

# ToddySoft Connect ADS Driver - Ignition 8.3

English version: [README.md](#)

Ignition-8.3-Modul zur Anbindung von Beckhoff-TwinCAT-SPSen über das ADS/AMS-Protokoll, mit Unterstützung für unverschlüsseltes TCP und verschlüsselte „Secure ADS“-Verbindungen (TLS).

Die Geräte-Konfiguration verwendet ein benutzerdefiniertes Konfigurationsformular, das sich an den ausgewählten **Transport** anpasst: Es werden nur die für den gewählten Transport relevanten Einstellungen angezeigt, sodass niemals Felder erscheinen, die nicht zutreffen.

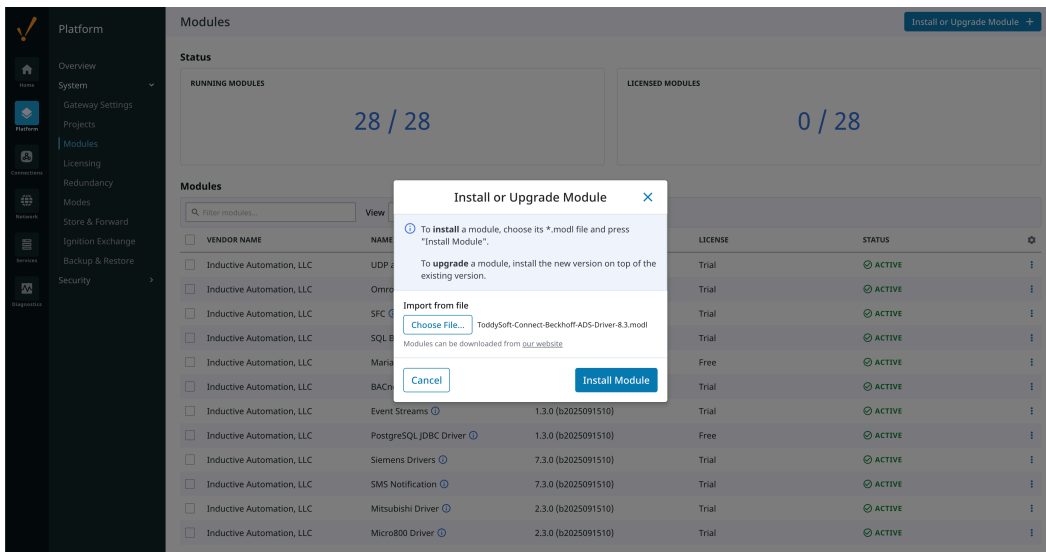
**Hinweis zur Sprache:** Bedienoberfläche, Feld- und Abschnittsnamen sowie Menüpfade sind in Ignition durchgängig **englisch**. Diese Begriffe (z. B. Host, Transport Settings, Keystore Path) bleiben daher auch in dieser deutschen Anleitung unverändert englisch, damit sie zu Oberfläche und Screenshots passen.

## Installation

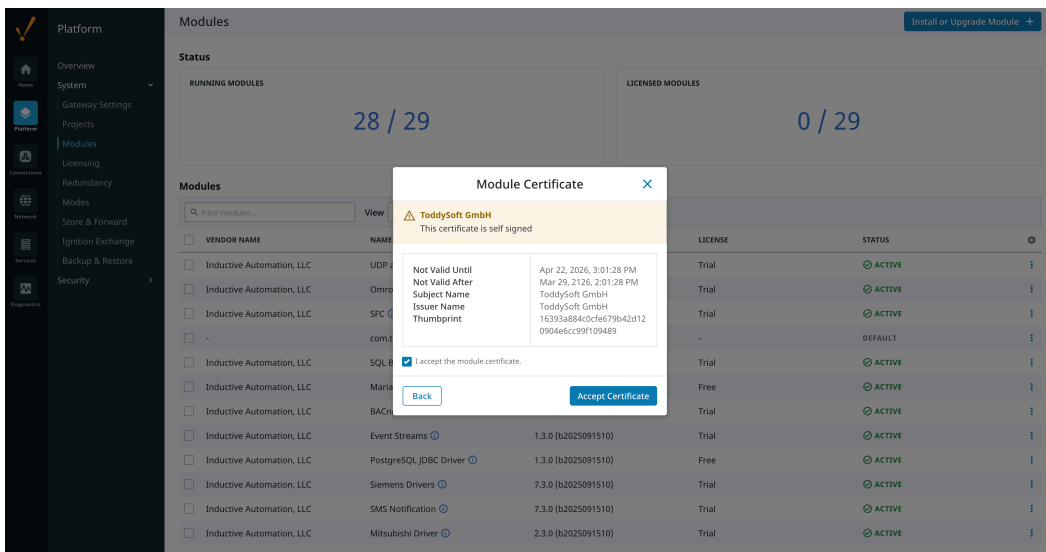
1. Öffnen Sie die Weboberfläche des Ignition Gateways und navigieren Sie zu **Config > System > Modules**.

<input type="checkbox"/>	VENDOR NAME	NAME	VERSION	LICENSE	STATUS	
<input type="checkbox"/>	Inductive Automation, LLC	UDP and TCP Drivers	7.3.0 (b2025091510)	Trial	ACTIVE	
<input type="checkbox"/>	Inductive Automation, LLC	Omron Driver	5.3.0 (b2025091510)	Trial	ACTIVE	
<input type="checkbox"/>	Inductive Automation, LLC	SFC	6.3.0 (b2025091510)	Trial	ACTIVE	
<input type="checkbox"/>	Inductive Automation, LLC	SQL Bridge	11.3.0 (b2025091510)	Trial	ACTIVE	
<input type="checkbox"/>	Inductive Automation, LLC	MariaDB JDBC Driver	1.3.0 (b2025091510)	Free	ACTIVE	
<input type="checkbox"/>	Inductive Automation, LLC	BACnet Driver	3.3.0 (b2025091510)	Trial	ACTIVE	
<input type="checkbox"/>	Inductive Automation, LLC	Event Streams	1.3.0 (b2025091510)	Trial	ACTIVE	
<input type="checkbox"/>	Inductive Automation, LLC	PostgreSQL JDBC Driver	1.3.0 (b2025091510)	Free	ACTIVE	
<input type="checkbox"/>	Inductive Automation, LLC	Siemens Drivers	7.3.0 (b2025091510)	Trial	ACTIVE	
<input type="checkbox"/>	Inductive Automation, LLC	SMS Notification	7.3.0 (b2025091510)	Trial	ACTIVE	
<input type="checkbox"/>	Inductive Automation, LLC	Mitsubishi Driver	2.3.0 (b2025091510)	Trial	ACTIVE	
<input type="checkbox"/>	Inductive Automation, LLC	Micro800 Driver	2.3.0 (b2025091510)	Trial	ACTIVE	

2. Klicken Sie auf **Install or Upgrade a Module....**



3. Wählen Sie die Datei `ToddySoft-Connect-Beckhoff-ADS-Driver-8.3.modl` aus und laden Sie sie hoch.



4. Bestätigen Sie die Lizenz-/Zertifikatsabfrage, um die Installation fortzusetzen.

**Modules**

**Status**

**RUNNING MODULES** 28 / 29

**LICENSED MODULES** 0 / 29

**Modules**

VENDOR NAME	NAME	VERSION	LICENSE	STATUS
Inductive Automation, LLC	UDP and TCP Drivers	7.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	Omron Driver	5.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	SFC	6.3.0 (b2025091510)	Trial	ACTIVE
ToddySoft GmbH	ToddySoft Connect Beckhoff ADS Driver	1.0.0-SNAPSHOT (b0)	n/a	INACTIVE PENDING RESTART
Inductive Automation, LLC	SQL Bridge	11.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	MariaDB JDBC Driver	1.3.0 (b2025091510)	Free	ACTIVE
Inductive Automation, LLC	BACnet Driver	3.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	Event Streams	1.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	PostgreSQL JDBC Driver	1.3.0 (b2025091510)	Free	ACTIVE
Inductive Automation, LLC	Siemens Drivers	7.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	SMS Notification	7.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	Mitsubishi Driver	2.3.0 (b2025091510)	Trial	ACTIVE

5. Warten Sie, bis das Gateway fertig ist, und prüfen Sie, ob das Modul in der Modulliste als **Running** angezeigt wird.

**Modules**

**Status**

**RUNNING MODULES** 29 / 29

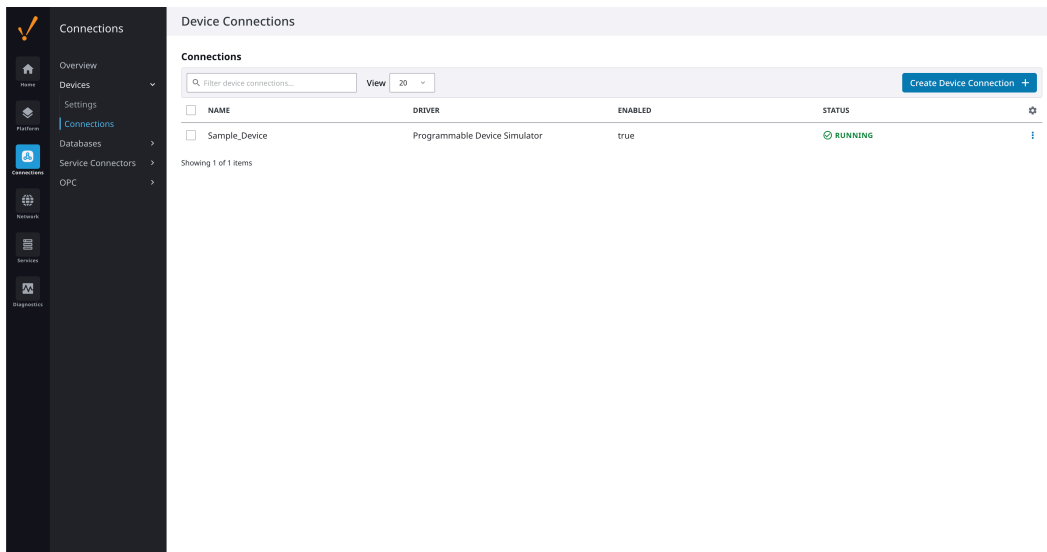
**LICENSED MODULES** 0 / 29

**Modules**

VENDOR NAME	NAME	VERSION	LICENSE	STATUS
Inductive Automation, LLC	UDP and TCP Drivers	7.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	Omron Driver	5.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	SFC	6.3.0 (b2025091510)	Trial	ACTIVE
ToddySoft GmbH	ToddySoft Connect Beckhoff ADS Driver	1.0.0-SNAPSHOT (b0)	Trial	ACTIVE
Inductive Automation, LLC	SQL Bridge	11.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	MariaDB JDBC Driver	1.3.0 (b2025091510)	Free	ACTIVE
Inductive Automation, LLC	BACnet Driver	3.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	Event Streams	1.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	PostgreSQL JDBC Driver	1.3.0 (b2025091510)	Free	ACTIVE
Inductive Automation, LLC	Siemens Drivers	7.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	SMS Notification	7.3.0 (b2025091510)	Trial	ACTIVE
Inductive Automation, LLC	Mitsubishi Driver	2.3.0 (b2025091510)	Trial	ACTIVE

## Erstellen einer Geräteverbindung (Device Connection)

1. Gehen Sie zu **Config > OPC UA > Device Connections**.



2. Klicken Sie auf **Create new Device...** und wählen Sie **ToddySoft Connect ADS Driver** als Gerätetyp.

### Create Device Connection

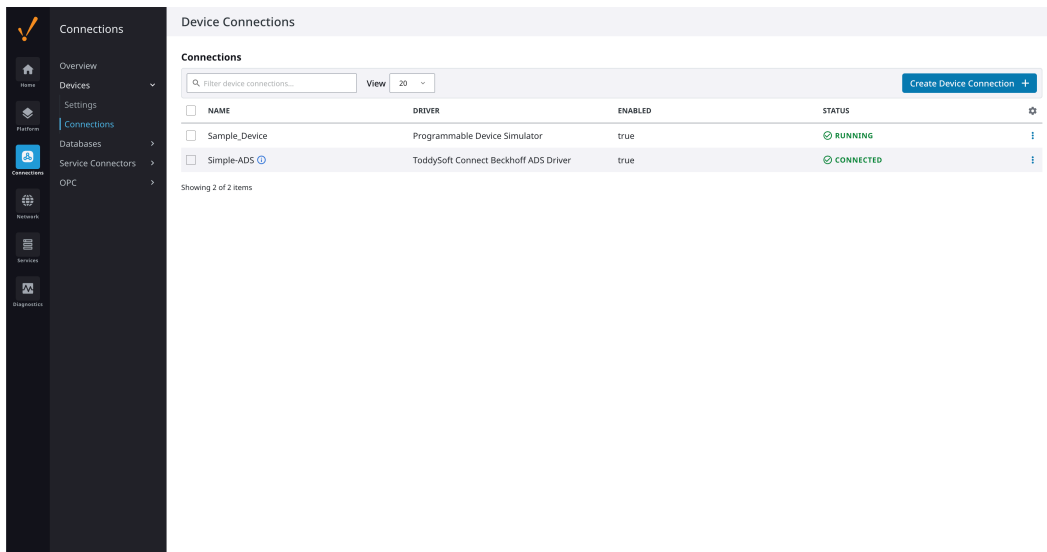
1. Select Driver

2. Configure Device

- Omron FINS/UDP**  
Connect to devices that implement FINS over UDP.
- Omron NJ Driver**  
Connect to Omron NJ series PLCs.
- Programmable Device Simulator**  
A simulator device that can be configured with a user-defined hierarchy of static or function-driven values.
- Siemens S7-1200 Driver**  
Connect to Siemens S7-1200 PLCs using absolute addressing.
- Siemens S7-1500 Driver**  
Connect to Siemens S7-1500 PLCs using absolute addressing.
- Siemens S7-300 Driver**  
Connect to Siemens S7-300 PLCs using absolute addressing.
- Siemens S7-400 Driver**  
Connect to Siemens S7-400 PLCs using absolute addressing.
- TCP Driver**
- ToddySoft Connect Beckhoff ADS Driver**  
ToddySoft Connect driver for Beckhoff TwinCAT ADS/AMS protocol
- UDP Driver**

3. Konfigurieren Sie die Verbindungseinstellungen (siehe die Abschnitte unten) und klicken Sie auf **Create Device Connection**.

4. Die neue Verbindung erscheint anschließend in der Liste der Device Connections.



## Konfiguration

Das Konfigurationsformular ist von oben nach unten in folgende Abschnitte gegliedert: **General**, **Transport**, **Transport Settings**, **ADS / AMS Settings**, **Advanced Transport Settings** und **Audit Log**.

### General

Vergibt einen Namen (und eine optionale Beschreibung) für die Verbindung und steuert, ob sie aktiviert ist.

**GENERAL**
\*Required

**Name \***

The name of this device connection.

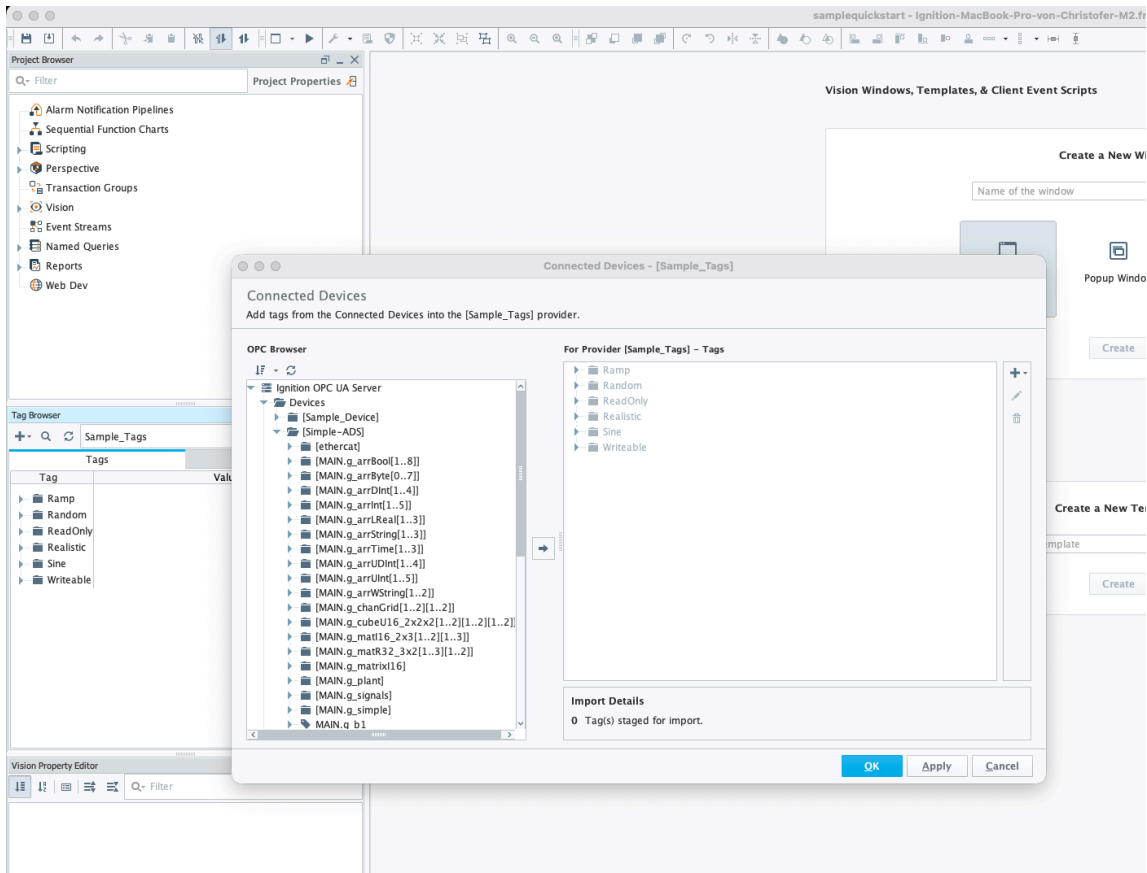
**Description**

**Enabled**

Set whether this device connection is enabled or disabled within the Gateway.

Einstellung	Beschreibung	Standard
<b>Name</b>	Eindeutiger Name für diese Geräteverbindung	
<b>Description</b>	Optionale Beschreibung dieser Verbindung	
<b>Enabled</b>	Ob die Verbindung aktiv ist	true

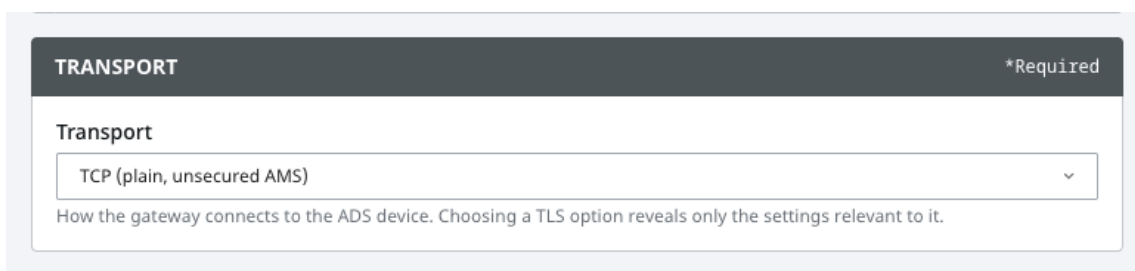
Unter diesem Namen wird die Verbindung in anderen Bereichen von Ignition referenziert:



Ist **Enabled** nicht aktiviert, wird keine Verbindung aufgebaut, bis sie aktiviert wird.

## Transport

Legt fest, wie das Gateway sich mit dem ADS-Gerät verbindet. Bei Auswahl einer der TLS-Optionen werden im darunterliegenden Abschnitt **Transport Settings** nur die jeweils relevanten Einstellungen angezeigt.



Transport	Beschreibung
<b>TCP (plain, unsecured AMS)</b>	Unverschlüsseltes ADS über TCP (Standard). Keine Zertifikate oder Schlüssel nötig.

<b>TLS-PSK</b>	Verschlüsselt („Secure ADS“) mit Pre-Shared Key + Identity. Keine Zertifikate.
<b>TLS-SSC (Self-Signed Certificate)</b>	Verschlüsselt mit einem automatisch erzeugten selbstsignierten Zertifikat.
<b>TLS-SCA (Shared Certificate Authority)</b>	Verschlüsselt mit Zertifikaten, die von einer gemeinsamen Zertifizierungsstelle (CA) signiert sind.

Sobald ein TLS-Transport ausgewählt ist, wechselt der Verbindungsport automatisch von **48898** auf **8016**, sofern nicht explizit ein abweichender Port gesetzt wurde.

**Speichern von Passwörtern und Schlüsseln:** Die von den TLS-Transporten verwendeten Geheimnisfelder ( *Keystore Password*, *Route Password* und *Pre-Shared Key* ) werden über die Secret-Verwaltung von Ignition 8.3 behandelt. Für jedes Feld können Sie **None** wählen, den Wert **Embedded** (verschlüsselt in der Gerätekonfiguration) speichern oder aus einem konfigurierten Secret-Provider **Referenced** referenzieren. Werte werden niemals im Klartext gespeichert.

## Transport Settings

Enthält immer **Host** und **Port**; die übrigen Felder hängen vom gewählten Transport ab.

Einstellung	Beschreibung	Standard
<b>Host</b>	Hostname oder IP-Adresse des TwinCAT-Geräts	localhost
<b>Port</b>	TCP-Portnummer (Standard 48898; TLS: 8016)	48898

### TCP (plain, unsecured AMS)

Bei reinem TCP werden nur Host und Port angezeigt — keine Sicherheitsfelder.

TRANSPORT SETTINGS
\*Required

**Host\***

Hostname or IP address of the ADS device.

**Port\***

ADS/AMS TCP port (default 48898; TLS transports use 8016).

### TLS-PSK

Verwendet TLS-PSK, bei dem beide Seiten einen geheimen Schlüssel und eine Identity-Zeichenkette teilen. Es sind keine Zertifikate nötig — dies ist die einfachste Möglichkeit, die ADS-Kommunikation zu verschlüsseln.

## TRANSPORT SETTINGS

\*Required

### Host\*

192.168.24.50

Hostname or IP address of the ADS device.

### Port\*

48898

ADS/AMS TCP port (default 48898; TLS transports use 8016).

### Identity\*

MYPSKUSER

PSK Identity name for TLS-PSK authentication.

### Pre-Shared Key\*

- None  
 Embedded

Secret

[SHOW](#)

.....

- Referenced

### Route Name

MyDevMachine222

Route name for secure ADS route registration. Defaults to the gateway hostname if left empty.

### Route Username

Administrator

Username for secure ADS route registration.

### Route Password

- None  
 Embedded

Secret

[SHOW](#)

.

- Referenced

Einstellung	Beschreibung	Standard
<b>Identity</b>	PSK-Identity-Zeichenkette (muss mit der SPS-Konfiguration übereinstimmen)	(leer)
<b>Pre-Shared Key</b>	Hex-kodierter gemeinsamer geheimer Schlüssel (Geheimnis-Feld)	(None)
<b>Route Name</b>	Name für die Secure-ADS-Route auf der SPS	(Gateway-Hostname)

<b>Route Username</b>	Benutzername für die Secure-ADS-Routenregistrierung	Administrator
<b>Route Password</b>	Passwort für die Secure-ADS-Routenregistrierung (Geheimnis-Feld)	(None)

**Konfiguration der SPS für PSK:** Die SPS muss mit passenden PSK-Einstellungen konfiguriert werden. In der TwinCAT-Secure-ADS-Konfiguration (üblicherweise in `/etc/TwinCAT/3.1/Target/StaticRoutes.xml`):

- Setzen Sie die **Identity** auf den in Ignition verwendeten Wert (z. B. `MYPISKUSER`)
- Setzen Sie das **Password/Key**, aus dem der Pre-Shared Key abgeleitet wird

```
<Server>
  <Tls>
    <Psk>
      <Identity>MYPISKUSER</Identity>
      <Pwd>MySecret</Pwd>
    </Psk>
  </Tls>
</Server>
</RemoteConnections>
</TcConfig>
```

TwinCAT leitet den PSK-Schlüssel durch Berechnung von `SHA-256(Identity + Password)` ab. Beachten Sie, dass die Identity **vollständig in Großbuchstaben** angegeben werden muss. So berechnen Sie den für die Ignition-Konfiguration benötigten Hex-Schlüssel:

```
echo -n "<Identity><Password>" | shasum -a 256
```

Beispiel mit Identity `MYPISKUSER` und Password `MySecret` :

```
echo -n "MYPISKUSERMySecret" | shasum -a 256
# Ergebnis: a50d3154fea7bb54eec6710164e33ced872223f0a0ff05179e93e89e7f76c6f0
```

Verwenden Sie die resultierende 64-stellige Hex-Zeichenkette als Wert für **Pre-Shared Key** in Ignition (Embedded oder Referenced gespeichert).

Bei erfolgreicher Verbindung wird eine neue Routenkonfiguration zu `/etc/TwinCAT/3.1/Target/StaticRoutes.xml` hinzugefügt:

```
<Route>
  <Name>MyDevMachine</Name>
  <Address>192.168.24.220</Address>
  <NetId>192.168.24.220.1</NetId>
  <Type>TCP_IP</Type>
  <Tls>
    <Psk>
      <Identity>MYPISKUSER</Identity>
      <Key>a50d3154fea7bb54eec6710164e33ced872223f0a0ff05179e93e89e7f76c6f0</Key>
    </Psk>
  </Tls>
</Route>
```

**TLS-SSC (Self-Signed Certificate) und TLS-SCA (Shared Certificate Authority)**

Beide zertifikatbasierten Transporte verwenden denselben Satz an Feldern. **TLS-SSC** verwendet ein automatisch erzeugtes selbstsigniertes Zertifikat (das Modul verwaltet einen PKCS12-Keystore und richtet die ADS-Route bei der ersten Verbindung ein). **TLS-SCA** verwendet Zertifikate, die von einer gemeinsamen Zertifizierungsstelle signiert sind, der sowohl Ignition als auch die SPS vertrauen — die sicherste Option für den Produktivbetrieb.

**TRANSPORT SETTINGS**
\*Required

**Host\***

Hostname or IP address of the ADS device.

**Port\***

ADS/AMS TCP port (default 48898; TLS transports use 8016).

**Keystore Path\***

Path to the PKCS12 keystore file. Defaults to the module's auto-generated keystore if left empty.

**Keystore Password**

None  
 Embedded  
 Referenced

**Secret** SHOW

**Ignore Common Name**

Skip common name (CN) validation on the server certificate.

**Route Name**

Route name for secure ADS route registration. Defaults to the gateway hostname if left empty.

**Route Username**

Username for secure ADS route registration.

**Route Password**

None  
 Embedded  
 Referenced

**Secret** SHOW

Einstellung	Beschreibung	Standard
-------------	--------------	----------

<b>Keystore Path</b>	Pfad zur PKCS12-Keystore-Datei. Bei TLS-SSC leer lassen, um den automatisch erzeugten Keystore des Moduls zu verwenden; bei TLS-SCA auf das CA-signierte Zertifikat verweisen.	<i>(automatisch / erforderlich)</i>
<b>Keystore Password</b>	Passwort für den Keystore (Geheimnis-Feld)	<i>(None)</i>
<b>Ignore Common Name</b>	Überspringt die Common-Name-(CN-)Prüfung des Server-Zertifikats (nur für Tests verwenden)	false
<b>Route Name</b>	Name für die Secure-ADS-Route auf der SPS	<i>(Gateway-Hostname)</i>
<b>Route Username</b>	Benutzername für die Secure-ADS-Routenregistrierung	Administrator
<b>Route Password</b>	Passwort für die Secure-ADS-Routenregistrierung (Geheimnis-Feld)	<i>(None)</i>

Wenn kein Keystore-Pfad angegeben ist (TLS-SSC), erzeugt das Modul automatisch einen Keystore im Einstellungsverzeichnis des Moduls. Bei erfolgreicher Verbindung wird eine neue Routenkonfiguration zur Datei `/etc/TwinCAT/3.1/Target/StaticRoutes.xml` der SPS hinzugefügt.

### **ADS / AMS Settings**

Konfiguriert die ADS-spezifische Adressierung. Diese Einstellungen gelten unabhängig vom gewählten Transport.

## ADS / AMS SETTINGS

### Target AMS Net ID

AMS Net ID of the target device, format x.x.x.x.x.x (6 octets).

### Target AMS Port\*

AMS port of the target (851 = TC3 runtime 1, 852/853 = runtime 2/3, 801 = TC2). Pick a common value or type a custom one.

### Source AMS Net ID

AMS Net ID of this gateway, format x.x.x.x.x.x. Leave empty to derive automatically.

### Source AMS Port

AMS port of this gateway (0 = auto-assign).

### Request Timeout (ms)

ADS request timeout in milliseconds.

### Browse Queries

Symbol browse query filter (e.g. MAIN.\*).

Einstellung	Beschreibung	Standard
<b>Target AMS Net ID</b>	AMS Net ID des Zielgeräts (Format x.x.x.x.x.x). Standard: {target-ip}.1.1	(automatisch)
<b>Target AMS Port</b>	AMS-Port der Ziel-SPS-Runtime — gängigen TwinCAT-Port wählen oder eigenen Wert eingeben	851
<b>Source AMS Net ID</b>	AMS Net ID dieses Gateways (Format x.x.x.x.x.x). Leer lassen für automatische Ableitung	(automatisch)
<b>Source AMS Port</b>	AMS-Port dieses Gateways (0 = automatisch zuweisen)	0
<b>Request Timeout</b>	Standard-Timeout für ADS-Anfragen in Millisekunden	4000
<b>Browse Queries</b>	Filter für die Symbol-Browse-Abfrage (z. B. MAIN.*)	MAIN.*

Wenn im Feld **Target AMS Net ID** kein Wert angegeben ist, wird er durch Anhängen von `.1.1` an die lokale IP-Adresse der TCP-Verbindung berechnet. Beachten Sie, dass es mehrere Pfade zur SPS geben kann (wenn

das Gerät mehrere IP-Adressen besitzt). Um zu steuern, welche lokale IP-Adresse verwendet wird, setzen Sie **Local Address** im Abschnitt Advanced Transport Settings.

Das Feld **Target AMS Port** bietet die gängigen TwinCAT-Runtime-Ports als Vorschläge mit Beschreibung an, erlaubt aber weiterhin beliebige eigene Werte:

Port	Beschreibung
851	TwinCAT 3 – PLC runtime 1 (Standard)
852 / 853	TwinCAT 3 – PLC runtime 2 / 3
801	TwinCAT 2 – PLC runtime 1
811 / 821 / 831	TwinCAT 2 – PLC runtime 2 / 3 / 4

### Advanced Transport Settings

Hardwarenähere TCP-Feineinstellungen. Diese gelten für den jeweils aktiven Transport.

## ADVANCED TRANSPORT SETTINGS

### Connect Timeout (ms)

Connection timeout in milliseconds (0 = default).

### Read Timeout (ms)

Socket read timeout in milliseconds (0 = no timeout).

### Write Timeout (ms)

Socket write timeout in milliseconds (0 = no timeout).

### TCP No-Delay

Enable TCP\_NODELAY (disable Nagle's algorithm).

### TCP Keep-Alive

Enable TCP\_KEEPALIVE.

### Send Buffer Size

Send buffer size in bytes.

### Receive Buffer Size

Receive buffer size in bytes.

### Local Address

Local address to bind to (blank = all interfaces).

### Local Port

Local port to bind to (0 = ephemeral port).

Einstellung	Beschreibung	Standard
<b>Connect Timeout</b>	Verbindungs-Timeout in Millisekunden (0 = Standard)	5000
<b>Read Timeout</b>	Socket-Lese-Timeout in Millisekunden (0 = kein Timeout)	0
<b>Write Timeout</b>	Socket-Schreib-Timeout in Millisekunden (0 = kein Timeout)	0
<b>TCP No-Delay</b>	TCP_NODELAY aktivieren (Nagle-Algorithmus deaktivieren)	true
<b>TCP Keep-Alive</b>	TCP_KEEPALIVE aktivieren	false

<b>Send Buffer Size</b>	Sendepuffergröße in Bytes	81920
<b>Receive Buffer Size</b>	Empfangspuffergröße in Bytes	81920
<b>Local Address</b>	Lokale Bind-Adresse, ausgewählt aus den Netzwerkschnittstellen des Gateways (leer = alle Schnittstellen)	( <i>alle</i> )
<b>Local Port</b>	Lokaler Bind-Port (0 = ephemerer Port)	0

Das Feld **Local Address** ist eine Auswahlliste mit den lokalen IPv4-Adressen des Gateway-Rechners, was besonders nützlich ist, wenn der Host mehrere Schnittstellen besitzt (siehe die Hinweise zu Docker und VPN unten).

### Audit Log

Das `Audit Log` schreibt wichtige Diagnoseinformationen in eine eigene Protokolldatei. Diese Datei kann schnell wachsen; es wird daher empfohlen, sie nur zur Fehleranalyse zu aktivieren.

**AUDIT LOG**

**Audit Log File**

Path to a file to which protocol audit events are written (leave empty to disable).

Einstellung	Beschreibung	Standard
<b>Audit Log File</b>	Absoluter Pfad zur Audit-Log-Datei, in die Ereignisse geschrieben werden. Leer lassen zum Deaktivieren.	( <i>leer</i> )

HINWEIS: Stellen Sie sicher, dass der Benutzer, unter dem der `Ignition`-Prozess läuft, Schreibzugriff auf diesen Pfad hat.

Das Audit-Log-System erstellt die Datei automatisch und rotiert sie (komprimierte Dateien werden daneben angelegt), sobald eine bestimmte Größe erreicht ist oder zeitgesteuert.

### Tag-Adressierung

Tags werden über symbolische Namen aus dem SPS-Programm adressiert:

<code>MAIN.bStart</code>	# Boolescher Wert
<code>MAIN.iCounter</code>	# Ganzzahl
<code>MAIN.fTemperature</code>	# Gleitkommazahl
<code>GVL.sStatus</code>	# Zeichenkette
<code>MAIN.stMotor.fSpeed</code>	# Struktur-Member
<code>MAIN.aValues[0]</code>	# Array-Element
<code>MAIN.stArray[1].nField</code>	# Feld eines Struktur-Array-Elements

Konfigurieren Sie **Browse Queries** (z. B. `MAIN.*`), um zu steuern, welche Symbole beim Durchsuchen der Tags im Ignition Designer angezeigt werden.

## Tag-Gruppen (Tag Groups)

Standardmäßig werden alle Tags in der Standard-Tag-Gruppe gesammelt, das heißt, alle ausgewählten Tags werden im Standardintervall von einmal pro Sekunde abgefragt.

Wenn unterschiedliche Intervalle gewünscht sind, erstellen Sie zusätzliche Tag-Gruppen, konfigurieren Sie dort die gewünschten Intervalle und weisen Sie die Tags den entsprechenden Tag-Gruppen zu.

## Fehlerbehebung

### Gerät zeigt „Faulted“:

- Prüfen Sie, ob Hostname/IP der SPS erreichbar ist
- Prüfen Sie, ob die AMS Net IDs mit der TwinCAT-Konfiguration übereinstimmen
- Stellen Sie sicher, dass Port 48898 (bzw. 8016 für TLS) nicht durch eine Firewall blockiert wird
- Prüfen Sie die Gateway-Protokolle: **Status > Diagnostics > Logs**

### Tags zeigen schlechte Qualität (bad quality):

- Prüfen Sie, ob die Variable im SPS-Programm existiert
- Prüfen Sie Schreibweise und Groß-/Kleinschreibung
- Stellen Sie sicher, dass das SPS-Programm läuft

### TLS-Verbindung schlägt fehl:

- Bei TLS-PSK: prüfen Sie, ob Identity und Schlüssel auf beiden Seiten übereinstimmen
- Bei TLS-SSC: prüfen Sie, ob die Route-Zugangsdaten korrekt sind
- Bei TLS-SCA: stellen Sie sicher, dass beide Zertifikate von derselben CA signiert sind

### Docker-bezogene Probleme

Wenn `Ignition` innerhalb von `Docker` läuft, erhält der Host eine IP-Adresse aus dem Docker-internen Netzwerk. Beim Verbinden mit der SPS stammt die Verbindung von einer der IP-Adressen des Hosts. In diesem Fall benötigt die Verbindung eine **Source AMS Net ID**, die auf die IP-Adresse des Hosts verweist (und über **Local Address** in den Advanced Transport Settings lässt sich die ausgehende Schnittstelle festlegen).

Üblicherweise muss zusätzlich der **Source AMS Port** gesetzt werden. Dessen Wert ist eigentlich unerheblich — `54321` funktioniert in der Regel.

### VPN-bezogene Probleme

Beim Verbinden mit einer entfernten SPS über ein VPN erhält der Host je nach VPN-Typ üblicherweise eine lokale VPN-IP-Adresse. Wie bei Docker setzen Sie eine **Source AMS Net ID**, die auf diese zugewiesene IP-Adresse verweist.

Üblicherweise muss zusätzlich der **Source AMS Port** gesetzt werden. Dessen Wert ist eigentlich unerheblich — `54321` funktioniert in der Regel.