

Handbuch | DE

TS6100

TwinCAT 2 | OPC UA Configurator



Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Vorwort..... | 5 |
| 1.1 | Hinweise zur Dokumentation | 5 |
| 1.2 | Zu Ihrer Sicherheit..... | 6 |
| 1.3 | Hinweise zur Informationssicherheit | 7 |
| 2 | Übersicht..... | 8 |
| 3 | Installation | 10 |
| 3.1 | Systemvoraussetzungen | 10 |
| 3.2 | Installation | 10 |
| 4 | Technische Einführung | 13 |
| 4.1 | Quick Start | 13 |
| 4.2 | Applikationsverzeichnisse | 19 |
| 4.3 | Visual Studio | 20 |
| 4.3.1 | Übersicht | 20 |
| 4.3.2 | Neues Projekt anlegen..... | 21 |
| 4.3.3 | Verbinden mit einem Server..... | 21 |
| 4.3.4 | Durchführen der Server-Initialisierung | 23 |
| 4.3.5 | ADS-Geräte hinzufügen | 24 |
| 4.3.6 | Konfiguration lesen und schreiben..... | 26 |
| 4.3.7 | Konfigurationsdateien importieren und exportieren | 28 |
| 4.3.8 | Historical Access konfigurieren | 29 |
| 4.3.9 | Alarms and Conditions konfigurieren | 30 |
| 4.3.10 | Alarmtexte konfigurieren | 34 |
| 4.3.11 | Endpunkte konfigurieren | 37 |
| 4.3.12 | Vertrauensstellung für Zertifikate | 37 |
| 4.3.13 | Sicherheitseinstellungen konfigurieren | 38 |
| 4.3.14 | Server neu starten..... | 46 |
| 4.3.15 | Logging | 46 |
| 4.4 | Standalone | 48 |
| 4.4.1 | Übersicht | 48 |
| 4.4.2 | Verbinden mit einem Server..... | 48 |
| 4.4.3 | Durchführen der Server-Initialisierung | 49 |
| 4.4.4 | ADS-Geräte hinzufügen | 49 |
| 4.4.5 | Konfiguration lesen und schreiben..... | 51 |
| 4.4.6 | Historical Access konfigurieren | 51 |
| 4.4.7 | Alarms and Conditions konfigurieren | 53 |
| 4.4.8 | Alarmtexte konfigurieren | 54 |
| 4.4.9 | Endpunkte konfigurieren | 57 |
| 4.4.10 | Vertrauensstellung für Zertifikate | 58 |
| 4.4.11 | Sicherheitseinstellungen konfigurieren | 58 |
| 4.4.12 | Server neu starten..... | 61 |
| 4.4.13 | Logging | 61 |
| 5 | Anhang..... | 63 |
| 5.1 | ADS Return Codes..... | 63 |

5.2 Support und Service..... 67

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.



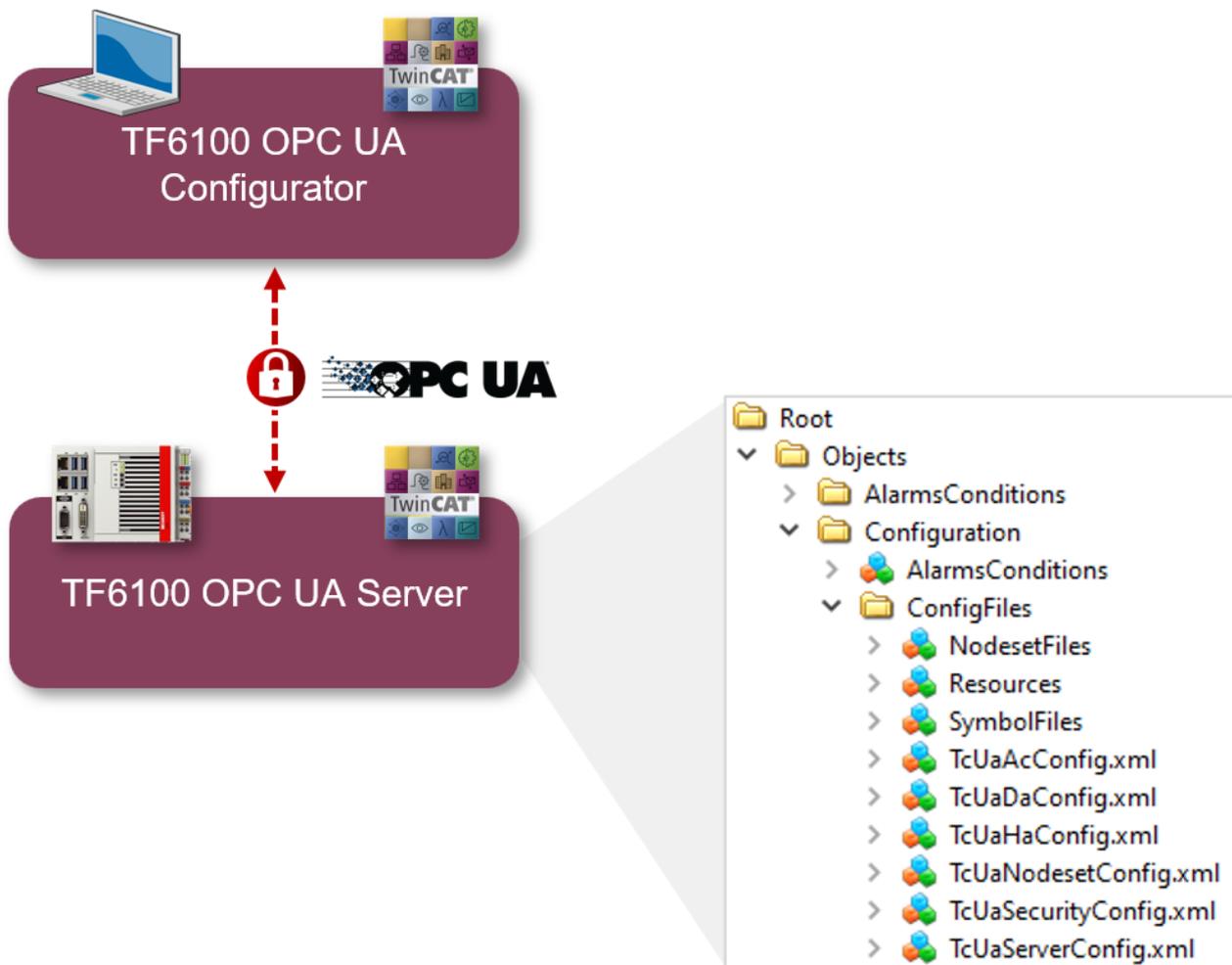
Detaillierte Informationen zu OPC UA finden Sie auf der Webseite der [OPC Foundation](#).

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 den TwinCAT OPC UA Configurator, bei welchem es sich um eine Engineering-Softwarekomponente handelt die eine grafische Benutzeroberfläche zur Konfiguration des TwinCAT OPC UA Servers anbietet. Der TwinCAT OPC UA Configurator wird hierbei in zwei Varianten ausgeliefert: eine in das Visual Studio (bzw. die TwinCAT XAE Shell) integrierte Oberfläche und ein Standalone-Tool. Beide Varianten haben die Eigenschaft, dass Sie eine OPC UA Kommunikationsverbindung zu einem TwinCAT OPC UA Server aufbauen und darüber den Server konfigurieren. Grundlage hierfür ist der sogenannte Configuration Namespace des TwinCAT OPC UA Servers, welcher alle relevanten Konfigurationsdateien für authentifizierte Benutzer über OPC UA bereitstellt.



Für einen schnellen Einstieg in das Produkt empfehlen wir unsere Kapitel [Installation \[► 10\]](#) und [Quick Start \[► 13\]](#). 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. Hierbei ist zwischen dem Standalone- und Visual Studio Konfigurator zu unterscheiden.

Visual Studio Konfigurator

| Technische Daten | Beschreibung |
|----------------------------|--|
| Betriebssystem | Windows 10 (>=21H2) Windows Server 2022 |
| Zielplattformen | PC-Architektur (x86, x64) |
| .NET Framework | 4.8.1 |
| TwinCAT-Installationslevel | TwinCAT 3 XAE |
| Benötigte TwinCAT-Lizenz | --- |

Standalone Konfigurator

| Technische Daten | Beschreibung |
|----------------------------|--|
| Betriebssystem | Windows 10 (>=21H2) Windows Server 2022 |
| Zielplattformen | PC-Architektur (x86, x64) |
| .NET Framework | 4.8.1 |
| TwinCAT-Installationslevel | TwinCAT 2 CP, PLC, NC-PTP TwinCAT 3 XAE, XAR, ADS |
| Benötigte TwinCAT-Lizenz | --- |

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

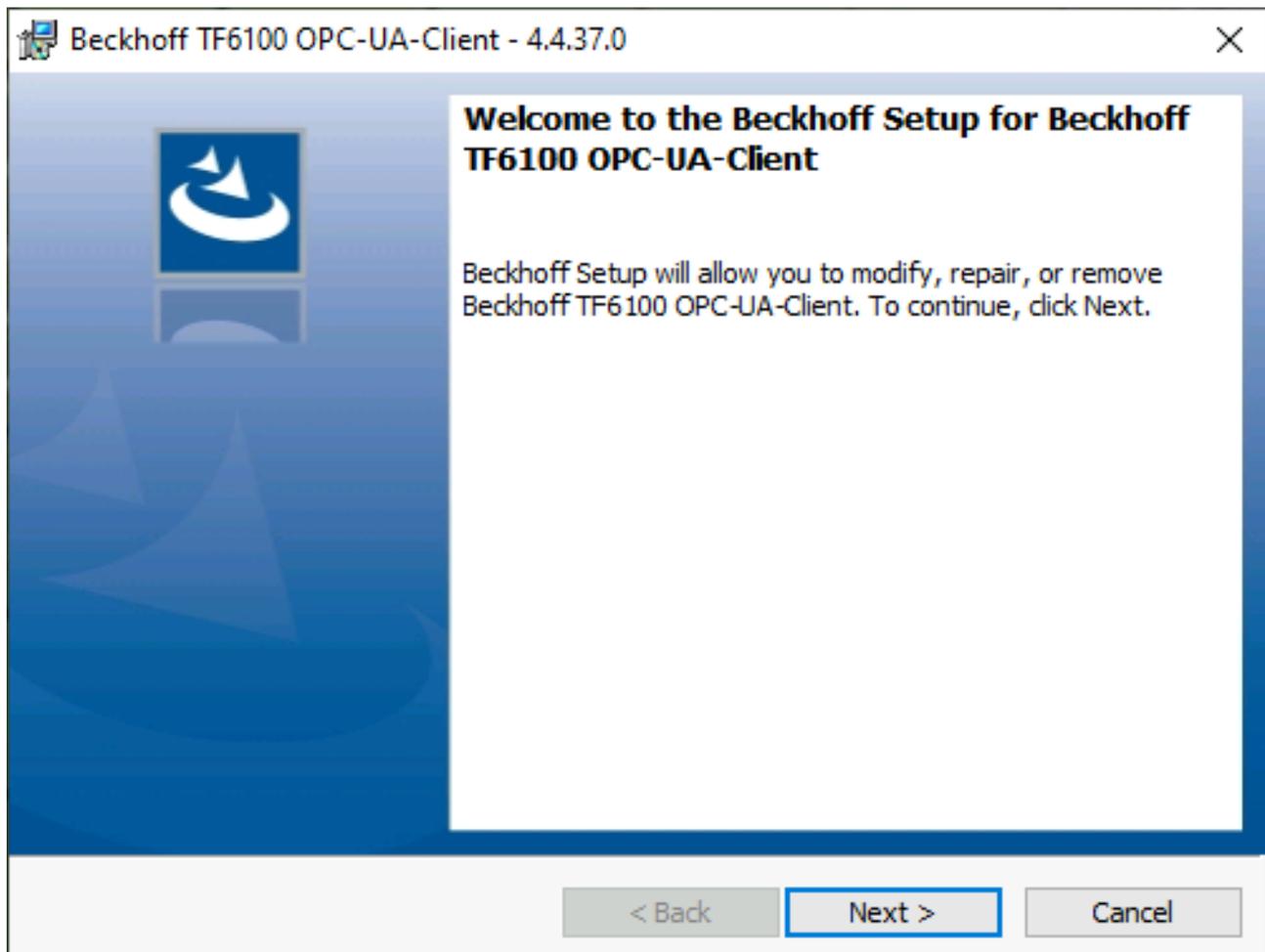
Unvorbereiteter TwinCAT-Neustart kann Datenverlust erzeugen

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.

4 Technische Einführung

4.1 Quick Start

Das folgende Kapitel ermöglicht einen schnellen Einstieg in den TwinCAT OPC UA Configurator. In dieser Anleitung wird der Standalone Configurator verwendet, um eine Verbindung mit dem lokal installierten TwinCAT OPC UA Server herzustellen und diesen zu konfigurieren. Als Voraussetzung müssen beide Produkte installiert worden sein – in diesem Beispiel auf demselben System.

Im Folgenden werden nun die folgenden Schritte näher beschrieben:

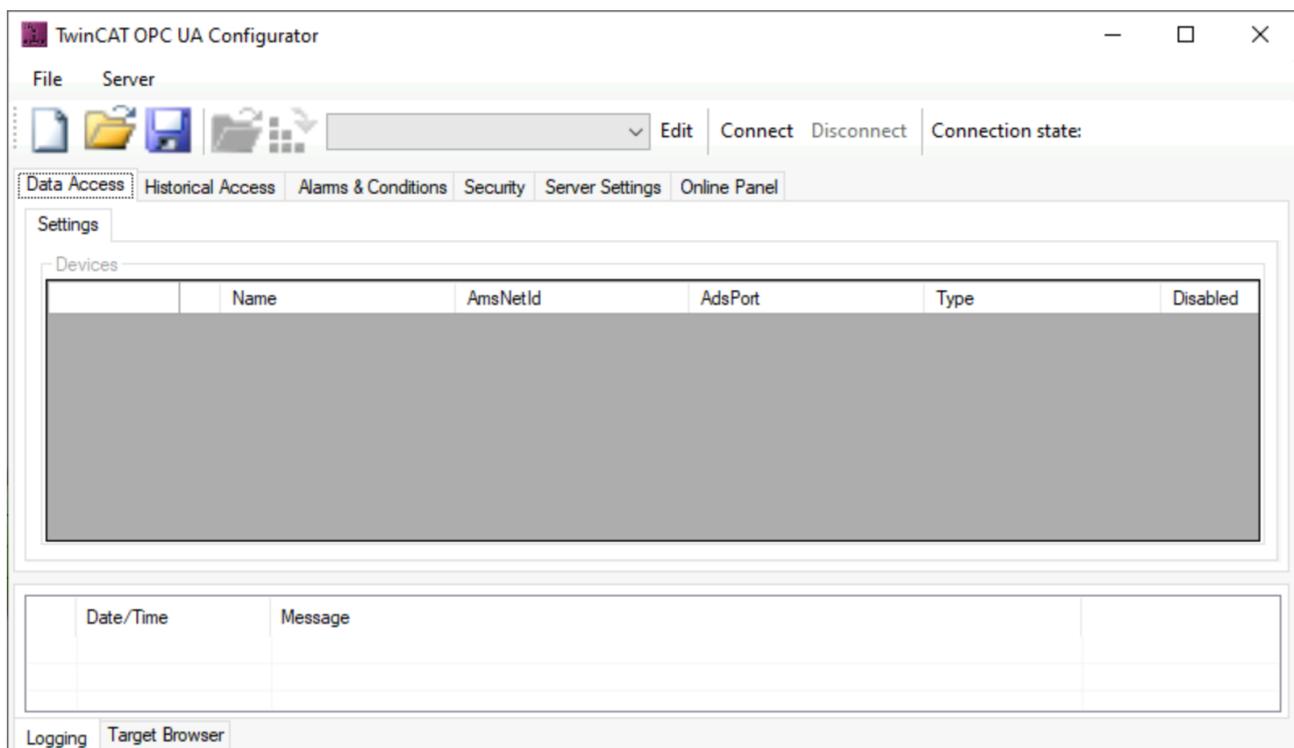
- Starten des Standalone Configurators
- Konfigurieren einer Serververbindung
- Verbinden mit dem Server und Auslesen der Konfiguration
- Durchführen von Änderungen an der Konfiguration
- Aktivieren der neuen Konfiguration auf dem Server

Starten des Standalone Configurators

Der TwinCAT OPC UA Configurator wird standardmäßig in ein Unterverzeichnis des TwinCAT Installationsverzeichnisses installiert. Weitere Informationen finden Sie in dem Dokumentationskapitel zu den Applikationsverzeichnissen [► 19].

Durch die Installation des Produkts wird eine Verknüpfung im Windows Startmenü angelegt, welche einen einfachen Zugriff auf die Applikation ermöglicht.

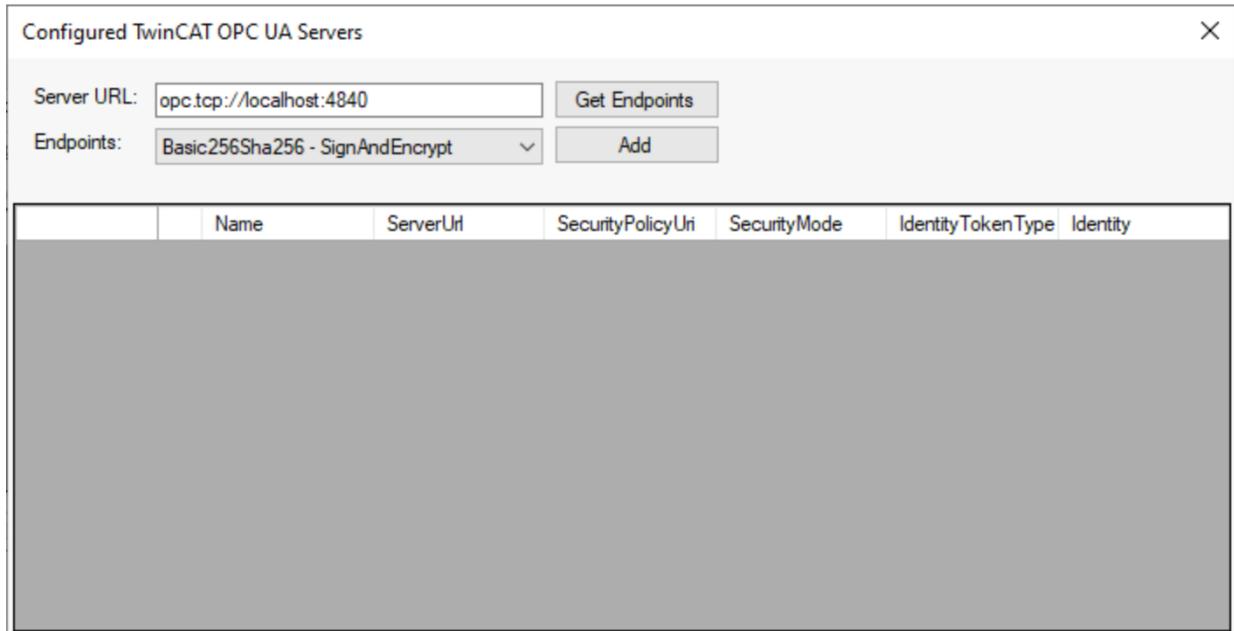
Nach dem Start der Applikation müssen Sie zunächst eine neue Serververbindung konfigurieren. Wie das geht, erfahren Sie im nächsten Schritt.



Konfigurieren einer Serververbindung

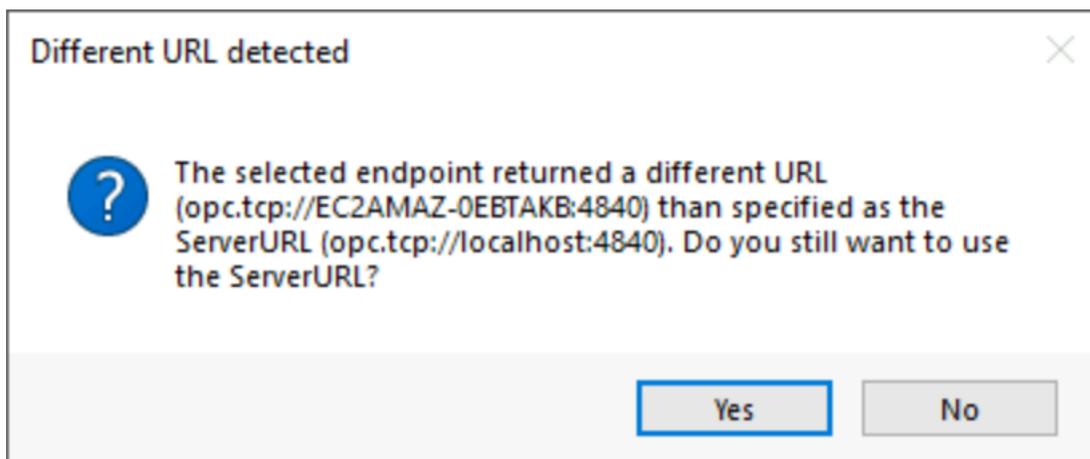
1. Öffnen Sie den Serverauswahl-Dialog, indem Sie in der Toolbar auf den Button **Edit** klicken. Tragen Sie in dem sich nun öffnenden Dialog die Server URL des zu konfigurierenden TwinCAT OPC UA Server ein. In diesem Beispiel ist der Server auf demselben System installiert und wir können die Default-Adresse (opc.tcp://localhost:4840) übernehmen. Klicken Sie auf den Button **Get Endpoints**, um eine

Liste mit allen Server-Endpunkten zu erhalten. Wählen Sie den Endpunkt „Basic256Sha256 – SignAndEncrypt“ aus.



| Name | ServerUrl | SecurityPolicyUri | SecurityMode | IdentityTokenType | Identity |
|------|-----------|-------------------|--------------|-------------------|----------|
|------|-----------|-------------------|--------------|-------------------|----------|

2. Klicken Sie anschließend auf **Add**, um den Server hinzuzufügen. Sollten Sie einen Warnhinweis bzgl. der Unterschiede in der ServerURL erhalten, bestätigen Sie diesen Hinweis mit **Yes**.



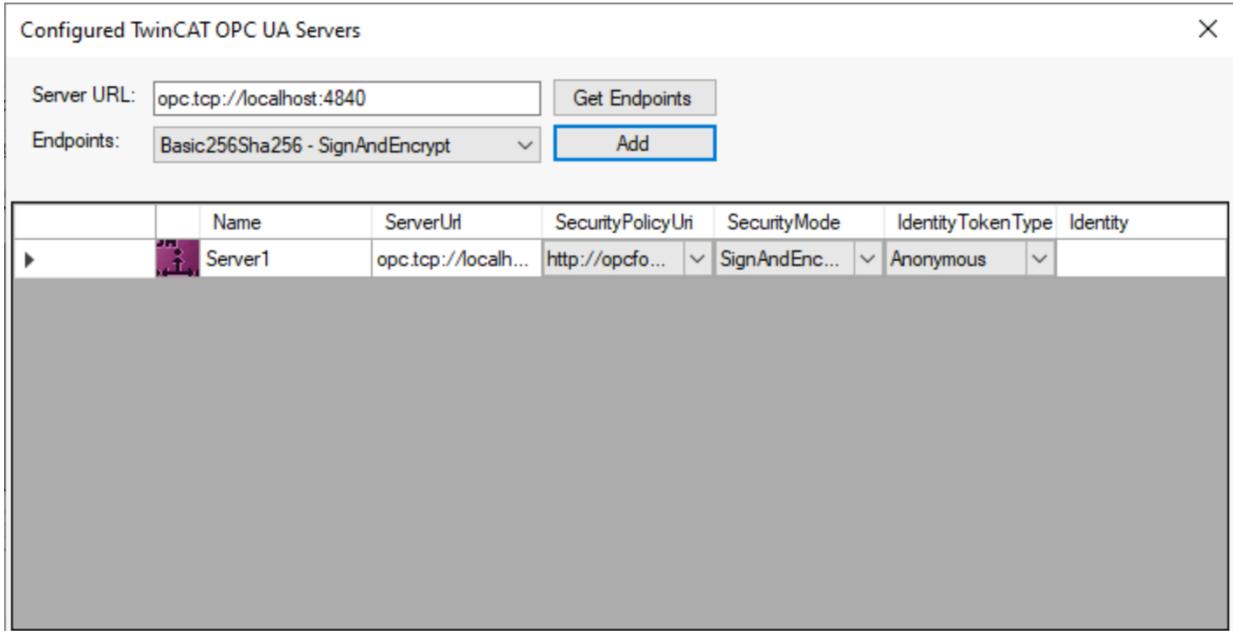
Different URL detected

?

The selected endpoint returned a different URL (opc.tcp://EC2AMAZ-0EBTAKB:4840) than specified as the ServerURL (opc.tcp://localhost:4840). Do you still want to use the ServerURL?

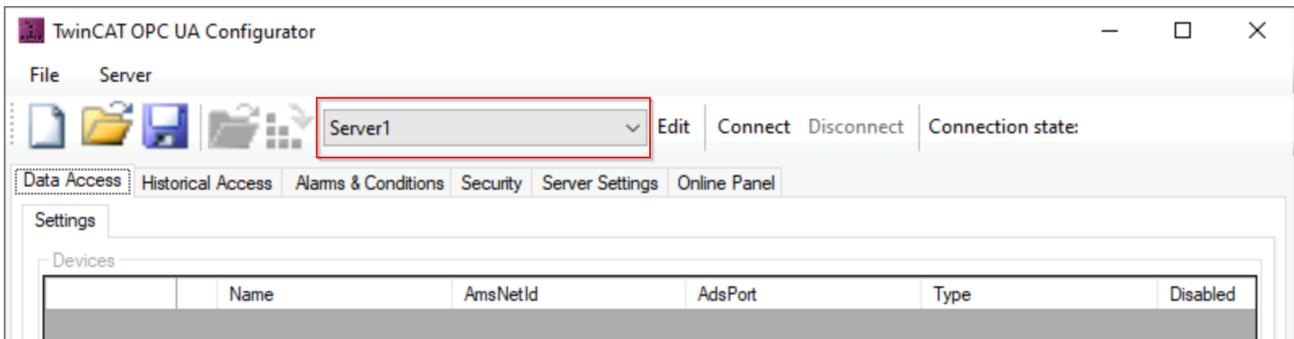
Yes No

⇒ Der TwinCAT OPC UA Server wurde nun zum Auswahldialog hinzugefügt.



Je nach Betriebsumgebung sind nun weitere Einstellungen für die Verbindungsparameter notwendig, z.B. Benutzername/Password für den Zugriff auf den Server. In diesem Beispiel gehen wir jedoch davon aus, dass sowohl der TwinCAT OPC UA Server als auch der TwinCAT OPC UA Configurator erstmalig auf diesem System in Betrieb genommen wurden. Daher belassen wir die Default-Einstellungen und schließen den Dialog.

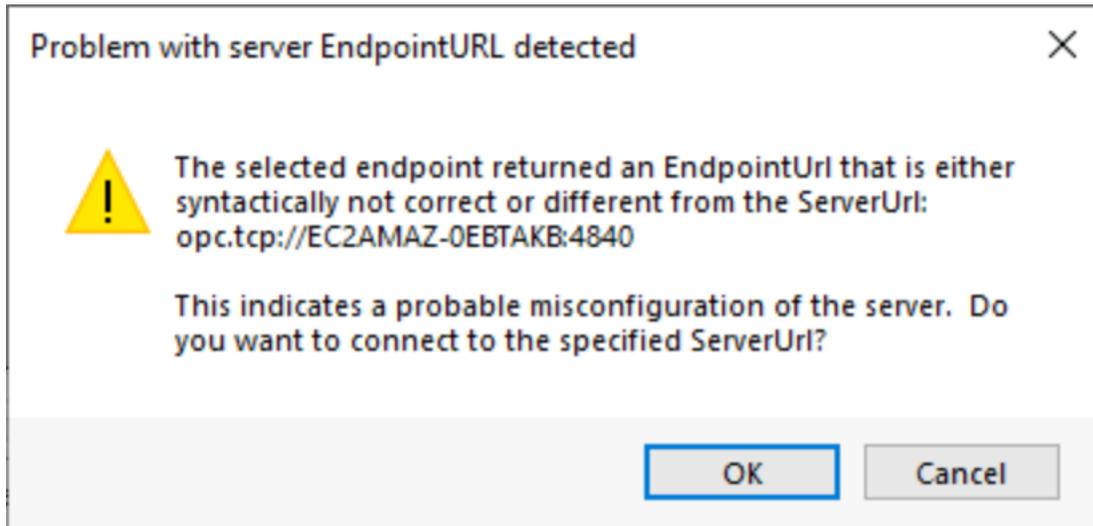
In der Server-Auswahlliste in der Toolbar finden Sie nun einen neuen Eintrag mit dem soeben konfigurierten Verbindungsprofil.



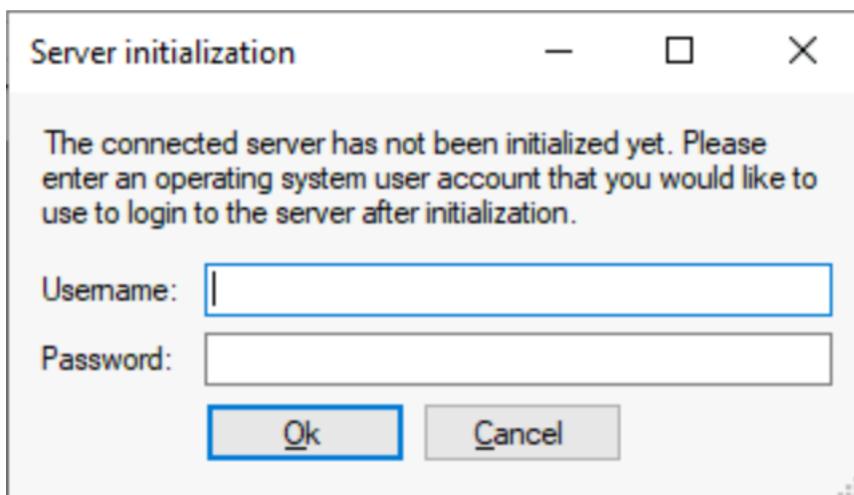
Verbinden mit dem Server und Auslesen der Konfiguration

- ✓ Zum Herstellen einer Verbindung mit dem Server stellen Sie sicher, dass der soeben konfigurierte Server selektiert ist.

1. Klicken Sie in der Toolbar auf **Connect**. Falls Sie einen Warnhinweis bzgl. einer abweichenden Server URL erhalten, bestätigen Sie diesen Dialog bitte mit **Ok**.



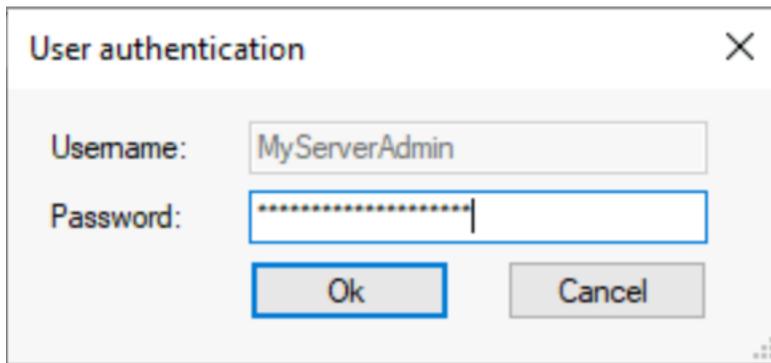
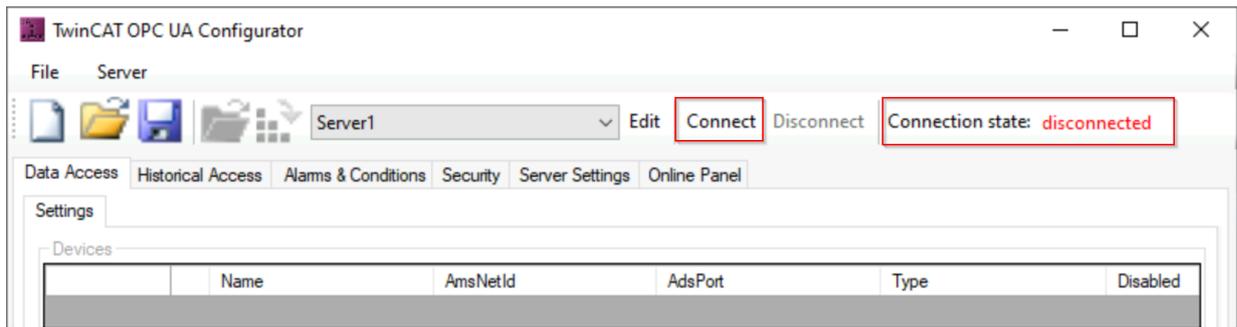
2. Da wir in diesem Tutorial von einer Neuinstallation ausgehen, d.h. sowohl der TwinCAT OPC UA Server als auch TwinCAT OPC UA Configurator werden erstmalig in Betrieb genommen, erkennt der Konfigurator nun, dass es sich bei dem Server um einen un-initialisierten Server im Auslieferungszustand handelt. Für weitere Informationen zum Initialisierungskonzept (auch TOFU Trust On First Use genannt) empfehlen wir Ihnen das zugehörige Dokumentationskapitel in der TwinCAT OPC UA Server Dokumentation.
3. Zur Initialisierung des Servers geben Sie nun eine Benutzername/Password-Kombination ein. Hierbei kann entweder ein im Betriebssystem existierender Benutzer oder auch ein neuer Benutzer verwendet werden, welcher dann im Betriebssystem automatisch angelegt wird.



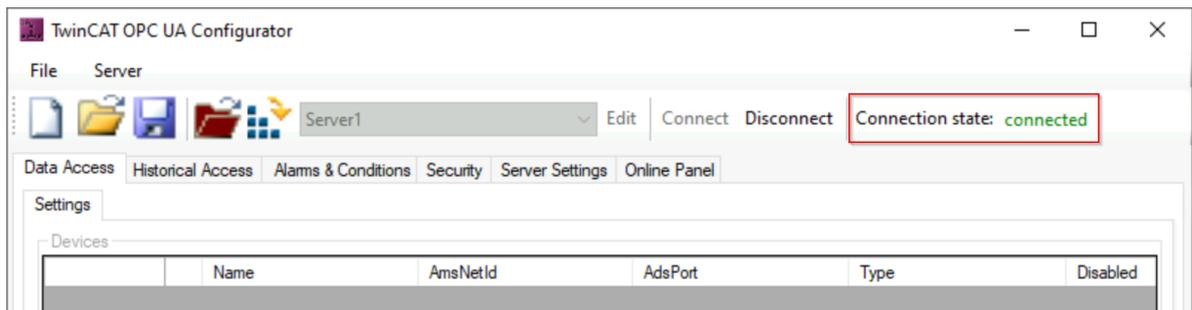
Bitte merken Sie sich die verwendete Benutzername/Password Kombination gut, da diese für den späteren Zugriff auf den Server über OPC UA benötigt wird.

⇒ Der Server wird nun initialisiert und neu gestartet.

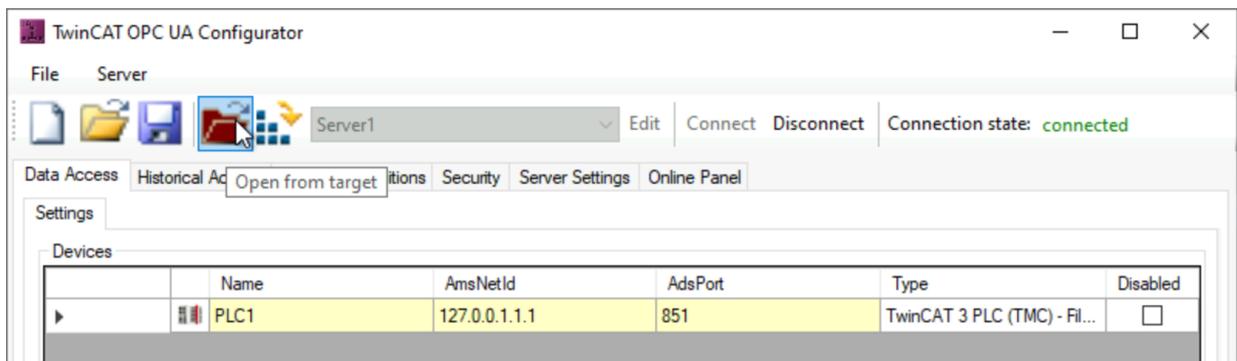
- Über die Toolbar können Sie nun erneut eine Verbindung zum Server herstellen. Der für die Initialisierung verwendete Benutzer wurde automatisch im Verbindungsprofil hinterlegt. Lediglich das Passwort muss bei einer Verbindung neu eingegeben werden.



⇒ Der **Connection State** wechselt nun zu „Connected“ (grün) und Sie sind mit dem Server verbunden.



- Sie können nun die Konfiguration des Servers auslesen, indem Sie den **Open from Target**-Button in der Toolbar klicken.

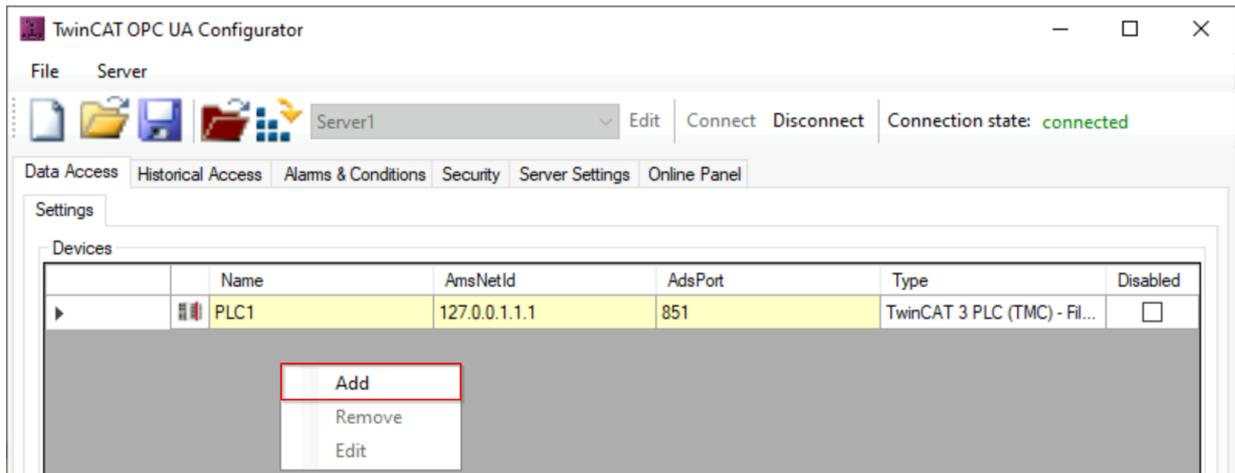


⇒ Die Konfiguration des Servers wird ausgelesen und in der Benutzeroberfläche des Konfigurators dargestellt.

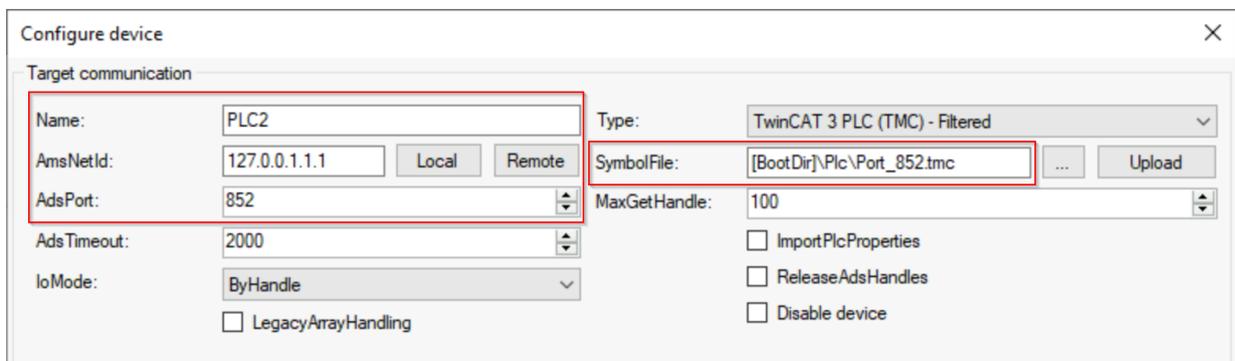
Durchführen von Änderungen an der Konfiguration

Sie können nun beliebige Änderungen an der Konfiguration durchführen. In diesem Beispiel wollen wir ein zusätzliches ADS-Gerät über den TwinCAT OPC UA Server verfügbar machen. Standardmäßig wird nur die erste, aus Sicht des Servers lokal laufende, SPS Runtime über OPC UA verfügbar gemacht. Diese mit „PLC1“ benannte SPS Runtime ist in der Registerkarte **Data Access** einsehbar.

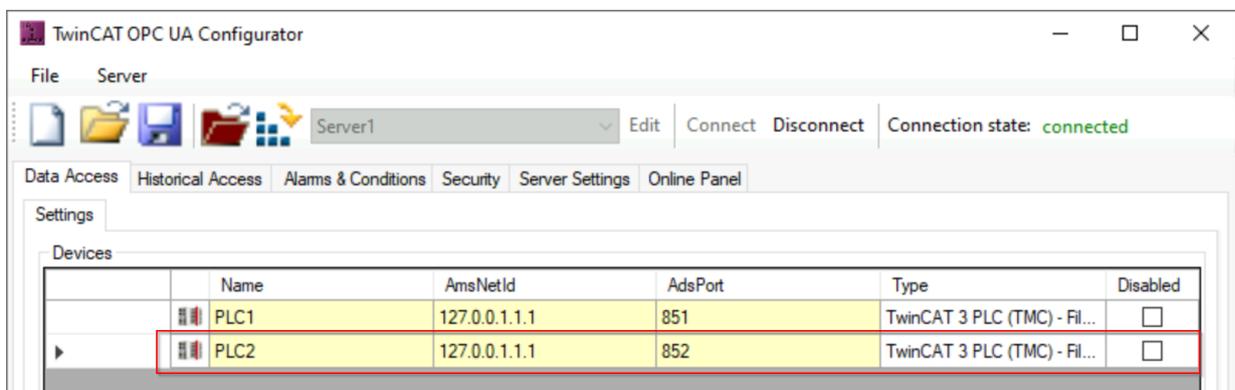
- Über das Kontextmenü fügen wir nun ein weiteres Data Access-Gerät hinzu.



- In den Geräteeigenschaften setzen wir die Parameter für **Name**, **AmsNetId**, **AdsPort** und **SymbolFile** auf die unten gezeigten Einstellungen und speichern diese Einstellungen über den **Ok**-Button.

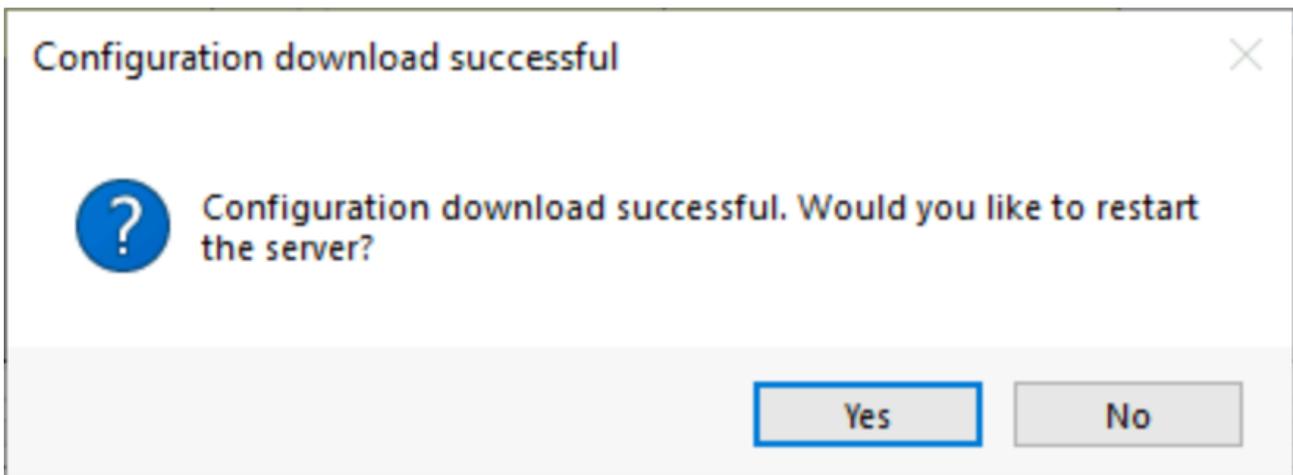


⇒ Wir haben nun ein zweites Data Access Gerät zu unserer Konfiguration hinzugefügt.

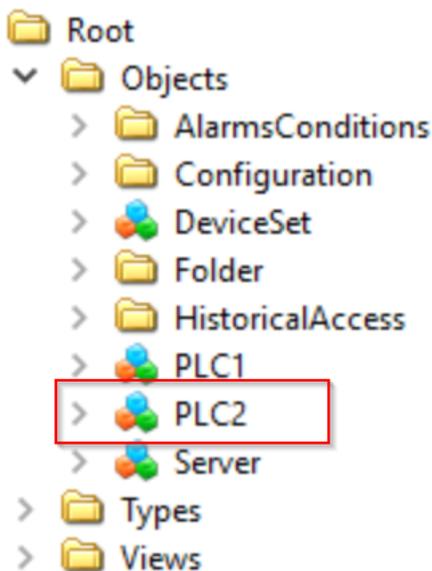


Aktivieren der neuen Konfiguration auf dem Server

Zum Abschluss müssen wir noch die Konfiguration auf den Server herunterladen. Hierzu können Sie den entsprechenden Button **Activate on Target** in der Toolbar verwenden. Ein abschließender Dialog informiert uns darüber, dass die Konfiguration erfolgreich auf den Server übertragen wurde und fragt, ob dieser neu gestartet werden soll. Dies bestätigen wir mit **Yes**.



Sie haben erfolgreich den TwinCAT OPC UA Configurator verwendet, um eine Konfigurationsänderung am TwinCAT OPC UA Server vorzunehmen. In diesem Beispiel haben wir ein zusätzliches Data Access Gerät zum Server hinzugefügt. Bei dem zusätzlichen Gerät handelt es sich um die zweite SPS Runtime auf dem lokalen System. Ein beliebiger OPC UA Client, der sich nun mit dem Server verbindet, findet diese zweite SPS Runtime nun unterhalb des Objekts „PLC2“ im Server-Adressraum wieder.



4.2 Applikationsverzeichnisse

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

Installationsverzeichnis

Das Basis-Installationsverzeichnis der Applikation ist 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\Configurator
```

Die Dateien des Visual Studio Konfigurators werden in folgendem Verzeichnis abgelegt:

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Configurator\Vsix
```

Zertifikatsverzeichnis

Zertifikatsdateien, welche zum Aufbau einer gesicherten Kommunikationsverbindung verwendet werden, werden in folgendem Verzeichnis abgelegt. Hierbei gibt es eine Unterscheidung zwischen Standalone und Visual Studio Konfigurator.

```
%ProgramData%\Beckhoff\TF6100-OPC-UA\TcOpcUaConfigurator\PKI
%ProgramData%\Beckhoff\TF6100-OPC-UA\TcOpcUaConfiguratorVs\PKI
```

Konfigurationsdateien

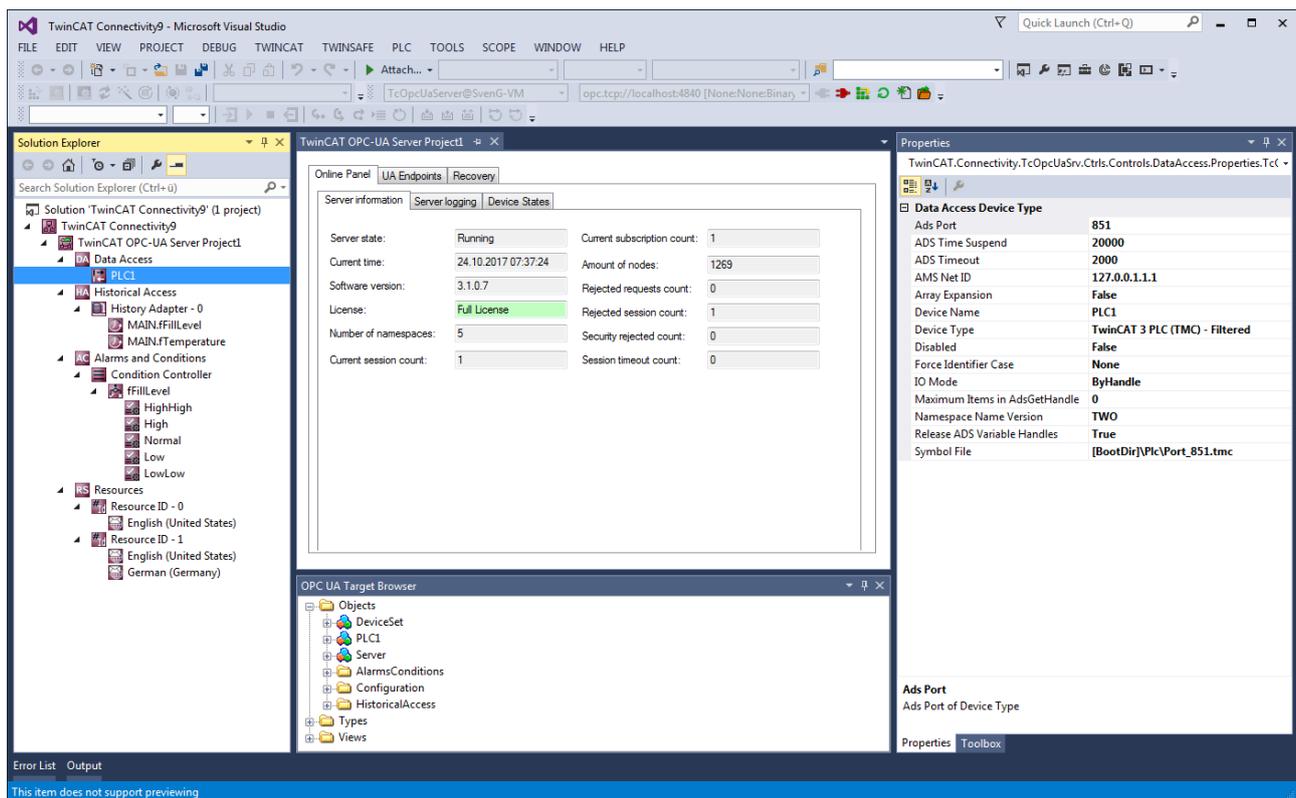
Sowohl der Standalone als auch der Visual Studio Konfigurator verwenden Konfigurationsdateien, z.B. für den Serverauswahldialog. Diese Konfigurationsdateien werden, abhängig vom Tool, in folgendem Verzeichnis abgelegt.

```
%ProgramData%\Beckhoff\TF6100-OPC-UA\TcOpcUaConfigurator
%ProgramData%\Beckhoff\TF6100-OPC-UA\TcOpcUaConfiguratorVs
```

4.3 Visual Studio

4.3.1 Übersicht

Das TF6100-Setup (Version 4.x.x und höher) beinhaltet die aktuellste Version des OPC-UA-Server-Konfigurators. Dieser wurde für ein durchgängiges und einheitliches Engineering-Konzept in Microsoft Visual Studio als eigener Projekttyp integriert. Sie können alle unterschiedlichen Facetten vom TwinCAT OPC UA Server konfigurieren und hierbei auch Source-Control-Mechanismen wie z. B. Team Foundation Server oder Subversion-Integrationen verwenden.



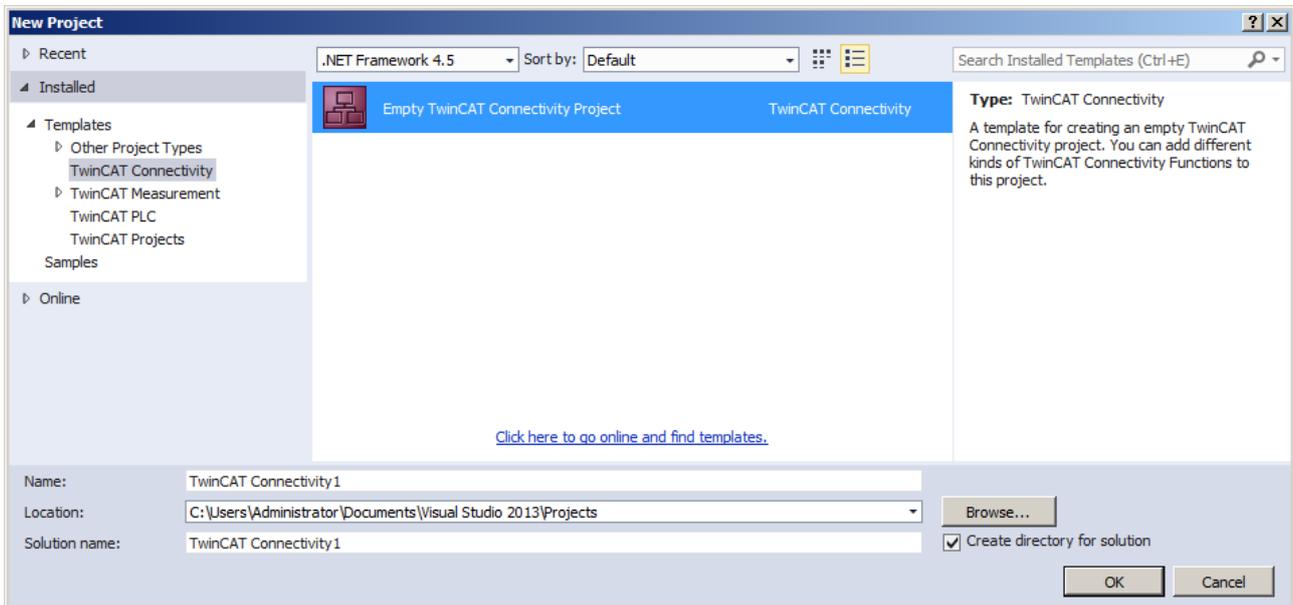
Voraussetzungen

| Produkte | Setup-Versionen | Zielplattform |
|----------|-----------------|-----------------------------|
| TF6100 | 4.x.x | IPC oder CX (x86, x64, ARM) |

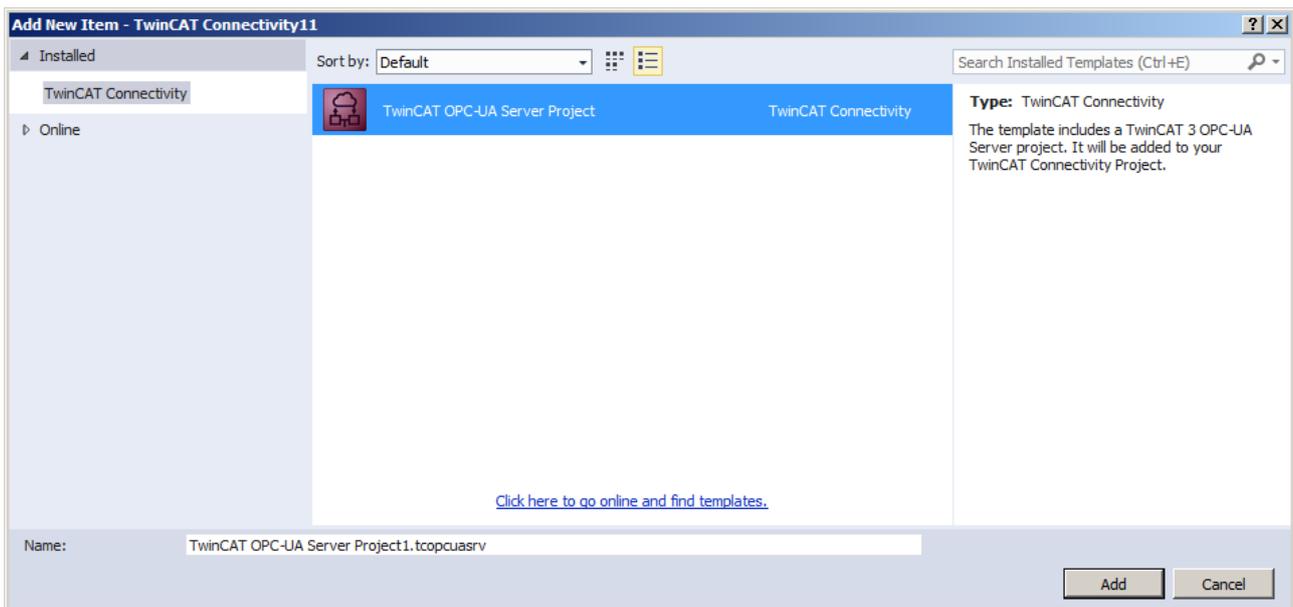
4.3.2 Neues Projekt anlegen

Das Projektpaket vom OPC-UA-Konfigurator bindet sich in das sogenannte Connectivity-Paket ein. Sie können dieses beim Anlegen eines neuen Visual-Studio-Projekts auswählen.

Projektvorlage „TwinCAT Connectivity Project“:



Projektvorlage „TwinCAT OPC-UA Server Project“:



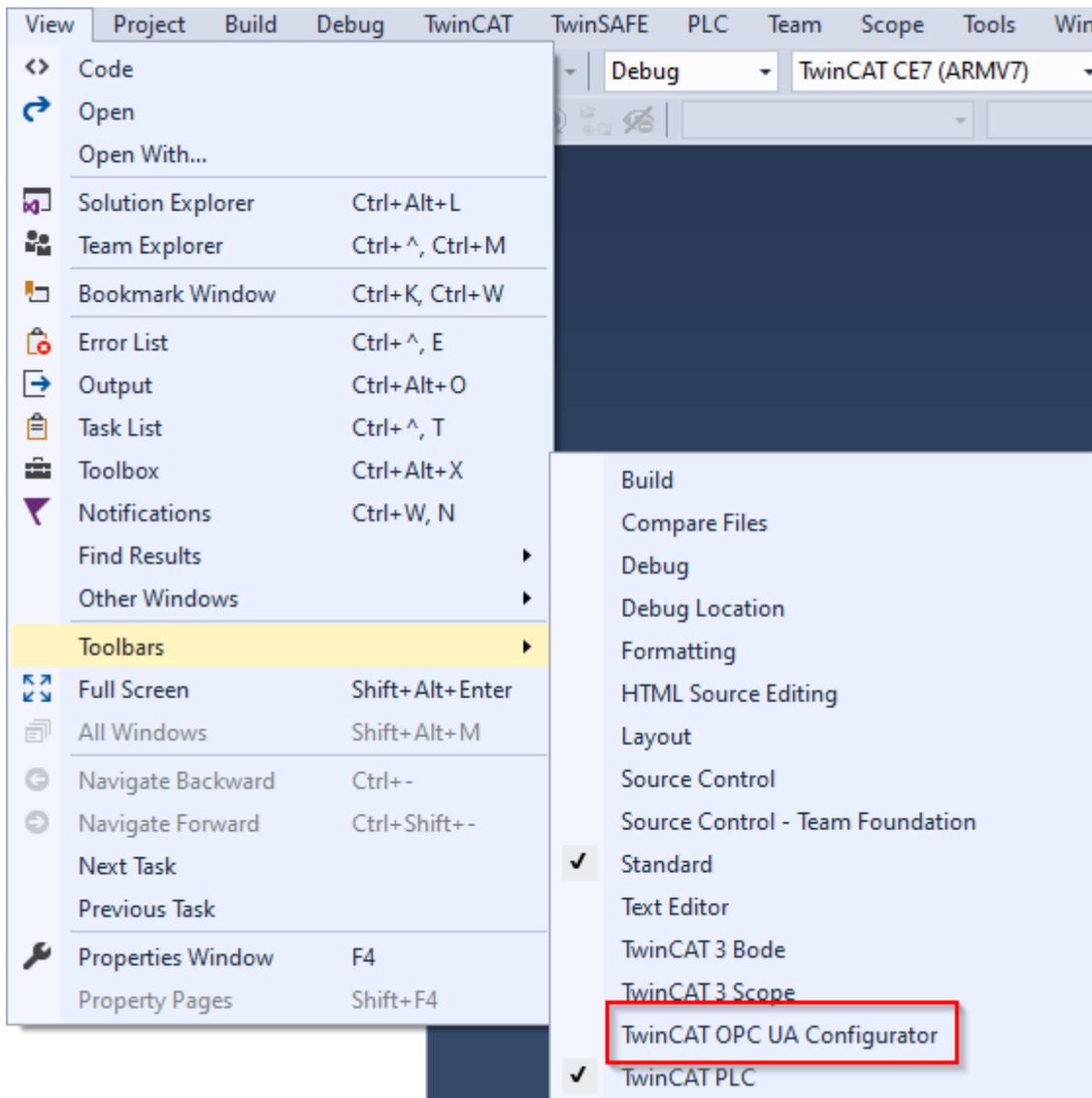
Voraussetzungen

| Produkte | Setup-Versionen | Zielplattform |
|----------|-----------------|-----------------------------|
| TF6100 | 4.x.x | IPC oder CX (x86, x64, ARM) |

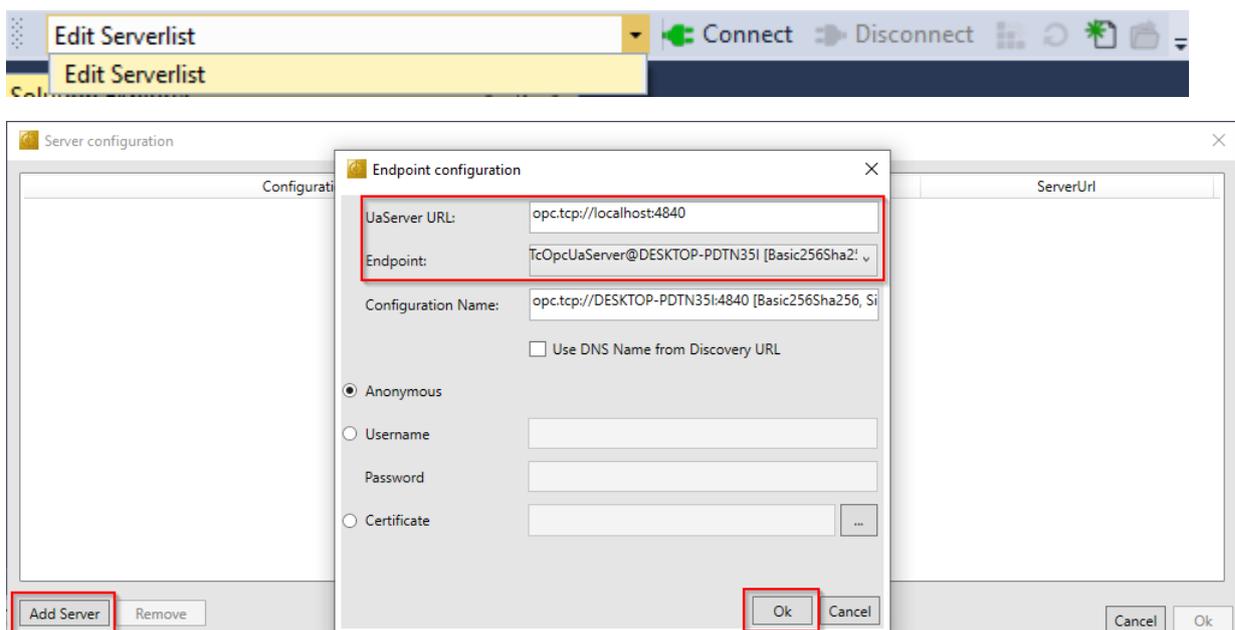
4.3.3 Verbinden mit einem Server

Der OPC-UA-Konfigurator ermöglicht die vollständige Parametrierung des Servers über OPC UA. Ähnlich wie im TwinCAT-XAE-System können Sie über die Symbolleiste einen OPC-UA-Server auswählen, mit dem Sie sich verbinden wollen.

1. Fügen Sie zunächst die entsprechende Toolbar zu Ihrer Visual Studio Oberfläche hinzu.

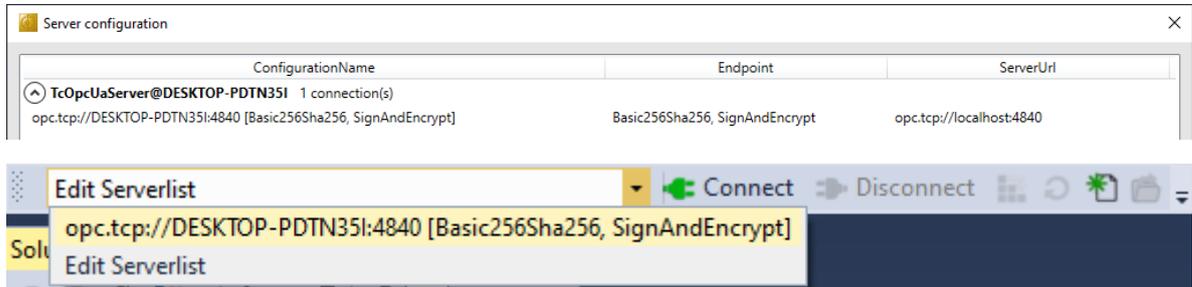


2. Anschließend fügen Sie über den Eintrag **Edit Serverlist** in der DropDownBox der Toolbar eine oder mehrere Serververbindungen hinzu.



3. Im Dialog **Endpoint configuration** nehmen Sie hierbei alle Einstellungen für die Verbindung mit dem Server vor, insbesondere die Server URL, die Auswahl eines vom Server angebotenen Endpunkts und optional auch das IdentityToken (z. B. Username/Password), mit dem sich der Konfigurator mit dem Server verbinden soll.

⇒ Die Server-Verbindung wird dann unter einem automatisch generierten Konfigurationsnamen zur Serverliste hinzugefügt und ist anschließend in der DropDownListe der Toolbar selektierbar.



⇒ Durch einen Klick auf den **Connect**-Button kann nun eine Verbindung mit dem Server hergestellt und dieser konfiguriert werden.

● Online-Konfiguration

I Sämtliche Einstellungen die Sie in Ihrem Projekt vornehmen, werden für den verbundenen TwinCAT OPC UA Server durchgeführt.

● Initialisierung des Servers

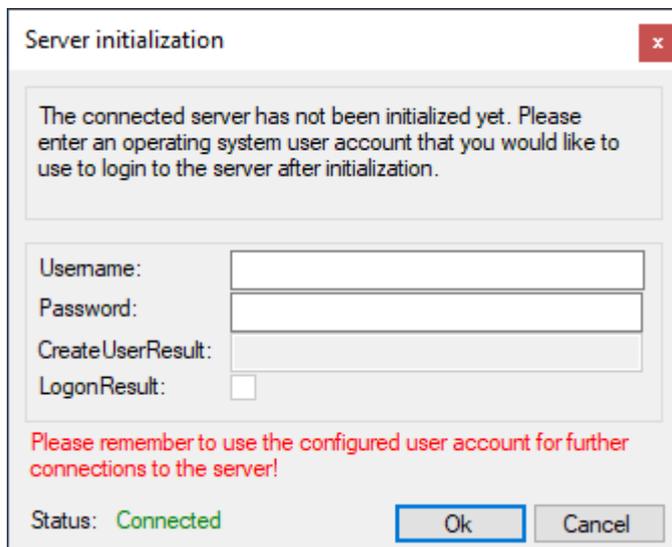
I Sollte sich der Server noch im (uninitialisierten) Auslieferungszustand befinden, so erhalten Sie einen entsprechenden Hinweis zur Server-Initialisierung. Dieser Vorgang ist im Kapitel zur Durchführung der Server-Initialisierung [▶ 23] näher beschrieben.

Voraussetzungen

| Produkte | Setup-Versionen | Zielplattform |
|----------|-----------------|-----------------------------|
| TF6100 | 4.x.x | IPC oder CX (x86, x64, ARM) |

4.3.4 Durchführen der Server-Initialisierung

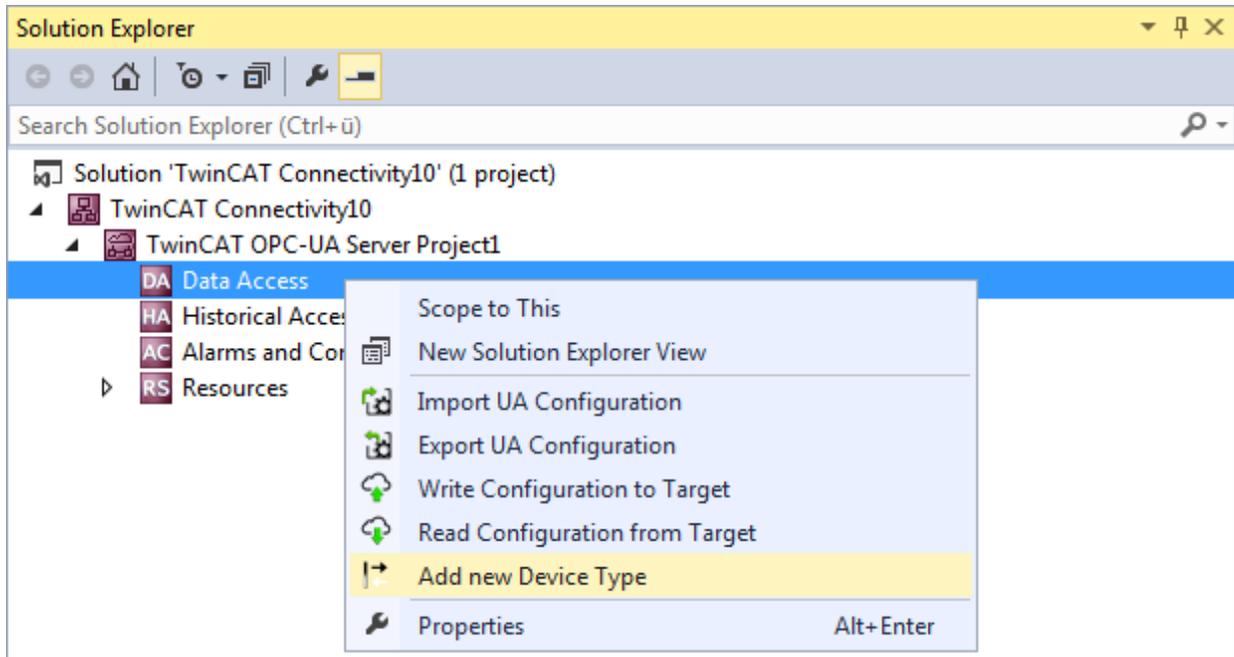
Der TwinCAT OPC UA Server wird in einem uninitialisierten Modus ausgeliefert, welcher auf dem sogenannten TOFU (Trust-On-First-Use) Prinzip begründet ist. Detaillierte Informationen zu diesem Server-Feature und die entsprechenden Hintergrundinformationen finden Sie hier. Der TwinCAT OPC UA Configurator ermöglicht die Initialisierung des Servers beim ersten Verbindungsaufbau. Ein entsprechender Warnhinweis weist auf den uninitialisierten Server hin und ermöglicht eine entsprechende Initialisierung.



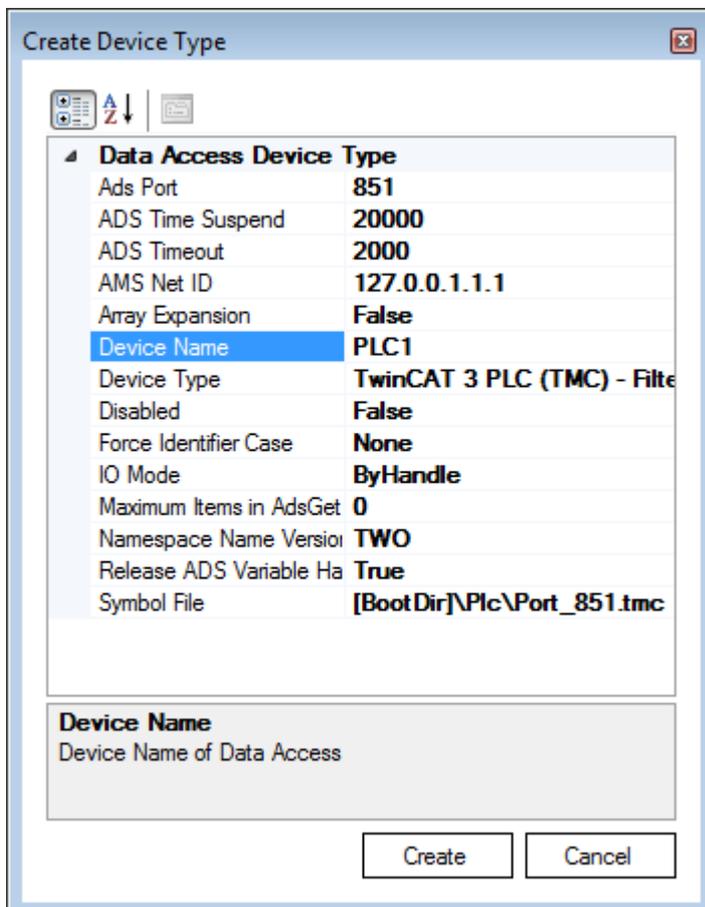
4.3.5 ADS-Geräte hinzufügen

Der OPC UA Server kann mit einem oder mehreren ADS-Geräten „sprechen“. Zur Herstellung einer Verbindung ist eine Route zu dem jeweiligen ADS-Gerät erforderlich. Im OPC-UA-Konfigurator werden ADS-Geräte in der Facette **Data Access** angelegt, konfiguriert und somit dem OPC UA Server bekannt gegeben.

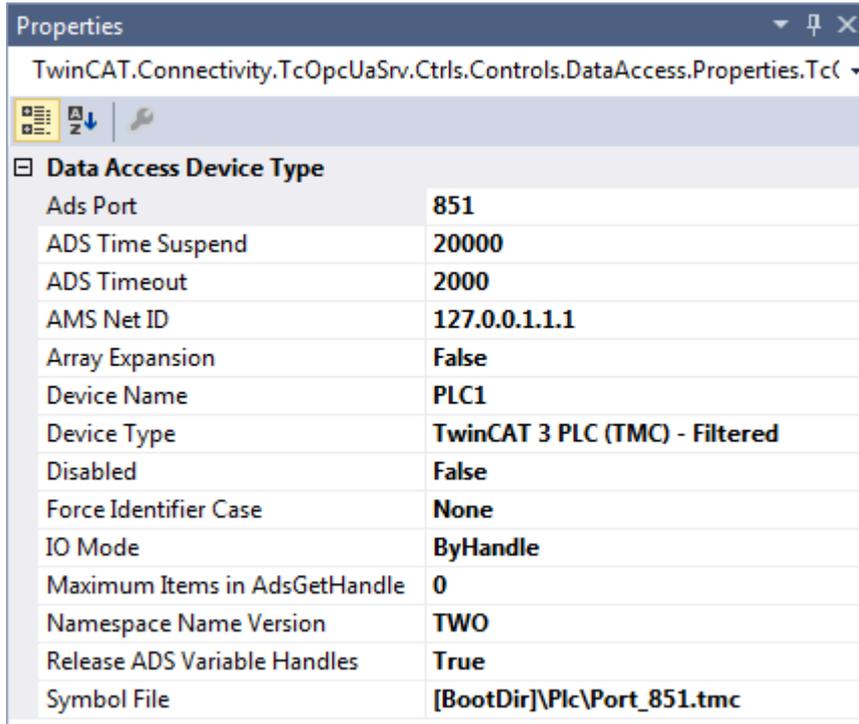
1. Neue ADS-Geräte fügen Sie der Konfiguration über den Kontextmenübefehl **Add new Device Type** hinzu.



2. Nach Ausführung des Befehls öffnet sich ein Dialogfenster, in dem Sie die Verbindungsparameter für dieses Gerät konfigurieren können, z. B. AMS Net ID, ADS-Port oder auch die Symboldatei.

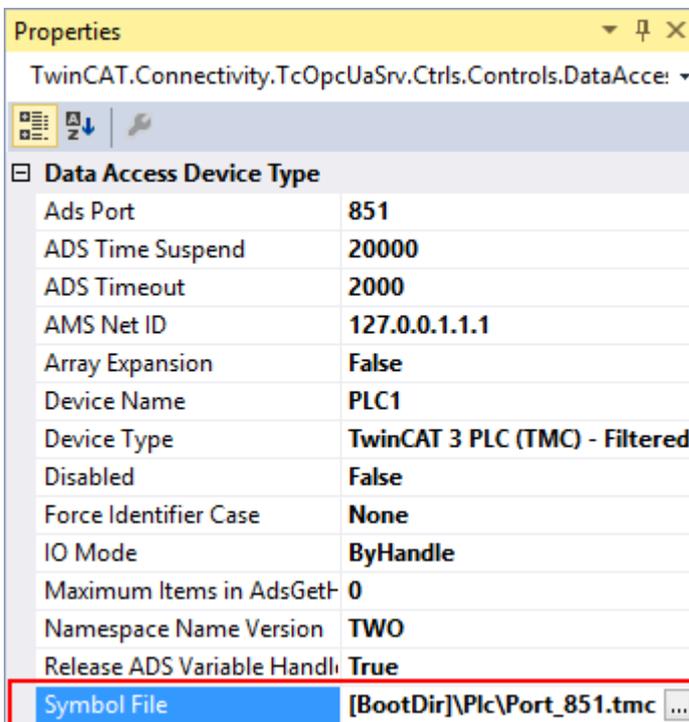


- Die Verbindungsparameter können Sie bei Bedarf nachträglich über das Eigenschaftfenster von Visual Studio modifizieren.

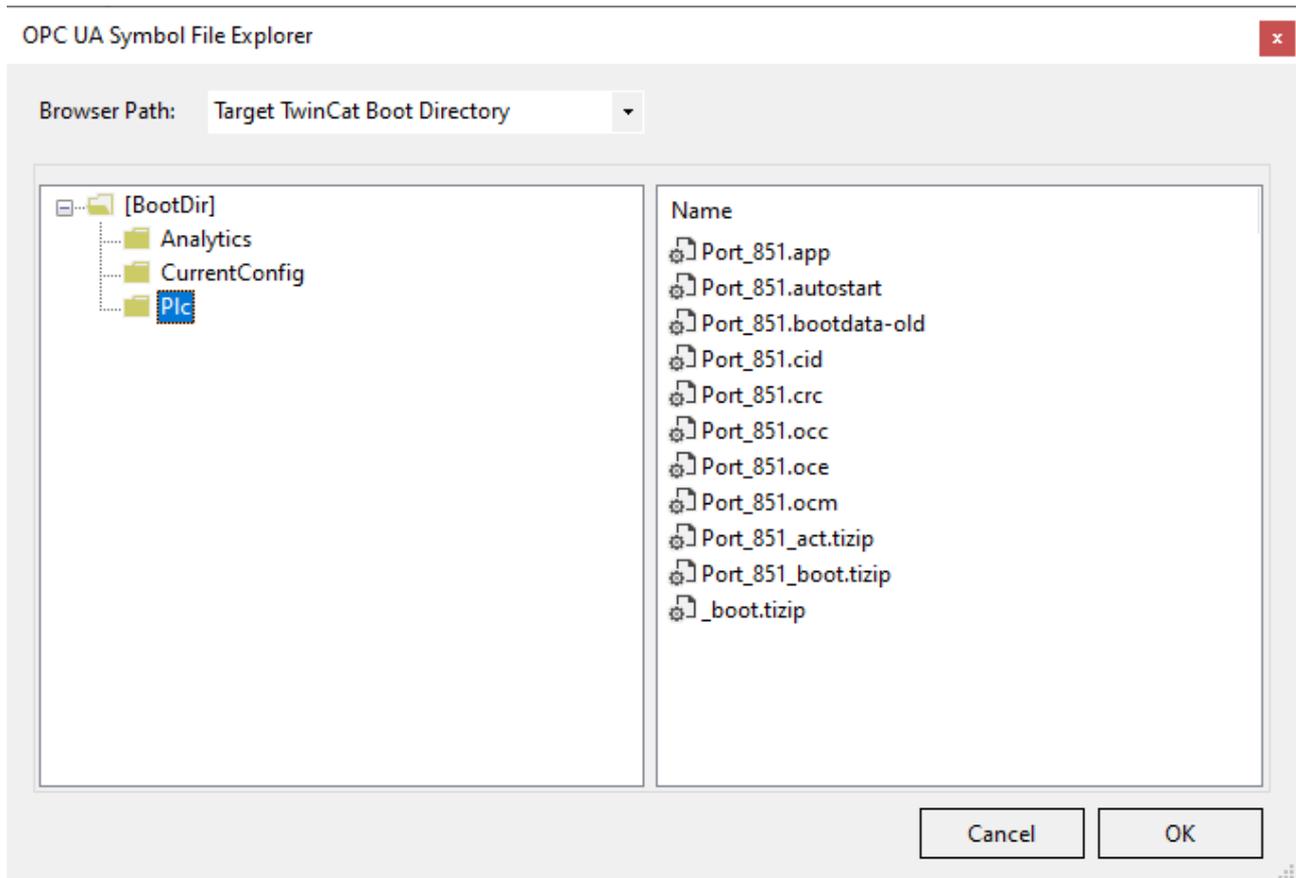


Symboldatei auswählen

Auf dem ausgewählten Zielgerät vorhandene Symboldateien können direkt eingelesen werden. Die Symboldateien können dabei entweder im TwinCAT-Bootverzeichnis oder im Symbolverzeichnis des OPC UA Servers hinterlegt sein. Über den entsprechenden Dialog bei der Symboldatei-Konfiguration können Sie die Dateien selektieren.



Der TwinCAT OPC UA File Explorer kann entweder mit dem lokalen TwinCAT-Verzeichnis oder dem Remote-Bootverzeichnis verbunden werden. Letzteres wird über den Configuration-namespace des Servers eingelesen (siehe Konfiguration des Namensraums).



Voraussetzungen

| Produkte | Setup-Versionen | Zielplattform |
|----------|-----------------|-----------------------------|
| TF6100 | 4.x.x | IPC oder CX (x86, x64, ARM) |

4.3.6 Konfiguration lesen und schreiben

Über den Konfigurator können Sie sowohl den Download/Upload von kompletten Server-Konfigurationen anstoßen als auch jede einzelne Facette (Data Access, Historical Access, etc.) einzeln auf ein Zielgerät aufspielen bzw. von dort öffnen. Die hierfür notwendigen Funktionen sind sowohl in die Symbolleiste als auch in das Kontextmenü der jeweiligen Facette eingebunden.

Konfiguration vom Zielgerät öffnen

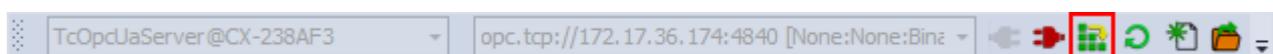
Über die entsprechende Schaltfläche in der Symbolleisten öffnen Sie die Konfiguration des selektierten Zielgeräts.



Siehe auch: [Verbinden mit einem Server](#) [▶ 21]

Konfiguration auf einem Zielgerät aktivieren

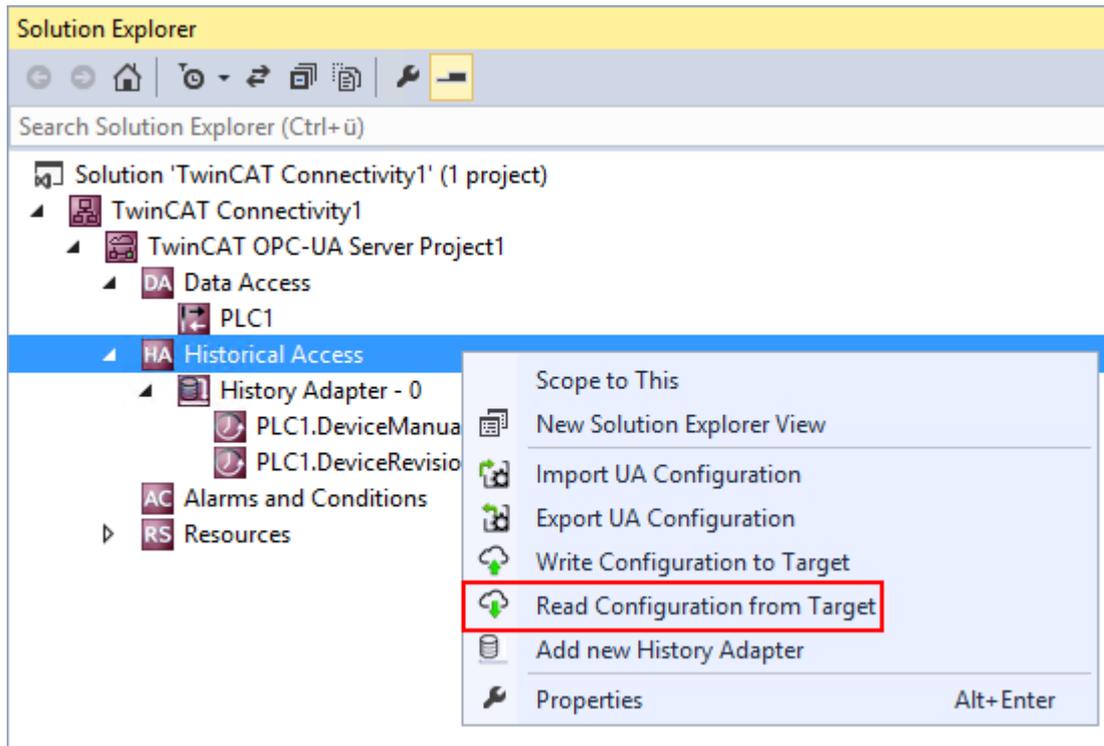
Über die entsprechende Schaltfläche in der Symbolleiste laden Sie die aktuell geöffnete Konfiguration auf das selektierte Zielgerät herunter.



Siehe auch: [Verbinden mit einem Server](#) [▶ 21]

Teilkonfiguration öffnen

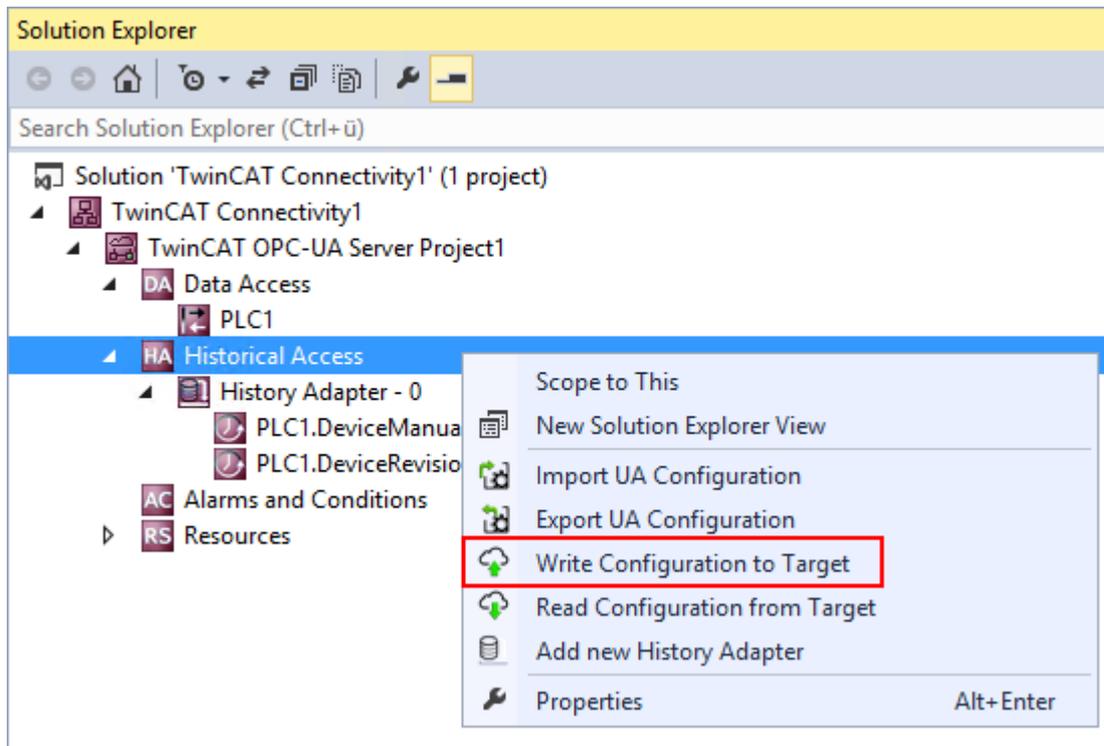
Über den Befehl **Read Configuration from Target** im Kontextmenü einer bestimmten Facette der Konfiguration öffnen Sie die Teilkonfiguration vom selektierten Zielgerät.



Siehe auch: [Verbinden mit einem Server](#) [▶ 21]

Teilkonfiguration herunterladen

Über den Befehl **Write Configuration to Target** im Kontextmenü einer bestimmten Facette der Konfiguration laden Sie die Teilkonfiguration auf das selektierte Zielgerät herunter.



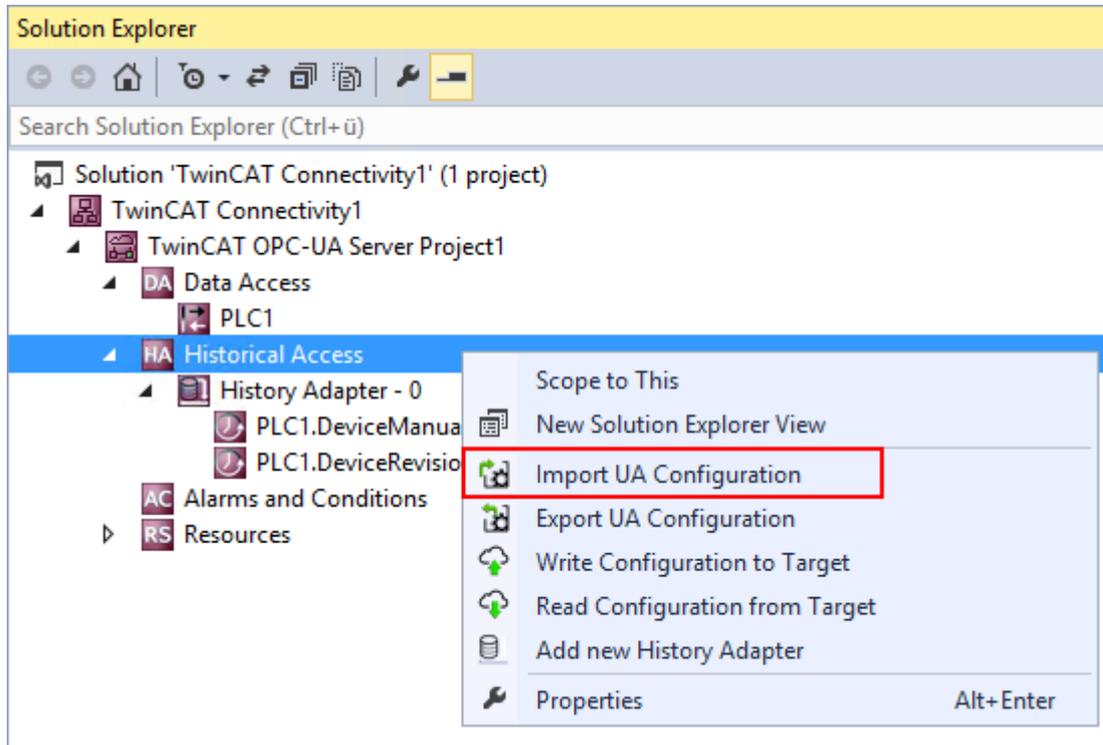
Siehe auch: [Verbinden mit einem Server](#) [▶ 21]

4.3.7 Konfigurationsdateien importieren und exportieren

Die Befehle des Kontextmenüs ermöglichen den Import/Export von Konfigurationsdateien des OPC UA Servers.

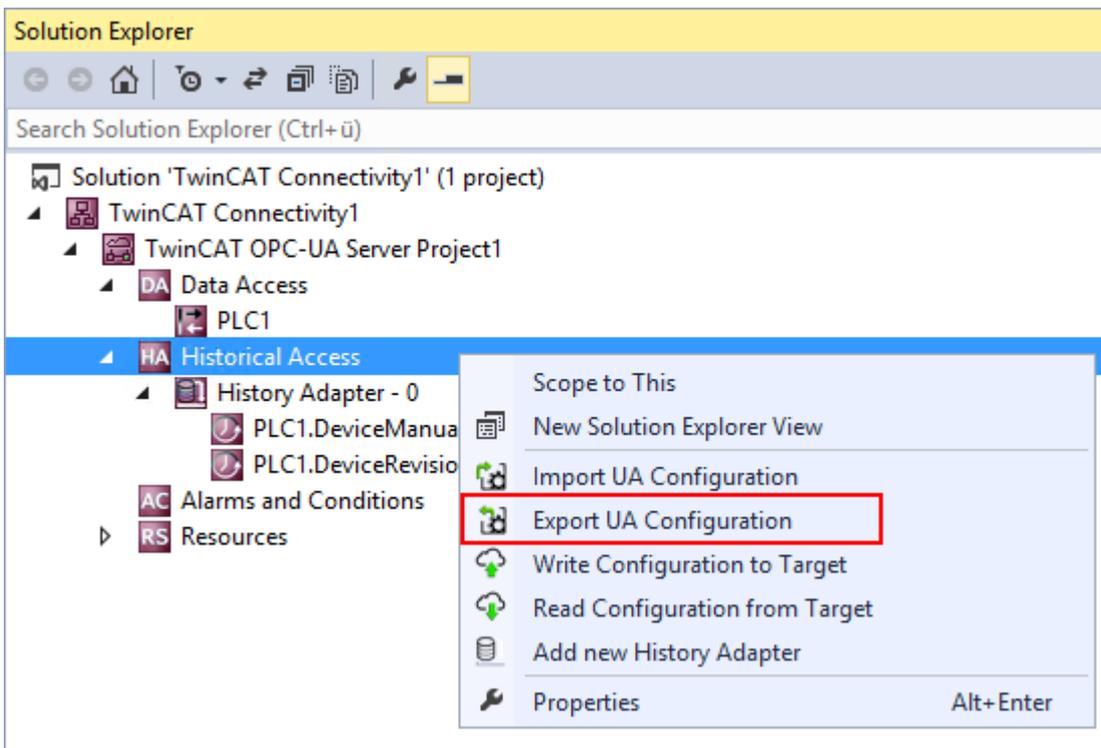
Teilkonfiguration importieren

Über den Befehl **Import UA Configuration** im Kontextmenü einer bestimmten Facette der Konfiguration importieren Sie die Teilkonfiguration (z. B. Historical Access) aus einer XML-Konfigurationsdatei.



Teilkonfiguration exportieren

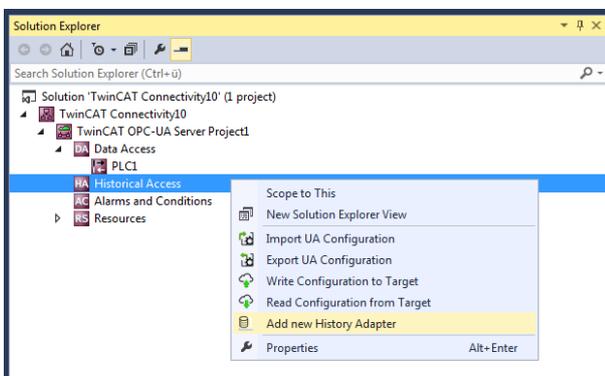
Über den Befehl **Export UA Configuration** im Kontextmenü einer bestimmten Facette der Konfiguration exportieren Sie die Teilkonfiguration (z. B. Historical Access) in eine XML-Konfigurationsdatei.



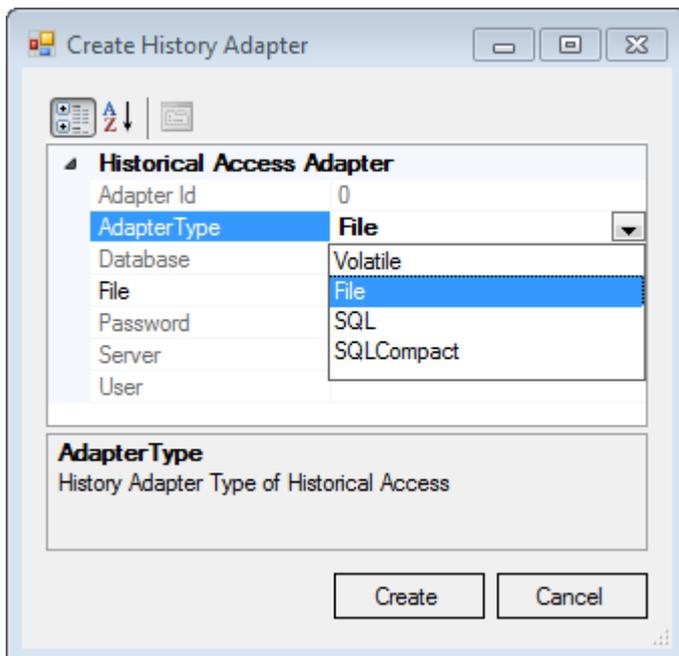
4.3.8 Historical Access konfigurieren

Zur Konfiguration von Historical Access müssen zunächst die History Adapter eingerichtet werden. Hierbei handelt es sich um die unterschiedlichen Speicherorte für die historischen Daten, z. B. RAM, Datei, SQL Server.

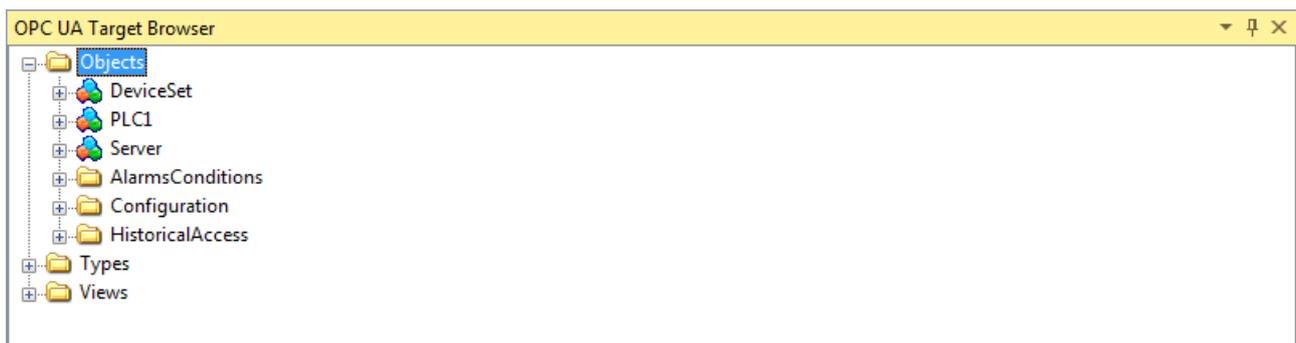
History Adapter fügen Sie der Konfiguration über den Kontextmenübefehl **Add new History Adapter** hinzu.



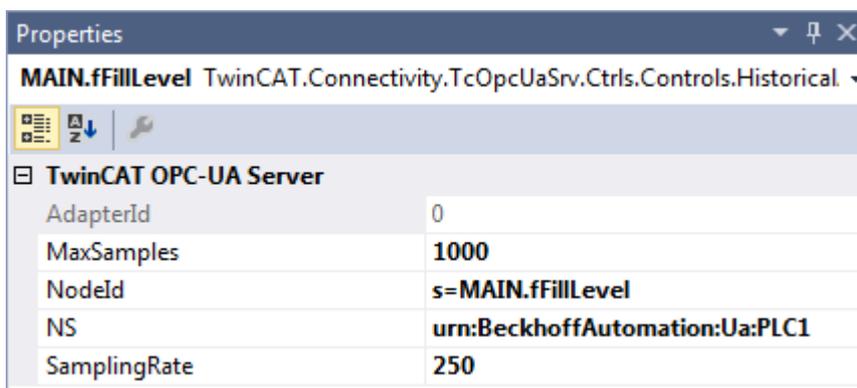
Je nach Adaptertyp müssen Sie weitere Parameter spezifizieren, z. B. den gewünschten Pfad zur Dateiablage oder die Zugangsdaten zum SQL-Server.



Nachdem Sie einen History Adapter angelegt haben, fügen Sie dem Adapter die gewünschten Variablen hinzu. Die Variablen müssen zum Zeitpunkt des Engineerings bereits auf dem selektierten OPC UA Server vorliegen. Zur Selektion der Variablen können Sie den integrierten **OPC UA Target Browser** verwenden und die Variablen aus dem Target Browser per Drag-and-drop zum History Adapter hinzufügen.



Im Eigenschaftensfenster der neu hinzugefügten Variable spezifizieren Sie weitere Parameter, z. B. die gewünschte SamplingRate oder die Größe des zu verwendenden Ringbuffers im History Adapter.

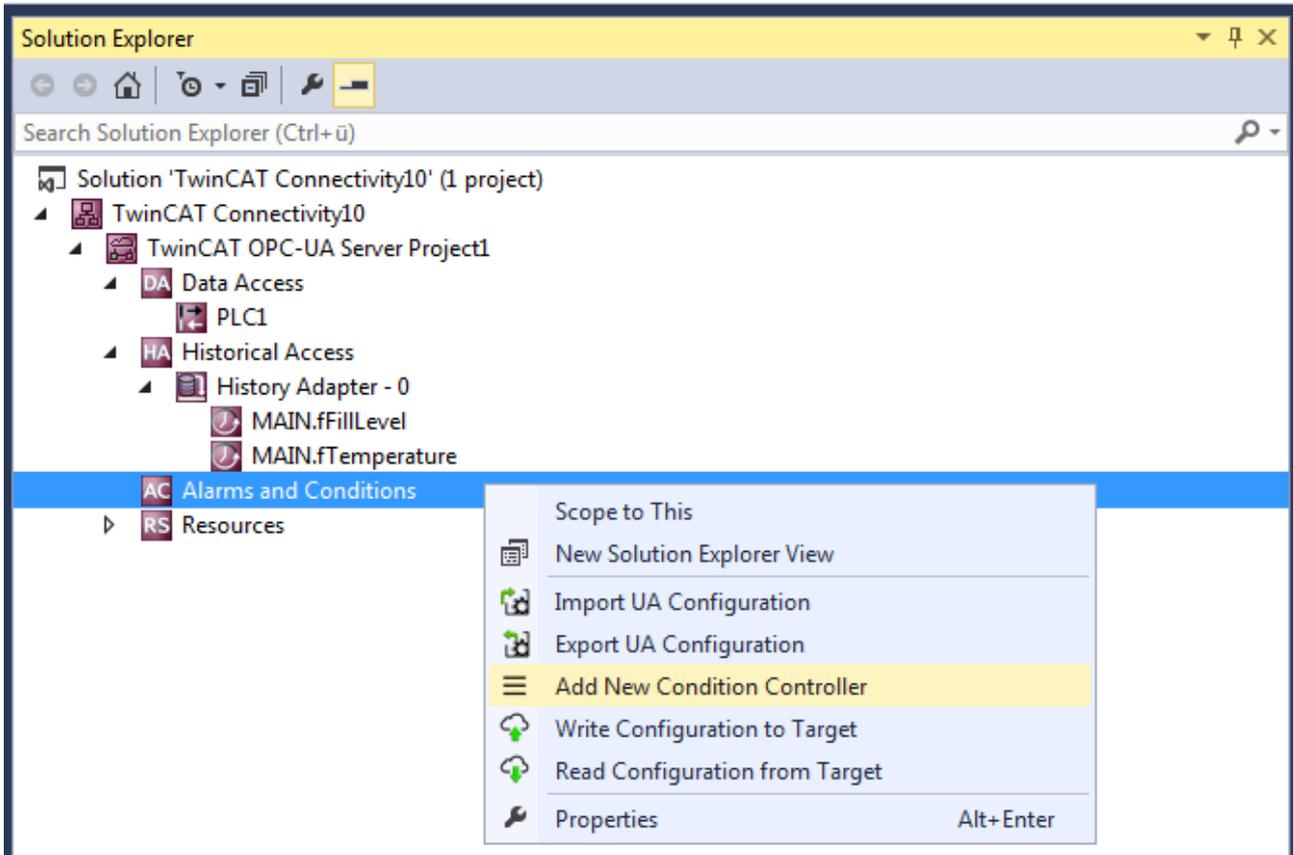


Siehe auch: [Verbinden mit einem Server](#) [► 21]

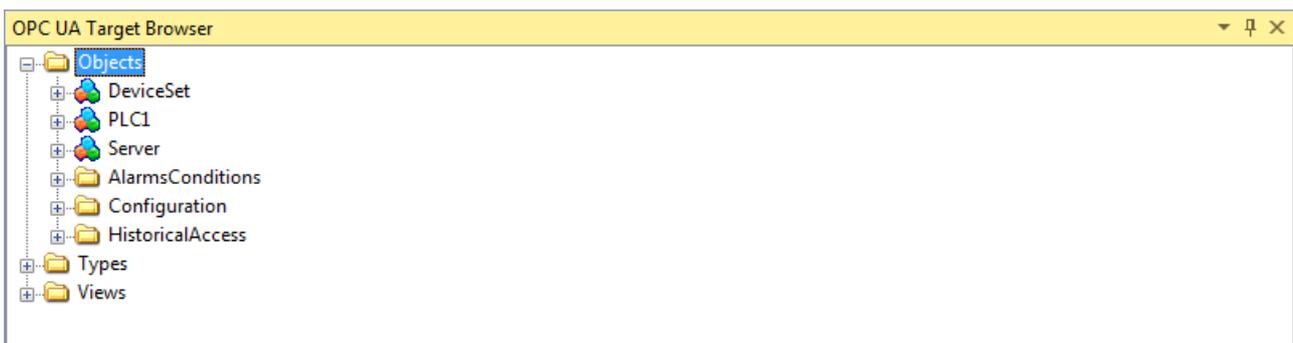
4.3.9 Alarms and Conditions konfigurieren

Zur Konfiguration von Alarms and Conditions (A&C) müssen zunächst die Condition Controller eingerichtet werden. Hierbei handelt es sich um Container-Einheiten, die Alarmer grupieren.

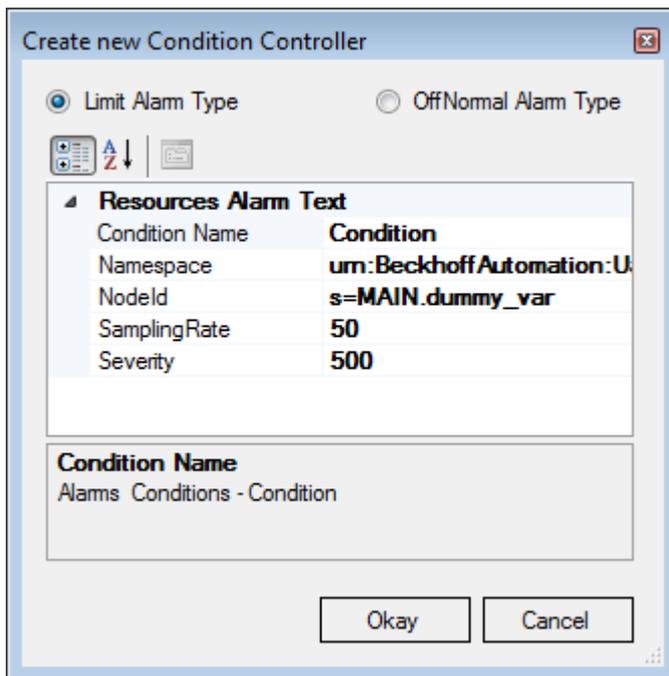
Condition Controller fügen Sie der Konfiguration über den Kontextmenübefehl **Add New Condition Controller** hinzu.



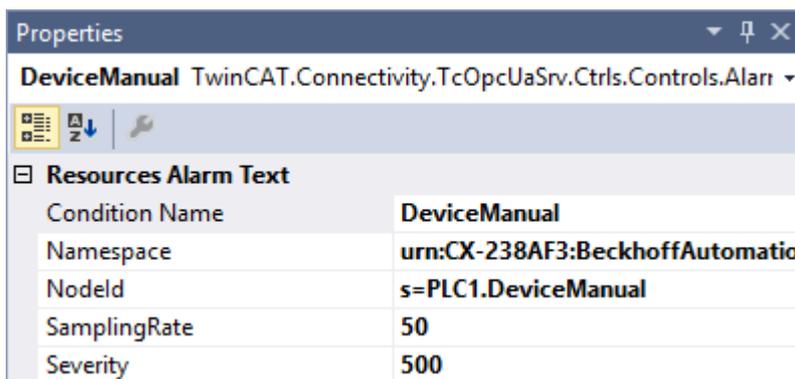
Nachdem Sie einen Condition Controller angelegt haben, fügen Sie dem Controller die gewünschten Variablen hinzu und überwachen sie im Sinne des Alarms and Conditions. Für jede Variable wird hierbei eine Condition angelegt, welche die Parameter für die Überwachung spezifiziert. Die Variablen müssen zum Zeitpunkt des Engineerings bereits auf dem selektierten OPC UA Server vorliegen. Zur Selektion der Variablen verwenden Sie den integrierten **OPC UA Target Browser** und fügen die Variablen aus dem Target Browser per Drag-and-drop zum Condition Controller hinzu.



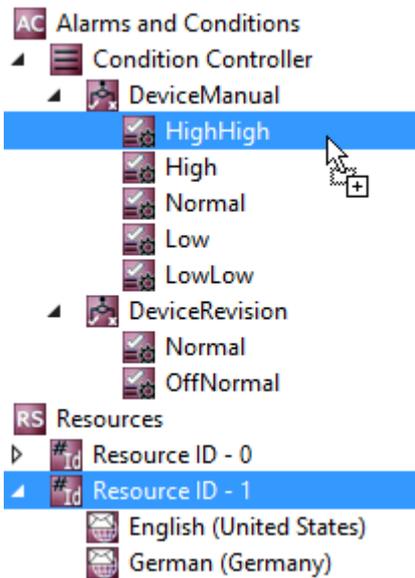
In dem sich öffnenden Dialogfenster definieren Sie den Condition-Typ und weitere Parameter für die Überwachung, z. B. SamplingRate und Severity.



Je nach ausgewähltem Condition-Typ spezifizieren Sie zusätzliche Parameter im Eigenschaftfenster der Condition. Die Schwellenwerte für den jeweiligen Condition-Typ werden als einzelne Einträge in der Baumansicht der Konfiguration angezeigt. Auch hier konfigurieren Sie die entsprechenden Parameter im Eigenschaftfenster.



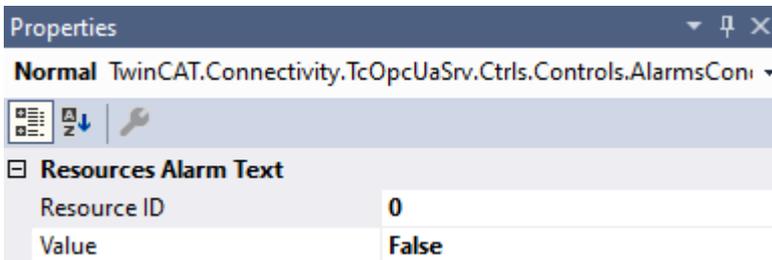
Anschließend müssen Sie die Alarmtexte definieren, die beim Triggern einer Condition an den OPC UA Client versendet werden sollen. Wie Sie Alarmtexte anlegen, wird im Kapitel [Alarmtexte konfigurieren](#) (► 34) beschrieben. Die Alarmtexte ziehen Sie per Drag-and-drop auf den jeweiligen Schwellenwert einer Condition.



Alarmtyp OffNormal

Bei einem Alarmtyp OffNormal definieren Sie, welcher Zustand einer Boolean-Variablen als Normal gewertet wird. Wenn der Variablenwert hiervon abweicht, wird ein Alarm ausgelöst. Für das Arbeiten mit Wertebereichen (bspw. Integer- oder Double-Variablen) muss die SPS verwendet werden. Dort wird dann je nach Wert ein entsprechender TRUE oder FALSE-Zustand an den OPC UA-Server weitergegeben.

| Zustand | Wertebereich |
|-----------|--|
| Normal | TRUE oder FALSE, je nach Entscheidung des Benutzers. |
| OffNormal | TRUE oder FALSE, je nach Konfiguration des Normal-Zustands. Kann nicht durch den Benutzer konfiguriert werden. |

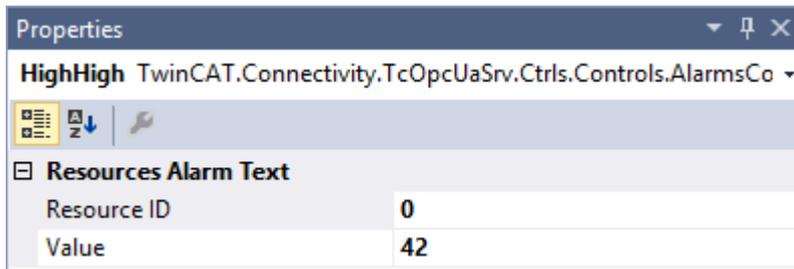


Im ersten Schritt wird - wie oben beschrieben - der Normalzustand konfiguriert. Anschließend definiert der Benutzer für den jeweiligen Zustand (OffNormal und Normal) einen Alarm-Text über die Resources. Das geschieht entweder per Drag-and-drop oder per Auswahl in der Dropdown-Liste **Resource ID**.

Alarmtyp Limit

Bei einem Alarmtyp Limit definieren Sie unterschiedliche Schwellenwerte, bei deren Erreichen ein Alarm verschickt werden soll. Die folgende Tabelle beschreibt die verschiedenen Schwellenwerte anhand einer Beispielkonfiguration.

| Zustand | Beispiel-Schwellenwerte | Zugehöriger Wertebereich (INT) |
|----------|-------------------------|--------------------------------|
| HighHigh | 5000 | 5000-32767 |
| High | 2000 | 2000-4999 |
| Normal | - | 1000-1999 |
| Low | 1000 | 500-999 |
| LowLow | 500 | -32768-499 |



Im ersten Schritt werden - wie oben beschrieben - die verschiedenen Schwellwerte konfiguriert. Anschließend definiert der Benutzer für den jeweiligen Zustand (HighHigh, High, Normal, Low, LowLow) einen Alarm-Text über die Resources. Das geschieht entweder per Drag-and-drop oder per Auswahl in der Dropdown-Liste **Resource ID**.

Voraussetzungen

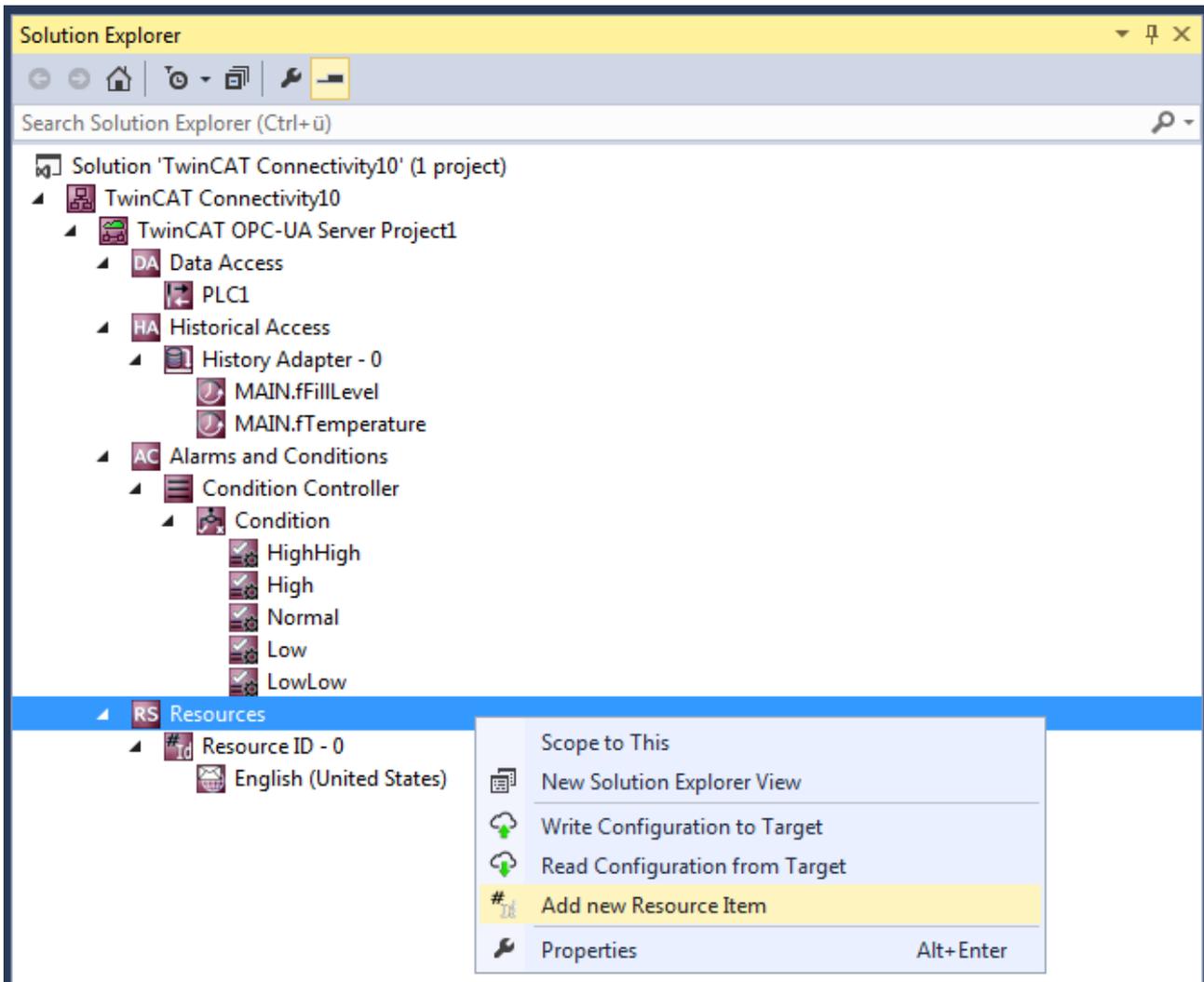
| Produkte | Setup-Versionen | Zielplattform |
|----------|-----------------|-----------------------------|
| TF6100 | 4.x.x | IPC oder CX (x86, x64, ARM) |

Siehe auch: [Verbinden mit einem Server](#) [▶ 21]

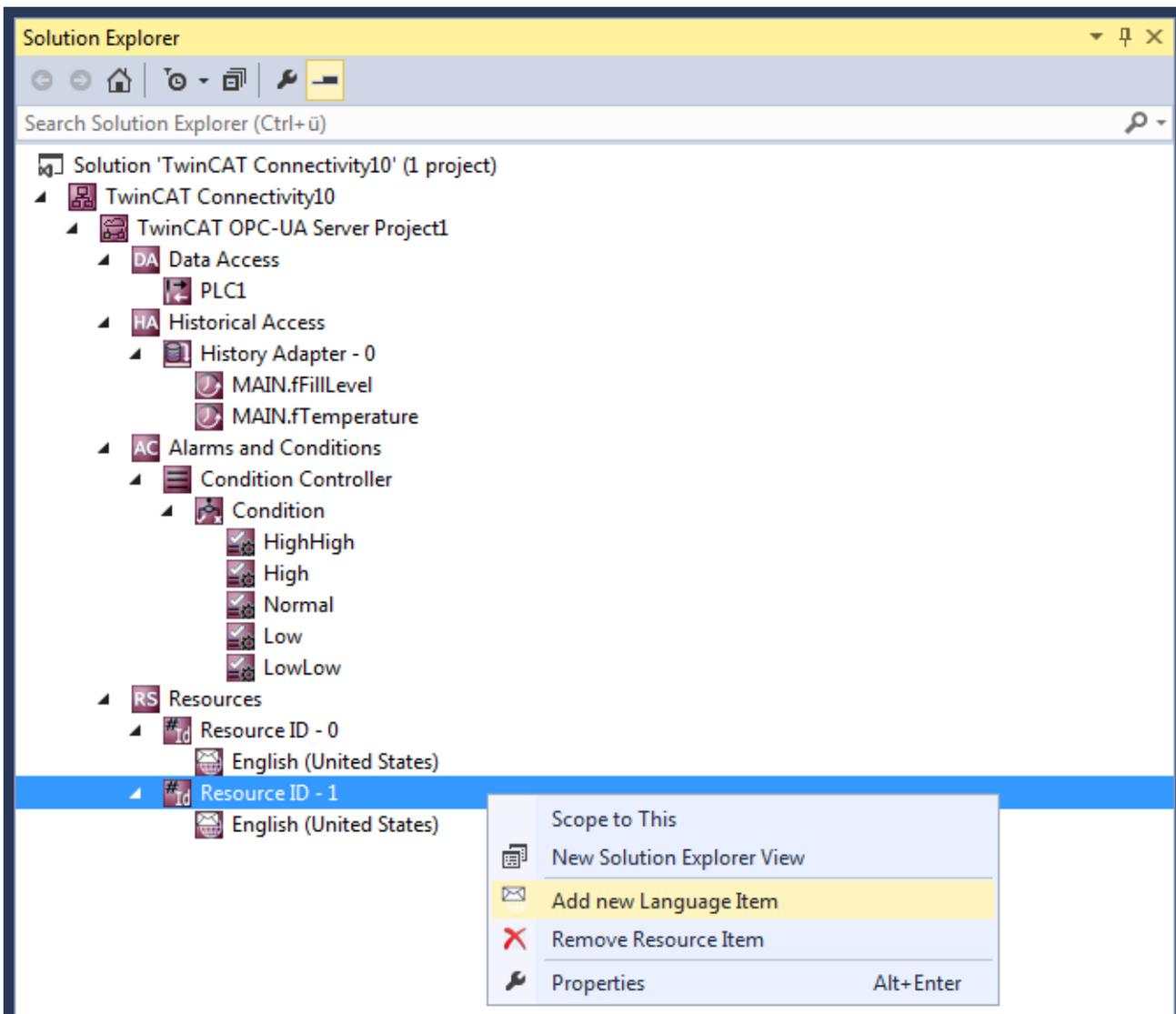
4.3.10 Alarmtexte konfigurieren

Der OPC-UA-Konfigurator ermöglicht die (mehrsprachige) Verwaltung von Alarmtexten, die zum Beispiel beim [Alarms and Conditions](#) [▶ 30] verwendet werden. Die Konfiguration der Alarmtexte erfolgt in der Facette **Resources**. Jeder Alarmtext wird durch eine eindeutige ID identifiziert. Dieser ID können dann mehrere Sprachtexte zugeordnet werden.

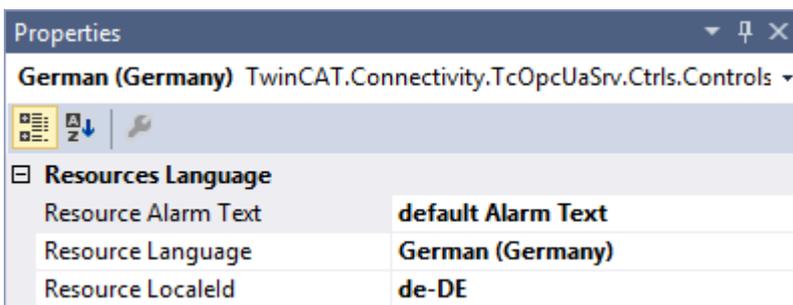
Über den Befehl **Add new Resource Item** im Kontextmenü können Sie Resource Items anlegen.



Über den Befehl **Add new Language Item** im Kontextmenü eines Resource Items fügen Sie diesem neue Sprachelemente (Language Items) hinzu.



Im Eigenschaftfenster können Sie ein Sprachelement weiter parametrieren, z. B. den Sprachtext und die zugeordnete Sprache. Wenn Sie die Sprache festlegen, wird automatisch die zugehörige LocaleID gesetzt. Die LocaleID wird vom OPC UA Client angefordert, um anzugeben, in welcher Sprache er Alarmtexte erwartet.



Voraussetzungen

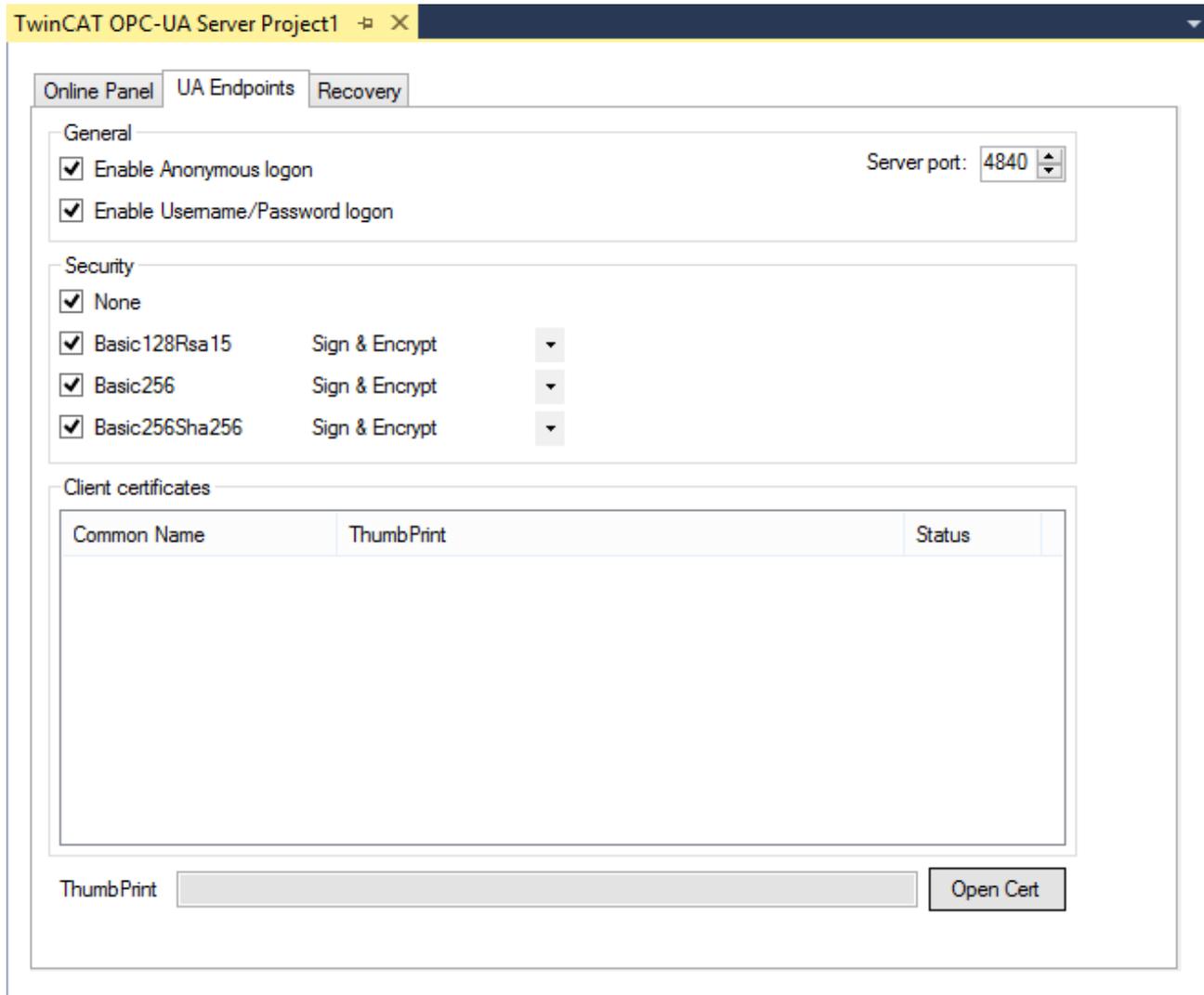
| Produkte | Setup-Versionen | Zielplattform |
|----------|-----------------|-----------------------------|
| TF6100 | 4.x.x | IPC oder CX (x86, x64, ARM) |

4.3.11 Endpunkte konfigurieren

Die Endpunkte des OPC UA Servers geben an, welche Security-Mechanismen bei der Verbindungsherstellung eines Clients benutzt werden sollen. Diese reichen von „unverschlüsselt“ bis zu „verschlüsselt und signiert“, basierend auf verschiedenen Schlüsselstärken.

Die Endpunkte können Sie über den Konfigurator aktivieren und deaktivieren. Es kann z. B. sinnvoll sein, den unverschlüsselten Endpunkt zu deaktivieren, damit sich alle Clients nur mit gültigem und als vertrauenswürdig eingestuftem Zertifikat verbinden können.

Sie konfigurieren die Endpunkte direkt auf Ebene des OPC-UA-Server-Projekts. Durch einen Doppelklick auf das Projekt können Sie in der Registerkarte **UA Endpoints** die entsprechenden Einstellungen vornehmen. Die Einstellungen werden nach einem Aktivieren der Konfiguration und einem anschließenden Neustart des Servers wirksam (siehe [Konfiguration lesen und schreiben \[► 26\]](#) und [Server neu starten \[► 46\]](#)).



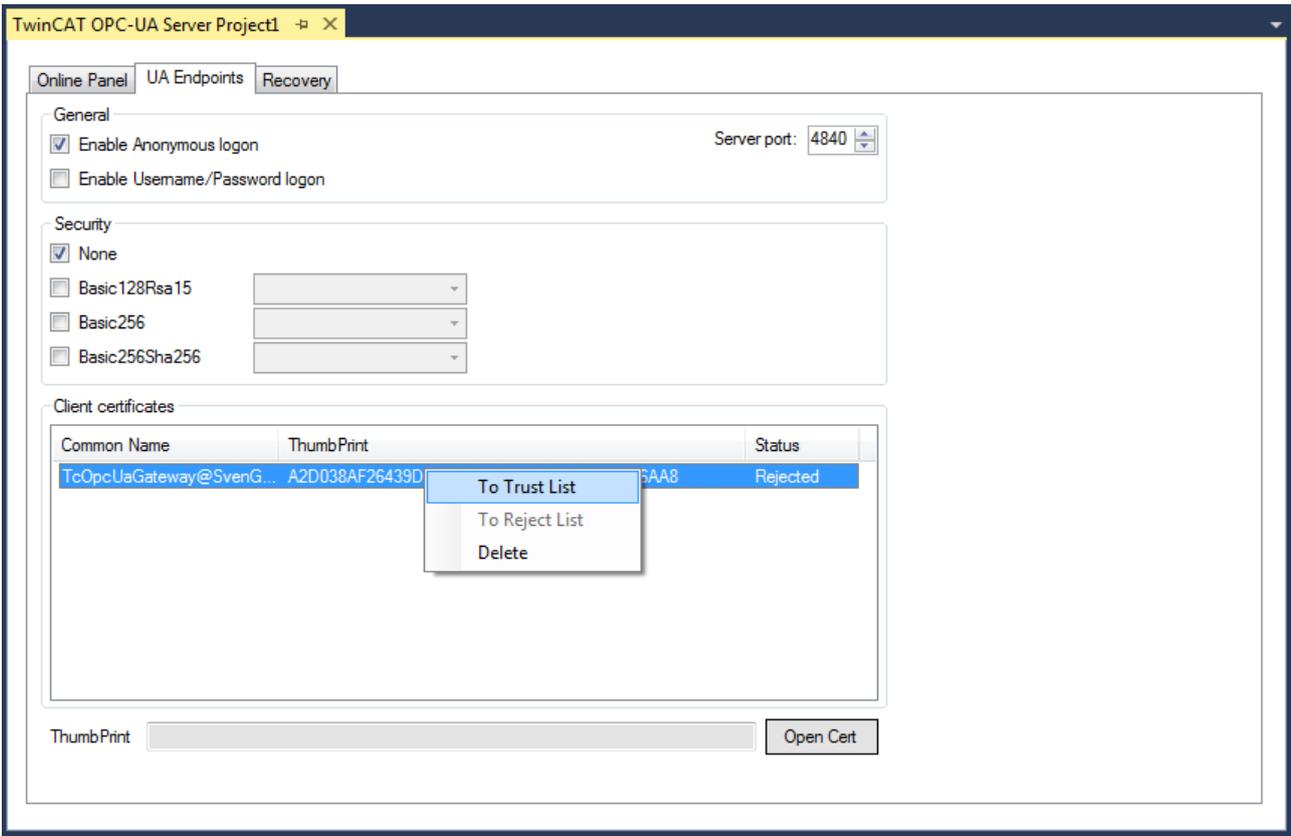
Voraussetzungen

| Produkte | Setup-Versionen | Zielplattform |
|----------|-----------------|-----------------------------|
| TF6100 | 4.x.x | IPC oder CX (x86, x64, ARM) |

4.3.12 Vertrauensstellung für Zertifikate

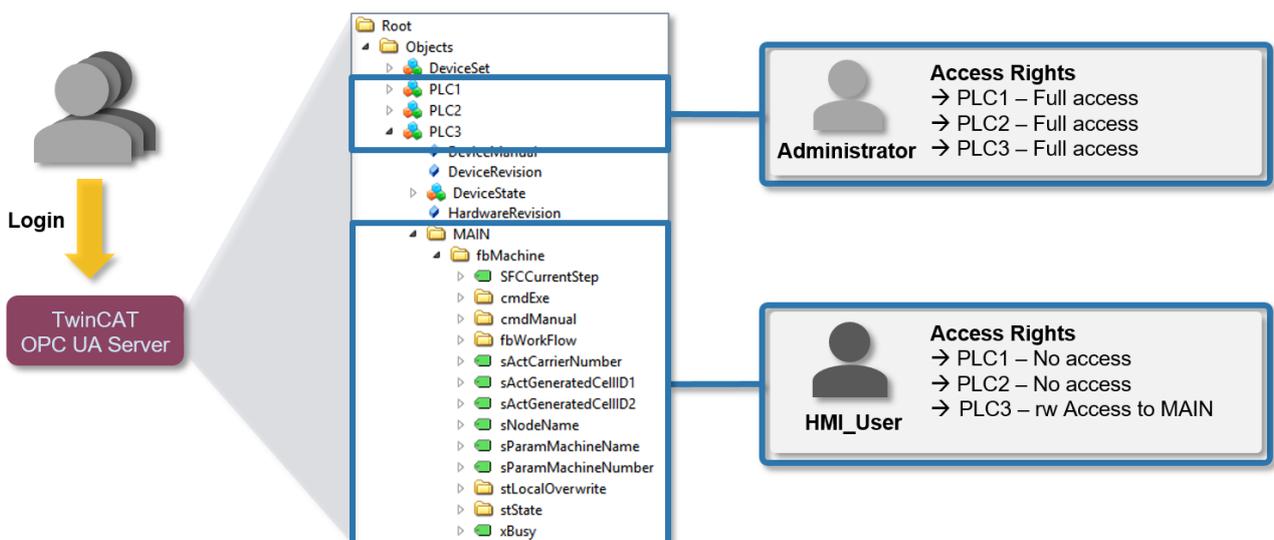
Die auf dem Server vorhandenen Client-Zertifikate können über den Konfigurator komfortabel verwaltet werden. In den Projekteinstellungen können Sie die Zertifikate in der Registerkarte **UA Endpoints** im Bereich **Client certificates** als vertrauenswürdig einstufen oder verweigern.

Nachdem ein OPC UA Client zum ersten Mal versucht hat, sich mit einem sicheren Endpunkt des Servers zu verbinden, wird das Client-Zertifikat auf dem Server hinterlegt und als „rejected“ deklariert. Anschließend kann der Server-Administrator das Zertifikat freischalten. Ein anschließender Verbindungsversuch des Clients mit einem gesicherten Endpunkt wird dann erfolgreich sein.



4.3.13 Sicherheitseinstellungen konfigurieren

Der OPC UA Server ermöglicht die Konfiguration von Berechtigungen auf Namespace- und Node-Ebene. Hierdurch kann sowohl der Zugriff auf ADS-Geräte (z. B. auf verschiedene SPS-Laufzeiten) als auch Variablen feingranular eingestellt werden. Diese Sicherheitseinstellungen sind für alle ADS-Geräte verfügbar, die im Server-Namespace dargestellt werden können.



Konfiguration

Die Konfiguration der Berechtigungen erfolgt auf Basis einer XML-basierten Konfigurationsdatei (*TcUaSecurityConfig.xml*), die in demselben Verzeichnis wie der Server liegt. Die Konfigurationsdatei besteht aus den drei Bereichen **Benutzer (Users)**, **Gruppen (Groups)** und **AccessInfos**.

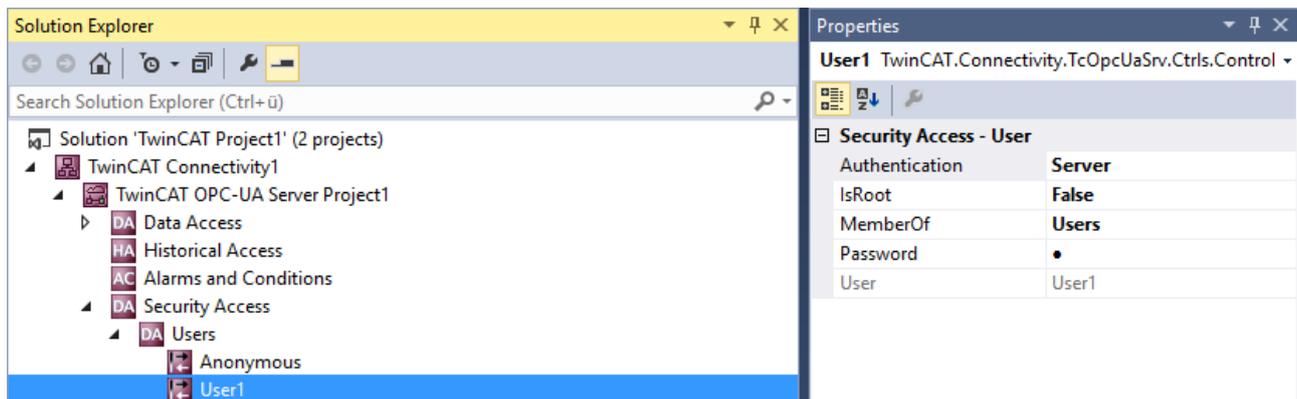
Benutzer (Users)

Im Bereich **Users** können Sie Benutzerkonten konfigurieren, die vom OPC UA Server als Login akzeptiert werden sollen. Hierbei gibt es drei verschiedene Authentifizierungsmethoden:

| | |
|---|--|
| OS (empfohlene Authentifizierungsmethode) | Es werden die Mechanismen vom Betriebssystem verwendet, um Benutzername und Passwort zu validieren. Das Benutzerkonto obliegt vollständig der Kontrolle des Betriebssystems und/oder der Domäne. |
| Server (nicht empfohlen) | Benutzername und Passwort sind nur dem OPC UA Server bekannt. Beide Informationen werden hierbei im Klartext in der XML-Datei hinterlegt. |
| None | Es wird nur der Benutzername vom Server ausgewertet, das Passwort wird ignoriert. |

Benutzer können mit einem Tag <DefaultAccess> konfiguriert werden, das den Standardzugriff des Benutzers auf einen bestimmten Namespace angibt.

Benutzer können Mitglied einer oder mehrerer Gruppen sein. Dies können Sie über das Attribut **MemberOf** spezifizieren. Bei Mitgliedschaft in mehreren Gruppen trennen Sie die Gruppen durch ein Semikolon.

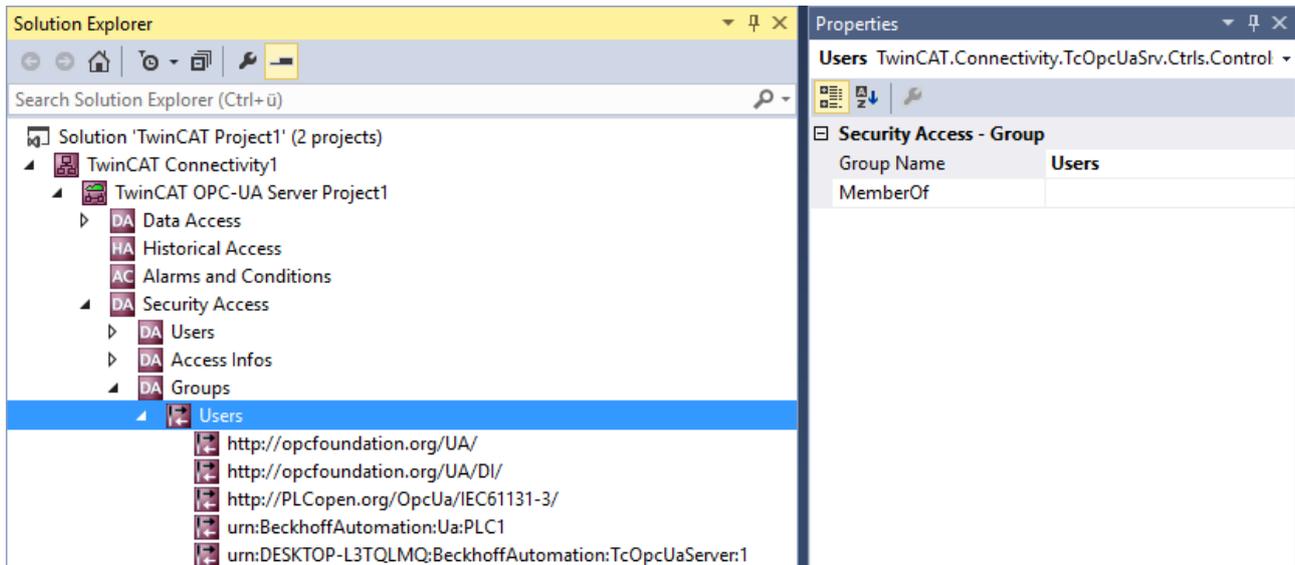


Gruppen (Groups)

Um eine einfachere Konfiguration mit mehreren Benutzeraccounts zu ermöglichen, können Sie die Benutzer in Gruppen zusammenfassen.

Gruppen können ebenfalls mit einem Tag <DefaultAccess> konfiguriert werden.

Über das Attribut **MemberOf** können Sie Gruppen verschachteln. Bei Mitgliedschaft in mehreren Gruppen trennen Sie die Gruppen durch ein Semikolon.

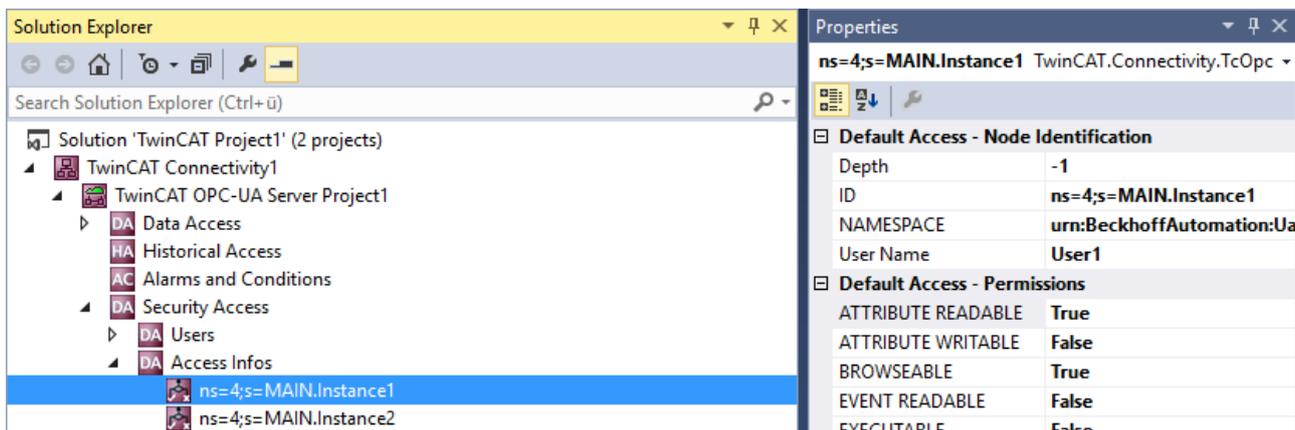


AccessInfos

Wenn eine feingranulare Einstellung von Berechtigungen auf Node-Ebene erfolgen soll, können Sie zusätzlich AccessInfos konfigurieren, welche die Zugriffsberechtigungen auf Nodes spezifizieren. Zugriffsrechte können hierbei auf Unterelemente vererbt werden. Obwohl AccessInfos die feingranularste Konfigurationsmöglichkeit von Berechtigungen ermöglichen, wird eine solche Konfiguration auch schnell unübersichtlich. Prüfen Sie daher, ob eine Konfiguration von Zugriffsrechten auf Namespace-Ebene (siehe oben) nicht ausreichend ist.

Die AccessInfo für eine Node beinhaltet die folgenden Einstellungen:

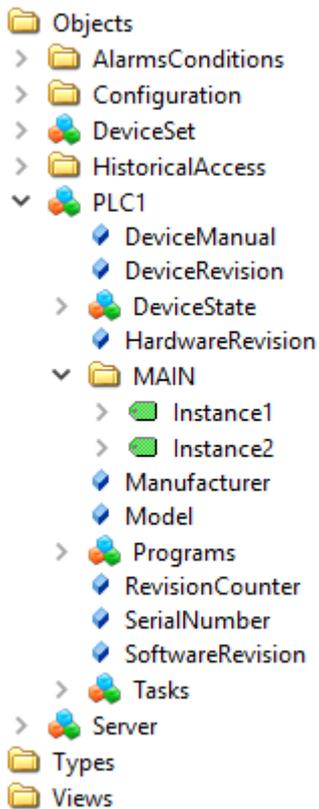
| | |
|------------|--|
| NS | Konfiguriert den NamespaceName, in dem die Node lokalisiert ist |
| Id | Konfiguriert den Identifier der Node, inklusive des IdentifierTypes (z. B. s = String) |
| Depth | Vererbungstiefe der Berechtigungen (-1 für unendlich) |
| User/Group | Benutzer oder Gruppe, der/die auf diese Node Zugriff erhalten soll, inklusive des AccessLevels |



AccessInfos können per Drag-and-drop von Variablen aus dem Target Browser konfiguriert werden. Die konfigurierbaren Berechtigungen sind kumulativ.

Beispielkonfiguration

Gegeben sei folgendes einfaches Steuerungsprogramm. Die Variablen sind bereits im OPC-UA-Namespace des Servers veröffentlicht. Der OPC UA Server befindet sich zunächst im Auslieferungszustand.



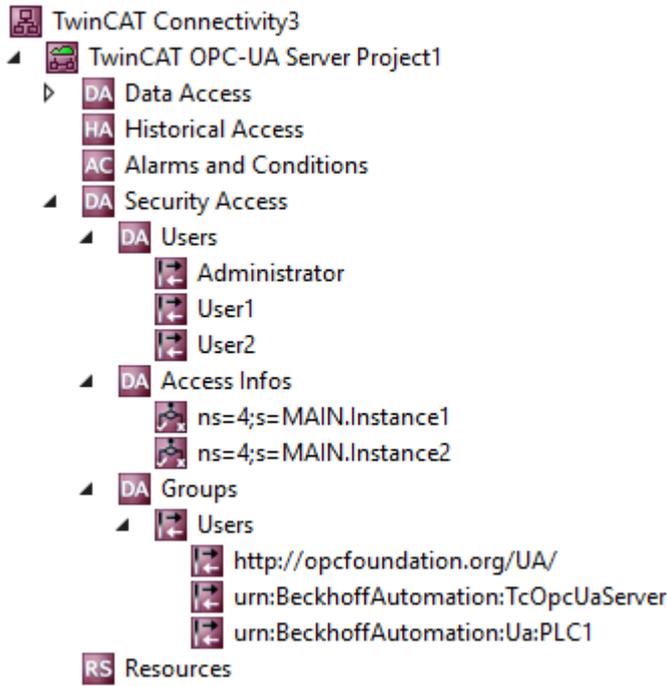
Zugriffbeschränkungen

Der Zugriff auf den Server soll für Clients wie folgt eingeschränkt werden:

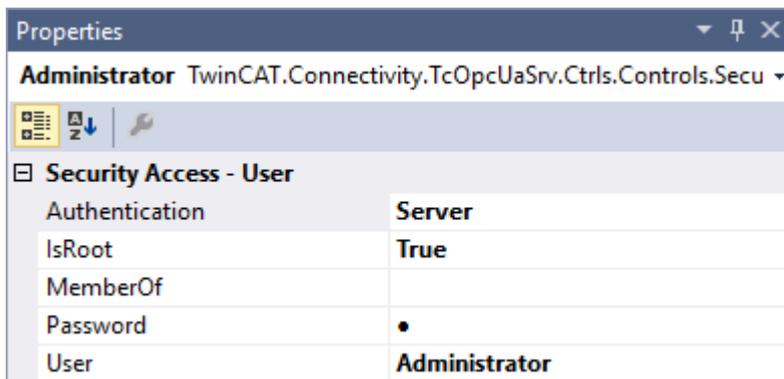
- Anonymous Zugriff soll deaktiviert werden.
- Es soll einen Benutzer „Administrator“ geben, der Vollzugriff auf den kompletten Server hat.
- Es soll einen Benutzer „User1“ geben, der ausschließlich Lesezugriff auf MAIN.Instance1 hat. Der Benutzer soll hierbei nicht aus dem Betriebssystem kommen, sondern nur intern im Server verwendet werden.
- Es soll einen Benutzer „User2“ geben, der ausschließlich Lesezugriff auf MAIN.Instance2 hat. Der Benutzer soll hierbei nicht aus dem Betriebssystem kommen, sondern nur intern im Server verwendet werden.
- Über eine Gruppe "Users" sollen allgemeine Zugriffsberechtigungen für alle Benutzer konfiguriert werden.

Einstellungen

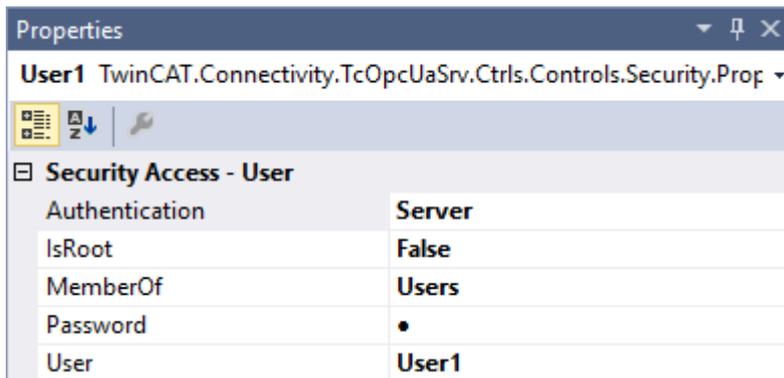
Die Konfiguration des OPC UA Server wird wie folgt eingestellt:



Einstellungen für den Benutzer „Administrator“:



Einstellungen für den Benutzer „User1“:



Einstellungen für den Benutzer „User2“:

| Security Access - User | |
|------------------------|--------|
| Authentication | Server |
| IsRoot | False |
| MemberOf | Users |
| Password | • |
| User | User2 |

Einstellungen Access Infos „MAIN.Instance1“:

| Default Access - Node Identification | |
|--------------------------------------|--------------------------------|
| Depth | -1 |
| ID | ns=4;s=MAIN.Instance1 |
| NAMESPACE | urn:BeckhoffAutomation:Ua:PLC1 |
| User Name | User1 |
| Default Access - Permissions | |
| ATTRIBUTE READABLE | True |
| ATTRIBUTE WRITABLE | False |
| BROWSEABLE | True |
| EVENT READABLE | False |
| EXECUTABLE | False |
| HISTORY DELETE | False |
| HISTORY INSERT | False |
| HISTORY MODIFY | False |
| HISTORY READABLE | False |
| PERMISSION ALL | False |
| READABLE | True |
| WRITABLE | False |

Einstellungen Access Infos „MAIN.Instance2“:

| Properties | |
|---|--------------------------------|
| ns=4;s=MAIN.Instance2 TwinCAT.Connectivity.TcOpcUaSrv.Ctrls.Coi | |
| <input checked="" type="checkbox"/> Default Access - Node Identification | |
| Depth | -1 |
| ID | ns=4;s=MAIN.Instance2 |
| NAMESPACE | urn:BeckhoffAutomation:Ua:PLC1 |
| User Name | User2 |
| <input checked="" type="checkbox"/> Default Access - Permissions | |
| ATTRIBUTE READABLE | True |
| ATTRIBUTE WRITABLE | False |
| BROWSEABLE | True |
| EVENT READABLE | False |
| EXECUTABLE | False |
| HISTORY DELETE | False |
| HISTORY INSERT | False |
| HISTORY MODIFY | False |
| HISTORY READABLE | False |
| PERMISSION ALL | False |
| READABLE | True |
| WRITABLE | False |

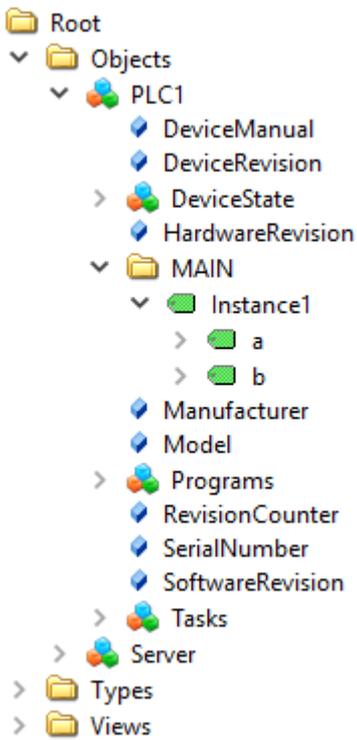
Einstellungen für die Gruppe „Users“:

Die Benutzergruppe wird sowohl mit grundlegendem Zugriff auf benötigte Server- und Typsystem-Namensräume ausgestattet als auch mit Read- und Browse-Berechtigungen auf den PLC1-Namensraum.

| Properties | |
|---|--------------------------------|
| urn:BeckhoffAutomation:Ua:PLC1 TwinCAT.Connectivity.TcOpcUaS | |
| <input checked="" type="checkbox"/> Default Access - Namespace | |
| NAMESPACE | urn:BeckhoffAutomation:Ua:PLC1 |
| <input checked="" type="checkbox"/> Default Access - Permissions | |
| ATTRIBUTE READABLE | True |
| ATTRIBUTE WRITABLE | False |
| BROWSEABLE | True |
| EVENT READABLE | False |
| EXECUTABLE | False |
| HISTORY DELETE | False |
| HISTORY INSERT | False |
| HISTORY MODIFY | False |
| HISTORY READABLE | False |
| PERMISSION ALL | False |
| READABLE | False |
| WRITABLE | False |

Ergebnis

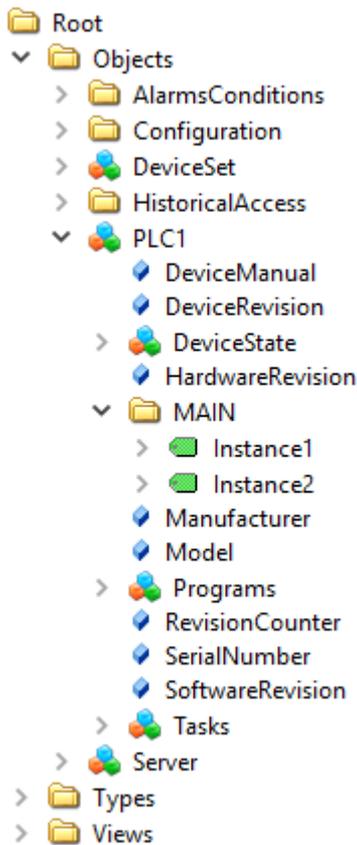
Nach Aktivierung der Konfiguration stellt sich der Namensraum des Servers für „User1“ nach einem Verbindungsaufbau wie folgt dar:



Auf die Node „Instance1“ hat der Benutzer nur Leserechte, was durch das Attribut UserAccessLevel deutlich wird:

| | |
|-----------------|-----------------------------------|
| DataType | ST_Test |
| NamespaceIndex | 4 |
| IdentifierType | String |
| Identifier | <StructuredDataType>:ST_Test |
| ValueRank | -1 |
| ArrayDimensions | BadAttributIdInvalid (0x80350000) |
| AccessLevel | CurrentRead, CurrentWrite |
| UserAccessLevel | CurrentRead |

Der Benutzer „Administrator“ hingegen hat volle Zugriffsrechte auf alle Elemente des Namensraums:



4.3.14 Server neu starten

Der OPC-UA-Konfigurator ermöglicht das Triggern eines Neustarts des OPC UA Server. Dies kann lokal oder remote erfolgen und bezieht sich auf das jeweils selektierte Zielgerät.

● Verbindungsverlust

i Ein Neustart des OPC UA Server führt immer zu einem Verbindungsverlust aller verbundenen Clients.

Den Neustart triggern Sie über die Symbolleiste.



Voraussetzungen

| Produkte | Setup-Versionen | Zielplattform |
|----------|-----------------|-----------------------------|
| TF6100 | 4.x.x | IPC oder CX (x86, x64, ARM) |

Siehe auch: [Verbinden mit einem Server \[► 21\]](#)

4.3.15 Logging

Für eine erweiterte Diagnose können Sie die Logging-Funktion des OPC UA Servers aktivieren.

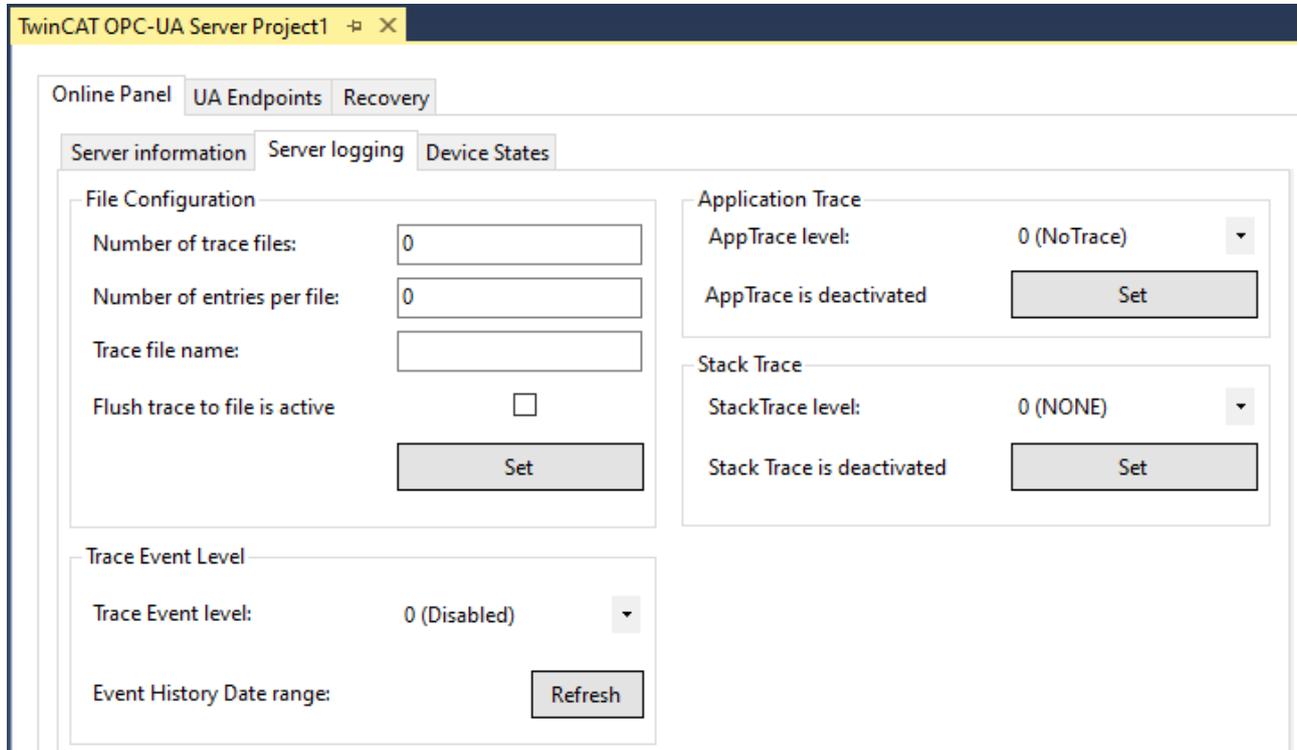
● Schreiben der Log-Datei

i Durch das Aktivieren der Logging-Funktion auf dem Server wird eine Protokolldatei auf dem Dateisystem geschrieben. Stellen Sie sicher, dass ausreichend Speicherplatz zur Verfügung steht und setzen Sie die Logging-Parameter entsprechend (Anzahl Log-Dateien, Größe pro Log-Datei).

i Performance- und Timingverhalten

Durch das Aktivieren der Protokollfunktionen verändert sich das Timing-Verhalten des OPC UA Servers. Hierdurch können je nach Plattform und Projekt Geschwindigkeitseinbußen entstehen.

Sie aktivieren die Logging-Funktion im Konfigurator des Projekts in der Registerkarte **Online Panel** über die Schaltfläche **Activate**. Sie können die Funktion je nach selektiertem Zielgerät lokal oder remote aktivieren. Die Logging-Funktion ist so lange aktiv, bis sie über den Konfigurator wieder deaktiviert oder bis der OPC UA Server neu gestartet wird.



Trace-Level

Generell gilt: Je höher der „Trace level“, desto detailliertere (und mehr) Daten werden geschrieben, desto mehr Last wird jedoch auch auf der Serverapplikation verursacht, wodurch sich das Timingverhalten entsprechend ändert. Bitte aktivieren Sie daher das Logging nur im Diagnosefall und in Absprache mit dem Beckhoff Support.

Activate App Trace

In den meisten Fällen ist es ausreichend ein sogenanntes „AppTrace“ zu erstellen. Hierbei werden Informationen der Serverapplikation protokolliert. Zum Aktivieren des AppTrace tragen Sie bitte die Anzahl an TraceFiles, sowie die Anzahl Einträge pro TraceFile in die zugehörigen Textfelder ein. Anschliessend wählen Sie einen Tracelevel aus und klicken auf den Button zum Aktivieren des AppTrace. Die Werte in den grau hinterlegten Textfeldern stellen die aktuellen Einstellungen auf dem Server dar.

Activate Stack Trace

In einigen wenigen Fällen ist es zusätzlich notwendig ein sogenanntes „StackTrace“ zu erstellen, wodurch Informationen vom OPC UA Stack protokolliert werden. Zum Aktivieren des StackTrace tragen Sie bitte die Anzahl an TraceFiles, sowie die Anzahl Einträge pro TraceFile in die zugehörigen Textfelder ein. Anschliessend wählen Sie einen Tracelevel aus und klicken auf den Button zum Aktivieren des StackTrace. Die Werte in den grau hinterlegten Textfeldern stellen die aktuellen Einstellungen auf dem Server dar.

Voraussetzungen

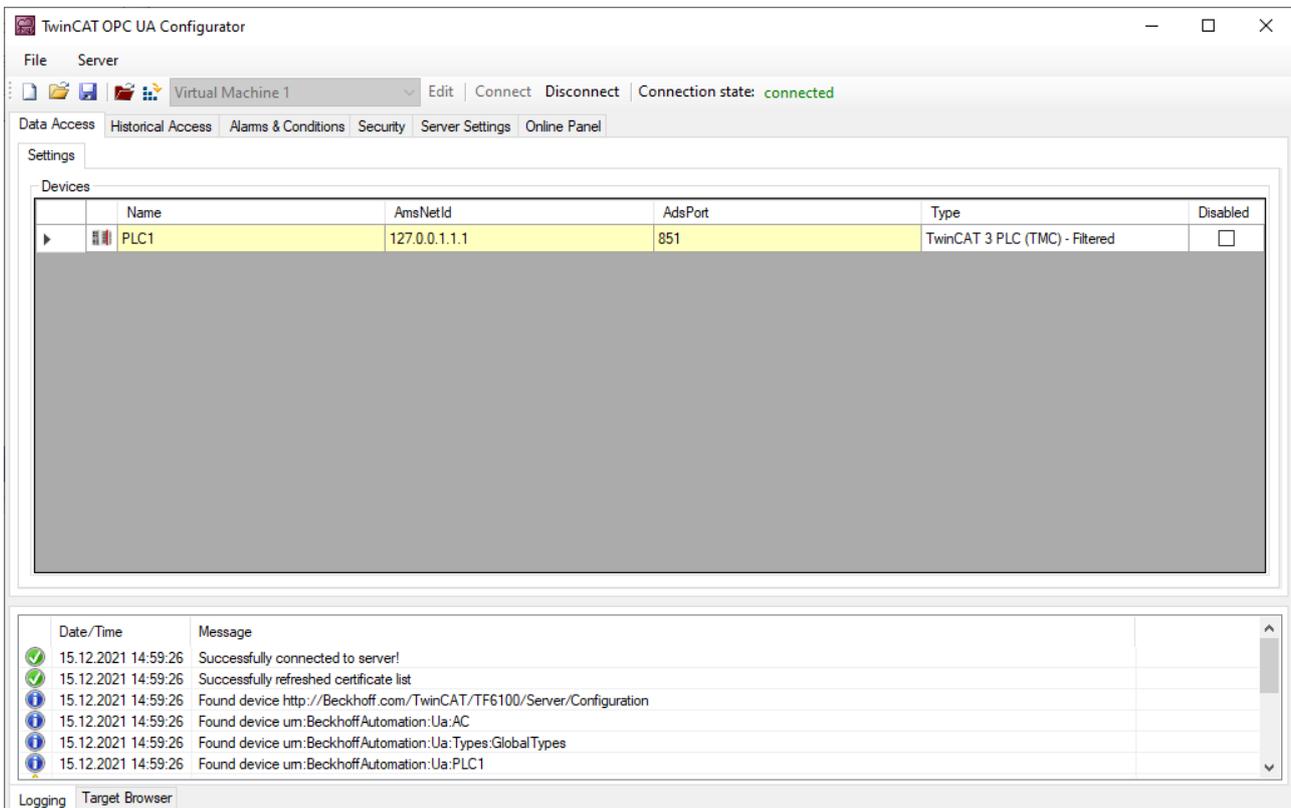
| Produkte | Setup-Versionen | Zielplattform |
|----------|-----------------|-----------------------------|
| TF6100 | 4.x.x | IPC oder CX (x86, x64, ARM) |

Siehe auch: [Auswahl eines Zielgeräts \[► 21\]](#)

4.4 Standalone

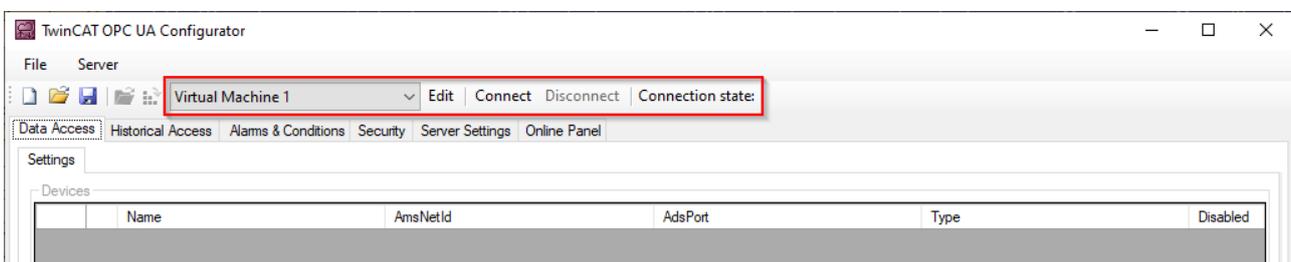
4.4.1 Übersicht

Der Standalone-Konfigurator ermöglicht eine Parametrisierung des TwinCAT OPC UA Servers unabhängig vom Visual Studio. Sie können alle unterschiedlichen Features des Servers konfigurieren.

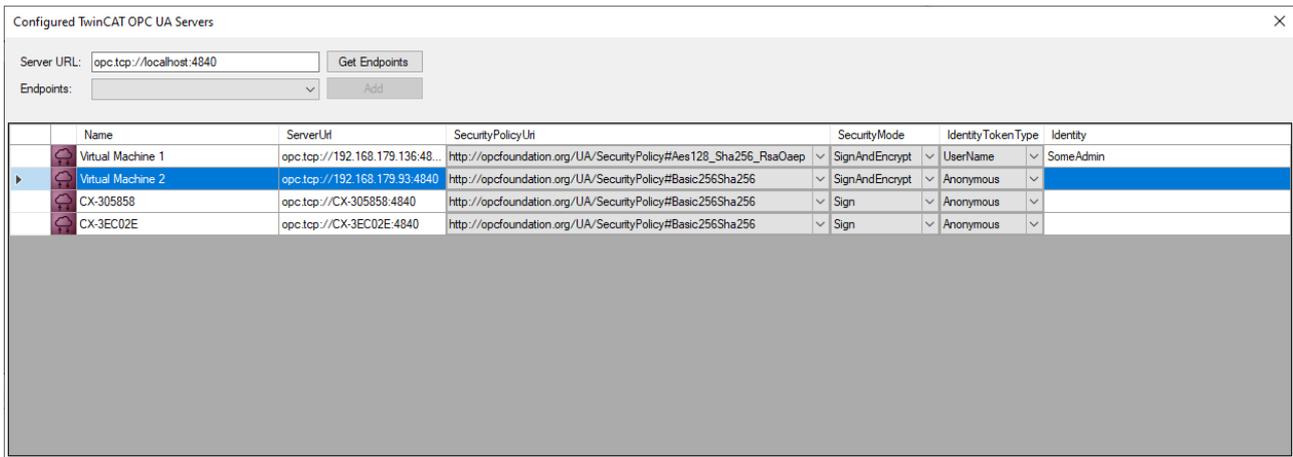


4.4.2 Verbinden mit einem Server

Der OPC-UA-Konfigurator ermöglicht die vollständige Parametrierung des Servers über OPC UA. Ähnlich wie im TwinCAT-XAE-System können Sie über die Symbolleiste einen OPC-UA-Server auswählen, mit dem Sie sich verbinden wollen.



Durch einen Klick auf den **Edit**-Button öffnen Sie den Serverlisten-Dialog. In diesem Dialog können Sie eine oder mehrere Server-Verbindungen hinzufügen.



Durch Eingabe einer ServerURL und Aufruf des **Get Endpoints**-Buttons kann eine Server-Verbindung zur Liste hinzugefügt werden. Etwaige Einstellungen zum IdentityToken, z. B., ob sich der Konfigurator als Anonymous-Benutzer oder mit einer Benutzername/Password-Kombination verbinden soll, müssen manuell eingestellt werden.

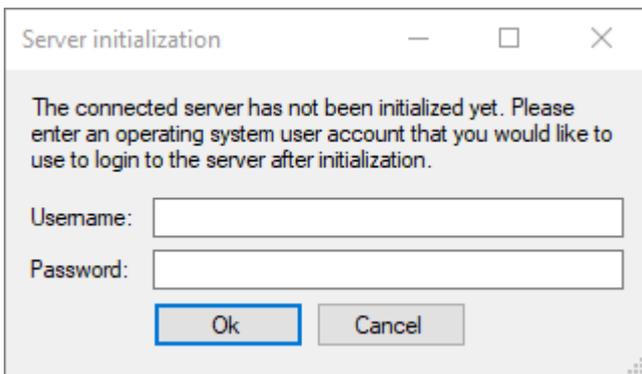
Bestätigen einer Konfiguration

i Bitte bestätigen Sie Änderungen an den Einträgen immer mit der **ENTER**-Taste, da sie nur dann im Hintergrund automatisch gespeichert werden.

Nach der Konfiguration einer Server-Verbindung ist der entsprechende Eintrag in der DropDownBox verfügbar und die Verbindung kann durch Klicken des **Connect**-Buttons hergestellt werden.

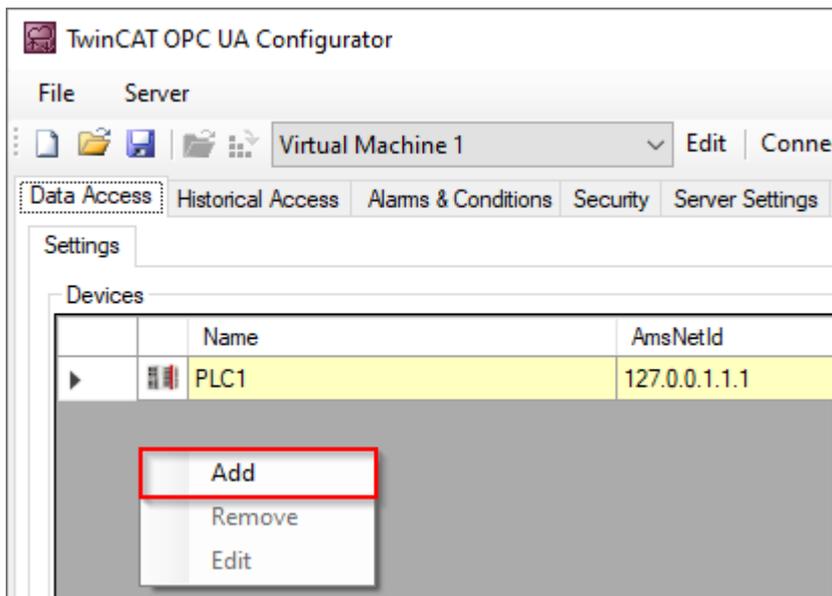
4.4.3 Durchführen der Server-Initialisierung

Der TwinCAT OPC UA Server wird in einem uninitialisierten Modus ausgeliefert, welcher auf dem sogenannten TOFU (Trust-On-First-Use) Prinzip begründet ist. Detaillierte Informationen zu diesem Server-Feature und die entsprechenden Hintergrundinformationen finden Sie hier. Der TwinCAT OPC UA Configurator ermöglicht die Initialisierung des Servers beim ersten Verbindungsaufbau. Ein entsprechender Warnhinweis weist auf den uninitialisierten Server hin und ermöglicht eine entsprechende Initialisierung.

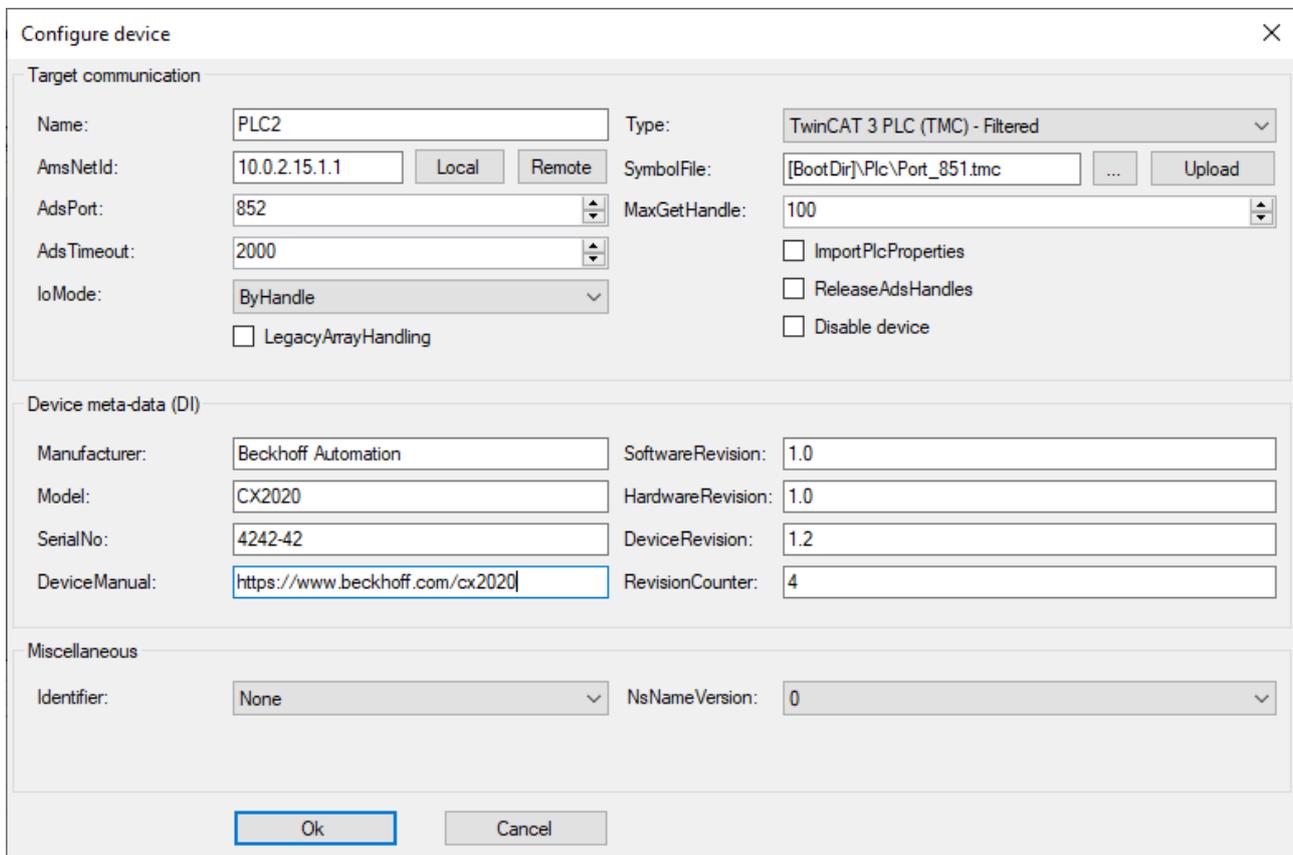


4.4.4 ADS-Geräte hinzufügen

Über die Registerkarte **Data Access** lassen sich ADS-Geräte zur TwinCAT OPC UA Server-Konfiguration hinzufügen. Im zugehörigen DataGrid legen Sie über das Kontextmenü ein neues Gerät an.



Im anschließenden Dialog setzen Sie die Geräte-spezifischen Parameter.



Auswählen einer AMS NetID

Zur Auswahl einer AMS NetID können entweder die ADS-Teilnehmer vom lokalen System oder dem verbundenen TwinCAT OPC UA Server selektiert werden. Als ADS-Teilnehmer wird hierbei ein System bezeichnet, welches eine ADS-Route zu dem lokalen oder Server-System besitzt. Durch einen Klick auf den Button **Local** werden die lokalen ADS-Routen angezeigt. Durch einen Klick auf den Button **Remote** werden die ADS-Routen auf dem verbundenen TwinCAT OPC UA Server angezeigt.

Auswählen einer Symboldatei

Die Auswahl einer Symboldatei erfolgt immer vom lokalen System aus. Die Symboldatei kann jedoch über den **Upload**-Button auf den verbundenen TwinCAT OPC UA Server hochgeladen werden. Die Symboldatei wird dabei in dem Unterordner „symbolfiles“ des TwinCAT OPC UA Server-Basisverzeichnisses abgelegt und automatisch über einen Platzhalter in der Konfigurationsdatei referenziert.

4.4.5 Konfiguration lesen und schreiben

Der Konfigurator ermöglicht sowohl das Auslesen/Schreiben der Konfigurationsdateien vom TwinCAT OPC UA Server als auch das Laden/Speichern der Konfigurationsdateien auf dem lokalen System. Diese Funktionalitäten stehen sowohl über das Menü als auch die Toolbar zur Verfügung.

Lokales Laden/Speichern

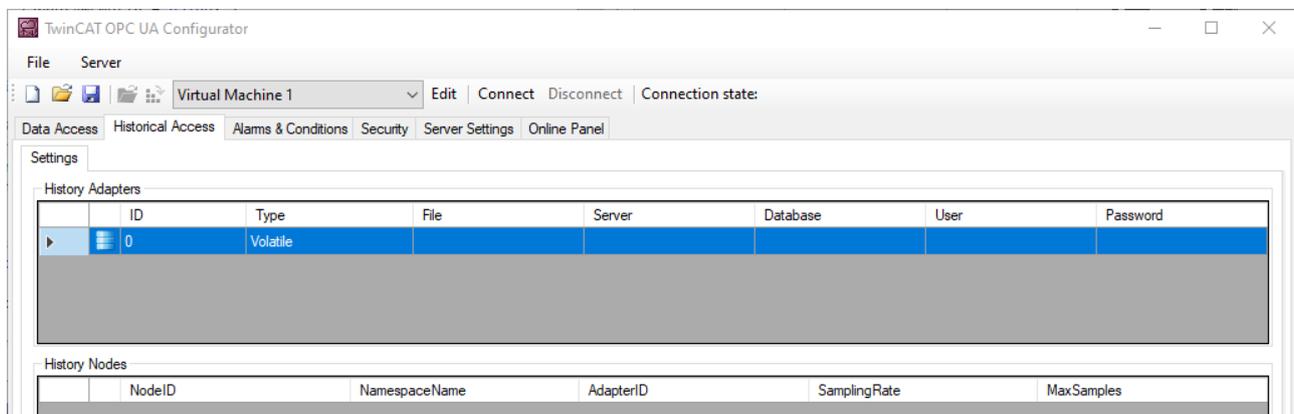
Diese Funktionen stehen über das **File**-Menü zur Verfügung. Die hier verfügbaren Buttons **Open** und **Save** ermöglichen ein Laden und Speichern der Konfigurationsdateien. Es werden hierbei immer alle Konfigurationsdateien geladen oder gespeichert.

Remotes Laden/Speichern

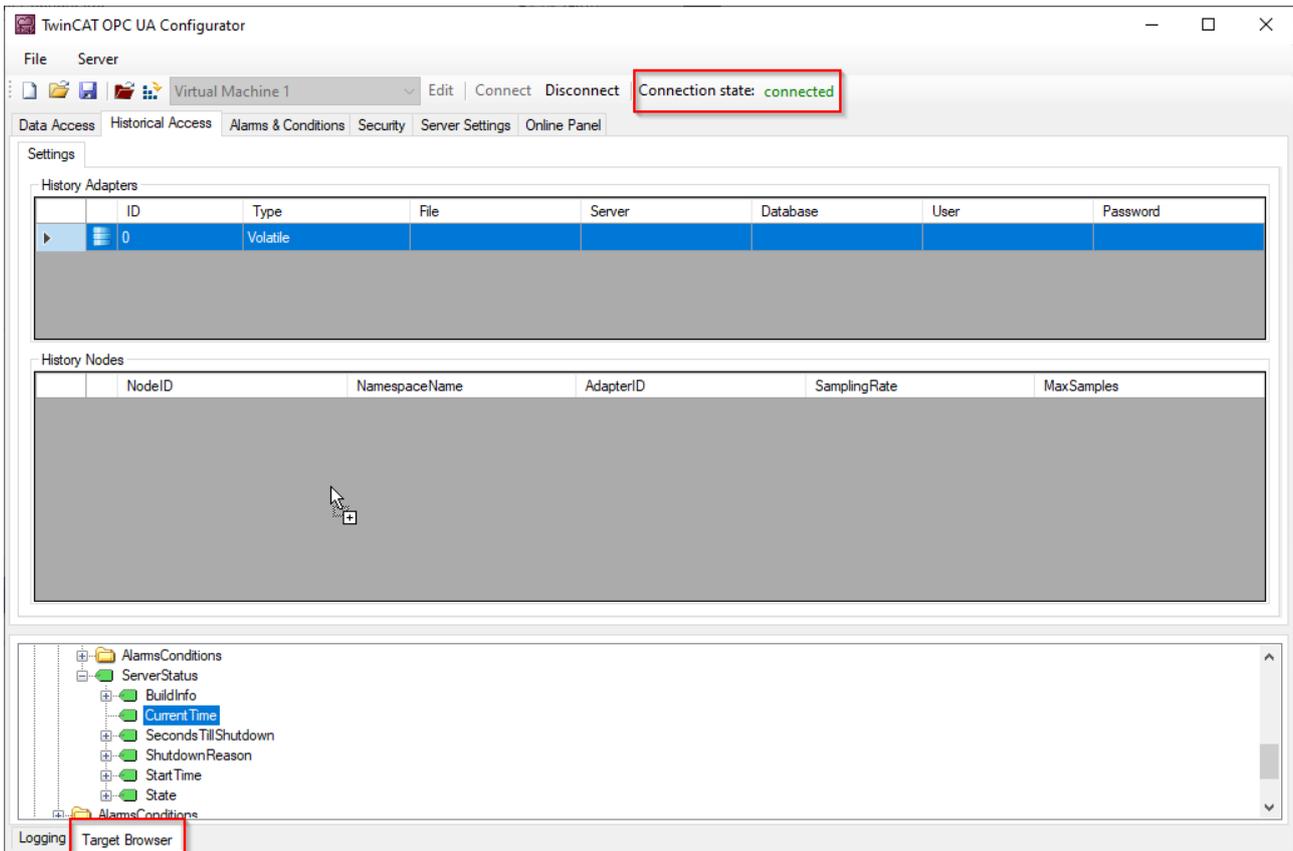
Diese Funktionen stehen über das **Server** Menü zur Verfügung. Die hier verfügbaren Buttons **Open from target** und **Activate from target** ermöglichen ein Laden und Speichern der Konfigurationsdateien vom verbundenen TwinCAT OPC UA Server. Es werden hierbei immer alle Konfigurationsdateien geladen oder gespeichert.

4.4.6 Historical Access konfigurieren

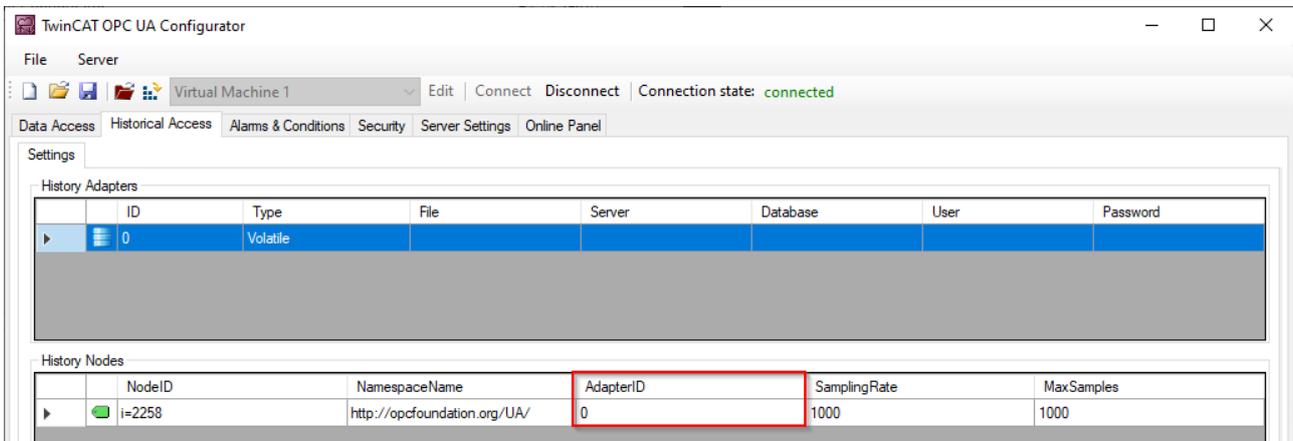
Über die Registerkarte **Historical Access** können Sie die entsprechende Konfiguration vornehmen und sowohl die **History Adapter** als auch die **History Nodes** konfigurieren. Ein **History Adapter** definiert hierbei die Art der Datenablage und eine **History Node** die Variable für die historische Daten in der Datenablage gespeichert werden sollen.



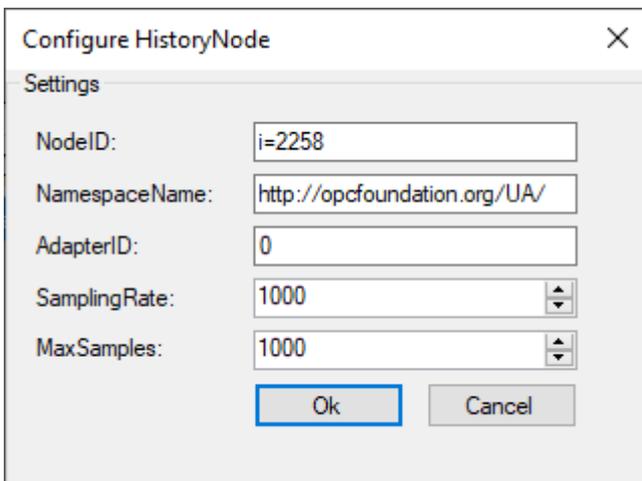
Über das Kontextmenü können Sie sowohl **History Adapter** als auch **History Nodes** anlegen. Wenn Sie mit einem TwinCAT OPC UA Server verbunden sind, dann können Sie auch komfortabel die zu konfigurierenden Nodes per Drag&Drop aus dem **Target Browser** zu den **History Nodes** hinzufügen.



Anschließend kann eine **History Node** über die AdapterID mit dem jeweiligen **History Adapter** verknüpft werden.

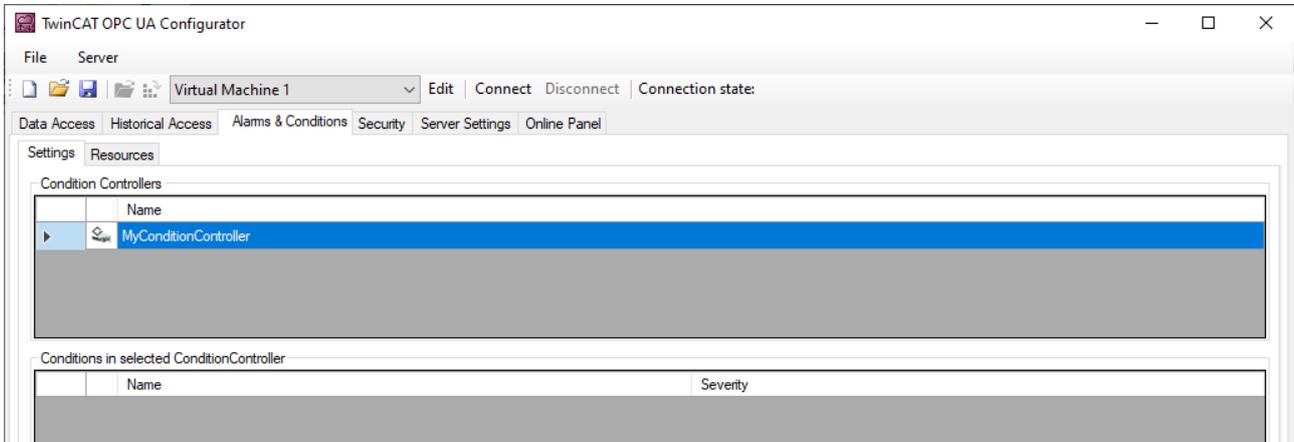


Durch einen Doppelklick auf die History Node gelangen Sie in den entsprechenden Konfigurationsdialog.

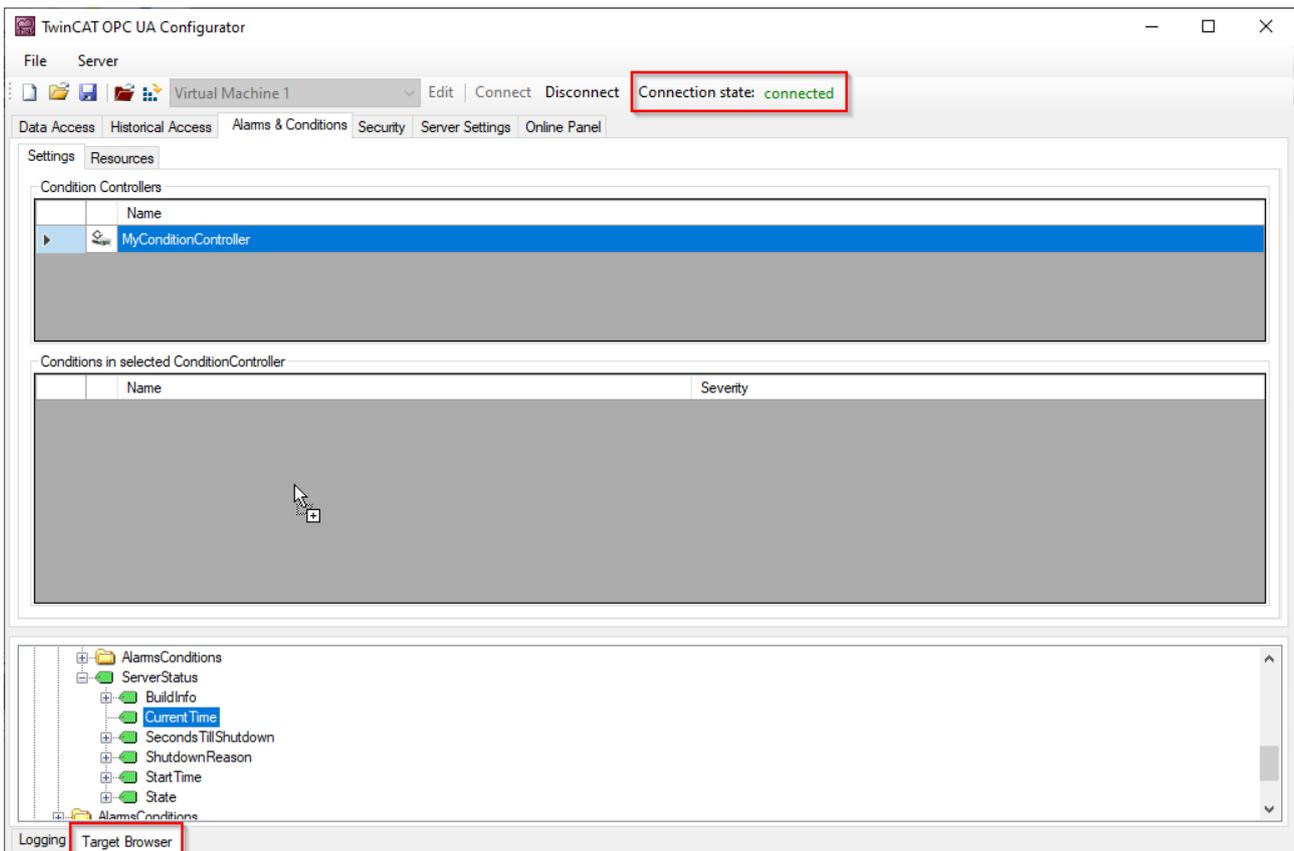


4.4.7 Alarms and Conditions konfigurieren

Über die Registerkarte **Alarms & Conditions** können Sie die entsprechende Konfiguration vornehmen und sowohl die **Condition Controller** als auch die **Conditions** konfigurieren. Ein **Condition Controller** ist hierbei eine Verwaltungseinheit zur Organisation der einzelnen **Conditions**. Eine **Condition** hingegen spiegelt eine Variable wider welche im Sinne von **Alarms & Conditions** anhand von konfigurierbaren Schwellenwerten überwacht werden soll.



Über das Kontextmenü können Sie sowohl **Condition Controller** als auch **Conditions** anlegen. Wenn Sie mit einem TwinCAT OPC UA Server verbunden sind, dann können Sie auch komfortabel die zu konfigurierenden Nodes per Drag&Drop aus dem **Target Browser** zu den **Conditions** hinzufügen.



Eine **Condition** wird immer zu dem aktuell selektierten **Condition Controller** hinzugefügt. Bei Verwendung von Drag&Drop öffnet sich der Konfigurationsdialog einer **Condition** automatisch.

Condition
✕

General

Name:

Severity:

Node settings

Identifier:

NamespaceName:

SamplingRate:

Alarm type

LimitAlarm Type OffNormalAlarm Type

LimitAlarm Type settings

| | Alarm text ID: | Detected languages: |
|----------------|----------------------|----------------------|
| HighHighLimit: | <input type="text"/> | <input type="text"/> |
| HighLimit: | <input type="text"/> | <input type="text"/> |
| LowLimit: | <input type="text"/> | <input type="text"/> |
| LowLowLimit: | <input type="text"/> | <input type="text"/> |

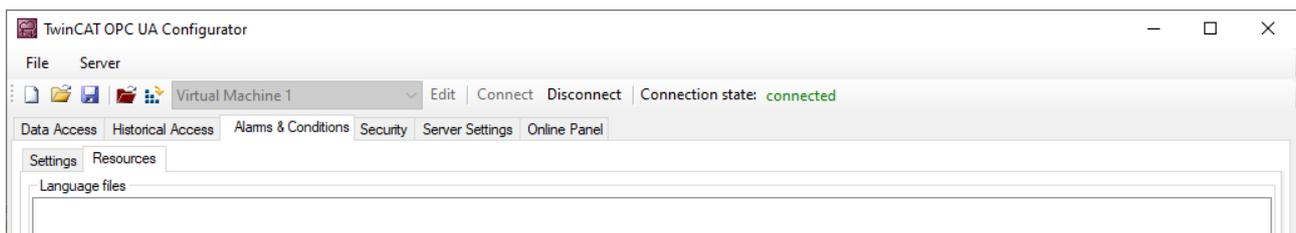
OffNormalAlarm Type settings

| | Alarm text ID: | Detected languages: |
|---------------|----------------------|----------------------|
| Normal value: | <input type="text"/> | <input type="text"/> |

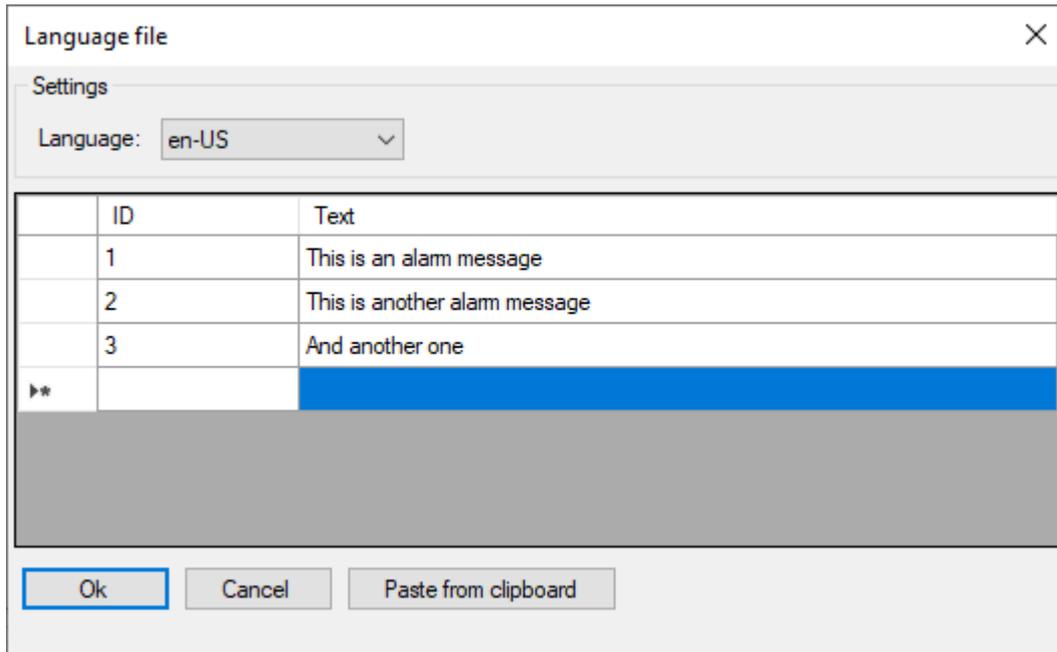
Die bei Selektion des jeweiligen **AlarmTypes** zu konfigurierenden Alarmtexte lassen sich über die entsprechenden DropDown-Boxes auswählen. Bitte beachten Sie, dass die Alarmtexte hierbei schon vorhanden sein müssen. In dem Kapitel [Alarmtexte konfigurieren](#) [► 54] erfahren Sie mehr zu diesem Thema.

4.4.8 Alarmtexte konfigurieren

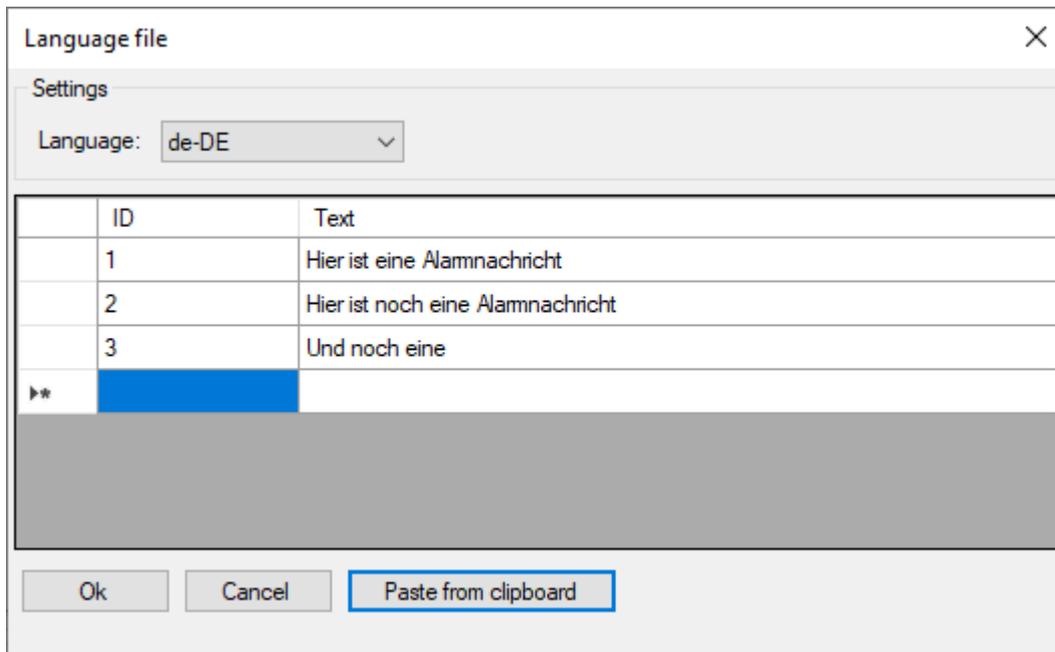
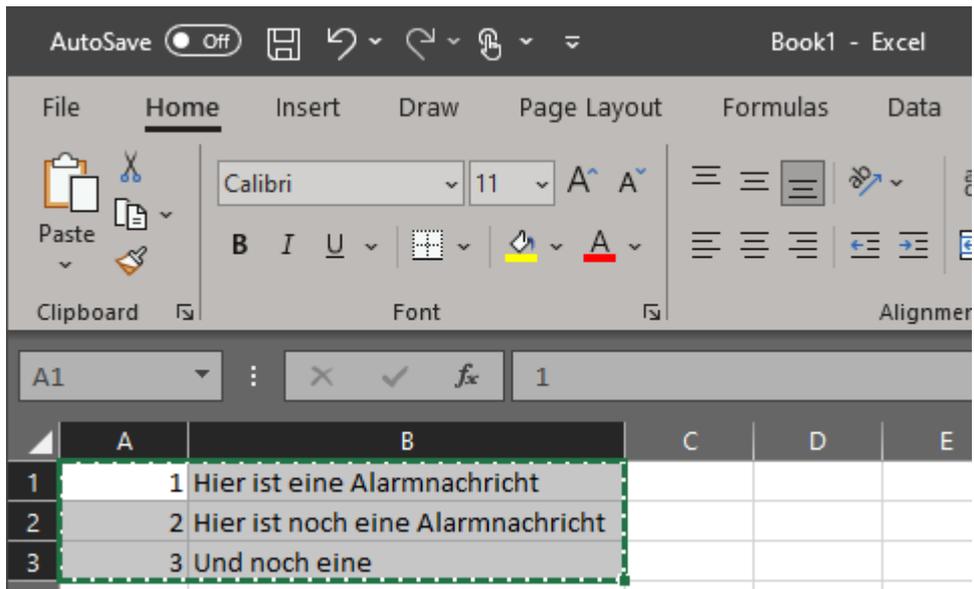
Innerhalb des **Alarms & Conditions**-Bereichs können Sie über die Registerkarte **Resources** Alarmtexte konfigurieren, welche Sie anschließend für eine Condition verwenden können.



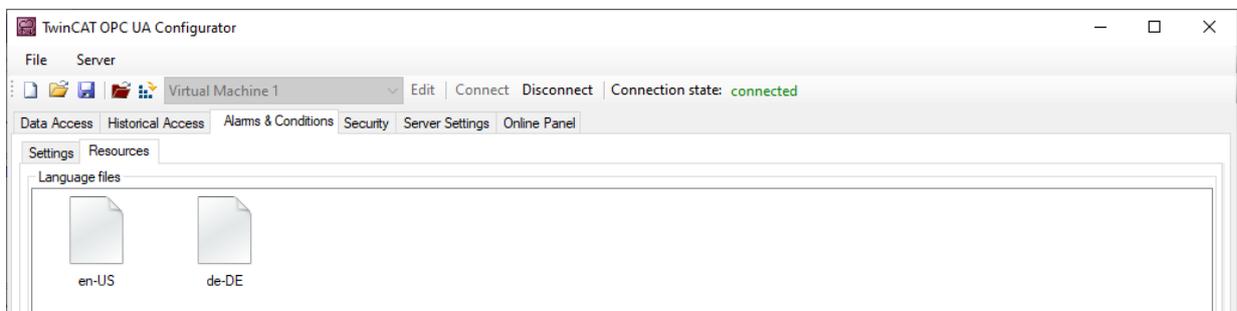
- Über das Kontextmenü fügen Sie eine neue Alarmtextdatei hinzu. Diese Dateien sind nach der jeweiligen Sprache gruppiert, für welche die Alarmtexte definiert werden.



- Über den **Paste from clipboard**-Button werden ID und Text aus einer Excel-Tabelle übernommen, indem sie von dort zuerst in die Zwischenablage kopiert (STRG+C) und dann über den Button importiert werden.



⇒ Nach der Konfiguration der Sprachdateien können Sie die Alarmtexte an einer Condition verwenden.



Condition
✕

General

Name:

Severity:

Node settings

Identifier:

NamespaceName:

SamplingRate:

Alarm type

LimitAlarm Type OffNormalAlarm Type

LimitAlarm Type settings

| | Alarm text ID: | Detected languages: |
|--|----------------------------------|--|
| HighHighLimit: <input type="text" value="10"/> | <input type="text" value="1"/> ▼ | <input type="text" value="en-US,de-DE"/> |
| HighLimit: <input type="text" value="20"/> | <input type="text" value="2"/> ▼ | <input type="text" value="en-US,de-DE"/> |
| LowLimit: <input type="text" value="0"/> | <input type="text" value="3"/> ▼ | <input type="text" value="en-US,de-DE"/> |
| LowLowLimit: <input type="text" value="-10"/> | <input type="text" value="1"/> ▼ | <input type="text" value="en-US,de-DE"/> |

OffNormalAlarm Type settings

Normal value:

Alarm text ID:

Detected languages:

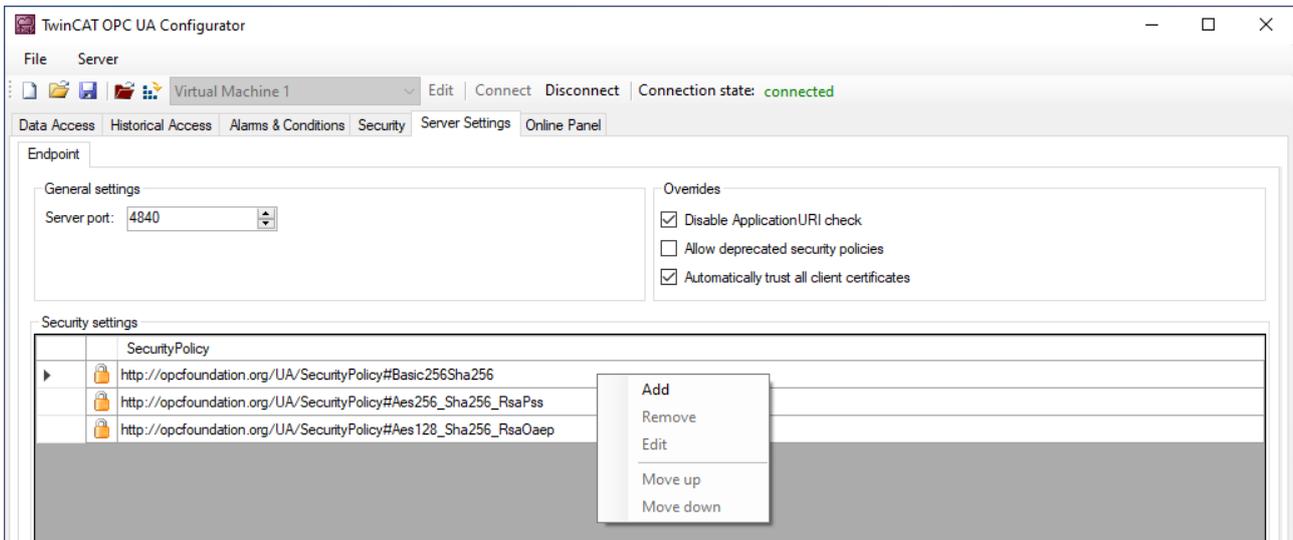
Über die **Detected languages**-Felder können Sie schnell überprüfen, ob Sie die selektierte AlarmtextID auch für alle Sprachen definiert haben, oder ob eventuell eine Sprache vergessen wurde.

4.4.9 Endpunkte konfigurieren

Die Endpunkte des OPC UA Servers geben an, welche Security-Mechanismen bei der Verbindungsherstellung eines Clients benutzt werden sollen. Diese reichen von „unverschlüsselt“ bis zu „verschlüsselt und signiert“, basierend auf verschiedenen Schlüsselstärken.

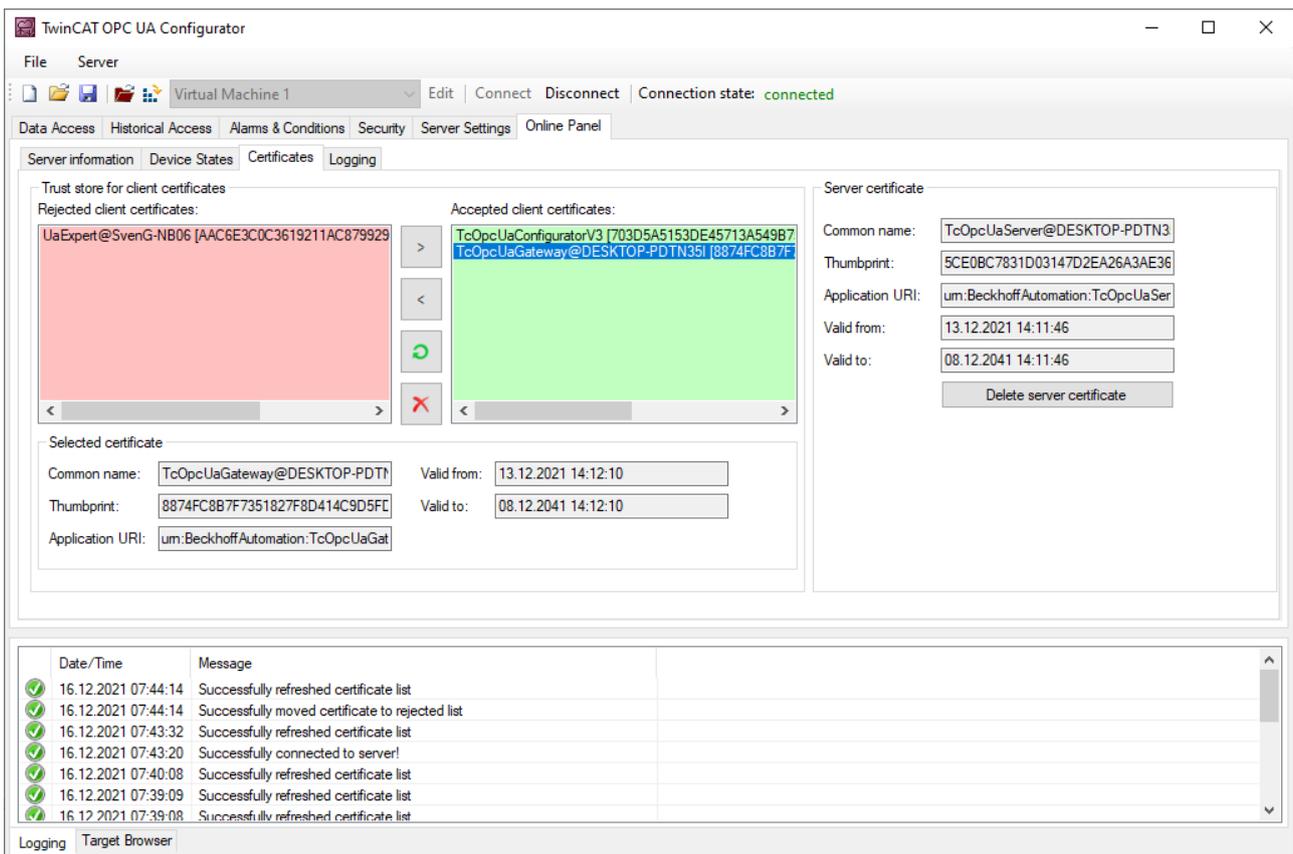
Die Endpunkte können Sie über den Konfigurator aktivieren und deaktivieren. Es kann z. B. sinnvoll sein, den unverschlüsselten Endpunkt zu deaktivieren, damit sich alle Clients nur mit gültigem und als vertrauenswürdig eingestuftem Zertifikat verbinden können.

Über die Registerkarte **Server Settings** können Sie die Endpunkte, sowie einige Zusatzparameter, konfigurieren. Über das Kontextmenü lassen sich Endpunkte hinzufügen oder aus der Konfiguration entfernen.



4.4.10 Vertrauensstellung für Zertifikate

Über die Registerkarte **Online Panel** und den dortigen Bereich **Certificates** lassen sich die Vertrauensstellungen für Clientzertifikate auf dem TwinCAT OPC UA Server konfigurieren. Durch Selektion eines Clientzertifikats in dem jeweiligen TrustStore (Rejected/Accepted) lassen sich Zertifikatsdetails anzeigen und dieses zwischen den TrustStores verschieben.

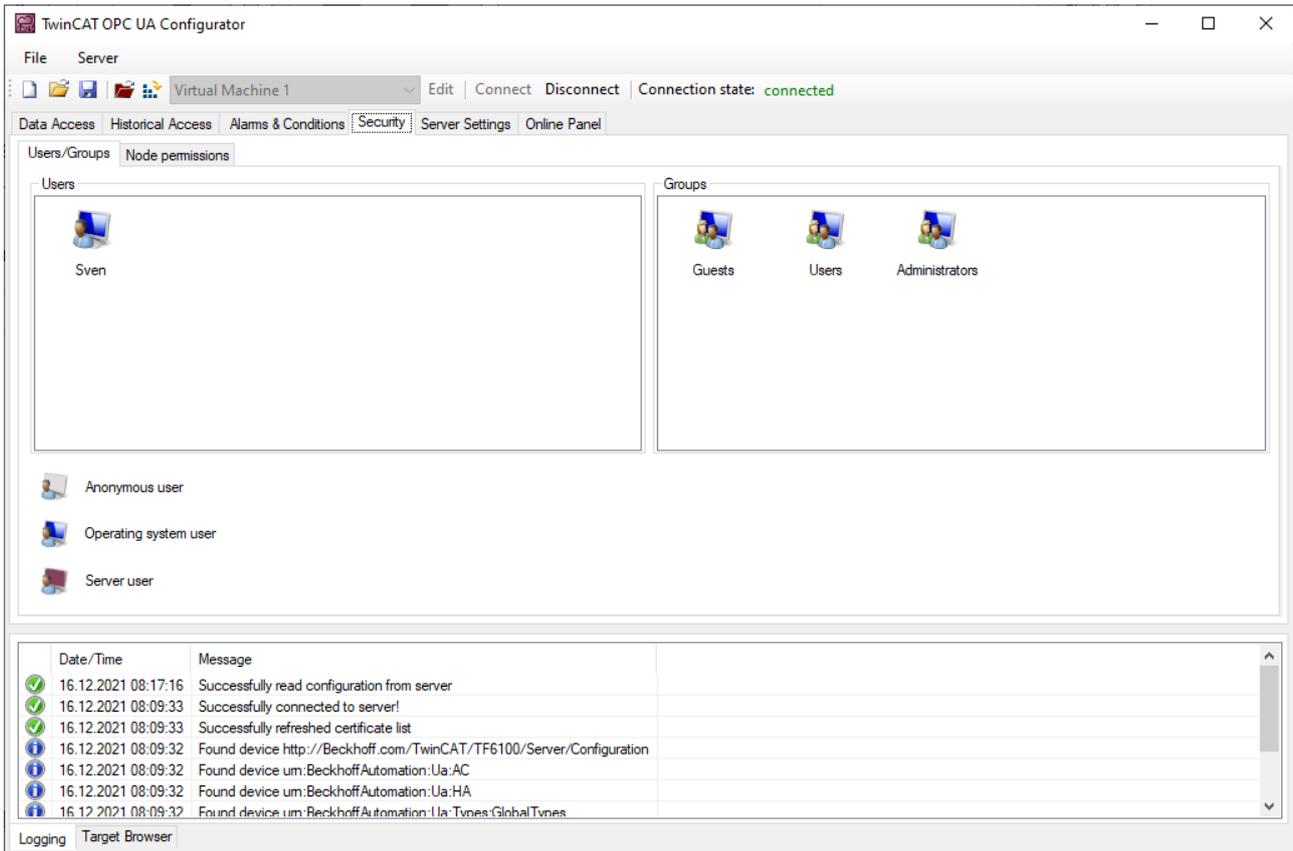


4.4.11 Sicherheitseinstellungen konfigurieren

Über die Registerkarte **Security** lassen sich Sicherheitseinstellungen am Server vornehmen. Diese Sicherheitseinstellungen können die folgenden Punkte beinhalten:

- Benutzer und Gruppen
- Zugriffsrechte für Gruppen auf Namespaces

- Zugriffsrechte für Gruppen auf einzelne Nodes



Benutzer und Gruppen

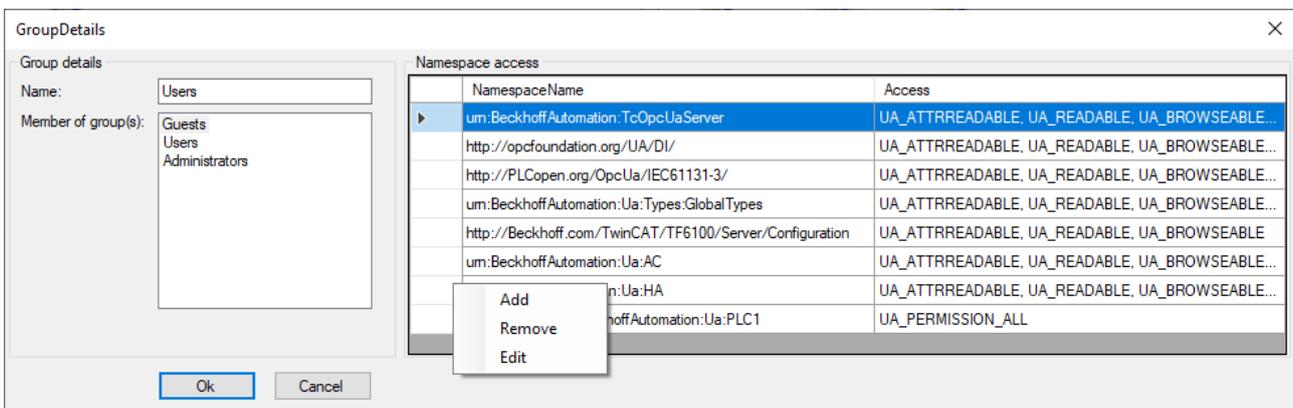
Zur Konfiguration von Zugriffsrechten müssen zunächst einmal Benutzer und Benutzergruppen erstellt werden. Im Auslieferungszustand des Servers sind bereits einige Gruppen vordefiniert. Über das Kontextmenü lassen sich neue Benutzer oder Gruppen zur Konfiguration hinzufügen.

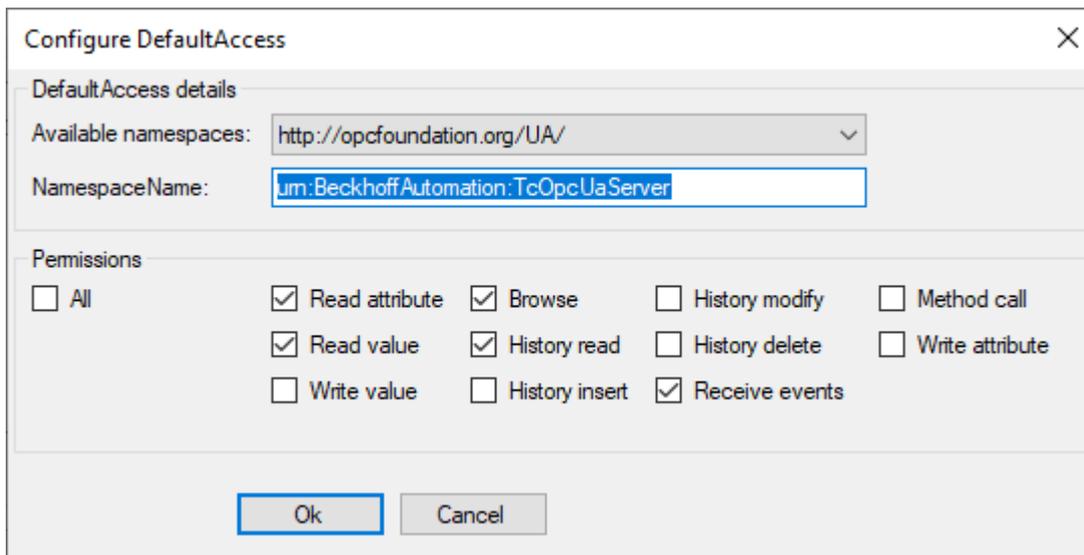
Ein Benutzer kann hierbei entweder der Anonymous-Benutzer, ein Betriebssystembenutzer oder ein Serverbenutzer sein. Wir empfehlen in jedem Fall die Konfiguration von Betriebssystembenutzern.

Eine Benutzergruppe kann einen sogenannten **Default-Access** konfiguriert haben. Hierbei handelt es sich um Zugriffsrechte auf einen bestimmten Namespace.

Zugriffsrechte auf Namespaces

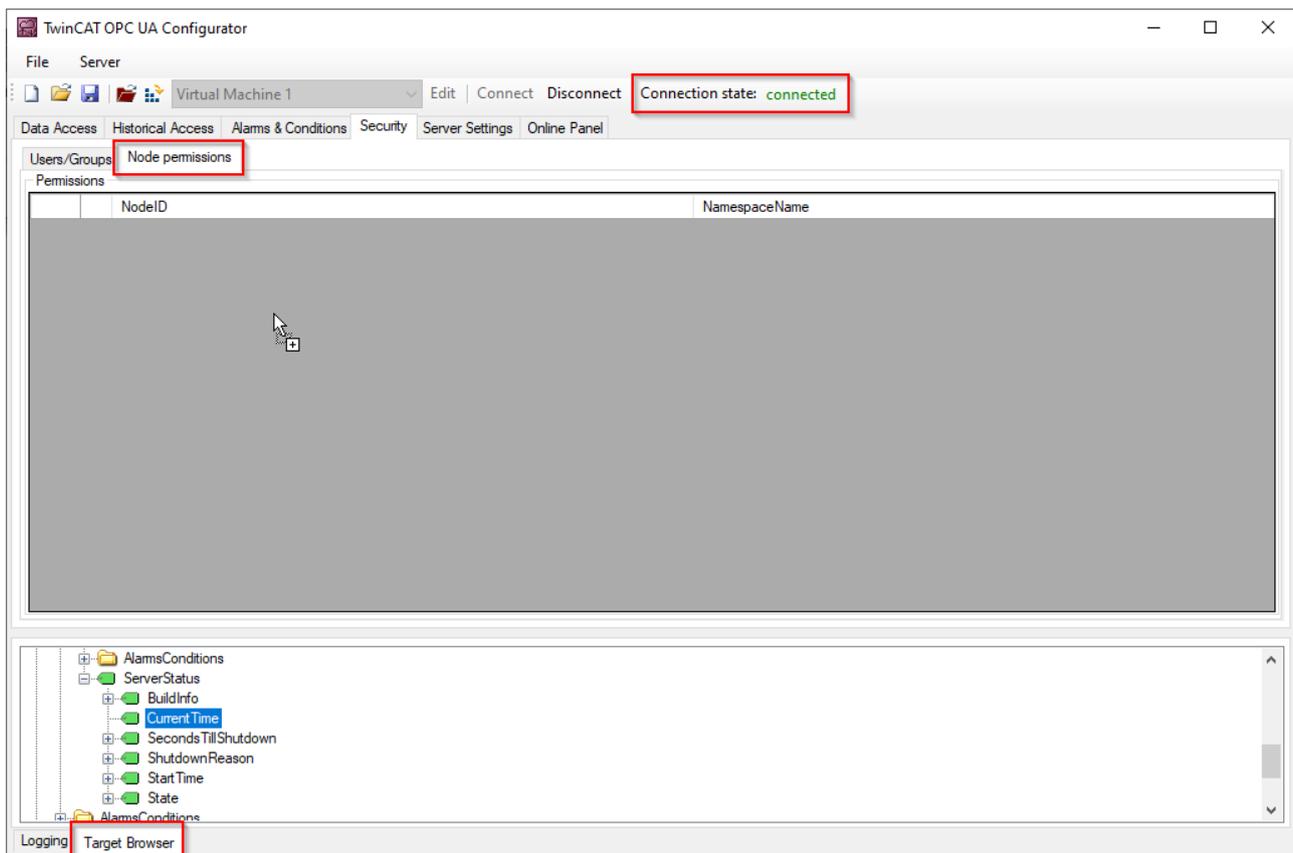
Zugriffsrechte auf bestimmte Namespaces lassen sich an einer Benutzergruppe definieren. In den Einstellungen der Gruppe gibt es hierbei einen entsprechenden Konfigurationsbereich, welcher sich über das Kontextmenü editieren lässt.



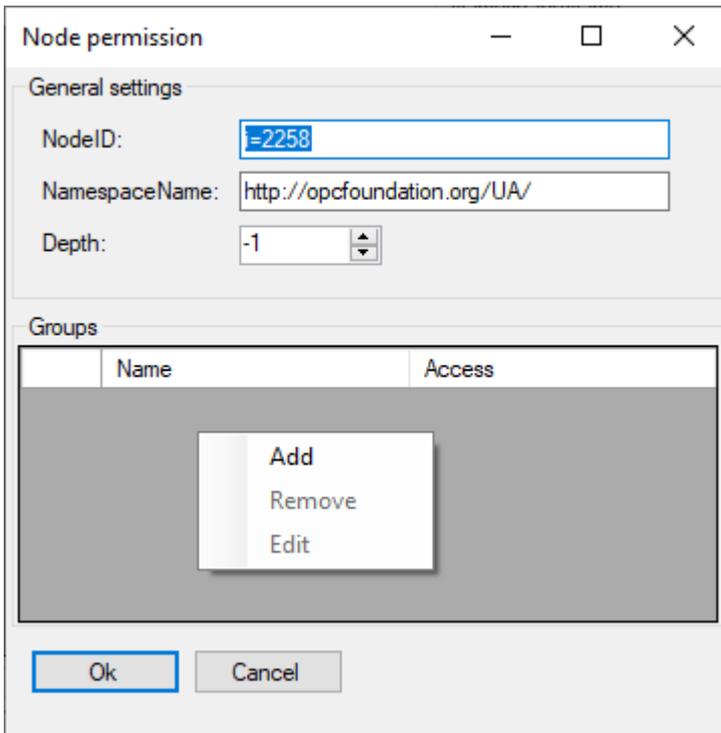


Zugriffsrechte auf einzelne Nodes

Über die Registerkarte **Node permissions** lassen sich Zugriffsrechte auf einzelne Nodes und deren Kindelemente definieren. Sie können die Nodes hierbei manuell über das Kontextmenü konfigurieren oder sie per Drag&Drop aus dem **Target Browser** zur Konfiguration hinzufügen, sofern Sie mit einem Server verbunden sind.



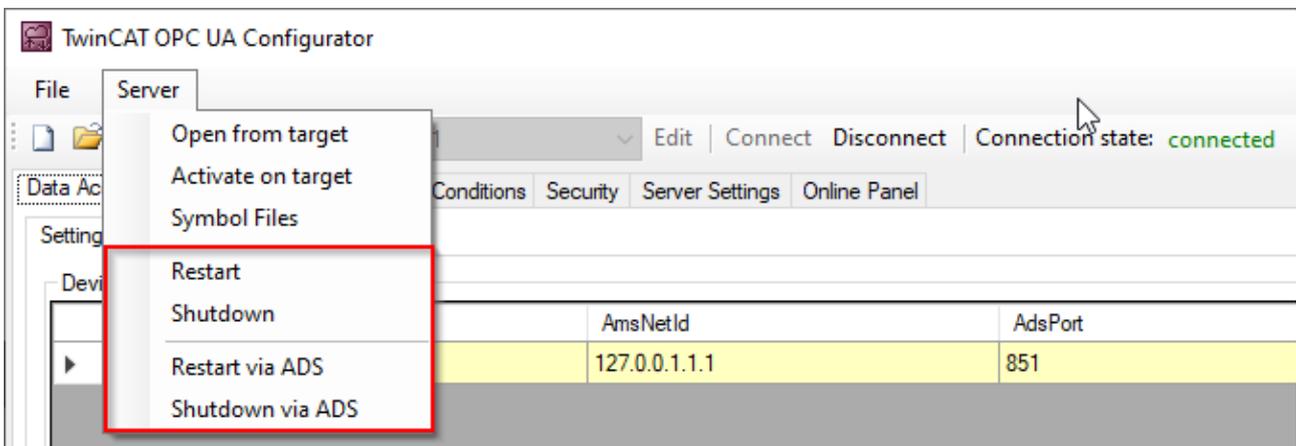
Im Node-Konfigurationsdialog lassen sich dann die Benutzergruppen und Zugriffsrechte der jeweiligen Gruppe definieren.



Über den Parameter **Depth** können Sie einstellen, ob die Berechtigungen auf Kindelemente vererbt werden sollen. Der Wert „-1“ gibt hierbei an, dass alle Kindelemente die Berechtigungen vererbt bekommen sollen.

4.4.12 Server neu starten

Über das **Server**-Menü lässt sich ein TwinCAT OPC UA Server neu starten. Üblicherweise möchten Sie den gerade über OPC UA verbundenen Server neu starten. Alternativ können Sie den Neustart auch über ADS antriggern, falls Sie eine ADS-Route zu dem Server-System hergestellt haben.



4.4.13 Logging

Für eine erweiterte Diagnose können Sie die Logging-Funktion des OPC UA Servers aktivieren.

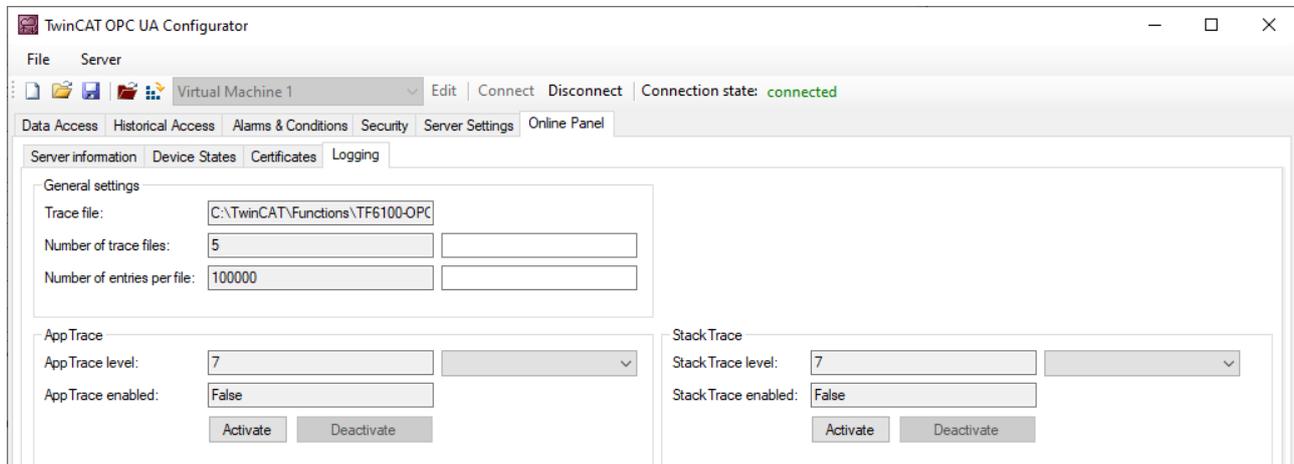
i **Schreiben der Log-Datei**

Durch das Aktivieren der Logging-Funktion auf dem Server wird eine Protokolldatei auf dem Dateisystem geschrieben. Stellen Sie sicher, dass ausreichend Speicherplatz zur Verfügung steht und setzen Sie die Logging-Parameter entsprechend (Anzahl Log-Dateien, Größe pro Log-Datei).

i Performance- und Timingverhalten

Durch das Aktivieren der Protokollfunktionen verändert sich das Timing-Verhalten des OPC UA Servers. Hierdurch können je nach Plattform und Projekt Geschwindigkeitseinbußen entstehen.

Über die Registerkarte **Online Panel** und den dortigen Bereich **Logging** lassen sich die Server-Protokollfunktionen aktivieren.



Trace-Level

Generell gilt: Je höher der „Trace level“, desto detailliertere (und mehr) Daten werden geschrieben, desto mehr Last wird jedoch auch auf der Serverapplikation verursacht, wodurch sich das Timingverhalten entsprechend ändert. Bitte aktivieren Sie daher das Logging nur im Diagnosefall und in Absprache mit dem Beckhoff Support.

Activate App Trace

In den meisten Fällen ist es ausreichend ein sogenanntes „AppTrace“ zu erstellen. Hierbei werden Informationen der Serverapplikation protokolliert. Zum Aktivieren des AppTrace tragen Sie bitte die Anzahl an TraceFiles, sowie die Anzahl Einträge pro TraceFile in die zugehörigen Textfelder ein. Anschliessend wählen Sie einen Tracelevel aus und klicken auf den Button zum Aktivieren des AppTrace. Die Werte in den grau hinterlegten Textfeldern stellen die aktuellen Einstellungen auf dem Server dar.

Activate Stack Trace

In einigen wenigen Fällen ist es zusätzlich notwendig ein sogenanntes „StackTrace“ zu erstellen, wodurch Informationen vom OPC UA Stack protokolliert werden. Zum Aktivieren des StackTrace tragen Sie bitte die Anzahl an TraceFiles, sowie die Anzahl Einträge pro TraceFile in die zugehörigen Textfelder ein. Anschliessend wählen Sie einen Tracelevel aus und klicken auf den Button zum Aktivieren des StackTrace. Die Werte in den grau hinterlegten Textfeldern stellen die aktuellen Einstellungen auf dem Server dar.

5 Anhang

5.1 ADS Return Codes

Gruppierung der Fehlercodes:

Globale Fehlercodes: 0x0000 [▶ 63]... (0x9811_0000 ...)

Router Fehlercodes: 0x0500 [▶ 63]... (0x9811_0500 ...)

Allgemeine ADS Fehler: 0x0700 [▶ 64]... (0x9811_0700 ...)

RTime Fehlercodes: 0x1000 [▶ 66]... (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_INVALIDAMSLLENGTH | 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_TLSSSEND | 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_LICENSEDEMODENIED | 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 | | | |

5.2 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

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

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

Beckhoff Unternehmenszentrale

Beckhoff Automation GmbH & Co. KG

Hülshorstweg 20
33415 Verl
Deutschland

Telefon: +49 5246 963-0
E-Mail: info@beckhoff.com
Internet: www.beckhoff.com

Mehr Informationen:
www.beckhoff.com/TS6100

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Deutschland
Telefon: +49 5246 9630
info@beckhoff.com
www.beckhoff.com

