

**TURCK**

Your Global Automation Partner

TAS

# Turck Automation Suite IIoT and Service Platform

Readme and notes

## 1 System requirements

- Compatible web browser (Google Chrome, Microsoft Edge, Mozilla Firefox)
- Access to all relevant networks
- Internet access:
  - IODD configurator: retrieval of IODDs from io-link.com
  - Retrieval of updates

## 2 Supported devices

- Turck devices with an Ethernet connection including connected devices.

**NOTE**

Functionality can be restricted depending on the device version.

---

- Turck USB IO-Link master, USB-2-IOL-0002, ID: 6825482

## 3 Other notes

### 3.1 TAS application

- TAS runs in the standard web browser of the PC.
- Launching TAS also starts the tool in the system tray where it stays active even if the web browser is closed.
- Double-clicking the icon in the system tray restarts the application in the standard web browser.
- TAS can be fully closed via the icon in the system tray.
- The log file can also be accessed.

**NOTE**

If the cache of the web browser is cleared, stored data from TAS will also be irrevocably deleted.

---

### 3.2 Device password

The execution of actions (except for the wink command) requires the entry of the relevant device password with the following exceptions:

- Devices with the default IP address can also be configured without entering the device password.
- After the device is restarted by switching the power supply off and back on again, it can then be reset to the default settings for 180 s without entering the device password.

### 3.3 IP host and port assignment

By default TAS launches on **port 8088** via **localhost**. If port 8088 is already assigned, the user can either automatically select the next available port or wait for the port to become available. Alternatively, the port can be set manually when the program launches:

- ▶ Launch TAS using the command line parameter **TAS.exe --serverUrl http://localhost:8088/**. The port number is freely selectable.
- ▶ or
- ▶ In the properties of the desktop shortcut for TAS, extend the target of the shortcut using the parameter **--serverUrl http://localhost:8088/**. The port number is freely selectable.

If the localhost cannot be reached, the IP host can be changed via the command line parameter **--serverUrl**.

- ▶ Make TAS accessible via all IP host interfaces via port 8090: Start TAS using the command line parameter **TAS.exe --serverUrl http://\*:8090/**.
  - ▶ Make TAS accessible via a defined IP host interface (here: 192.168.1.1) via Port 8090: Start TAS using the command line parameter **TAS.exe --serverUrl http://192.168.1.1:8090/**.
- ⇒ The IP host interface and port are displayed in the address bar of the browser after TAS is started.



### 3.4 Selecting the network adapter

By default, TAS automatically scans all active network adapters.

The command line parameter **--adapterIps** can be used to restrict the selection of network adapters (for example "--adapterIps 192.168.1.7, 192.168.10.235").

### 3.5 Setting firewall rules

When the application is started for the first time, the firewall rules are set automatically if the user has administrator rights.

For other user profiles, the firewall rules must be set manually by an administrator.

- ▶ Enable TAS.exe via an incoming rule using the following parameters.
  - Port: 58553
  - UDP
  - Path to TAS.exe
- ▶ Do not change the path to TAS.exe after the firewall has been enabled.
- ▶ Do not rename TAS.exe after the firewall has been enabled.

### 3.6 Specifying the storage location for the log file

The location of the log file can be changed via the command line parameter **--logFile**.

- ▶ In the command prompt, enter the parameter **--logFile** with the desired save location and file name.
- ⇒ A log file is created in the specified directory.

## 4 FAQ

Question	Possible cause	Possible solution
Why do I get an error message in the browser?	The web browser used only allows communication via HTTPS. TAS, on the other hand, communicates via HTTP by default.	Use a different web browser. Set up communication via HTTPS. Disable automatic browser redirect from HTTP to HTTPS.
Why are the values set in TAS not adopted by the device? Why are values visualized incorrectly?	Accessing the device from various control systems, software tools or web pages concurrently can cause malfunctions.	Access the device using only one system. Disable access from all other systems. If the problem persists, contact Turck.

### 4.1 Setting up communication via HTTPS

TAS can use HTTPS instead of HTTP for communication between client and backend.

Proceed as follows for the setup:

- ▶ Install SSL certificate under **Trusted Root Certification Authorities**.
- ▶ Configure the computer for using this certificate.
- ▶ Launch TAS using the command line parameter **--serverUrl** to switch to HTTPS (for example "--serverUrl https://localhost:8443/").

### 4.2 Disabling automatic browser redirect from HTTP to HTTPS

The automatic redirect of HTTP requests to HTTPS via the browser prevents communication between TAS client and backend.

- ▶ To force forwarding, add an exception for **LOCALHOST** (Chrome, Edge) or disable forwarding to https in **FALLBACK** (Firefox).
- ⇒ The communication functions again via the selected browser.

### 4.3 Displaying and editing network settings in PROFINET view

The network settings for DCP-capable PROFINET devices can be displayed and edited via PROFINET view. Npcap or WinPcap must be installed to use the DCP function in PROFINET view.

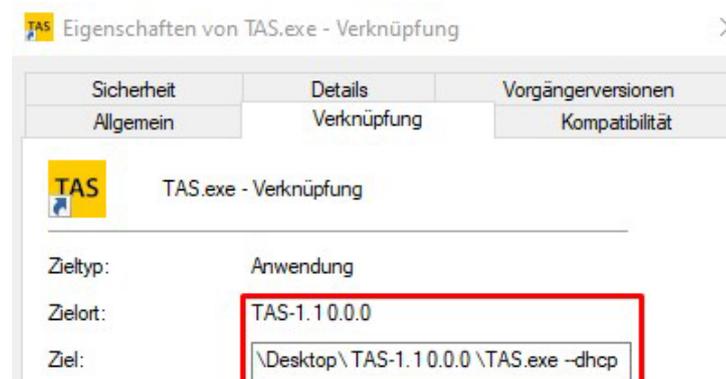
### 4.4 Enabling the DHCP server function

The DHCP server function can be enabled via the command prompt or an adapted link.

- ▶ Launch TAS in the command prompt using the command **TAS.exe --dhcp**.

or

- ▶ In the properties of the desktop shortcut for TAS, extend the target of the shortcut using the parameter **--dhcp**.



# TURCK

Your Global Automation Partner

Over 30 subsidiaries and  
60 representations worldwide!

100046012 | 2025/03



[www.turck.com](http://www.turck.com)