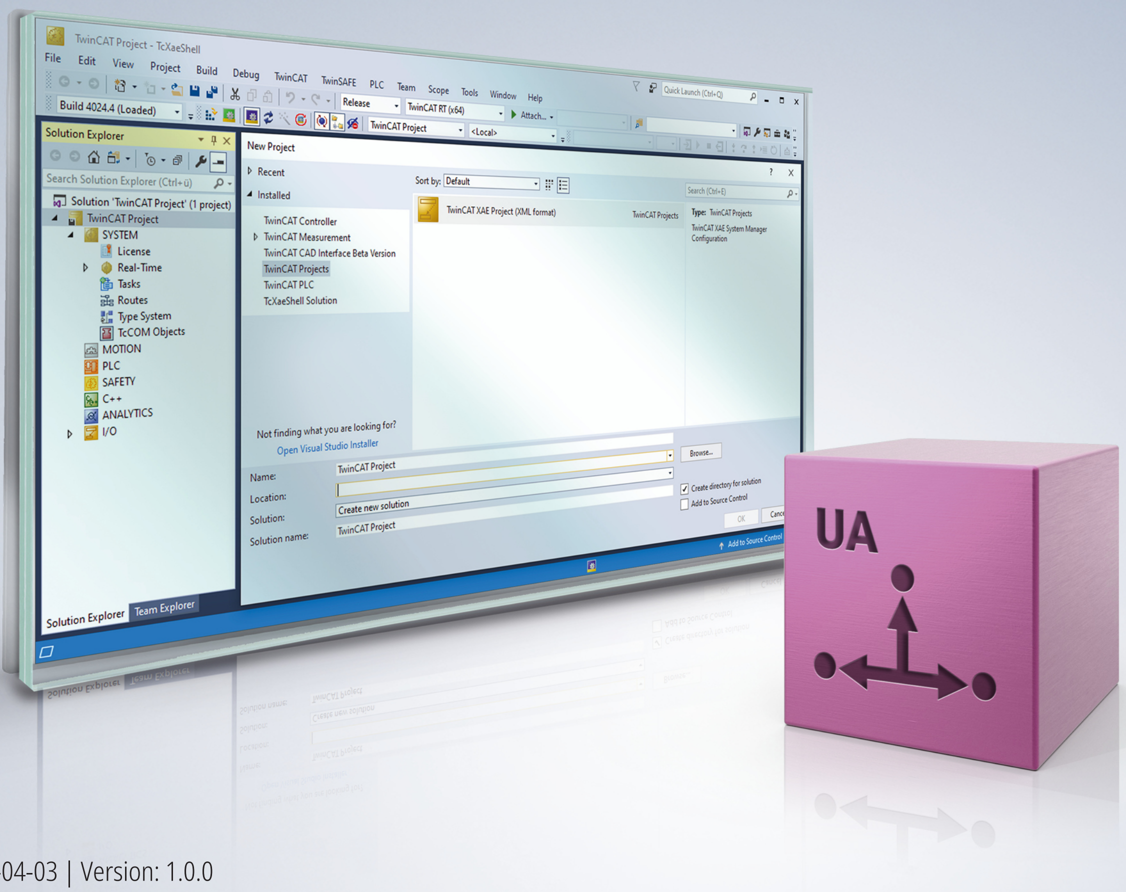
BECKHOFF New Automation Technology

Manual | EN

TF6100

TwinCAT 3 | OPC UA Gateway



2024-04-03 | Version: 1.0.0

Table of contents

1 Foreword

1.1 Notes on the documentation

This description is intended exclusively for trained specialists in control and automation technology who are familiar with the applicable national standards.
For installation and commissioning of the components, it is absolutely necessary to observe the documentation and the following notes and explanations.
The qualified personnel is obliged to always use the currently valid documentation.

The responsible staff must ensure that the application or use of the products described satisfies all requirements for safety, including all the relevant laws, regulations, guidelines, and standards.

Disclaimer

The documentation has been prepared with care. The products described are, however, constantly under development.
We reserve the right to revise and change the documentation at any time and without notice.
No claims to modify products that have already been supplied may be made on the basis of the data, diagrams, and descriptions in this documentation.

Trademarks

Beckhoff®, TwinCAT®, TwinCAT/BSD®, TC/BSD®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® and XPlanar® are registered and licensed trademarks of Beckhoff Automation GmbH.
If third parties make use of designations or trademarks used in this publication for their own purposes, this could infringe upon the rights of the owners of the said designations.

Patents

The EtherCAT Technology is covered, including but not limited to the following patent applications and patents:
EP1590927, EP1789857, EP1456722, EP2137893, DE102015105702
and similar applications and registrations in several other countries.

EtherCAT

EtherCAT® is registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany

Copyright

1.2 For your safety

Safety regulations

Read the following explanations for your safety.
Always observe and follow product-specific safety instructions, which you may find at the appropriate places in this document.

Exclusion of liability

All the components are supplied in particular hardware and software configurations which are appropriate for the application. Modifications to hardware or software configurations other than those described in the documentation are not permitted, and nullify the liability of Beckhoff Automation GmbH & Co. KG.

Personnel qualification

This description is only intended for trained specialists in control, automation, and drive technology who are familiar with the applicable national standards.

Signal words

The signal words used in the documentation are classified below. In order to prevent injury and damage to persons and property, read and follow the safety and warning notices.

Personal injury warnings

⚠ DANGER
Hazard with high risk of death or serious injury.

⚠ WARNING
Hazard with medium risk of death or serious injury.

⚠ CAUTION
There is a low-risk hazard that could result in medium or minor injury.

Warning of damage to property or environment

NOTICE
The environment, equipment, or data may be damaged.

Information on handling the product

This information includes, for example:
recommendations for action, assistance or further information on the product.

1.3 Notes on information security

The products of Beckhoff Automation GmbH & Co. KG (Beckhoff), insofar as they can be accessed online, are equipped with security functions that support the secure operation of plants, systems, machines and networks. Despite the security functions, the creation, implementation and constant updating of a holistic security concept for the operation are necessary to protect the respective plant, system, machine and networks against cyber threats. The products sold by Beckhoff are only part of the overall security concept. The customer is responsible for preventing unauthorized access by third parties to its equipment, systems, machines and networks. The latter should be connected to the corporate network or the Internet only if appropriate protective measures have been set up.

In addition, the recommendations from Beckhoff regarding appropriate protective measures should be observed. Further information regarding information security and industrial security can be found in our https://www.beckhoff.com/secguide.

Beckhoff products and solutions undergo continuous further development. This also applies to security functions. In light of this continuous further development, Beckhoff expressly recommends that the products are kept up to date at all times and that updates are installed for the products once they have been made available. Using outdated or unsupported product versions can increase the risk of cyber threats.

To stay informed about information security for Beckhoff products, subscribe to the RSS feed at https://www.beckhoff.com/secinfo.

2 Overview

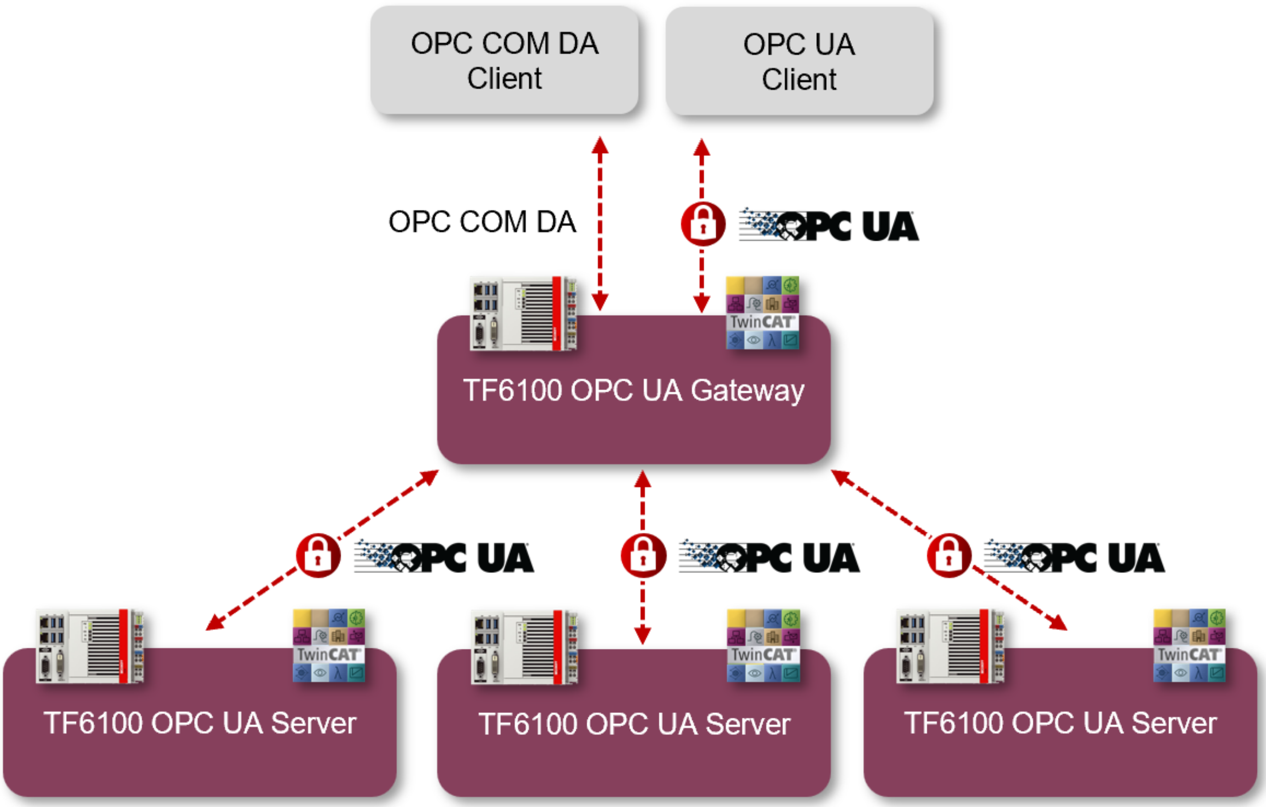
OPC **U**nified **A**rchitecture (OPC UA) is the next generation of the familiar OPC standard. This is a globally standardized communication protocol via which machine data can be exchanged irrespective of the manufacturer and platform. OPC UA already integrates common security standards directly in the protocol. Another major advantage of OPC UA over the conventional OPC standard is its independence from the COM/DCOM system.

Detailed information on OPC UA can be found on the web pages of the OPC Foundation.

The TwinCAT 3 Function TF6100 OPC UA consists of several software components that enable data exchange with TwinCAT based on OPC UA.
The following table provides an overview of the individual product components.

Software component	Description
TwinCAT OPC UA Server	Provides an OPC UA Server interface so that UA clients can access the TwinCAT runtime.
TwinCAT OPC UA Client	Provides OPC UA Client functionality to enable communication with other OPC UA Servers based on PLCopen-standardized function blocks and an easy-to-configure I/O device.
TwinCAT OPC UA Configurator	Graphical user interface for configuring the TwinCAT OPC UA Server.
TwinCAT OPC UA Sample Client	Graphical sample implementation of an OPC UA Client in order to carry out a first connection test with the TwinCAT OPC UA Server.
TwinCAT OPC UA Gateway	Wrapper technology that provides both an OPC COM DA Server interface and OPC UA Server aggregation capabilities.

This documentation describes the TwinCAT OPC UA Gateway, which is a software component that provides an OPC COM DA interface and enables OPC UA server aggregation.



For a quick introduction to the product, we recommend our chapters Installation [▶ 10] and Quick start [▶ 15]. Please also note the System requirements [▶ 10] for this product.

3 Installation

3.1 System requirements

The following system requirements apply for the installation and operation of this product.

Technical data	Description
Operating system	Windows 7, 10 Windows Server
Target platforms	PC architecture (x86, x64, ARM)
.NET Framework	---
TwinCAT version	A TwinCAT installation is not necessary for the operation of this software.
Required TwinCAT license	A TwinCAT license is not necessary for the operation of this software.
Supported servers	The TwinCAT OPC UA Gateway communicates exclusively with TwinCAT OPC UA Servers for which a TF6100 license is required. If you want to connect third-party devices to the gateway, you will need the "UA Gateway" software from Unified Automation.
COM/DCOM	Local OPC COM DA communication is supported by this software. Communication based on DCOM is not supported.

Installation variants

Please also note the different supported installation variants [▶ 12] of the TwinCAT OPC UA Gateway.

Firewall port

To enable communication via OPC UA with the TwinCAT OPC UA Gateway, the following network port must be opened in the firewall of the device:

```
48050/tcp (incoming)
```

If, for example, the TwinCAT OPC UA Gateway is installed on a Beckhoff Industrial PC, this port must be opened as incoming communication in the operating system's firewall.

3.2 Installation

Depending on the TwinCAT version and operating system used, this TwinCAT 3 Function can be installed in different ways, which are described in more detail below.

NOTICE

Update installation

An update installation always uninstalls the previous installation. Please make sure that you have backed up your configuration files beforehand.

TwinCAT Package Manager

If you are using TwinCAT 3.1 Build 4026 (and higher) on the Microsoft Windows operating system, you can install this function via the TwinCAT Package Manager, see Installation documentation.

Normally you install the function via the corresponding workload; however, you can also install the packages contained in the workload individually. This documentation briefly describes the installation process via the workload.

Command line program TcPkg

You can use the TcPkg **C**ommand **L**ine **I**nterface (CLI) to display the available workloads on the system:

```
tcpkg list -t workload
```

You can use the following command to install the workload of a function.
Shown here using the example of the TF6100 TwinCAT OPC UA Client:

```
tcpkg install tf6100-opc-ua-client
```

TwinCAT Package Manager UI

You can use the **U**ser **I**nterface (UI) to display all available workloads and install them if required.
To do this, follow the corresponding instructions in the interface.

NOTICE

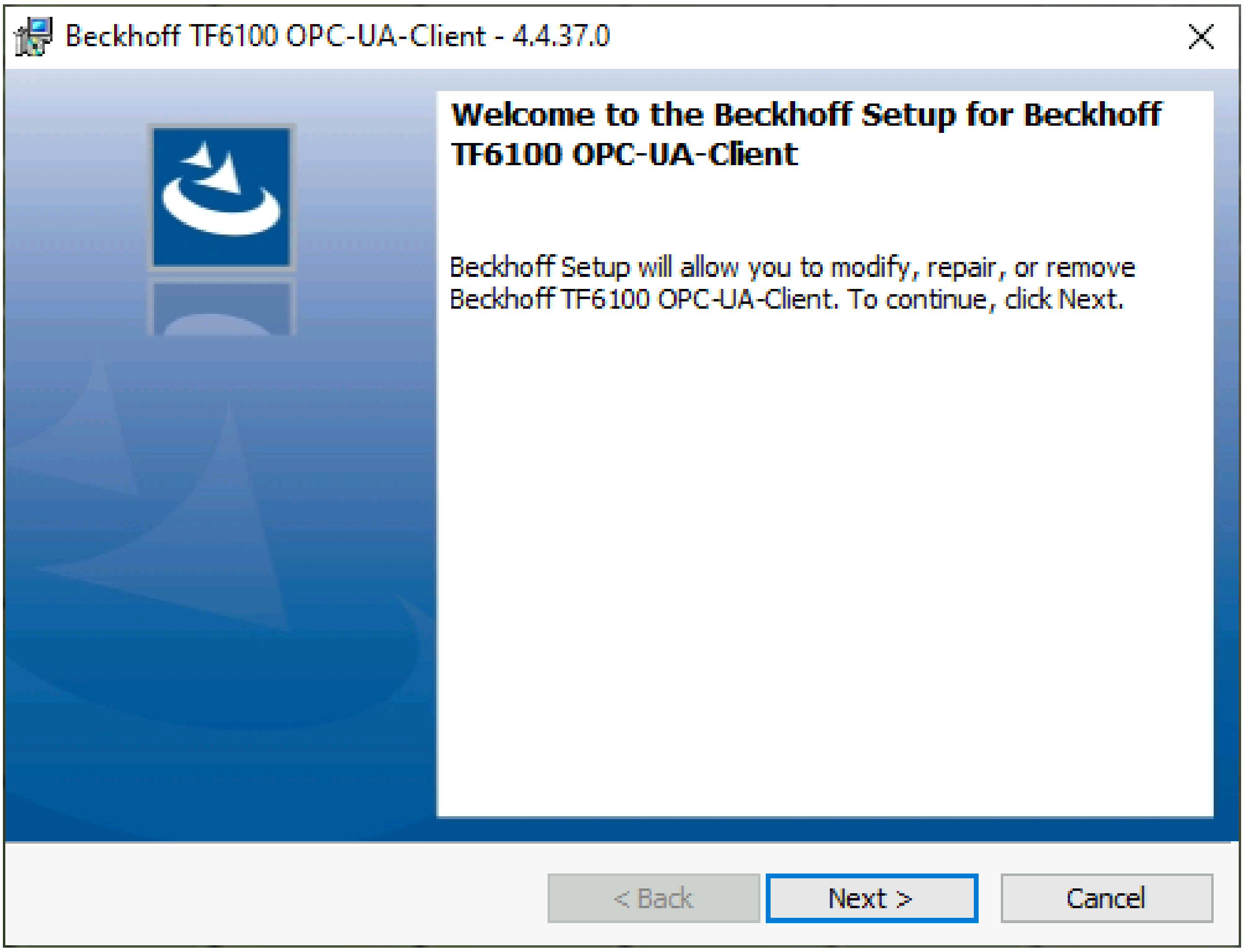
Unprepared TwinCAT restart can cause data loss

The installation of this function may result in a TwinCAT restart.
Make sure that no critical TwinCAT applications are running on the system or shut them down in an orderly manner first.

Setup

If you are using TwinCAT 3.1 Build 4024 on the Microsoft Windows operating system, you can install this function via a setup package, which you can download from the Beckhoff website at https://www.beckhoff.com/download.

Depending on the system on which you need the function, the installation can be done on either the engineering or runtime side. The following screenshot shows an example of the setup interface using the TF6100 TwinCAT OPC UA Client setup.



Beckhoff TF6100 OPC-UA-Client - 4.4.37.0

Welcome to the Beckhoff Setup for Beckhoff TF6100 OPC-UA-Client

Beckhoff Setup will allow you to modify, repair, or remove Beckhoff TF6100 OPC-UA-Client. To continue, click Next.

To complete the installation process, follow the instructions in the Setup dialog.

NOTICE

Unprepared TwinCAT restart can cause data loss

Installing this function may cause TwinCAT to restart.
Make sure that no critical TwinCAT applications are running on the system or shut them down in an orderly manner first.

3.3 Installation variants

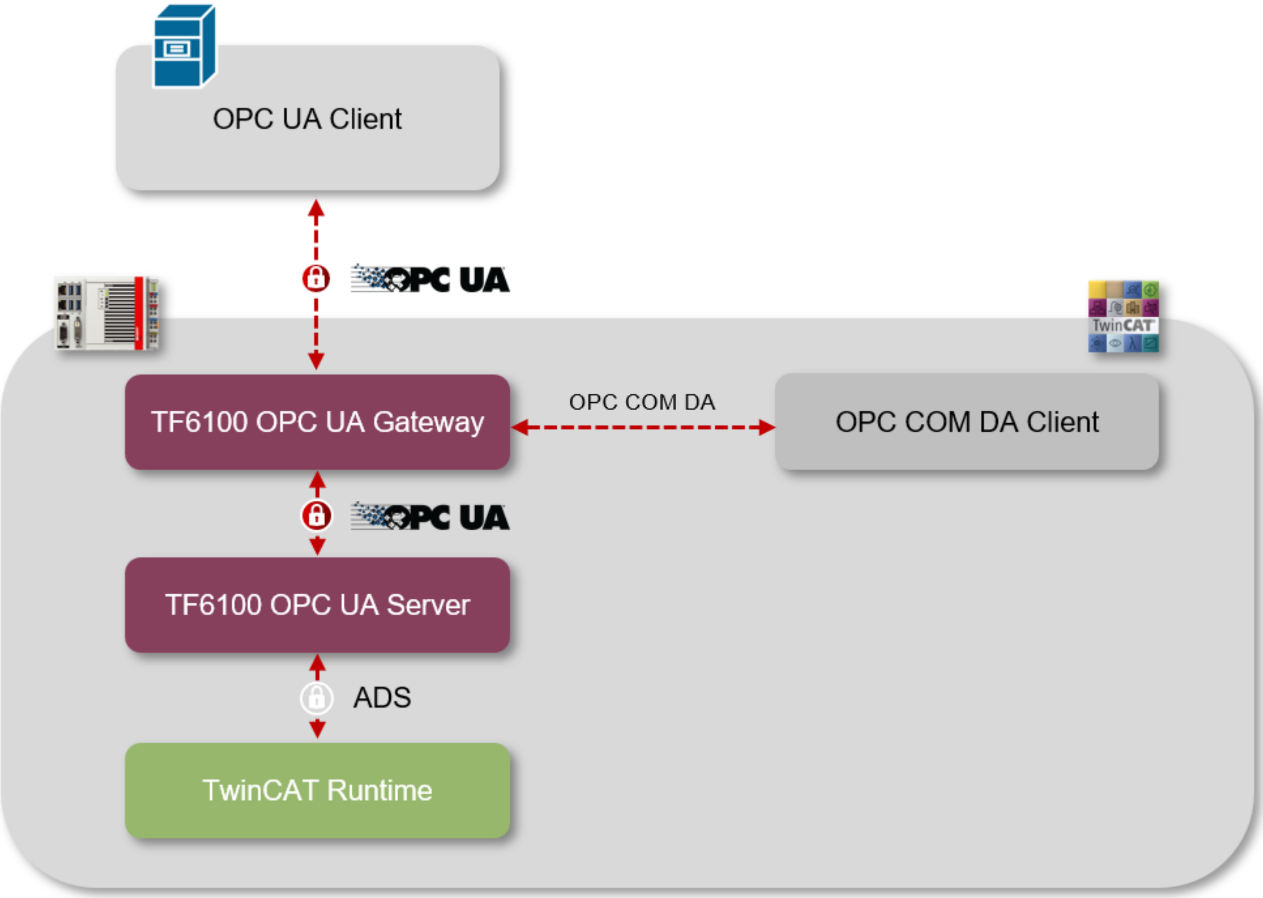
This chapter describes the different supported installation variants of the TwinCAT OPC UA Gateway. Please note that the complexity of these variants can be extended almost at will. The examples given only represent frequently occurring installation variants.

Gateway and server on the same device

In this scenario, the TwinCAT OPC UA Gateway and the TwinCAT OPC UA Server are installed on the same device. The gateway is configured with the default settings in order to establish a connection with the local TwinCAT OPC UA Server with the following Server URL: opc.tcp://localhost:4840.

From the client's point of view, two scenarios are supported in this case:

- An OPC UA client accesses the lower-level server via the gateway in order to access symbols from the TwinCAT Runtime. The client can be located on the same device or on a device in the network. The communication connection between the client and gateway is OPC UA.
- An OPC COM DA client accesses the lower-level server via the gateway in order to access symbols from the TwinCAT Runtime. The client must be located on the same device. The communication connection between client and gateway is OPC COM DA.

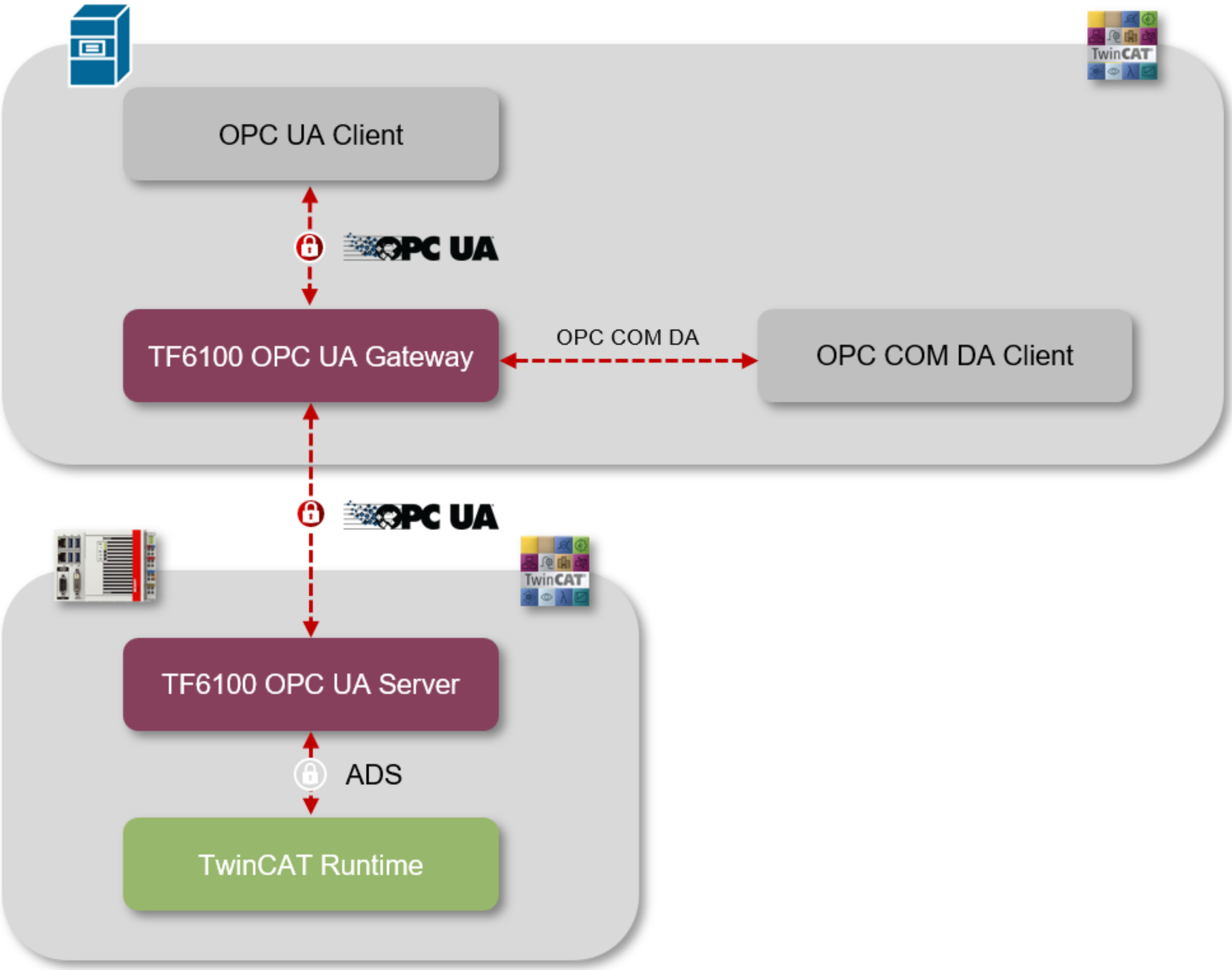


Gateway and server on different devices

In this scenario, the TwinCAT OPC UA Gateway and the TwinCAT OPC UA Server are installed on different devices. The gateway is configured to establish a connection with the remote TwinCAT OPC UA Server by storing its server URL, e.g. opc.tcp://192.168.1.1:4840, in the gateway.

From the client's point of view, two scenarios are supported in this case:

- An OPC UA client accesses the lower-level server via the gateway in order to access symbols from the TwinCAT Runtime. The client can be located on the same device or on a device in the network. The communication connection between the client and gateway is OPC UA.
- An OPC COM DA client accesses the lower-level server via the gateway in order to access symbols from the TwinCAT Runtime. The client must be located on the same device. The communication connection between client and gateway is OPC COM DA.

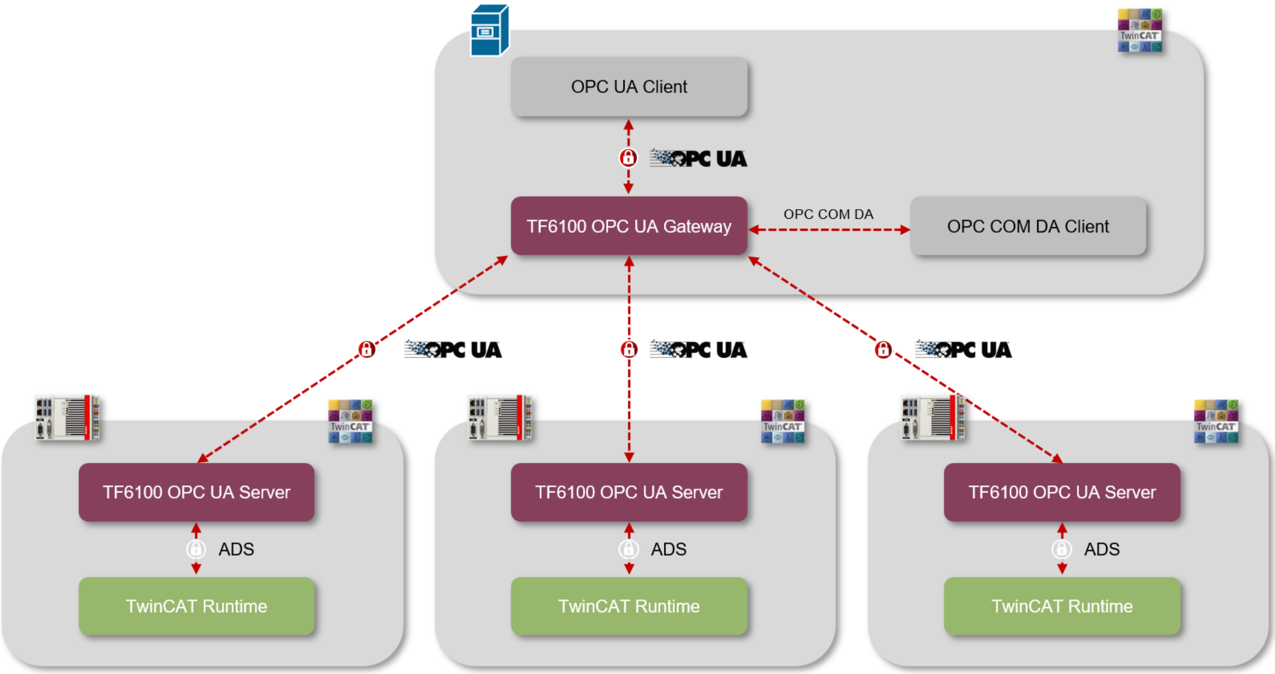


Connecting the gateway to several servers

You can also connect the TwinCAT OPC UA Gateway to several lower-level TwinCAT OPC UA Servers. The servers can be installed on the same device or on devices in the network. This scenario can of course be extended as required. The following diagram illustrates a scenario in which three TwinCAT OPC UA Servers were connected to the gateway in the network.

From the client's point of view, two scenarios are supported in this case:

- An OPC UA client accesses the lower-level servers via the gateway in order to access symbols from the individual TwinCAT Runtimes. The client can be located on the same device or on a device in the network. The communication connection between the client and gateway is OPC UA.
- An OPC COM DA client accesses the lower-level servers via the gateway in order to access symbols from the TwinCAT Runtimes. The client must be located on the same device. The communication connection between client and gateway is OPC COM DA.


OPC UA Client
OPC UA
TF6100 OPC UA Gateway
OPC COM DA
OPC COM DA Client
TwinCAT
OPC UA
OPC UA
OPC UA
TF6100 OPC UA Server
ADS
TwinCAT Runtime
TF6100 OPC UA Server
ADS
TwinCAT Runtime
TF6100 OPC UA Server
ADS
TwinCAT Runtime

4 Technical introduction

4.1 Quick start

The TwinCAT OPC UA Gateway is available for download as a separate setup. The setup automatically configures access to a TwinCAT OPC UA Server running on the same computer as the gateway.

If more than one OPC UA server is added to the gateway, or if the server is running on a different computer, the standard configuration has to be modified. Use the Configurator to configure these settings.

Configuration of the TwinCAT OPC UA Server

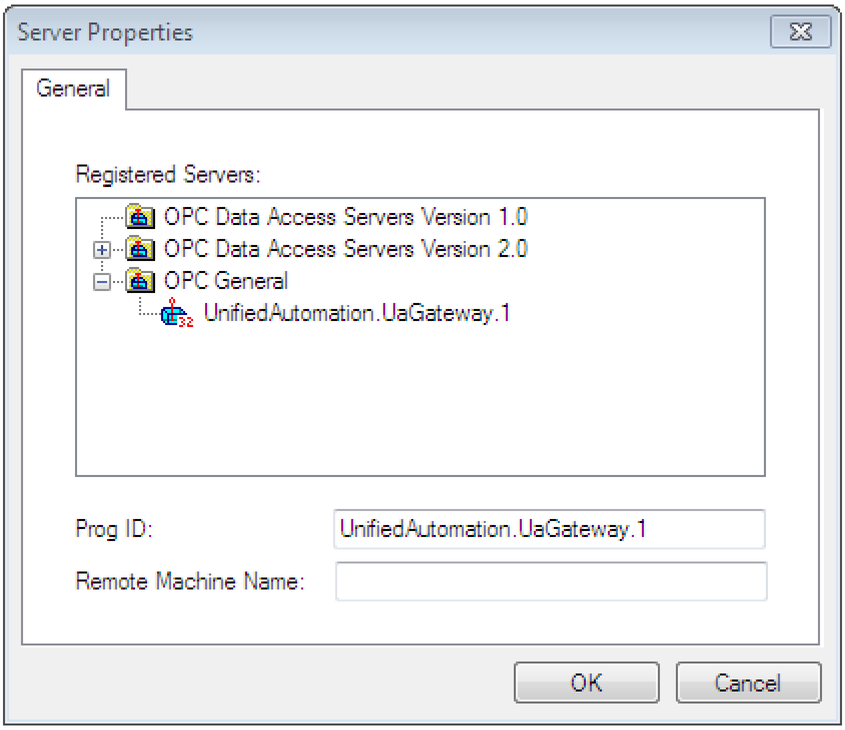
Check the configuration of the OPC UA server and make sure that it is operating as expected before continuing.

For further information regarding the configuration of the OPC UA Server, read the Quick Start in the chapter "OPC UA Server".

Quick start – OPC COM DA

To connect an OPC COM DA Client to the gateway, start the client and establish a connection to the following ProgId:

```
UnifiedAutomation.UaGateway.1
```



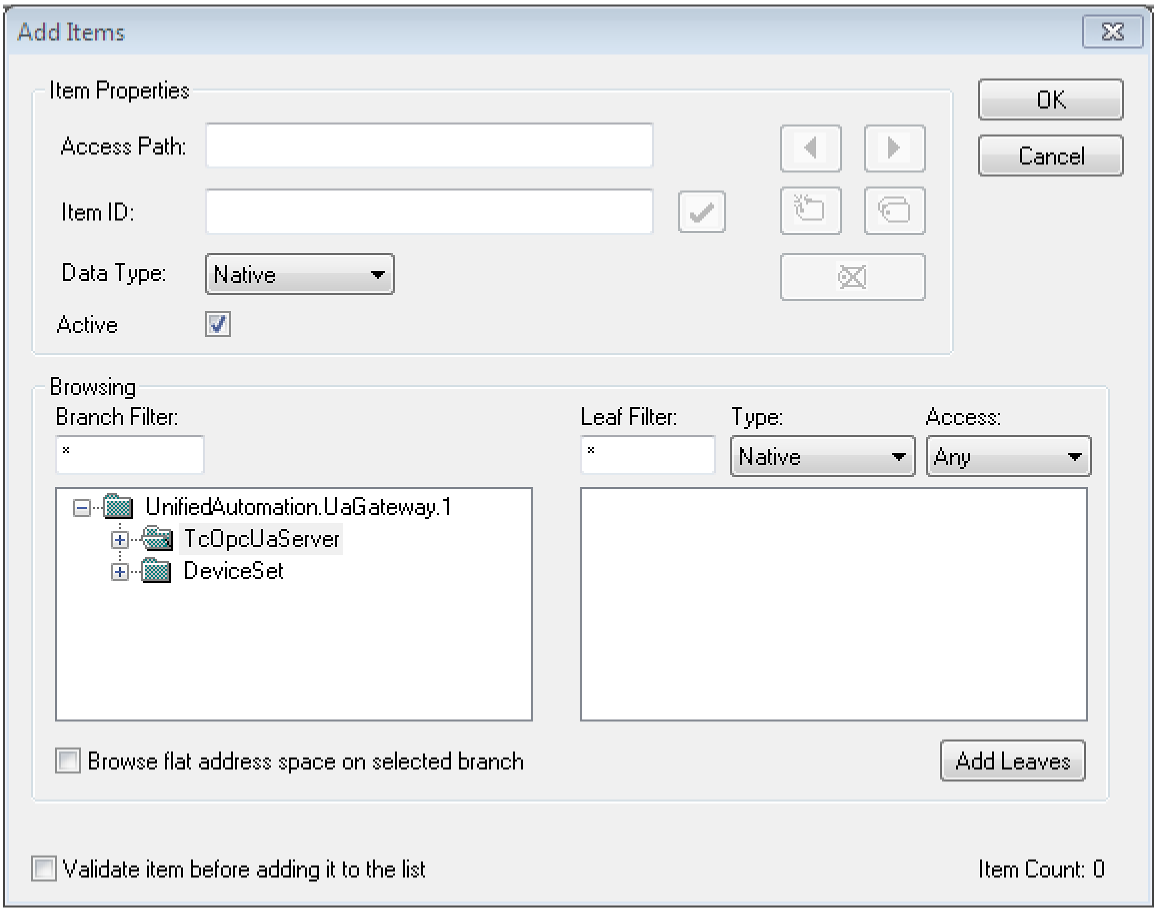
Registered Servers:

- OPC Data Access Servers Version 1.0
- OPC Data Access Servers Version 2.0
- OPC General
  - UnifiedAutomation.UaGateway.1

Prog ID: UnifiedAutomation.UaGateway.1

Remote Machine Name:

When browsing the gateway, one or more OPC UA Servers will be visible in the namespace of the gateway.



Access Path:

Item ID:

Data Type: Native

Active ☑

Branch Filter: *

Leaf Filter: *

Type: Native

Access: Any

- UnifiedAutomation.UaGateway.1
  - TcOpcUaServer
  - DeviceSet

□ Browse flat address space on selected branch

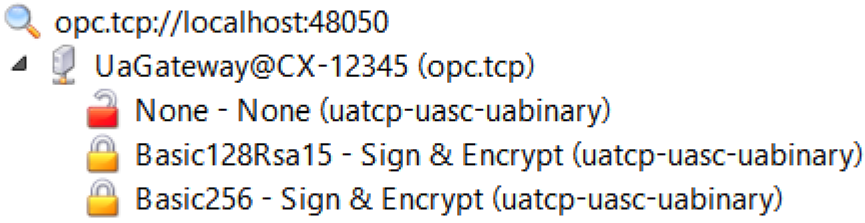
□ Validate item before adding it to the list

Item Count: 0

Quick start – OPC UA

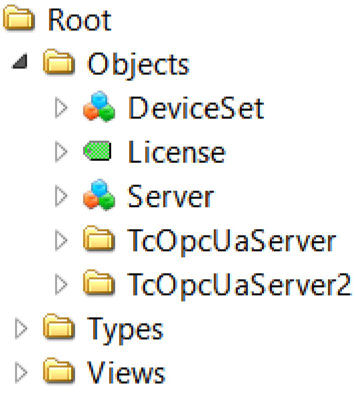
The gateway not only offers an OPC COM DA interface, but also allows the aggregation of one or more OPC UA Servers. The gateway also opens an OPC UA interface for this purpose. The gateway can be accessed via the following OPC UA Server URL:

```
opc.tcp://[HostnameOrIpAddressOrLocalhost]:48050
```



opc.tcp://localhost:48050
- UaGateway@CX-12345 (opc.tcp)
  - None - None (uatcp-uasc-uabinary)
  - Basic128Rsa15 - Sign & Encrypt (uatcp-uasc-uabinary)
  - Basic256 - Sign & Encrypt (uatcp-uasc-uabinary)

The namespace of the gateway then contains all underlying TwinCAT OPC UA Servers.



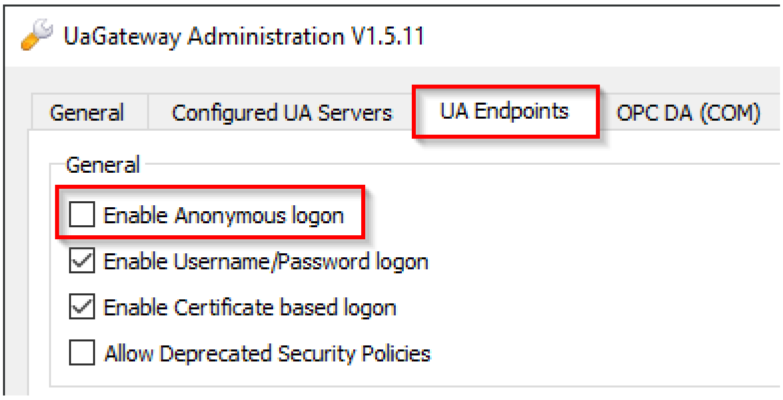
- Root
  - Objects
    - DeviceSet
    - License
    - Server
    - TcOpcUaServer
    - TcOpcUaServer2
  - Types
  - Views

4.2 Recommended steps

After the initial commissioning, we recommend that you pay attention to the following points to further configure the gateway and ensure a stable and secure operating environment.

Only use secure IdentityTokens

The gateway is configured with the activated IdentityToken "Anonymous" in the delivery state. We recommend disabling this IdentityToken so that only authenticated users can connect to the OPC UA server interface of the gateway. You can disable this setting in the configuration of the endpoints [▸ 23] of the TwinCAT OPC UA Gateway Configurator.



UaGateway Administration V1.5.11

General

☐ Enable Anonymous logon

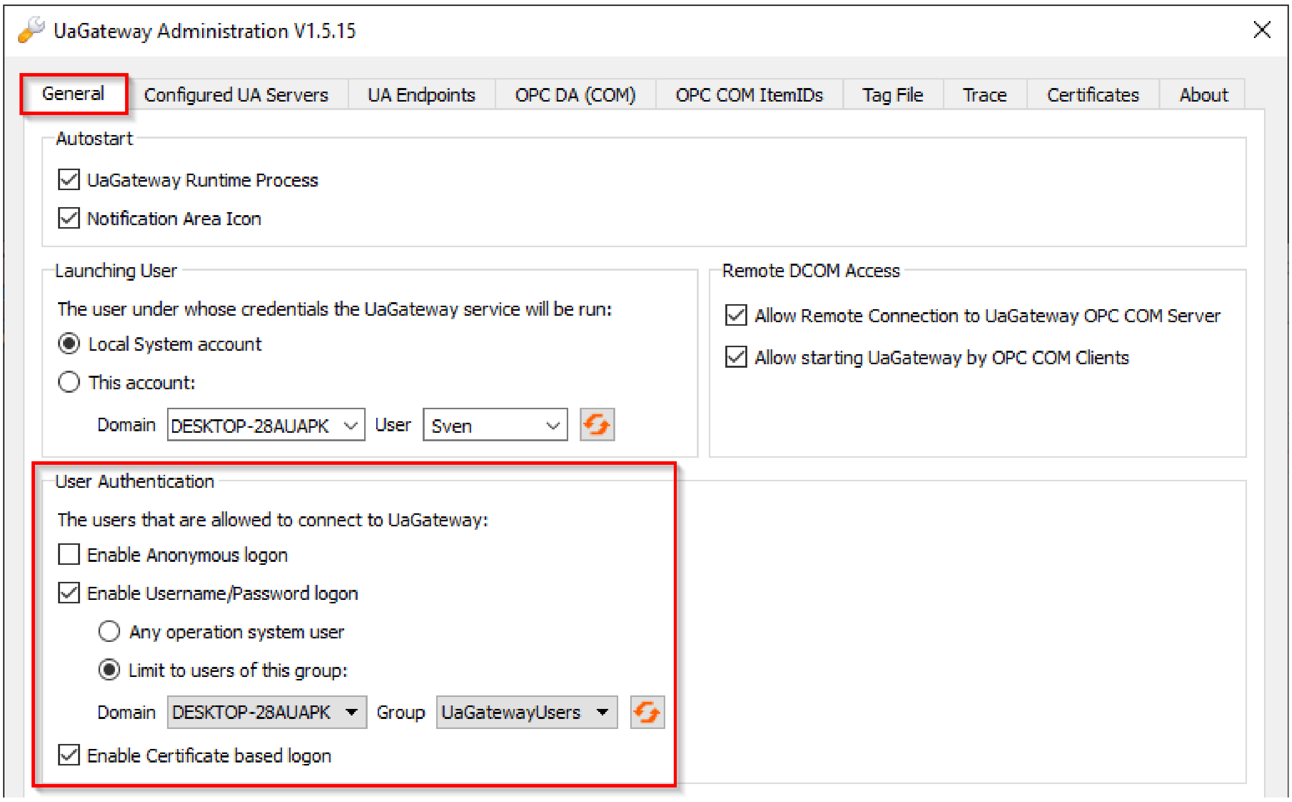
☑ Enable Username/Password logon

☑ Enable Certificate based logon

☐ Allow Deprecated Security Policies

Configuration of a user group with access rights

You should use the TwinCAT OPC UA Gateway Configurator to define a user group that has access rights to the gateway. Users from this user group can then be specified as IdentityToken when connecting an OPC UA client to the gateway.



UaGateway Administration V1.5.15

Autostart

☑ UaGateway Runtime Process

☑ Notification Area Icon

Launching User

The user under whose credentials the UaGateway service will be run:

● Local System account

○ This account:

Domain DESKTOP-28AUAPK User Sven

Remote DCOM Access

☑ Allow Remote Connection to UaGateway OPC COM Server

☑ Allow starting UaGateway by OPC COM Clients

User Authentication

The users that are allowed to connect to UaGateway:

☐ Enable Anonymous logon

☑ Enable Username/Password logon

○ Any operation system user

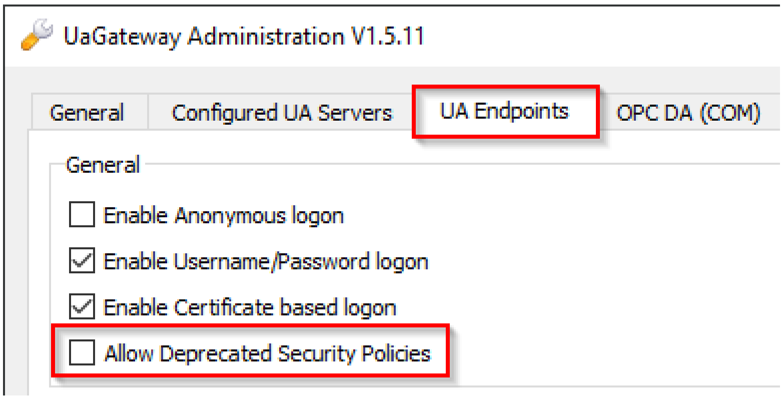
● Limit to users of this group:

Domain DESKTOP-28AUAPK Group UaGatewayUsers

☑ Enable Certificate based logon

Leave insecure endpoints disabled

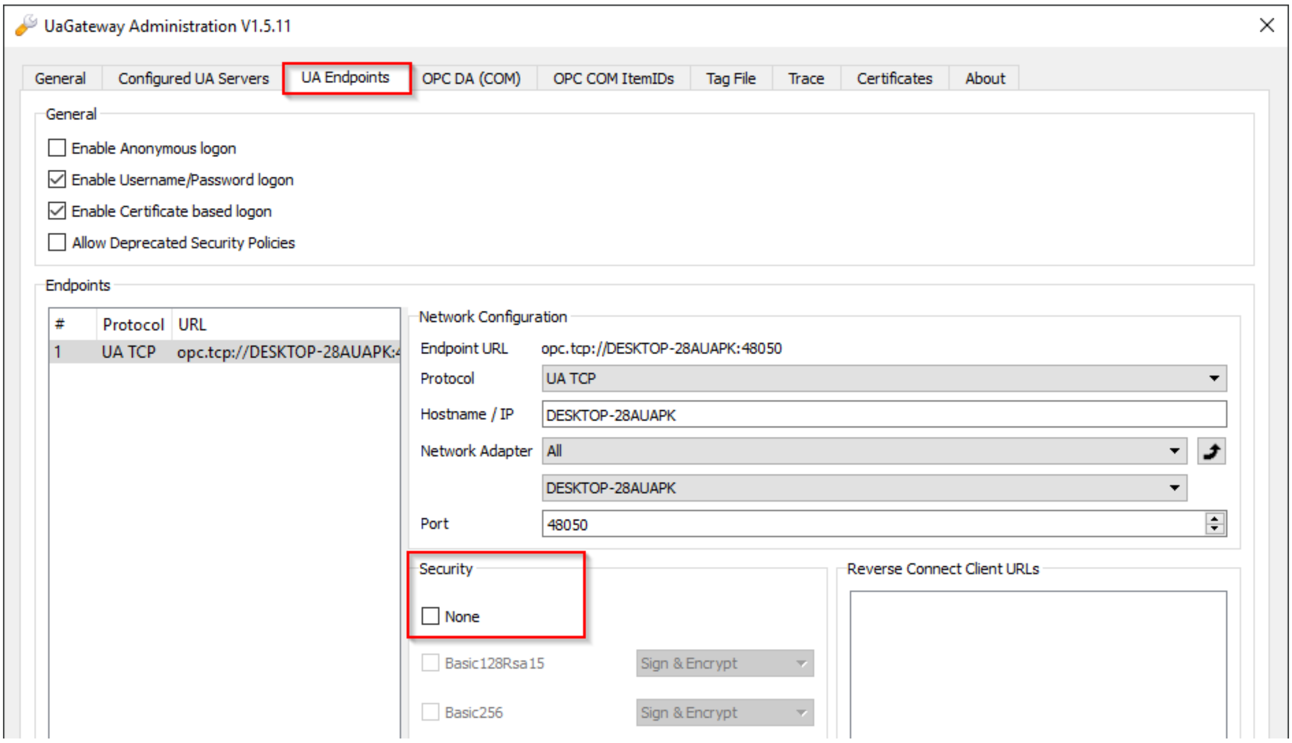
Endpoints classified as insecure are not offered by the TwinCAT OPC UA Gateway by default. These can be made available in the gateway via a configuration parameter when configuring the endpoints [▶ 23] – however, we strongly advise against this and only recommend using the endpoints that are currently considered secure.



General

- ☐ Enable Anonymous logon
- ☑ Enable Username/Password logon
- ☑ Enable Certificate based logon
- ☐ Allow Deprecated Security Policies

Furthermore, the unencrypted endpoint ("None/None") is disabled in the gateway's delivery state and we recommend leaving it disabled. If this needs to be activated for compatibility reasons, this can also be done via the configuration parameters in the configurator.



General

- ☐ Enable Anonymous logon
- ☑ Enable Username/Password logon
- ☑ Enable Certificate based logon
- ☐ Allow Deprecated Security Policies

Endpoints

#	Protocol	URL
1	UA TCP	opc.tcp://DESKTOP-28AUAPK:4

Network Configuration

Endpoint URL opc.tcp://DESKTOP-28AUAPK:48050

Protocol UA TCP

Hostname / IP DESKTOP-28AUAPK

Network Adapter All

DESKTOP-28AUAPK

Port 48050

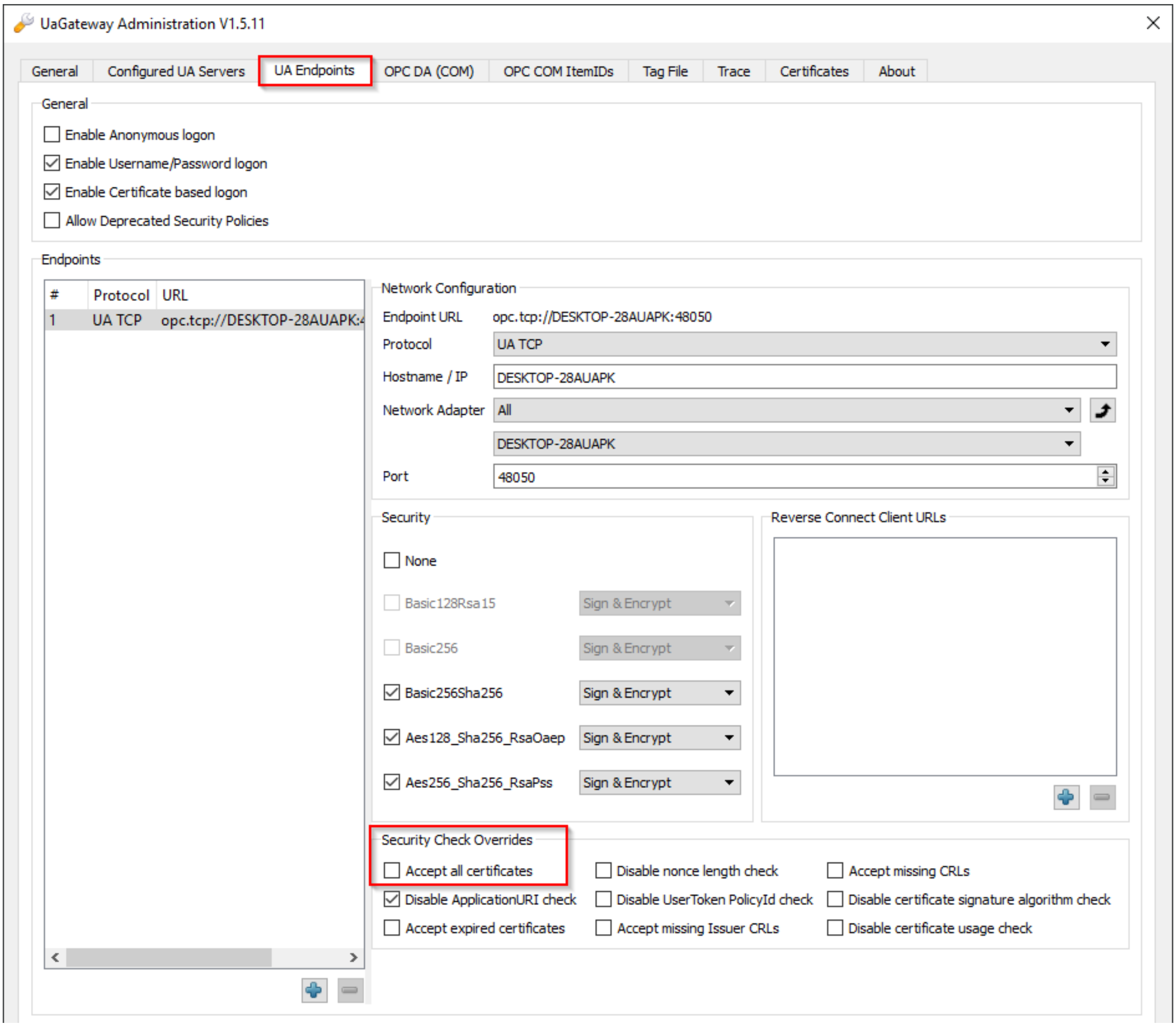
Security

- ☐ None
- ☐ Basic128Rsa15 Sign & Encrypt
- ☐ Basic256 Sign & Encrypt

Reverse Connect Client URLs

Disable 'Accept all certificates'

By default, the gateway is configured for easy commissioning so that it automatically trusts all client certificates without having to manually exchange certificates on the gateway side. For security reasons, we recommend disabling this setting. This setting can be disabled via the TwinCAT OPC UA Gateway configurator when configuring the endpoints [▶ 23].


UaGateway Administration V1.5.11
General | Configured UA Servers | UA Endpoints | OPC DA (COM) | OPC COM ItemIDs | Tag File | Trace | Certificates | About

General

☐ Enable Anonymous logon
☑ Enable Username/Password logon
☑ Enable Certificate based logon
☐ Allow Deprecated Security Policies

Endpoints

#	Protocol	URL
1	UA TCP	opc.tcp://DESKTOP-28AUAPK:4

Network Configuration

Endpoint URL: opc.tcp://DESKTOP-28AUAPK:48050
Protocol: UA TCP
Hostname / IP: DESKTOP-28AUAPK
Network Adapter: All
DESKTOP-28AUAPK
Port: 48050

Security

☐ None
☐ Basic128Rsa15 – Sign & Encrypt
☐ Basic256 – Sign & Encrypt
☑ Basic256Sha256 – Sign & Encrypt
☑ Aes128_Sha256_RsaOaep – Sign & Encrypt
☑ Aes256_Sha256_RsaPss – Sign & Encrypt

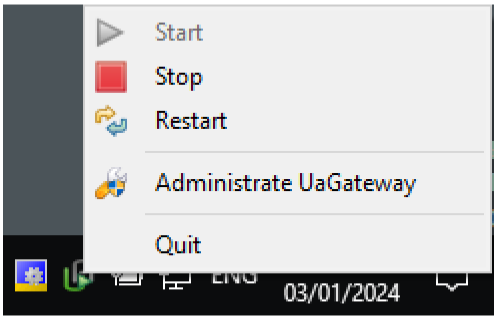
Reverse Connect Client URLs

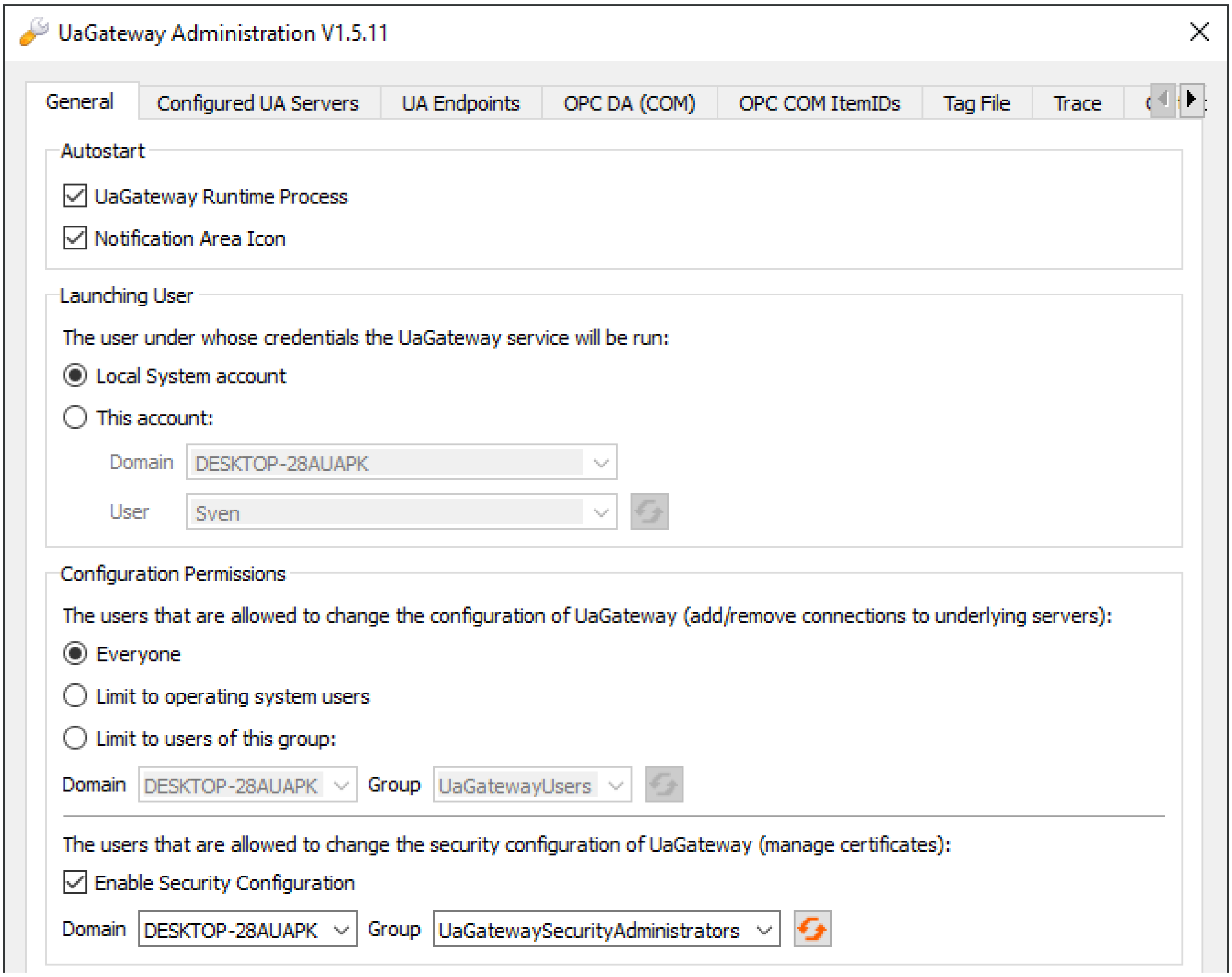
Security Check Overrides

☐ Accept all certificates
☐ Disable nonce length check
☐ Accept missing CRLs
☑ Disable ApplicationURI check
☐ Disable UserToken PolicyId check
☐ Disable certificate signature algorithm check
☐ Accept expired certificates
☐ Accept missing Issuer CRLs
☐ Disable certificate usage check

4.3 Configurator

The TwinCAT OPC UA Gateway includes a graphical user interface for configuring the software. You can open this configurator via the **Administrate UaGateway** entry in the context menu of the gateway icon in the Windows system tray.





UaGateway Administration V1.5.11

Autostart

☑ UaGateway Runtime Process

☑ Notification Area Icon

Launching User

The user under whose credentials the UaGateway service will be run:

● Local System account

○ This account:

Domain DESKTOP-28AUAPK

User Sven

Configuration Permissions

The users that are allowed to change the configuration of UaGateway (add/remove connections to underlying servers):

● Everyone

○ Limit to operating system users

○ Limit to users of this group:

Domain DESKTOP-28AUAPK Group UaGatewayUsers

The users that are allowed to change the security configuration of UaGateway (manage certificates):

☑ Enable Security Configuration

Domain DESKTOP-28AUAPK Group UaGatewaySecurityAdministrators

4.4 Application directories

This application uses various directories to store relevant information, e.g. configuration or certificate files.

Installation directory

The base installation directory of the application is always relative to the TwinCAT installation directory on all operating systems.

```
%TcInstallDir%\Functions\TF6100-OPC-UA
```

The application is then installed in the following directory below this directory.

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway
```

Base directory for PKI infrastructure (server)

Certificate files, which are used to establish a secure communication connection with the OPC UA server of the gateway, are stored in the following directory:

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver
```

Directory for trusted certificates (server)

Client certificates in this directory are declared as "trusted".

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\trusted\certs
```

Directory for rejected certificates (server)

Client certificates in this directory are declared as "rejected".

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\rejected
```

Base directory for PKI infrastructure (client)

Certificate files that the gateway uses as an OPC UA client to establish a secure communication connection with the lower-level TwinCAT OPC UA Servers are stored in the following directory:

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiclient
```

Directory for trusted certificates (client)

Client certificates in this directory are declared as "trusted".

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiclient\trusted\certs
```

Directory for rejected certificates (client)

Server certificates in this directory are declared as "rejected".

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiclient\rejected
```

Directory for the server and client certificate

The directories for the OPC UA server and client certificate of the gateway are defined as follows, whereby a distinction is made between the directory for the public key ("certs") and private key ("private"). Server and client use the same certificate.

```
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\own\certs
%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Gateway\pkiserver\own\private
```

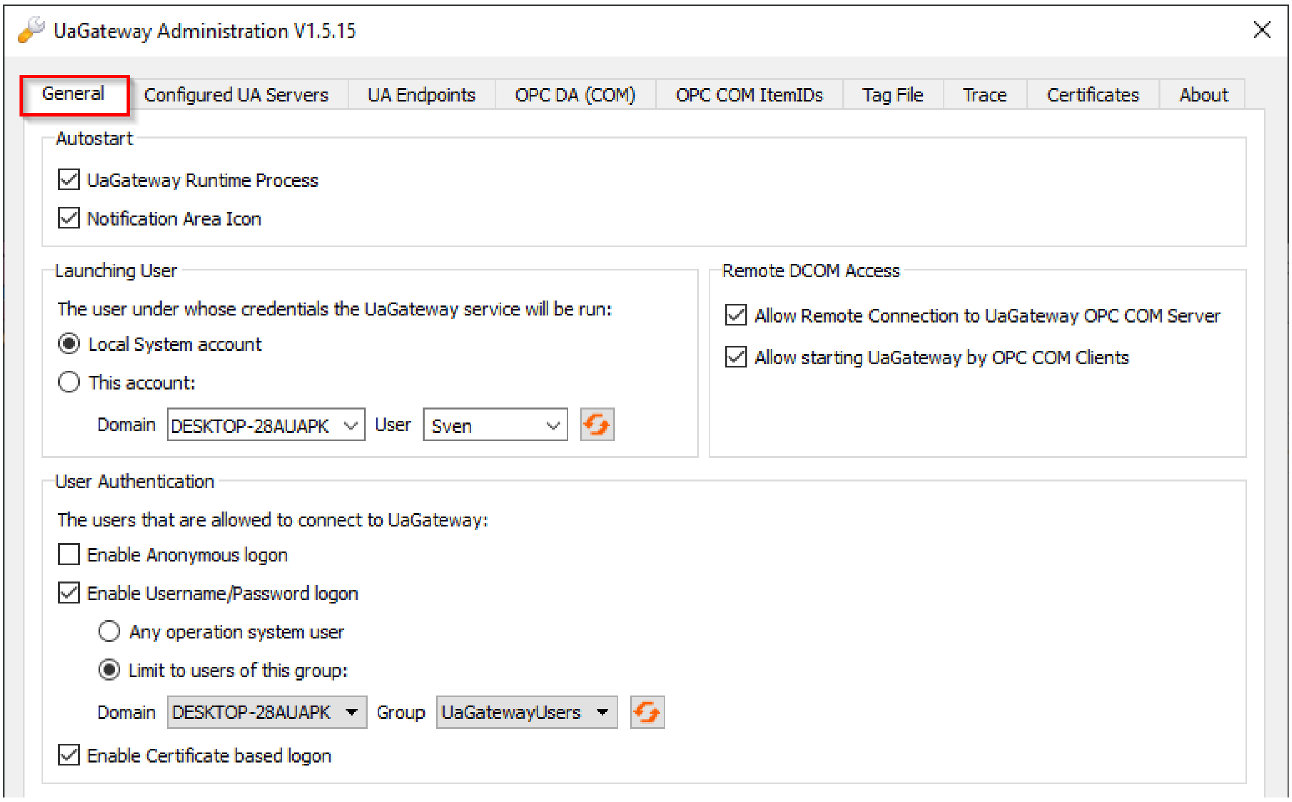
Log files

Log files are stored in the following directory.

```
%ProgramData%\UnifiedAutomation\TwinCAT OPC UA Gateway\Trace
```

4.5 General settings

The **General** tab in the TwinCAT OPC UA Gateway Configurator [▶ 19] can be used to make general settings for the gateway.



Autostart

☑ UaGateway Runtime Process

☑ Notification Area Icon

Launching User

The user under whose credentials the UaGateway service will be run:

● Local System account

○ This account:

Domain DESKTOP-28AUAPK User Sven

Remote DCOM Access

☑ Allow Remote Connection to UaGateway OPC COM Server

☑ Allow starting UaGateway by OPC COM Clients

User Authentication

The users that are allowed to connect to UaGateway:

☐ Enable Anonymous logon

☑ Enable Username/Password logon

○ Any operation system user

● Limit to users of this group:

Domain DESKTOP-28AUAPK Group UaGatewayUsers

☑ Enable Certificate based logon

These settings are described in more detail below.

Autostart

In this area you can configure the autostart behavior of the TwinCAT OPC UA Gateway. Activate the **UaGateway Runtime Process** option to start the Windows service of the gateway automatically when the computer is switched on. Activate the **Notification Area Icon** option to start the Windows system tray icon of the gateway when a user logs on.

Launching User

The TwinCAT OPC UA Gateway is registered as a Windows service by default and is automatically started when the system is started. A specific user context is assigned to the Windows service. The user you select here is assigned to the Windows service. In addition, the user is granted the "LogOnAsService" right and is added to the local user group "UaGatewayUsers".

User Authentication

In this area, you can define which IdentityTokens are available when an OPC UA client is connected to the gateway. You can also define a user group that should have access to the gateway. Users from this user group can then be used by an OPC UA client when establishing a connection.

Configuration Permissions

It is possible to allow only certain users to change the configuration of the gateway, i.e. to add or remove connections to lower-level servers. You can select from the following settings:

Everyone	Any user (including users logged in anonymously via OPC UA) who can establish a connection with the gateway can change the configuration.
Limit to operating system users	Only local users and users from the same domain can change the configuration.
Limit to users of this group	Only users in a specific group are allowed to change the configuration.

UA Discovery Registration

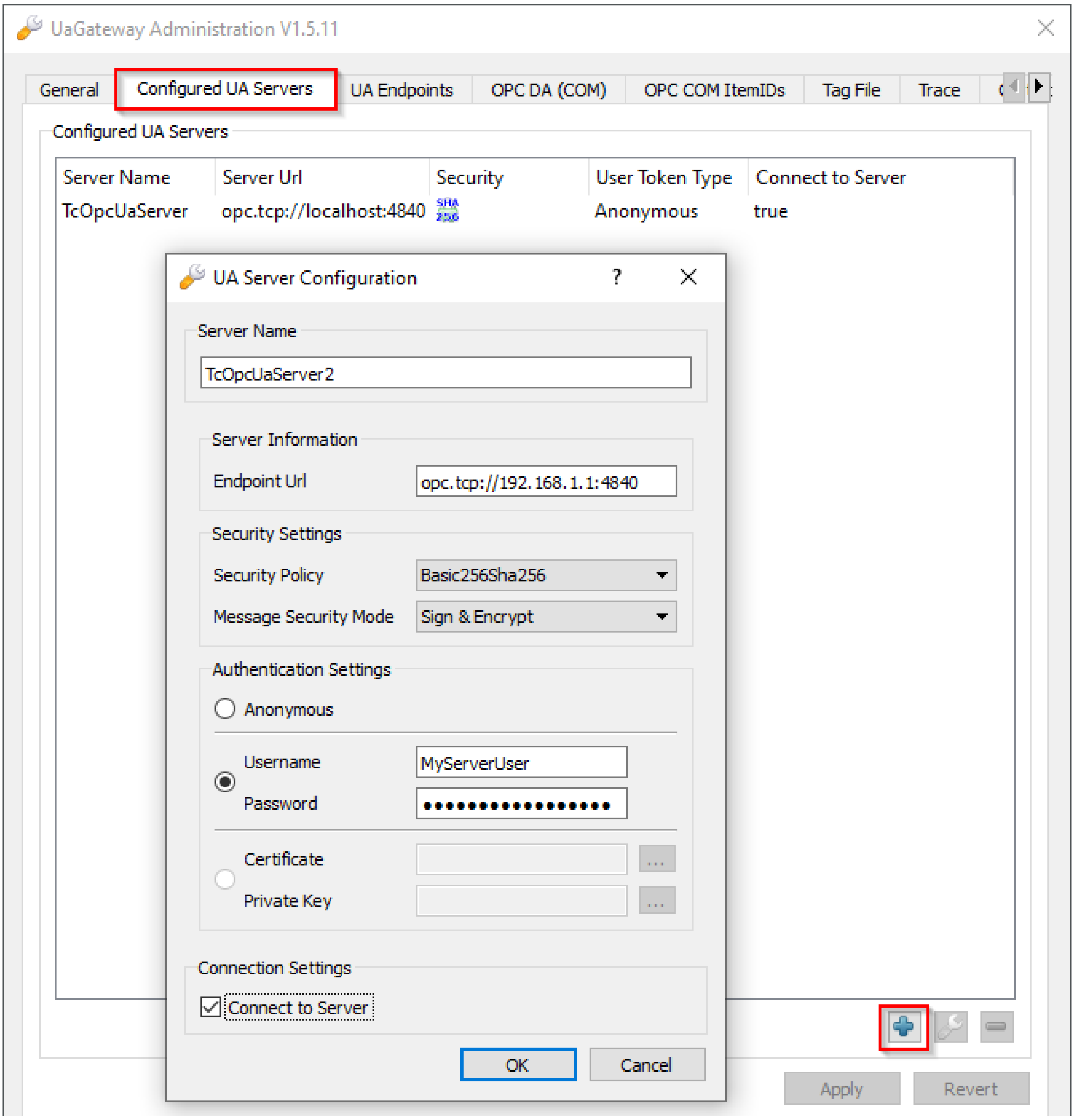
Activate the **Register at Local Discovery Server** option if the gateway is to be registered with the local Local Discovery Server (LDS).

Remote DCOM Access

Depending on the version of the TwinCAT OPC UA Gateway used, the configuration option **Remote DCOM Access** may also be displayed. These configuration parameters are not supported by the gateway and can be ignored. See also System requirements [▶ 10].

4.6 Configuration of additional servers

Via the **Configured UA Servers** tab in the TwinCAT OPC UA Gateway Configurator [▶ 19], you can add further lower-level TwinCAT OPC UA Servers to the gateway. On delivery, the gateway already establishes a connection to a TwinCAT OPC UA Server that has been installed on the same system.



Configured UA Servers

Server Name	Server Url	Security	User Token Type	Connect to Server
TcOpcUaServer	opc.tcp://localhost:4840	SHA 256	Anonymous	true

Server Name: TcOpcUaServer2

Server Information

Endpoint Url: opc.tcp://192.168.1.1:4840

Security Settings

Security Policy: Basic256Sha256

Message Security Mode: Sign & Encrypt

Authentication Settings

○ Anonymous

● Username: MyServerUser
Password: •••••••••••••••••

○ Certificate
Private Key

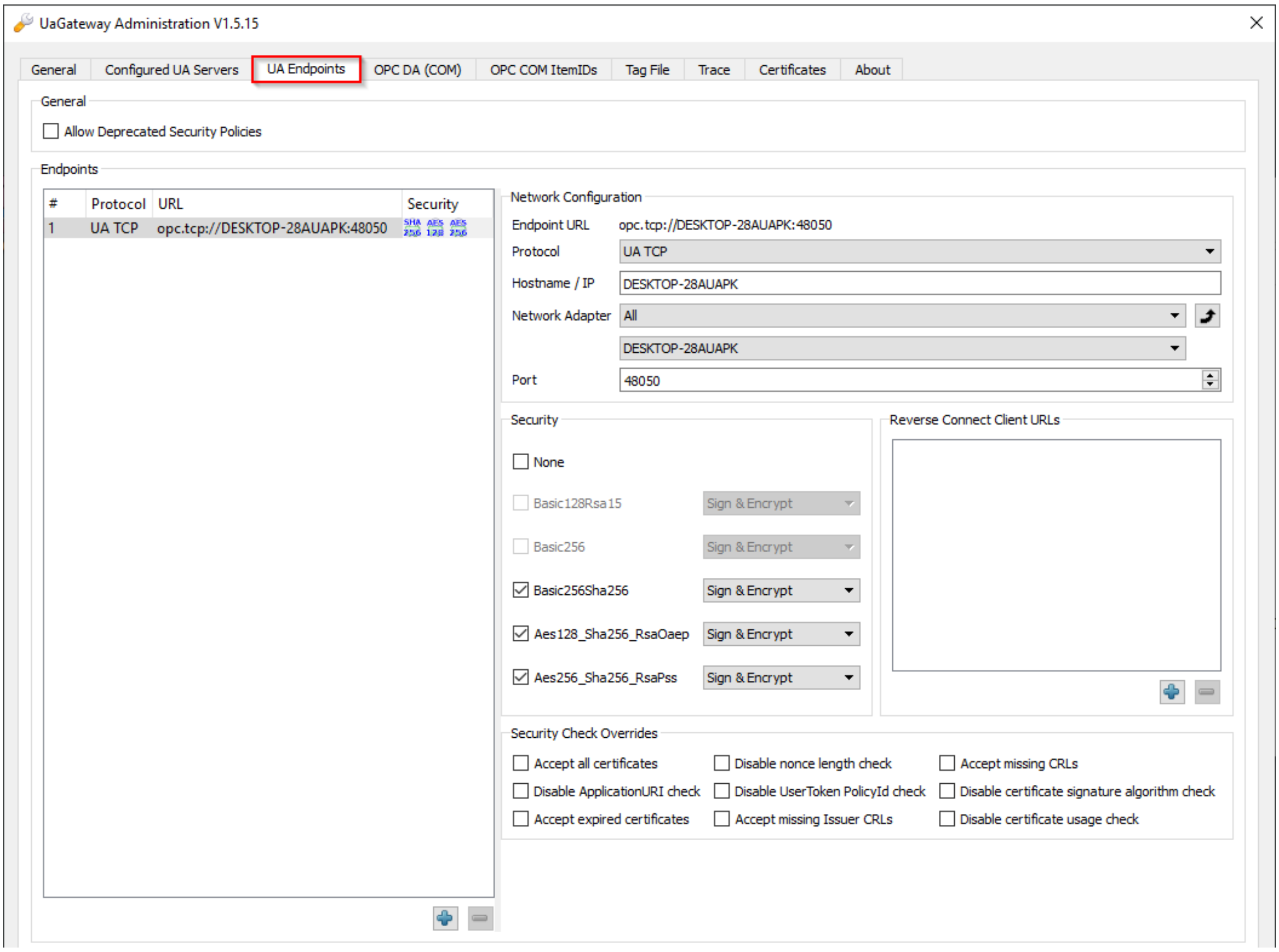
Connection Settings

☑ Connect to Server

To configure additional TwinCAT OPC UA Servers or to remove them from the configuration, click on the plus or minus button and then on **Apply** to save the changes.

4.7 Configuration of the endpoints

The **UA Endpoints** tab in the TwinCAT OPC UA Gateway Configurator [▸ 19] allows you to make settings for the OPC UA endpoint configuration. The OPC UA endpoint is the connection information required by an OPC UA client to connect to the gateway.



General

□ Allow Deprecated Security Policies

Endpoints

#	Protocol	URL	Security
1	UA TCP	opc.tcp://DESKTOP-28AUAPK:48050	SHA 256 AES 128 AES 256

Network Configuration

Endpoint URL opc.tcp://DESKTOP-28AUAPK:48050

Protocol UA TCP

Hostname / IP DESKTOP-28AUAPK

Network Adapter All

DESKTOP-28AUAPK

Port 48050

Security

□ None

□ Basic128Rsa15 Sign & Encrypt

□ Basic256 Sign & Encrypt

☑ Basic256Sha256 Sign & Encrypt

☑ Aes128_Sha256_RsaOaep Sign & Encrypt

☑ Aes256_Sha256_RsaPss Sign & Encrypt

Reverse Connect Client URLs

Security Check Overrides

□ Accept all certificates □ Disable nonce length check □ Accept missing CRLs

□ Disable ApplicationURI check □ Disable UserToken PolicyId check □ Disable certificate signature algorithm check

□ Accept expired certificates □ Accept missing Issuer CRLs □ Disable certificate usage check

The configuration options available in this tab are described in more detail below.

General

In this area, you can enable the configuration switch **Allow deprecated security policies** to activate deprecated and potentially insecure security policies in the gateway. However, we recommend leaving this option disabled and enabling it only in case of compatibility issues with old OPC UA clients. In this case, however, the correct procedure would be to contact the client vendor for an update.

Endpoints

Here you can define all necessary settings for the different OPC UA endpoints, create new endpoints or remove them. A predefined endpoint is already available on delivery, which should normally be sufficient for all applications. This endpoint defines the available security policies, as well as settings for the Network Configuration, Port, Reverse Connect Client URLs and any Security Check Overrides.

These configuration elements are described in more detail in the following sections.

Network Configuration

In this area, you can define the network interface for which the endpoint is to be configured. The endpoint that is defined in the delivery state of the gateway is automatically configured for all network interfaces. This means that the gateway can be accessed through any network interface installed and configured in the operating system. The following configuration parameters can be defined here:

Configuration parameters	Description
Endpoint URL	Endpoint URL of the gateway as it appears in the OPC UA client when GetEndpoint is called.
Protocol	Protocol to be used. Only the "UA TCP" protocol is supported.
Hostname / IP	Host name or IP address of the device on which the gateway was installed.
Network Adapter	Selection of the network adapter under which the gateway should be accessible for OPC UA clients.
Port	Network port (TCP) under which the gateway should be accessible for OPC UA clients.

Security

In this area, you can configure the supported security policies of the endpoint. Activate the checkboxes in front of the respective security policy to configure it for the endpoint. Next to the security policy is a selection element for the Message Security Mode that applies to the endpoint.

Reverse Connect Client URLs

In this area, you can enter the endpoint URLs of clients that are to be used for the Reverse Connect functionality.

Security Check Overrides

In this area, you can configure exception rules for the validation of various security options.

4.8 Migration of TF6120

One of the primary purposes of the UA Gateway is to provide a sustainable connectivity in order to replace the Tx6120 OPC DA supplement/function. Observe the following notes if you wish to migrate Tx6120 OPC DA to UA Gateway.

Standard configuration

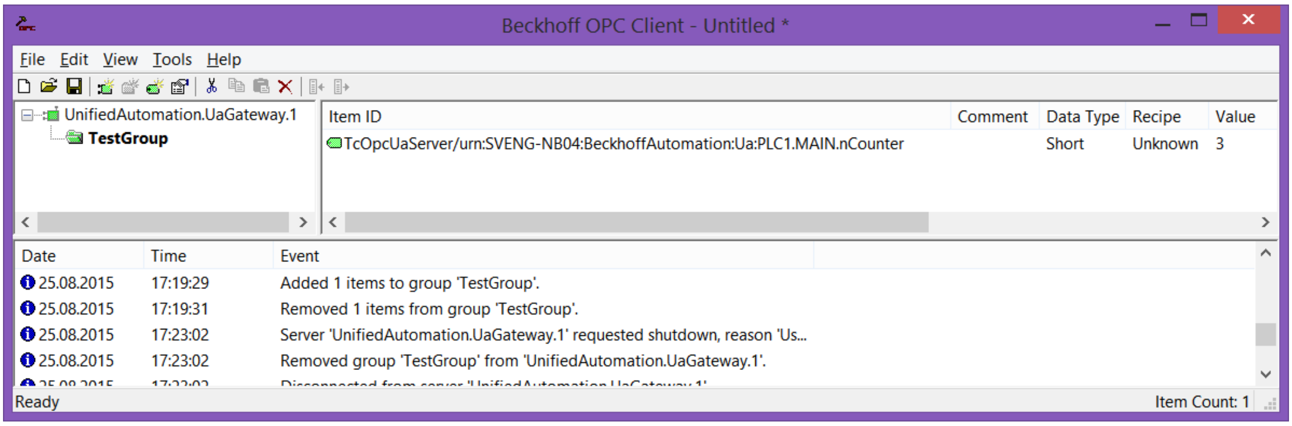
The standard configuration of the UA Gateway automatically establishes a connection with the local OPC UA Server and offers the OPC DA clients an OPC DA interface. For a connection based on this standard configuration, the OPC DA clients must take the following into account:

- The default ProgID of the UA Gateway is "UnifiedAutomation.Gateway.1". The TwinCAT OPC DA Server uses a different ProgID ("Beckhoff.TwinCATOpcServerDA").
- The UA Gateway always uses a ProgID instead of multiple clones.
- The ItemIdentifie of an OPC symbol is generated differently in the UA Gateway than in the TwinCAT OPC DA Server. This behavior can be changed to be more similar to that of the OPC DA server.

Changing the syntax of an ItemIdentifier

The syntax used by the UA Gateway for ItemIdentifier can be changed so that the latter corresponds more to the type of the TwinCAT OPC DA Server. By default, the UA Gateway uses a different syntax to that of the TwinCAT OPC DA Server when creating its identifiers.

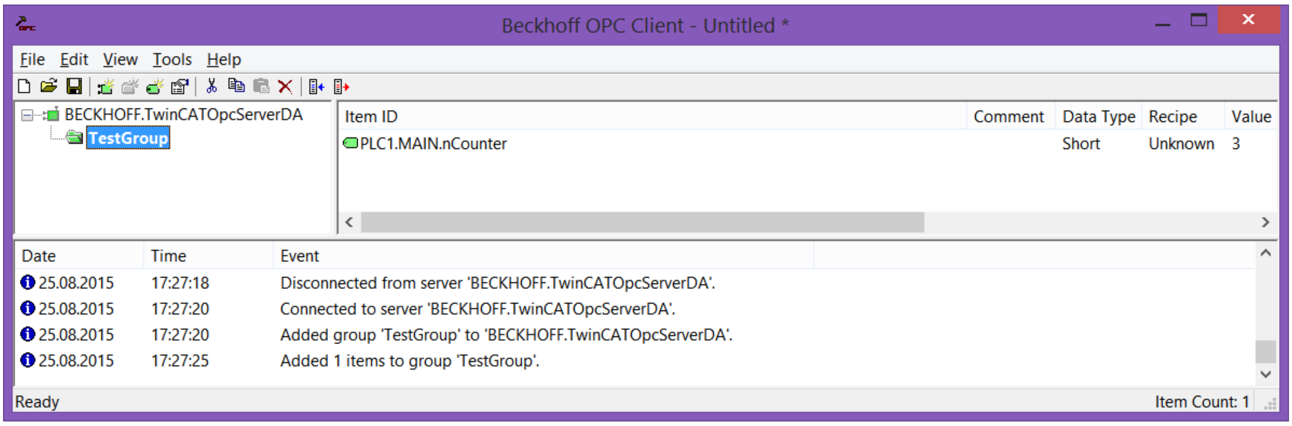
UA Gateway sample:


Beckhoff OPC Client - Untitled *
File Edit View Tools Help
UnifiedAutomation.UaGateway.1
TestGroup
Ready
Item Count: 1

Item ID	Comment	Data Type	Recipe	Value
TcOpcUaServer/urn:SVENG-NB04:BeckhoffAutomation:Ua:PLC1.MAIN.nCounter		Short	Unknown	3

Date	Time	Event
25.08.2015	17:19:29	Added 1 items to group 'TestGroup'.
25.08.2015	17:19:31	Removed 1 items from group 'TestGroup'.
25.08.2015	17:23:02	Server 'UnifiedAutomation.UaGateway.1' requested shutdown, reason 'Us...
25.08.2015	17:23:02	Removed group 'TestGroup' from 'UnifiedAutomation.UaGateway.1'.
25.08.2015	17:23:02	Disconnected from server 'UnifiedAutomation.UaGateway.1'.

Sample TwinCAT OPC DA Server:


Beckhoff OPC Client - Untitled *
File Edit View Tools Help
BECKHOFF.TwinCATOpcServerDA
TestGroup
Ready
Item Count: 1

Item ID	Comment	Data Type	Recipe	Value
PLC1.MAIN.nCounter		Short	Unknown	3

Date	Time	Event
25.08.2015	17:27:18	Disconnected from server 'BECKHOFF.TwinCATOpcServerDA'.
25.08.2015	17:27:20	Connected to server 'BECKHOFF.TwinCATOpcServerDA'.
25.08.2015	17:27:20	Added group 'TestGroup' to 'BECKHOFF.TwinCATOpcServerDA'.
25.08.2015	17:27:25	Added 1 items to group 'TestGroup'.

The UA Gateway uses a prefix so that the underlying OPC UA Client from which the variable originates can be clearly identified.

The following steps are required to configure the UA Gateway so that it forms its identifiers in approximately the same way as the TwinCAT OPC DA Server. The functionality has been implemented to simplify the migration process.

1. Open the UA Gateway configuration file *C:\Program Files (x86)\UnifiedAutomation\UaGateway\bin\uagateway.config.xml*
2. Look for the following XML tags in the XML file:

```
<OpcServerConfig>
  <ComDaServerConfig>
    <ComDaNamespaceUseAlias>false</ComDaNamespaceUseAlias>
  </ComDaServerConfig>
</OpcServerConfig>
```

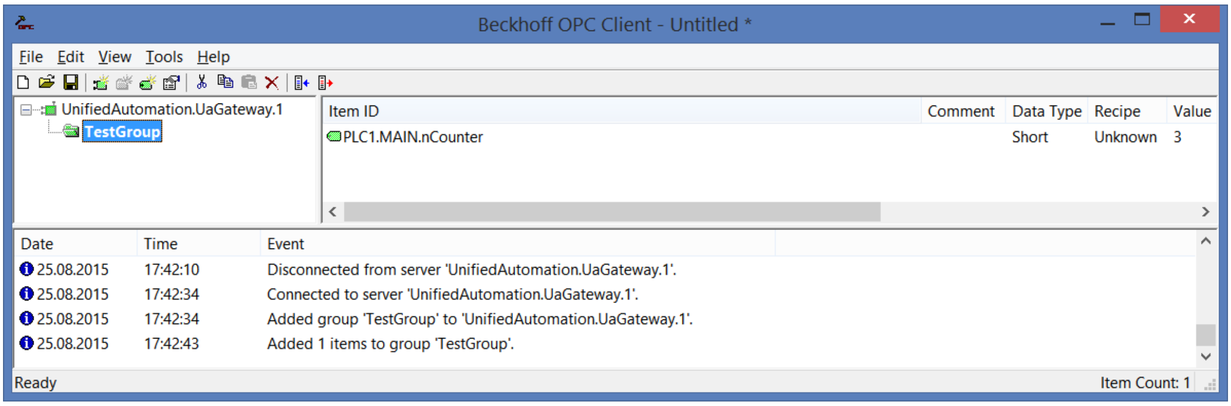
3. If the XML tag ComDaNamespaceUseAlias is set to "true", user-defined prefixes can be specified. To do this, look for the following XML tag in the same XML file:

```
<OpcServerConfig>
  <UaServerConfig>
    <ConfiguredNamespaces>
      ...
    </ConfiguredNamespaces>
  </UaServerConfig>
</OpcServerConfig>
```

4. In this XML structure, identify the TwinCAT OPC UA Server namespace. By default, it should read as follows:

```
<OpcServerConfig>
  <UaServerConfig>
    <ConfiguredNamespaces>
      ...
      <Namespace>
        <Index>...</Index>
        <Uri>TcOpcUaServer/urn:Hostname:BeckhoffAutomation:Ua:PLC1</Uri>
        <AllowRenameUri>false</AllowRenameUri>
        <UniqueId>TcOpcUaServer#TcOpcUaServer/urn:Hostname:BeckhoffAutomation:Ua:PLC1</UniqueId>
        <ComAlias>...</ComAlias>
      </Namespace>
      ...
    </ConfiguredNamespaces
  </UaServerConfig>
</OpcServerConfig>
```

5. On your computer, the placeholder "..." may look different. Set <ComAlias> to your preferred prefix, for example "PLC1". The identifiers are then created with the prefix "PLC1".


Beckhoff OPC Client - Untitled *
File
Edit
View
Tools
Help
UnifiedAutomation.UaGateway.1
TestGroup

Item ID	Comment	Data Type	Recipe	Value
PLC1.MAIN.nCounter		Short	Unknown	3

Date	Time	Event
25.08.2015	17:42:10	Disconnected from server 'UnifiedAutomation.UaGateway.1'.
25.08.2015	17:42:34	Connected to server 'UnifiedAutomation.UaGateway.1'.
25.08.2015	17:42:34	Added group 'TestGroup' to 'UnifiedAutomation.UaGateway.1'.
25.08.2015	17:42:43	Added 1 items to group 'TestGroup'.

Ready
Item Count: 1

4.9 Security

4.9.1 Overview

One of the reasons for the success of OPC UA as a communication technology is the integrated security mechanisms. Data communication based on OPC UA can be secured on two layers: transport and application layer. When connecting to the server, the client first selects an endpoint, which specifies the security functions to be used.

Endpoints

A server offers the client a list of different endpoints [▶ 27] to which the client can connect. An endpoint describes, among other things, which security functions (e.g. Message Security mode, Security Policy and available Identity Tokens) the communication connection via this endpoint should fulfill. For example, an endpoint may require signing and encryption of data packets (transport layer), as well as additional authentication of the client based on user name/password (application layer).

Transport layer

A communication connection based on OPC UA can be secured at the transport layer. This is done through the use of client/server certificates and a mutual trust relationship between client and server application. Here, the client must trust the server certificate and vice versa in order for a communication connection to be established. This requires a mutual certificate exchange [▶ 29].

Application layer

In addition to the transport layer, a communication connection can also be secured at the application layer. For this purpose, various authentication mechanisms [▶ 30] are available, which are offered by the server endpoint.

4.9.2 Endpoints

The TwinCAT OPC UA Gateway provides various endpoints for OPC UA clients via the standard port 48050/tcp. The endpoints define the connection type between client and server and whether it should be secured or unsecured.

Relationship of trust

Please note that in order to use the secure endpoints, a trust relationship must be established between server and client, which is usually done via their certificates. The configuration of such a trust relationship on the gateway side is explained here [▸ 29].

Deprecated endpoints

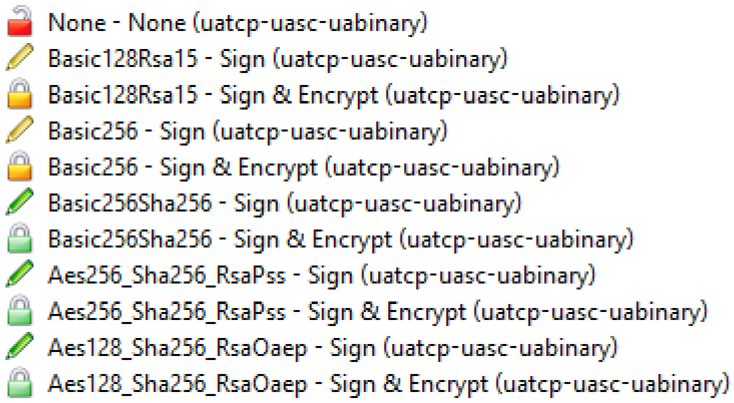
Please note that the security profiles currently available in the endpoints may be classified as potentially insecure over time and will be replaced by newer ones. In this case, an update of the TwinCAT OPC UA Gateway is recommended. A configuration switch can be used to reactivate security policies that are deprecated and classified as insecure. However, we recommend leaving this configuration switch disabled for security reasons.

List of endpoints

The following list summarizes the endpoints of the TwinCAT OPC UA Gateway. This includes endpoints that have already been discontinued. By default, the TwinCAT OPC UA Gateway only offers endpoints that are currently considered secure.

Security profile	Security mode	Short description
None	None	No encryption or signing of messages is carried out at this endpoint. Authentication [▸ 30], on the other hand, is possible.
Basic128Rsa15 (deprecated)	Sign / Sign & Encrypt	This endpoint has been classified as deprecated from a security perspective and is disabled by default. If necessary, the endpoint can be enabled again.
Basic256 (deprecated)	Sign / Sign & Encrypt	This endpoint has been classified as deprecated from a security perspective and is disabled by default. If necessary, the endpoint can be enabled again.
Basic256Sha256	Sign / Sign & Encrypt	Endpoint currently present in the server for secure signing and encryption. Additional authentication [▸ 30] is possible.
Aes256_Sha256_RsaPss	Sign / Sign & Encrypt	Endpoint currently present in the server for secure signing and encryption. Additional authentication [▸ 30] is possible.
Aes256_Sha256_RsaOaep	Sign / Sign & Encrypt	Endpoint currently present in the server for secure signing and encryption. Additional authentication [▸ 30] is possible.

All endpoints in the list can be enabled or disabled via the gateway configuration. In the following figure, all endpoints are enabled.



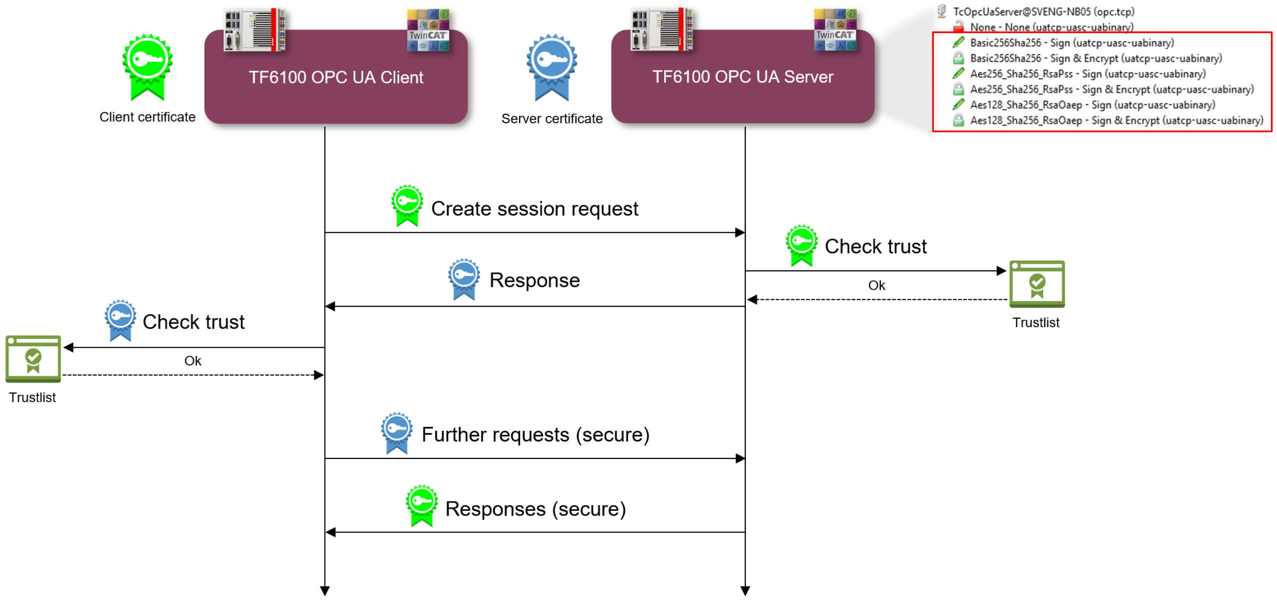
None - None (uatcp-uasc-uabinary)
Basic128Rsa15 - Sign (uatcp-uasc-uabinary)
Basic128Rsa15 - Sign & Encrypt (uatcp-uasc-uabinary)
Basic256 - Sign (uatcp-uasc-uabinary)
Basic256 - Sign & Encrypt (uatcp-uasc-uabinary)
Basic256Sha256 - Sign (uatcp-uasc-uabinary)
Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary)
Aes256_Sha256_RsaPss - Sign (uatcp-uasc-uabinary)
Aes256_Sha256_RsaPss - Sign & Encrypt (uatcp-uasc-uabinary)
Aes128_Sha256_RsaOaep - Sign (uatcp-uasc-uabinary)
Aes128_Sha256_RsaOaep - Sign & Encrypt (uatcp-uasc-uabinary)

4.9.3 Certificate exchange

To secure the communication connection at transport layer via a secure endpoint [▶ 27], it is necessary to establish a mutual trust between client and server. By default, the TwinCAT OPC UA Gateway generates a machine-specific, self-signed key pair consisting of a public and a private key when it is started for the first time. However, you can also use any certificate authority or technology for integration into your IT infrastructure, e.g. Active Directory or OpenSSL. For easy administration and secure access to certificates, it makes sense to set up a Global Discovery Server.

To establish a trust relationship between any OPC UA client and the TwinCAT OPC UA Gateway, you need the public key of the client certificate. The gateway must trust this server accordingly. The gateway manages the trust settings for client certificates in a subdirectory of the application directory.

The following diagram illustrates the relationship between the client and server certificate when establishing a secure communication connection using the example of TwinCAT OPC UA Client and TwinCAT OPC UA Server. In the case of the latter, however, this can also be transferred 1:1 to the gateway.


Client certificate
TF6100 OPC UA Client
Server certificate
TF6100 OPC UA Server
TcOpcUaServer@SVENG-NB05 (opc.tcp)
None - None (uatcp-uasc-uabinary)
Basic256Sha256 - Sign (uatcp-uasc-uabinary)
Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary)
Aes256_Sha256_RsaPss - Sign (uatcp-uasc-uabinary)
Aes256_Sha256_RsaPss - Sign & Encrypt (uatcp-uasc-uabinary)
Aes128_Sha256_RsaOaep - Sign (uatcp-uasc-uabinary)
Aes128_Sha256_RsaOaep - Sign & Encrypt (uatcp-uasc-uabinary)
Create session request
Check trust
Ok
Trustlist
Response
Check trust
Ok
Trustlist
Further requests (secure)
Responses (secure)

The client transmits its public key with the CreateSession Request. The server then has the option of checking the trust relationship. If the server trusts the client, it transmits its own public key in its response. The client therefore also has the option of checking the trust relationship with the server.

If mutual trust is ensured, the communication connection is initiated. The server's public key is then used to encrypt a request from the client to the server. The response from the server to the client is then encrypted with the client's public key. Both communication participants then have the option of decrypting the received message with their private key.

Messages are signed in reverse: a message is signed with the sender's private key. Since the recipient recognizes the sender's public key, the signature can be verified.

Configure trust relationship via file system

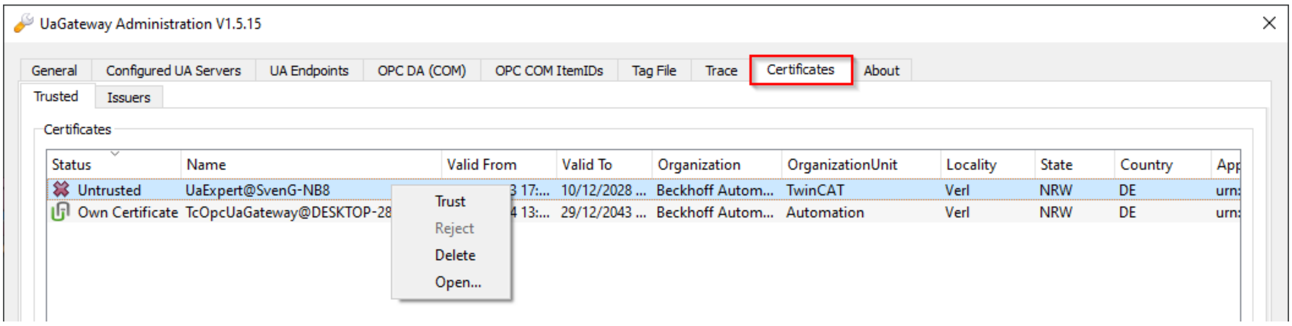
By moving client certificates between the trusted/rejected directories, the trust settings can be adjusted accordingly. The public key of a client certificate is automatically stored in the directory for rejected certificates the first time the client attempts to connect to a secure endpoint. By subsequently moving the public key to the directory for trusted certificates, the client is trusted at the next connection attempt and can connect.

Accept all certificates

If this option is enabled in the configuration of the endpoints [▶ 23] of the gateway, the gateway automatically trusts all client certificates. In this case, they will not be listed in any of the above directories.

Configure the trust relationship using the configurator

You can also make the trust settings via Configurator. The configurator includes a graphical user interface for configuring the trust settings. You can trust or reject a certificate via the context menu.



Status	Name	Valid From	Valid To	Organization	OrganizationUnit	Locality	State	Country	App
Untrusted	UaExpert@SvenG-NB8	3 17:...	10/12/2028 ...	Beckhoff Autom...	TwinCAT	Verl	NRW	DE	urn:
Own Certificate	TcOpcUaGateway@DESKTOP-28	4 13:...	29/12/2043 ...	Beckhoff Autom...	Automation	Verl	NRW	DE	urn:

4.9.4 Authentication

An OPC UA client can authenticate itself to the TwinCAT OPC UA Gateway using various logon methods. The following "IdentityTokens" are supported:

- Anonymous
- User name/Password
- User certificate

Delivery state

The IdentityToken "Anonymous" is enabled when the gateway is delivered. We recommend configuring a user or user group for access to the server after initial commissioning. For more information, see Recommended steps [▶ 17].

Anonymous

This type of authentication allows any OPC UA client to establish a connection to the gateway. It is not necessary to specify a user identity. We recommend disabling this authentication method after commissioning the gateway. This can be done via the configurator.

User name/Password

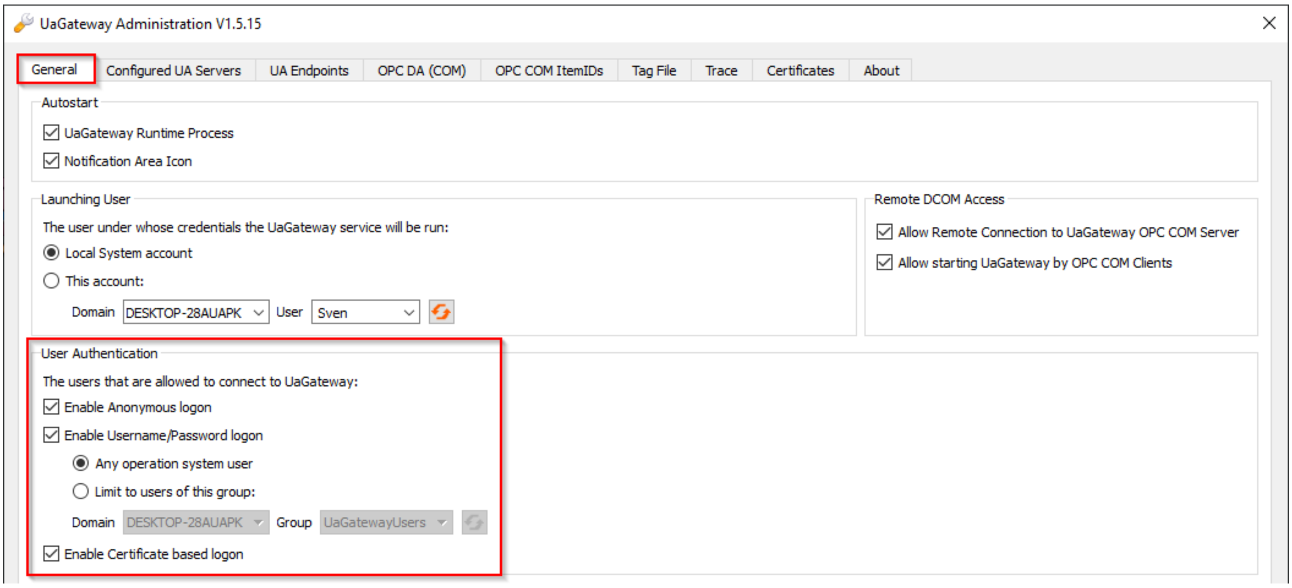
This authentication method uses a user name/password combination to authenticate the client on the OPC UA server of the gateway. The user or user group is created and managed in the operating system.

User certificate

This type of authentication uses a certificate to authenticate to the OPC UA server of the gateway. The handling of user certificates on the gateway side is identical to the use of certificates at transport layer, i.e. the gateway must trust the (user) certificate before the client can successfully authenticate itself to the gateway with the certificate. A separate application directory [▶ 20] ("pkiuser") for managing the user certificates is available in the gateway for this purpose.

Configuration

The individual authentication methods are usually enabled/disabled via the configurator.



Autostart

☑ UaGateway Runtime Process

☑ Notification Area Icon

Launching User

The user under whose credentials the UaGateway service will be run:

● Local System account

○ This account:

Domain DESKTOP-28AUAPK User Sven

Remote DCOM Access

☑ Allow Remote Connection to UaGateway OPC COM Server

☑ Allow starting UaGateway by OPC COM Clients

User Authentication

The users that are allowed to connect to UaGateway:

☑ Enable Anonymous logon

☑ Enable Username/Password logon

● Any operation system user

○ Limit to users of this group:

Domain DESKTOP-28AUAPK Group UaGatewayUsers

☑ Enable Certificate based logon

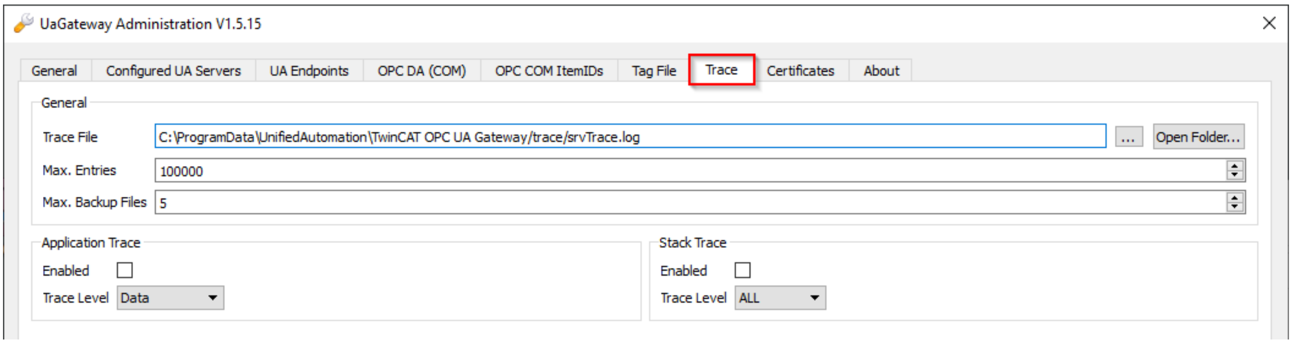
4.10 Logging

You can enable a log file in the gateway for extended diagnostics, in which various information is then recorded on the basis of different log levels.

Influence of logging on the operating behavior

Please note that activating the log file can have a negative impact on the speed and operating behavior of the TwinCAT OPC UA Gateway.

The default path for the created log files is described in more detail in the chapter Application directories [▶ 20] and can also be viewed in the TwinCAT OPC UA Gateway configurator.



General

Trace File C:\ProgramData\UnifiedAutomation\TwinCAT OPC UA Gateway/trace/srvTrace.log

Max. Entries 100000

Max. Backup Files 5

Application Trace

Enabled □

Trace Level Data

Stack Trace

Enabled □

Trace Level ALL

5 Appendix

5.1 Error diagnosis

Behavior	Notes
The gateway cannot connect to the server.	One of the possible causes is that an old configuration is being used. For example, if there is a new server certificate, the gateway only notices this when the configured endpoint is deleted and reinserted under a different name. With the same endpoint or a new endpoint with the same name, the gateway would use the connection information from a cache and as a result would no longer be able to connect to the server.

5.2 ADS Return Codes

Grouping of error codes:
Global error codes: ADS Return Codes [▶ 32]... (0x9811_0000 ...)
Router error codes: ADS Return Codes [▶ 33]... (0x9811_0500 ...)
General ADS errors: ADS Return Codes [▶ 33]... (0x9811_0700 ...)
RTime error codes: ADS Return Codes [▶ 35]... (0x9811_1000 ...)

Global error codes

Hex	Dec	HRESULT	Name	Description
0x0	0	0x98110000	ERR_NOERROR	No error.
0x1	1	0x98110001	ERR_INTERNAL	Internal error.
0x2	2	0x98110002	ERR_NORTIME	No real time.
0x3	3	0x98110003	ERR_ALLOCLOCKEDMEM	Allocation locked – memory error.
0x4	4	0x98110004	ERR_INSERTMAILBOX	Mailbox full – the ADS message could not be sent. Reducing the number of ADS messages per cycle will help.
0x5	5	0x98110005	ERR_WRONGRECEIVEHMSG	Wrong HMSG.
0x6	6	0x98110006	ERR_TARGETPORTNOTFOUND	Target port not found – ADS server is not started or is not reachable.
0x7	7	0x98110007	ERR_TARGETMACHINENOTFOUND	Target computer not found – AMS route was not found.
0x8	8	0x98110008	ERR_UNKNOWNCMDID	Unknown command ID.
0x9	9	0x98110009	ERR_BADTASKID	Invalid task ID.
0xA	10	0x9811000A	ERR_NOIO	No IO.
0xB	11	0x9811000B	ERR_UNKNOWNAMSCMD	Unknown AMS command.
0xC	12	0x9811000C	ERR_WIN32ERROR	Win32 error.
0xD	13	0x9811000D	ERR_PORTNOTCONNECTED	Port not connected.
0xE	14	0x9811000E	ERR_INVALIDAMSLENGTH	Invalid AMS length.
0xF	15	0x9811000F	ERR_INVALIDAMSNETID	Invalid AMS Net ID.
0x10	16	0x98110010	ERR_LOWINSTLEVEL	Installation level is too low –TwinCAT 2 license error.
0x11	17	0x98110011	ERR_NODEBUGINTAVAILABLE	No debugging available.
0x12	18	0x98110012	ERR_PORTDISABLED	Port disabled – TwinCAT system service not started.
0x13	19	0x98110013	ERR_PORTALREADYCONNECTED	Port already connected.
0x14	20	0x98110014	ERR_AMSSYNC_W32ERROR	AMS Sync Win32 error.
0x15	21	0x98110015	ERR_AMSSYNC_TIMEOUT	AMS Sync Timeout.
0x16	22	0x98110016	ERR_AMSSYNC_AMSERROR	AMS Sync error.
0x17	23	0x98110017	ERR_AMSSYNC_NOINDEXINMAP	No index map for AMS Sync available.
0x18	24	0x98110018	ERR_INVALIDAMSPORT	Invalid AMS port.
0x19	25	0x98110019	ERR_NOMEMORY	No memory.
0x1A	26	0x9811001A	ERR_TCPSEND	TCP send error.
0x1B	27	0x9811001B	ERR_HOSTUNREACHABLE	Host unreachable.
0x1C	28	0x9811001C	ERR_INVALIDAMSFRAGMENT	Invalid AMS fragment.
0x1D	29	0x9811001D	ERR_TLSSEND	TLS send error – secure ADS connection failed.
0x1E	30	0x9811001E	ERR_ACCESSDENIED	Access denied – secure ADS access denied.

Router error codes

Hex	Dec	HRESULT	Name	Description
0x500	1280	0x98110500	ROUTERERR_NOLOCKEDMEMORY	Locked memory cannot be allocated.
0x501	1281	0x98110501	ROUTERERR_RESIZEMEMORY	The router memory size could not be changed.
0x502	1282	0x98110502	ROUTERERR_MAILBOXFULL	The mailbox has reached the maximum number of possible messages.
0x503	1283	0x98110503	ROUTERERR_DEBUGBOXFULL	The Debug mailbox has reached the maximum number of possible messages.
0x504	1284	0x98110504	ROUTERERR_UNKNOWNPORTTYPE	The port type is unknown.
0x505	1285	0x98110505	ROUTERERR_NOTINITIALIZED	The router is not initialized.
0x506	1286	0x98110506	ROUTERERR_PORTALREADYINUSE	The port number is already assigned.
0x507	1287	0x98110507	ROUTERERR_NOTREGISTERED	The port is not registered.
0x508	1288	0x98110508	ROUTERERR_NOMOREQUEUES	The maximum number of ports has been reached.
0x509	1289	0x98110509	ROUTERERR_INVALIDPORT	The port is invalid.
0x50A	1290	0x9811050A	ROUTERERR_NOTACTIVATED	The router is not active.
0x50B	1291	0x9811050B	ROUTERERR_FRAGMENTBOXFULL	The mailbox has reached the maximum number for fragmented messages.
0x50C	1292	0x9811050C	ROUTERERR_FRAGMENTTIMEOUT	A fragment timeout has occurred.
0x50D	1293	0x9811050D	ROUTERERR_TOBEREMOVED	The port is removed.

General ADS error codes

Hex	Dec	HRESULT	Name	Description
0x700	1792	0x98110700	ADSERR_DEVICE_ERROR	General device error.
0x701	1793	0x98110701	ADSERR_DEVICE_SRVNOTSUPP	Service is not supported by the server.
0x702	1794	0x98110702	ADSERR_DEVICE_INVALIDGRP	Invalid index group.
0x703	1795	0x98110703	ADSERR_DEVICE_INVALIDOFFSET	Invalid index offset.
0x704	1796	0x98110704	ADSERR_DEVICE_INVALIDACCESS	Reading or writing not permitted.
0x705	1797	0x98110705	ADSERR_DEVICE_INVALIDSIZE	Parameter size not correct.
0x706	1798	0x98110706	ADSERR_DEVICE_INVALIDDATA	Invalid data values.
0x707	1799	0x98110707	ADSERR_DEVICE_NOTREADY	Device is not ready to operate.
0x708	1800	0x98110708	ADSERR_DEVICE_BUSY	Device is busy.
0x709	1801	0x98110709	ADSERR_DEVICE_INVALIDCONTEXT	Invalid operating system context. This can result from use of ADS blocks in different tasks. It may be possible to resolve this through multitasking synchronization in the PLC.
0x70A	1802	0x9811070A	ADSERR_DEVICE_NOMEMORY	Insufficient memory.
0x70B	1803	0x9811070B	ADSERR_DEVICE_INVALIDPARM	Invalid parameter values.
0x70C	1804	0x9811070C	ADSERR_DEVICE_NOTFOUND	Not found (files, ...).
0x70D	1805	0x9811070D	ADSERR_DEVICE_SYNTAX	Syntax error in file or command.
0x70E	1806	0x9811070E	ADSERR_DEVICE_INCOMPATIBLE	Objects do not match.
0x70F	1807	0x9811070F	ADSERR_DEVICE_EXISTS	Object already exists.
0x710	1808	0x98110710	ADSERR_DEVICE_SYMBOLNOTFOUND	Symbol not found.
0x711	1809	0x98110711	ADSERR_DEVICE_SYMBOLVERSIONINVALID	Invalid symbol version. This can occur due to an online change. Create a new handle.
0x712	1810	0x98110712	ADSERR_DEVICE_INVALIDSTATE	Device (server) is in invalid state.
0x713	1811	0x98110713	ADSERR_DEVICE_TRANSMODENOTSUPP	AdsTransMode not supported.
0x714	1812	0x98110714	ADSERR_DEVICE_NOTIFYHNDINVALID	Notification handle is invalid.
0x715	1813	0x98110715	ADSERR_DEVICE_CLIENTUNKNOWN	Notification client not registered.
0x716	1814	0x98110716	ADSERR_DEVICE_NOMOREHDLS	No further handle available.
0x717	1815	0x98110717	ADSERR_DEVICE_INVALIDWATCHSIZE	Notification size too large.
0x718	1816	0x98110718	ADSERR_DEVICE_NOTINIT	Device not initialized.
0x719	1817	0x98110719	ADSERR_DEVICE_TIMEOUT	Device has a timeout.
0x71A	1818	0x9811071A	ADSERR_DEVICE_NOINTERFACE	Interface query failed.
0x71B	1819	0x9811071B	ADSERR_DEVICE_INVALIDINTERFACE	Wrong interface requested.
0x71C	1820	0x9811071C	ADSERR_DEVICE_INVALIDCLSID	Class ID is invalid.
0x71D	1821	0x9811071D	ADSERR_DEVICE_INVALIDOBJID	Object ID is invalid.
0x71E	1822	0x9811071E	ADSERR_DEVICE_PENDING	Request pending.
0x71F	1823	0x9811071F	ADSERR_DEVICE_ABORTED	Request is aborted.
0x720	1824	0x98110720	ADSERR_DEVICE_WARNING	Signal warning.
0x721	1825	0x98110721	ADSERR_DEVICE_INVALIDARRAYIDX	Invalid array index.
0x722	1826	0x98110722	ADSERR_DEVICE_SYMBOLNOTACTIVE	Symbol not active.
0x723	1827	0x98110723	ADSERR_DEVICE_ACCESSDENIED	Access denied.
0x724	1828	0x98110724	ADSERR_DEVICE_LICENSENOTFOUND	Missing license.
0x725	1829	0x98110725	ADSERR_DEVICE_LICENSEEXPIRED	License expired.
0x726	1830	0x98110726	ADSERR_DEVICE_LICENSEEXCEEDED	License exceeded.
0x727	1831	0x98110727	ADSERR_DEVICE_LICENSEINVALID	Invalid license.
0x728	1832	0x98110728	ADSERR_DEVICE_LICENSESYSTEMID	License problem: System ID is invalid.
0x729	1833	0x98110729	ADSERR_DEVICE_LICENSENOTIMELIMIT	License not limited in time.
0x72A	1834	0x9811072A	ADSERR_DEVICE_LICENSEFUTUREISSUE	Licensing problem: time in the future.
0x72B	1835	0x9811072B	ADSERR_DEVICE_LICENSETIMETOLONG	License period too long.
0x72C	1836	0x9811072C	ADSERR_DEVICE_EXCEPTION	Exception at system startup.
0x72D	1837	0x9811072D	ADSERR_DEVICE_LICENSEDUPLICATED	License file read twice.
0x72E	1838	0x9811072E	ADSERR_DEVICE_SIGNATUREINVALID	Invalid signature.
0x72F	1839	0x9811072F	ADSERR_DEVICE_CERTIFICATEINVALID	Invalid certificate.
0x730	1840	0x98110730	ADSERR_DEVICE_LICENSEOEMNOTFOUND	Public key not known from OEM.
0x731	1841	0x98110731	ADSERR_DEVICE_LICENSERESTRICTED	License not valid for this system ID.
0x732	1842	0x98110732	ADSERR_DEVICE_LICENSEDEMODENIED	Demo license prohibited.
0x733	1843	0x98110733	ADSERR_DEVICE_INVALIDFNCID	Invalid function ID.
0x734	1844	0x98110734	ADSERR_DEVICE_OUTOFRANGE	Outside the valid range.
0x735	1845	0x98110735	ADSERR_DEVICE_INVALIDALIGNMENT	Invalid alignment.
0x736	1846	0x98110736	ADSERR_DEVICE_LICENSEPLATFORM	Invalid platform level.

Hex	Dec	HRESULT	Name	Description
0x737	1847	0x98110737	ADSERR_DEVICE_FORWARD_PL	Context – forward to passive level.
0x738	1848	0x98110738	ADSERR_DEVICE_FORWARD_DL	Context – forward to dispatch level.
0x739	1849	0x98110739	ADSERR_DEVICE_FORWARD_RT	Context – forward to real time.
0x740	1856	0x98110740	ADSERR_CLIENT_ERROR	Client error.
0x741	1857	0x98110741	ADSERR_CLIENT_INVALIDPARM	Service contains an invalid parameter.
0x742	1858	0x98110742	ADSERR_CLIENT_LISTEMPTY	Polling list is empty.
0x743	1859	0x98110743	ADSERR_CLIENT_VARUSED	Var connection already in use.
0x744	1860	0x98110744	ADSERR_CLIENT_DUPLINVOKEID	The called ID is already in use.
0x745	1861	0x98110745	ADSERR_CLIENT_SYNCTIMEOUT	Timeout has occurred – the remote terminal is not responding in the specified ADS timeout. The route setting of the remote terminal may be configured incorrectly.
0x746	1862	0x98110746	ADSERR_CLIENT_W32ERROR	Error in Win32 subsystem.
0x747	1863	0x98110747	ADSERR_CLIENT_TIMEOUTINVALID	Invalid client timeout value.
0x748	1864	0x98110748	ADSERR_CLIENT_PORTNOTOPEN	Port not open.
0x749	1865	0x98110749	ADSERR_CLIENT_NOAMSADDR	No AMS address.
0x750	1872	0x98110750	ADSERR_CLIENT_SYNCINTERNAL	Internal error in Ads sync.
0x751	1873	0x98110751	ADSERR_CLIENT_ADDHASH	Hash table overflow.
0x752	1874	0x98110752	ADSERR_CLIENT_REMOVEHASH	Key not found in the table.
0x753	1875	0x98110753	ADSERR_CLIENT_NOMORESYM	No symbols in the cache.
0x754	1876	0x98110754	ADSERR_CLIENT_SYNCRESINVALID	Invalid response received.
0x755	1877	0x98110755	ADSERR_CLIENT_SYNCPORTLOCKED	Sync Port is locked.
0x756	1878	0x98110756	ADSERR_CLIENT_REQUESTCANCELLED	The request was cancelled.

RTime error codes

Hex	Dec	HRESULT	Name	Description
0x1000	4096	0x98111000	RTERR_INTERNAL	Internal error in the real-time system.
0x1001	4097	0x98111001	RTERR_BADTIMERPERIODS	Timer value is not valid.
0x1002	4098	0x98111002	RTERR_INVALIDTASKPTR	Task pointer has the invalid value 0 (zero).
0x1003	4099	0x98111003	RTERR_INVALIDSTACKPTR	Stack pointer has the invalid value 0 (zero).
0x1004	4100	0x98111004	RTERR_PRIOEXISTS	The request task priority is already assigned.
0x1005	4101	0x98111005	RTERR_NOMORETCB	No free TCB (Task Control Block) available. The maximum number of TCBs is 64.
0x1006	4102	0x98111006	RTERR_NOMORESEMAS	No free semaphores available. The maximum number of semaphores is 64.
0x1007	4103	0x98111007	RTERR_NOMOREQUEUES	No free space available in the queue. The maximum number of positions in the queue is 64.
0x100D	4109	0x9811100D	RTERR_EXTIRQALREADYDEF	An external synchronization interrupt is already applied.
0x100E	4110	0x9811100E	RTERR_EXTIRQNOTDEF	No external sync interrupt applied.
0x100F	4111	0x9811100F	RTERR_EXTIRQINSTALLFAILED	Application of the external synchronization interrupt has failed.
0x1010	4112	0x98111010	RTERR_IRQLNOTLESSOREQUAL	Call of a service function in the wrong context
0x1017	4119	0x98111017	RTERR_VMXNOTSUPPORTED	Intel VT-x extension is not supported.
0x1018	4120	0x98111018	RTERR_VMXDISABLED	Intel VT-x extension is not enabled in the BIOS.
0x1019	4121	0x98111019	RTERR_VMXCONTROLSMISSING	Missing function in Intel VT-x extension.
0x101A	4122	0x9811101A	RTERR_VMXENABLEFAILS	Activation of Intel VT-x fails.

Specific positive HRESULT Return Codes:

HRESULT	Name	Description
0x0000_0000	S_OK	No error.
0x0000_0001	S_FALSE	No error. Example: successful processing, but with a negative or incomplete result.
0x0000_0203	S_PENDING	No error. Example: successful processing, but no result is available yet.
0x0000_0256	S_WATCHDOG_TIMEOUT	No error. Example: successful processing, but a timeout occurred.

TCP Winsock error codes

Hex	Dec	Name	Description
0x274C	10060	WSAETIMEDOUT	A connection timeout has occurred - error while establishing the connection, because the remote terminal did not respond properly after a certain period of time, or the established connection could not be maintained because the connected host did not respond.
0x274D	10061	WSAECONNREFUSED	Connection refused - no connection could be established because the target computer has explicitly rejected it. This error usually results from an attempt to connect to a service that is inactive on the external host, that is, a service for which no server application is running.
0x2751	10065	WSAEHOSTUNREACH	No route to host - a socket operation referred to an unavailable host.
More Winsock error codes: Win32 error codes			

5.3 Support and Service

Beckhoff and their partners around the world offer comprehensive support and service, making available fast and competent assistance with all questions related to Beckhoff products and system solutions.

Download finder

Our download finder contains all the files that we offer you for downloading. You will find application reports, technical documentation, technical drawings, configuration files and much more.

The downloads are available in various formats.

Beckhoff's branch offices and representatives

Please contact your Beckhoff branch office or representative for local support and service on Beckhoff products!

The addresses of Beckhoff's branch offices and representatives round the world can be found on our internet page: www.beckhoff.com

You will also find further documentation for Beckhoff components there.

Beckhoff Support

Support offers you comprehensive technical assistance, helping you not only with the application of individual Beckhoff products, but also with other, wide-ranging services:

- support
- design, programming and commissioning of complex automation systems
- and extensive training program for Beckhoff system components

Hotline:	+49 5246 963-157
e-mail:	support@beckhoff.com

Beckhoff Service

The Beckhoff Service Center supports you in all matters of after-sales service:

- on-site service
- repair service
- spare parts service
- hotline service

Hotline:	+49 5246 963-460
e-mail:	service@beckhoff.com

Beckhoff Headquarters

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20
33415 Verl
Germany

Phone:	+49 5246 963-0
e-mail:	info@beckhoff.com
web:	www.beckhoff.com

More Information:
www.beckhoff.com/TF6100

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