ToddySoft Connect ADS Driver - Ignition 8.1

English version: README.md

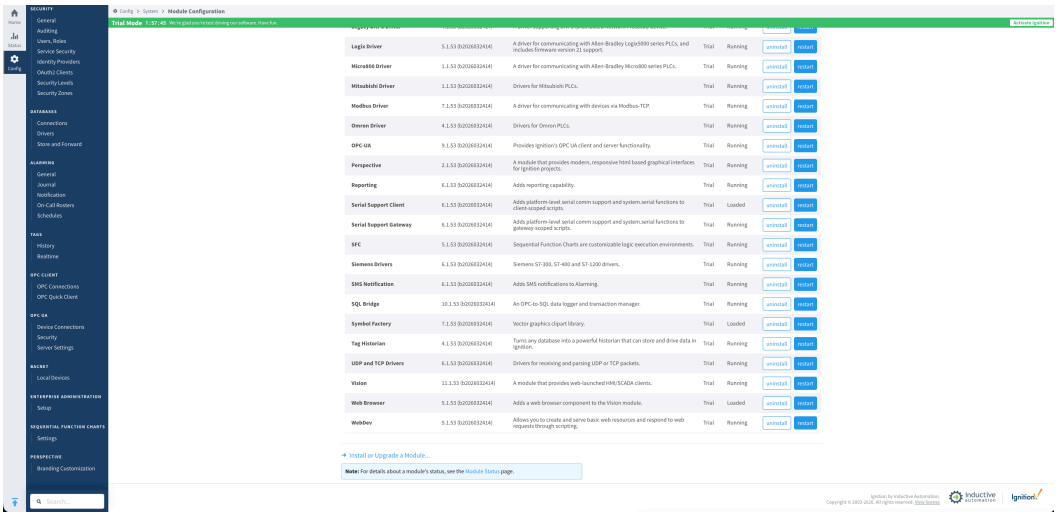
Ignition-8.1-Modul zur Anbindung von Beckhoff-TwinCAT-SPSen über das ADS/AMS-Protokoll, mit Unterstützung für unverschlüsseltes TCP und verschlüsselte „Secure ADS"-Verbindungen (TLS).

> ***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.*

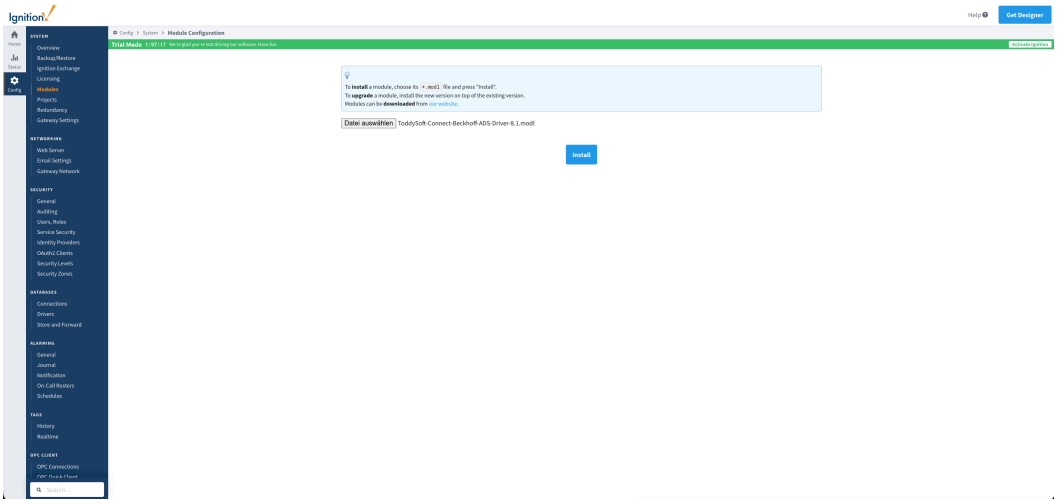
Installation

Die ToddySoft-Connect-Module sind mit einem selbstsignierten Zertifikat (ausgestellt auf *ToddySoft GmbH*) signiert und nicht mit einem öffentlich anerkannten Code-Signing-Zertifikat. Ignition bittet Sie daher einmalig, dieses Zertifikat während der Installation zu prüfen und zu akzeptieren - danach wird es für alle künftigen ToddySoft-Module mit demselben Zertifikat dauerhaft akzeptiert.

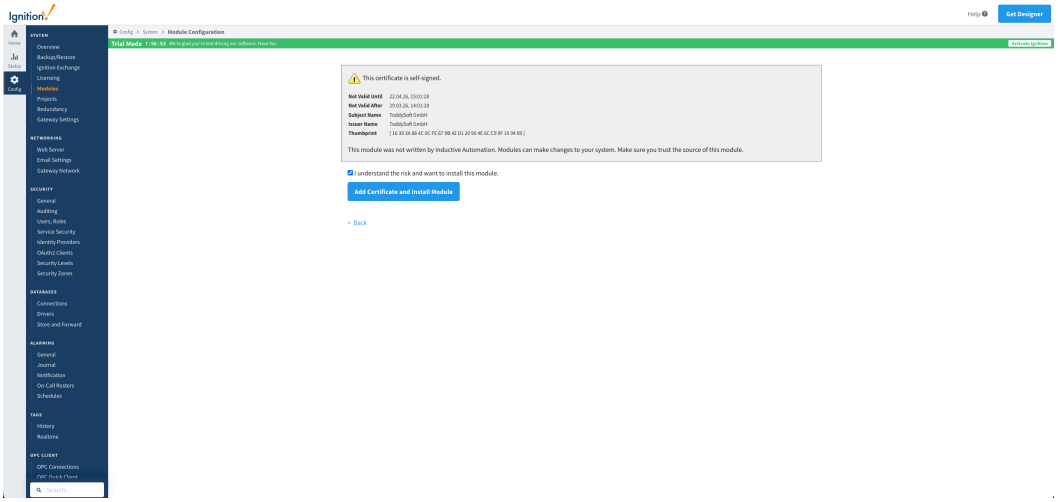
1. Öffnen Sie die Weboberfläche des Ignition Gateways und navigieren Sie zu **Config > System > Modules**. Scrollen Sie nach unten und klicken Sie auf **Install or Upgrade a Module...**.



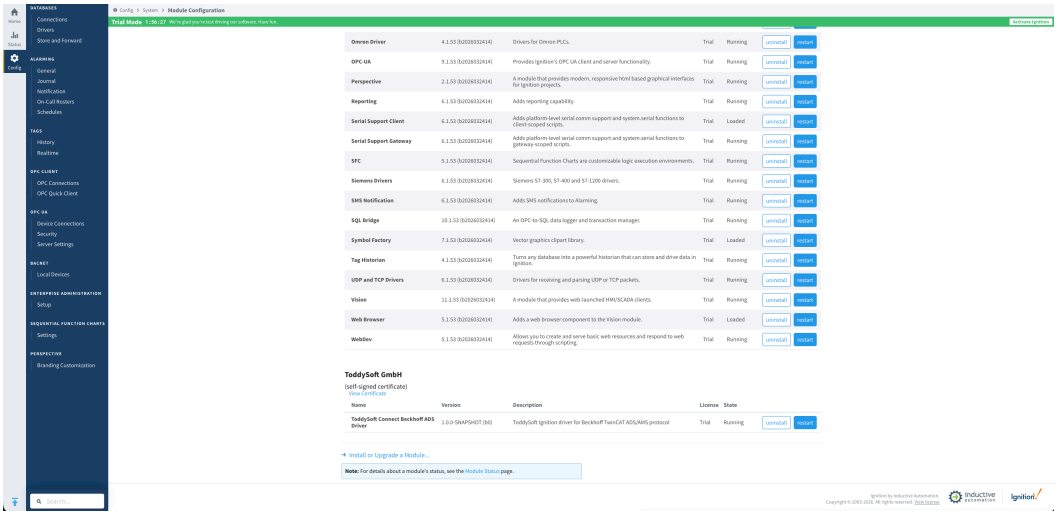
2. Wählen Sie die Datei `ToddySoft-Connect-Beckhoff-ADS-Driver-8.1.modl` aus und klicken Sie auf **Install**.



3. Ignition zeigt die Details des selbstsignierten Zertifikats (Subject und Issuer *ToddySoft GmbH*) zusammen mit einem Hinweis, dass das Modul nicht von Inductive Automation stammt. Prüfen Sie das Zertifikat, setzen Sie das Häkchen bei **I understand the risk and want to install this module** und klicken Sie auf **Add Certificate and Install Module**.

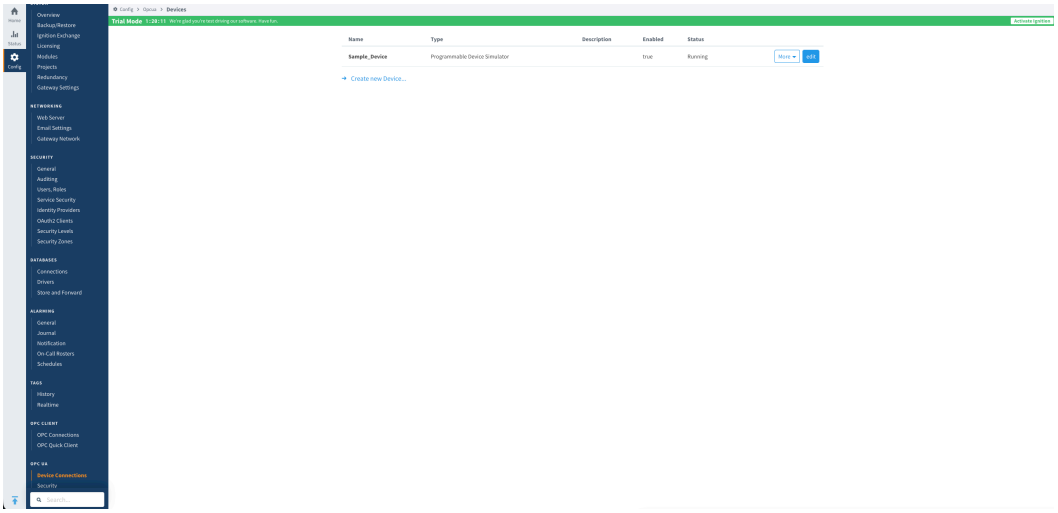


4. Das Modul ist nun vertrauenswürdig und wird unter der Gruppe **ToddySoft GmbH (self-signed certificate)** mit dem Status **Running** aufgeführt.

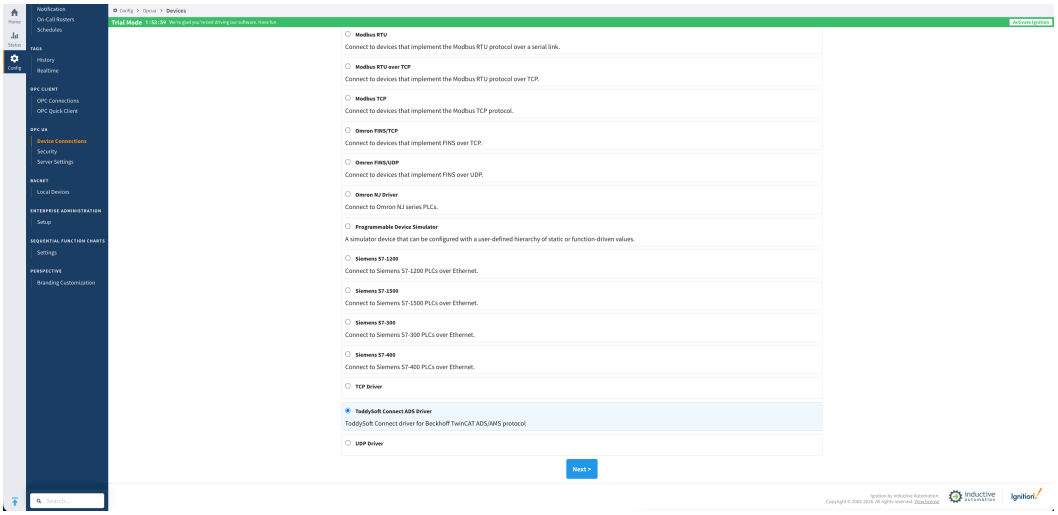


Erstellen einer Geräteverbindung (Device Connection)

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

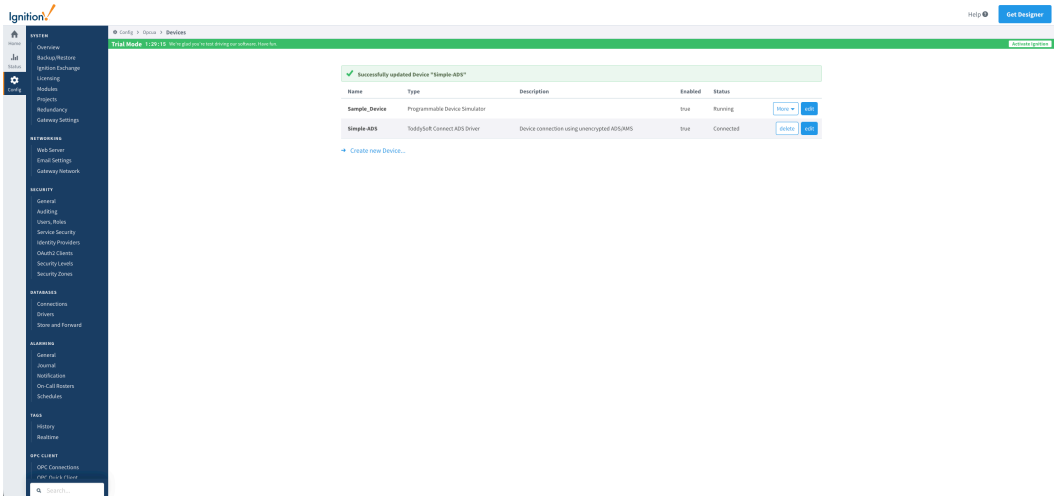


2. Klicken Sie auf **Create new Device...**, wählen Sie **ToddySoft Connect ADS Driver** als Gerätetyp und klicken Sie auf **Next**.



3. Konfigurieren Sie die Verbindungseinstellungen (siehe die Abschnitte unten) und klicken Sie auf **Save**.

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

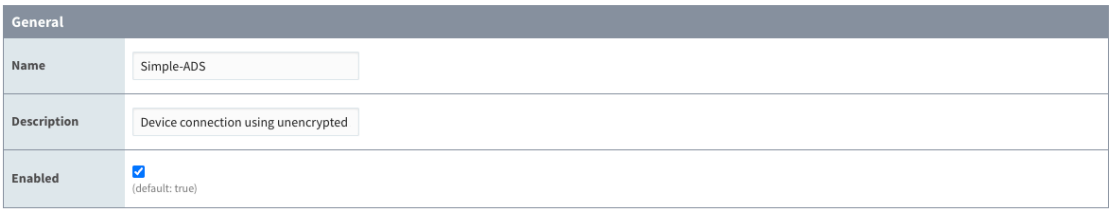


Einstellungsblöcke

Die Konfiguration ist in Kategorien gegliedert: **General**, **Transport Settings**, **ADS Settings**, **TCP Advanced Settings**, **Audit Log Settings** und **TLS Settings**.

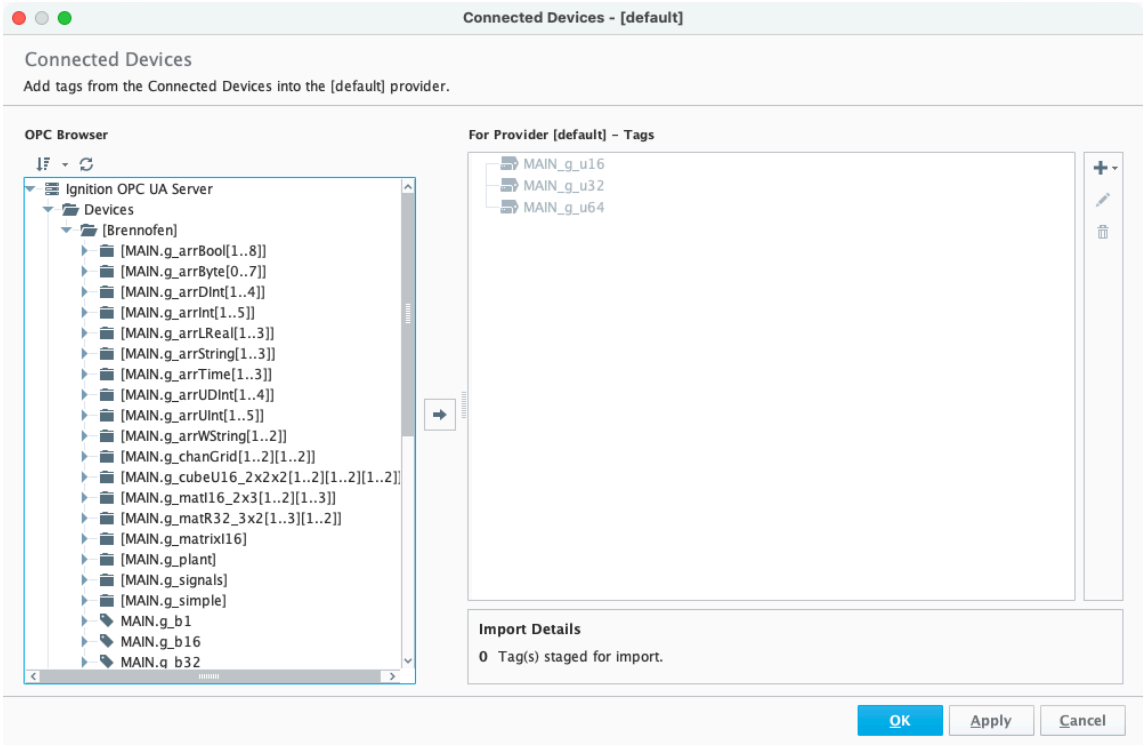
General

Dieser Block vergibt im Wesentlichen einen Namen für die Verbindung.



Einstellung	Beschreibung	Standard
Name	Eindeutiger Name für diese Geräteverbindung	
Description	Optionale Beschreibung dieser Verbindung	
Enabled	Ob die Verbindung aktiv ist	`true`

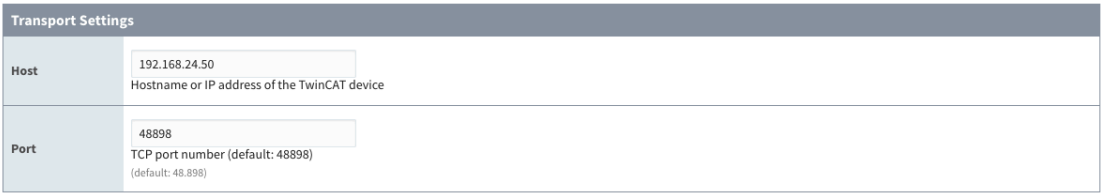
Unter diesem Namen wird die Verbindung in anderen Bereichen von Ignition referenziert:



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

Transport Settings

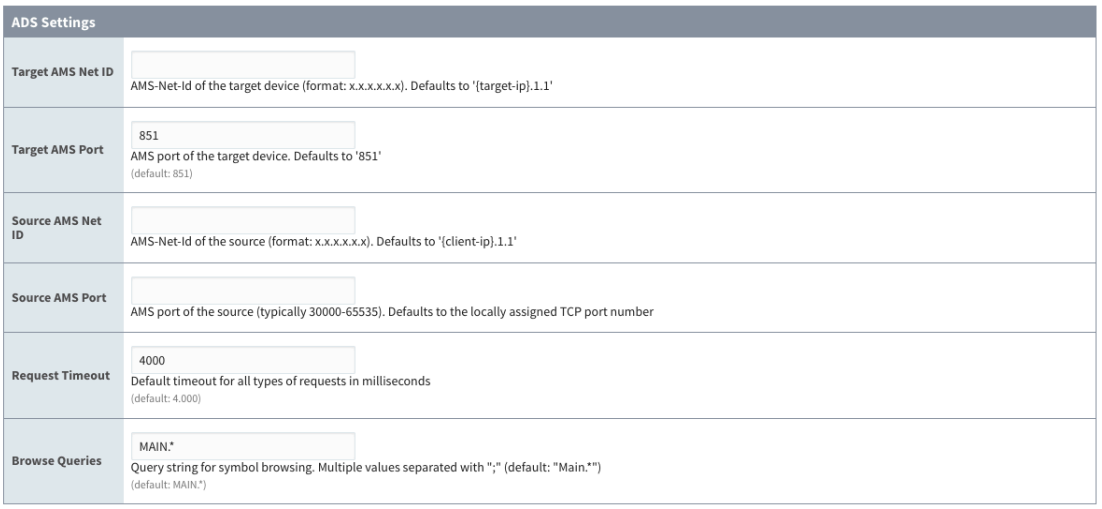
Der Endpunkt des TwinCAT-Geräts.



Einstellung	Beschreibung	Standard
Host	Hostname oder IP-Adresse des TwinCAT-Geräts	`localhost`
Port	TCP-Portnummer (Standard: 48898, TLS: 8016)	`48898`

ADS Settings

Dieser Block konfiguriert die ADS-spezifischen Einstellungen.



Einstellung	Beschreibung	Standard
Target AMS Net ID	AMS Net ID des Zielgeräts (Format: `x.x.x.x.x.x`). Standard: `{target-ip}.1.1`	*(automatisch)*
Target AMS Port	AMS-Port des Zielgeräts	`851`
Source AMS Net ID	AMS Net ID der Quelle (Format: `x.x.x.x.x.x`). Standard: `{client-ip}.1.1`	*(automatisch)*
Source AMS Port	AMS-Port der Quelle (üblicherweise 30000-65535). Standard: der lokal zugewiesene TCP-Port	*(automatisch)*
Request Timeout	Standard-Timeout für alle Arten von Anfragen in Millisekunden	`4000`

Browse Queries	Abfragezeichenkette für das Symbol-Browsing. Mehrere Werte mit `;` trennen	`MAIN.*`

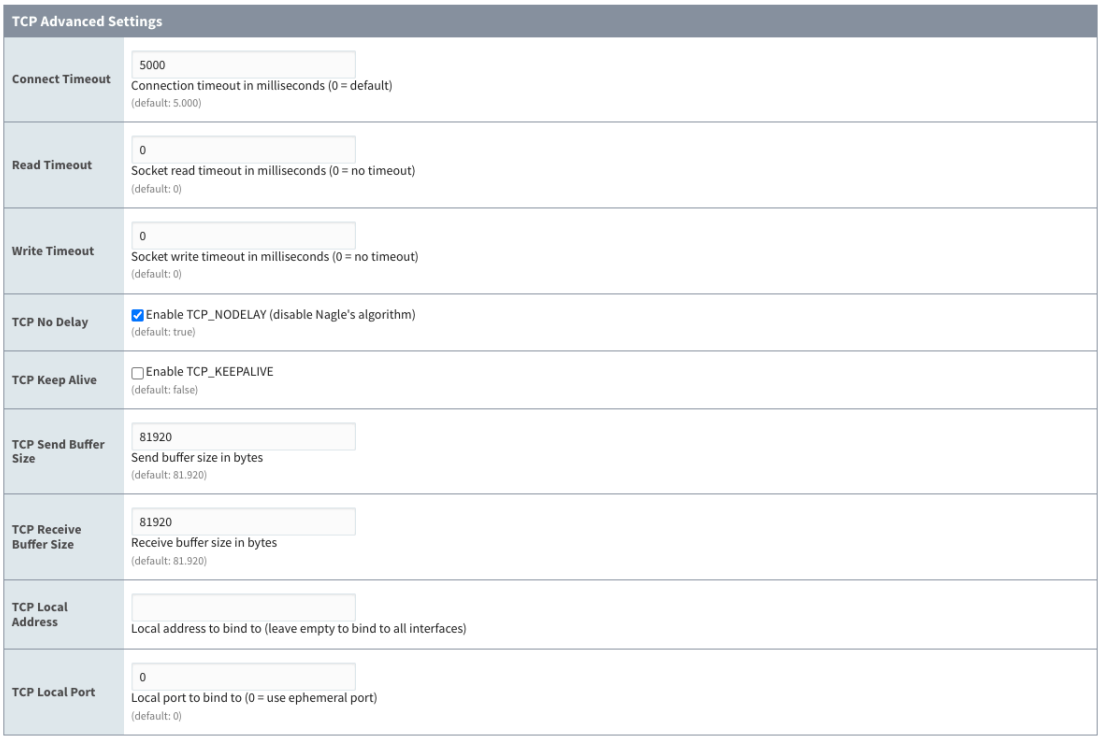
Wenn im Feld `Target AMS Net ID` kein Wert angegeben ist, wird er durch Anhängen von `.1.1` an die lokale IP-Adresse der TCP-Verbindung berechnet. Beachten Sie, dass es mehrere Pfade zur SPS geben kann (wenn Ihrem Gerät mehrere IP-Adressen zugewiesen sind). Um zu steuern, welche IP-Adresse verwendet wird, beachten Sie die Einstellung `TCP Local Address` im Abschnitt `TCP Advanced Settings`.

Gängige AMS-Ports:

Port	Beschreibung
851	TwinCAT 3 PLC Runtime 1 (Standard)
852	TwinCAT 3 PLC Runtime 2
853	TwinCAT 3 PLC Runtime 3
801	TwinCAT 2 PLC Runtime 1
811	TwinCAT 2 PLC Runtime 2

> ***Hinweis (Source AMS Net ID und SPS-Routen):*** *Bei reinen TCP-Verbindungen akzeptiert die Ziel-SPS ADS nur von AMS Net IDs, für die bereits eine Route existiert. Wird die Verbindung sofort abgewiesen (die SPS schließt die TCP-Verbindung), legen Sie auf der TwinCAT-Seite eine statische Route für die im Gateway-Log angezeigte Source AMS Net ID an. Die unten beschriebenen TLS-Modi legen diese Route automatisch an.*

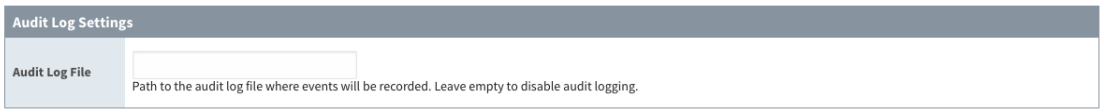
TCP Advanced Settings



Einstellung	Beschreibung	Standard
Connect Timeout	Verbindungs-Timeout in Millisekunden (0 = Standard)	`5000`
Read Timeout	Socket-Lese-Timeout in Millisekunden (0 = kein Timeout)	`0`
Write Timeout	Socket-Schreib-Timeout in Millisekunden (0 = kein Timeout)	`0`
TCP No Delay	TCP_NODELAY aktivieren (Nagle-Algorithmus deaktivieren)	`true`
TCP Keep Alive	TCP_KEEPALIVE aktivieren	`false`
TCP Send Buffer Size	Sendepuffergröße in Bytes	`81920`
TCP Receive Buffer Size	Empfangspuffergröße in Bytes	`81920`
TCP Local Address	Lokale Bind-Adresse (leer lassen, um an alle Schnittstellen zu binden)	*(leer)*
TCP Local Port	Lokaler Bind-Port (0 = ephemerer Port)	`0`

Audit Log Settings

Das `Audit Log` schreibt wichtige Informationen in eine eigene Protokolldatei. Diese Datei wächst sehr schnell; es wird daher empfohlen, diese Einstellung nur zur Fehleranalyse zu aktivieren.



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

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 legt komprimierte Dateien daneben an, sobald eine bestimmte Größe erreicht ist oder zeitgesteuert.

TLS Settings

Standardmäßig verwendet die ADS-Verbindung unverschlüsseltes TCP. Um die Kommunikation zu verschlüsseln („Secure ADS"), aktivieren Sie TLS und wählen einen der drei unterstützten Authentifizierungsmodi. Die beiden von allen verschlüsselten Modi gemeinsam genutzten Einstellungen sind:

Einstellung	Beschreibung	Standard
TLS Enabled	Die ADS-Verbindung mittels TLS verschlüsseln	`false`
TLS Authentication Mode	Authentifizierungsmethode: `Pre-Shared Key`, `Self Signed Certificate` oder `Shared Certificate Authority`	`Self Signed Certificate`

Wenn TLS aktiviert ist, wechselt der Verbindungsport automatisch von `48898` auf `8016`, sofern in den Transport Settings nicht explizit ein abweichender Port gesetzt wurde.

> ***Speichern von Passwörtern und Schlüsseln:*** *Die von den verschlüsselten Modi verwendeten Passwort- und Schlüsselfelder (`Keystore Password`, `Route Password` und `Pre-Shared Key`) werden in kodierter Form in der internen Gateway-Datenbank von Ignition gespeichert. Wird ein Feld leer gelassen, wird der dokumentierte Standardwert verwendet.*

Kein TLS (Standard)

Wenn **TLS Enabled** deaktiviert bleibt, verbindet sich der Treiber über unverschlüsseltes TCP (Standardport `48898`), und es wird keine Verschlüsselung angewendet. Alle übrigen Einstellungen der Kategorie TLS Settings werden ignoriert. Dies ist der Standardmodus und erfordert über die oben beschriebenen Transport- und ADS-Einstellungen hinaus keine weitere Konfiguration.

TLS Settings	
Enable TLS	☐ Enable TLS encryption for this ADS connection (default: false)
TLS Authentication Mode	SELF_SIGNED_CERTIFICATE Select the TLS authentication method (default: SELF_SIGNED_CERTIFICATE)
Keystore Path	Path to PKCS12 keystore file. Defaults to the module's auto-generated keystore if left empty.
Keystore Password	Password for the PKCS12 keystore. Defaults to the module's keystore password if left empty.
Route Name	Route name for Secure ADS route registration. Defaults to the gateway hostname if left empty.
Route Username	Administrator Username for Secure ADS route registration (default: Administrator)
Route Password	Password for Secure ADS route registration
Ignore Common Name	☐ Skip common name (CN) validation on the server certificate (default: false)
Identity	PSK identity name for TLS-PSK authentication
Pre-Shared Key	Pre-shared key as hexadecimal string (e.g. 0123456789abcdef)

Secure AMS - Pre-Shared Keys

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.

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. `MYPSKUSER`)
- Setzen Sie das **Password/Key**, aus dem der Pre-Shared Key abgeleitet wird

```
                <Server>
                        <Tls>
                                <Psk>
                                        <Identity>MYPSKUSER</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
```

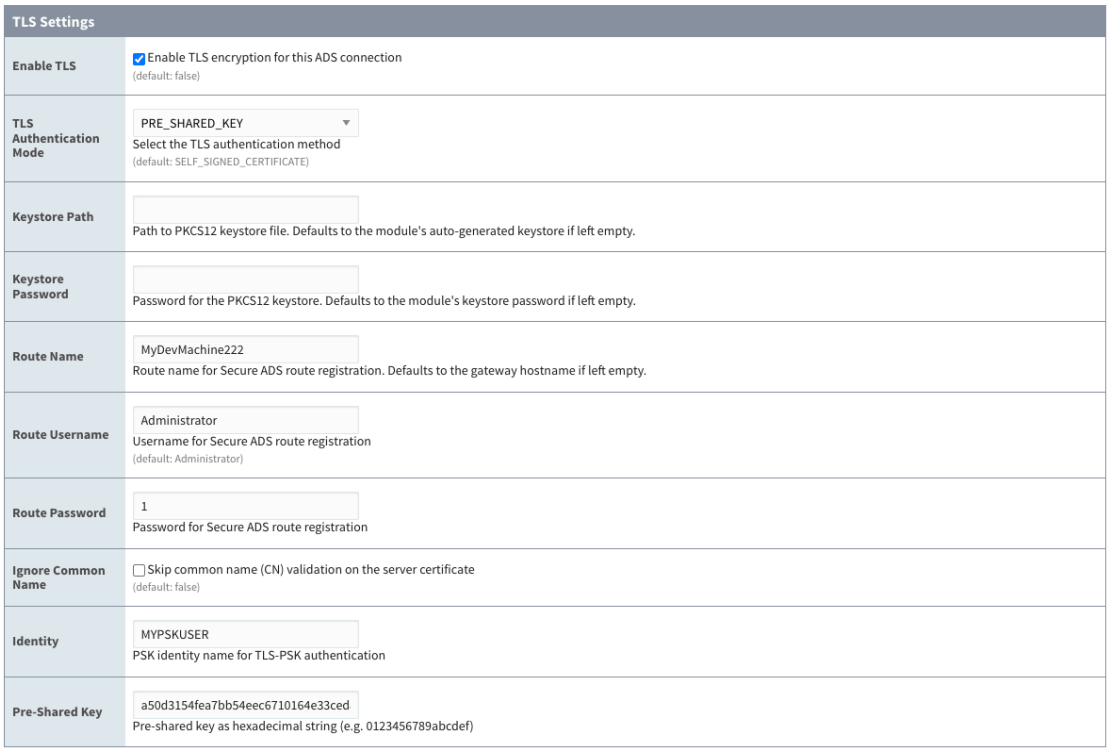
Beispiel mit Identity `MYPSKUSER` und Password `MySecret`:

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

Verwenden Sie die resultierende 64-stellige Hex-Zeichenkette als Wert für **Pre-Shared Key** in Ignition.

So aktivieren Sie diesen Modus:

1. Setzen Sie in der Kategorie **TLS Settings** den Wert **TLS Enabled** auf `true`
2. Setzen Sie **TLS Authentication Mode** auf `Pre-Shared Key`
3. Konfigurieren Sie die PSK-Felder:



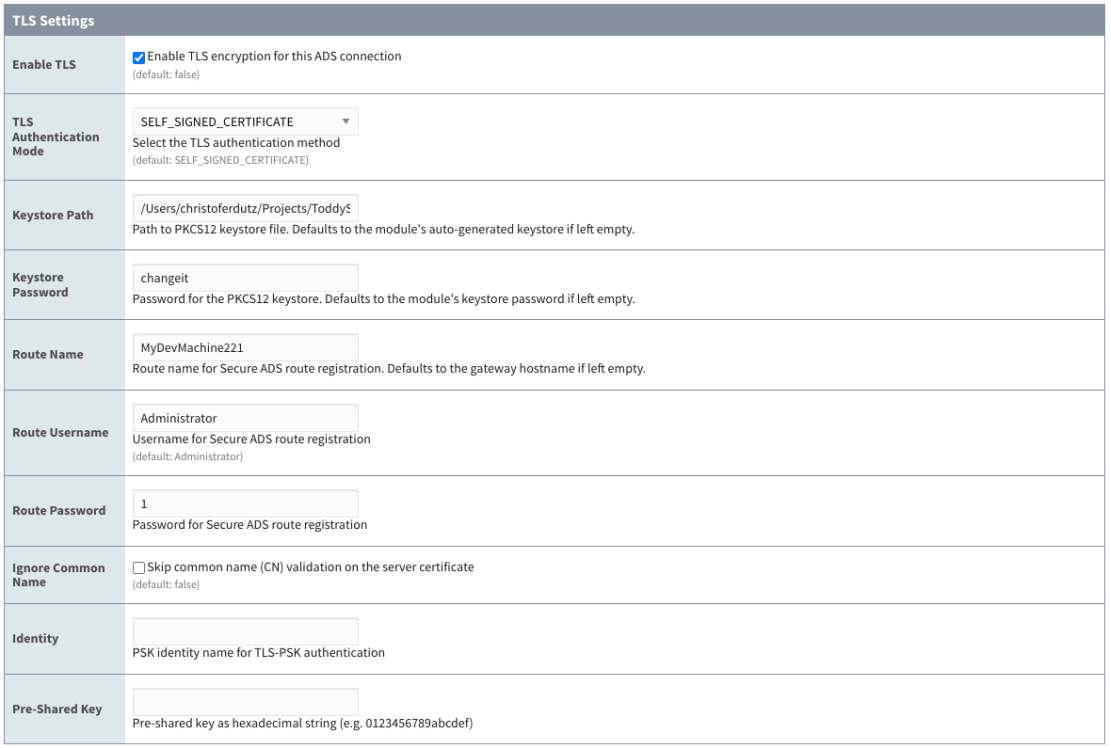
Einstellung	Beschreibung	Standard
Route Name	Name für die ADS-Route auf der SPS	*(Gateway-Hostname)*
Identity	PSK-Identity-Zeichenkette (muss mit der SPS-Konfiguration übereinstimmen)	*(leer)*
Pre-Shared Key	Hex-kodierter gemeinsamer geheimer Schlüssel	*(leer)*

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>192.168.24.220.1.1</NetId>
        <Type>TCP_IP</Type>
        <Tls>
                <Psk>
                        <Identity>MYPSKUSER</Identity>
                        <Key>a50d3154fea7bb54eec6710164e33ced872223f0a0ff05179e93e89e7f76c6f0</Key>
                </Psk>
        </Tls>
</Route>
```

Secure AMS - Self Signed Certificates

Verwendet TLS mit automatisch erzeugten selbstsignierten Zertifikaten. Das Modul verwaltet einen PKCS12-Keystore und richtet bei der ersten Verbindung eine ADS-Route auf der SPS ein.



So aktivieren Sie diesen Modus:

1. Setzen Sie in der Kategorie **TLS Settings** den Wert **TLS Enabled** auf `true`
2. Setzen Sie **TLS Authentication Mode** auf `Self Signed Certificate`
3. Konfigurieren Sie die TLS-spezifischen Felder:

Einstellung	Beschreibung	Standard
Keystore Path	Pfad zur PKCS12-Keystore-Datei (wird bei leerem Feld automatisch erzeugt)	*(automatisch)*
Keystore Password	Passwort für den Keystore	`toddysoft-connect`

Route Name	Name für die ADS-Route auf der SPS	*(Gateway-Hostname)*
Route Username	TwinCAT-Admin-Benutzername für die Routenerstellung	`Administrator`
Route Password	TwinCAT-Admin-Passwort für die Routenerstellung	`1`

Die Einstellungen `Identity`, `Pre-Shared Key` und `Ignore Common Name` werden bei diesem Verbindungstyp ignoriert.

Wenn kein Keystore-Pfad angegeben ist, 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.

Secure AMS - Shared Certificate Authority

Verwendet TLS mit Zertifikaten, die von einer gemeinsamen Zertifizierungsstelle (CA) signiert sind. Sowohl Ignition als auch die SPS müssen über Zertifikate verfügen, die von derselben CA ausgestellt wurden. Dies ist die sicherste Option für den Produktivbetrieb. Es werden dieselben TLS-Felder wie im Modus „Self Signed Certificate" verwendet (siehe oben).

So aktivieren Sie diesen Modus:

1. Setzen Sie in der Kategorie **TLS Settings** den Wert **TLS Enabled** auf `true`
2. Setzen Sie **TLS Authentication Mode** auf `Shared Certificate Authority`
3. Konfigurieren Sie die TLS-Felder:

Einstellung	Beschreibung	Standard
Keystore Path	Pfad zum PKCS12-Keystore mit dem CA-signierten Zertifikat	*(erforderlich)*
Keystore Password	Passwort für den Keystore	`toddysoft-connect`
Ignore Common Name	CN-Prüfung überspringen (nur für Tests verwenden)	`false`
Route Name	Name für die ADS-Route auf der SPS	*(Gateway-Hostname)*

Bei erfolgreicher Verbindung wird eine neue Routenkonfiguration zur Datei `/etc/TwinCAT/3.1/Target/StaticRoutes.xml` der SPS hinzugefügt.

Tag-Adressierung

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

```
MAIN.bStart                  # Boolescher Wert
MAIN.iCounter                # Ganzzahl
MAIN.fTemperature            # Gleitkommazahl
GVL.sStatus                  # Zeichenkette
MAIN.stMotor.fSpeed          # Struktur-Member
```

```
MAIN.aValues[0]                # Array-Element
MAIN.stArray[1].nField         # 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 bei reinem TCP, ob die SPS eine AMS-Route für die Source AMS Net ID hat (siehe Hinweis unter ADS Settings)
- 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 PSK: prüfen Sie, ob Identity und Schlüssel auf beiden Seiten übereinstimmen
- Bei Self-Signed: prüfen Sie, ob die Route-Zugangsdaten korrekt sind
- Bei Shared CA: 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.

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 muss in diesem Fall eine `Source AMS Net ID` gesetzt werden, 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.