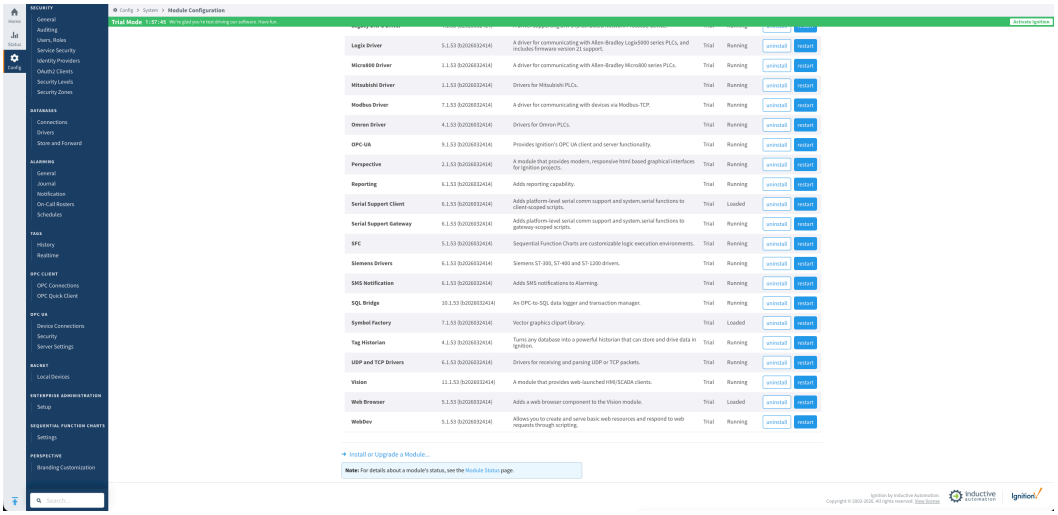
ToddySoft Connect ADS Driver - Ignition 8.1

Ignition 8.1 module for connecting to Beckhoff TwinCAT PLCs via the ADS/AMS protocol, with support for plain TCP and encrypted "Secure ADS" (TLS) connections.

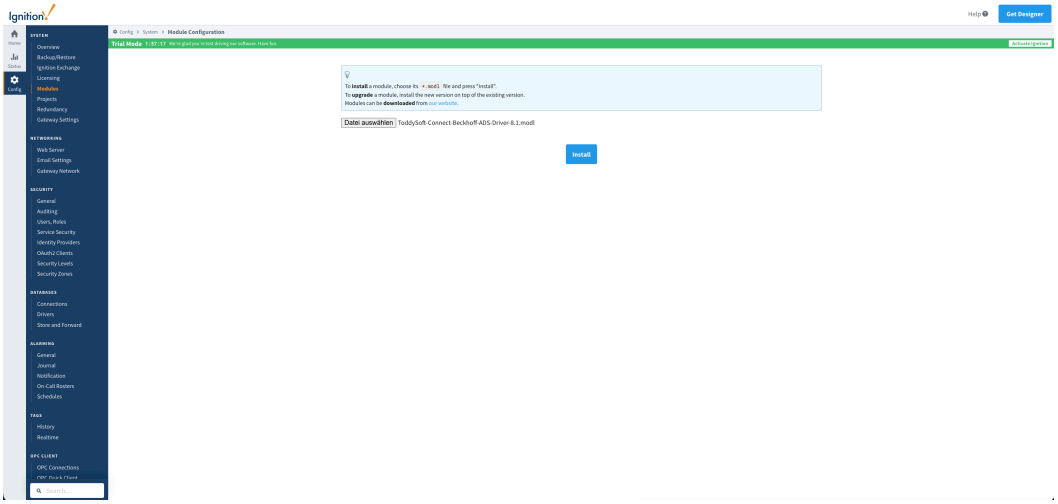
Installation

The ToddySoft Connect modules are signed with a self-signed certificate (issued to *ToddySoft GmbH*) rather than a publicly accredited code-signing certificate. Ignition therefore asks you to review and accept that certificate once during installation - it is then remembered for all future ToddySoft modules signed with the same certificate.

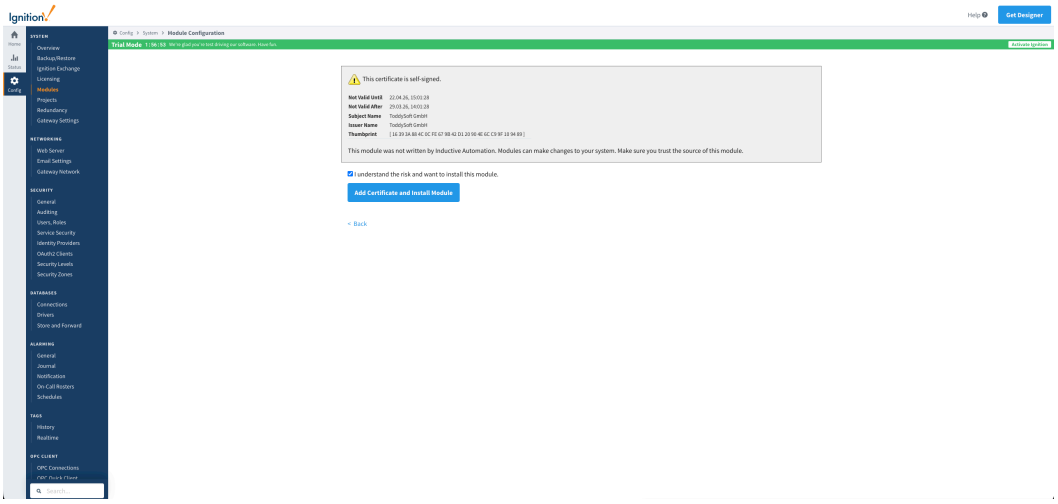
1. Open the Ignition Gateway web interface and navigate to **Config > System > Modules**. Scroll to the bottom and click **Install or Upgrade a Module...**.



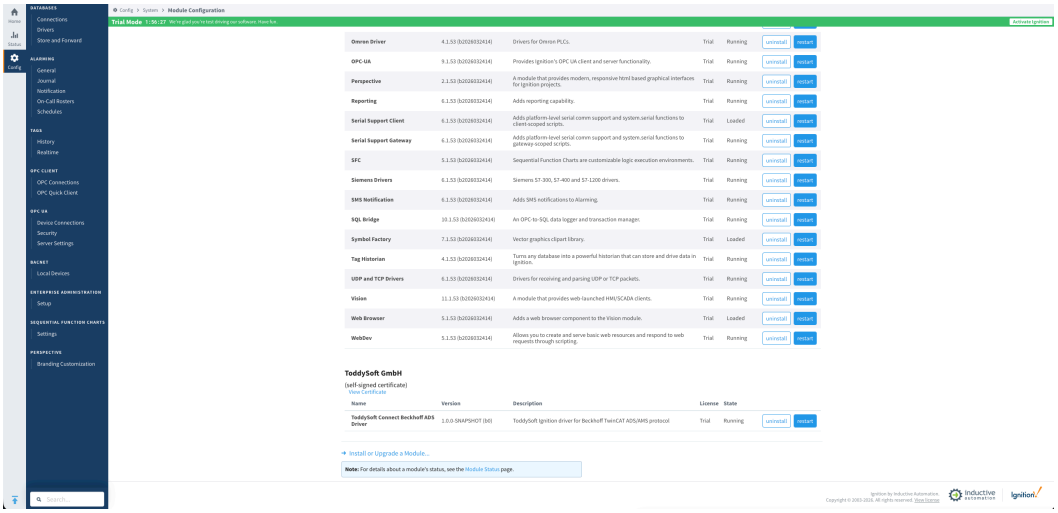
2. Choose the `ToddySoft-Connect-Beckhoff-ADS-Driver-8.1.modl` file and click **Install**.



3. Ignition shows the self-signed certificate details (subject and issuer *ToddySoft GmbH*) together with a warning that the module was not written by Inductive Automation. Review the certificate, tick **I understand the risk and want to install this module** and click **Add Certificate and Install Module**.

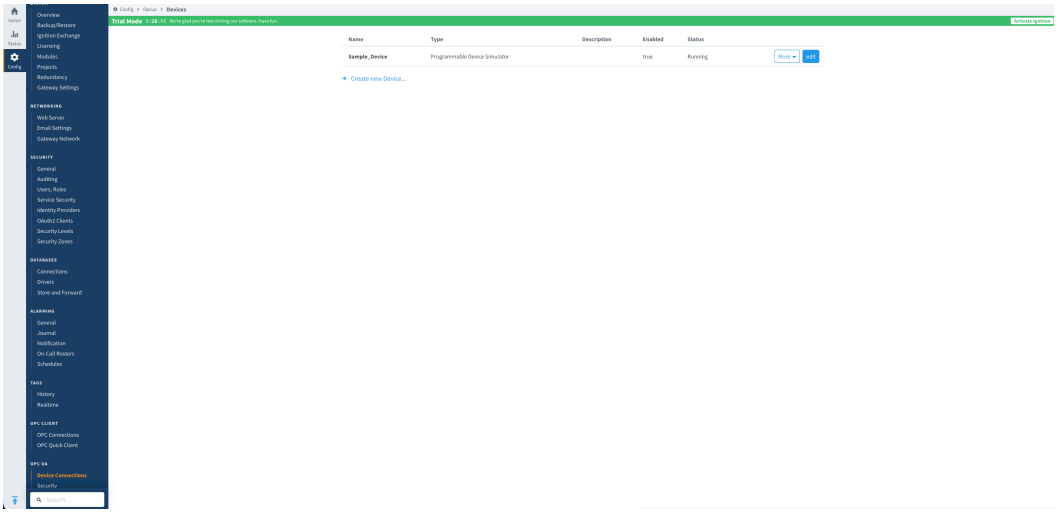


4. The module is now trusted and listed under the **ToddySoft GmbH (self-signed certificate)** group with the state **Running**.

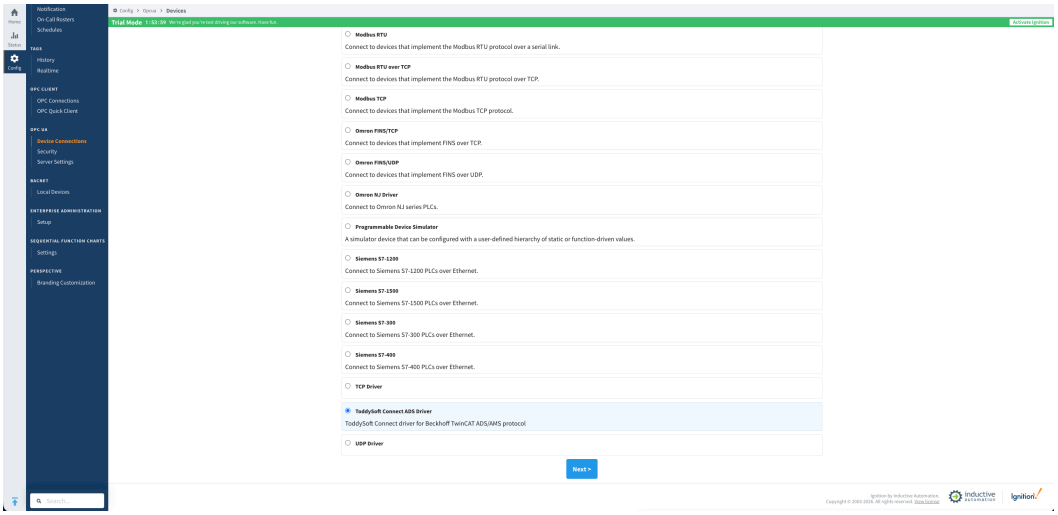


Creating a Device Connection

1. Go to **Config > OPC UA > Device Connections**.

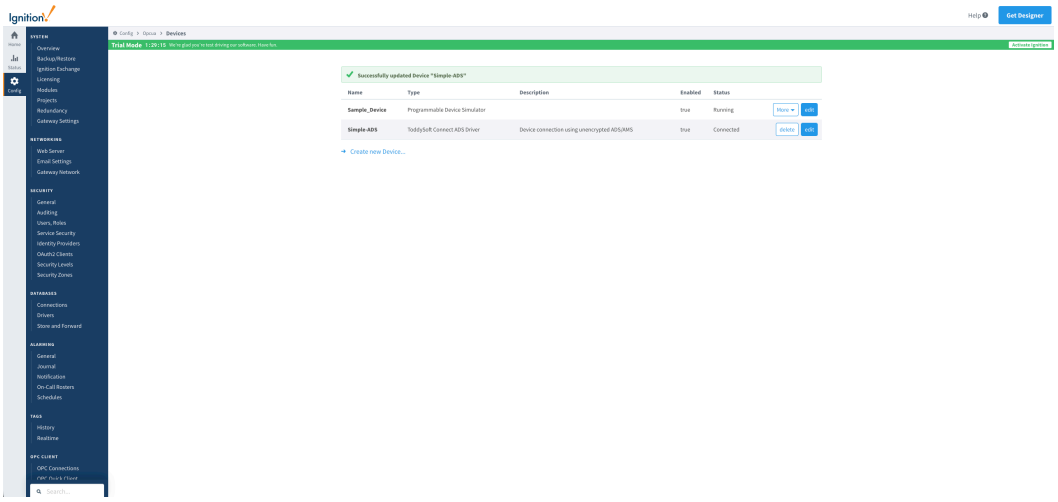


2. Click **Create new Device...**, select **ToddySoft Connect ADS Driver** as the device type and click **Next**.



3. Configure the connection settings (see the sections below) and click **Save**.

4. The new device then appears in the Device Connections list.

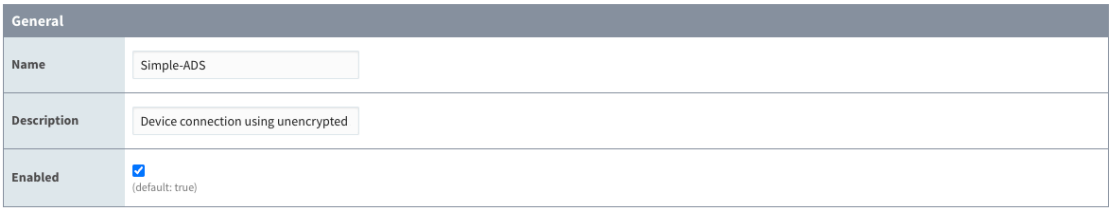


Setting blocks

The configuration is organized into categories: **General**, **Transport Settings**, **ADS Settings**, **TCP Advanced Settings**, **Audit Log Settings** and **TLS Settings**.

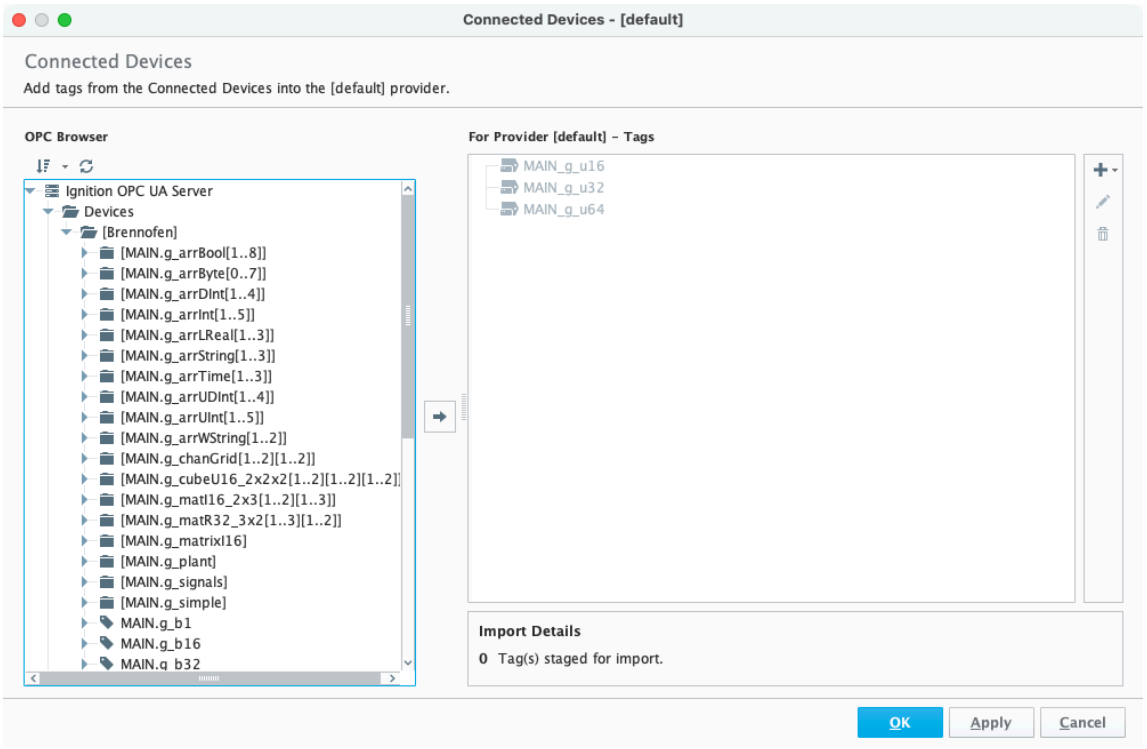
General

This block generally simply assigns a name to the connection.



Setting	Description	Default
Name	Unique name for this device connection	
Description	Optional description for this connection	
Enabled	Whether the connection is active	`true`

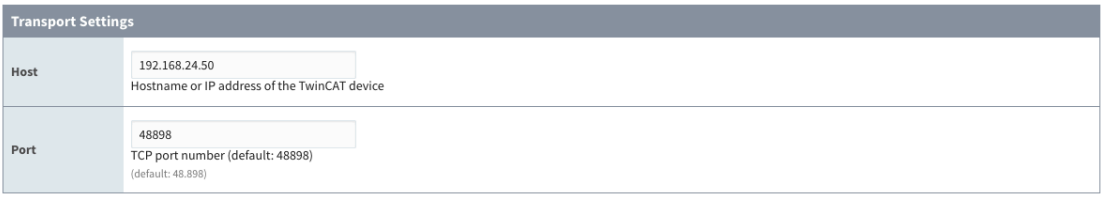
This is the name the connection is then referenced under in other parts of Ignition:



If `Enabled` is not checked, no connection is established until it is enabled.

Transport Settings

The endpoint of the TwinCAT device.



Setting	Description	Default
Host	Hostname or IP address of the TwinCAT device	`localhost`
Port	TCP port number (default: 48898, TLS: 8016)	48898

ADS Settings

This block configures the ADS-specific settings.

Setting	Description	Default
Target AMS Net ID	AMS Net ID of the target device (format: `x.x.x.x.x.x`). Defaults to `{target-ip}.1.1`	*(auto)*
Target AMS Port	AMS port of the target device	`851`
Source AMS Net ID	AMS Net ID of the source (format: `x.x.x.x.x.x`). Defaults to `{client-ip}.1.1`	*(auto)*
Source AMS Port	AMS port of the source (typically 30000-65535). Defaults to the locally assigned TCP port	*(auto)*
Request Timeout	Default timeout for all types of requests in milliseconds	`4000`
Browse Queries	Query string for symbol browsing. Multiple values separated with `;`	`MAIN.*`

If not provided in the `Target AMS Net ID` field, the value is calculated by appending `.1.1` after the local IP address of the TCP connection. Please beware that there could be multiple paths to reach the PLC (if your device is assigned multiple IP addresses). If you want to control the IP address used, please refer to the `TCP Local Address` setting in the `TCP Advanced Settings` section.

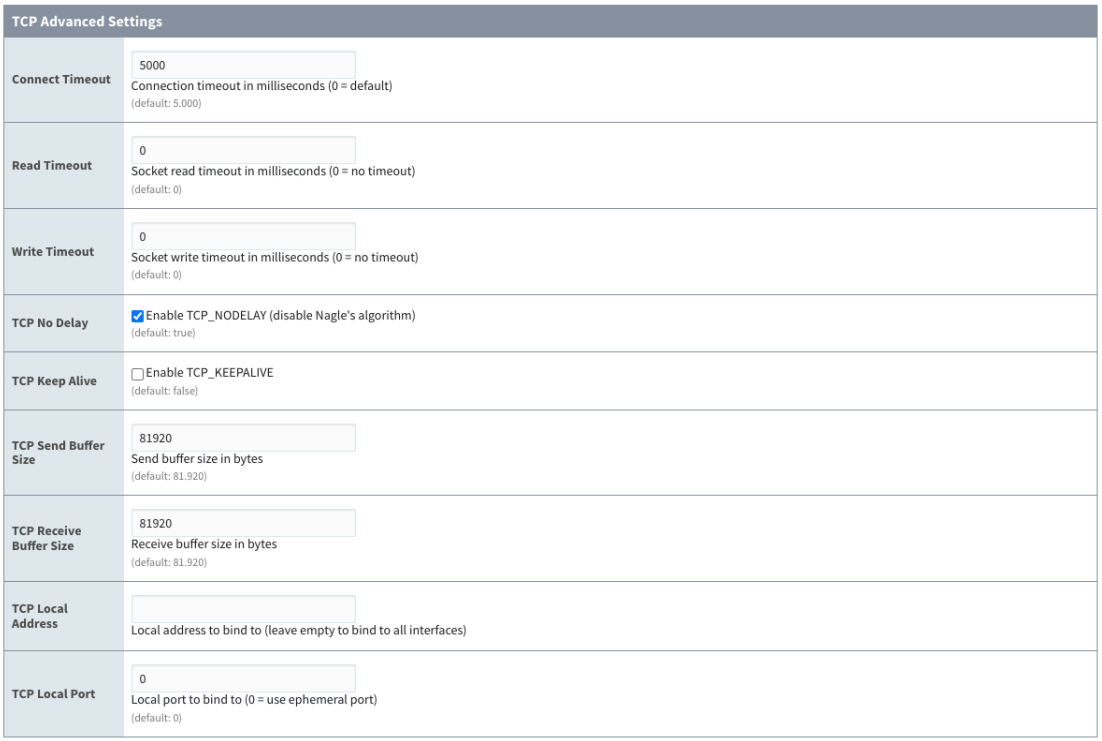
Common AMS ports:

Port	Description
851	TwinCAT 3 PLC Runtime 1 (default)
852	TwinCAT 3 PLC Runtime 2
853	TwinCAT 3 PLC Runtime 3
801	TwinCAT 2 PLC Runtime 1

811	TwinCAT 2 PLC Runtime 2

> ***Note (Source AMS Net ID and PLC routes):*** *For plain TCP connections, the target PLC only accepts ADS from AMS Net IDs it already has a route for. If the connection is refused immediately (the PLC closes the TCP connection), add a static route on the TwinCAT side for the source AMS Net ID shown in the gateway log. The TLS modes below create this route automatically.*

TCP Advanced Settings

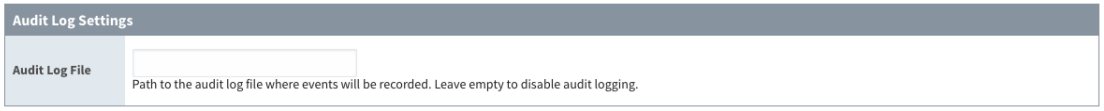


Setting	Description	Default
Connect Timeout	Connection timeout in milliseconds (0 = default)	`5000`
Read Timeout	Socket read timeout in milliseconds (0 = no timeout)	`0`
Write Timeout	Socket write timeout in milliseconds (0 = no timeout)	`0`
TCP No Delay	Enable TCP_NODELAY (disable Nagle's algorithm)	`true`
TCP Keep Alive	Enable TCP_KEEPALIVE	`false`
TCP Send Buffer Size	Send buffer size in bytes	`81920`
TCP Receive Buffer Size	Receive buffer size in bytes	`81920`
TCP Local Address	Local address to bind to (leave empty to bind to all interfaces)	*(empty)*

TCP Local Port	Local port to bind to (0 = use ephemeral port)	`0`

Audit Log Settings

The `Audit Log` logs important information to a dedicated log file. This will grow in size very quickly, so it is advised to only use this setting when investigating issues.



Setting	Description	Default
Audit Log File	Absolute path to the audit log file where events will be recorded. Leave empty to disable.	*(empty)*

NOTE: Please ensure the user the `Ignition` process is running under has write access to this path.

The Audit Log system will automatically create the file and create compressed files next to it, if a certain size is reached or on a time-based schedule.

TLS Settings

By default the ADS connection uses plain, unencrypted TCP. To encrypt the communication ("Secure ADS"), enable TLS and select one of the three supported authentication modes. The two settings shared by all encrypted modes are:

Setting	Description	Default
TLS Enabled	Encrypt the ADS connection using TLS	`false`
TLS Authentication Mode	Authentication method: `Pre-Shared Key`, `Self Signed Certificate` or `Shared Certificate Authority`	`Self Signed Certificate`

When TLS is enabled, the connection port automatically switches from `48898` to `8016`, unless a non-default port has been set explicitly in the Transport Settings.

> ***Storing passwords and keys:*** *The password and key fields used by the encrypted modes below (`Keystore Password`, `Route Password` and `Pre-Shared Key`) are stored in encoded form in Ignition's internal gateway database. When a field is left empty, the documented fallback default is used.*

No TLS (default)

With **TLS Enabled** left unchecked, the driver connects over plain TCP (default port `48898`) and no encryption is applied. All other settings in the TLS Settings category are ignored. This is the default mode and requires no configuration beyond the Transport and ADS settings described above.

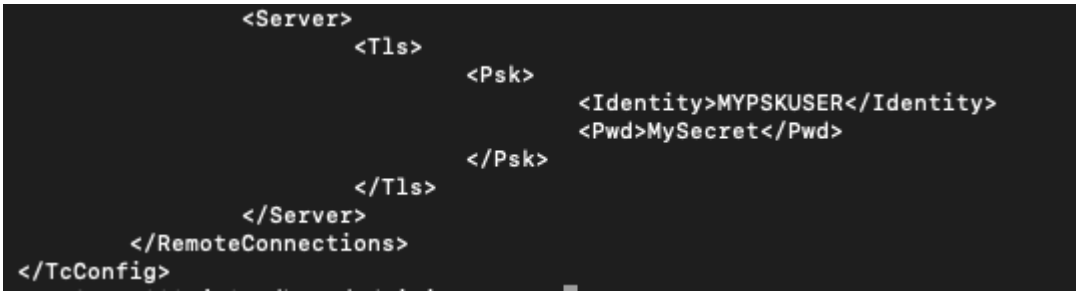
TLS Settings	
Enable TLS	☐ Enable TLS encryption for this ADS connection (default: false)
TLS Authentication Mode	SELF_SIGNED_CERTIFICATE Select the TLS authentication method (default: SELF_SIGNED_CERTIFICATE)
Keystore Path	Path to PKCS12 keystore file. Defaults to the module's auto-generated keystore 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

Uses TLS-PSK, where both sides share a secret key and identity string. No certificates are needed - this is the simplest way to encrypt ADS communication.

The PLC must be configured with matching PSK settings. In the TwinCAT Secure ADS configuration (usually in `/etc/TwinCAT/3.1/Target/StaticRoutes.xml`):

- Set the **Identity** to match the value in Ignition (e.g., `MYPSKUSER`)
- Set the **Password/Key** that will be used to derive the pre-shared key



TwinCAT derives the PSK key by computing `SHA–256(Identity + Password)`. Note that the Identity must be **all uppercase**. To calculate the hex key needed for the Ignition configuration:

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

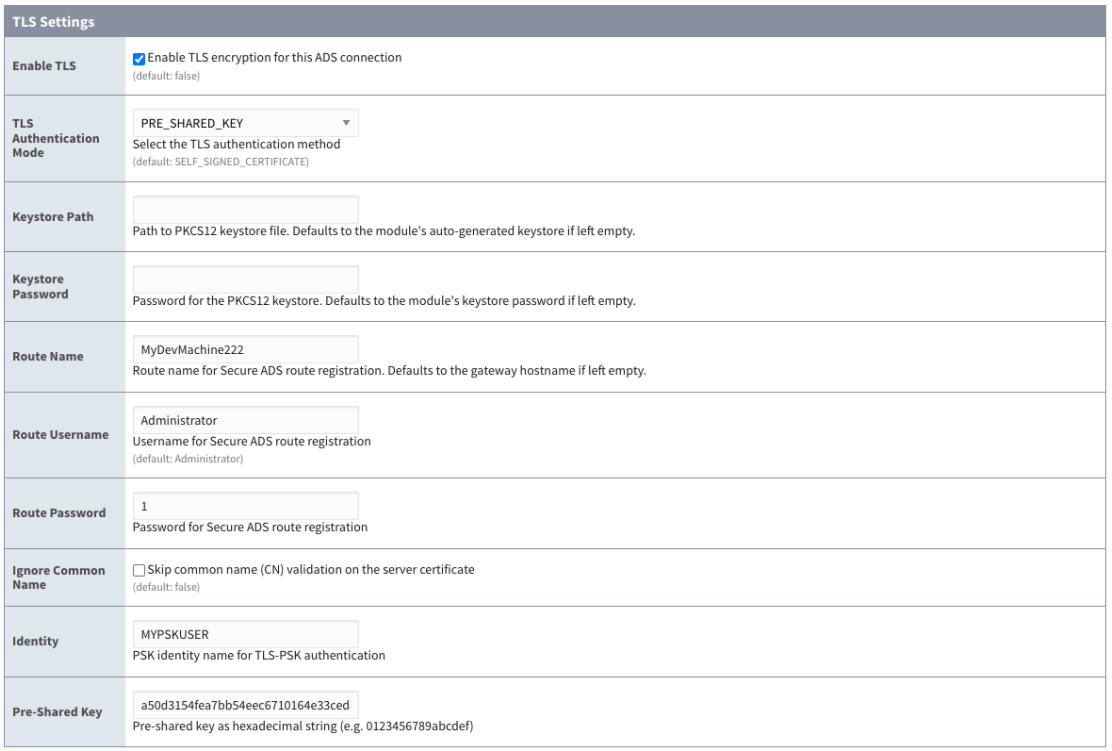
For example, with Identity `MYPSKUSER` and Password `MySecret`:

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

Use the resulting 64-character hex string as the **Pre-Shared Key** value in Ignition.

To enable:

1. In the **TLS Settings** category, set **TLS Enabled** to `true`
2. Set **TLS Authentication Mode** to `Pre-Shared Key`
3. Configure the PSK fields:



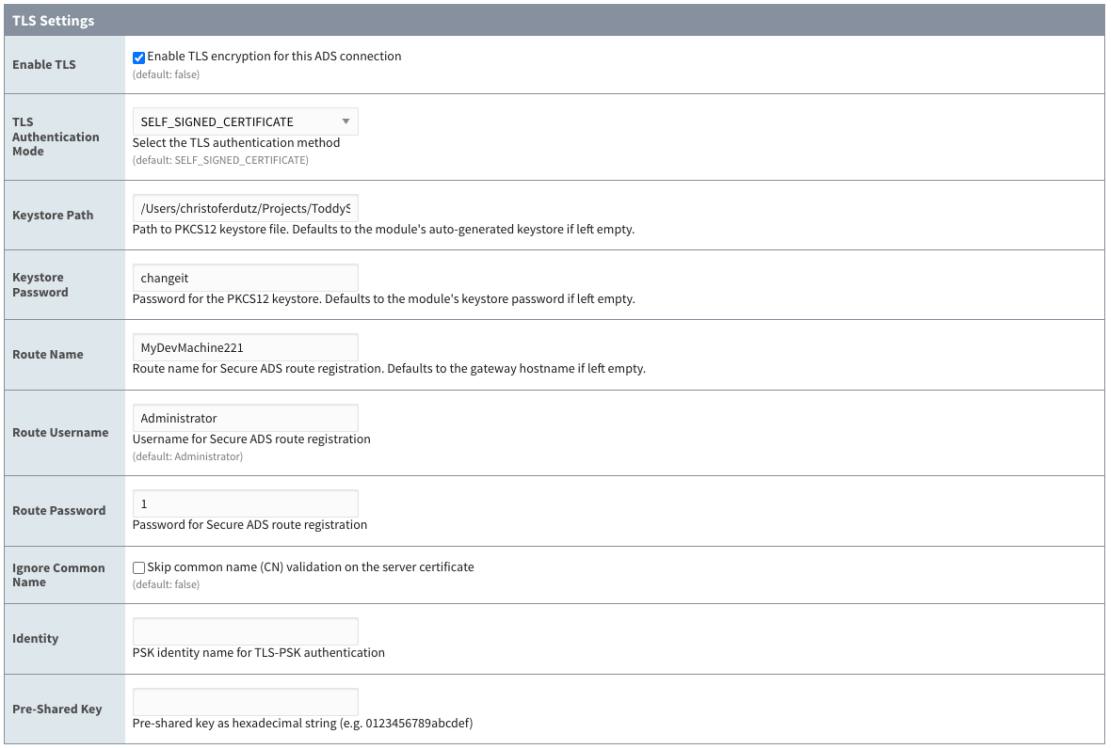
Setting	Description	Default
Route Name	Name for the ADS route on the PLC	*(gateway hostname)*
Identity	PSK identity string (must match the PLC configuration)	*(empty)*
Pre-Shared Key	Hex-encoded shared secret key	*(empty)*

If the connection was successful, a new route configuration will be added to `/etc/TwinCAT/3.1/Target/StaticRoutes.xml` :

```
<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

Uses TLS with automatically generated self-signed certificates. The module manages a PKCS12 keystore and establishes an ADS route on the PLC during the initial connection.



To enable:

1. In the **TLS Settings** category, set **TLS Enabled** to `true`
2. Set **TLS Authentication Mode** to `Self Signed Certificate`
3. Configure the TLS-specific fields:

Setting	Description	Default
Keystore Path	Path to the PKCS12 keystore file (auto-generated if empty)	*(auto)*
Keystore Password	Password for the keystore	`toddysoft-connect`

Route Name	Name for the ADS route on the PLC	*(gateway hostname)*
Route Username	TwinCAT admin username for route creation	`Administrator`
Route Password	TwinCAT admin password for route creation	`1`

The settings `Identity`, `Pre-Shared Key` and `Ignore Common Name` are ignored for this type of connection.

When a keystore path is not specified, the module automatically generates a keystore in the Ignition module settings directory.

On a successful connection, a new route configuration is added to the PLC's `/etc/TwinCAT/3.1/Target/StaticRoutes.xml`.

Secure AMS - Shared Certificate Authority

Uses TLS with certificates signed by a shared Certificate Authority (CA). Both Ignition and the PLC must have certificates issued by the same CA. This is the most secure option for production environments. It uses the same TLS fields as the Self-Signed Certificate mode (shown above).

To enable:

1. In the **TLS Settings** category, set **TLS Enabled** to `true`
2. Set **TLS Authentication Mode** to `Shared Certificate Authority`
3. Configure the TLS fields:

Setting	Description	Default
Keystore Path	Path to the PKCS12 keystore containing the CA-signed certificate	*(required)*
Keystore Password	Password for the keystore	`toddysoft-connect`
Ignore Common Name	Skip CN validation (use for testing only)	`false`
Route Name	Name for the ADS route on the PLC	*(gateway hostname)*

On a successful connection, a new route configuration is added to the PLC's `/etc/TwinCAT/3.1/Target/StaticRoutes.xml`.

Tag Addressing

Tags are addressed using symbolic names from the PLC program:

```
MAIN.bStart                    # Boolean
MAIN.iCounter                  # Integer
MAIN.fTemperature              # Float
GVL.sStatus                    # String
MAIN.stMotor.fSpeed            # Struct member
```

```
MAIN.aValues[0]                # Array element
MAIN.stArray[1].nField         # Struct array element field
```

Configure **Browse Queries** (e.g., `MAIN.*`) to control which symbols appear when browsing tags in the Ignition Designer.

Tag Groups

By default, all tags are collected in the default tag group, which means all selected tags are fetched at the default interval of once a second.

If different intervals are desired, create additional tag groups, configure the desired intervals there, and assign tags to the corresponding tag groups.

Troubleshooting

Device shows "Faulted":

- Verify the PLC hostname/IP is reachable
- Check that AMS Net IDs match the TwinCAT configuration
- Ensure port 48898 (or 8016 for TLS) is not blocked by a firewall
- For plain TCP, verify the PLC has an AMS route for the source AMS Net ID (see the note in ADS Settings)
- Review Gateway logs: **Status > Diagnostics > Logs**

Tags show bad quality:

- Verify the variable exists in the PLC program
- Check spelling and case sensitivity
- Ensure the PLC program is running

TLS connection fails:

- For PSK: verify the identity and key match on both sides
- For Self-Signed: check that route credentials are correct
- For Shared CA: ensure both certificates are signed by the same CA

Docker related issues

When running `Ignition` inside `Docker`, the host receives an IP address on the Docker-internal network. When connecting to the PLC, the connection originates from one of the host's IP addresses. In this case the connection needs a `Source AMS Net ID` that refers to the host's IP address.

Usually setting the `Source AMS Port` is also required. However, in this case the value does not really matter. Simply setting it to `54321` usually works.

VPN related issues

When connecting to a remote PLC over a VPN, depending on the type of VPN the host usually gets assigned a local VPN IP address. Similar to when using `Docker`, in this case a `Source AMS Net ID` needs to be set that references this assigned IP address.

Usually setting the `Source AMS Port` is also required. However, in this case the value does not really matter. Simply setting it to `54321` usually works.