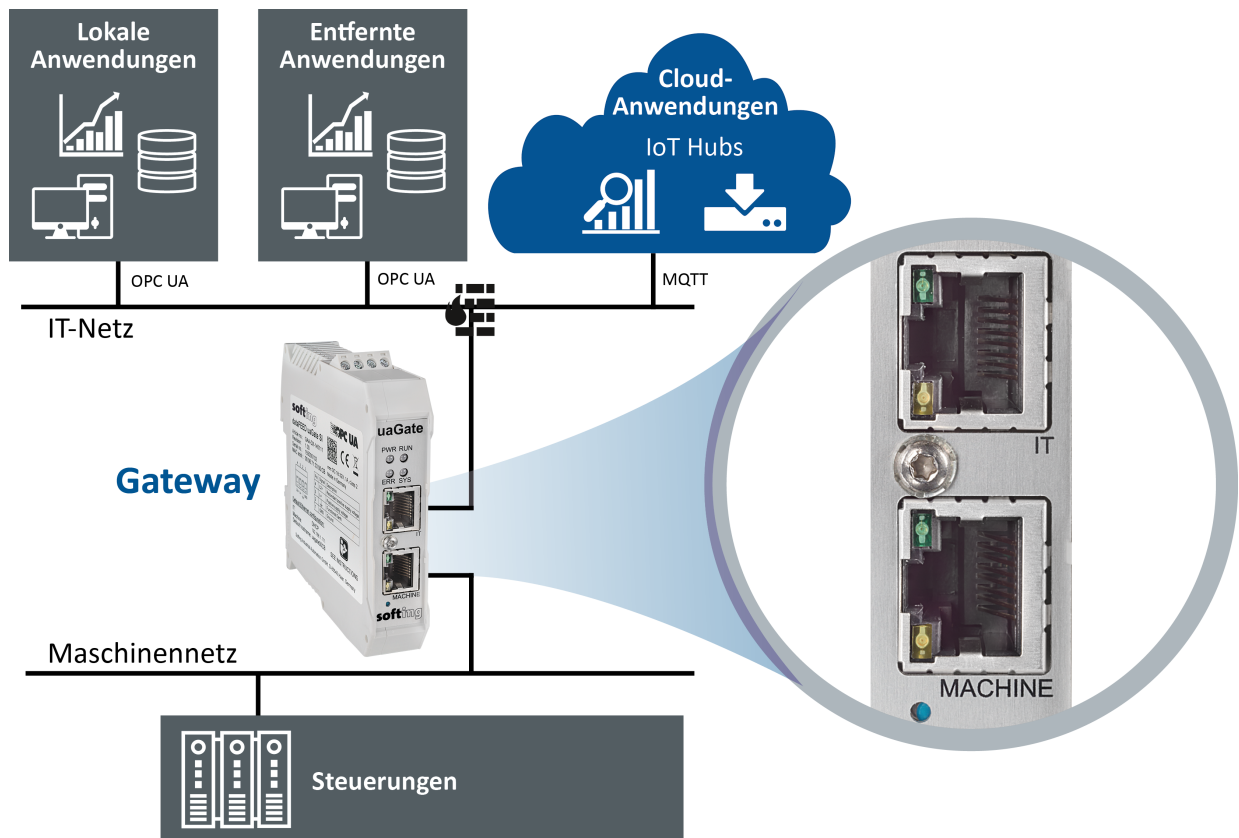


1. Entfernen Sie die Steckplatzabdeckung auf der Unterseite des Geräts.
2. Schieben Sie die micro SD-Karte vorsichtig in den Steckplatz bis sie einrastet.
3. Setzen Sie die Abdeckung wieder auf das Gehäuse.
4. Öffnen Sie die Bedienoberfläche des Gateways und prüfen Sie, ob die micro SD-Karte vom Gerät erkannt wird (siehe [Konfiguration und Anmeldung](#)<sup>9</sup>).
5. Gehen Sie zu **Information / Gateway-Status / Hardware-Status**.  
Hier wird Ihnen die Verfügbarkeit der micro SD-Karte im Dateisystem sowie die prozentuale Verwendung des Speicherplatzes angezeigt.

## 2.5 Mit dem Netz verbinden

Das dataFEED Gateway ist mit zwei 10/100 Base-T Ethernet-Schnittstellenbuchsen (RJ45) ausgestattet. Die Schnittstellen entsprechen der IEEE 802.3:

- **IT**  
für den Anschluss des IT-Netzes (oberer Teil des Diagramm)
- **MACHINE**  
für den Anschluss des Maschinennetzes



### Zwei unterschiedliche logische Netzverbindungen

Beide Netzanschlüsse am Gerät (Ports) verfügen über ein eigenes Netzsegment. Stellen Sie daher sicher, dass sich die verwendeten IP-Adressen in Abhängigkeit vom Netzsegment unterscheiden.

#### Beispiel

Subnetzmaske:	255.255.255.0
IP-Adresse 1:	192.168.1.1
IP-Adresse 2:	192.168.2.1

### Gemeinsames Netzwerk

Falls nur ein (logisches) Netz vorhanden ist, so empfiehlt es sich, nur den Ethernet-Anschluss der IT-Seite mit diesem Netz zu verbinden. Der Ethernet-Anschluss der Maschinen-Seite sollte dann durch Setzen der IP-Adresse 0.0.0.0 und der Subnetzmaske 0.0.0.0 deaktiviert werden (siehe [Maschinennetz](#)<sup>(32)</sup>).



## 2.6 Das Gerät einschalten

Schalten Sie die Spannungsversorgung ein. Das Hochfahren dauert ein paar Sekunden.

Mehr zur Anzeige des korrekten Betriebs eines dataFEED Gateway finden Sie in [LED-Statusanzeigen](#)<sup>53</sup>.

## 2.7 Das Gerät zurücksetzen

Wenn das dataFEED Gateway nicht erreicht werden kann, z.B. aufgrund eines Konfigurationsfehlers, dann drücken Sie den Rückstellknopf auf der Gerätevorderseite unten. Damit setzen Sie das dataFEED Gateway auf die Werkseinstellungen zurück.



### Auf Werkseinstellungen zurücksetzen

1. Trennen Sie das dataFEED Gateway vom Netzanschluss.
2. Verbinden Sie es dann wieder mit dem Netzanschluss und halten Sie den Rückstellknopf gedrückt, bis die LEDs **SYS**, **RUN** und **ERR** für ungefähr eine Sekunde in rot leuchten.



### Tipp

Um ein versehentliches Zurücksetzen der Konfiguration zu vermeiden, ist der Rückstellknopf nur wenige Sekunden während des Neustarts aktiv.

## 3 Information

In der Webserver-Ansicht **Information** finden Sie allgemeine Informationen über den Gerätestatus sowie weitere Informationen zu folgenden Themen:

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

[Hilfe und Support](#) <sup>14</sup>

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

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

### 3.1 Gateway-Status

Die Ansicht **Gateway-Status** enthält folgende Informationen:

#### **Allgemeiner Status**

- **Bedienstatus**  
Status der Hauptanwendung  
Die folgenden Zustände können angezeigt werden: "*Main application running*" (Hauptanwendung läuft) und "*Main application not running*" (Hauptanwendung läuft nicht).
- **Systemverfügbarkeit**  
Verstrichene Zeit seit dem letzten Neustart oder "Power Cycle" (Einschaltzyklus)
- **Verbindung zur Maschine**  
Der Verbindungsstatus zwischen Gerät und Steuerung, wie sie in der Webserver-Ansicht **Maschineneinstellungen** konfiguriert wurde (siehe [Maschinennetz](#) <sup>32</sup>). Wurde die Verbindung erfolgreich aufgebaut, so wird der Status "OK" angezeigt.

#### **Hardware-Status**

- **Temperatur**  
Gerätetemperatur in °C
- **Speicherauslastung**  
Prozentuale Verwendung des RAM
- **Flashspeicher-Auslastung**  
Prozentuale Verwendung des internen Flash-Dateisystems
- **Auslastung der micro SD-Karte**  
Information ob die micro SD-Karte im Dateisystem verfügbar ist bzw. die prozentuale Verwendung des entsprechenden Flash-Dateisystems.

#### **MQTT Verbindungs Status**

Status der MQTT-Verbindung und weitere Informationen zur Verbindung, sofern verfügbar.

### 3.2 Hilfe und Support

Die Ansicht **Hilfe und Support** enthält folgende Informationen:

- Link für Dokumentation des dataFEED Gateway
- E-Mail-Adresse des Supports
- Kontaktinformation für Softing

### 3.3 Version

Die Ansicht **Version** enthält folgende Informationen:

- Seriennummer
- Firmware-Version
- Kernel-Version
- Hardware-Version
- Bestellnummer

### 3.4 Lizenzvereinbarungen

Die Ansicht **Lizenzvereinbarungen** enthält Links für:

- Liste der Public Domain-Software und ihrer jeweiligen Lizenzen
- Copyright-Information der Packages

Eine Übersicht der verwendeten Lizenzen ist auf der Webseite <http://opensource.softing.com/IA/dataFEEDUAGateway/V1.75/> zu finden.

## 4 IT-Einstellungen

In der Webserver-Ansicht **IT-Einstellungen** können Sie den Teil des dataFEED Gateway konfigurieren, das mit dem gemeinsamen Netz verbunden ist. Insbesondere sollte der vom Gerät bereitgestellte OPC UA-Server im gemeinsamen Netz verfügbar sein.

- [Netzwerkconfiguration](#) <sup>16</sup>
- [OPC UA-Server](#) <sup>17</sup>
- [MQTT Broker-Konfiguration](#) <sup>23</sup>

### 4.1 IT-Netzwerkconfiguration

Die Ansicht **Netzwerkconfiguration** ermöglicht die Konfiguration der verschiedenen Netzeinstellungen für die IT-Ethernet-Schnittstelle.

- **MAC**  
MAC-Adresse der Ethernet-Schnittstelle (nur Lesezugriff)
- **Host**  
Für die Registrierung beim DHCP-Server verwendeter Hostname  
Je nach Konfiguration Ihrer lokalen DHCP- und DNS-Server können Sie das Gerät über diesen Hostnamen in Ihrem Netzwerk erreichen.
- **IPv4-Adresse**  
IPv4-Adresse der Ethernet-Schnittstelle  
Wenn DHCP deaktiviert ist, kann eine statische IP-Adresse zugewiesen werden.
- **Subnetzmaske**  
Netzmaske der IPv4-Adresse in Dezimalpunktschreibweise, z.B. 255.255.255.0
- **Standardgateway**  
Voreingestellte Routeradresse, die im gemeinsamen Netzwerk verwendet werden soll
- **Eine IP-Adresse von einem DHCP-Server beziehen**  
Ist diese Option aktiviert, so sollte das Gerät seine Netzeinstellungen für die IT-Ethernet-Schnittstelle über DHCP erhalten. Falls deaktiviert, werden statische Einstellungen verwendet (siehe oben).  
Als Voreinstellung ist die Netzeinstellung über den DHCP-Server aktiviert.
- **DNS-Adresse**  
IP-Adresse des Domain Name Servers, der vom dataFEED Gateway verwendet werden soll  
Diese Einstellung kann durch den DHCP-Server überschrieben werden.
- **IPv6**  
(Nicht veränderbare) IPv6 Adresse(n) der IT-Ethernet-Schnittstelle, wie sie durch *IPv6 Autoconf* konfiguriert wurde(n).  
Die Anzeige **IPv6** steht nur zur Verfügung, wenn das verwendete Netz für die Verwendung von IPv6 konfiguriert wurde. Für die IT-Ethernet-Schnittstelle können bis zu 16 IPv6-Adressen vergeben werden.



#### Hinweis

Wenn Sie die IP-Einstellungen der Schnittstelle, die Sie für die Konfiguration verwenden ändern, dann müssen Sie das Gerät anschließend mit dieser neu-konfigurierten IP-Adresse verbinden.

### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern. Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:

Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen. Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.
3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.

## 4.2 OPC UA-Server

Die Ansicht **OPC UA-Server** erlaubt die Konfiguration des vom Gerät zur Verfügung gestellten OPC UA-Servers. Im Einzelnen stehen auf dieser Seite zur Verfügung:

- **Endpoint URI**  
OPC UA-Endpunkt-URI  
Anzeige der Endpunkt-URI in verschiedenen Formaten (Hostname, IP-Adresse, IPv4, IPv6), abhängig von der eingesetzten Netzkonfiguration  
Die Zeichenkette kann nicht geändert werden. Zur leichteren Konfiguration Ihres OPC UA-Clients kopieren Sie diese URI und fügen Sie in das entsprechende Feld Ihrer OPC UA-Client-Konfiguration ein.  
Siehe [Netzwerkkonfiguration](#) <sup>16</sup> für weitere Information zur IPv6-Anzeige
- **Port**  
Portnummer des internen OPC UA-Servers  
Der zulässige Wertebereich für die Portnummer-Einstellung beträgt 1024 ... 65535.  
Voreingestellt ist die Portnummer 4840.

### 4.2.1 Serverzertifikat erzeugen

Die Ansicht **Serverzertifikat erzeugen** zeigt Details des OPC UA-Server-Zertifikats im dataFEED Gateway an.

#### Zertifikat-Details

Die Anwendereingaben in den Feldern **Länderkennung (zwei Buchstaben)**, **Stadt**, **Bundesland/Provinz**, **Organisation**, **Abteilung**, **Name**, **E-Mail-Adresse** und **Gültigkeitsdauer des zu generierenden Zertifikats in Tagen** werden für die Erzeugung eines OPC UA-Server-Zertifikats verwendet.

Das Eingabefeld **Gültigkeitsdauer des zu generierenden Zertifikats in Tagen** erlaubt Ihnen, den Zeitraum festzulegen, für den das neue Zertifikat gültig ist. Die Gültigkeitsdauer beginnt mit der aktuellen Systemzeit und endet nach der Anzahl der in diesem Feld eingegebenen Tage. Stellen Sie sicher, dass Sie zuvor die Systemzeit korrekt eingestellt haben (siehe [Zeiteinstellungen](#)<sup>48</sup> für weitere Informationen).

Die Voreinstellung für diesen Wert wird nicht vom aktuellen Zertifikat übernommen.

Klicken Sie auf die Schaltfläche **Serverzertifikat erzeugen**, um ein neues selbst-signiertes OPC UA-Serverzertifikat im dataFEED Gateway zu erzeugen.

#### CA zertifiziertes Zertifikat

Netzadministratoren können für das OPC UA-Server-Zertifikat ebenfalls die Signatur der eigener Zertifizierungsstelle verwenden. Dazu muss zunächst der Zertifikatsantrag über die Schaltfläche **OPC-UA-certificate\_req.pem** heruntergeladen und dieser für die Erzeugung der signierten Zertifikatsdatei an die Zertifizierungsstelle gesendet werden. Anschließend kann diese Zertifikatsdatei über den Dateidialog **Durch CA signiertes Server-Zertifikat hochladen** in das Gerät hochgeladen werden.

#### Server-Zertifikat herunterladen

Das Zertifikat kann vom Gerät im *PEM*- oder *DER*-Format über die Schaltflächen **OPC-UA-certificate.pem** bzw. **OPC-UA-certificate.der** heruntergeladen werden.



#### Hinweis

Das hier erzeugte Zertifikat ist auch für den Webserver gültig. Der Webserver wird das neu erzeugte Zertifikat nach dem nächsten Neustart verwenden.

### 4.2.2 OPC UA-Sicherheit

Die Ansicht **OPC UA-Sicherheit** erlaubt die Konfiguration der Sicherheitseinstellungen der OPC UA-Transportschicht für den Zugriff durch OPC UA-Clients.

#### Sicherheitsmodus

Folgende Optionen des Sicherheitsmodus stehen zur Verfügung:

- **signieren**  
Meldungen werden zum Schutz gegen Manipulationen digital signiert.
- **signieren & verschlüsseln**  
Meldungen werden zum Schutz gegen Manipulationen digital signiert und verschlüsselt.
- **keine**  
Meldungen werden nicht digital signiert und verschlüsselt.

#### Sicherheitsrichtlinie

Bei Auswahl des Sicherheitsmodus **signieren** oder **signieren & verschlüsseln** muss zumindest eine der nachfolgenden Sicherheitsrichtlinien aktiviert sein.

- **Basic128Rsa15**  
Unterstützung einer mittleren Meldungssicherheit  
Das Zertifikat des OPC UA-Clients muss vertrauenswürdig sein (siehe [Client-Zertifikate verwalten](#)<sup>(21)</sup>).
- **Basic256**  
Unterstützung einer hohen Meldungssicherheit  
Das Zertifikat des OPC UA-Clients muss vertrauenswürdig sein (siehe [Client-Zertifikate verwalten](#)<sup>(21)</sup>).
- **Basic256Sha256**  
Unterstützung einer sehr hohen Meldungssicherheit  
Das Zertifikat des OPC UA-Clients muss vertrauenswürdig sein (siehe [Client-Zertifikate verwalten](#)<sup>(21)</sup>).



#### Hinweis

Die Sicherheitsrichtlinie **Basic256Sha256** kann nur verwendet werden, wenn das Zertifikat mit der Firmware-Version V1.40 oder höher erzeugt wurde.

### 4.2.3 OPC UA-Authentifizierung

Die Ansicht **OPC UA-Authentifizierung** erlaubt die Auswahl der Authentifizierungseinstellungen des OPC UA-Servers des dataFEED Gateway.

Die folgenden Authentifizierungseinstellungen werden unterstützt:

- **Zertifikatrichtlinie**  
OPC UA-Clients, die durch ein vertrauenswürdiges Zertifikat authentifiziert werden, können auf Daten des OPC UA-Servers zugreifen.  
(siehe [Client-Zertifikate verwalten](#)<sup>(21)</sup>)
- **Anonymous-Richtlinie**  
Jeder OPC UA-Client kann auf Daten des OPC UA-Servers zugreifen.

- ***Benutzernamen-Richtlinie***  
OPC UA-Clients, die durch einen gültigen Benutzernamen und Passwort authentifiziert werden, können auf Daten des OPC UA-Servers zugreifen.



#### 4.2.4 Client-Zertifikate verwalten

Die Ansicht **Client-Zertifikate verwalten** erlaubt die Verwaltung bestehender Zertifikate, das Hochladen neuer Zertifikate und die Anzeige der Zertifikateigenschaften in einer Tabelle.

Damit ein Zertifikat eines OPC UA-Clients (aus Sicht des OPC UA-Servers im dataFEED Gateway) als vertrauenswürdig eingestuft wird, müssen folgende Bedingungen erfüllt sein:

1. Das Zertifikat ist digital signiert und die gesamte Zertifikatkette, die zum Signieren verwendet wird, steht das dataFEED Gateway zur Verfügung. Es ist entweder im Ordner **CA** (Zertifizierungsstelle) oder im Ordner **Vertrauenswürdige Zertifikate** gespeichert (siehe unten).
2. Das Zertifikat ist im dataFEED Gateway gespeichert. Selbstsignierte Zertifikate müssen im Ordner **Vertrauenswürdige Zertifikate** gespeichert werden, um als vertrauenswürdig eingestuft zu werden. Diese Einstufung bleibt solange bestehen, bis sie zurückgezogen wird.
3. Zusätzlich wird zur Benutzerauthentifizierung noch sichergestellt, dass das Zertifikat nicht im Ordner **Unerwünschte Zertifikate** im dataFEED Gateway gespeichert ist.

##### Neues Zertifikat hochladen

Um die Zertifikatverwaltung zu vereinfachen, speichert der OPC UA-Server im dataFEED Gateway jedes neue Client-Zertifikat im Ordner **Neue Zertifikate** im DER-Binärformat. Zusätzliche Zertifikate im DER-Format können über die Schaltfläche **Durchsuchen...** in das dataFEED Gateway hochgeladen werden.

##### Ein Zertifikat als vertrauenswürdig einstufen

Um ein Zertifikat als vertrauenswürdig einzustufen, verschieben Sie das Zertifikat in den Ordner **Vertrauenswürdige Zertifikate**. Wählen Sie dazu das Zertifikat aus und klicken Sie die Schaltfläche **Verschiebe in Vertrauenswürdige Zertifikate** (✓).



##### Hinweis

Überprüfen Sie den Fingerabdruck des Zertifikats um sicherzustellen, dass Sie das korrekte Zertifikat als vertrauenswürdig einstufen.

##### Ein Zertifikat als nicht vertrauenswürdig einstufen

Um ein Zertifikat als nicht vertrauenswürdig einzustufen, löschen Sie es aus dem Ordner **Vertrauenswürdige Zertifikate**. Wählen Sie dazu das Zertifikat aus und löschen Sie es durch Anklicken der Schaltfläche **Zertifikat löschen** (🗑️) oder verschieben Sie es in den Ordner **Unerwünschte Zertifikate** durch Auswahl der Schaltfläche **Verschiebe in Unerwünschte Zertifikate** (✗).




##### Hinweis

Ist das Zertifikat gelöscht, so kann es erneut im Ordner **Neue Zertifikate** erscheinen, wenn der Zertifikateigentümer versucht, sich neu zu verbinden.

##### Zertifikate der Zertifizierungsstelle verwalten

Zertifikate der Zertifizierungsstelle (CA) sind Zertifikate, die sicherstellen sollen, dass (nicht selbstsignierte) Zertifikate im Ordner **Vertrauenswürdige Zertifikate** gültig sind. Diese Zertifikate werden wie folgt im dataFEED Gateway hochgeladen:

1. Laden Sie das Zertifikat im DER-Format in den Ordner **Neue Zertifikate** (siehe oben).

2. Wählen Sie das hochgeladene Zertifikat aus und klicken anschließend auf die Schaltfläche ***Verschiebe in Zertifizierungsstelle (CA)*** () , um es in den Ordner **CA** (Zertifizierungsstelle) zu verschieben.

## 4.3 MQTT Broker-Konfiguration

### MQTT-Einführung

Das MQTT-Protokoll kennt folgende Teilnehmer:

#### 1. MQTT Broker

Der MQTT Broker ist die zentrale Instanz im MQTT-Netz. Die übrigen Teilnehmer bauen zu ihm jeweils eine TCP- oder SSL/TLS-Verbindung auf. Abhängig von der Konfiguration des MQTT Brokers ist eine Authentifizierung mit Benutzername und Passwort bzw. ein SSL-Zertifikat erforderlich. Der MQTT Broker nimmt von MQTT Publishern Daten entgegen. Falls ein Publisher nicht über die notwendigen Rechte zum Schreiben verfügt, so wird das jeweilige Datum vom Broker verworfen. Andernfalls liefert er die Daten an alle MQTT Subscriber, die diese Daten abonniert haben.

#### 2. MQTT Publisher

Die MQTT Publisher erzeugen den MQTT-Adressraum (Topics) und füllen ihn mit Inhalt (Daten). Diese Daten sendet der MQTT Publisher an den MQTT Broker. Das MQTT Publisher-Modul im dataFEED Gateway wurde genau mit dieser Funktionalität implementiert.

#### 3. MQTT Subscriber

Die MQTT Subscriber abonnieren MQTT Topics. Für die Festlegung der abonnierten Topics können die Wildcard-Zeichen `+` und `#` verwendet werden. Beispielsweise abonniert ein MQTT Subscriber, der ausschließlich das Zeichen `#` für das Topic-Abonnement verwendet, alle Daten vom Broker.

Das Datenformat ist nicht durch die MQTT-Protokoll-Spezifikation festgelegt, sondern kann vom jeweiligen MQTT Publisher bestimmt werden. Das MQTT Publisher-Modul im dataFEED Gateway verwendet Zeichenketten (Strings) als Datenformat.

Die Ansicht **MQTT Broker-Konfiguration** erlaubt die Konfiguration sämtlicher Einstellungen für die Verbindung zum MQTT Broker.

Die folgenden Einstellungen stehen zur Verfügung:

- **MQTT Broker URI**

Die Broker URI setzt sich aus dem Transport-Protokoll, dem Fully Qualified Domain Name (FQDN), bestehend aus Hostname und Domainname (siehe [https://de.wikipedia.org/wiki/Domain\\_\(Internet\)#Fully\\_Qualified\\_Domain\\_Name\\_\(FQDN\)](https://de.wikipedia.org/wiki/Domain_(Internet)#Fully_Qualified_Domain_Name_(FQDN)) für Details), und optional der Portnummer zusammen.

Folgende Transport-Protokolle werden unterstützt:

- **tcp://**  
MQTT setzt direkt auf TCP auf. Häufig bieten MQTT Broker diese Variante auf Port 1883 an.
- **ssl://**  
MQTT setzt auf dem SSL- bzw. TLS-Protokoll oberhalb von TCP auf. Häufig bieten MQTT Broker diese Variante auf Port 8883 an.

Der **Hostname** wird durch den Fully Qualified Domain Name (FQDN) festgelegt. Optional kann der Hostname durch die IPv4- oder IPv6-Adresse ersetzt werden. (IPv6-Adressen werden durch eckige Klammern gekennzeichnet).

- **Client-ID**

Client-ID legt die Kennung des dataFEED Gateway fest.

Die Kennungen der verschiedenen MQTT-Clients müssen für den jeweiligen MQTT Broker eindeutig sein. Falls zwei MQTT Clients dieselbe Kennung verwenden, werden die Verbindungen dieser Clients zum MQTT Broker getrennt. Dabei ist es für einzelne Clients, z.B. das dataFEED Gateway, nicht erkennbar, ob eine bestimmte Client-ID bereits von einem anderen Client verwendet wird oder nicht.

In der Konfiguration eines MQTT Brokers können bestimmte Client-IDs von Clients festgelegt werden, zu denen ausschließlich eine Verbindung aufgebaut wird.

- **Clean Session**

Manche MQTT-Broker setzen für die Verbindung die Benutzung des Clean-Session-Flags voraus. Mit diesem Kontrollkästchen aktivieren Sie diese Funktion.

- **Authentifizierung**

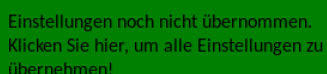
Abhängig von der Konfiguration des MQTT Brokers kann es erforderlich sein, dass sich das dataFEED Gateway als MQTT Client mit Benutzernamen und Passwort identifiziert. In diesem Fall wählen Sie die Optionsschaltfläche **Benutzername und Passwort** andernfalls die Optionsschaltfläche **Anonym**. Wird die Authentifizierung über Benutzername und Passwort ausgewählt, müssen Benutzername und Passwort in den entsprechenden Eingabefeldern angegeben werden. Gegebenenfalls legen Sie für diese Verbindung unter [MQTT Client Zertifikat](#) <sup>(30)</sup> die entsprechenden Zertifikatsdateien fest.

- **Aktiviere MQTT**

Dieses Flag legt fest, ob die MQTT-Verbindung aktiviert wird oder nicht.

### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern. Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:



Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen. Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.
3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.

#### 4.3.1 MQTT Topic-Einstellungen

Die Ansicht **MQTT Topic-Einstellungen** erlaubt die Konfiguration der Einstellungen für die Topics, die zum MQTT Broker übertragen werden.

##### MQTT Topic-Konfiguration

Die folgenden Einstellungen stehen zur Verfügung:

- **MQTT Root Topic (Topic Prefix)**

Das eingegebene Root Topic wird den Namen aller zu übertragenden MQTT Topics vorangestellt.

Wenn diese Einstellung nicht leer ist, dann wird ein Schrägstrich (/) zwischen das Root Topic und dem automatisch generierten Teil des Topic-Namens eingefügt.

- **Hierarchie**

Folgende Hierarchieoptionen stehen zur Verfügung:

- **Entsprechend SPS-Symbolhierarchie**  
Die Hierarchie der SPS-Symbole wird unterhalb des Root Topics in eine entsprechenden MQTT Topic-Hierarchie umgewandelt.
- **Flache SPS-Symbole**  
Die SPS-Symbole werden unterhalb des Root Topics in genau eine MQTT Topic-Hierarchieebene umgewandelt.
- **Ohne SPS-Symbolnamen**  
Die SPS-Symbolnamen werden im MQTT Topic-Namensraum nicht verwendet.  
Wählen Sie diese Einstellung, falls der MQTT Broker nur die Verwendung eines einzigen MQTT Topic-Namens erlaubt.

- **MQTT Suffix Topic**

Das angegebene Suffix Topic wird hinten an den Namen aller zu übertragenden MQTT Topics angefügt.

Abhängig von den Anforderungen Ihres MQTT Brokers und Ihrer Anwendung können Sie das Suffix Topic mit einem Schrägstrich (/) beginnen lassen.

- **MQTT QoS**

Folgende Optionen stehen für MQTT QoS zur Verfügung:

- **Level 0**  
Die MQTT-Nachricht wird mit der Zuverlässigkeit der aktuellen TCP-Verbindung übertragen.
- **Level 1**  
Im Falle eines Verbindungsabbruchs wird die MQTT-Nachricht in der nächsten TCP-Verbindung wiederholt.
- **Level 2**  
Das MQTT-Protokoll verwendet die Quittierung von Quittungen um sicherzustellen, dass eine Nachricht genau einmal geliefert wird.

- **Aktiviere MQTT Retain**

Durch Setzen des Retain-Flags wird der MQTT Broker angewiesen, den jeweils letzten Datenwert für das Topic zu speichern. Je nach Konfiguration des Brokers speichert er die Daten im Arbeitsspeicher oder persistent im Dateisystem/in der Datenbank.

Datenwerte ohne Retain-Flag werden vom MQTT Broker nur an diejenigen MQTT Subscriber geliefert, die in dem Moment, in dem die Daten an den Broker gesendet werden, bei diesem angemeldet sind und das entsprechende Topic abonniert haben.

Über dieses Kontrollkästchen können Sie festlegen, ob das MQTT Publisher-Modul für das jeweilige Topic das Retain-Flag setzt oder nicht.

- **Schreiben nur bei Wertänderung**

Durch Aktivieren dieser Einstellung werden nur dann Werte an den MQTT Broker übertragen, wenn diese sich geändert haben und das minimale Schreibintervall (siehe unten) abgelaufen ist.

- **Gruppieren mehrerer SPS Werte in einer MQTT Nachricht**

Um die Anzahl der MQTT-Nachrichten zu reduzieren, können mehrere SPS-Werte in einer MQTT-Nachricht zusammengefasst werden.

Das Setzen dieser Option führt automatisch zur Auswahl der Hierarchieoption **Ohne SPS-Symbolnamen**.

- **Maximale Anzahl von SPS Werten pro MQTT-Nachricht**

Bei einer aktivierten Gruppierung von Nachrichten, kann hier die maximale Anzahl der SPS-Werte festgelegt werden.

Es können maximal 10 SPS-Werte in einer MQTT-Nachricht zusammengefasst werden.

- **Minimales Schreibintervall [s]**

Mit dieser Einstellung legen Sie den minimalen zeitlichen Abstand (in Sekunden) von zwei aufeinander folgenden Schreibvorgängen für das identische MQTT Topic fest.

Diese Einstellung erlaubt es, MQTT Broker und MQTT Subscriber vor einer Überflutung durch diesen Publisher zu schützen. Falls das Polling Interval (Abfrageintervall, siehe [Siemens S7-Einstellungen](#)<sup>(35)</sup> bzw. [Modbus-Einstellungen](#)<sup>(39)</sup>) größer ist, so überstimmt das festgelegte Polling Interval das festgelegte Schreibintervall.

- **Format**

Der Benutzer kann ein Format (Schablone) für die zu schreibenden Daten vorgeben.

Die folgenden Platzhalter (Großschreibung beachten) werden durch die jeweiligen Daten ersetzt:

- **@VALUE@**  
Der Wert des SPS-Datenpunkts
- **@TIME@**  
Der Zeitstempel des SPS-Datenpunkts
- **@QUALITY@**  
Das Qualitätsattribut des SPS-Datenpunkts

- **@ITEM@**  
Der symbolische Name des SPS-Datenpunkts

### MQTT Nachrichten Separator

Falls Sie das Gruppieren von Nachrichten aktiviert haben, können Sie in diesen Eingabefeldern die Separatoren für **Anfang**, **Trenner** und **Ende** festlegen.

### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern.  
Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:

Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen.  
Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.
3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.

## 4.3.2 MQTT Topic-Auswahl

Ein SPS-Projekt enthält häufig eine sehr große Anzahl an SPS-Datenpunkten. Üblicherweise ist nur eine geringe Anzahl dieser Datenpunkte für die Übertragung über das MQTT-Protokoll von Interesse. Aus Performance-Gründen sollten Sie daher nur diejenigen Datenpunkte für die Übertragung aktivieren, die für Sie wichtig sind.

Die Ansicht **MQTT Topic-Auswahl** ermöglicht die Auswahl der SPS-Datenpunkten, die zum MQTT Broker übertragen werden sollen. Dafür wird der verfügbare SPS-Adressraum in einer hierarchischen Ansicht dargestellt.

Nur skalare Datenpunkte stehen zur Auswahl.

### Aktivieren und Deaktivieren von Datenpunkten

- Durch das Anklicken des zugehörigen Kontrollkästchens aktivieren bzw. deaktivieren Sie einen einzelnen SPS-Datenpunkt für die Übertragung.
- Durch Auswahl des Kontrollkästchens für einen übergeordneten Knotenpunkt werden alle darunter liegenden Knotenpunkte zusammen mit dem darüber liegenden Knotenpunktes aktiviert oder deaktiviert.

### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern.  
Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:

Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen.  
Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.

3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.



### 4.3.3 MQTT Sicherheits-Einstellungen

Für das MQTT-Protokoll ist die Handhabung von Zertifikaten ähnlich wie bei HTTPS. Der Client überprüft die Identität des Servers anhand des vom Server vorgelegten Zertifikats. Dazu benötigt der Client vorab die gesamte Zertifikatskette, der er vertrauen soll.

Wenn vor dem Verbindungsaufbau im Ordner **Vertrauenswürdige Zertifikate** ein Zertifikat hinterlegt wurde, überprüft das dataFEED Gateway beim Verbindungsaufbau die Identität des MQTT Brokers anhand dieses Zertifikats. Kann der MQTT Broker seine Identität anhand des Zertifikats nicht nachweisen, so wird die Verbindung nicht vollständig aufgebaut. Wurde im Ordner **Vertrauenswürdige Zertifikate** kein Zertifikat hinterlegt, so findet keine Identitätsprüfung statt.

Die Ansicht **MQTT Sicherheit-Einstellungen** erlaubt für das dataFEED Gateway die Verwaltung bestehender Zertifikate, das Hochladen neuer Zertifikate und die Anzeige der Zertifikateigenschaften in einer Tabelle.

#### Neues Zertifikat hochladen

Um die Zertifikatverwaltung zu vereinfachen, speichert der MQTT Publisher im dataFEED Gateway jedes neue Client-Zertifikat im Ordner **Neue Zertifikate** im *PEM*-Format. Zusätzliche Zertifikate im *PEM*-Format können über die Schaltfläche **Durchsuchen...** in das dataFEED Gateway hochgeladen werden.

Zertifikatsdateien im *PEM*-Format können mehr als ein Zertifikat enthalten. So wird für das MQTT-Protokoll die gesamte Kette der vertrauenswürdigen Zertifikate in der *PEM*-Datei erwartet.

#### Herunterladen der Zertifikatskette vom Server

Durch Auswahl der Schaltfläche **Hole Zertifikat vom Server** (⬇️) aktiviert das dataFEED Gateway den *openssl*-Befehl um die gesamte Zertifikatskette vom Server abzufragen und diese im Ordner **Neue Zertifikate** abzulegen.



#### Hinweis

Der Befehl *openssl* steht nur für IPv4-Verbindungen zur Verfügung.

#### Ein Zertifikat als vertrauenswürdige einstufen

Um ein Zertifikat als vertrauenswürdige einzustufen, verschieben Sie das Zertifikat in den Ordner **Vertrauenswürdige Zertifikate**. Wählen Sie dazu das Zertifikat aus und klicken Sie die Schaltfläche **Verschiebe in Vertrauenswürdige Zertifikate** (✔️).

Im Ordner **Vertrauenswürdige Zertifikate** darf nur ein vertrauenswürdige Zertifikat abgelegt sein.



#### Hinweis

Überprüfen Sie den Fingerabdruck des Zertifikats um sicherzustellen, dass Sie das korrekte Zertifikat als vertrauenswürdige einstufen.

#### 4.3.4 MQTT Client-Zertifikat

Die Ansicht **MQTT Client-Zertifikat** erlaubt die Auswahl eines Zertifikats, mit dem sich ein MQTT Client gegenüber dem MQTT Broker authentifiziert.

Für die Festlegung des Zertifikats stehen folgende Eingabemöglichkeiten zur Verfügung:

1. Die eigene Client-Zertifikats-Datei mit dem öffentlichen Schlüssel im *PEM*-Format. Diese Datei kann ebenfalls den (optional verschlüsselten) privaten Schlüssel enthalten.  
Die Client-Zertifikats-Datei kann über Anklicken der Schaltfläche **Durchsuchen...** ausgewählt werden.
2. Falls nicht bereits in der Zertifikats-Datei (siehe Punkt 1.) enthalten, muss die Datei im *PEM*-Format mit dem privaten Schlüssel in diesem Eingabefeld festgelegt werden.  
Die Datei mit dem privaten Schlüssel kann über Anklicken der Schaltfläche **Durchsuchen...** ausgewählt werden.
3. Festlegung des Passworts zum Laden des privaten Schlüssel, falls dieser in den oben beschriebenen Dateien verschlüsselt ist.
4. Aktivieren der Verwendung des MQTT Client-Zertifikats

##### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern.  
Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:

Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen.  
Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.
3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.

#### 4.3.5 MQTT Last Will-Einstellungen

Beim Aufbau einer Verbindung können MQTT Clients, wie z.B. das MQTT Publisher-Modul des dataFEED Gateway, den Namen eines MQTT Topics sowie eine Nachricht an den MQTT Broker übergeben. Falls der MQTT Broker feststellt, dass die Verbindung zum Client nicht mehr besteht (z.B. weil ein Switch im Netz ausgefallen ist), veröffentlicht der MQTT Broker diese Nachricht in diesem Topic.

Die Ansicht **MQTT Last Will-Einstellungen** erlaubt die Festlegung der Einstellungen *Last Will und Testament* für die MQTT-Verbindung:

- **Topic-Name**  
Das Feld für die Festlegung des Topic-Namens enthält den vollständigen Namens des Last Will-Topics einschließlich aller Hierarchieebenen. Die einzelnen Hierarchieebenen werden durch das Zeichen / getrennt.
- **Testament**  
Das Testamentfeld legt die Nachricht fest, die vom MQTT Broker als Testament veröffentlicht werden soll.

- **Aktiviere MQTT Retain**

Durch Setzen des Retain-Flags wird der MQTT Broker angewiesen, den jeweils letzten Datenwert für das Topic zu speichern. Je nach Konfiguration des Brokers speichert er die Daten im Arbeitsspeicher oder persistent im Dateisystem/in der Datenbank.

Datenwerte ohne Retain-Flag werden vom MQTT Broker nur an diejenigen MQTT Subscriber geliefert, die in dem Moment, in dem die Daten an den Broker gesendet werden, bei diesem angemeldet sind und das entsprechende Topic abonniert haben.

- **Aktiviere Last Will-Option**

Mit diesem Kontrollkästchen legen Sie fest, ob die MQTT-Verbindungsoption *Last Will und Testament* für die Verbindung genutzt werden soll oder nicht. Falls sie genutzt wird, stehen Ihnen die weiteren Konfigurationsfelder zur Verfügung.

### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern. Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:

Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen. Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.
3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.

### 4.3.6 MQTT Cloud-Beispielkonfigurationen

Die hier angegebenen Webseiten enthalten Beispiele für die dataFEED Gateway-Konfiguration zur Verwendung mit dem MQTT Broker eines bestimmten Cloud-Anbieters.

- IBM Watson / Bluemix  
Link: <https://developer.ibm.com/recipes/tutorials/send-plc-data-via-sofing-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-sofing-uagate-c.md](https://github.com/SoftingIndustrial/azure-iot-device-ecosystem/blob/master/get_started/embedded-linux-sofing-uagate-c.md)

## 5 Maschinen-Einstellungen

In der Ansicht **Maschinen-Einstellungen** wird der Teil des Geräts konfiguriert, der mit dem Maschinennetz verbunden ist. Insbesondere wird erwartet, dass die SPS Teil des Maschinennetzes ist.

Es wird aber auch die Verwendung nur eines Netzes unterstützt. In diesem Fall wird nur eine Ethernet-Schnittstelle des Geräts für die Verbindung verwendet.

### 5.1 Maschinennetz

In der Ansicht **Maschinennetzwerk** erlaubt die Konfiguration der Netzeinstellungen der Maschinen-Ethernet-Schnittstelle.

Die folgenden Einstellungen stehen zur Verfügung:

#### Maschinennetz-Schnittstelle

- **MAC**  
MAC-Adresse der Ethernet-Schnittstelle (nur Lesezugriff)
- **IPv4-Adresse**  
IPv4-Adresse der Ethernet-Schnittstelle  
Durch Setzen der IPv4-Adresse auf *0.0.0.0* wird der Anschluss deaktiviert (für IPv4-Verbindungen).
- **Subnetzmaske**  
Netzmaske der IPv4-Adresse in Dezimalpunktschreibweise, z.B. *255.255.255.0*
- **IPv6**  
(Nicht veränderbare) IPv6 Adresse(n) der Ethernet-Schnittstelle des Maschinennetzes, wie sie durch *IPv6 Autoconf* konfiguriert wurde(n).  
Die Anzeige **IPv6** steht nur zur Verfügung, wenn das verwendete Netz für die Verwendung von IPv6 konfiguriert wurde. Für die Ethernet-Schnittstelle des Maschinennetzes können bis zu 16 IPv6-Adressen vergeben werden.



#### Hinweis

Wenn Sie die IP-Einstellungen der Schnittstelle, die Sie für die Konfiguration verwenden ändern, dann müssen Sie das Gerät anschließend mit dieser neu-konfigurierten IP-Adresse verbinden.

#### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern.  
Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:

Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen.  
Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.
3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.

## 5.2 SPS-Verbindung

Die Anzeige **SPS-Verbindung** erlaubt, neue Verbindungen zu einer Steuerung hinzuzufügen, bestehende Verbindungen zu konfigurieren und Verbindungen wieder zu entfernen. Außerdem zeigt diese Seite die bereits konfigurierten SPS-Verbindungen mit ihrem jeweiligen Status an.

**edgeGate** unterstützt bis zu 5 SPS-Verbindungen (SIMATIC S7-300/400/1200/1500 und/oder Modbus TCP-Steuerungen).

**uaGate SI** erlaubt die Anlage einer Verbindung zu einer SIMATIC S7-300/400/1200/1500 oder einer SIMATIC S7-1200/1500 mit optimiertem Speicherzugriff.

**uaGate MB** erlaubt die Anlage einer Verbindung zu einer Modbus TCP-Steuerung.

**uaGate 840D** unterstützt die Anlage einer Verbindung zu einer SINUMERIK 840D.

### Verbindung hinzufügen

Abhängig vom aktuellen Gateway öffnet sich nach dem Betätigen der Schaltfläche **Hinzufügen** die Seite für die Konfiguration einer [Siemens S7-Verbindung](#)<sup>(35)</sup>, [Siemens S7-2-Verbindung](#)<sup>(37)</sup>, [Modbus-Verbindung](#)<sup>(39)</sup> oder einer [SINUMERIK 840D-Verbindung](#)<sup>(46)</sup>.

Bei der Arbeit mit **edgeGate** kann eine Verbindung zu einer SIMATIC S7-SPS oder zu einer Modbus TCP-Steuerung angelegt werden. Dazu muss der entsprechende Steuerungstyp aus der Auswahlliste **SPS-Typ** ausgewählt werden.

Bei der Arbeit mit **uaGate SI** kann eine Verbindung zu einer SIMATIC S7-SPS oder zu einer SIMATIC S7-1200/1500-SPS angelegt werden. Dazu muss der entsprechende Steuerungstyp aus der Auswahlliste **SPS-Typ** ausgewählt werden.

Ein Verbindungsname kann nur beim Hinzufügen einer SPS-Verbindung festgelegt werden.



#### Hinweis

Ist die maximale Anzahl der unterstützten Steuerungsverbindungen für das dataFEED Gateway bereits erreicht, können für das dataFEED Gateway keine weiteren Steuerungsverbindungen hinzugefügt werden.

Durch Betätigen der Schaltfläche **Speichern** wird die Verbindungskonfiguration mit dem Verbindungsnamen im Gerät gespeichert.

### Verbindung ändern

Um die Konfiguration einer bestehenden SPS-Verbindung zu ändern, wählen Sie zunächst die Zeile der zu ändernden Verbindung aus und betätigen anschließend die Schaltfläche **Ändern**. Abhängig Danach wird die Seite zur Konfiguration einer [Siemens S7-Verbindung](#)<sup>(35)</sup>, [Siemens S7-2-Verbindung](#)<sup>(37)</sup>, [Modbus-Verbindung](#)<sup>(39)</sup> oder einer [SINUMERIK 840D-Verbindung](#)<sup>(46)</sup> angezeigt.

### Steuerungssymbole importieren

Für eine festgelegte Steuerungskonfiguration können Symbole aus einem Steuerungsprojekt importiert werden. Dazu wählen Sie zunächst die Zeile der zu ändernden Verbindung aus und betätigen anschließend die Schaltfläche **Symbol-Import**. Danach wird die Seite zum [Siemens S7 Symbol-Import](#)<sup>(36)</sup>, [Siemens S7-2-Adressraum-Filter](#)<sup>(37)</sup>, [Modbus-Symbol-Import](#)<sup>(40)</sup> oder zum [SINUMERIK 840D-Symbol-Import](#)<sup>(47)</sup> angezeigt.

### **Verbindung entfernen**

Um eine SPS-Verbindung zu entfernen, wählen Sie diese zunächst aus und betätigen anschließend die Schaltfläche **Entfernen**.

### 5.2.1 Siemens S7-Einstellungen

In der Ansicht **Siemens Einstellungen** können Sie IP-Adressen und Typ der zu verbindenden SPS einstellen.



#### Hinweis

Diese Beschreibung gilt nur für die Produkte **edgeGate** und **uaGate SI**!

Folgende Einstellungen stehen zur Verfügung:

#### Maschinenzugriff

- **Verbindungsname**  
Name, der für die Verbindung verwendet wird  
Sonderzeichen sind nicht erlaubt.
- **IPv4-Adresse**  
IPv4-Adresse der SPS, zu der eine Verbindung aufgebaut werden soll
- **SPS-Typ**  
Typ der SIMATIC S7-Steuerung, zu der eine Verbindung aufgebaut werden soll  
Mögliche Werte sind: *S7 300/400* und *S7 1200/1500*.
- **Abfrageintervall**  
Zeit in Millisekunden zwischen den Leseanfragen an die SPS  
Diese Einstellung wird verwendet, um den Datenverkehr zwischen dem Gerät und der SPS zu begrenzen. Das Abfrageintervall gibt auch den unteren Grenzwert für das OPC UA-Abfrageintervall an. Dieser Wert muss größer oder gleich 50 ms sein.

In speziellen Fällen kann es möglich sein, für die die Verbindung zu einer SIMATIC S7-Steuerung die TSAP-Einstellungen zu konfigurieren. Dazu muss das Kontrollkästchen **Default TSAP-Einstellungen** deaktiviert werden.

- **Eigener TSAP**  
TSAP, der als eigene Adresse verwendet werden soll  
Standardmäßig ist dieser Wert in Abhängigkeit von Ihrem SPS-Typ in Maschinennetzwerk-Teil der Webseite konfiguriert.
- **Ferner TSAP**  
TSAP, der als Fremdadresse verwendet werden soll  
Standardmäßig ist dieser Wert in Abhängigkeit von Ihrem SPS-Typ in Maschinennetzwerk-Teil der Webseite konfiguriert.

#### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern.  
Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:

Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen.  
Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.
3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.

### 5.2.1.1 Symbol-Import



#### Hinweis

Diese Beschreibung gilt nur für die Produkte **edgeGate**, **uaGate SI** und **uaGate 840D**!

Die symbolischen Namen der SIMATIC S7-Daten müssen in einer *SDFI*-Datei zur Verfügung gestellt werden.

Sie können eine *SDFI*-Datei mit dem Softing-Werkzeug **dataFEED Exporter** erstellen. Dieses Werkzeug verwendet **STEP 7**- oder **TIA Portal**-Projektdateien als Eingangsdaten und ermöglicht Ihnen die Auswahl einer S7-SPS für die Erzeugung der *SDFI*-Datei mit den Symboldefinitionen.

Für die Erstellung der Symboldatei und den Symbolimport gehen Sie wie folgt vor:

1. Laden Sie [dataFEED Exporter](#) auf denjenigen PC herunter, auf dem die SPS-Konfigurations-Software (**STEP 7** oder **TIA Portal** V13/V14/V15/V16/V17/V18) installiert ist.
2. Starten Sie die Installation und folgen Sie den Anweisungen des Installationsassistenten.
3. Starten Sie **dataFEED Exporter** am Standard-Installationsort (*Start/Alle Programme/Softing/dataFEED Exporter/dataFEED Exporter*) oder an Ihrem spezifischen Installationsort.
4. Folgen Sie den **dataFEED Exporter**-Anweisungen um Ihre **STEP 7**- oder **TIA Portal**-Symboldateien zu laden und zu konvertieren.
5. Speichern Sie die konvertierte *SDFI*-Datei auf Ihrem PC.
6. Gehen Sie zurück zum dataFEED Gateway und betätigen Sie unter **Ausgewählte Datei** die Schaltfläche **Durchsuchen...** Wählen Sie Ihre zuvor erstellte *SDFI*-Datei aus.
7. Klicken Sie die Schaltfläche **Importieren**, um die *SDFI*-Datei in das dataFEED Gateway zu laden. Die importierten Symbole ersetzen die bereits existierenden Symbole. Dabei werden maximal 20.000 OPC UA Nodes(\*) importiert.

(\*) Jeder Datenpunkt, Tag, Variable, Symbol wird als ein OPC UA Node betrachtet. Das System erstellt automatisch zusätzliche OPC UA Nodes, um die OPC UA Adressraumstruktur zu erzeugen.



#### Hinweis

Je nach Anzahl der in der *SDFI*-Datei enthaltenen Symbole können Import und interne Verarbeitung längere Zeit beanspruchen.

Der Import von symbolischen Namen mit dem Sonderzeichen Punkt (.) wird nicht unterstützt.

Das dataFEED Gateway kann OPC UA-Subscriptions mit bis zu 2.500 Datenpunkten des Datentyps *Byte* und einem Abfrageintervall von 200 ms verarbeiten.



## 5.2.2 Siemens S7-2 Einstellungen

In der Ansicht **Siemens Einstellungen** können Sie die IP-Adresse für Steuerungen der S7-1200/1500-Serie einstellen.



### Hinweis

Diese Beschreibung gilt nur für das Produkt **uaGate SI**!

Die folgenden Einstellungen stehen zur Verfügung:

#### Maschinenzugriff

- **Verbindungsname**  
Name der für die Verbindung verwendet wird  
Sonderzeichen sind nicht erlaubt.
- **IPv4-Adresse**  
IPv4-Adresse der SPS, zu der eine Verbindung aufgebaut werden soll.
- **Experteneinstellungen**  
Ändern Sie die Experteneinstellungen nur, wenn dies vom Softing-Support ausdrücklich empfohlen wurde.

#### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern.  
Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:

Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen.  
Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.
3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.

### 5.2.2.1 Adressraum einer Siemens-SPS mit optimierten Bausteinen einschränken



### Hinweis

Diese Beschreibung gilt nur für das Produkt **uaGate SI**!

Ohne Einschränkung des Adressraums ist mit **uaGate SI** der gesamte unterstützte Adressbereich einer S7-1200/S7-1500-Steuerung mit optimierten Bausteinen für den Datenaustausch über OPC UA und MQTT verfügbar. Es ist aber möglich, den für OPC UA und MQTT sichtbaren Adressbereich der SPS einzuschränken.

Dazu wählen Sie in der Ansicht **SPS-Verbindung** die bereits aufgebaute Verbindung zu einer S7-1200/S7-1500 mit optimierten Bausteinen aus und wählen Sie die Schaltfläche **Symbol-Import** aus. Anschließend lassen sich in der Ansicht **Adress-Raum** der gesamte verfügbare Adressraum der Steuerung aufklappen und die einzelnen Variablen für die Übernahme in den für OPC UA und MQTT sichtbaren Adressbereich anklicken bzw. deren Markierung wieder löschen.

Bei der Auswahl einer einzelnen Variablen des Adressraums der Steuerung werden unter **Eigenschaften** deren **Node-Id**, **Node-Klasse**, **Browse-Name**, **Display-Name** und **Beschreibung** angezeigt.

Falls auf den gesamten Adressraum zugegriffen werden soll, empfiehlt es sich, alle zuvor konfigurierten Adressraumbeschränkungen zu löschen.

#### **Einstellungen speichern und übernehmen**

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern und anzuwenden.

### 5.2.3 Modbus-Einstellungen

Die Ansicht **Modbus Einstellungen** erlaubt die Festlegung der IP-Adresse sowie von Details der zu verbindenden Modbus-Steuerung.



#### Hinweis

Diese Beschreibung gilt nur für die Produkte **edgeGate** und **uaGate MB!**



#### Hinweis

Das Produkt **edgeGate** unterstützt die Festlegung von mehr als einer Modbus-Verbindung.

Folgende Einstellungen stehen zur Verfügung:

#### Maschinenzugriff

- **Verbindungsname**  
Name, der für die Verbindung verwendet wird  
Sonderzeichen sind nicht erlaubt.
- **IPv4-Adresse**  
IPv4-Adresse der SPS, zu der eine Verbindung aufgebaut werden soll
- **Port**  
Portnummer der SPS, zu der eine Verbindung aufgebaut werden soll
- **Unit-Id**  
Slave-Adresse der SPS, zu der eine Verbindung aufgebaut werden soll
- **Abfrageintervall [ms]**  
Zeit in Millisekunden zwischen den Leseanfragen an die SPS  
Diese Einstellung wird verwendet, um den Datenverkehr zwischen dem Gerät und der SPS zu begrenzen. Das Abfrageintervall gibt auch den unteren Grenzwert für das OPC UA-Abfragintervall an. Dieser Wert muss größer oder gleich 50 ms sein.
- **Start Adresse**  
Festlegung der Startadresse für Adresszuordnung  
Einige Modbus-Steuerungen beginnen die Adresszuordnung für die angeschlossenen Geräte bei 0, andere beginnen diese bei 1.
  - **Start Adresse 0**  
Optionsschaltfläche für Festlegung, dass für Modbus-Steuerung Startadresse bei 0 beginnt
  - **Start Adresse 1**  
Optionsschaltfläche für Festlegung, dass für Modbus-Steuerung Startadresse bei 1 beginnt
- **Reihenfolgen-Einstellungen**  
Festlegung der Reihenfolge von Daten in Telegrammen
  - **Bytes tauschen**  
Kontrollkästchen für Festlegung, dass Bytes innerhalb eines Wortes (16 Bit) gedreht werden
  - **Wörter tauschen**  
Kontrollkästchen für Festlegung, dass Worte innerhalb eines Doppelwortes (32 Bit) gedreht werden
  - **Doppelwörter tauschen**  
Kontrollkästchen für Festlegung, dass Doppelworte innerhalb einer Fließkommazahl (64 Bit) gedreht werden
- **Functioncode-Einstellungen**  
Festlegung des Funktionscodes für Schreiben von Werten

- **Write Single Register**  
Kontrollkästchen für Festlegung, dass für Schreiben von Werten der Modbus-Funktionscode *Write Single Register 06* anstatt des Modbus-Funktionscodes *Write Multiple Registers 16* verwendet wird
- **Write Single Coil**  
Kontrollkästchen für Festlegung, dass für Schreiben von Werten der Modbus-Funktionscode *Write Single Coil 05* anstatt des Modbus-Funktionscodes *Write Multiple Coils 15* verwendet wird

### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern.  
Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:

Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen.  
Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.
3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.

#### 5.2.3.1 Symbol-Import



##### Hinweis

Diese Beschreibung gilt nur für die Produkte **edgeGate** und **uaGate MB**!



##### Hinweis

Die symbolischen Namen der Modbus-Datenpunkte müssen in einer ASCII-Textdatei bereitgestellt werden. In dieser Textdatei beschreibt jeweils eine Zeile die Zuordnung zwischen einem symbolischem Namen und dem entsprechenden Modbus-Datenpunkt. Am Anfang der Zeile steht der symbolische Name, gefolgt vom Gleichheitszeichen = und der Festlegung des Modbus-Datenpunkts. Wobei durch das Punktzeichen . Hierarchieebenen jeweils eine Hierarchie-Ebene können über das Punktzeichen . festgelegt werden.

Beispiel einer Modbus-Symboldatei:

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

Die Ansicht **Symbol-Import** erlaubt den Import symbolischer Namen für eine verbundene Modbus-Steuerung.



##### Hinweis

Für den Import einer Modbus-Symboldatei muss zunächst die entsprechende Modbus-Verbindung konfiguriert sein (siehe [Modbus Einstellungen](#))<sup>39</sup>.

1. Klicken Sie unter **Ausgewählte Datei** die Schaltfläche **Durchsuchen....** Wählen Sie die zu importierende Symboldatei aus.
2. Klicken Sie die Schaltfläche **Importieren**, um die Symboldatei in das dataFEED Gateway zu laden. Die importierten Symbole ersetzen die bereits existierenden Symbole.

### 5.2.3.1.1 Modbus Item Syntax



#### Hinweis

Diese Beschreibung gilt nur für die Produkte **edgeGate** und **uaGate MB**!

#### Syntax der Modbus-Datenpunkte

- Die Syntax eines Modbus-Datenpunkts ist wie folgt aufgebaut:  
*[Gruppe.]<Bereich><Datentyp><StartAdresse>[.FeldGröße][Suffix]*
- Für Modbus-Datenpunkte vom Datentyp *BOOL* ist die Angabe der Bitnummer erforderlich:  
*[Gruppe.]<Bereich><Datentyp><StartAdresse><.Bitnummer>[.FeldGröße][Suffix]*
- Ist für die Verbindung *UnitID individuell mit Itemsyntax* angewählt, ist folgende Syntax notwendig:  
*[UnitID.][Gruppe.]<Bereich><Datentyp><StartAdresse><.Bitnummer>[.FeldGröße][Suffix]*

Legende:

*<>* = zwingend erforderliche Komponente eines Modbus-Datenpunkts

*[ ]* = optionale Komponente eines Modbus-Datenpunkts

#### [Gruppe.]

Operandenbereiche können zu Gruppen zusammengefasst werden.

Ist *UnitID individuell mit Itemsyntax* im Bereich 0 - 65535 angewählt so reduziert sich der Bereich auf 0 - 255.

Sind in der Peripherie Lücken vorhanden, können diese durch Bildung unterschiedlicher Gruppen übersprungen werden. Die Lücke wird dann nicht angefordert. Dazu wird einfach der Gruppenname vor den Datenpunktnamen gesetzt und durch einen Punkt getrennt (*Gruppenname.Datenpunktname*).

Der Gruppenname setzt sich zusammen aus G und der Nummer.

Beispiel:

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

#### [UnitID.]

Die UnitID wird für diesen Datenpunkt mit der Datenpunktsyntax angegeben. Dazu wird einfach der UnitID-Name vor den Datenpunktnamen gesetzt und durch einen Punkt getrennt (*UnitID-Name.Datenpunktname*).

Der UnitID-Name setzt sich zusammen aus *Id* und der Nummer.

Wird eine Gruppe angegeben, so reduziert sich der Bereich der Gruppennummer auf 0 - 255.

Fehlt die UnitID in der Datenpunktsyntax, so wird die parametrisierte UnitID zur Steuerung übertragen.

Beispiel:

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

## &lt;Bereich&gt;

	Syntax Kürzel	Nummer	Orientierung*	Zugriffsrechte
Diskreter Eingang	I E DI DE	1xxxxx	BIT	Lesen
Diskreter Ausgang	A O Q DA DO DQ	0xxxxx	BIT	Lesen / Schreiben
Eingangsregister	ER IR	3xxxxx	WORD	Lesen
Register (Betriebsregister)	R HR	4xxxxx	WORD	Lesen / Schreiben
Diskreter Eingang Oktal **	J	-	BIT	Lesen
Diskreter Ausgang Oktal **	P	-	BIT	Lesen / Schreiben

\* BIT-orientiert bedeutet, dass je physikalischer Adresse ein Bit angesprochen wird. WORD-orientiert bedeutet, dass je physikalischer Adresse ein Wort (16 Bit) angesprochen wird.

\*\* Die Eingabe der Startadresse ist Oktal; damit sind die Zahlen 8 und 9 ungültige Zeichen. Intern wird die Adresse dezimal verwaltet und ist bei Protokollierung und Status zu berücksichtigen.

Diskrete Ein- und Ausgänge belegen in der SPS 1 Bit. Beim Lesen und Schreiben werden sie als 8 Bit-Wert bearbeitet. **Das bedeutet, dass das Schreiben von einzelnen Bits nicht unterstützt wird.**

Bereiche können entweder über die oben genannte Buchstabenfolge oder über eine Nummer adressiert werden. So kann ein diskreter Eingang über das Kürzel *E* ebenso angesprochen werden wie über die Nummer *1*.

## &lt;Datentyp&gt;

	Syntax	Syntax R	Syntax E / A	Syntax ER	Mit Array	Sinnvolle Suffixe
<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 3I12034 ERI120 IRI120 3I12034	R50.2 HR50.2 400050.2 ER120.2 IR120.2 3I12034.2	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</b> <b>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</b> <b>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	----	----

\* falls unter Datentypen *nur Standard-Typen* (Server-Einstellungen) ausgewählt wurde

\*\* falls unter Datentypen *auch vorzeichenlose* (Server-Einstellungen) gewählt

\*\*\* Bei Suffix *WDT* (*Wago Date and Time*) werden 4 Register (8 Bytes) gelesen

\*\*\*\* Es ist herstellerabhängig, welches Byte als erstes oder zweites von dem Word / Double-Word angegeben ist. Es gibt zwei Möglichkeit für die Anlage von Verbindungen:

- (1) Eine für Wort/Doppelwort-Zugriffe, möglicherweise mit der Option *Wörter tauschen* (je nach Doppelwort-Implementierung in der Modbus-Klemme).
- (2) Eine zweite für Byte-Zugriffe und der Option *Bytes tauschen*



**<Startadresse>**

Die Startadresse gibt die Adresse an, ab der gelesen bzw. geschrieben wird.

Beispiel:

- ER120: Input Register 120

Ist die Startadresse ein bestimmtes Bit, ist zusätzlich die Angabe der Bitnummer erforderlich

**<.Bitnummer>**

Immer dann, wenn der Datentyp *BOOL* ist, ist die Angabe der Bitnummer erforderlich!

Beispiel:

- HRX5.2: Bit 2 des Holding Register 5

**[.FeldGröße]**

Um mehrere Einheiten eines Datentyp zusammenzufassen, werden Felder gebildet.

Beispiel:

- HRD50.3

**[Strings]**

Um bei Modbus Steuerungen Strings zu unterstützen, erlauben wir die Interpretation von aufeinander folgenden Modbus Registern als eine Zeichenkette mit 8-Bit ASCII Kodierung.

*Für String werden beide Bytes der 16 Bit Register verwendet.*

Beispiel:

- RS100.8 kann die Modbus-Register 100 bis 108 als einen String von 8 Zeichen zu je 8-Bit interpretieren.

**[Suffix]**

Suffixe können verwendet werden, um einen Wert in einem anderen Format darzustellen.

Suffix	Syntax	Verwendung	Bereich	Datentyp	Anmerkungen
BitArray	BA		No. of bits:		Mit dem Suffix <i>BA</i> werden die auf der SPS gesicherten Datenspeicher als Feld von Bits angezeigt.
		Byte	Size in bytes times 8	BOOLEAN	
		Word	Size in words times 16	BOOLEAN	
		Int	Size in bytes times 8	BOOLEAN	
		DWord	Size in bytes times 8	BOOLEAN	
BCD	BCD	DInt	Size in bytes times 8	BOOLEAN	Mit dem Suffix <i>BCD</i> werden die auf der SPS gesicherten Daten als non-signed binary-coded-Werte angezeigt. So wird z.B. der Dezimalwert 65535 als 9999 angezeigt.
		Byte	Byte: 0 bis 99	SHORT	
		Word	Word: 0 bis 99	SHORT	
		Int	Int: 0 bis 999		
		DWord	DWord: 0 bis 999999		
		DInt	DInt: 0 bis 999999		

### 5.2.4 SINUMERIK 840D-Einstellungen

Die Anzeige **Siemens Einstellungen** ermöglicht die Konfiguration einer SINUMERIK 840D-Verbindung.



#### Hinweis

Diese Beschreibung gilt nur für das Produkt **uaGate 840D**!

Folgende Einstellungen stehen zur Verfügung:

#### Maschinenzugriff

Eine SINUMERIK 840D-Verbindung wird durch folgende Angaben festgelegt:

- **Verbindungsname**  
Für die Verbindung zu verwendende Name  
Sonderzeichen werden nicht unterstützt.
- **IPv4-Adresse**  
IPv4-Adresse der SINUMERIK 840D, zu der eine Verbindung aufgebaut werden soll
- **Aktivierte Verbindungsarten**  
Über die Kontrollkästchen **NCK** und **SPS** kann die Verbindung zum NCK- als auch zum SPS-Teil der SINUMERIK 840D aktiviert bzw. deaktiviert werden.
- **NCK TSAP Auswahl**  
Vordefinierte Auswahl aus fernen TSAPs (Sinumerik 840D SL NCK, benutzerdefiniert) für die NCK Verbindung. Vorauswahl ist **Sinumerik 840D SL NCK**. Mit der Auswahl **benutzerdefiniert** wird das Eingabefeld **NCK Ferner TSAP** eingeblendet.
- **NCK Ferner TSAP**  
Eingabefeld für den benutzerdefinierten fernen NCK TSAP.
- **SPS TSAP Auswahl**  
Vordefinierte Auswahl aus fernen TSAPs (Sinumerik 840D SL PLC, S7 300/400, S7 1200/1500, benutzerdefiniert) für die PLC Verbindung. Vorauswahl ist **Sinumerik 840D SL PLC**. Mit der Auswahl **benutzerdefiniert** wird das Eingabefeld **PLC Ferner TSAP** eingeblendet.
- **PLC Ferner TSAP**  
Eingabefeld für den benutzerdefinierten fernen PLC TSAP.
- **Alarmüberwachung**  
Aktiviert den Versandt von Alarmmeldungen von der Sinumerik an das **uaGate 840D**. Bei einigen Firmwareversionen der Sinumerik 840D PL kann dies zu Problemen führen.
- **Werkzeugüberwachung**  
Dies fügt werkzeugspezifische Einträge dem OPC UA Addressraum hinzu.
- **Experteneinstellungen**  
Ändern Sie die Experteneinstellungen nur, wenn dies vom Softing-Support ausdrücklich empfohlen wurde.

▪ **Verbiete Schreibzugriff auf Gerätekomponente**

Mit diesen Einstellungen können Sie den Schreibzugriff auf die SPS und NCK Komponenten der Sinumerik 840D zulassen, bzw. komplett verbieten. Falls Sie den Schreibzugriff auf die SPS erlauben, gilt dies nur für die Einträge in der SDFI-Datei, die dort ebenfalls über Schreibrechte verfügen. Falls Sie den Schreibzugriff auf die NCK Komponente zulaassen, gilt dies nur insoweit die Sinumerik den Schreibzugriff zulässt.

**Warnung: Schreibzugriff auf die Sinumerik 840D kann gefährlich sein. Wenn Sie ihn aktivieren, müssen Sie sicherstellen, dass nur Daten geändert werden, bei denen dies gefahrlos möglich ist!**

### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern. Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:

Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen. Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.
3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.

#### 5.2.4.1 Symbol-Import NCK



#### Hinweis

Diese Beschreibung gilt nur für das Produkt **uaGate 840D**!

In **uaGate 840D** ist bereits eine Standard-Symboldatei enthalten. Sie wird aktiviert, sobald eine Verbindung konfiguriert wurde.

Durch den Import einer Symboldatei im AWL-Format kann der Namensraum geändert werden.

1. Bestätigen Sie unter **Ausgewählte Datei** die Schaltfläche **Durchsuchen...** und wählen Sie die zu importierende AWL-Datei aus.
2. Wählen Sie die Schaltfläche **Importieren**, um die AWL-Datei in **uaGate 840D** zu laden. Die importierten Symbole ersetzen die bereits existierenden Symbole.



#### Hinweis

Dem Namensraum wird auf Wurzelebene automatisch ein Symbol **alarm** hinzugefügt, welches die NCK-Alarme anzeigt.

Wenn in der importierten Symboldatei ebenfalls ein Symbol mit Namen **alarm** vorhanden ist, wird dieses durch das automatisch generierte Symbol **alarm** überschrieben.

## 5.3 Symbol-Ansicht

Diese Seite stellt den gefilterten Namensraum der konfigurierten Steuerung bzw. den Namensraum der importierten Symboldatei(en) in einer hierarchischen Ansicht dar.

## 6 Service-Einstellungen

Die Anzeige **Service-Einstellungen** ermöglicht allgemeine Geräteeinstellungen.

Diese Einstellungen werden in den folgenden Abschnitten näher beschrieben.

- [Zeiteinstellungen](#) <sup>(48)</sup>
- [Zurücksetzen](#) <sup>(48)</sup>
- [Firmware-Update](#) <sup>(49)</sup>
- [Sichern und Wiederherstellen](#) <sup>(50)</sup>
- [Benutzerpasswort](#) <sup>(51)</sup>
- [micro SD-Karte](#) <sup>(52)</sup>
- [Support](#) <sup>(52)</sup>

### 6.1 Zeiteinstellungen

In der Ansicht **Zeiteinstellungen** können Sie die Systemzeit des dataFEED Gateway einstellen.

Die lokale Zeit wird vom dataFEED Gateway nicht unterstützt. Alle Zeiten müssen im *UTC*-Format eingegeben werden.

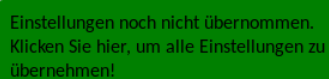
Die Systemzeit kann über NTPv4 [RFC 5905] synchronisiert werden, entweder über einen NTP-Server innerhalb Ihres LAN-Netzes oder über einen beliebigen NTP-Server im Internet (z.B. 0.pool.ntp.org). Im zweiten Fall müssen Sie sicherstellen dass der UDP-Port 123 nicht von einer Firewall blockiert ist.

Für die Verwendung von NTP aktivieren Sie das Kontrollkästchen **Zeit automatisch beziehen** und geben Sie entweder die IP-Adresse oder den Host- und Domännennamen des NTP-Servers in das Eingabefeld **NTP-Serveradresse** ein.

Wenn Sie NTP auf dem dataFEED Gateway aktiviert haben, können andere Geräte in Ihrem Netz das dataFEED Gateway als NTP-Server verwenden.

#### Einstellungen speichern und übernehmen

1. Klicken Sie auf die Schaltfläche **Speichern**, um Ihre Einstellungen zu speichern. Ein Hinweis erscheint und erinnert Sie, dass die Übernahme weiterer geänderter Einstellungen noch offen ist:



Einstellungen noch nicht übernommen.  
Klicken Sie hier, um alle Einstellungen zu übernehmen!

2. Klicken Sie auf diesen Hinweis. Ihre Einstellungen werden vom System übernommen. Je nach Umfang der Einstellungsänderungen kann dieser Vorgang einige Zeit dauern bis er abgeschlossen ist.
3. Eine Meldung im oberen Fensterteil gibt Ihnen Bescheid, wenn der Vorgang erfolgreich abgeschlossen ist.

### 6.2 Zurücksetzen

In der Ansicht **Zeiteinstellungen** lassen sich verschiedene Teilaspekte des dataFEED Gateway zurücksetzen.

### Gateway-Neustart

- Durch einen Klick auf die Schaltfläche **Neustart** im Abschnitt **Hardware-Neustart** starten Sie das dataFEED Gateway neu.  
Durch den Neustart der Hardware werden auch alle neue Konfigurationen übernommen.

### Konfiguration auf Standardwerte zurücksetzen

- Wählen Sie das Kontrollkästchen **IT-Einstellungen**, falls die dataFEED Gateway-Konfiguration des IT-Netzes zurückgesetzt werden soll.
- Wählen Sie das Kontrollkästchen **Maschinen-Einstellungen**, falls die dataFEED Gateway-Konfiguration des Maschinennetzes zurückgesetzt werden soll.
- Klicken Sie auf die Schaltfläche **Konfiguration auf Standardwerte zurücksetzen** um den ausgewählten Teil/die ausgewählten Teile der Konfiguration auf die Firmware-Voreinstellungen zurückzusetzen.

## 6.3 Firmware-Update

Die Ansicht **Firmware-Update** ermöglicht die Aktualisierung der dataFEED Gateway-Firmware.

### Firmware-Update

1. Klicken Sie die Schaltfläche **Durchsuchen** im Abschnitt **Firmware aus Datei aktualisieren** um eine verfügbare Firmware-Imagedatei auszuwählen und klicken Sie die Schaltfläche **Öffnen**.  
Das Hochladen der Datei nimmt einige Zeit in Anspruch.
1. Nach dem vollständigen Hochladen der Datei, wird das Firmware-Image automatisch entpackt.  
Während des Entpackens leuchtet die LED **SYS** konstant grün.
2. In einem nächsten Schritt wird die Firmware-Imagedatei geprüft.  
Während der Überprüfung blinkt die LED **SYS** grün.
3. Nach erfolgreicher Überprüfung startet das dataFEED Gateway neu und schließt so die Aktualisierung der Firmware ab.  
Während des Neustarts des dataFEED Gateway blinkt die LED **SYS** rot.  
Erkennt das dataFEED Gateway während der Aktualisierung einen Fehler (z.B. wenn eine falsche Firmware-Imagedatei ausgewählt wurde), so wird die Aktualisierung abgebrochen und die LED **ERR** blinkt rot.  
Mehr Informationen über die LEDs finden Sie in [LED-Statusanzeigen](#) <sup>53</sup>.

## 6.4 Sichern und wiederherstellen

Die Ansicht **Firmware-Update** ermöglicht das Sichern und Wiederherstellen der Gerätekonfiguration entweder in/von einer Datei auf dem Rechner oder auf der micro SD-Karte des dataFEED Gateway .

### Sicherung in Datei

- Klicken Sie die Schaltfläche **Durchsuchen** im Abschnitt **Konfiguration aus Datei laden**, um eine zuvor gespeicherte Konfigurationsdatei von Ihrem Rechner in das dataFEED Gateway zu laden.
- Klicken Sie die Schaltfläche **Sicherung** im Abschnitt **Konfiguration in Datei sichern**, um die aktuelle Konfiguration in eine Sicherungsdatei auf Ihrem Rechner zu speichern.

### Sicherung auf Karte

- Klicken Sie auf die Schaltfläche **Wiederherstellen** im Abschnitt **Konfiguration der SD-Karte wiederherstellen**, um die zuvor auf der micro SD-Karte gespeicherte Konfigurationsdatei in das dataFEED Gateway zu laden.
- Klicken Sie auf die Schaltfläche **Speichern** im Abschnitt **Konfiguration auf SD-Karte sichern**, um die aktuelle Konfiguration auf der micro SD-Karte zu speichern
- Klicken Sie auf die Schaltfläche **Browse** im Abschnitt **SD-Karte-Inhalt**, um den aktuellen Inhalt der micro SD-Karte anzuzeigen.



#### Hinweis

Bei einer Änderung der IP-Einstellungen der Schnittstelle, die Sie für die Konfiguration verwenden, ist anschließend die erneute Verbindung dieser Schnittstelle mit der neukonfigurierten IP-Adresse notwendig.



#### Hinweis

Beim Wiederherstellen der Konfiguration wird nur der Teil der Konfiguration berücksichtigt, der vom angemeldeten Benutzer (*Administrator, IT-Verantwortlicher, Servicetechniker*) bearbeitet werden darf.

Nur der Benutzer *Administrator* kann die komplette Konfiguration wiederherstellen.

#### Ausnahme:

Beim Wiederherstellen der Konfiguration durch den Servicetechniker werden auch die Symbole für die MQTT Topic-Auswahl aus den IT-Einstellungen wiederhergestellt, da diese Symbole aus dem Symbolimport der Maschinen-Einstellungen abgeleitet werden.

Beim Sichern wird immer die komplette dataFEED Gateway-Konfiguration gespeichert.

## 6.5 Benutzerpasswort

Die Ansicht **Benutzerpasswort** ermöglicht die Änderung eines oder mehrerer dataFEED Gateway-Benutzerpasswörter in Abhängigkeit von der aktuellen Benutzerrolle: Während ein Benutzer, der sich als *Administrator* angemeldet hat, alle einzelnen dataFEED Gateway-Passwörter ändern kann, kann der Benutzer *IT-Verantwortlicher* nur das *IT-Verantwortlicher*-Passwort und der Benutzer *Servicetechniker* nur das *Servicetechniker*-Passwort ändern.

**Passwort ändern - administrator**

**Passwort ändern - itadmin**

**Passwort ändern - mfadmin**

Mit den folgenden Schritten ändern Sie das Benutzerpasswort für die verschiedenen Benutzerrollen. Die einzelnen Passwörter, die geändert werden können, hängen von der Rolle des aktuellen Benutzers ab.

1. Geben Sie in das Eingabefeld des Abschnitts **Aktuelles Passwort** das aktuelle Passwort ein. Die Eingabe des aktuellen Passworts ist nur dann notwendig, wenn das zu ändernde Passwort der Benutzerrolle zugeordnet ist, mit der der aktuelle Benutzer angemeldet ist.
2. Geben Sie in das Eingabefeld des Abschnitts **Neues Passwort** das aktuelle Passwort ein.
3. Bestätigen Sie das eingegebene neue Passwort durch erneute Eingabe des neuen Passworts im Eingabefeld **Passwort bestätigen**.
4. Klicken Sie die Schaltfläche **Speichern**, um Ihre Änderungen zu speichern.



### Hinweis

Das Klicken auf die Schaltfläche **Speichern** wird das neue Passwort umgehend aktiv. Greift der Browser anschließend auf eine Webseite mit dynamische Daten zu, ist eine erneute Anmeldung notwendig.

### Rolle der Benutzer und deren zugehörige Aufgaben

Aufgabe	Administrator (administrator)	IT-Verantwortlicher (itadmin)	Servicetechniker (mfadmin)
Konfiguration ändern, Firmware aktualisieren, Passwort auch für andere Benutzerrollen als <i>Administrator</i> ändern	<input checked="" type="checkbox"/>		
<a href="#">IT-Einstellungen</a> <sup>(16)</sup> und <a href="#">Zeiteinstellungen</a> <sup>(48)</sup> ändern	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">Maschinen-Einstellungen</a> <sup>(32)</sup> und <a href="#">Zeiteinstellungen</a> <sup>(48)</sup> ändern	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>



### Hinweis

Bitte seien Sie bei Änderungen des *Administrator*-Passworts vorsichtig. Wenn Sie das *Administrator*-Passwort verlieren, so können Sie das Gerät auf die Werkseinstellungen (einschließlich des *Administrator*-Passworts) zurücksetzen, Sie werden dabei aber Ihre Konfigurationsdaten verlieren (siehe auch [Gerät zurücksetzen](#)) <sup>(13)</sup>.

## 6.6 micro SD-Karte

Die Ansicht **SD-Karte** stellt Informationen und Optionen zur micro SD-Karte zur Verfügung.

- **SD-Speicher-Auslastung**  
Zeigt an, ob die micro SD-Karte im Dateisystem verfügbar ist und zu wieviel Prozent der Speicher ausgelastet ist  
Die Information *not mounted* sagt aus, dass die micro SD-Karte nicht erkannt wird bzw. nicht verfügbar ist).
- Klicken Sie die Schaltfläche **Browse** im Abschnitt **SD-Karten-Inhalt**, um den Inhalt der micro SD-Karte anzuzeigen.
- Klicken Sie die Schaltfläche **Entfernen** im Abschnitt **SD-Karte sicher entfernen**, um das Dateisystem der micro SD-Karte zu deaktivieren und diese sicher aus dem dataFEED Gateway zu entfernen.

## 6.7 Support

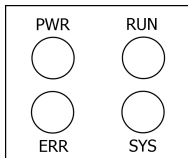
Die Seite **Support** stellt Hilfsmittel zum Zugriff auf Informationen bereit, die Sie beim Auftreten von Auftreten von Problemfällen nutzen können.

- Klicken Sie die Schaltfläche **Start** im Abschnitt **Netzwerktaufzeichnung**, um die Aufzeichnung des Netzverkehrs auf allen Ethernet-Schnittstellen des dataFEED Gateway zu beginnen.  
Nach der Betätigung der Schaltfläche **Start** wird der Netzwerkverkehr in einem Ring-Speicher von Aufzeichnungsdateien aufgezeichnet. Nach einem Neustart des Gerätes endet die Aufzeichnung.  
Die Aufzeichnungsdateien werden auf der micro SD-Karte abgelegt. Das bedeutet, dass diese Funktionalität nur dann zur Verfügung steht, wenn in das dataFEED Gateway eine beschreibbare micro SD-Karte eingelegt ist, die wenigstens 8 GB freien Speicher bereitstellt.
- Klicken Sie die Schaltfläche **Stop** im Abschnitt **Netzwerktaufzeichnung**, um die Aufzeichnung des Netzverkehrs zu beenden.
- Klicken Sie die Schaltfläche **Browse** im Abschnitt **Vorhandene Netzwerktaufzeichnungen**, um die zuvor angelegten Aufzeichnungsdateien zuzugreifen.  
Diese Dateien können mit der freien Software *Wireshark* zur Analyse von Datenprotokollen ausgewertet werden (siehe [www.wireshark.org](http://www.wireshark.org)).
- Klicken Sie die Schaltflächen **Browse** im Abschnitt **Logausgaben** um auf die Log-Dateien des dataFEED Gateway zu zugreifen.



## 7 LED-Statusanzeigen

dataFEED Gateway ist auf der Vorderseite mit vier LEDs ausgestattet:



<b>PWR</b>	<b>Spannungsversorgung (power)</b> (dauerhaft grün, wenn die 24-Volt-Spannungsversorgung in Ordnung ist)
<b>RUN</b>	<b>Betrieb (running)</b>
<b>ERR</b>	<b>Fehler (error)</b>
<b>SYS</b>	<b>System</b>

Die LEDs können dauerhaft leuchten oder in unterschiedlichen Farben und Frequenzen blinken. Wir verwenden folgende Symbole:

Symbol	Farbe	Anzeige
	Keine	Aus
	Rot	Permanent
	Grün	Permanent
	Rot	Blinkend
	Grün	Blinkend

### Bedeutung der LEDs

<b>RUN</b>		Dauerhaft grün während der OPC UA-Endpoint geöffnet wurde, das Gerät vollständig betriebsbereit und der Web-Server verfügbar ist.
		Blinkt grün während der OPC UA-Namensraum aufgebaut wird (Symbolevaluierung etc.)
<b>SYS</b>		Dauerhaft grün während das Firmware-Image entpackt wird.
		Blinkt grün während die Image-Konsistenz geprüft und der Kernel ausgetauscht wird.
		Blinkt rot während die Firmware mit dem Firmware-Image-Inhalt ersetzt wird. (Während dieser Zeit ist das Gerät nicht voll funktionsfähig.)
<b>ERR</b>		Dauerhaft rot, wenn der OPC UA-Endpoint nicht geöffnet werden konnte oder wenn ein Fehler während der Firmware-Aktualisierung auftrat.
		Blinkt grün solange in der Gerätekonfiguration noch nicht alle Änderungen übernommen worden sind.



### Hinweis

Die LEDs werden kurzzeitig ausgeschaltet, wenn Sie das Gerät mit dem Rückstellknopf unten auf der Gerätevorderseite zurücksetzen oder auf die Schaltfläche **Neustart** unter **Service-Einstellungen** → **Zurücksetzen** → **Gateway-Neustart** in der Web-Server-Bedienoberfläche klicken.

## 8 Technische Daten

Spannungsversorgung	18 VDC ... 32 VDC; SELV/PELV-Versorgung obligatorisch Typischer Eingangsstrom sind 200 mA; maximal erlaubt ist 1 A (bei Berücksichtigung des Einschaltstroms)
Ethernet	2x IEEE 802.3 100BASE-TX/10BASE-T (Schnittstellen, unabhängig voneinander)
Betriebstemperatur, horizontale Montage auf Hutschiene	-40 °C ... +50 °C (0 mm Minimalabstand) -40 °C ... +55 °C (22,5 mm Minimalabstand)
Betriebstemperatur, vertikale Montage auf Hutschiene	-40 °C ... +35 °C (0 mm Minimalabstand) -40 °C ... +40 °C (22,5 mm Minimalabstand)
Lagertemperatur	-40 °C ... +85 °C
Relative Luftfeuchtigkeit	10 % ... 95 % (keine Betauung)
Einbauhöhe	Darf 2.000 m nicht überschreiten
Einbauort	Nur für den Einsatz in Innenräumen; keine direkte Sonneneinstrahlung
Abmessungen (H x B x T)	100 mm x 22,5 mm x 105 mm
Montage	Hutschiene (35 mm)
Schutzart	IP20
Gewicht	ca. 0,2 kg
IT-Netz- / Cloud-Anbindung	OPC UA (Server, insgesamt 20.000 OPC UA Nodes(*), MQTT (Publisher, bis zu 1.000 Topics)
Industrienetzanbindung	OPC UA, Steuerungen (Siemens SIMATIC S7-300/400/1200/1500, Modbus TCP-kompatible Steuerungen, Siemens SINUMERIK 840D Solution Line)
Unterstützte Entwicklungswerkzeuge	SIMATIC Step 7, TIA Portal, Siemens NCVar Selector

(\*) Jeder Datenpunkt, Tag, Variable, Symbol wird als ein OPC UA Node betrachtet. Das System erstellt automatisch zusätzliche OPC UA Nodes, um die OPC UA Adressraumstruktur zu erzeugen.

## 9 Herstellererklärung

Dieses Gerät erfüllt die Anforderungen der Richtlinie 2014/30/EU für Elektromagnetische Verträglichkeit (EMV) sowie folgende harmonisierte Normen:

EN 55011	Industrielle, wissenschaftliche und medizinische Geräte - Funkstörungen - Grenzwerte und Messverfahren
EN 61000-6-4	Elektromagnetische Verträglichkeit (EMV) - Teil 6-4: Fachgrundnormen - Störaussendung für Industriebereiche
EN 61000-6-2	Elektromagnetische Verträglichkeit (EMV) - Teil 6-2: Fachgrundnormen - Störfestigkeit für Industriebereiche



### Hinweis

Um die o.g. EMV-Anforderungen zu erfüllen, müssen die anderen Komponenten in Ihrer Installation (Wechselstromadapter, Industrial-Ethernet-Geräte usw.) ebenfalls EMV-Anforderungen erfüllen. Ein geschirmtes Kabel muss verwendet werden. Außerdem muss die Kabelschirmung gründlich geerdet sein.



### VORSICHT

Das Gerät ist eine Einrichtung der Klasse A und kann im Wohnbereich Funkstörungen verursachen. In diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.



### CE

Für dieses Gerät wurde eine Konformitätserklärung für die Übereinstimmung mit dem CE-Standard abgegeben.  
Diese kann bei Softing Industrial Automation GmbH eingesehen werden.



### ROHS

Dieses Gerät ist ROHS-konform.



### FCC

Dieses Gerät wurde getestet und unterliegt den für digitale Geräte der Klasse A festgelegten Beschränkungen gemäß Teil 15 der FCC-Vorschriften. Diese Grenzwerte sehen für die Installation in gewerblichem Umfeld einen ausreichenden Schutz vor störenden Abstrahlungen vor. Dieses Gerät erzeugt, arbeitet mit und kann Rundfunkwellen ausstrahlen sowie bei nicht korrekter Verwendung Störungen des Rundfunkempfangs verursachen.

Der Betrieb dieses Geräts im Wohnbereich kann zu schädlichen Störungen führen; in diesem Fall ist der Benutzer verpflichtet, die Störungen auf eigene Kosten zu beheben.



### VCCI

Dieses Gerät der Klasse A entspricht den Bestimmungen des *Voluntary Control Council for Interference by Information Technology Equipment* (VCCI).



#### **WEEE**

Elektro- und Elektronikgeräte müssen am Ende ihrer Lebensdauer getrennt vom normalen Hausmüll entsorgt werden. Verpackungsmaterial und verschlissene Bauteile müssen nach den im jeweils installierten Land gültigen rechtlichen Bestimmungen entsorgt werden.

#### **REACH**

##### **REACH**

Für dieses Gerät wurde eine Erklärung für die Übereinstimmung mit dem Standard European Union Directive "REACH" N°1907/2006 abgegeben.  
Diese kann bei Softing Industrial Automation GmbH eingesehen werden.

**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)

