

Handbuch | DE

# TS6100

TwinCAT 2 | OPC UA Gateway





# Inhaltsverzeichnis

<b>1</b>	<b>Vorwort.....</b>	<b>5</b>
1.1	Hinweise zur Dokumentation .....	5
1.2	Zu Ihrer Sicherheit.....	6
1.3	Hinweise zur Informationssicherheit .....	7
<b>2</b>	<b>Übersicht.....</b>	<b>8</b>
<b>3</b>	<b>Installation .....</b>	<b>10</b>
3.1	Systemvoraussetzungen .....	10
3.2	Installation .....	10
3.3	Installationsvarianten .....	12
<b>4</b>	<b>Technische Einführung .....</b>	<b>16</b>
4.1	Quick Start .....	16
4.2	Empfohlene Schritte .....	18
4.3	Konfigurator.....	20
4.4	Applikationsverzeichnisse .....	21
4.5	Allgemeine Einstellungen.....	22
4.6	Konfiguration von zusätzlichen Servern .....	24
4.7	Konfiguration der Endpunkte.....	25
4.8	Migration von TF6120 .....	26
4.9	Security .....	28
4.9.1	Übersicht.....	28
4.9.2	Endpunkte .....	29
4.9.3	Zertifikatsaustausch .....	30
4.9.4	Authentifizierung .....	31
4.10	Logging .....	32
<b>5</b>	<b>Anhang .....</b>	<b>33</b>
5.1	Fehlerdiagnose .....	33
5.2	ADS Return Codes.....	33
5.3	Support und Service.....	38



# 1 Vorwort

## 1.1 Hinweise zur Dokumentation

Diese Beschreibung wendet sich ausschließlich an ausgebildetes Fachpersonal der Steuerungs- und Automatisierungstechnik, das mit den geltenden nationalen Normen vertraut ist.

Zur Installation und Inbetriebnahme der Komponenten ist die Beachtung der Dokumentation und der nachfolgenden Hinweise und Erklärungen unbedingt notwendig.

Das Fachpersonal ist verpflichtet, stets die aktuell gültige Dokumentation zu verwenden.

Das Fachpersonal hat sicherzustellen, dass die Anwendung bzw. der Einsatz der beschriebenen Produkte alle Sicherheitsanforderungen, einschließlich sämtlicher anwendbaren Gesetze, Vorschriften, Bestimmungen und Normen erfüllt.

### Disclaimer

Diese Dokumentation wurde sorgfältig erstellt. Die beschriebenen Produkte werden jedoch ständig weiterentwickelt.

Wir behalten uns das Recht vor, die Dokumentation jederzeit und ohne Ankündigung zu überarbeiten und zu ändern.

Aus den Angaben, Abbildungen und Beschreibungen in dieser Dokumentation können keine Ansprüche auf Änderung bereits gelieferter Produkte geltend gemacht werden.

### Marken

Beckhoff®, TwinCAT®, TwinCAT/BSD®, TC/BSD®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® und XPlanar® sind eingetragene und lizenzierte Marken der Beckhoff Automation GmbH.

Die Verwendung anderer in dieser Dokumentation enthaltenen Marken oder Kennzeichen durch Dritte kann zu einer Verletzung von Rechten der Inhaber der entsprechenden Bezeichnungen führen.

### Patente

Die EtherCAT-Technologie ist patentrechtlich geschützt, insbesondere durch folgende Anmeldungen und Patente:

EP1590927, EP1789857, EP1456722, EP2137893, DE102015105702

mit den entsprechenden Anmeldungen und Eintragungen in verschiedenen anderen Ländern.



EtherCAT® ist eine eingetragene Marke und patentierte Technologie lizenziert durch die Beckhoff Automation GmbH, Deutschland

### Copyright

© Beckhoff Automation GmbH & Co. KG, Deutschland.

Weitergabe sowie Vervielfältigung dieses Dokuments, Verwertung und Mitteilung seines Inhalts sind verboten, soweit nicht ausdrücklich gestattet.

Zu widerhandlungen verpflichten zu Schadenersatz. Alle Rechte für den Fall der Patent-, Gebrauchsmuster- oder Geschmacksmustereintragung vorbehalten.

## 1.2 Zu Ihrer Sicherheit

### Sicherheitsbestimmungen

Lesen Sie die folgenden Erklärungen zu Ihrer Sicherheit.  
Beachten und befolgen Sie stets produktspezifische Sicherheitshinweise, die Sie gegebenenfalls an den entsprechenden Stellen in diesem Dokument vorfinden.

### Haftungsausschluss

Die gesamten Komponenten werden je nach Anwendungsbestimmungen in bestimmten Hard- und Software-Konfigurationen ausgeliefert. Änderungen der Hard- oder Software-Konfiguration, die über die dokumentierten Möglichkeiten hinausgehen, sind unzulässig und bewirken den Haftungsausschluss der Beckhoff Automation GmbH & Co. KG.

### Qualifikation des Personals

Diese Beschreibung wendet sich ausschließlich an ausgebildetes Fachpersonal der Steuerungs-, Automatisierungs- und Antriebstechnik, das mit den geltenden Normen vertraut ist.

### Signalwörter

Im Folgenden werden die Signalwörter eingeordnet, die in der Dokumentation verwendet werden. Um Personen- und Sachschäden zu vermeiden, lesen und befolgen Sie die Sicherheits- und Warnhinweise.

### Warnungen vor Personenschäden

#### **GEFAHR**

Es besteht eine Gefährdung mit hohem Risikograd, die den Tod oder eine schwere Verletzung zur Folge hat.

#### **WARNUNG**

Es besteht eine Gefährdung mit mittlerem Risikograd, die den Tod oder eine schwere Verletzung zur Folge haben kann.

#### **VORSICHT**

Es besteht eine Gefährdung mit geringem Risikograd, die eine mittelschwere oder leichte Verletzung zur Folge haben kann.

### Warnung vor Umwelt- oder Sachschäden

#### **HINWEIS**

Es besteht eine mögliche Schädigung für Umwelt, Geräte oder Daten.

### Information zum Umgang mit dem Produkt



Diese Information beinhaltet z. B.:  
Handlungsempfehlungen, Hilfestellungen oder weiterführende Informationen zum Produkt.

## 1.3 Hinweise zur Informationssicherheit

Die Produkte der Beckhoff Automation GmbH & Co. KG (Beckhoff) sind, sofern sie online zu erreichen sind, mit Security-Funktionen ausgestattet, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Trotz der Security-Funktionen sind die Erstellung, Implementierung und ständige Aktualisierung eines ganzheitlichen Security-Konzepts für den Betrieb notwendig, um die jeweilige Anlage, das System, die Maschine und die Netzwerke gegen Cyber-Bedrohungen zu schützen. Die von Beckhoff verkauften Produkte bilden dabei nur einen Teil des gesamtheitlichen Security-Konzepts. Der Kunde ist dafür verantwortlich, dass unbefugte Zugriffe durch Dritte auf seine Anlagen, Systeme, Maschinen und Netzwerke verhindert werden. Letztere sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn entsprechende Schutzmaßnahmen eingerichtet wurden.

Zusätzlich sollten die Empfehlungen von Beckhoff zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Informationssicherheit und Industrial Security finden Sie in unserem <https://www.beckhoff.de/secguide>.

Die Produkte und Lösungen von Beckhoff werden ständig weiterentwickelt. Dies betrifft auch die Security-Funktionen. Aufgrund der stetigen Weiterentwicklung empfiehlt Beckhoff ausdrücklich, die Produkte ständig auf dem aktuellen Stand zu halten und nach Bereitstellung von Updates diese auf die Produkte aufzuspielen. Die Verwendung veralteter oder nicht mehr unterstützter Produktversionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Hinweise zur Informationssicherheit zu Produkten von Beckhoff informiert zu sein, abonnieren Sie den RSS Feed unter <https://www.beckhoff.de/secinfo>.

## 2 Übersicht

**OPC Unified Architecture (OPC UA)** ist die nächste Generation des klassischen OPC-Standards. Es handelt sich hierbei um ein weltweit standardisiertes Kommunikationsprotokoll, über das Maschinendaten hersteller- und plattformunabhängig ausgetauscht werden können. OPC UA integriert gängige Sicherheitsstandards bereits direkt im Protokoll. Ein weiterer großer Vorteil von OPC UA gegenüber dem klassischen OPC-Standard ist die Unabhängigkeit vom COM/DCOM-System.



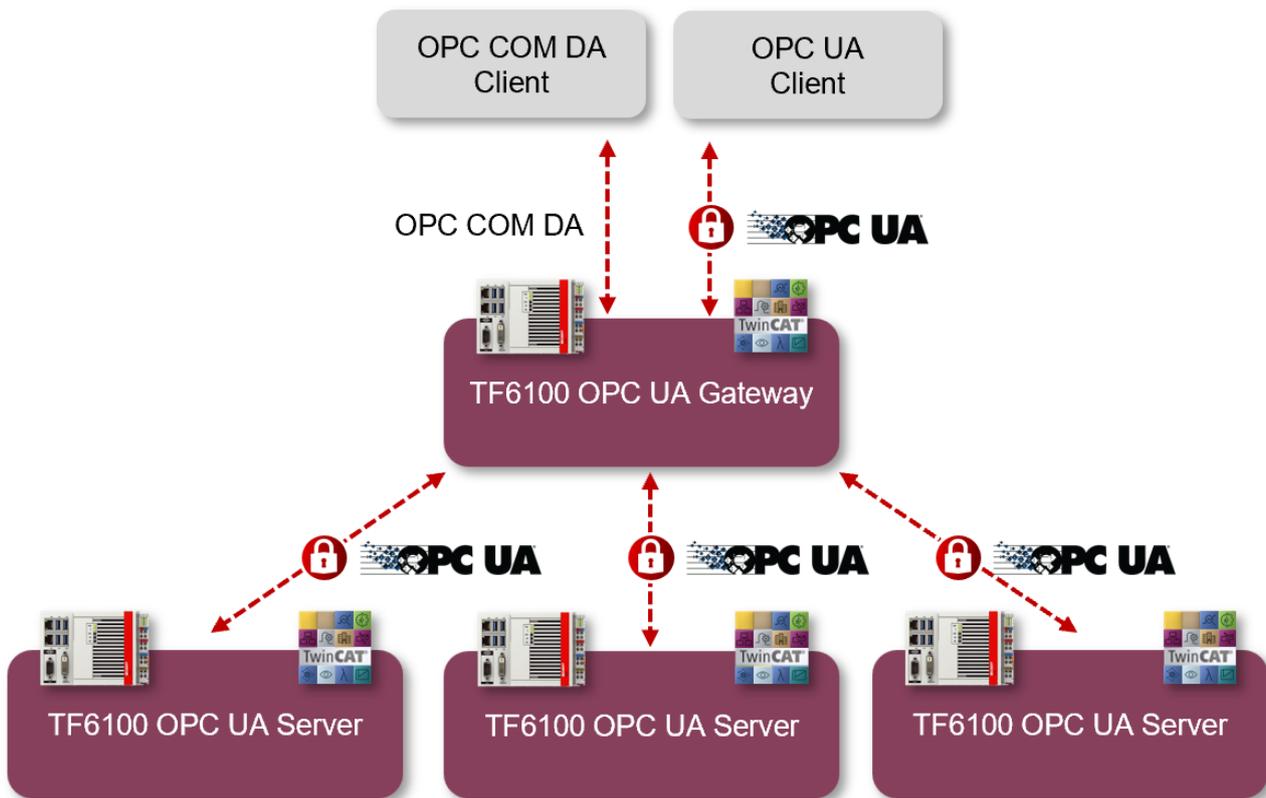
Detaillierte Informationen zu OPC UA finden Sie auf der Webseite der [OPC Foundation](#).

Die TwinCAT 3 Function TF6100 OPC UA besteht aus mehreren Softwarekomponenten, welche einen Datenaustausch mit TwinCAT, basierend auf OPC UA, ermöglichen.

Die folgende Tabelle gibt einen Überblick über die einzelnen Produktbestandteile.

Software-Komponente	Beschreibung
TwinCAT OPC UA Server	Stellt eine OPC-UA-Server-Schnittstelle zur Verfügung, damit UA-Clients auf die TwinCAT-Laufzeit zugreifen können.
TwinCAT OPC UA Client	Stellt eine OPC-UA-Client-Funktionalität zur Verfügung, damit die Kommunikation mit anderen OPC UA Servern auf der Grundlage von PLCopen-normten Funktionsbausteinen sowie einem einfach zu konfigurierenden I/O-Gerät möglich ist.
TwinCAT OPC UA Configurator	Grafische Benutzerschnittstelle für die Konfiguration des TwinCAT OPC UA Servers.
TwinCAT OPC UA Sample Client	Grafische Beispielimplementierung eines OPC UA Clients um einen ersten Verbindungstest mit dem TwinCAT OPC UA Server durchführen zu können.
TwinCAT OPC UA Gateway	Wrapper-Technologie, die sowohl eine OPC-COM-DA-Server-Schnittstelle als auch OPC-UA-Server-Aggregationsfähigkeiten zur Verfügung stellt.

Diese Dokumentation beschreibt das TwinCAT OPC UA Gateway, bei welchem es sich um eine Softwarekomponente handelt die eine OPC COM DA Schnittstelle anbietet, sowie eine OPC UA Serveraggregation ermöglicht.



Für einen schnellen Einstieg in das Produkt empfehlen wir unsere Kapitel [Installation](#) [▶ 10] und [Quick Start](#) [▶ 16]. Bitte beachten Sie auch die [Systemvoraussetzungen](#) [▶ 10] zu diesem Produkt.

## 3 Installation

### 3.1 Systemvoraussetzungen

Für die Installation und den Betrieb dieses Produkts gelten die folgenden Systemvoraussetzungen.

Technische Daten	Beschreibung
Betriebssystem	Windows 7, 10 Windows Server
Zielplattformen	PC-Architektur (x86, x64, ARM)
.NET Framework	---
Minimale TwinCAT-Version	Eine TwinCAT Installation ist für den Betrieb dieser Software nicht notwendig.
Benötigte TwinCAT-Lizenz	Eine TwinCAT Lizenz ist für den Betrieb dieser Software nicht notwendig.
Unterstützte Server	Das TwinCAT OPC UA Gateway kommuniziert ausschließlich mit TwinCAT OPC UA Servern, für die eine TF6100 Lizenz benötigt wird. Möchten Sie Fremdgeräte an das Gateway anschließen, so benötigen Sie die Software „UA Gateway“ der Firma Unified Automation.
COM/DCOM	Lokale OPC COM DA Kommunikation wird von dieser Software unterstützt. Eine Kommunikation basierend auf DCOM wird nicht unterstützt.



#### Installationsvarianten

Bitte beachten Sie auch die verschiedenen unterstützten [Installationsvarianten](#) [► 12] des TwinCAT OPC UA Gateway.

#### Firewall-Port

Um eine Kommunikation über OPC UA mit dem TwinCAT OPC UA Gateway zu ermöglichen, muss der folgende Netzwerkport in der Firewall des Geräts geöffnet werden:

```
48050/tcp (incoming)
```

Wird das TwinCAT OPC UA Gateway zum Beispiel auf einem Beckhoff Industrie-PC installiert, so muss in der Firewall des Betriebssystems dieser Port als eingehende Kommunikation geöffnet werden.

### 3.2 Installation

Die Installation dieser TwinCAT 3 Function kann, abhängig von der verwendeten TwinCAT-Version und dem Betriebssystem, auf unterschiedliche Arten erfolgen, welche im Folgenden näher beschrieben werden sollen.

#### HINWEIS

##### Updateinstallation

Bei einer Updateinstallation wird immer die vorherige Installation deinstalliert. Bitte stellen Sie sicher, dass Sie vorher ein Backup Ihrer Konfigurationsdateien erstellt haben.

#### TwinCAT Package Manager

Wenn Sie TwinCAT 3.1 Build 4026 (und höher) auf dem Betriebssystem Microsoft Windows verwenden, können Sie diese Function über den TwinCAT Package Manager installieren, siehe [Dokumentation zur Installation](#).

Normalerweise installieren Sie die Function über den entsprechenden Workload; dennoch können Sie die im Workload enthaltenen Pakete auch einzeln installieren. Diese Dokumentation beschreibt im Folgenden kurz den Installationsvorgang über den Workload.

## Kommandozeilenprogramm TcPkg

Über das TcPkg Command Line Interface (CLI) können Sie sich die verfügbaren Workloads auf dem System anzeigen lassen:

```
tcpkg list -t workload
```

Über das folgende Kommando können Sie den Workload einer Function installieren. Hier exemplarisch dargestellt am Beispiel des TF6100 TwinCAT OPC UA Client:

```
tcpkg install tf6100-opc-ua-client
```

## TwinCAT Package Manager UI

Über das User Interface (UI) können Sie sich alle verfügbaren Workloads anzeigen lassen und diese bei Bedarf installieren.

Folgen Sie hierzu den entsprechenden Anweisungen in der Oberfläche.

### HINWEIS

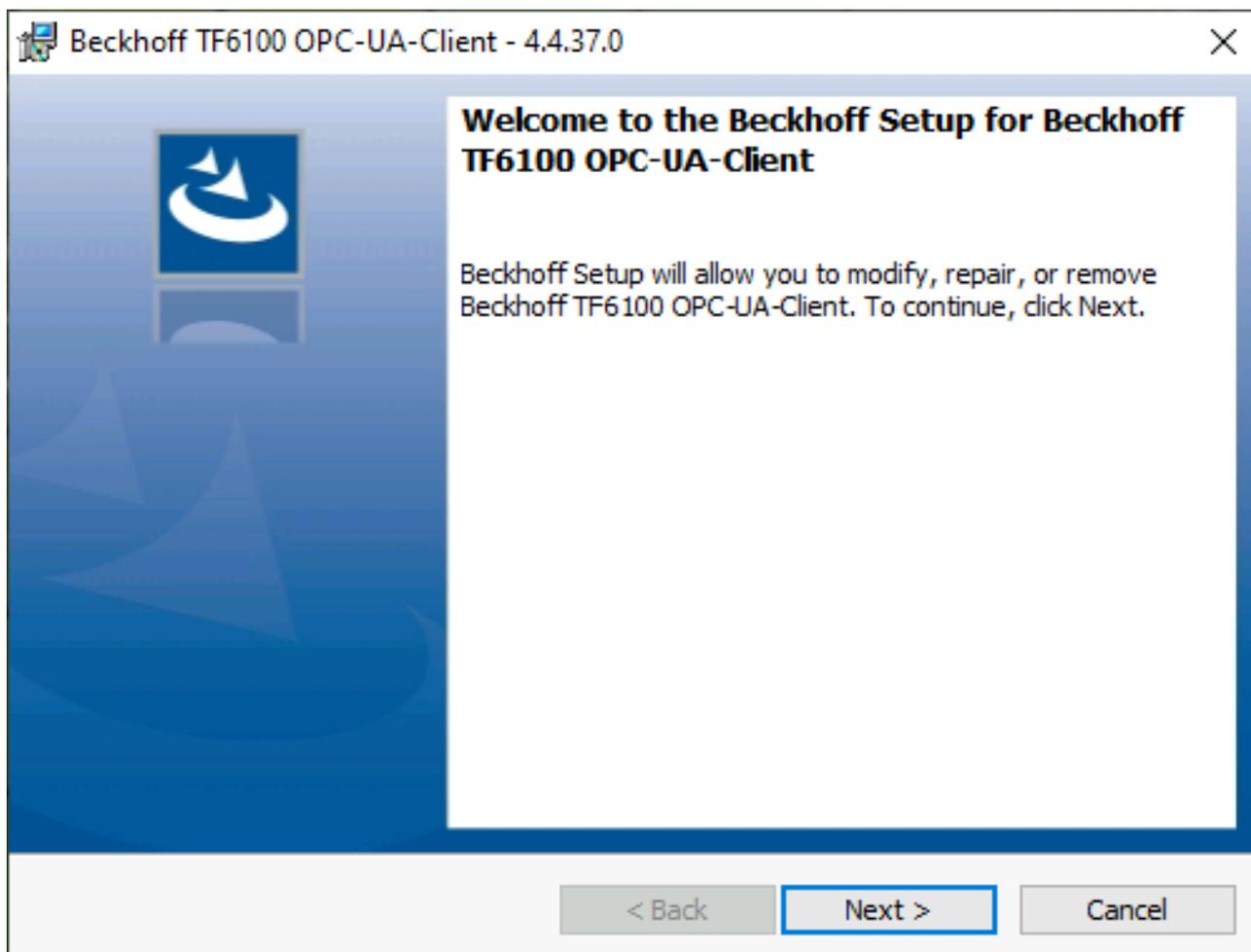
#### Unvorbereiteter TwinCAT-Neustart kann Datenverlust erzeugen

Die Installation dieser Function hat unter Umständen einen TwinCAT-Neustart zur Folge. Stellen Sie sicher, dass keine kritischen TwinCAT-Applikationen auf dem System laufen oder fahren Sie diese zunächst geordnet herunter.

## Setup

Wenn Sie TwinCAT 3.1 Build 4024 auf dem Betriebssystem Microsoft Windows verwenden, können Sie diese Function über ein Setup-Paket installieren, welches Sie auf der Beckhoff Webseite unter <https://www.beckhoff.com/download> herunterladen können.

Die Installation kann hierbei sowohl auf Engineering- als auch Runtime-Seite erfolgen, je nachdem, auf welchem System Sie die Function benötigen. Der folgende Screenshot zeigt exemplarisch die Setup-Oberfläche am Beispiel des TF6100 TwinCAT OPC UA Client-Setups.



Zur Durchführung des Installationsvorgangs, folgen Sie den entsprechenden Anweisungen im Setup-Dialog.

### HINWEIS

#### Unvorbereiteter TwinCAT-Neustart kann Datenverlust erzeugen

Die Installation dieser Function hat unter Umständen einen TwinCAT-Neustart zur Folge. Stellen Sie sicher, dass keine kritischen TwinCAT-Applikationen auf dem System laufen oder fahren Sie diese zunächst geordnet herunter.

## 3.3 Installationsvarianten

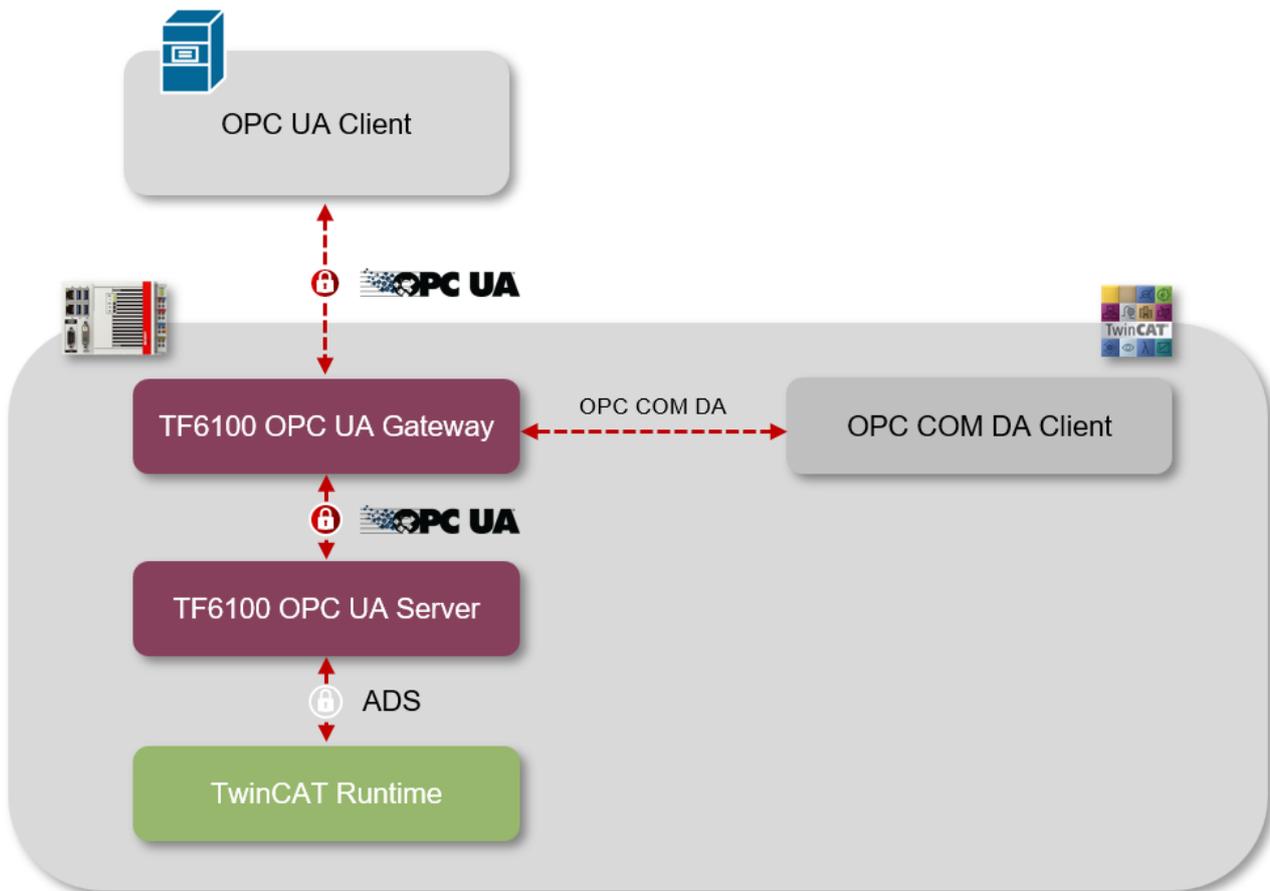
In diesem Kapitel werden die verschiedenen unterstützten Installationsvarianten des TwinCAT OPC UA Gateways beschrieben. Bitte beachten Sie, daß sich die genannten Varianten in Ihrer Komplexität fast beliebig erweitern lassen. Die genannten Beispiele stellen nur häufig vorkommende Installationsvarianten dar.

### Gateway und Server auf demselben Gerät

Bei diesem Szenario sind das TwinCAT OPC UA Gateway und der TwinCAT OPC UA Server auf demselben Gerät installiert. Das Gateway ist mit den Standardeinstellungen konfiguriert, um eine Verbindung mit dem lokalen TwinCAT OPC UA Server unter der folgenden Server-URL herzustellen: `opc.tcp://localhost:4840`.

Aus Sicht des Clients werden in diesem Fall zwei Szenarien unterstützt:

- Ein OPC UA Client greift über das Gateway auf den unterlagerten Server zu, um auf Symbole aus der TwinCAT Runtime zuzugreifen. Der Client kann sich hierbei auf demselben Gerät oder einem Gerät im Netzwerk befinden. Die Kommunikationsverbindung zwischen Client und Gateway ist hierbei OPC UA.
- Ein OPC COM DA Client greift über das Gateway auf den unterlagerten Server zu, um auf Symbole aus der TwinCAT Runtime zuzugreifen. Der Client befindet sich hierbei zwingend auf demselben Gerät. Die Kommunikationsverbindung zwischen Client und Gateway ist hierbei OPC COM DA.

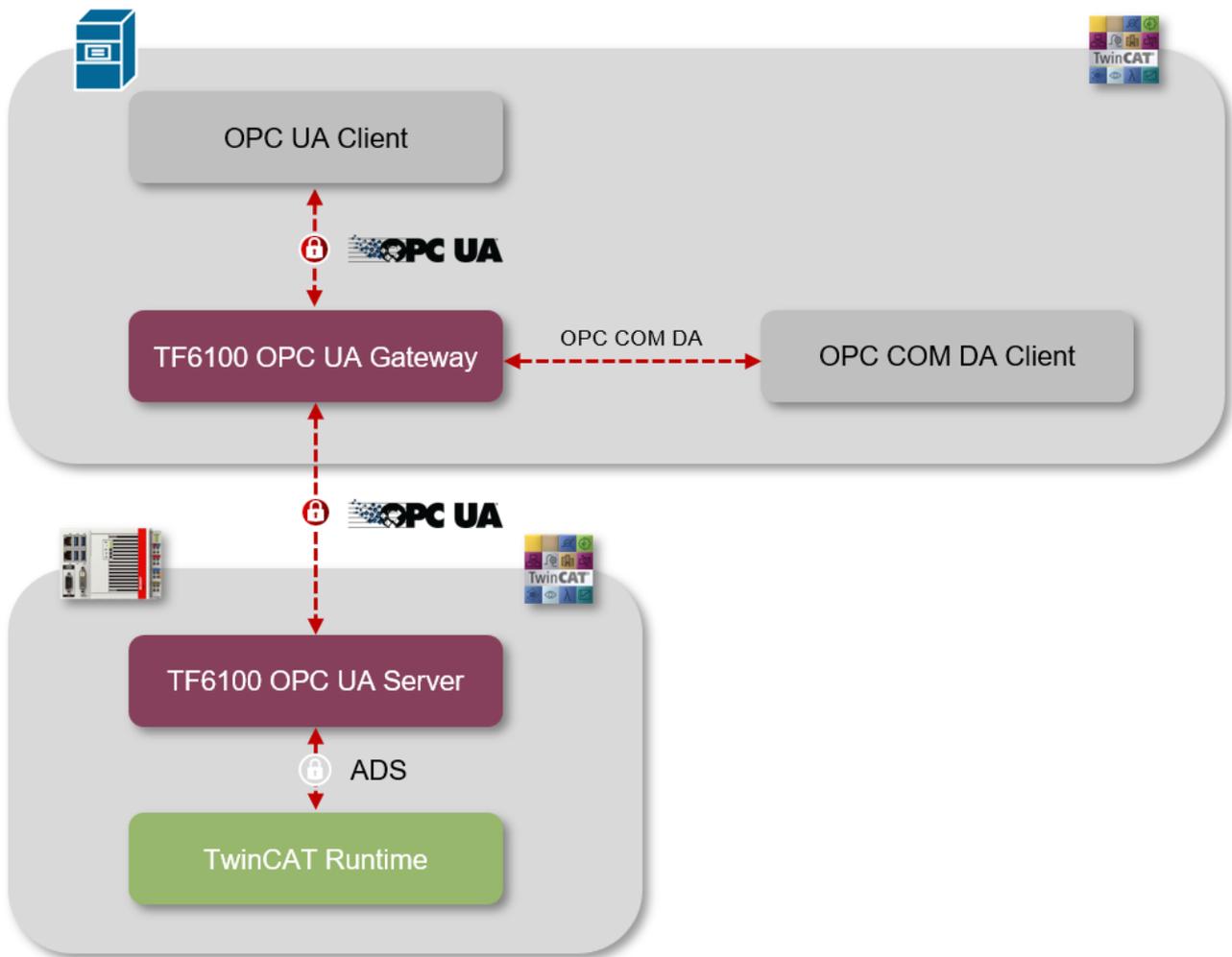


**Gateway und Server auf verschiedenen Geräten**

Bei diesem Szenario sind das TwinCAT OPC UA Gateway und der TwinCAT OPC UA Server auf verschiedenen Geräten installiert. Das Gateway ist für die Herstellung einer Verbindung mit dem remote TwinCAT OPC UA Server konfiguriert, indem dessen Server-URL, z. B. `opc.tcp://192.168.1.1:4840`, im Gateway hinterlegt wird.

Aus Sicht des Clients werden in diesem Fall zwei Szenarien unterstützt:

- Ein OPC UA Client greift über das Gateway auf den unterlagerten Server zu, um auf Symbole aus der TwinCAT Runtime zuzugreifen. Der Client kann sich hierbei auf demselben Gerät oder einem Gerät im Netzwerk befinden. Die Kommunikationsverbindung zwischen Client und Gateway ist hierbei OPC UA.
- Ein OPC COM DA Client greift über das Gateway auf den unterlagerten Server zu, um auf Symbole aus der TwinCAT Runtime zuzugreifen. Der Client befindet sich hierbei zwingend auf demselben Gerät. Die Kommunikationsverbindung zwischen Client und Gateway ist hierbei OPC COM DA.

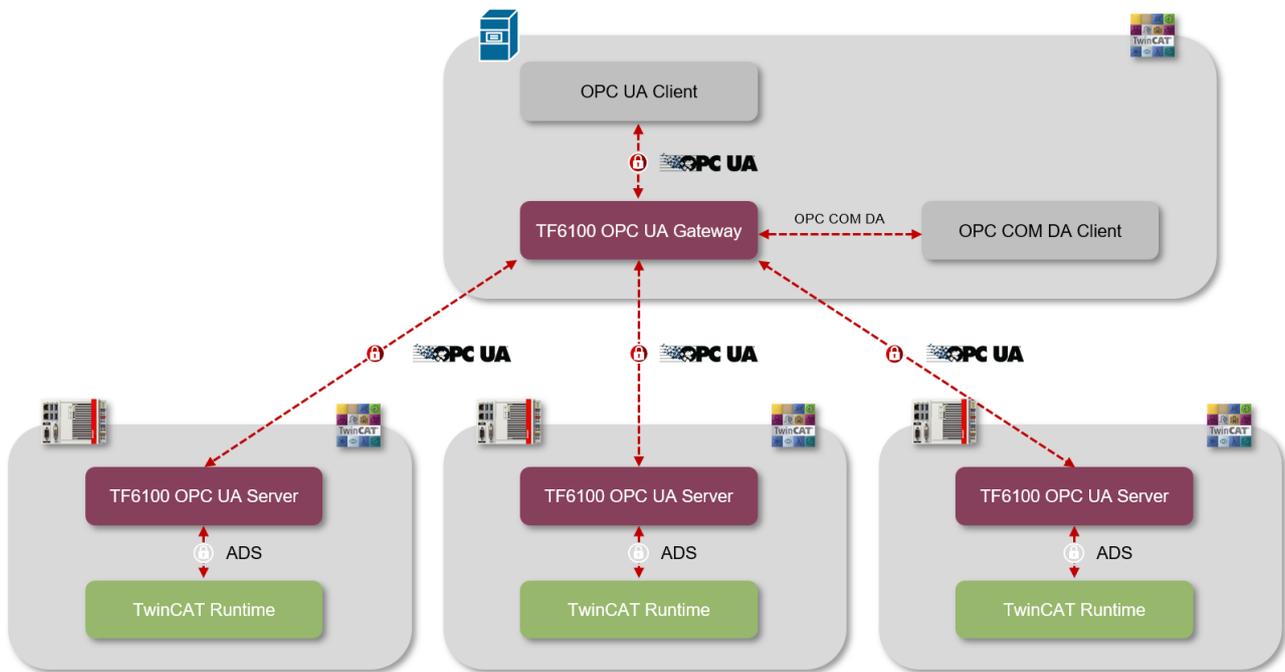


### Gateway mit mehreren Servern verbinden

Sie können das TwinCAT OPC UA Gateway auch mit mehreren unterlagerten TwinCAT OPC UA Servern verbinden. Die Server können hierbei auf demselben Gerät oder auch auf Geräten im Netzwerk installiert sein. Dieses Szenario lässt sich dabei natürlich beliebig erweitern. Das folgende Schaubild veranschaulicht ein Szenario, bei dem drei TwinCAT OPC UA Server im Netzwerk an das Gateway angeschlossen wurden.

Aus Sicht des Clients werden in diesem Fall zwei Szenarien unterstützt:

- Ein OPC UA Client greift über das Gateway auf die unterlagerten Server zu, um auf Symbole aus den einzelnen TwinCAT Runtimes zuzugreifen. Der Client kann sich hierbei auf demselben Gerät oder einem Gerät im Netzwerk befinden. Die Kommunikationsverbindung zwischen Client und Gateway ist hierbei OPC UA.
- Ein OPC COM DA Client greift über das Gateway auf die unterlagerten Server zu, um auf Symbole aus den TwinCAT Runtimes zuzugreifen. Der Client befindet sich hierbei zwingend auf demselben Gerät. Die Kommunikationsverbindung zwischen Client und Gateway ist hierbei OPC COM DA.



## 4 Technische Einführung

### 4.1 Quick Start

Das TwinCAT OPC UA Gateway steht als separates Setup zum Download zur Verfügung. Das Setup konfiguriert automatisch den Zugang zu einem TwinCAT OPC UA Server, der auf demselben Computer wie das Gateway läuft.

Wenn dem Gateway mehr als ein OPC UA Server hinzugefügt werden soll oder der Server auf einem anderen Computer läuft, müssen Änderungen an der Standardkonfiguration vorgenommen werden. Verwenden Sie den Konfigurator, um diese Einstellungen zu konfigurieren.

#### ● Konfiguration des TwinCAT OPC UA Servers

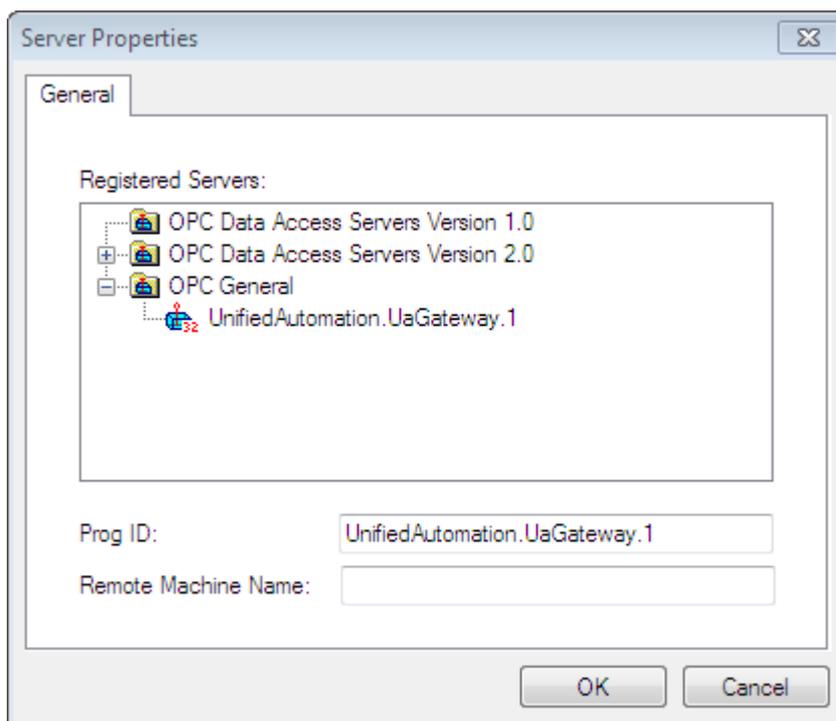
**i** Prüfen Sie die Konfiguration des OPC UA Servers und vergewissern Sie sich, dass er wie erwartet arbeitet, bevor Sie fortfahren.

Für weitere Informationen bezüglich der Konfiguration des OPC UA Servers lesen Sie den Quick Start im Kapitel „OPC UA Server“.

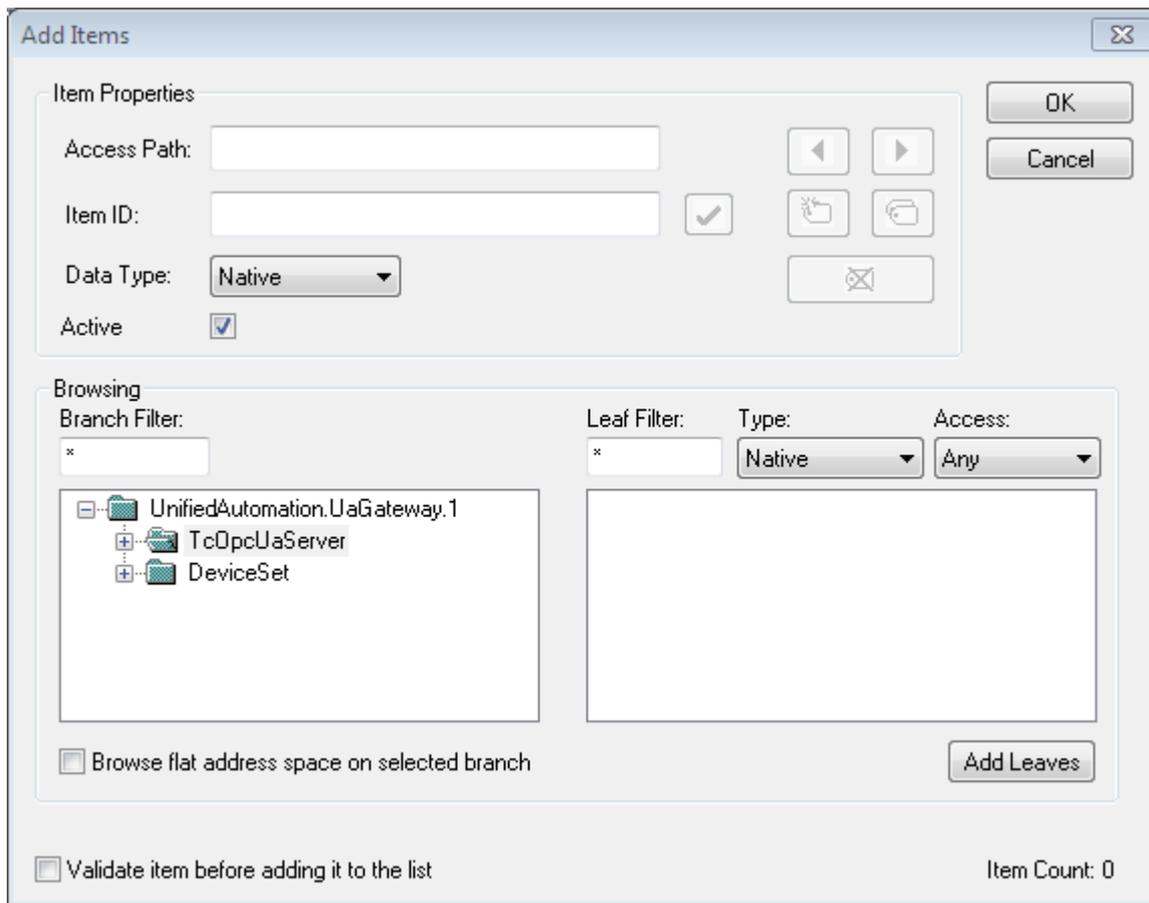
#### Schnelleinstieg OPC COM DA

Um einen OPC COM DA Client mit dem Gateway zu verbinden, starten Sie den Client und stellen Sie eine Verbindung zu der folgenden ProgId her:

UnifiedAutomation.UaGateway.1



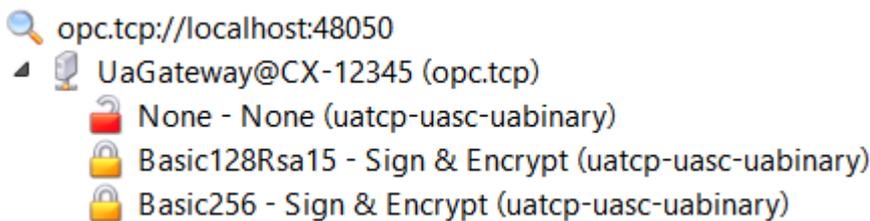
Beim Durchsuchen des Gateway werden ein oder mehrere OPC UA Server im Namensraum des Gateway sichtbar.



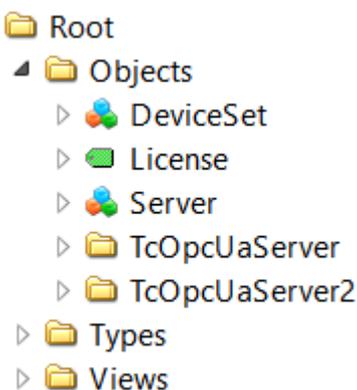
### Schnelleinstieg OPC UA

Das Gateway bietet nicht nur eine OPC-COM-DA-Schnittstelle, sondern erlaubt die Aggregation von einem oder mehreren OPC UA Servern. Hierzu öffnet das Gateway ebenfalls eine OPC-UA-Schnittstelle. Das Gateway ist über folgende OPC UA Server URL erreichbar:

`opc.tcp://[HostnameOrIpAddressOrLocalhost]:48050`



Der Namensraum des Gateway beinhaltet dann alle zugrunde liegenden TwinCAT OPC UA Server.

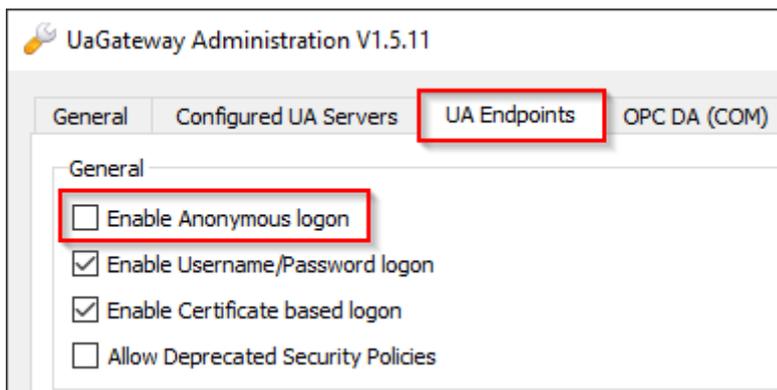


## 4.2 Empfohlene Schritte

Nach der Erstinbetriebnahme empfehlen wir die Beachtung der folgenden Punkte, um das Gateway weiter zu konfigurieren und eine stabile und sichere Betriebsumgebung zu gewährleisten.

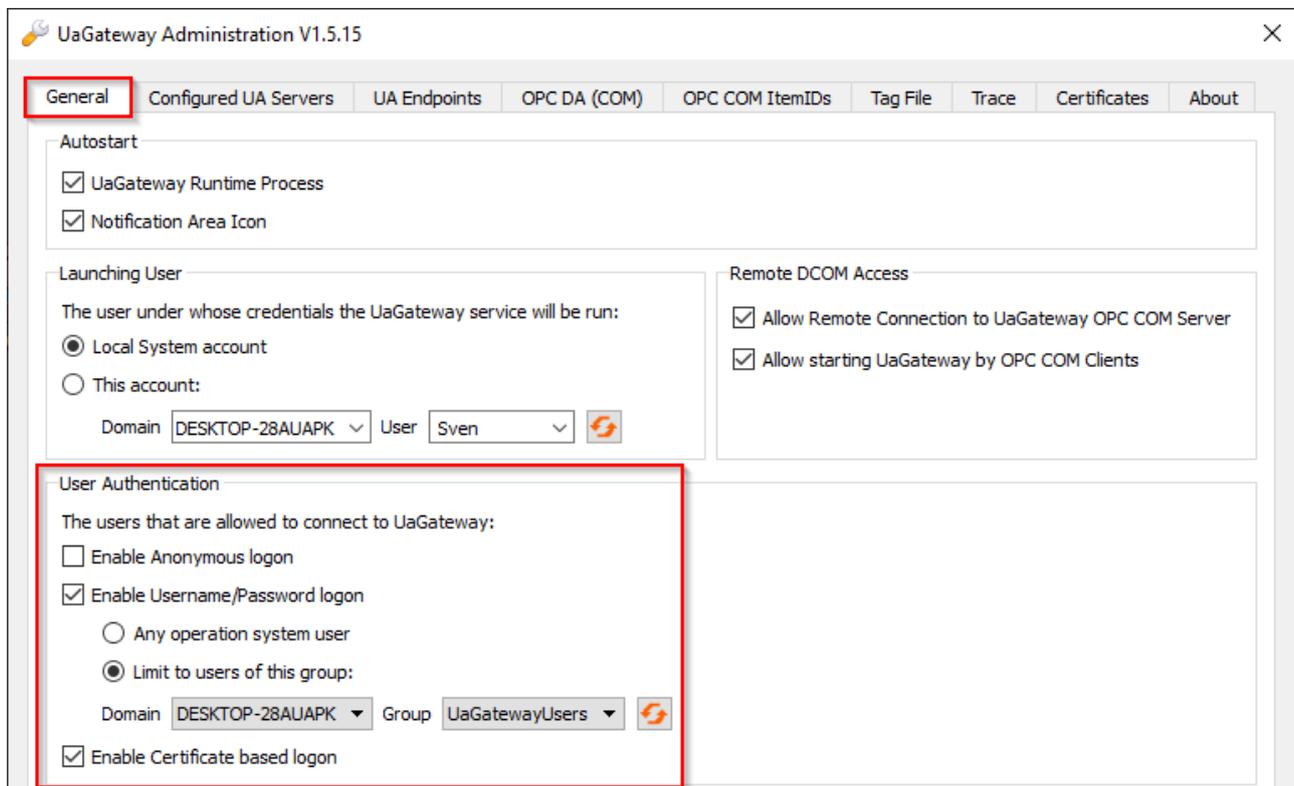
### Nur sichere IdentityToken verwenden

Das Gateway wird im Auslieferungszustand mit dem aktivierten IdentityToken „Anonymous“ konfiguriert. Wir empfehlen dieses IdentityToken zu deaktivieren, damit sich nur authentifizierte Benutzer mit der OPC UA Server Schnittstelle des Gateways verbinden können. Diese Einstellung können Sie in der [Konfiguration der Endpunkte \[► 25\]](#) vom TwinCAT OPC UA Gateway Konfigurator deaktivieren.



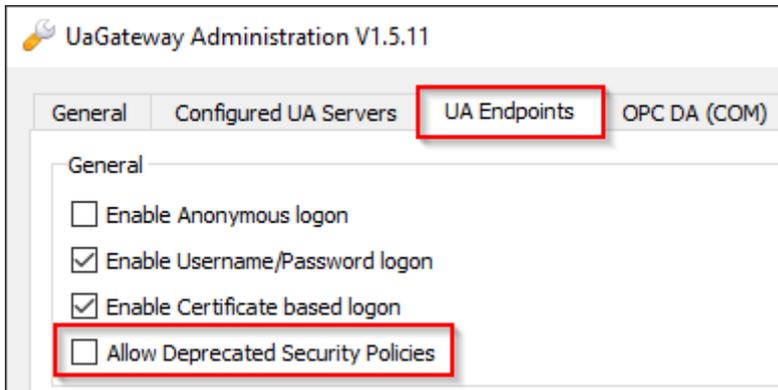
### Konfigurieren einer Benutzergruppe mit Zugriffsberechtigung

Sie sollten über den TwinCAT OPC UA Gateway Konfigurator eine Benutzergruppe definieren, welche Zugriffsberechtigung auf das Gateway bekommt. Benutzer aus dieser Benutzergruppe können dann als IdentityToken bei der Verbindung eines OPC UA Clients mit dem Gateway angegeben werden.

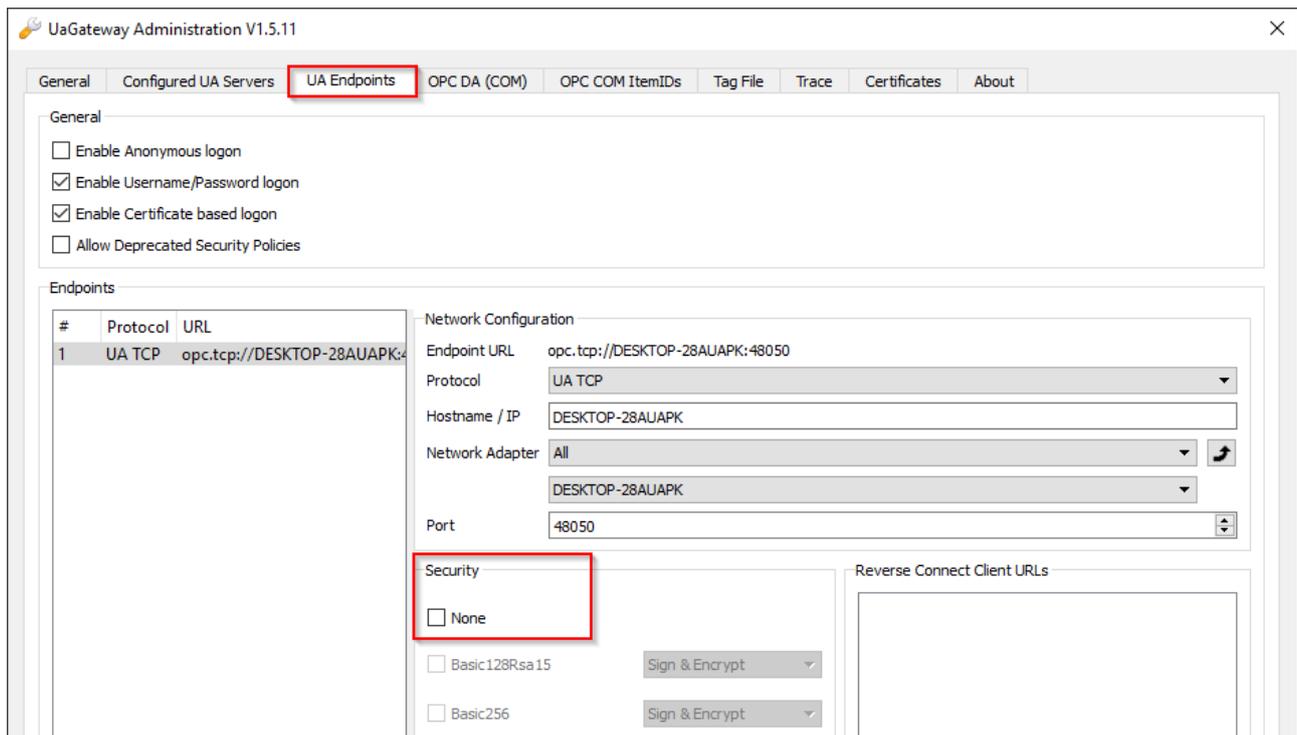


**Unsichere Endpunkte deaktiviert lassen**

Als unsicher eingestufte Endpunkte werden standardmäßig nicht vom TwinCAT OPC UA Gateway angeboten. Über einen Konfigurationsparameter bei der Konfiguration der Endpunkte [► 25] lassen sich diese im Gateway verfügbar machen – wir empfehlen dies jedoch ausdrücklich nicht und nur die Verwendung der aktuell als sicher geltenden Endpunkte.

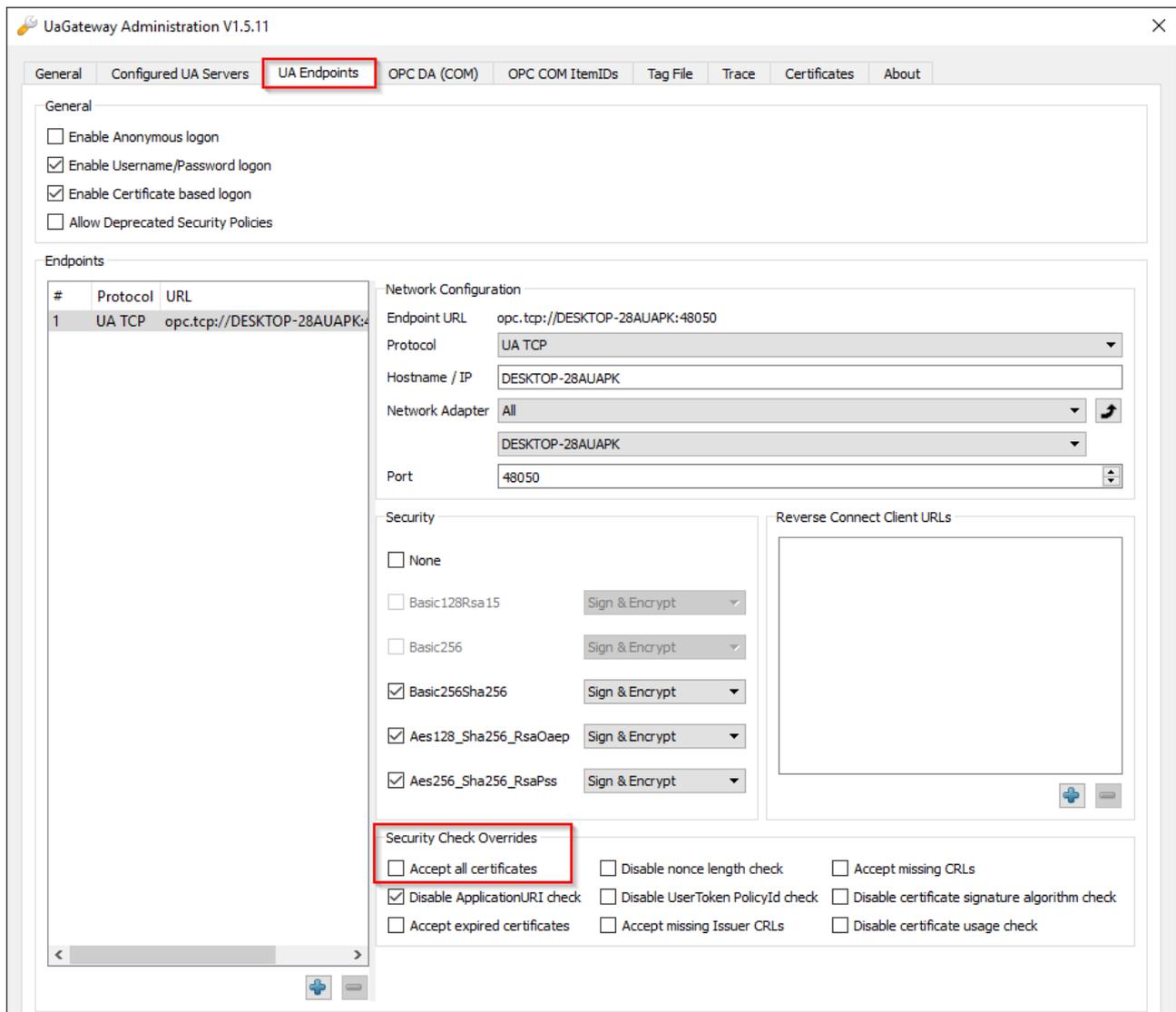


Des Weiteren ist im Auslieferungszustand des Gateway der unverschlüsselte Endpunkt („None/None“) deaktiviert und wir empfehlen diesen deaktiviert zu lassen. Muss dieser aus Kompatibilitätsgründen aktiviert werden, so kann dies ebenfalls über die Konfigurationsparameter im Konfigurator erfolgen.



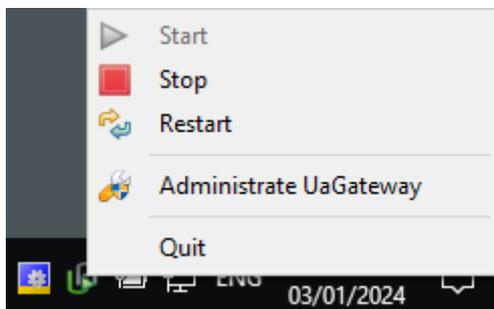
**‘Accept all certificates‘ deaktivieren**

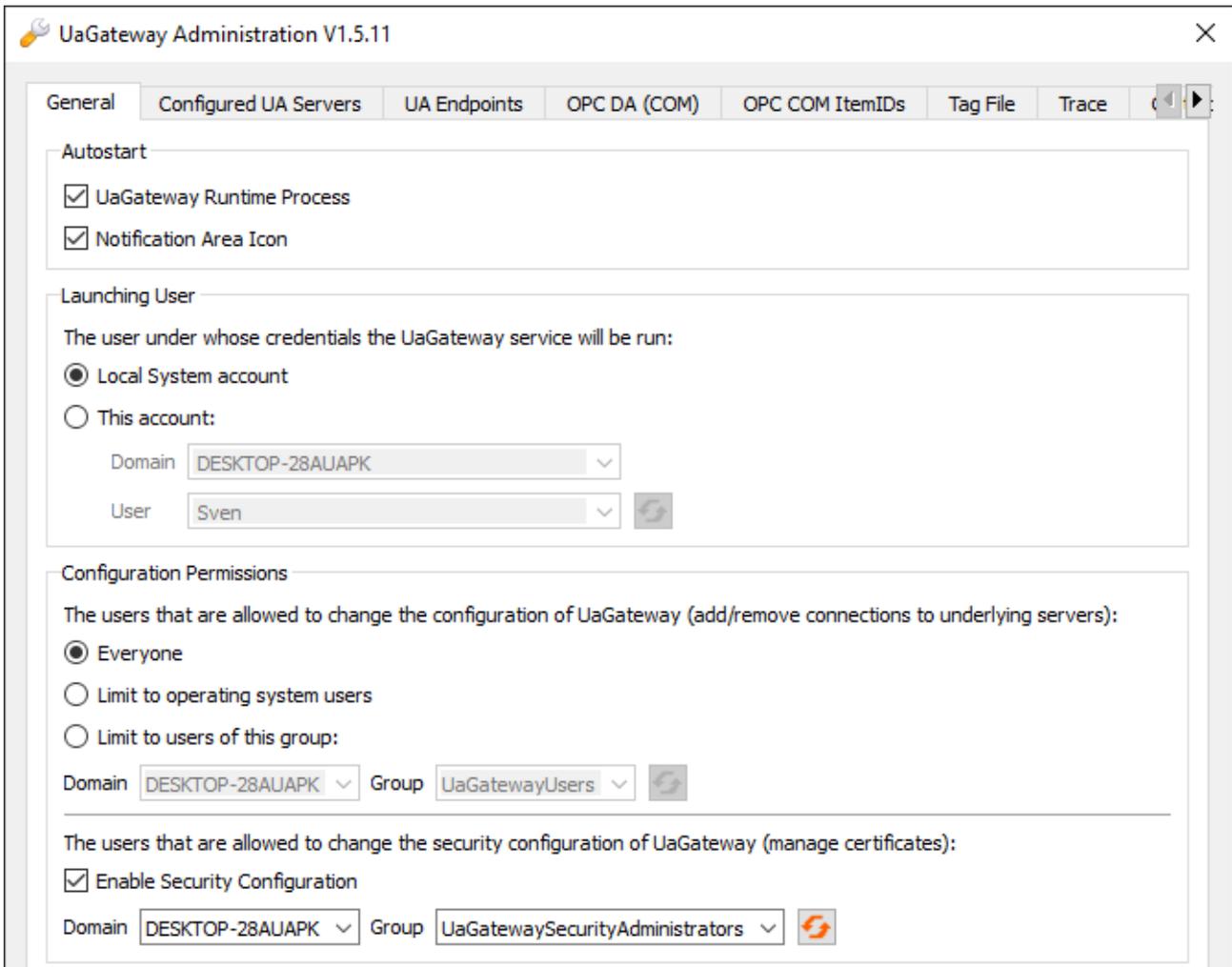
Im Auslieferungszustand wird das Gateway für die einfache Inbetriebnahme so konfiguriert, dass dieses allen Client-Zertifikaten automatisch vertraut, ohne auf Gateway-Seite einen manuellen Zertifikatsaustausch durchführen zu müssen. Aus Sicherheitsgründen empfehlen wir die Deaktivierung dieser Einstellung. Diese Einstellung kann über den TwinCAT OPC UA Gateway Konfigurator bei der Konfiguration der Endpunkte [► 25] deaktiviert werden.



### 4.3 Konfigurator

Das TwinCAT OPC UA Gateway beinhaltet eine grafische Benutzeroberfläche für die Konfiguration der Software. Diesen Konfigurator öffnen Sie über den Eintrag **Administrare UaGateway** im Kontextmenü des Gateway Symbols im Windows System Tray.





## 4.4 Applikationsverzeichnisse

Diese Applikation verwendet verschiedene Verzeichnisse, um relevante Informationen abzuspeichern, z.B. Konfigurations- oder Zertifikatsdateien.

### Installationsverzeichnis

Das Basis-Installationsverzeichnis der Applikation ist auf allen Betriebssystemen immer relativ zum TwinCAT Installationsverzeichnis.

```
%TcInstallDir%\Functions\TF6100-OPC-UA
```

Unterhalb dieses Verzeichnisses wird die Applikation dann in folgendes Verzeichnis installiert.

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway
```

### Basisverzeichnis für PKI Infrastruktur (Server)

Zertifikatsdateien, welche zum Aufbau einer gesicherten Kommunikationsverbindung mit dem OPC UA Server des Gateways verwendet werden, werden in folgendem Verzeichnis abgelegt:

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver
```

### Verzeichnis für Zertifikats-Vertrauensstellung (Server, trusted)

Clientzertifikate in diesem Verzeichnis werden als „vertrauenswürdig“ deklariert.

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\trusted\certs
```

### Verzeichnis für Zertifikats-Vertrauensstellung (Server, rejected)

Clientzertifikate in diesem Verzeichnis werden als „nicht vertrauenswürdig“ deklariert.

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\rejected
```

### Basisverzeichnis für PKI Infrastruktur (Client)

Zertifikatsdateien, welche das Gateway als OPC UA Client zum Aufbau einer gesicherten Kommunikationsverbindung mit den unterlagerten TwinCAT OPC UA Servers verwendet, werden in folgendem Verzeichnis abgelegt:

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiclient
```

### Verzeichnis für Zertifikats-Vertrauensstellung (Client, trusted)

Clientzertifikate in diesem Verzeichnis werden als „vertrauenswürdig“ deklariert.

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiclient\trusted\certs
```

### Verzeichnis für Zertifikats-Vertrauensstellung (Client, rejected)

Serverzertifikate in diesem Verzeichnis werden als „nicht vertrauenswürdig“ deklariert.

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiclient\rejected
```

### Verzeichnis für das Server- und Clientzertifikat

Die Verzeichnisse für das OPC UA Server- und Clientzertifikat des Gateways sind wie folgt festgelegt, wobei zwischen dem Verzeichnis für den Public-Key („certs“) und Private-Key („private“) unterschieden wird. Server und Client verwenden dasselbe Zertifikat.

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\own\certs  
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\own\private
```

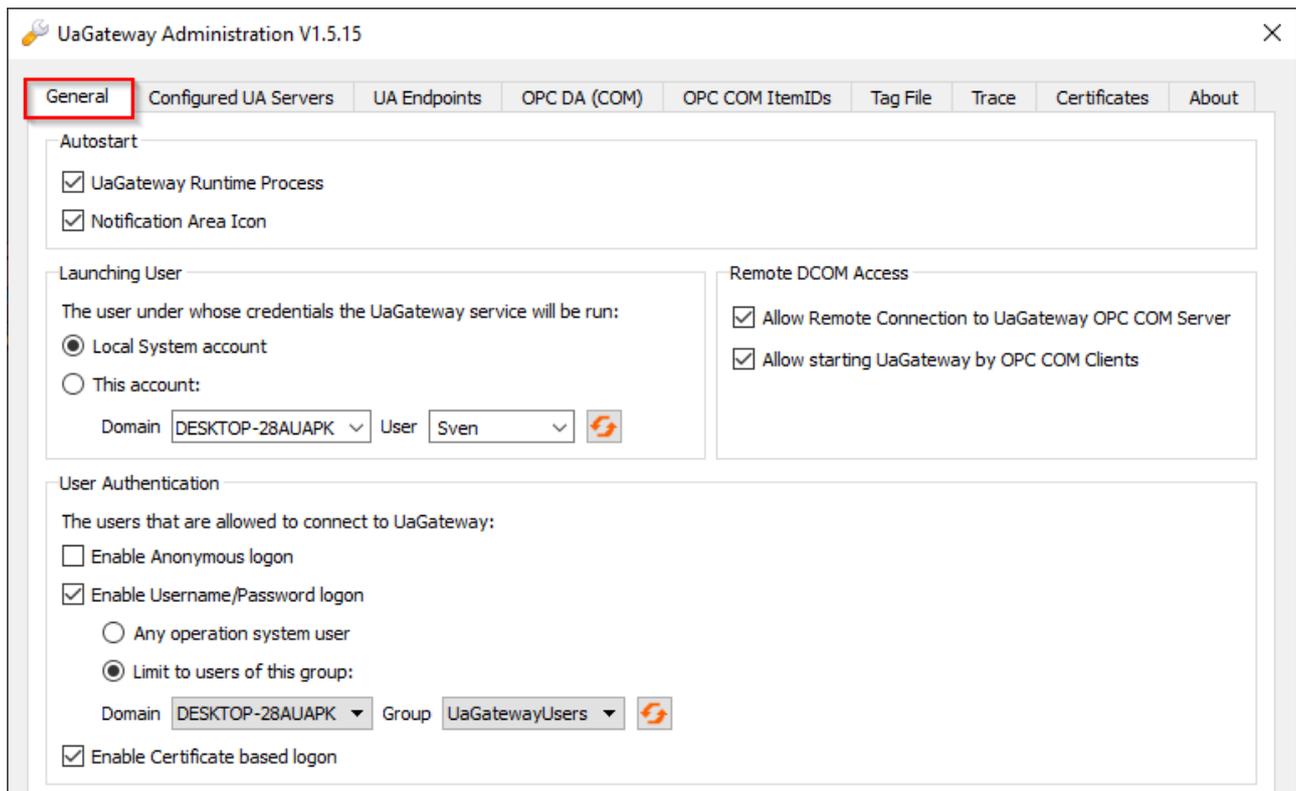
### Logdateien

Logdateien werden in dem folgenden Verzeichnis abgelegt.

```
%ProgramData%\UnifiedAutomation\TwinCAT OPC UA Gateway\Trace
```

## 4.5 Allgemeine Einstellungen

Über die Registerkarte **General** im TwinCAT OPC UA Gateway [Konfigurator](#) [► 20] lassen sich allgemeine Einstellungen des Gateways vornehmen.



Diese Einstellungen sollen im Folgenden näher beschrieben werden.

**Autostart**

In diesem Bereich können Sie das Autostart-Verhalten des TwinCAT OPC UA Gateway konfigurieren. Aktivieren Sie die Option **UaGateway Runtime Process**, um den Windows-Dienst des Gateways automatisch beim Einschalten des Computers zu starten. Aktivieren Sie die Option **Notification Area Icon**, um das Windows System Tray Icon des Gateway bei der Anmeldung eines Benutzers zu starten.

**Launching User**

Das TwinCAT OPC UA Gateway wird standardmäßig als Windows-Dienst registriert und beim Systemstart automatisch mitgestartet. Dem Windows-Dienst wird ein spezifischer Benutzerkontext zugewiesen. Der Benutzer, den Sie hier auswählen, wird dem Windows-Dienst zugeordnet. Darüber hinaus wird dem Benutzer die Berechtigung „LogOnAsService“ eingeräumt und er wird der lokalen Benutzergruppe „UaGatewayUsers“ hinzugefügt.

**User Authentication**

In diesem Bereich können Sie definieren, welche IdentityToken bei der Verbindung eines OPC UA Clients mit dem Gateway zur Verfügung stehen. Sie können hier auch eine Benutzergruppe definieren, welche Zugriffsberechtigung auf das Gateway bekommen soll. Benutzer aus dieser Benutzergruppe können dann von einem OPC UA Client beim Verbindungsaufbau verwendet werden.

**Configuration Permissions**

Es besteht die Möglichkeit, nur bestimmten Benutzern zu erlauben, die Konfiguration des Gateways zu verändern, sprich Verbindungen zu unterlagerten Servern hinzuzufügen oder zu entfernen. Sie können aus den folgenden Einstellungen auswählen:

Everyone	Jeder (auch anonym über OPC UA angemeldete Benutzer), der mit dem Gateway in Verbindung treten kann, kann die Konfiguration verändern.
Limit to operating system users	Nur lokale Benutzer und Benutzer aus derselben Domain können die Konfiguration ändern.
Limit to users of this group	Die Berechtigung die Konfiguration zu ändern steht nur Benutzern einer bestimmten Gruppe zu.

## UA Discovery Registration

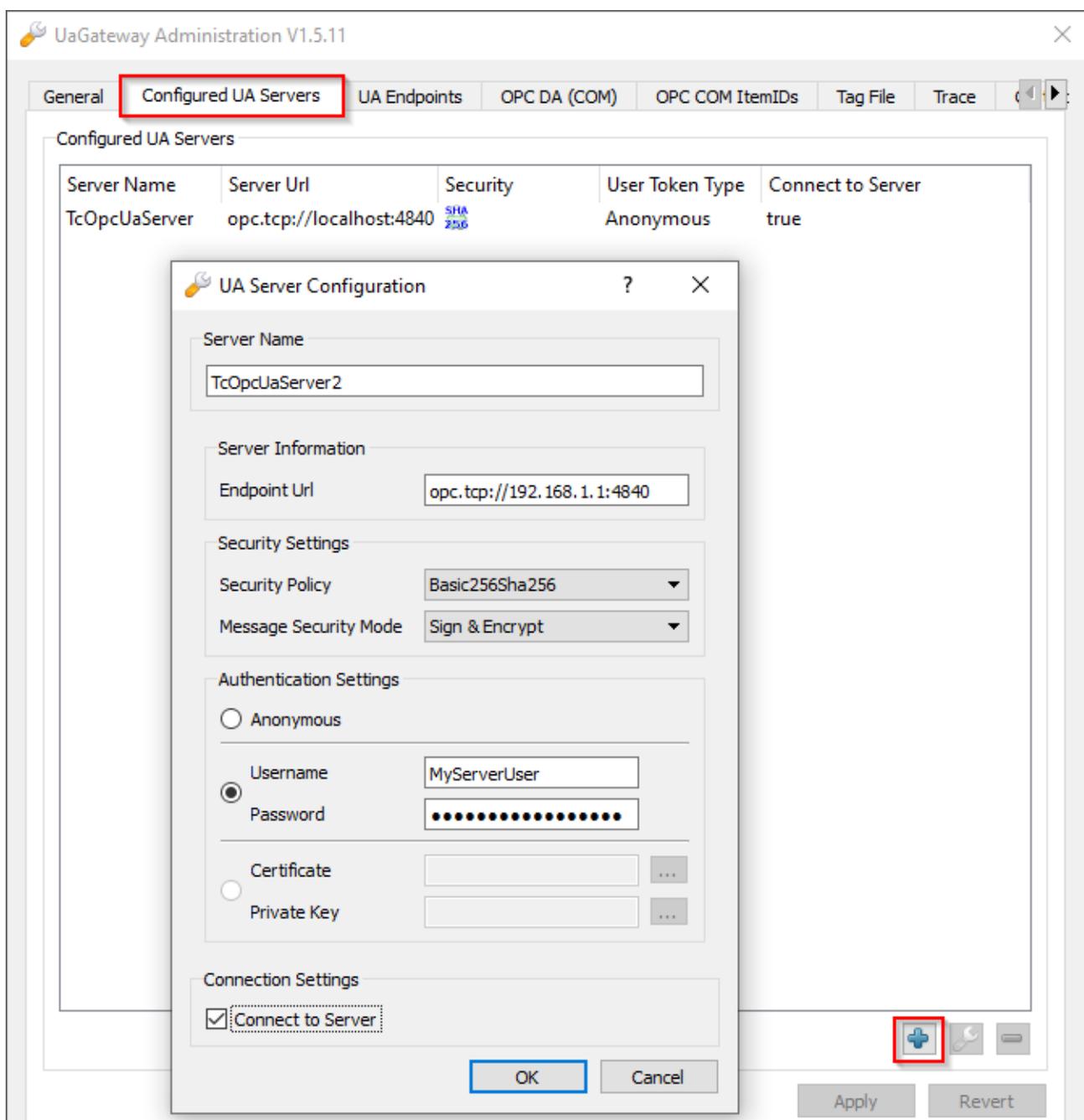
Aktivieren Sie die Option **Register at Local Discovery Server**, wenn das Gateway beim lokalen Local Discovery Server (LDS) registriert werden soll.

### **i** Remote DCOM Access

Abhängig von der verwendeten Version des TwinCAT OPC UA Gateway, wird Ihnen ggf. noch die Konfigurationsoption **Remote DCOM Access** angezeigt. Diese Konfigurationsparameter werden nicht vom Gateway unterstützt und können ignoriert werden. Siehe auch [Systemvoraussetzungen](#) [▶ 10].

## 4.6 Konfiguration von zusätzlichen Servern

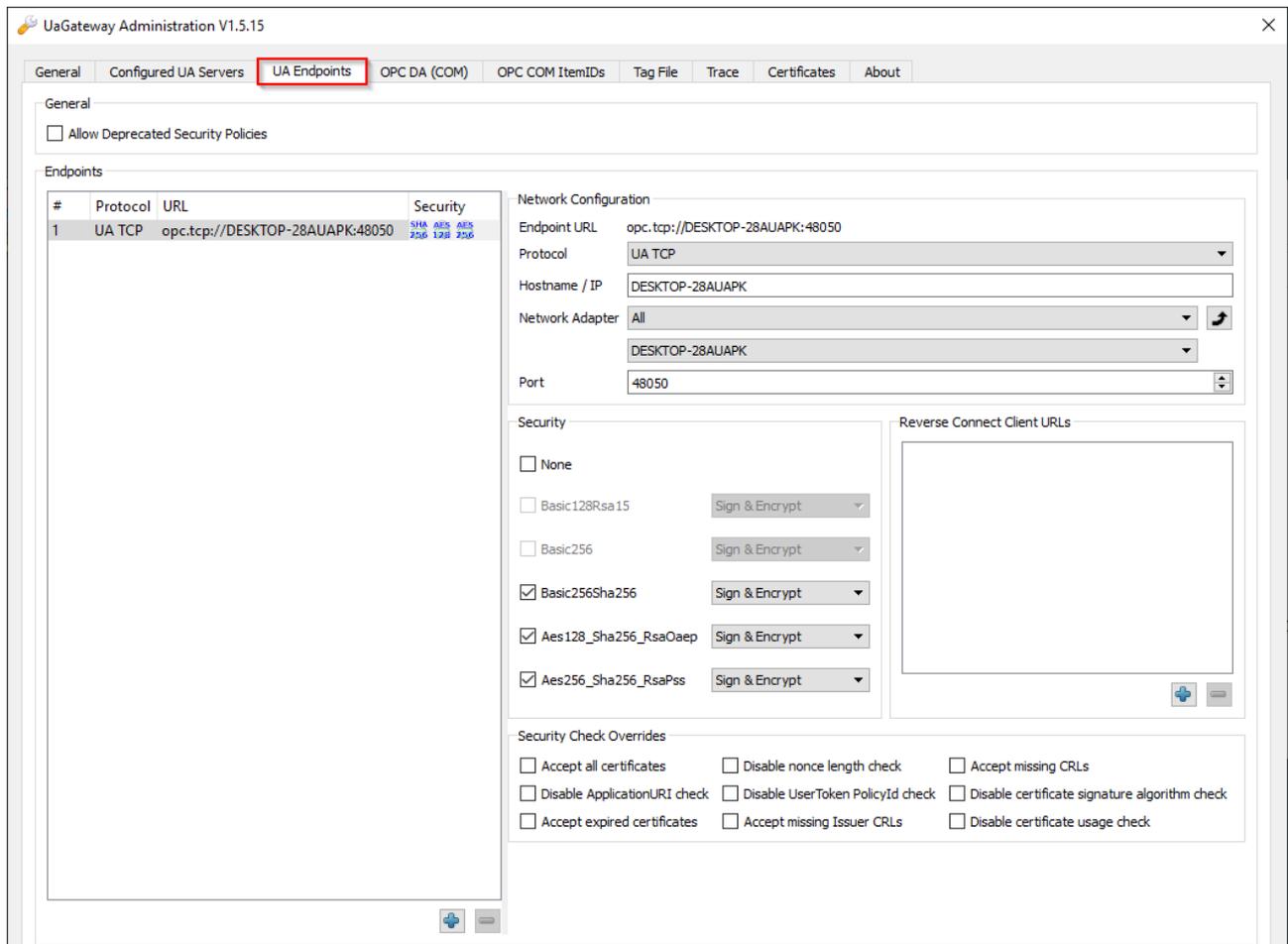
Über die Registerkarte **Configured UA Servers** im TwinCAT OPC UA Gateway [Konfigurator](#) [▶ 20] können Sie weitere unterlagerte TwinCAT OPC UA Server zum Gateway hinzufügen. Im Auslieferungszustand stellt das Gateway bereits eine Verbindung zu einem TwinCAT OPC UA Server her, der auf demselben System installiert wurde.



Um weitere TwinCAT OPC UA Server zu konfigurieren, oder aus der Konfiguration zu entfernen, klicken Sie auf den Plus- oder Minus-Button und anschließend auf **Apply**, um die Änderungen zu speichern.

## 4.7 Konfiguration der Endpunkte

Über die Registerkarte **UA Endpoints** im TwinCAT OPC UA Gateway Konfigurator [► 20] können Sie Einstellungen zur OPC UA Endpunktkonfiguration vornehmen. Der OPC UA Endpunkt (Endpoint) ist die Verbindungsinformation, die ein OPC UA Client benötigt, um eine Verbindung mit dem Gateway herzustellen.



Die in dieser Registerkarte verfügbaren Konfigurationsoptionen sollen im Folgenden näher beschrieben werden.

### General

In diesem Bereich können Sie den Konfigurationsschalter **Allow deprecated security policies** aktivieren, um veraltete und potenziell als unsicher geltende Security Policies im Gateway zu aktivieren. Wir empfehlen diese Option jedoch deaktiviert zu lassen und nur im Falle von Kompatibilitätsproblemen mit alten OPC UA Clients zu aktivieren. In diesem Fall wäre jedoch die richtige Vorgehensweise den Clienthersteller nach einem Update zu fragen.

### Endpoints

An dieser Stelle können Sie alle notwendigen Einstellungen für die verschiedenen OPC UA Endpunkte festlegen, neue Endpunkte anlegen oder auch entfernen. Im Auslieferungszustand ist bereits ein vordefinierter Endpunkt verfügbar, welcher im Normalfall für alle Anwendungsfälle ausreichend sein sollte. Dieser Endpunkt definiert die verfügbaren SecurityPolicies, sowie Einstellungen zur Netzwerkkonfiguration, Port, Reverse Connect Client URLs und auch etwaigen Security Check Overrides.

Diese Konfigurationselemente werden in den folgenden Abschnitten näher beschrieben.

## Network Configuration

In diesem Bereich können Sie definieren, für welche Netzwerkschnittstelle der Endpunkt konfiguriert werden soll. Der Endpunkt, der im Auslieferungszustand des Gateways definiert wird, ist automatisch für alle Netzwerkschnittstellen konfiguriert. D.h. dass das Gateway über alle im Betriebssystem installierten und konfigurierten Netzwerkschnittstellen erreichbar ist. Die folgenden Konfigurationsparameter können hier definiert werden:

Konfigurationsparameter	Beschreibung
Endpoint URL	Endpoint URL des Gateways, so wie sie im OPC UA Client beim GetEndpoint Aufruf zu sehen ist.
Protocol	Zu verwendendes Protokoll. Es wird nur das Protokoll „UA TCP“ unterstützt.
Hostname / IP	Hostname oder IP-Adresse des Geräts, auf dem das Gateway installiert wurde.
Network Adapter	Auswahl des Netzwerkadapters, unter welchem das Gateway für OPC UA Clients erreichbar sein soll.
Port	Netzwerk-Port (TCP), unter welchem das Gateway für OPC UA Clients erreichbar sein soll.

## Security

In diesem Bereich können Sie die unterstützten Security Policies des Endpunkts konfigurieren. Aktivieren Sie die Kontrollkästchen vor der jeweiligen Security Policy, um diese für den Endpunkt zu konfigurieren. Neben der Security Policy befindet sich dann ein Auswahlelement für den im Endpunkt geltenden Message Security Mode.

## Reverse Connect Client URLs

In diesem Bereich können Sie Endpunkt URLs von Clients eintragen, welche für die Reverse Connect Funktionalität verwendet werden sollen.

## Security Check Overrides

In diesem Bereich können Sie Ausnahmeregeln bei der Validierung von verschiedenen Security-Optionen konfigurieren.

## 4.8 Migration von TF6120

Einer der vorrangigen Zwecke des UA Gateway ist die Bereitstellung einer zukunftsfähigen Konnektivität, um das Supplement / die Function Tx6120 OPC DA zu ersetzen. Wenn Sie Tx6120 OPC DA nach UA Gateway migrieren möchten, beachten Sie die nachfolgenden Hinweise.

### Standardkonfiguration

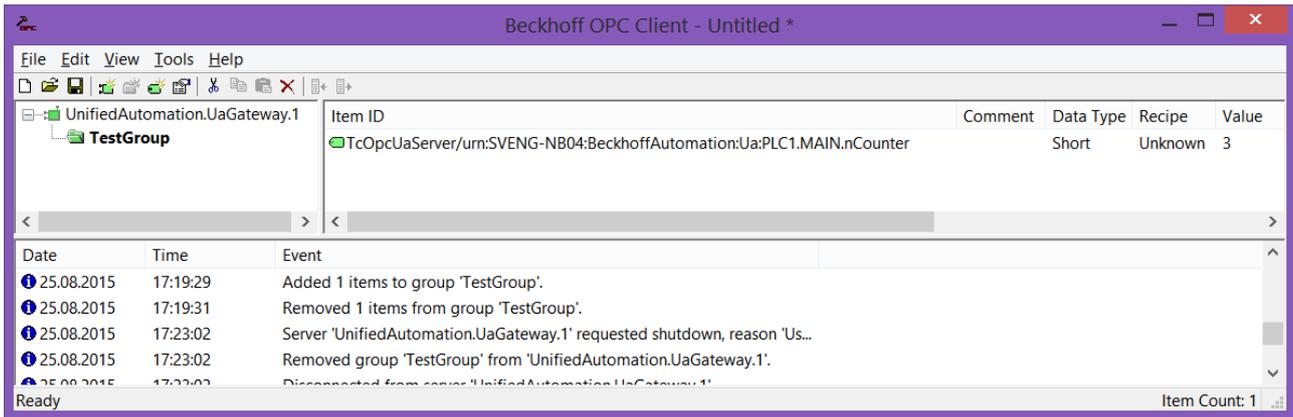
Die Standardkonfiguration des UA Gateway stellt automatisch eine Verbindung mit dem lokalen OPC UA Server her und bietet den OPC DA Clients eine OPC-DA-Schnittstelle. Bei einer Verbindung auf der Grundlage dieser Standardkonfiguration müssen die OPC-DA-Clients Folgendes berücksichtigen:

- Die standardmäßige ProgID des UA Gateway lautet „UnifiedAutomation.Gateway.1“. Der TwinCAT OPC DA Server verwendet eine andere ProgID („Beckhoff.TwinCATOpcServerDA“).
- Das UA Gateway verwendet stets eine ProgID anstelle von mehreren Klonen.
- Der ItemIdentifier eines OPC-Symbols wird im UA Gateway anders erzeugt als beim TwinCAT OPC DA Server. Dieses Verhalten kann geändert werden, damit es dem des OPC DA Servers ähnlicher ist.

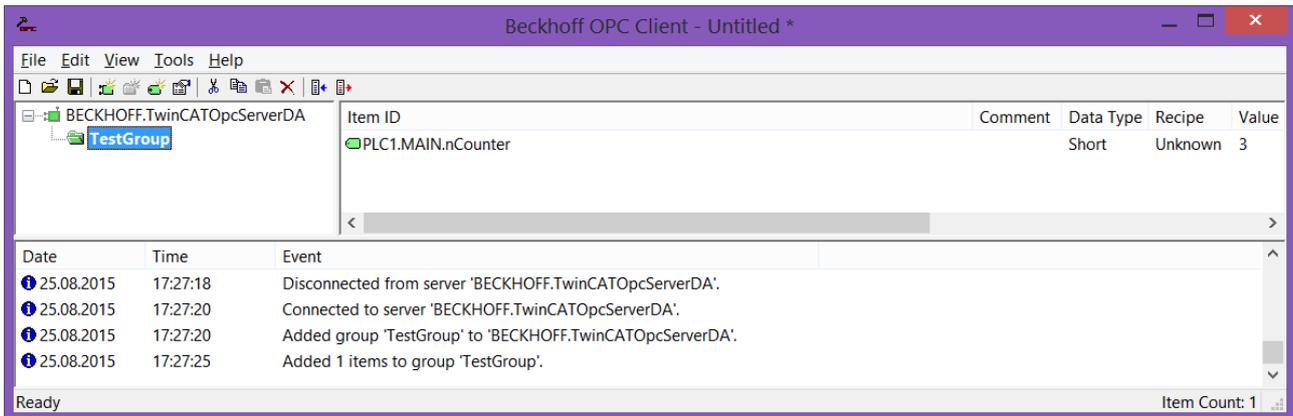
### Syntax eines ItemIdentifiers verändern

Die Syntax, die das UA Gateway für ItemIdentifier verwendet, kann verändert werden, damit letztere eher der Art des TwinCAT OPC DA Servers entspricht. Standardmäßig verwendet das UA Gateway bei der Bildung seiner Identifier eine andere Syntax als der TwinCAT OPC DA Server.

Beispiel UA Gateway:



Beispiel TwinCAT OPC DA Server:



Das UA Gateway verwendet ein Präfix, sodass der zugrunde liegende OPC UA Client, von dem die Variable stammt, eindeutig identifiziert werden kann.

Um das UA Gateway so zu konfigurieren, dass es seine Identifier in etwa so bildet, wie der TwinCAT OPC DA Server, sind die nachfolgenden Schritte erforderlich. Die Funktionalität wurde implementiert, um den Migrationsprozess zu vereinfachen.

1. Öffnen Sie die UA-Gateway-Konfigurationsdatei  
*C:\Program Files (x86)\UnifiedAutomation\UaGateway\bin\uagateway.config.xml*
2. Suchen Sie nach den folgenden XML-Tags in der XML-Datei:

```
<OpcServerConfig>
  <ComDaServerConfig>
    <ComDaNamespaceUseAlias>>false</ComDaNamespaceUseAlias>
  </ComDaServerConfig>
</OpcServerConfig>
```

3. Wenn das XML-Tag ComDaNamespaceUseAlias auf „true“ gesetzt wird, können benutzerdefinierte Präfixes bestimmt werden. Suchen Sie hierfür nach dem folgenden XML-Tag in derselben XML-Datei:

```
<OpcServerConfig>
  <UaServerConfig>
    <ConfiguredNamespaces>
      ...
    </ConfiguredNamespaces>
  </UaServerConfig>
</OpcServerConfig>
```

4. Identifizieren Sie in dieser XML-Struktur den TwinCAT-OPC-UA-Server-Namensraum. Standardmäßig sollte dieser folgendermaßen lauten:

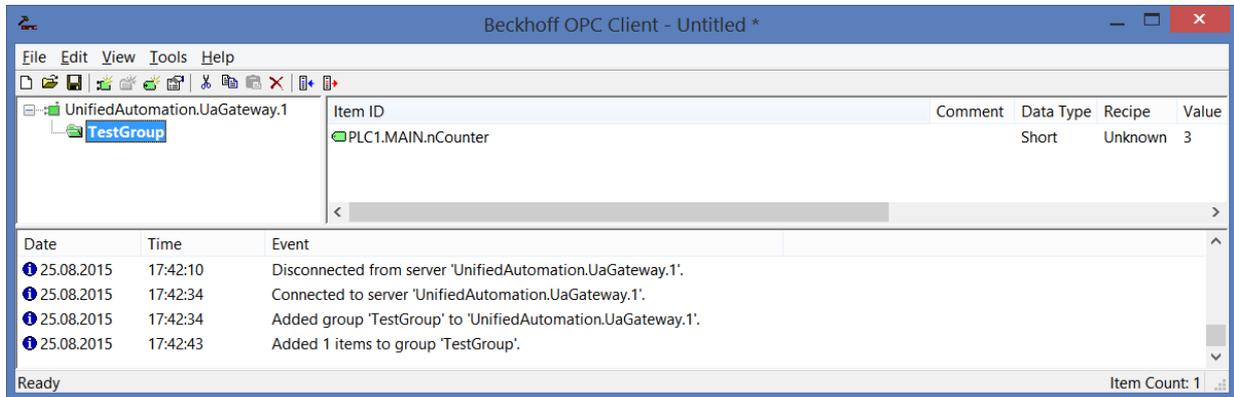
```
<OpcServerConfig>
  <UaServerConfig>
    <ConfiguredNamespaces>
      ...
    <Namespace>
      <Index>...</Index>
      <Uri>TcOpcUaServer/urn:Hostname:BeckhoffAutomation:Ua:PLC1</Uri>
      <AllowRenameUri>>false</AllowRenameUri>
    </Namespace>
  </UaServerConfig>
</OpcServerConfig>
```

```

<UniqueId>TcOpcUaServer#TcOpcUaServer/urn:Hostname:BeckhoffAutomation:Ua:PLC1</UniqueId>
<ComAlias>...</ComAlias>
</Namespace>
...
</ConfiguredNamespaces
</UaServerConfig>
</OpcServerConfig>

```

5. Auf Ihrem Computer kann der Platzhalter „...“ anders aussehen. Setzen Sie <ComAlias> auf das von Ihnen bevorzugte Präfix, zum Beispiel „PLC1“. Daraufhin werden die Bezeichner mit dem Präfix „PLC1“ gebildet.



## 4.9 Security

### 4.9.1 Übersicht

Einer der Gründe für den Erfolg von OPC UA als Kommunikationstechnologie sind unter Anderem auch die integrierten Sicherheitsmechanismen. Eine auf OPC UA basierte Datenkommunikation lässt sich dabei auf zwei Ebenen absichern: auf Transport- und Applikationsebene. Beim Verbindungsaufbau mit dem Server wählt der Client zunächst einen sogenannten Endpunkt aus, welcher unter Anderem die zu verwendenden Sicherheitsfunktionen angibt.

#### Endpunkte

Ein Server bietet dem Client eine Liste mit verschiedenen [Endpunkten](#) [► 29] an mit denen sich der Client verbinden kann. Ein Endpunkt beschreibt hierbei unter Anderem welche Sicherheitsfunktionen (z. B. Message Security Mode, Security Policy und zur Verfügung stehende Identity Token) die Kommunikationsverbindung über diesen Endpunkt erfüllen soll. So kann ein Endpunkt z. B. eine Signierung und Verschlüsselung der Datenpakete erfordern (Transportebene), sowie eine zusätzliche Authentifizierung des Clients auf Basis von Benutzername/Password (Applikationsebene).

#### Transportebene

Eine auf OPC UA basierte Kommunikationsverbindung kann auf Transportebene abgesichert werden. Dies geschieht durch die Verwendung von Client/Server-Zertifikaten und eine gegenseitige Vertrauensstellung zwischen Client- und Server-Applikation. Hierbei muss der Client dem Server-Zertifikat vertrauen und umgekehrt, damit eine Kommunikationsverbindung hergestellt werden kann. Hierfür ist ein gegenseitiger [Zertifikatsaustausch](#) [► 30] notwendig.

#### Applikationsebene

Zusätzlich zur Transportebene lässt sich eine Kommunikationsverbindung auch auf Applikationsebene absichern. Hierfür stehen verschiedene [Authentifizierungsmechanismen](#) [► 31] zur Verfügung, die vom Server-Endpunkt angeboten werden.

## 4.9.2 Endpunkte

Das TwinCAT OPC UA Gateway stellt verschiedene Endpunkte über den Standard-Port 48050/tcp für OPC UA Clients zur Verfügung. Die Endpunkte definieren hierbei die Art der Verbindung zwischen Client und Server und ob diese gesichert oder ungesichert erfolgen soll.

**● Vertrauensverhältnis**  
**i** Bitte beachten Sie, dass zur Verwendung der sicheren Endpunkte ein Vertrauensverhältnis zwischen Server und Client hergestellt werden muss, was üblicherweise über deren Zertifikate erfolgt. Wie Sie ein solches Vertrauensverhältnis auf Seite des Gateways konfigurieren können, erfahren Sie [hier \[▶ 30\]](#).

**● Deprecated Endpunkte**  
**i** Bitte beachten Sie, dass die aktuell in den Endpunkten zur Verfügung stehenden Security-Profile im Laufe der Zeit gegebenenfalls als potenziell unsicher eingestuft werden könnten und durch neuere ersetzt werden. In diesem Fall ist ein Update des TwinCAT OPC UA Gateways empfehlenswert. Über einen Konfigurationsschalter lassen sich veraltete und als unsicher eingestufte Security Policies wieder aktivieren. Wir empfehlen jedoch aus Sicherheitsgründen diesen Konfigurationsschalter deaktiviert zu lassen.

### Liste der Endpunkte

Die folgende Liste fasst die Endpunkte des TwinCAT OPC UA Gateway zusammen. Dabei sind auch bereits abgekündigte Endpunkte enthalten. Im Auslieferungszustand bietet das TwinCAT OPC UA Gateway nur aktuell als sicher geltende Endpunkte an.

Security-Profil	Security-Modus	Kurzbeschreibung
None	None	Bei diesem Endpunkt wird keinerlei Verschlüsselung oder Signierung der Nachrichten durchgeführt. Eine <a href="#">Authentifizierung [▶ 31]</a> hingegen ist möglich.
Basic128Rsa15 (veraltet)	Sign / Sign & Encrypt	Dieser Endpunkt ist aus Security-Sicht als veraltet eingestuft worden und ist standardmäßig deaktiviert. Bei Bedarf kann der Endpunkt wieder freigeschaltet werden.
Basic256 (veraltet)	Sign / Sign & Encrypt	Dieser Endpunkt ist aus Security-Sicht als veraltet eingestuft worden und ist standardmäßig deaktiviert. Bei Bedarf kann der Endpunkt wieder freigeschaltet werden.
Basic256Sha256	Sign / Sign & Encrypt	Aktuell im Server vorhandener Endpunkt für sichere Signierung und Verschlüsselung. Eine zusätzliche <a href="#">Authentifizierung [▶ 31]</a> ist möglich.
Aes256_Sha256_RsaPss	Sign / Sign & Encrypt	Aktuell im Server vorhandener Endpunkt für sichere Signierung und Verschlüsselung. Eine zusätzliche <a href="#">Authentifizierung [▶ 31]</a> ist möglich.
Aes256_Sha256_RsaOaep	Sign / Sign & Encrypt	Aktuell im Server vorhandener Endpunkt für sichere Signierung und Verschlüsselung. Eine zusätzliche <a href="#">Authentifizierung [▶ 31]</a> ist möglich.

Alle in der Liste aufgeführten Endpunkte können über die Konfiguration des Gateways aktiviert oder deaktiviert werden. In der folgenden Abbildung sind alle Endpunkte aktiviert.

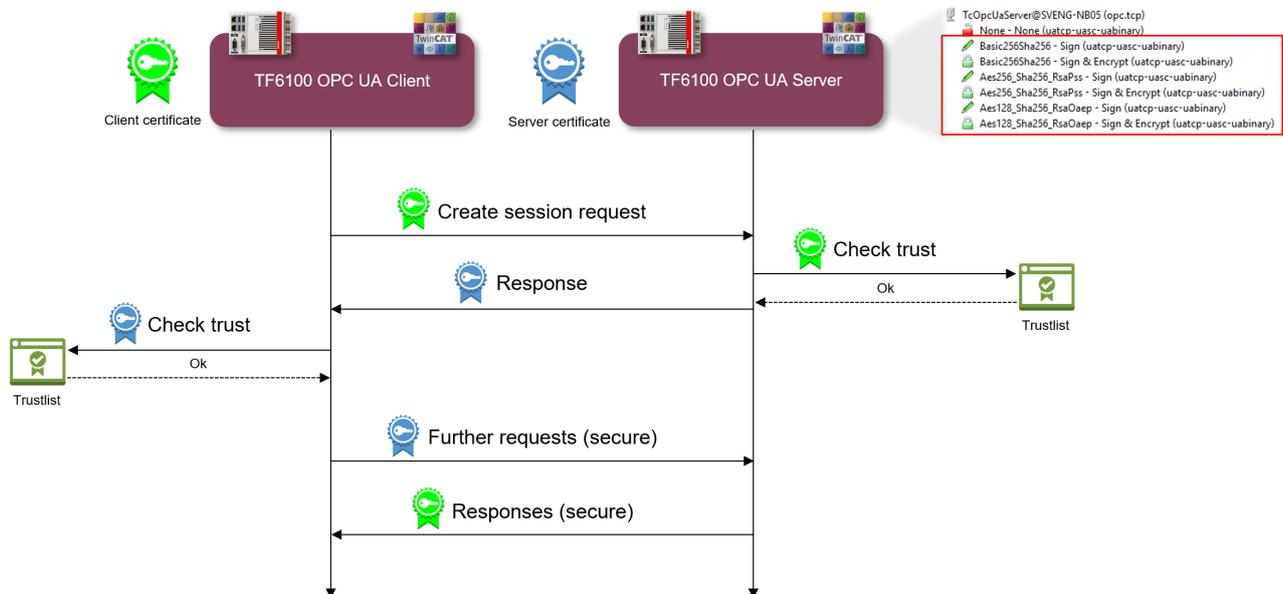
-  None - None (uatcp-uasc-uabinary)
-  Basic128Rsa15 - Sign (uatcp-uasc-uabinary)
-  Basic128Rsa15 - Sign & Encrypt (uatcp-uasc-uabinary)
-  Basic256 - Sign (uatcp-uasc-uabinary)
-  Basic256 - Sign & Encrypt (uatcp-uasc-uabinary)
-  Basic256Sha256 - Sign (uatcp-uasc-uabinary)
-  Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary)
-  Aes256\_Sha256\_RsaPss - Sign (uatcp-uasc-uabinary)
-  Aes256\_Sha256\_RsaPss - Sign & Encrypt (uatcp-uasc-uabinary)
-  Aes128\_Sha256\_RsaOaep - Sign (uatcp-uasc-uabinary)
-  Aes128\_Sha256\_RsaOaep - Sign & Encrypt (uatcp-uasc-uabinary)

### 4.9.3 Zertifikatsaustausch

Für eine Absicherung der Kommunikationsverbindung auf Transportebene über einen sicheren Endpunkt [► 29] ist die Herstellung einer gegenseitigen Vertrauensstellung zwischen Client und Server notwendig. Standardmäßig generiert hierzu das TwinCAT OPC UA Gateway beim ersten Start ein maschinenspezifisches, selbstsigniertes Schlüsselpaar bestehend aus einem Public- und einem Private-Key. Sie können jedoch zur Integration in Ihre IT-Infrastruktur auch eine beliebige Zertifizierungsstelle bzw. -technologie verwenden, z.B. Active Directory oder OpenSSL. Für die einfache Verwaltung, sowie den sicheren Zugriff auf Zertifikate, ist die Einrichtung eines Global Discovery Server sinnvoll.

Zur Einrichtung einer Vertrauensstellung zwischen einem OPC UA Client und dem TwinCAT OPC UA Gateway, benötigen Sie den öffentlichen Schlüssel des Client-Zertifikats. Das Gateway muss diesem als Server entsprechend vertrauen. Das Gateway verwaltet die Vertrauenseinstellungen für Client-Zertifikate in einem Unterverzeichnis des Applikationsverzeichnis.

Das folgende Schaubild verdeutlicht einmal den Zusammenhang von Client- und Server-Zertifikat beim Aufbau einer sicheren Kommunikationsverbindung am Beispiel von TwinCAT OPC UA Client und TwinCAT OPC UA Server. Im Falle von letzterem lässt sich dies jedoch 1:1 auch auf das Gateway übertragen.



Beim CreateSession Request übermittelt der Client seinen Public Key. Der Server hat daraufhin die Möglichkeit, die Vertrauensstellung zu überprüfen. Vertraut der Server dem Client, so übermittelt er in seiner Response seinen eigenen Public Key. Der Client hat somit ebenfalls die Möglichkeit die Vertrauensstellung mit dem Server zu überprüfen.

Ist die beiderseitige Vertrauensstellung gewährleistet, so wird die Kommunikationsverbindung initiiert. Für die Verschlüsselung eines Requests vom Client an den Server wird dann der Public Key des Servers verwendet. Die Response vom Server an den Client wird dann mit dem Public Key des Clients verschlüsselt. Beide Kommunikationsteilnehmer haben dann die Möglichkeit, die jeweils empfangene Nachricht mit ihrem Private-Key zu entschlüsseln.

Das Signieren von Nachrichten erfolgt jeweils umgekehrt: die Signatur einer Nachricht erfolgt jeweils mit dem Private-Key des Absenders. Da der Empfänger den Public-Key des Absenders erkennt, so kann damit die Signatur überprüft werden.

**Vertrauensstellung per Dateisystem konfigurieren**

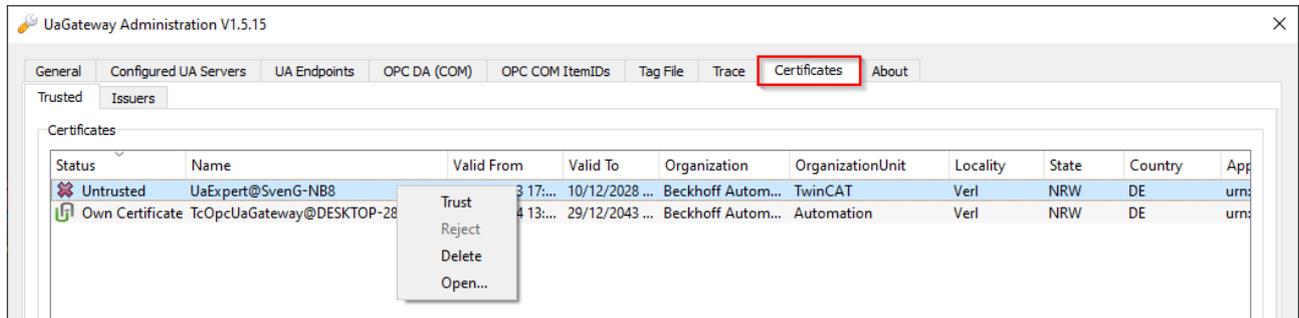
Durch das Verschieben von Client-Zertifikaten zwischen den trusted/rejected-Verzeichnissen können die Vertrauenseinstellungen entsprechend angepasst werden. Der öffentliche Schlüssel eines Client-Zertifikats wird beim ersten Verbindungsversuch des Clients mit einem sicheren Endpunkt automatisch im Verzeichnis für nicht-vertrauenswürdige Zertifikate abgelegt. Durch das anschließende Verschieben des öffentlichen Schlüssels in das Verzeichnis für vertrauenswürdige Zertifikate wird dem Client beim nächsten Verbindungsversuch vertraut und er kann sich verbinden.

**● Accept all certificates**

**I** Ist diese Option in der [Konfiguration der Endpunkte](#) [► 25] des Gateways aktiviert, so vertraut das Gateway automatisch allen Clientzertifikaten. Diese werden in diesem Fall nicht in einem der oben genannten Verzeichnisse aufgelistet.

**Vertrauensstellung per Konfigurator konfigurieren**

Sie können die Vertrauenseinstellungen auch über den Konfigurator durchführen. Der Konfigurator beinhaltet entsprechend eine grafische Benutzeroberfläche zur Konfiguration der Vertrauenseinstellungen. Über das Kontextmenü können Sie ein Zertifikat trusten oder rejecten.



**4.9.4 Authentifizierung**

Ein OPC UA Client kann sich über verschiedene Anmeldemethoden am TwinCAT OPC UA Gateway authentifizieren. Hierbei werden die folgenden sogenannten „IdentityToken“ unterstützt:

- Anonymous
- Benutzername/Passwort
- Benutzerzertifikat

**● Auslieferungszustand**

**I** Im Auslieferungszustand des Gateways ist das IdentityToken „Anonymous“ aktiviert. Wir empfehlen nach der Erstinbetriebnahme die Konfiguration eines Benutzers oder einer Benutzergruppe für den Zugriff auf den Server. Für weitere Informationen siehe [Empfohlene Schritte](#) [► 18].

**Anonymous**

Diese Art der Authentifizierung ermöglicht es beliebigen OPC UA Clients, eine Verbindung zum Gateway herzustellen. Die Angabe einer Benutzeridentität ist hierbei nicht erforderlich. Wir empfehlen diese Authentifizierungsmethode nach der Inbetriebnahme des Gateways zu deaktivieren. Dies kann über den Konfigurator erfolgen.

## Benutzername/Passwort

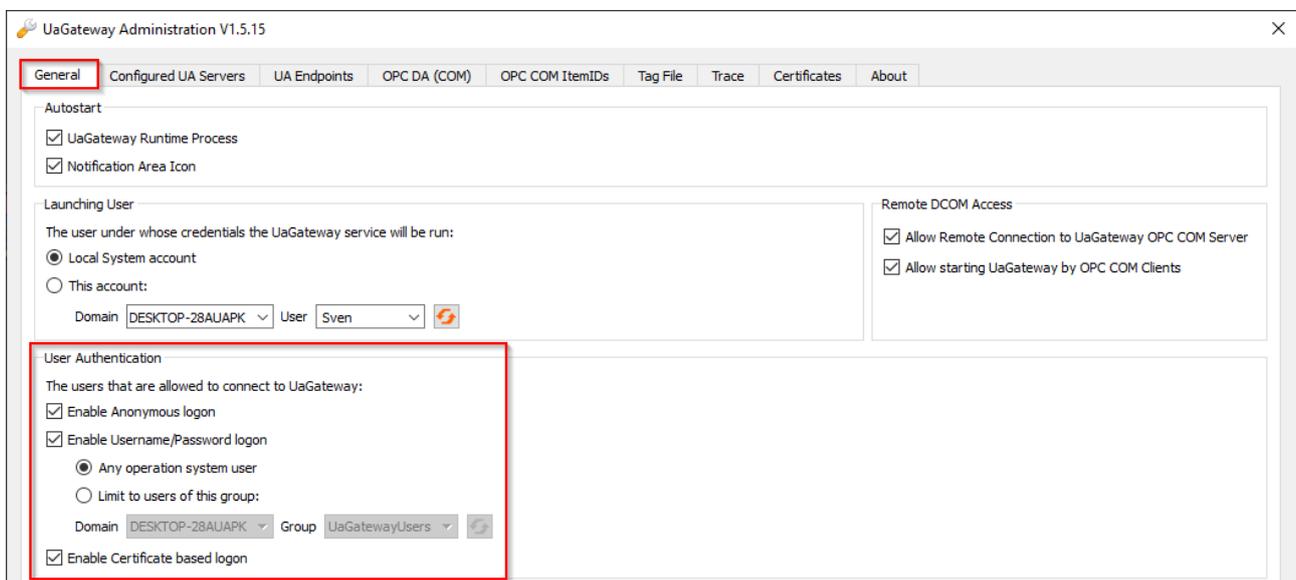
Diese Authentifizierungsmethode verwendet eine Benutzername/Passwort-Kombination zum Authentifizieren des Clients am OPC UA Server des Gateways. Der Benutzer oder die Benutzergruppe werden hierbei im Betriebssystem angelegt und verwaltet.

## Benutzerzertifikat

Diese Art der Authentifizierung verwendet ein Zertifikat, um sich an dem OPC UA Server des Gateways zu authentifizieren. Die Handhabung der Benutzerzertifikate auf Seite des Gateways ist identisch zur Verwendung von Zertifikaten auf Transportebene, d. h. das Gateway muss dem (Benutzer-) Zertifikat vertrauen, bevor sich der Client mit dem Zertifikat erfolgreich am Gateway authentifizieren kann. Ein separates [Applikationsverzeichnis \[► 21\]](#) ("pkuser") zur Verwaltung der Benutzerzertifikate steht hierfür im Gateway zur Verfügung.

## Konfiguration

Die Aktivierung/Deaktivierung der einzelnen Authentifizierungsmethode erfolgt üblicherweise über den Konfigurator.



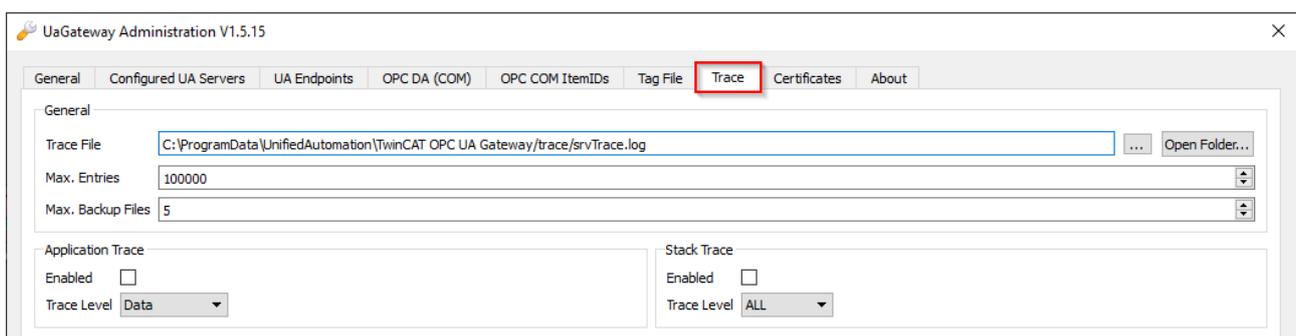
## 4.10 Logging

Sie können für eine erweiterte Diagnose eine Protokolldatei im Gateway aktivieren, in welcher dann auf Basis von unterschiedlichen Protokollleveln verschiedene Informationen mitgeschrieben werden.

### **i** Einfluss des Loggings auf das Betriebsverhalten

Bitte beachten Sie, dass die Aktivierung der Protokolldatei negative Einflüsse auf die Geschwindigkeit und das Betriebsverhalten des TwinCAT OPC UA Gateways haben kann.

Der Standardpfad für die erstellten Protokolldateien wird in dem Kapitel [Applikationsverzeichnisse \[► 21\]](#) näher beschrieben und kann auch im TwinCAT OPC UA Gateway Konfigurator eingesehen werden.



## 5 Anhang

### 5.1 Fehlerdiagnose

Verhalten	Hinweise
Das Gateway kann sich nicht mit dem Server verbinden.	Eine der möglichen Ursachen ist, dass eine alte Konfiguration benutzt wird. Wenn es beispielsweise ein neues Server-Zertifikat gibt, merkt das Gateway dies erst, wenn der konfigurierte Endpoint gelöscht und unter anderem Namen wieder eingefügt wird. Bei gleichem Endpoint oder einem neuen Endpoint mit gleichem Namen würde das Gateway die Verbindungsinformationen aus einem Cache verwenden und infolgedessen keine Verbindung mehr zum Server herstellen können.

### 5.2 ADS Return Codes

Gruppierung der Fehlercodes:

Globale Fehlercodes: [0x0000 \[▶ 33\]](#)... (0x9811\_0000 ...)

Router Fehlercodes: [0x0500 \[▶ 34\]](#)... (0x9811\_0500 ...)

Allgemeine ADS Fehler: [0x0700 \[▶ 35\]](#)... (0x9811\_0700 ...)

RTime Fehlercodes: [0x1000 \[▶ 37\]](#)... (0x9811\_1000 ...)

#### Globale Fehlercodes

Hex	Dec	HRESULT	Name	Beschreibung
0x0	0	0x98110000	ERR_NOERROR	Kein Fehler.
0x1	1	0x98110001	ERR_INTERNAL	Interner Fehler.
0x2	2	0x98110002	ERR_NORTIME	Keine Echtzeit.
0x3	3	0x98110003	ERR_ALLOCLOCKEDMEM	Zuweisung gesperrt - Speicherfehler.
0x4	4	0x98110004	ERR_INSERTMAILBOX	Postfach voll – Es konnte die ADS Nachricht nicht versendet werden. Reduzieren der Anzahl der ADS Nachrichten pro Zyklus bringt Abhilfe.
0x5	5	0x98110005	ERR_WRONGRECEIVEHMSG	Falsches HMSG.
0x6	6	0x98110006	ERR_TARGETPORTNOTFOUND	Ziel-Port nicht gefunden – ADS Server ist nicht gestartet oder erreichbar.
0x7	7	0x98110007	ERR_TARGETMACHINENOTFOUND	Zielrechner nicht gefunden – AMS Route wurde nicht gefunden.
0x8	8	0x98110008	ERR_UNKNOWNCMDID	Unbekannte Befehl-ID.
0x9	9	0x98110009	ERR_BADTASKID	Ungültige Task-ID.
0xA	10	0x9811000A	ERR_NOIO	Kein IO.
0xB	11	0x9811000B	ERR_UNKNOWNAMSCMD	Unbekannter AMS-Befehl.
0xC	12	0x9811000C	ERR_WIN32ERROR	Win32 Fehler.
0xD	13	0x9811000D	ERR_PORTNOTCONNECTED	Port nicht verbunden.
0xE	14	0x9811000E	ERR_INVALIDAMSLENGTH	Ungültige AMS-Länge.
0xF	15	0x9811000F	ERR_INVALIDAMSNETID	Ungültige AMS Net ID.
0x10	16	0x98110010	ERR_LOWINSTLEVEL	Installations-Level ist zu niedrig –TwinCAT 2 Lizenzfehler.
0x11	17	0x98110011	ERR_NODEBUGINTAVAILABLE	Kein Debugging verfügbar.
0x12	18	0x98110012	ERR_PORTDISABLED	Port deaktiviert – TwinCAT System Service nicht gestartet.
0x13	19	0x98110013	ERR_PORTALREADYCONNECTED	Port bereits verbunden.
0x14	20	0x98110014	ERR_AMSSYNC_W32ERROR	AMS Sync Win32 Fehler.
0x15	21	0x98110015	ERR_AMSSYNC_TIMEOUT	AMS Sync Timeout.
0x16	22	0x98110016	ERR_AMSSYNC_AMSERROR	AMS Sync Fehler.
0x17	23	0x98110017	ERR_AMSSYNC_NOINDEXINMAP	Keine Index-Map für AMS Sync vorhanden.
0x18	24	0x98110018	ERR_INVALIDAMSPORT	Ungültiger AMS-Port.
0x19	25	0x98110019	ERR_NOMEMORY	Kein Speicher.
0x1A	26	0x9811001A	ERR_TCPSEND	TCP Sendefehler.
0x1B	27	0x9811001B	ERR_HOSTUNREACHABLE	Host nicht erreichbar.
0x1C	28	0x9811001C	ERR_INVALIDAMSFRAGMENT	Ungültiges AMS Fragment.
0x1D	29	0x9811001D	ERR_TLSEND	TLS Sendefehler – Secure ADS Verbindung fehlgeschlagen.
0x1E	30	0x9811001E	ERR_ACCESSDENIED	Zugriff Verweigert – Secure ADS Zugriff verweigert.

## Router Fehlercodes

Hex	Dec	HRESULT	Name	Beschreibung
0x500	1280	0x98110500	ROUTERERR_NOLOCKEDMEMORY	Lockierter Speicher kann nicht zugewiesen werden.
0x501	1281	0x98110501	ROUTERERR_RESIZEMEMORY	Die Größe des Routerspeichers konnte nicht geändert werden.
0x502	1282	0x98110502	ROUTERERR_MAILBOXFULL	Das Postfach hat die maximale Anzahl der möglichen Meldungen erreicht.
0x503	1283	0x98110503	ROUTERERR_DEBUGBOXFULL	Das Debug Postfach hat die maximale Anzahl der möglichen Meldungen erreicht.
0x504	1284	0x98110504	ROUTERERR_UNKNOWNPORTTYPE	Der Porttyp ist unbekannt.
0x505	1285	0x98110505	ROUTERERR_NOTINITIALIZED	Router ist nicht initialisiert.
0x506	1286	0x98110506	ROUTERERR_PORTALREADYINUSE	Die Portnummer ist bereits vergeben.
0x507	1287	0x98110507	ROUTERERR_NOTREGISTERED	Der Port ist nicht registriert.
0x508	1288	0x98110508	ROUTERERR_NOMOREQUEUES	Die maximale Portanzahl ist erreicht.
0x509	1289	0x98110509	ROUTERERR_INVALIDPORT	Der Port ist ungültig.
0x50A	1290	0x9811050A	ROUTERERR_NOTACTIVATED	Der Router ist nicht aktiv.
0x50B	1291	0x9811050B	ROUTERERR_FRAGMENTBOXFULL	Das Postfach hat die maximale Anzahl für fragmentierte Nachrichten erreicht.
0x50C	1292	0x9811050C	ROUTERERR_FRAGMENTTIMEOUT	Fragment Timeout aufgetreten.
0x50D	1293	0x9811050D	ROUTERERR_TOBEREMOVED	Port wird entfernt.

**Allgemeine ADS Fehlercodes**

Hex	Dec	HRESULT	Name	Beschreibung
0x700	1792	0x98110700	ADSERR_DEVICE_ERROR	Allgemeiner Gerätefehler.
0x701	1793	0x98110701	ADSERR_DEVICE_SRVNOTSUPP	Service wird vom Server nicht unterstützt.
0x702	1794	0x98110702	ADSERR_DEVICE_INVALIDGRP	Ungültige Index-Gruppe.
0x703	1795	0x98110703	ADSERR_DEVICE_INVALIDOFFSET	Ungültiger Index-Offset.
0x704	1796	0x98110704	ADSERR_DEVICE_INVALIDACCESS	Lesen oder Schreiben nicht gestattet.
0x705	1797	0x98110705	ADSERR_DEVICE_INVALIDSIZE	Parametergröße nicht korrekt.
0x706	1798	0x98110706	ADSERR_DEVICE_INVALIDDATA	Ungültige Daten-Werte.
0x707	1799	0x98110707	ADSERR_DEVICE_NOTREADY	Gerät nicht betriebsbereit.
0x708	1800	0x98110708	ADSERR_DEVICE_BUSY	Gerät beschäftigt.
0x709	1801	0x98110709	ADSERR_DEVICE_INVALIDCONTEXT	Ungültiger Kontext vom Betriebssystem - Kann durch Verwendung von ADS Bausteinen in unterschiedlichen Tasks auftreten. Abhilfe kann die Multitasking-Synchronisation in der SPS geben.
0x70A	1802	0x9811070A	ADSERR_DEVICE_NOMEMORY	Nicht genügend Speicher.
0x70B	1803	0x9811070B	ADSERR_DEVICE_INVALIDPARM	Ungültige Parameter-Werte.
0x70C	1804	0x9811070C	ADSERR_DEVICE_NOTFOUND	Nicht gefunden (Dateien,...).
0x70D	1805	0x9811070D	ADSERR_DEVICE_SYNTAX	Syntax-Fehler in Datei oder Befehl.
0x70E	1806	0x9811070E	ADSERR_DEVICE_INCOMPATIBLE	Objekte stimmen nicht überein.
0x70F	1807	0x9811070F	ADSERR_DEVICE_EXISTS	Objekt ist bereits vorhanden.
0x710	1808	0x98110710	ADSERR_DEVICE_SYMBOLNOTFOUND	Symbol nicht gefunden.
0x711	1809	0x98110711	ADSERR_DEVICE_SYMBOLVERSIONINVALID	Symbol-Version ungültig – Kann durch einen Online-Change auftreten. Erzeuge einen neuen Handle.
0x712	1810	0x98110712	ADSERR_DEVICE_INVALIDSTATE	Gerät (Server) ist im ungültigen Zustand.
0x713	1811	0x98110713	ADSERR_DEVICE_TRANSMODENOTSUPP	AdsTransMode nicht unterstützt.
0x714	1812	0x98110714	ADSERR_DEVICE_NOTIFYHANDINVALID	Notification Handle ist ungültig.
0x715	1813	0x98110715	ADSERR_DEVICE_CLIENTUNKNOWN	Notification-Client nicht registriert.
0x716	1814	0x98110716	ADSERR_DEVICE_NOMOREHDL	Keine weiteren Handles verfügbar.
0x717	1815	0x98110717	ADSERR_DEVICE_INVALIDWATCHSIZE	Größe der Notification zu groß.
0x718	1816	0x98110718	ADSERR_DEVICE_NOTINIT	Gerät nicht initialisiert.
0x719	1817	0x98110719	ADSERR_DEVICE_TIMEOUT	Gerät hat einen Timeout.
0x71A	1818	0x9811071A	ADSERR_DEVICE_NOINTERFACE	Interface Abfrage fehlgeschlagen.
0x71B	1819	0x9811071B	ADSERR_DEVICE_INVALIDINTERFACE	Falsches Interface angefordert.
0x71C	1820	0x9811071C	ADSERR_DEVICE_INVALIDCLSID	Class-ID ist ungültig.
0x71D	1821	0x9811071D	ADSERR_DEVICE_INVALIDOBJID	Object-ID ist ungültig.
0x71E	1822	0x9811071E	ADSERR_DEVICE_PENDING	Anforderung steht aus.
0x71F	1823	0x9811071F	ADSERR_DEVICE_ABORTED	Anforderung wird abgebrochen.
0x720	1824	0x98110720	ADSERR_DEVICE_WARNING	Signal-Warnung.
0x721	1825	0x98110721	ADSERR_DEVICE_INVALIDARRAYIDX	Ungültiger Array-Index.
0x722	1826	0x98110722	ADSERR_DEVICE_SYMBOLNOTACTIVE	Symbol nicht aktiv.
0x723	1827	0x98110723	ADSERR_DEVICE_ACCESSDENIED	Zugriff verweigert.
0x724	1828	0x98110724	ADSERR_DEVICE_LICENSENOTFOUND	Fehlende Lizenz.
0x725	1829	0x98110725	ADSERR_DEVICE_LICENSEEXPIRED	Lizenz abgelaufen.
0x726	1830	0x98110726	ADSERR_DEVICE_LICENSEEXCEEDED	Lizenz überschritten.
0x727	1831	0x98110727	ADSERR_DEVICE_LICENSEINVALID	Lizenz ungültig.
0x728	1832	0x98110728	ADSERR_DEVICE_LICENSESYSTEMID	Lizenzproblem: System-ID ist ungültig.
0x729	1833	0x98110729	ADSERR_DEVICE_LICENSENOTIMELIMIT	Lizenz nicht zeitlich begrenzt.
0x72A	1834	0x9811072A	ADSERR_DEVICE_LICENSEFUTUREISSUE	Lizenzproblem: Zeitpunkt in der Zukunft.
0x72B	1835	0x9811072B	ADSERR_DEVICE_LICENSETIMETOLONG	Lizenz-Zeitraum zu lang.
0x72C	1836	0x9811072C	ADSERR_DEVICE_EXCEPTION	Exception beim Systemstart.
0x72D	1837	0x9811072D	ADSERR_DEVICE_LICENSEDUPLICATED	Lizenz-Datei zweimal gelesen.
0x72E	1838	0x9811072E	ADSERR_DEVICE_SIGNATUREINVALID	Ungültige Signatur.
0x72F	1839	0x9811072F	ADSERR_DEVICE_CERTIFICATEINVALID	Zertifikat ungültig.
0x730	1840	0x98110730	ADSERR_DEVICE_LICENSEOEMNOTFOUND	Public Key vom OEM nicht bekannt.
0x731	1841	0x98110731	ADSERR_DEVICE_LICENSERESTRICTED	Lizenz nicht gültig für diese System.ID.
0x732	1842	0x98110732	ADSERR_DEVICE_LICENSEDEMOTDENIED	Demo-Lizenz untersagt.
0x733	1843	0x98110733	ADSERR_DEVICE_INVALIDFNCID	Funktions-ID ungültig.
0x734	1844	0x98110734	ADSERR_DEVICE_OUTOFRANGE	Außerhalb des gültigen Bereiches.
0x735	1845	0x98110735	ADSERR_DEVICE_INVALIDALIGNMENT	Ungültiges Alignment.

Hex	Dec	HRESULT	Name	Beschreibung
0x736	1846	0x98110736	ADSERR_DEVICE_LICENSEPLATFORM	Ungültiger Plattform Level.
0x737	1847	0x98110737	ADSERR_DEVICE_FORWARD_PL	Kontext – Weiterleitung zum Passiv-Level.
0x738	1848	0x98110738	ADSERR_DEVICE_FORWARD_DL	Kontext – Weiterleitung zum Dispatch-Level.
0x739	1849	0x98110739	ADSERR_DEVICE_FORWARD_RT	Kontext – Weiterleitung zur Echtzeit.
0x740	1856	0x98110740	ADSERR_CLIENT_ERROR	Clientfehler.
0x741	1857	0x98110741	ADSERR_CLIENT_INVALIDPARM	Dienst enthält einen ungültigen Parameter.
0x742	1858	0x98110742	ADSERR_CLIENT_LISTEMPTY	Polling-Liste ist leer.
0x743	1859	0x98110743	ADSERR_CLIENT_VARUSED	Var-Verbindung bereits im Einsatz.
0x744	1860	0x98110744	ADSERR_CLIENT_DUPLINVOKEID	Die aufgerufene ID ist bereits in Benutzung.
0x745	1861	0x98110745	ADSERR_CLIENT_SYNC TIMEOUT	Timeout ist aufgetreten – Die Gegenstelle antwortet nicht im vorgegebenen ADS Timeout. Die Routeneinstellung der Gegenstelle kann falsch konfiguriert sein.
0x746	1862	0x98110746	ADSERR_CLIENT_W32ERROR	Fehler im Win32 Subsystem.
0x747	1863	0x98110747	ADSERR_CLIENT_TIMEOUTINVALID	Ungültiger Client Timeout-Wert.
0x748	1864	0x98110748	ADSERR_CLIENT_PORTNOTOPEN	Port nicht geöffnet.
0x749	1865	0x98110749	ADSERR_CLIENT_NOAMSADDR	Keine AMS Adresse.
0x750	1872	0x98110750	ADSERR_CLIENT_SYNCINTERNAL	Interner Fehler in Ads-Sync.
0x751	1873	0x98110751	ADSERR_CLIENT_ADDHASH	Überlauf der Hash-Tabelle.
0x752	1874	0x98110752	ADSERR_CLIENT_REMOVEHASH	Schlüssel in der Tabelle nicht gefunden.
0x753	1875	0x98110753	ADSERR_CLIENT_NOMORESVM	Keine Symbole im Cache.
0x754	1876	0x98110754	ADSERR_CLIENT_SYNCRESINVALID	Ungültige Antwort erhalten.
0x755	1877	0x98110755	ADSERR_CLIENT_SYNCPORTLOCKED	Sync Port ist verriegelt.
0x756	1878	0x98110756	ADSERR_CLIENT_REQUESTCANCELLED	Die Anfrage wurde abgebrochen.

**RTime Fehlercodes**

Hex	Dec	HRESULT	Name	Beschreibung
0x1000	4096	0x98111000	RTERR_INTERNAL	Interner Fehler im Echtzeit-System.
0x1001	4097	0x98111001	RTERR_BADTIMERPERIODS	Timer-Wert nicht gültig.
0x1002	4098	0x98111002	RTERR_INVALIDTASKPTR	Task-Pointer hat den ungültigen Wert 0 (null).
0x1003	4099	0x98111003	RTERR_INVALIDSTACKPTR	Stack-Pointer hat den ungültigen Wert 0 (null).
0x1004	4100	0x98111004	RTERR_PrioEXISTS	Die Request Task Priority ist bereits vergeben.
0x1005	4101	0x98111005	RTERR_NOMORETCB	Kein freier TCB (Task Control Block) verfügbar. Maximale Anzahl von TCBs beträgt 64.
0x1006	4102	0x98111006	RTERR_NOMORESEMAS	Keine freien Semaphoren zur Verfügung. Maximale Anzahl der Semaphoren beträgt 64.
0x1007	4103	0x98111007	RTERR_NOMOREQUEUES	Kein freier Platz in der Warteschlange zur Verfügung. Maximale Anzahl der Plätze in der Warteschlange beträgt 64.
0x100D	4109	0x9811100D	RTERR_EXTIRQALREADYDEF	Ein externer Synchronisations-Interrupt wird bereits angewandt.
0x100E	4110	0x9811100E	RTERR_EXTIRQNOTDEF	Kein externer Sync-Interrupt angewandt.
0x100F	4111	0x9811100F	RTERR_EXTIRQINSTALLFAILED	Anwendung des externen Synchronisierungs-Interrupts ist fehlgeschlagen.
0x1010	4112	0x98111010	RTERR_IRQLNOTLESSOREQUAL	Aufruf einer Service-Funktion im falschen Kontext
0x1017	4119	0x98111017	RTERR_VMXNOTSUPPORTED	Intel VT-x Erweiterung wird nicht unterstützt.
0x1018	4120	0x98111018	RTERR_VMXDISABLED	Intel VT-x Erweiterung ist nicht aktiviert im BIOS.
0x1019	4121	0x98111019	RTERR_VMXCONTROLSMISSING	Fehlende Funktion in Intel VT-x Erweiterung.
0x101A	4122	0x9811101A	RTERR_VMXENABLEFAILS	Aktivieren von Intel VT-x schlägt fehl.

**Spezifische positive HRESULT Return Codes:**

HRESULT	Name	Beschreibung
0x0000_0000	S_OK	Kein Fehler.
0x0000_0001	S_FALSE	Kein Fehler. Bsp.: erfolgreiche Abarbeitung, bei der jedoch ein negatives oder unvollständiges Ergebnis erzielt wurde.
0x0000_0203	S_PENDING	Kein Fehler. Bsp.: erfolgreiche Abarbeitung, bei der jedoch noch kein Ergebnis vorliegt.
0x0000_0256	S_WATCHDOG_TIMEOUT	Kein Fehler. Bsp.: erfolgreiche Abarbeitung, bei der jedoch eine Zeitüberschreitung eintrat.

### TCP Winsock-Fehlercodes

Hex	Dec	Name	Beschreibung
0x274C	10060	WSAETIMEDOUT	Verbindungs Timeout aufgetreten - Fehler beim Herstellen der Verbindung, da die Gegenstelle nach einer bestimmten Zeitspanne nicht ordnungsgemäß reagiert hat, oder die hergestellte Verbindung konnte nicht aufrecht erhalten werden, da der verbundene Host nicht reagiert hat.
0x274D	10061	WSAECONNREFUSED	Verbindung abgelehnt - Es konnte keine Verbindung hergestellt werden, da der Zielcomputer dies explizit abgelehnt hat. Dieser Fehler resultiert normalerweise aus dem Versuch, eine Verbindung mit einem Dienst herzustellen, der auf dem fremden Host inaktiv ist—das heißt, einem Dienst, für den keine Serveranwendung ausgeführt wird.
0x2751	10065	WSAEHOSTUNREACH	Keine Route zum Host - Ein Socketvorgang bezog sich auf einen nicht verfügbaren Host.

Weitere Winsock-Fehlercodes: Win32-Fehlercodes

## 5.3 Support und Service

Beckhoff und seine weltweiten Partnerfirmen bieten einen umfassenden Support und Service, der eine schnelle und kompetente Unterstützung bei allen Fragen zu Beckhoff Produkten und Systemlösungen zur Verfügung stellt.

### Downloadfinder

Unser [Downloadfinder](#) beinhaltet alle Dateien, die wir Ihnen zum Herunterladen anbieten. Sie finden dort Applikationsberichte, technische Dokumentationen, technische Zeichnungen, Konfigurationsdateien und vieles mehr.

Die Downloads sind in verschiedenen Formaten erhältlich.

### Beckhoff Niederlassungen und Vertretungen

Wenden Sie sich bitte an Ihre Beckhoff Niederlassung oder Ihre Vertretung für den lokalen Support und Service zu Beckhoff Produkten!

Die Adressen der weltweiten Beckhoff Niederlassungen und Vertretungen entnehmen Sie bitte unserer Internetseite: [www.beckhoff.com](http://www.beckhoff.com)

Dort finden Sie auch weitere Dokumentationen zu Beckhoff Komponenten.

### Beckhoff Support

Der Support bietet Ihnen einen umfangreichen technischen Support, der Sie nicht nur bei dem Einsatz einzelner Beckhoff Produkte, sondern auch bei weiteren umfassenden Dienstleistungen unterstützt:

- Support
- Planung, Programmierung und Inbetriebnahme komplexer Automatisierungssysteme
- umfangreiches Schulungsprogramm für Beckhoff Systemkomponenten

Hotline: +49 5246 963-157  
E-Mail: [support@beckhoff.com](mailto:support@beckhoff.com)

**Beckhoff Service**

Das Beckhoff Service-Center unterstützt Sie rund um den After-Sales-Service:

- Vor-Ort-Service
- Reparaturservice
- Ersatzteilservice
- Hotline-Service

Hotline: +49 5246 963-460  
E-Mail: [service@beckhoff.com](mailto:service@beckhoff.com)

**Beckhoff Unternehmenszentrale**

Beckhoff Automation GmbH & Co. KG

Hülshorstweg 20  
33415 Verl  
Deutschland

Telefon: +49 5246 963-0  
E-Mail: [info@beckhoff.com](mailto:info@beckhoff.com)  
Internet: [www.beckhoff.com](http://www.beckhoff.com)



Mehr Informationen:  
**[www.beckhoff.de/TS6100](http://www.beckhoff.de/TS6100)**

Beckhoff Automation GmbH & Co. KG  
Hülshorstweg 20  
33415 Verl  
Deutschland  
Telefon: +49 5246 9630  
[info@beckhoff.com](mailto:info@beckhoff.com)  
[www.beckhoff.com](http://www.beckhoff.com)

