BECKHOFF New Automation Technology

Manual | EN TS6100 TwinCAT 2 | OPC UA Configurator



Table of contents

1	Fore	word		5
	1.1	Notes or	n the documentation	5
	1.2	For your	safety	5
	1.3	Notes or	n information security	7
2	Over	view		8
3	Insta	llation		10
	3.1		requirements	
	3.2		on	
4	Tech	nical intr	oduction	12
	4.1		art	
	4.2	Applicati	on directories	18
	4.3	Visual S	tudio	19
		4.3.1	Overview	19
		4.3.2	Creating a new project	19
		4.3.3	Connecting to a server	20
		4.3.4	Performing the server initialization	22
		4.3.5	Adding ADS devices	23
		4.3.6	Reading and writing the configuration	25
		4.3.7	Importing and exporting configuration files	27
		4.3.8	Configuring historical access	28
		4.3.9	Configuring Alarms and Conditions	29
		4.3.10	Configuring alarm texts	32
		4.3.11	Configuring endpoints	34
		4.3.12	Trust relationship for certificates	34
		4.3.13	Configuring security settings	35
		4.3.14	Restarting the server	43
		4.3.15	Logging	43
	4.4	Standalo	one	45
		4.4.1	Overview	45
		4.4.2	Connecting to a server	45
		4.4.3	Performing the server initialization	46
		4.4.4	Adding ADS devices	
		4.4.5	Reading and writing the configuration	
		4.4.6	Configuring historical access	
		4.4.7	Configuring Alarms and Conditions	
		4.4.8	Configuring alarm texts	
		4.4.9	Configuring endpoints	
		4.4.10	Trust relationship for certificates	
		4.4.11	Configuring security settings	
		4.4.12	Restarting the server	
		4.4.13	Logging	58
5	Арре			
	5.1	ADS Ret	turn Codes	60

BECKHOFF

5.2 \$	Support and Service	64
--------	---------------------	----

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.

Ether**CAT**

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

Copyright

© Beckhoff Automation GmbH & Co. KG, Germany.

The distribution and reproduction of this document as well as the use and communication of its contents without express authorization are prohibited.

Offenders will be held liable for the payment of damages. All rights reserved in the event that a patent, utility model, or design are registered.

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

Hazard with high risk of death or serious injury.					
Hazard with medium risk of death or serious injury.					
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 <u>https://www.beckhoff.com/secguide</u>.

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 <u>https://www.beckhoff.com/secinfo</u>.

2 Overview

OPC Unified **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.

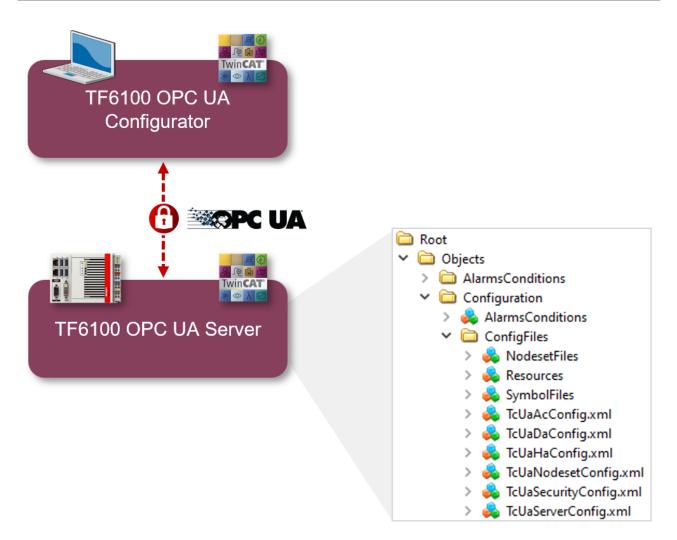
The TwinCAT 3 Function TF6100 OPC UA consists of several software components that enable data exchange with TwinCAT based on OPC UA.

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 Configurator, which is an engineering software component that provides a graphical user interface for configuring the TwinCAT OPC UA Server. The TwinCAT OPC UA Configurator is delivered in two variants: an interface integrated into Visual Studio (or the TwinCAT XAE Shell) and a standalone tool. Both variants have the characteristic that you establish an OPC UA communication connection to a TwinCAT OPC UA Server and configure the server via this connection. The basis for this is the so-called configuration namespace of the TwinCAT OPC UA Server, which provides all relevant configuration files for authenticated users via OPC UA.

BECKHOFF



For a quick introduction to the product, we recommend our chapters <u>Installation [\blacktriangleright 10]</u> and <u>Quick Start</u> [\blacktriangleright 12]. Please also note the <u>system requirements [\blacktriangleright 10]</u> for this product.

3 Installation

3.1 System requirements

The following system requirements apply to the installation and operation of this product. A distinction must be made between the Standalone Configurator and Visual Studio Configurator.

Visual Studio Configurator

Technical data	Description
Operating system	Windows 10 (>=21H2)
	Windows Server 2022
Target platforms	PC architecture (x86, x64)
.NET Framework	4.8.1
TwinCAT installation level	TwinCAT 3 XAE
Required TwinCAT license	

Standalone Configurator

Technical data	Description
Operating system	Windows 10 (>=21H2)
	Windows Server 2022
Target platforms	PC architecture (x86, x64)
.NET Framework	4.8.1
TwinCAT installation level	TwinCAT 2 CP, PLC, NC-PTP
	TwinCAT 3 XAE, XAR, ADS
Required TwinCAT license	

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 <u>Installation documentation</u>.

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 Command Line Interface (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 Interface (UI) to display all available workloads and install them if required. To do this, follow the corresponding instructions in the interface.

NOTICE

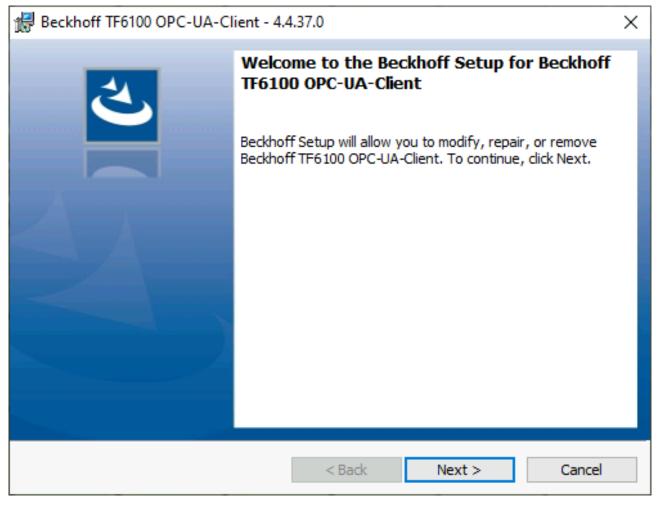
Unprepared TwinCAT restart can cause data loss

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 <u>https://www.beckhoff.com/download</u>.

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.



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.

4 Technical introduction

4.1 Quick start

The following chapter provides a quick introduction to the TwinCAT OPC UA Configurator. In these instructions, the Standalone Configurator is used to establish a connection with the locally installed TwinCAT OPC UA Server and to configure it. This requires both products to be installed - on the same system in this example.

The following steps are described in more detail below:

- Starting the Standalone Configurator
- · Configuring a server connection
- Connecting to the server and reading the configuration
- · Making changes to the configuration
- · Activating the new configuration on the server

Starting the Standalone Configurator

The TwinCAT OPC UA Configurator is installed by default in a subdirectory of the TwinCAT installation directory. Further information can be found in the documentation chapter on the <u>application directories</u> $[\blacktriangleright 18]$.

When the product is installed, a shortcut is created in the Windows Start menu, which enables easy access to the application.

After starting the application, you must first configure a new server connection. In the next step, you will learn how to do this.

TwinCAT OPC UA Configurator				_		×
File Server						
🗋 📂 🛃 📂 🔐 💷 💷	∼ Edi	t Connect Disconnect	Connection state:			
Data Access Historical Access Alarms & Conditions	Security Server Settings (Online Panel				
Settings						
Devices						
Name	AmsNetId	AdsPort	Туре		Disabled	
Date/Time Message						
Logging Target Browser						

Configuring a server connection

1. Open the server selection dialog by clicking on the **Edit** button in the toolbar. Enter the server URL of the TwinCAT OPC UA Server to be configured in the dialog that opens. In this example, the server is installed on the same system and we can use the default address (opc.tcp://localhost:4840). Click on the

Get Endpoints button to obtain a list of all server endpoints. Select the endpoint "Basic256Sha256 - SignAndEncrypt".

Configured Tv	Configured TwinCAT OPC UA Servers X										
Server URL: Endpoints:	opc.tcp://localhost:4840 Basic256Sha256 - SignA		Get Endpoints Add]							
	Name	ServerUrl	SecurityPolicyUri	SecurityMode	IdentityTokenType	Identity					

2. Then click **Add** to add the server. If you receive a warning regarding the differences in the server URL, confirm this message with **Yes**.

Different URL detected							
?	The selected endpoint returned a different URL (opc.tcp://EC2AMAZ-0EBTAKB:4840) than specified as the ServerURL (opc.tcp://localhost:4840). Do you still want to use the ServerURL?						
	Yes No						

⇒ The TwinCAT OPC UA Server has now been added to the selection dialog.

Configured TwinCAT OPC UA Servers X									×		
Server URL: opc.tcp://localhost:4840 Get Endpoints Endpoints: Basic256Sha256 - SignAndEncrypt Add											
		Name	ServerUrl	SecurityPolicyU	ri	SecurityMode		IdentityTokenTy	ре	Identity	
•	, Ť.	Server1	opc.tcp://localh	http://opcfo	\sim	SignAndEnc	\sim	Anonymous	\sim		

Depending on the operating environment, further settings for the connection parameters may now be necessary, e.g. user name/password for access to the server. In this example, however, it is assumed that both the TwinCAT OPC UA Server and the TwinCAT OPC UA Configurator were used on this system for the first time. So we leave the default settings and close the dialog.

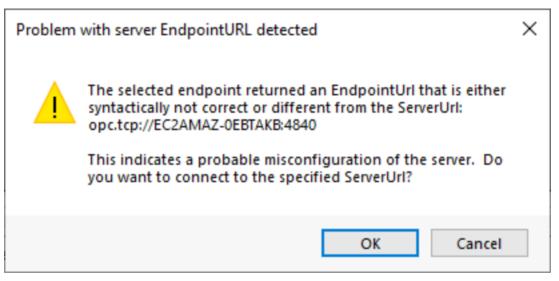
In the server selection list in the toolbar, you will now find a new entry with the connection profile you have just configured.

TwinCAT OPC UA Configurator		- 🗆 X							
File Server									
Edit Connect Disc	connect Connection state:								
Data Access Historical Access Alarms & Conditions Security Server Settings Online Panel									
Settings									
Devices									
Name AmsNetId AdsPort	Туре	Disabled							

Connecting to the server and reading the configuration

✓ To establish a connection with the server, make sure the server you just configured is selected.

1. Click on **Connect** in the toolbar. If you receive a warning regarding a different server URL, please confirm this dialog with **Ok**.



- 2. Since we assume a new installation in this tutorial, i.e. both the TwinCAT OPC UA Server and the TwinCAT OPC UA Configurator are used for the first time, the Configurator now recognizes that the server is an uninitialized server in the delivery state. For more information on the initialization concept (also known as TOFU Trust On First Use), we recommend the corresponding documentation chapter in the TwinCAT OPC UA Server documentation.
- 3. Enter a username/password combination to initialize the server. You can either use an existing user in the operating system or a new user, which is then automatically created in the operating system.

Server initia	lization	_		×				
The connected server has not been initialized yet. Please enter an operating system user account that you would like to use to login to the server after initialization.								
Usemame:								
Password:								
	<u>O</u> k	<u>C</u> ancel						

Please make a note of the username/password combination used, as this is required for later access to the server via OPC UA.

 \Rightarrow The server is now initialized and restarted.

4. You can now re-establish a connection to the server via the toolbar. The user used for initialization was automatically stored in the connection profile. Only the password needs to be re-entered for a connection.

TwinCAT OPC U	A Configurator				- 🗆	Х
File Server						
🗋 📂 🛃	Server1		V Edit Connect Disco	Onnect Connection state	disconnected	
Data Access Historie	cal Access Alarms & Condit	tions Security Server Setti	ings Online Panel			
Settings						
Devices						
	Name	AmsNetId	AdsPort	Туре	Disabled	11
User auther	ntication		×			
Usemame:	MyServerA	dmin				
Password:	•••••	•••••				
	Ok	Car	ncel			

⇒ The **Connection State** will change to "Connected" (green) and you will be connected to the server.

TwinCAT C	OPC UA Configura	ator						- 0	×
File Serve	er								
1 💕	3 📂	Server1		~ E	dit Connect	Disconnect	Connection state:	connected	
Data Access	Historical Access	Alarms & Conditions	Security	Server Settings	Online Panel				
Settings									
- Devices									
	Name		AmsNetle	ł	AdsPort		Туре	Dis	abled

5. You can now read the configuration of the server by clicking the **Open from Target** button in the toolbar.

L. TwinCAT	OPC UA C	onfigurator			-	· 🗆 X				
File Sen	File Server									
🗋 📂	Edit Connect Disconnect Connection state: connected									
Data Access Historical Ad Open from target itions Security Server Settings Online Panel										
Settings Devices										
		Name	AmsNetId	AdsPort	Туре	Disabled				
•	1	PLC1	127.0.0.1.1.1	851	TwinCAT 3 PLC (TMC) -	Fil				

 \Rightarrow The configuration of the server is read and displayed in the user interface of the Configurator.

Making changes to the configuration

You can now make any changes to the configuration. In this example, we want to make an additional ADS device available via the TwinCAT OPC UA Server. By default, only the first, locally running PLC runtime from the server perspective is made available via OPC UA. This PLC runtime named "PLC1" can be viewed in the **Data Access** tab.

1. We now add another Data Access device via the context menu.

. TwinCAT	OPC UA C	onfigura	tor						_		>
File Serv	/er										
1 📂		É.	Server1		~ E	dit Connect	Disconnect	Connection state: o	onnect	ed	
lata Access	Historical	Access	Alarms & Conditions	Security	Server Settings	Online Panel					
Settings											
Devices											
		Name		AmsNet	d	AdsPort		Туре		Disabled	
•	11	PLC1		127.0.0.1	.1.1	851		TwinCAT 3 PLC (TMC) - Fil		
			Add								
			Remove								

2. In the device properties, we set the parameters for **Name**, **AmsNetId**, **AdsPort** and **SymbolFile** to the settings shown below and save these settings using the **OK** button.

(Configure device			×
	Target communication			
	Name:	PLC2	Туре:	TwinCAT 3 PLC (TMC) - Filtered $\qquad \checkmark$
	AmsNetId:	127.0.0.1.1.1 Local Remote	SymbolFile:	[BootDir]\Plc\Port_852.tmc Upload
	AdsPort:	852	MaxGetHandle:	100
	AdsTimeout:	2000		ImportPlcProperties
	loMode:	ByHandle ~		ReleaseAdsHandles
		LegacyArrayHandling		Disable device

⇒ We have now added a second Data Access device to our configuration.

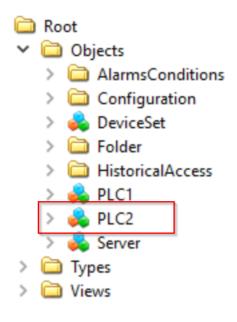
TwinCAT OPC	UA Config	urator			_			
File Server								
) 🞽 🖌	1 📂	Server1	✓ Ed	lit Connect Disconnect	Connection state: connect	ted		
Data Access Historical Access Alams & Conditions Security Server Settings Online Panel								
Settings								
Devices								
-	Name	8	AmsNetId	AdsPort	Туре	Disabled		
-	Name	ð	AmsNetId 127.0.0.1.1.1	AdsPort 851	Type TwinCAT 3 PLC (TMC) - Fil	Disabled		

Activating the new configuration on the server

Finally, we need to download the configuration to the server. You can use the corresponding **Activate on Target** button in the toolbar to do this. A final dialog informs us that the configuration has been successfully transferred to the server and asks whether it should be restarted. Confirm this with **Yes**.

Configur	ation download successful	\times
?	Configuration download successful. Would you like to restart the server?	
	Yes No	

You have successfully used the TwinCAT OPC UA Configurator to make a configuration change to the TwinCAT OPC UA Server. In this example, we have added an additional Data Access device to the server. The additional device is the second PLC runtime on the local system. Any OPC UA Client connecting to the server will now find this second PLC runtime under the "PLC2" object in the server address space.



4.2 Application directories

This application uses various directories to store relevant information, such as configuration or certificate files.

Installation directory

The base installation directory of the application is relative to the TwinCAT installation directory.

%TcInstallDir%\Functions\TF6100-OPC-UA

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

%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Configurator

The Visual Studio Configurator files are stored in the following directory:

%TcInstallDir%\Functions\TF6100-OPC-UA\Win32\Configurator\Vsix

Certificate directory

Certificate files, which are used to establish a secure communication connection, are stored in the following directory. There is a difference between the Standalone Configurator and the Visual Studio Configurator.

%ProgramData%\Beckhoff\TF6100-OPC-UA\TcOpcUaConfigurator\PKI
%ProgramData%\Beckhoff\TF6100-OPC-UA\TcOpcUaConfiguratorVs\PKI

Configuration files

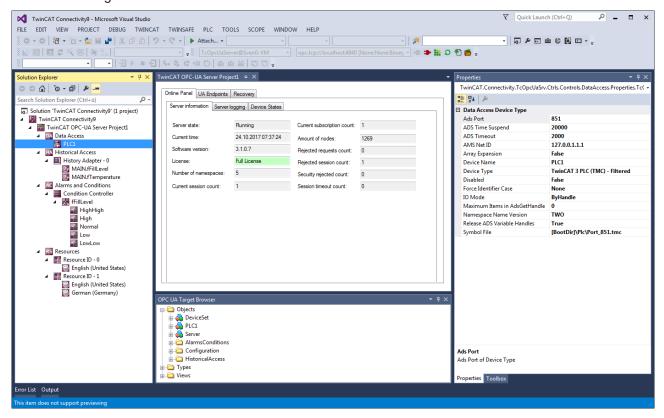
Both the Standalone Configurator and the Visual Studio Configurator use configuration files, e.g. for the server selection dialog. Depending on the tool, these configuration files are stored in the following directory.

```
%ProgramData%\Beckhoff\TF6100-OPC-UA\TcOpcUaConfigurator
%ProgramData%\Beckhoff\TF6100-OPC-UA\TcOpcUaConfiguratorVs
```

4.3 Visual Studio

4.3.1 Overview

The TF6100 setup (version 4.x.x and higher) contains the latest version of the OPC UA Server Configurator. This was integrated in Microsoft Visual Studio as a separate project type to provide an integrated and consistent engineering concept. You can configure all the different facets of the TwinCAT OPC UA Server and in doing so also use source control mechanisms such as Team Foundation Server or Subversion Integrations.



Requirements

Products	Setup versions	Target platform
TF6100	4.x.x	IPC or CX (x86, x64, ARM)

4.3.2 Creating a new project

The project package of the OPC UA Configurator integrates itself in the so-called connectivity package. You can select this when creating a new Visual Studio project.

Project template "TwinCAT Connectivity Project":

BECKHOFF

New Project					<u>? ×</u>
▷ Recent		.NET Framework 4.5	- Sort by: Default	• # E	Search Installed Templates (Ctrl+E)
⊿ Installed		Empty TwinCAT Co	ennestivity Dreiest	TwinCAT Connectivity	Type: TwinCAT Connectivity
 Templates Other Project Tyj TwinCAT Connect TwinCAT Measure TwinCAT PLC TwinCAT Projects Samples Online 	tivity ement	Empty IwinCAT Co	onnectivity Project	TwinCAT Connectivity	A template for creating an empty TwinCAT Connectivity project. You can add different kinds of TwinCAT Connectivity Functions to this project.
		Ω	Dick here to go online and find	templates.	
Name:	TwinCAT Connectiv	vity 1			
Location:	C:\Users\Administr	ator \Documents \Visual Studio	2013\Projects	•	Browse
Solution name:	TwinCAT Connectiv	vity1		[Create directory for solution
					OK Cancel

Project template "TwinCAT OPC-UA Server Project":

Add New Item - TwinCAT Connectivity	11			<u>?</u> ×
∡ Installed	Sort by: Default		Search Installed Templates (Ctrl+E)	ρ-
TwinCAT Connectivity ▷ Online	TwinCAT OPC-UA Server Project	TwinCAT Connectivity	Type: TwinCAT Connectivity The template includes a TwinCAT 3 OPC Server project. It will be added to your TwinCAT Connectivity Project.	
Name: TwinCAT OPC-UA	Server Project1.tcopcuasrv		Add Car	ncel

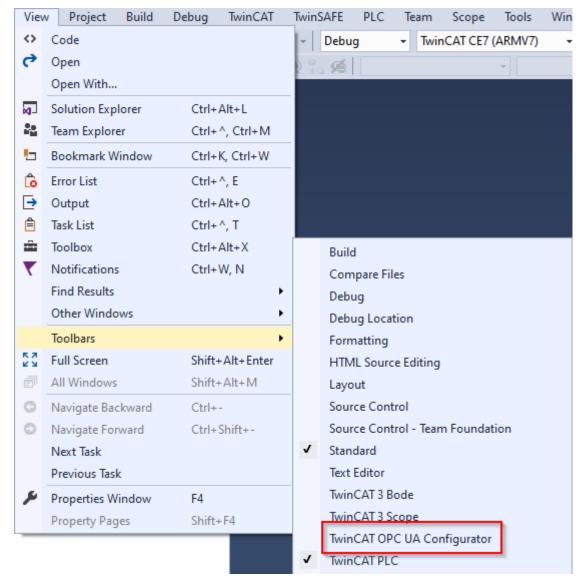
Requirements

Products	Setup versions	Target platform
TF6100	4.x.x	IPC or CX (x86, x64, ARM)

4.3.3 Connecting to a server

The OPC UA Configurator enables the complete parameterization of the Server via OPC UA. Similar to the TwinCAT XAE system, you can select an OPC UA Server to connect to via the toolbar.

1. To do this, first add the appropriate toolbar to your Visual Studio interface.



2. You can then add one or more server connections via the entry **Edit Serverlist** in the DropDownBox of the toolbar.

Edit Serverlist		🝷 🗲 Connect 📰	Disconnect	🗄 Ə 🏝 🖨 📮
Edit Serverlist				
Server configuration	Endpoint configuratio	n	×	×
Configurati	UaServer URL: Endpoint: Configuration Name: Anonymous Username	opc.tcp://localhost:4840 TcOpcUaServer@DESKTOP-PDTN35I [Basic256S opc.tcp://DESKTOP-PDTN35I:4840 [Basic256Sh Use DNS Name from Discovery URL		ServerUrl
Add Server Remove	Password Certificate	Ok	Cancel	Cancel

- 3. In the dialog **Endpoint configuration** you make all settings for the connection with the server, especially the server URL, the selection of an endpoint offered by the server and optionally also the IdentityToken (e.g. username/password) with which the configurator should connect to the server.
 - ⇒ The server connection is then added to the server list under an automatically generated configuration name and can then be selected in the drop-down list of the toolbar.

256Sha256, SignAndEncn			
Estonaest, orginalidencij	ypt opc.tcp://lo	calhost:4840	
Connect	Disconnec	t 🔝 D	*)
		Connect Disconnec	Connect Disconnect

⇒ By clicking on the Connect button, a connection to the server can now be established and the server configured.



Online configuration

All settings that you make in your project are carried out for the connected TwinCAT OPC UA Server.

i

Initialization of the server

If the server is still in the (uninitialized) delivery state, you will receive a corresponding note for server initialization. This process is described in more detail in the chapter on <u>Performing the server</u> initialization [\blacktriangleright 22].

Requirements

Products	Setup versions	Target platform
TF6100	4.x.x	IPC or CX (x86, x64, ARM)

4.3.4 **Performing the server initialization**

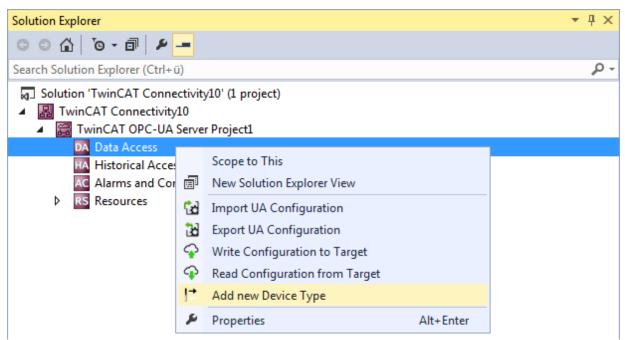
The TwinCAT OPC UA Server is delivered in an uninitialized mode, which is based on the so-called TOFU (Trust-On-First-Use) principle. Detailed information about this server feature and the corresponding background information can be found here. The TwinCAT OPC UA Configurator enables the initialization of the server during the first connection establishment. A corresponding warning message indicates the uninitialized server and enables an appropriate initialization.

Server initialization		x				
enter an operating s	ver has not been initialized yet. Please system user account that you would like to erver after initialization.					
Usemame: Password: CreateUserResult: LogonResult:						
Please remember to use the configured user account for further connections to the server!						
Status: Connected	Ok Cancel					

4.3.5 Adding ADS devices

The OPC UA Server can "talk" to one of more ADS devices. To establish a connection, a route to the respective ADS device is required. In the OPC UA Configurator, ADS devices are created, configured and thus announced to the OPC UA Server in the **Data Access** facet.

1. New ADS devices are added to the configuration via the context menu command **Add new Device Type**.



2. When the command is executed, a dialog box opens in which connection parameters can be configured for this device, e.g. AMS Net ID, ADS port or the symbol file.

]2↓ 🖾	
⊿	Data Access Device	
	Ads Port	851
	ADS Time Suspend	20000
	ADS Timeout	2000
	AMS Net ID	127.0.0.1.1.1
	Array Expansion	False
	Device Name	PLC1
	Device Type	TwinCAT 3 PLC (TMC) - Filte
	Disabled	False
	Force Identifier Case	None
	IO Mode	ByHandle
	Maximum Items in AdsGet	-
	Namespace Name Version	
	Release ADS Variable Ha	
	Symbol File	[BootDir]\Plc\Port_851.tmc
-	e vice Name evice Name of Data Access	

3. You can subsequently modify the connection parameters if necessary via the Properties window in Visual Studio.

Properties	- म ×				
$TwinCAT.Connectivity.TcOpcUaSrv.Ctrls.Controls.DataAccess.Properties.TcC \ \textbf{-}$					
Data Access Device Type					
Ads Port	851				
ADS Time Suspend	20000				
ADS Timeout	2000				
AMS Net ID	127.0.0.1.1.1				
Array Expansion	False				
Device Name	PLC1				
Device Type	TwinCAT 3 PLC (TMC) - Filtered				
Disabled	False				
Force Identifier Case	None				
IO Mode	ByHandle				
Maximum Items in AdsGetHandle	0				
Namespace Name Version	тwo				
Release ADS Variable Handles	True				
Symbol File	[BootDir]\Plc\Port_851.tmc				

Selecting the symbol file

Symbol files that are present on the selected target device can be imported directly. These symbol files can be stored either in the TwinCAT boot directory or in the symbol directory of the OPC UA Server. You can select the files via the corresponding dialog during the symbol file configuration.

Pr	operties	- म ×			
1	$eq:twinCAT.Connectivity.TcOpcUaSrv.Ctrls.Controls.DataAcce: \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$				
0					
Ξ	Data Access Device Type				
	Ads Port	851			
	ADS Time Suspend	20000			
	ADS Timeout	2000			
	AMS Net ID	127.0.0.1.1.1			
	Array Expansion	False			
	Device Name	PLC1			
	Device Type	TwinCAT 3 PLC (TMC) - Filtered			
	Disabled	False			
	Force Identifier Case	None			
	IO Mode	ByHandle			
	Maximum Items in AdsGetH	0			
	Namespace Name Version	тwo			
	Release ADS Variable Handle	True			
	Symbol File	[BootDir]\Plc\Port_851.tmc			

The TwinCAT OPC UA File Explorer can be connected to either the local TwinCAT directory or the remote boot directory. The latter can be read in via the configuration namespace of the server (see Configuration namespace).

OPC UA Symbol File Explorer

BECKHOFF

EE BootDir] E Analytics E CurrentConfig E PIC	Name Port_851.app Port_851.autostart Port_851.bootdata-old Port_851.cid Port_851.crc Port_851.occ Port_851.oce Port_851.ocm Port_851_act.tizip Port_851_boot.tizip Dot_851_boot.tizip Dot_851_boot.tizip
--	--

Requirements

Products	Setup versions	Target platform
TF6100	4.x.x	IPC or CX (x86, x64, ARM)

4.3.6 Reading and writing the configuration

Via the configurator you can initiate the download/upload of complete server configurations as well as loading every single facet (data access, historical access, etc.) individually to the target device and opening it there. The functions necessary for this are integrated both in the toolbar and in the context menu of the respective facet.

Opening a configuration from the target device

You can open the configuration of the selected target device via the corresponding button in the toolbar.

🕴 TcOpcUaServer@CX-238AF3 🔹 🔹 opc.tcp://172.17.36.174:4840 [None:None:Bina 👻 🐗 ⊅ 🏗 🥥 🏝 💼 🖕

See also: <u>Connecting to a server [> 20]</u>

Activating the configuration on a target device

Use the corresponding button in the toolbar to download the currently open configuration to the selected target device.

🕈 TcOpcUaServer@CX-238AF3 🔹 opc.tcp://172.17.36.174:4840 [None:None:Bina 👻 🖝 🖬 🥥 🐔 🚔 🖕

See also: <u>Connecting to a server [> 20]</u>

Opening a partial configuration

Use the command **Read Configuration from Target** in the context menu of a specific facet of the configuration to open the partial configuration of the selected target device.

) 🖸 🟠 To - Z 🗇 🛅 🖉			
	-		
arch Solution Explorer (Ctrl+ü)			
 Solution 'TwinCAT Connectivity1' TwinCAT Connectivity1 TwinCAT OPC-UA Server Pr Data Access PLC1 		ect)	
HA Historical Access		6 ·	
 History Adapter - 0 PLC1.DeviceManu 	Ja 🗐	Scope to This New Solution Explorer View	
PLC1.DeviceRevisio AC Alarms and Conditions RS Resources	io 🔂	Import UA Configuration	
	33	Export UA Configuration	
P Resources	Ŷ	Write Configuration to Target	
	Ŷ	Read Configuration from Target	
	0	Add new History Adapter	
	لكر	Properties	Alt+Enter

See also: Connecting to a server [20]

Downloading a partial configuration

Use the command **Write Configuration to Target** in the context menu of a specific facet of the configuration to download the partial configuration to the selected target device.

Solution Explorer			
o o 🏠 'o - 2 🗇 🕼 🗡 🗕	ı –		
Search Solution Explorer (Ctrl+ü)			
 Solution 'TwinCAT Connectivity1' (1 TwinCAT Connectivity1 TwinCAT OPC-UA Server Project Data Access PLC1 		ct)	
HA Historical Access			
 History Adapter - 0 PLC1.DeviceManua PLC1.DeviceRevisio Alarms and Conditions RS Resources 		Scope to This New Solution Explorer View Import UA Configuration Export UA Configuration Write Configuration to Target	
	ĵ ↓ ↓	Read Configuration from Target Add new History Adapter	

See also: <u>Connecting to a server</u> [▶ 20]

4.3.7 Importing and exporting configuration files

The context menu commands enable the import/export of configuration files of the OPC UA Server.

Importing a partial configuration

Use the **Import UA Configuration** command in the context menu of a specific facet of the configuration to import the partial configuration (e.g. Historical Access) from an XML configuration file.

Solution Explorer						
G O 🔂 🗿 - 2 🗇 🕲 🗶 💻						
Search Solution Explorer (Ctrl+ü)						
 Solution 'TwinCAT Connectivity1' (1 project) Image: TwinCAT Connectivity1 Image: TwinCAT OPC-UA Server Project1 Image: Data Access Image: PLC1 						
 Historical Access History Adapter - 0 PLC1.DeviceManua PLC1.DeviceRevisio Alarms and Conditions RS Resources 		Scope to This New Solution Explorer View Import UA Configuration Export UA Configuration Write Configuration to Target Read Configuration from Target Add new History Adapter				
	ų	Properties	Alt+Enter			

Exporting a partial configuration

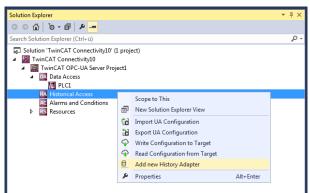
Use the command **Export UA Configuration** in the context menu of a specific facet of the configuration to export the partial configuration (e.g. Historical Access) to an XML configuration file.

Solution Explorer					
○ ○ ☆ ĭo - ≠ 司 in ≯ -					
Search Solution Explorer (Ctrl+ü)					
 Solution 'TwinCAT Connectivity1' (1 Solution 'TwinCAT Connectivity1 TwinCAT OPC-UA Server Proj Data Access PLC1 		ct)			
HA Historical Access		Scope to This			
 History Adapter - 0 PLC1.DeviceManua 		New Solution Explorer View			
PLC1.DeviceRevisio	යි	Import UA Configuration			
AC Alarms and Conditions RS Resources	ゐ	Export UA Configuration			
resources	Ŷ	Write Configuration to Target			
	Ŷ	Read Configuration from Target			
	٥	Add new History Adapter			
	¥	Properties	Alt+Enter		

4.3.8 Configuring historical access

To configure Historical Access, you must first set up the History Adapters. These are the different locations for storing historical data, such as RAM, file, SQL Server.

History Adapters are added to the configuration using the context menu command **Add new History Adapter**.



Depending on the adapter type you have to specify further parameters, e.g. the desired file storage path or the access data for the SQL Server.

	ate History Adapter		
	Adapter Id	0	
	vdapterType	File	-
[)atabase	Volatile	
F	ìle	File	
F	assword	SQL	
9	erver	SQLCompact	
1	lser		
-	oterType ry Adapter Type of Hi	storical Access Create	Cancel

After you have created a History Adapter you can add the desired variables to the adapter. These variables must already exist on the selected OPC UA Server when the engineering is implemented. You can use the integrated **OPC UA Target Browser** to select the variables and then add the variables from the target browser to the History Adapter by drag and drop.



Additional parameters can be specified in the properties window of the newly added variable, e.g. the desired SamplingRate or the size of the ring buffer to be used in the History Adapter.

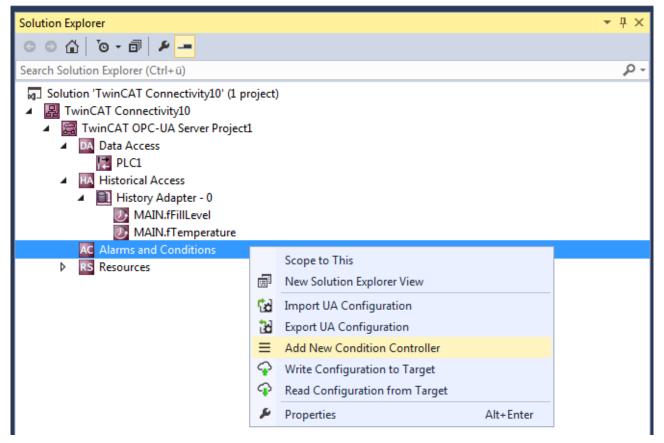
Properties	▼ ₽ ×
MAIN.fFillLevel TwinCAT.Connect	tivity.TcOpcUaSrv.Ctrls.Controls.Historical. 🗸
TwinCAT OPC-UA Server	
AdapterId	0
MaxSamples	1000
NodeId	s=MAIN.fFillLevel
NS	urn:BeckhoffAutomation:Ua:PLC1
SamplingRate	250

See also: <u>Connecting to a server [> 20]</u>

4.3.9 Configuring Alarms and Conditions

In order to configure Alarms and Conditions (A&C) you must first set up the Condition Controllers. These are container units that group together alarms.

Condition Controllers are added to the configuration using the context menu command **Add New Condition Controller**.



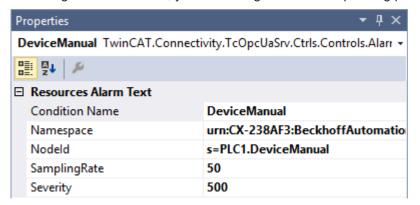
Once you have created a Condition Controller, add the desired variables to the controller and monitor them in terms of alarms and conditions. A Condition is created for each variable, which specifies the parameters for monitoring. These variables must already exist on the selected OPC UA Server when the engineering is implemented. You can use the integrated **OPC UA Target Browser** to select the variables and then add the variables from the Target Browser to the Condition Controller by drag and drop.



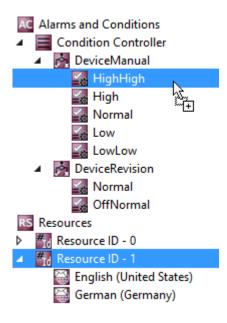
In the dialog box which then opens you can define the Condition type and further parameters for the monitoring, e.g. SamplingRate and Severity.

Creat	e new Condition Co	ntroller 🛛 🖻
۲	Limit Alarm Type	OffNormal Alarm Type
] <mark>2</mark> ↓	
4	Resources Alarm	Text
	Condition Name	Condition
	Namespace	um:BeckhoffAutomation:U
	Nodeld	s=MAIN.dummy_var
	SamplingRate	50
	Severity	500
	ondition Name arms Conditions - Cond	lition
		Okay Cancel

Depending on the Condition type selected, specify additional parameters in the Condition properties window. The threshold values for the respective Condition type are displayed as individual entries in the tree view of the configuration. Here too, you can configure the corresponding parameters in the properties window.



Subsequently you have to define the alarm texts that are to be sent to the OPC UA Client when a Condition is triggered. How to create alarm texts is described in the chapter <u>Configuring alarm texts</u> [> 32]. You can drag and drop the alarm texts onto the respective threshold value of a Condition.



Alarm type OffNormal

An OffNormal alarm type is used to define which state of a Boolean variable is evaluated as normal. An alarm is triggered if the variable value deviates from this. The PLC must be used for working with value ranges (e.g., integer or double variables). Depending on the value, a corresponding TRUE or FALSE state is then passed to the OPC UA Server.

State	Value range
Normal	TRUE or FALSE, depending on the user's decision.
	TRUE or FALSE, depending on the configuration of the normal state. Cannot be configured by the user.

Properties	- ₽ ×
Normal TwinCAT.Connectivity.TcC	pcUaSrv.Ctrls.Controls.AlarmsCon 👻
Resources Alarm Text	
Resource ID	0
Value	False

The first step is to configure the normal state as described above. The user then defines an alarm text for the respective state (OffNormal and Normal) via Resources. This can be done either by drag and drop or by selecting from the **Resource ID** drop-down list.

Alarm type limit

With an alarm type limit you define different threshold values upon whose reaching an alarm is to be sent. The following table describes the different threshold values using an example configuration.

State	Example threshold values	Associated value range (INT)
HighHigh	5000	5000-32767
High	2000	2000-4999
Normal	-	1000-1999
Low	1000	500-999
LowLow	500	-32768-499

Properties	- ₽ ×
HighHigh TwinCAT.Connectiv	/ity.TcOpcUaSrv.Ctrls.Controls.AlarmsCo 👻
Resources Alarm Text	
Resource ID	0
Value	42

In the first step, the various threshold values are configured as described above. The user then defines an alarm text for the respective state (HighHigh, High, Normal, Low, LowLow) via Resources. This can be done either by drag and drop or by selecting from the **Resource ID** drop-down list.

Requirements

Products	Setup versions	Target platform
TF6100	4.x.x	IPC or CX (x86, x64, ARM)

See also: <u>Connecting to a server [> 20]</u>

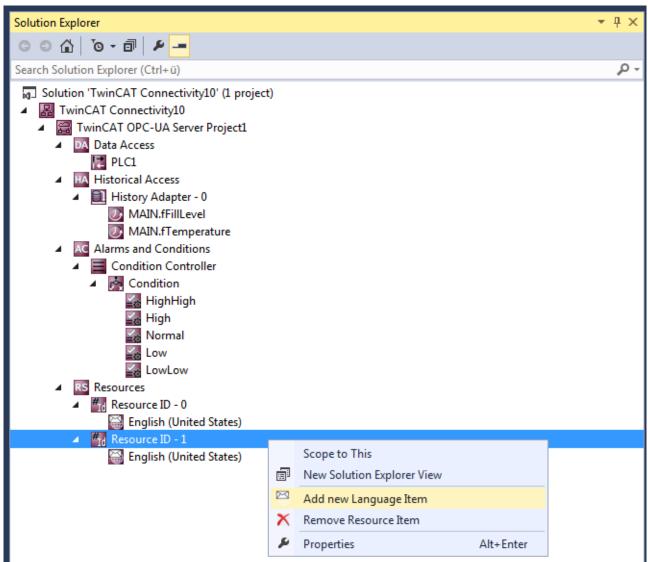
4.3.10 Configuring alarm texts

The OPC UA Configurator enables the (multilingual) management of alarm texts that are used, for example, with <u>Alarms and Conditions [> 29]</u>. The configuration of the alarm texts takes place in the **Resources** facet. Each alarm text is identified by a unique ID. Multiple language texts can then be assigned to this ID.

You can create so-called Resource Items using the context menu command Add new Resource Item.

Solution Explorer			- ₽ ×
© ⊃ ☆ 'o - i / ≁			
Search Solution Explorer (Ctrl+ü)			<i>-</i> ۹
 Solution 'TwinCAT Connectivity10' (1 project) TwinCAT Connectivity10 TwinCAT OPC-UA Server Project1 Data Access PLC1 Historical Access History Adapter - 0 History Adapter - 0 MAIN.fFillLevel MAIN.fT emperature A larms and Conditions Condition Condition HighHigh High Normal Low LowLow 			
Resource ID - 0	Scope to This		
English (United States)	New Solution Explorer View		
<u> </u>	Write Configuration to Target		
9	nead configuration for anget		
# 20	Add new Resource Item		
2	Properties	Alt+Enter	

You add new Language Items to a Resource Item using the command **Add new Language Item** in the context menu of a Resource Item.



You can further parameterize a Language Item, e.g. the language text and the assigned language, in the properties window. When you define the language, the associated LocaleID is automatically set. The LocaleID is requested by the OPC UA Client to indicate in which language it expects alarm texts.

Properties	- ↓ ×
German (Germany) TwinCAT	.Connectivity.TcOpcUaSrv.Ctrls.Controls 👻
Resources Language	
Resource Alarm Text	default Alarm Text
Resource Language	German (Germany)
Resource Localeld	de-DE

Requirements

Products	Setup versions	Target platform
TF6100	4.x.x	IPC or CX (x86, x64, ARM)

4.3.11 Configuring endpoints

The endpoints of the OPC UA Server indicate which security mechanisms are to be used during the connection establishment of a client. These range from "unencrypted" to "encrypted and signed", based on different key strengths.

The endpoints can be activated and deactivated using the configurator. It may be useful to deactivate the unencrypted endpoint so that all clients can only connect themselves with valid certificates that are classified as trustworthy.

The endpoints are configured directly at the level of the OPC UA Server project. By double-clicking on the project you can make the corresponding settings on the **UA Endpoints** tab. The settings become effective after an activation of the configuration and a subsequent restart of the server (see <u>Reading and writing the configuration [\blacktriangleright 25] and <u>Restarting the server [\blacktriangleright 43]</u>).</u>

line Panel UA Endpoir	nts Recovery		
General			
Enable Anonymous lo	ogon		Server port: 4840 🖨
Enable Usemame/Pa	assword logon		
Security			
✓ None			
 Basic 128Rsa 15 	Sign & Encrypt	-	
Basic256	Sign & Encrypt	•	
✓ Basic256Sha256	Sign & Encrypt	-	
Client certificates			
Common Name	ThumbPrint		Status
ThumbPrint			Open Cert

Requirements

Products	Setup versions	Target platform
TF6100	4.x.x	IPC or CX (x86, x64, ARM)

4.3.12 Trust relationship for certificates

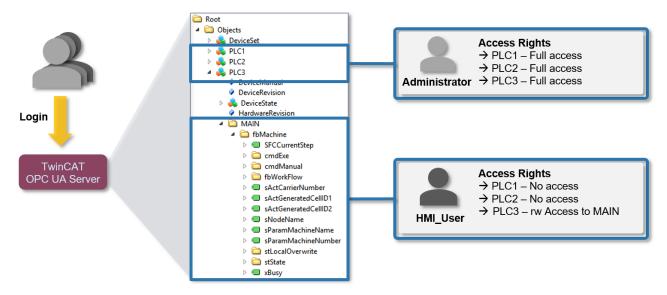
The Configurator facilitates management of the client certificates on the server. In the project settings you can classify the certificates as trustworthy or refuse them on the **UA Endpoints** tab in the **Client certificates** area.

After an OPC UA Client has attempted to connect to a secure server endpoint for the first time, the client certificate is deposited on the server and declared "rejected". The server administrator can subsequently enable the certificate. A subsequent connection attempt of the client with a secured endpoint will then be successful.

inCAT OPC-UA Server Project1 + × Online Panel UA Endpoints Recovery		
General Carlos Enable Anonymous logon Enable Usemame/Password logon		Server port: 4840
Security Security None Basic 128Rsa 15 Basic 256 Basic 256Sha 256	* *	
Client certificates Common Name Thumb	Print	Status
TcOpcUaGateway@SvenG A2D03	BAF26439D To Trust List To Reject List Delete	3AA8 Rejected
ThumbPrint		Open Cert

4.3.13 Configuring security settings

The OPC UA Server enables the configuration of permissions at namespace and node level. This allows you to fine-granulate the access to ADS devices (for example, to different PLC runtimes) as well as variables. These security settings are available for all ADS devices that can be displayed in the server namespace.



Configuration

The permissions are configured on the basis of an XML-based configuration file (*TcUaSecurityConfig.xml*), which is located in the same directory as the server. The configuration file consists of the three areas **Users**, **Groups**, and **AccessInfos**.

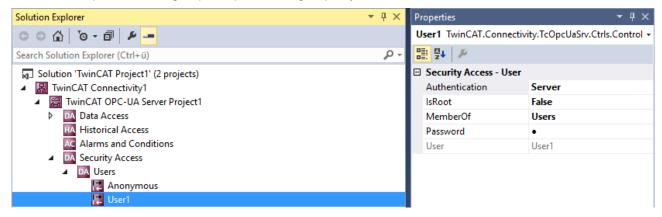
Users

In the **Users** area you can configure user accounts that are to be accepted by the OPC UA Server as logins. There are three different authentication methods:

OS (recommended authentication method)	The mechanisms of the operating system are used to validate user name and password. The user account is subject completely to the control of the operating system and/or domain.
Server (not recommended)	User name and password are known only to the OPC UA Server. Both pieces of information are stored in plain text in the XML file.
None	Only the user name of the server is evaluated, the password is ignored.

Users can be configured with a tag <DefaultAccess> that specifies the standard access of the user to a certain namespace.

Users can be members of one or more groups. You can specify this using the **MemberOf** attribute. In case of memberships of several groups, separate the groups by a semicolon.

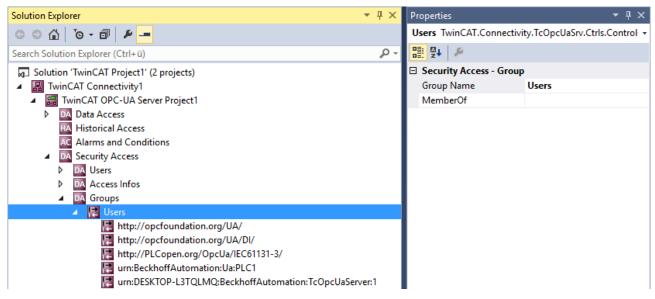


Groups

In order to enable a simpler configuration with several user accounts, you can combine the users into groups.

Groups can also be configured with a tag <DefaultAccess>.

You can nest groups using the **MemberOf** attribute. In case of memberships of several groups, separate the groups by a semicolon.



AccessInfos

If a fine-granular setting of permissions at the node level is to be implemented, then AccessInfos can be configured additionally, which specify the access permissions on nodes. Access rights can be passed on to subelements. Although AccessInfos allow the most fine-grained configuration of permissions, such a configuration can quickly become confusing. Therefore, check whether configuring access rights at the namespace level (see above) is not sufficient.

The AccessInfo for a node contains the following settings:

NS	Configures the NamespaceName in which the node is localized
ld	Configures the identifier of the node, including the IdentifierType (e.g. s = String)
Depth	Inheritance depth of permissions (-1 for infinite)
User/Group	User or group that is to be given access to this node, including the AccessLevels

Solution Explorer	▼ ₽×	Properties	- ₽ ×
G O 🔂 To - 🖻 🔎 🗕		ns=4;s=MAIN.Instance1	TwinCAT.Connectivity.TcOpc 👻
Search Solution Explorer (Ctrl+ü)	ب م		
Solution 'TwinCAT Project1' (2 projects)		Default Access - Node	Identification
TwinCAT Connectivity1		Depth	-1
TwinCAT OPC-UA Server Project1		ID	ns=4;s=MAIN.Instance1
DA Data Access		NAMESPACE	urn:BeckhoffAutomation:Ua
HA Historical Access		User Name	User1
Ac Alarms and Conditions		Default Access - Permi	issions
A DA Security Access		ATTRIBUTE READABLE	True
DA Users		ATTRIBUTE WRITABLE	False
A DA Access Infos		BROWSEABLE	True
ns=4;s=MAIN.Instance1		EVENT READABLE	False
ns=4;s=MAIN.Instance2	I	EVECTITARI E	Falco

AccessInfos can be configured by dragging & dropping variables from the Target Browser. The configurable permissions are cumulative.

Sample configuration

Let's take the following simple control program. The variables are already published in the OPC UA namespace of the server. The OPC UA Server is initially in the delivery state.

🛅 Objects
> i AlarmsConditions
> in Configuration
> 🚕 DeviceSet
> istoricalAccess
🗸 👶 PLC1
DeviceManual
DeviceRevision
> 뤚 DeviceState
HardwareRevision
🗸 🚞 MAIN
> 🔲 Instance1
> 🔘 Instance2
Manufacturer
Model
> 🚕 Programs
RevisionCounter
SerialNumber
SoftwareRevision
> 뤚 Tasks
> 🚕 Server
🛅 Types
🚞 Views

Access restrictions

Access to the server is to be restricted for clients as follows:

- Anonymous access is to be deactivated.
- There is to be a user "Administrator" who has full access to the complete server.
- There is to be a user "User1" who only has read access to MAIN.Instance1. The user should not come from the operating system here, but should only be used internally in the server.
- There is to be a user "User2" who only has read access to MAIN.Instance2. The user should not come from the operating system here, but should only be used internally in the server.
- · General access permissions are to be configured for all users via a group called "Users".

Settings

The configuration of the OPC UA Server is set as follows:

- TwinCAT Connectivity3

88	Т	vinCAT OPC-UA Server Project1
⊳	DA	Data Access
	ΗA	Historical Access
	AC	Alarms and Conditions
4	DA	Security Access
	4	DA Users
		🛃 Administrator
		🛃 User1
		🛃 User2
	4	DA Access Infos
		ns=4;s=MAIN.Instance1
		ns=4;s=MAIN.Instance2
	4	DA Groups
		Users
		http://opcfoundation.org/UA/
		🔣 urn:BeckhoffAutomation:TcOpcUaServer
		📰 urn:BeckhoffAutomation:Ua:PLC1
	RS	Resources

Settings for the user "Administrator":

Properties – 🖣 🗙		
Administrator TwinCAT.Connectivity.TcOpcUaSrv.Ctrls.Controls.Secu -		
Security Access - User		
Authentication	Server	
IsRoot	True	
MemberOf		
Password	•	
User	Administrator	

Settings for the user "User1":

Properties	~ ₽ ×	
User1 TwinCAT.Connectivity.TcC	DpcUaSrv.Ctrls.Controls.Security.Prop 👻	
Security Access - User		
Authentication	Server	
IsRoot	False	
MemberOf	Users	
Password	•	
User	User1	

Settings for the user "User2":

Properties	▼ ₽ ×	
User2 TwinCAT.Connectivit	ty.TcOpcUaSrv.Ctrls.Controls.Security.Prop 👻	
E Security Access - User		
Authentication	Server	
IsRoot	False	
MemberOf	Users	
Password	•	
User	User2	

Settings for AccessInfos "MAIN.Instance1":

Properties 🝷 🕂 🗙		
ns=4;s=MAIN.Instance1 TwinCAT.Connectivity.TcOpcUaSrv.Ctrls.Col -		
Default Access - Node Identi	fication	
Depth	-1	
ID	ns=4;s=MAIN.Instance1	
NAMESPACE	urn:BeckhoffAutomation:Ua:PLC1	
User Name	User1	
Default Access - Permissions		
ATTRIBUTE READABLE	True	
ATTRIBUTE WRITABLE	False	
BROWSEABLE	True	
EVENT READABLE	False	
EXECUTABLE	False	
HISTORY DELETE	False	
HISTORY INSERT	False	
HISTORY MODIFY	False	
HISTORY READABLE	False	
PERMISSION ALL	False	
READABLE	True	
WRITABLE	False	

Settings for AccessInfos "MAIN.Instance2":

Properties	- ₽ ×	
ns=4;s=MAIN.Instance2 TwinCAT.Connectivity.TcOpcUaSrv.Ctrls.Col -		
Default Access - Node Identification		
Depth	-1	
ID	ns=4;s=MAIN.Instance2	
NAMESPACE	urn:BeckhoffAutomation:Ua:PLC1	
User Name	User2	
Default Access - Permissions		
ATTRIBUTE READABLE	True	
ATTRIBUTE WRITABLE	False	
BROWSEABLE	True	
EVENT READABLE	False	
EXECUTABLE	False	
HISTORY DELETE	False	
HISTORY INSERT	False	
HISTORY MODIFY	False	
HISTORY READABLE	False	
PERMISSION ALL	False	
READABLE	True	
WRITABLE	False	

Settings for the group "Users":

The user group is equipped both with basic access to required server and type system namespaces and with read and browse permissions to the PLC1 namespace.

Pr	operties	- ₽ ×	
u	urn:BeckhoffAutomation:Ua:PLC1 TwinCAT.Connectivity.TcOpcUaS -		
0	2 · /		
Ξ	Default Access - Namespace		
	NAMESPACE	urn:BeckhoffAutomation:Ua:PLC1	
Ξ	Default Access - Permissions		
	ATTRIBUTE READABLE	True	
	ATTRIBUTE WRITABLE	False	
	BROWSEABLE	True	
	EVENT READABLE	False	
	EXECUTABLE	False	
	HISTORY DELETE	False	
	HISTORY INSERT	False	
	HISTORY MODIFY	False	
	HISTORY READABLE	False	
	PERMISSION ALL	False	
	READABLE	False	
	WRITABLE	False	

Result

Following activation of the configuration, the namespace of the server for "User1" looks like the following after establishment of a connection:

🛱 Root
Objects
✓ 💑 PLC1
DeviceManual
DeviceRevision
> 骉 DeviceState
HardwareRevision
🗸 🛅 MAIN
✓
> 💷 a
> 💷 b
Manufacturer
Model
> 骉 Programs
RevisionCounter
SerialNumber
SoftwareRevision
> 骉 Tasks
> 🖂 Server
> 🛅 Types
> 🛅 Views

The user has only read rights to the node "Instance1", which is clear from the attribute UserAccessLevel:

DataType	ST_Test
NamespaceIndex	4
IdentifierType	String
Identifier	<structureddatatype>:ST_Test</structureddatatype>
ValueRank	-1
ArrayDimensions	BadAttributeldInvalid (0x80350000)
AccessLevel	CurrentRead, CurrentWrite
UserAccessLevel	CurrentRead

The user "Administrator", conversely, has full access rights to all elements of the namespace:

🛅 Root
✓
> 🚞 AlarmsConditions
> 🚞 Configuration
> 뤚 DeviceSet
> 🚞 HistoricalAccess
Y 👶 PLC1
DeviceManual
DeviceRevision
> 뤚 DeviceState
HardwareRevision
Y 🛅 MAIN
> 🍩 Instance1
> 🏼 Instance2
Manufacturer
Model
> 뤚 Programs
RevisionCounter
SerialNumber
SoftwareRevision
> 뤚 Tasks
> 븛 Server
> 🚞 Types
> 🚞 Views

4.3.14 Restarting the server

The OPC UA Configurator enables the triggering of a restart of the OPC UA Server. This can be done locally or remotely and refers to the selected target device.

Loss of connection

A restart of the OPC UA Server always leads to a loss of the connection of all connected clients.

The restart is triggered via the toolbar.

3	TcOpcUaServer@CX-238AF3 -	opc.tcp://172.17.36.174:4840 [None:None:Bina 👻	ie: :	. IR	ວ	*ን 🖻	<u>-</u>	
·.·					\sim			

Requirements

Products	Setup versions	Target platform
TF6100	4.x.x	IPC or CX (x86, x64, ARM)

See also: <u>Connecting to a server [> 20]</u>

4.3.15 Logging

For an advanced diagnostics you can activate the logging function of the OPC UA Server.



Writing the log file

Activating the logging function on the server causes a log file to be written on the file system. Make sure that there is sufficient storage space available and set the logging parameters accordingly (number of log files, size per log file).

Performance and timing behavior

Activation of the logging function will change the timing behavior of the OPC UA Server. As a result there may be losses of speed, depending on the platform and project.

The logging function is activated using the **Activate** button on the **Online Panel** tab in the project configurator. You can activate the function locally or remotely depending on the selected target device. The logging function remains active until it is deactivated again via the configurator or until the OPC UA Server is restarted.

TwinCAT OPC-UA Server Project1 😕 🗙		
Online Panel UA Endpoints Recovery		
Server information Server logging Device States		
File Configuration	Application Trace	
Number of trace files: 0	AppTrace level:	0 (NoTrace) 🔹
Number of entries per file: 0	AppTrace is deactivated	Set
Trace file name:	Stack Trace	
Flush trace to file is active	StackTrace level:	0 (NONE) -
Set	Stack Trace is deactivated	Set
Trace Event Level		
Trace Event level: 0 (Disabled)		
Event History Date range: Refresh		

Trace Level

In general, the higher the trace level, the more detailed (and more) data is written, but the more load is also placed on the server application, which changes the timing behavior accordingly. Please therefore only activate logging in the event of diagnostics and in consultation with Beckhoff Support.

Activate App Trace

In most cases it is sufficient to create a so-called "AppTrace". This logs information from the server application. To activate the AppTrace, please enter the number of TraceFiles and the number of entries per TraceFile in the corresponding text fields. Then select a trace level and click the button to activate the AppTrace. The values in the gray text boxes represent the current settings on the server.

Activate Stack Trace

In a few cases it is also necessary to create a so-called "StackTrace", whereby information from the OPC UA stack is logged. To activate the StackTrace please enter the number of TraceFiles as well as the number of entries per TraceFile into the corresponding text boxes. Then select a trace level and click on the button to activate the StackTrace. The values in the gray text boxes represent the current settings on the server.

Requirements

Products	Setup versions	Target platform
TF6100	4.x.x	IPC or CX (x86, x64, ARM)

See also: <u>Selecting a target device [} 20]</u>

4.4 Standalone

4.4.1 Overview

The standalone configurator enables parameterization of the TwinCAT OPC UA Server independently of Visual Studio. You can configure all the different features of the server.

Ą	TwinC	CAT OPC UA Cor	figurator				-		×
File		Server							
: 🖻	P	💷 i 🚘 💀 🔽	irtual Machine 1	✓ Edit Connect Disconnect C	Connection state: connected				
					connected				
Data	a Acce	ess Historical Ac	cess Alarms & Conditions Sec	urity Server Settings Online Panel					
Se	ttings								
	Device	es							
Г		Name		AmsNetId	AdsPort	Туре		Disabled	a
	•	PLC1		127.0.0.1.1.1	851	TwinCAT 3 PLC (TMC) - Filtered			
						The second second second			
	D-4	te/Time	M						^
			Message Successfully connected to serv						
Ĭ			Successfully refreshed certifica						
ŏ				com/TwinCAT/TF6100/Server/Configuration					_
ŏ			Found device nup.77 Beckhoff Aut						-
ŏ			Found device um:BeckhoffAut						-
ŏ			Found device um:BeckhoffAut						~
			r sana device am.beokholi/Adi	analon.od.t Eo t					~
Log	ging	Target Browser							

4.4.2 Connecting to a server

The OPC UA Configurator enables the complete parameterization of the Server via OPC UA. Similar to the TwinCAT XAE system, you can select an OPC UA Server to connect to via the toolbar.

Ç,	TwinCAT OPC UA Configurator			_		
F	le Server					
1	😂 🛃 📄 🔐 Virtual Machine 1	✓ Edit Connect Disconnect Connect Co	onnection state:			
D	ta Access Historical Access Alarms & Conditions Sec	urity Server Settings Online Panel				
1	ettings					
	Devices					
	Name	AmsNetId	AdsPort	Туре	Disabled	

Click on the **Edit** button to open the server list dialog. In this dialog you can add one or more server connections.

er URL: opc.tcp://localhost: points:	4840 Get Endpoints							
Name	ServerUrl	SecurityPolicyUri	_	SecurityMode		IdentityToken	Туре	Identity
Virtual Machine 1	opc.tcp://192.168.179.136:4	8 http://opcfoundation.org/UA/SecurityPolicy#Aes128_Sha256_RsaOaep	• ~	SignAndEncrypt	\sim	UserName	~	SomeAdmin
Virtual Machine 2	opc.tcp://192.168.179.93:46	http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256	~	SignAndEncrypt	~	Anonymous	\sim	
CX-305858	opc.tcp://CX-305858:4840	http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256	~	Sign	\sim	Anonymous	~	
CX-3EC02E	opc.tcp://CX-3EC02E:4840	http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256	~	Sign	~	Anonymous	~	

By entering a ServerURL and pressing the **Get Endpoints** button, a server connection can be added to the list. Any settings for the IdentityToken, e.g. whether the Configurator should connect as an anonymous user or with a user name/password combination, must be set manually.

Confirming a configuration

Please always confirm changes to the entries with the **ENTER** key, as only then will they be automatically saved in the background.

After configuring a server connection, the corresponding entry is available in the DropDownBox and the connection can be established by clicking the **Connect** button.

4.4.3 **Performing the server initialization**

The TwinCAT OPC UA Server is delivered in an uninitialized mode, which is based on the so-called TOFU (Trust-On-First-Use) principle. Detailed information about this server feature and the corresponding background information can be found here. The TwinCAT OPC UA Configurator enables the initialization of the server during the first connection establishment. A corresponding warning message indicates the uninitialized server and enables an appropriate initialization.

Server initia	lization		\times
enter an op	cted server has not b erating system user a to the server after ini	ccount that y	
Usemame:			
Password:			
	Ok	Cancel	

4.4.4 Adding ADS devices

ADS devices can be added to the TwinCAT OPC UA Server configuration via the **Data Access** tab. In the associated DataGrid, create a new device via the context menu.

R	TwinC	AT O	PC UA Configur	ator		
Fi	le s	Server	r			
1) 🚰		🗳 🔛 Virtual	Machine 1	~	Edit Conne
Da	ita Acce	ss	listorical Access	Alarms & Conditions	Security	Server Settings
S	ettings					
	Device	es				
			Name		Am	sNetId
	•		PLC1		127.	0.0.1.1.1
			Add			
			Remove			
			Edit			

Set the device-specific parameters in the subsequent dialog.

Configure device			×
- Target communication -			
Name:	PLC2	Туре:	TwinCAT 3 PLC (TMC) - Filtered \checkmark
AmsNetId:	10.0.2.15.1.1 Local Remote	SymbolFile:	[BootDir]\Plc\Port_851.tmc Upload
AdsPort:	852	MaxGetHandle:	100
AdsTimeout:	2000		ImportPIcProperties
loMode:	ByHandle \checkmark		ReleaseAdsHandles
	LegacyArrayHandling		Disable device
Device meta-data (DI) Manufacturer:	Beckhoff Automation	SoftwareRevision:	1.0
Model:	CX2020	HardwareRevision:	1.0
SerialNo:	4242-42	DeviceRevision:	1.2
DeviceManual:	https://www.beckhoff.com/cx2020	RevisionCounter:	4
Miscellaneous			
			-
Identifier:	None ~	NsNameVersion:	0 ~
	Ok Cancel		

Selecting an AMS NetID

To select an AMS NetID, either the ADS devices from the local system or the connected TwinCAT OPC UA Server can be selected. An ADS device is a system that has an ADS route to the local system or server system. By clicking on the **Local** button the local ADS routes are displayed. By clicking the **Remote** button the ADS routes on the connected TwinCAT OPC UA Server are displayed.

Selecting a symbol file

The selection of a symbol file is always done from the local system. However, the symbol file can be uploaded to the connected TwinCAT OPC UA Server via the **Upload** button. The symbol file is stored in the subfolder "symbolfiles" of the TwinCAT OPC UA Server home directory and automatically referenced via a placeholder in the configuration file.

4.4.5 Reading and writing the configuration

The configurator enables both reading/writing of the configuration files from the TwinCAT OPC UA Server and loading/saving of the configuration files on the local system. These functionalities are available via the menu as well as the toolbar.

Local loading/saving

These functions are available via the **File** menu. The buttons available here **Open** and **Save** enable the configuration files to be loaded and saved. All configuration files are always loaded or saved.

Remote loading/saving

These functions are available from the **server** menu. The buttons **Open from target** and **Activate from target** available here enable loading and saving of the configuration files from the connected TwinCAT OPC UA Server. All configuration files are always loaded or saved.

4.4.6 Configuring historical access

Use the **Historical Access** tab to configure both the **History Adapter** and the **History Nodes**. A **History Adapter** defines the type of data storage and a **History Node** the variable for which historical data should be saved in the data storage.

😭 TwinCAT	T OPC UA Configura	ator					_	
File Se	rver							
🗋 💕 🔒	🛛 🔛 🔛 Virtual	Machine 1	✓ Edit Connect	Disconnect Connectio	n state:			
Data Access	Historical Access	Alarms & Conditions	Security Server Settings Or	nline Panel				
Settings								
History A	dapters							
	ID	Туре	File	Server	Database	User	Password	
•	0	Volatile						
History N	odes							
	NodeID		NamespaceName	AdapterID	SamplingRate		MaxSamples	

You can use the context menu to create both **History Adapter** and **History Nodes**. If you are connected to a TwinCAT OPC UA Server, you can also conveniently add the nodes to be configured via drag & drop from the **Target Browser** to the **History Nodes**.

C _T	Twin (CAT OPC UA Con	figurator					-		×	
	File	Server									
	1 🖻	🛃 📂 於 V	irtual Machine 1	✓ Edit Conn	ect Disconnect Connect	ion state: connected					
)ata Acc	ess Historical Ac	cess Alarms & Condition	s Security Server Settings	Online Panel						
	Settings										
	_	y Adapters									
		ID	Туре	File	Server	Database	User	Password			
	•	0	Volatile								
	Histor	y Nodes									
			NamespaceName	AdapterID	AdapterID SamplingRate			MaxSamples			
			L.	<u>;</u> ™∓							
			i.	÷							
F		🗄 🗀 AlamsCon	ditione							^	
l		ServerStat									
l		🗄 🕘 BuildIn									
l		≪ <mark>Curren</mark> ⊡-≪⊜ Secon	dsTillShutdown								
l		🗄 🕘 Shutdo									
		iartTi iare State	me								
L		AlamsConditio	ne							~	
L	ogging	gging Target Browser									

Subsequently, a History Node can be linked to the respective History Adapter via the AdapterID.

R)	TwinCAT OPC UA Configurator X												
File	File Server												
	🗋 🚰 🛃 🕍 Virtual Machine 1 🛛 Virtual Machine 1 🖉 Edit Connect Connect Connection state: connected												
Data	Data Access Historical Access Alarms & Conditions Security Server Settings Online Panel												
Settings													
History Adapters													
		ID	Туре		File	Server	Databa	se	User		Password		
		0	Volatile										
	History Nodes												
Γ		NodeID		Namespa	ceName	AdapterID		SamplingRate		MaxSam	ples		
1 þ		i=2258		http://opc	foundation.org/UA/	0		1000		1000			

Double-click on the History Node to open the corresponding configuration dialog.

Configure HistoryNode							
Settings							
NodeID:	i=2258						
NamespaceName:	http://opcfoundation.org/UA/						
AdapterID:	0						
SamplingRate:	1000						
MaxSamples:	1000						
	Ok Cancel						

4.4.7 Configuring Alarms and Conditions

Use the **Alarms & Conditions** tab to configure both the **Condition Controller** and the **Conditions**. A **Condition Controller** is a management unit for organizing the individual **Conditions**. A **Condition** on the other hand reflects a variable which is to be monitored in the sense of **Alarms & Conditions** on the basis of configurable threshold values.

You can use the context menu to create both **Condition Controller** and **Conditions**. If you are connected to a TwinCAT OPC UA Server, you can also conveniently add the nodes to be configured to the **Conditions** via drag and drop from the **Target Browser**.

📓 TwinCAT OPC UA Configurator		-	×
File Server			
🗄 🗋 💣 🛃 📂 Virtual Machine 1 🛛 🗸 Edit Connect Disconnect Connection state: conr	nected		
Data Access Historical Access Alarms & Conditions Security Server Settings Online Panel			
Settings Resources			
Condition Controllers			
Name			
MyConditionController			
Conditions in selected ConditionController			- 1
Name Severity			- 11
N N			
			_
ia- <mark>ia</mark> AlamsConditions ia- ia ServerStatus			^
BuildInfo			
teconds TillShutdown			
ShutdownReason Start Time			
Gradient State			~
Logging Target Browser			

A **Condition** is always added to the currently selected **Condition Controller**. When using drag and drop, the configuration dialog of a **Condition** opens automatically.

Condition General Name: 2258 Severity: 0	×						
Name: 2258							
Severity: 0							
Node settings							
Identifier: i=2258							
NamespaceName: http://opcfoundation.org/UA/							
SamplingRate: 0							
Alam type							
LimitAlarmType OffNormalAlarmType							
LimitAlarm Type settings							
Alam text ID:	Detected languages:						
HighHighLimit:							
HighLimit:							
LowLimit: ~							
LowLowLimit:							
OffNormalAlarmType settings							
OffNormalAlarmType settings							
Alarm text ID:	Detected languages:						
	Detected languages:						
Alarm text ID:	Detected languages:						

The alarm texts to be configured when selecting the respective **AlarmType** can be selected via the corresponding drop-down boxes. Please note that the alarm texts must already be available. Read the chapter <u>Configuring alarm texts</u> [\blacktriangleright 51] to learn more about this topic.

4.4.8 Configuring alarm texts

Within the **Alarms & Conditions** area, you can configure alarm texts via the **Resources** tab, which you can then use for a Condition.

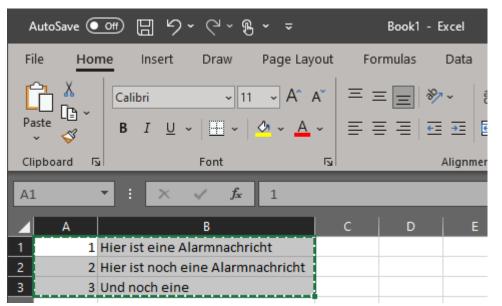
TwinCAT OPC UA Configurator	_	\times
File Server		
🗄 🗋 Թ 🛃 📔 💒 Virtual Machine 1 🛛 🗸 Edit 🕴 Connect 🛛 Disconnect 🖉 Connection state: connected		
Data Access Historical Access Alarms & Conditions Security Server Settings Online Panel		
Settings Resources		
Language files		



1. You can add a new alarm text file via the context menu. These files are grouped according to the language for which the alarm texts are defined.

Langua	Language file ×								
Settings									
Langu	lage: en-US	~							
	ID	Text							
	1	This is an alarm message							
	2	This is another alarm message							
	3	And another one							
b #									
0	k Cancel	Paste from clipboard							

2. The **Paste from clipboard** button can be used to copy ID and text from an Excel spreadsheet by first copying them to the clipboard (CTRL+C) and then importing them via the button.



Language file X								
Settings								
Langu	lage: de-DE	\sim						
	ID	Text						
	1	Hier ist eine Alamnachricht						
	2	Hier ist noch eine Alamnachricht						
	3	Und noch eine						
b #								
0	Ok Cancel	Paste from clipboard						

⇒ After configuring the language files, you can use the alarm texts on a Condition.



Condition								
General								
Name:	2258							
Severity:	0	* *						
Node settings								
ldentifier:	i=2258							
NamespaceName: http://opcfoundation.org/UA/								
SamplingRate:	0	-						
Alam tunc								
Alarm type	0	_						
LimitAlarm Type	 OffNormalAla 	ттуре						
LimitAlarmType settings								
- LimitAlarm Type se	ttings		10	B				
	_	Alarm text		Detected languages:				
HighHighLimit:	10	1	~	en-US,de-DE				
HighHighLimit: HighLimit:	10 20	1 2	~	en-US,de-DE en-US,de-DE				
HighHighLimit:	10 20 0	1 2 3	~	en-US,de-DE en-US,de-DE en-US,de-DE				
HighHighLimit: HighLimit:	10 20	1 2	~	en-US,de-DE en-US,de-DE				
HighHighLimit: HighLimit: LowLimit: LowLowLimit:	10 20 0 -10	1 2 3	~	en-US,de-DE en-US,de-DE en-US,de-DE				
HighHighLimit: HighLimit: LowLimit:	10 20 0 -10	1 2 3 1	× × ×	en-US,de-DE en-US,de-DE en-US,de-DE en-US,de-DE				
HighHighLimit: HighLimit: LowLimit: LowLowLimit: OffNormalAlarmTy	10 20 0 -10	1 2 3	× × ×	en-US,de-DE en-US,de-DE en-US,de-DE				
HighHighLimit: HighLimit: LowLimit: LowLowLimit:	10 20 0 -10	1 2 3 1	× × ×	en-US,de-DE en-US,de-DE en-US,de-DE en-US,de-DE				
HighHighLimit: HighLimit: LowLimit: LowLowLimit: OffNormalAlarmTy	10 20 0 -10	1 2 3 1	× × × × ×	en-US,de-DE en-US,de-DE en-US,de-DE en-US,de-DE				

Using the **Detected languages** fields, you can quickly check whether you have defined the selected AlarmtextID for all languages, or whether a language may have been forgotten.

4.4.9 Configuring endpoints

The endpoints of the OPC UA Server indicate which security mechanisms are to be used during the connection establishment of a client. These range from "unencrypted" to "encrypted and signed", based on different key strengths.

The endpoints can be activated and deactivated using the configurator. It may be useful to deactivate the unencrypted endpoint so that all clients can only connect themselves with valid certificates that are classified as trustworthy.

The **Server Settings** tab allows you to configure the endpoints, as well as some additional parameters. The context menu can be used to add or remove endpoints from the configuration.

ŝ	TwinCA		PC UA Configurator				_	×
F	ile S	erve	r					
1) 💕 🕻		篖 🔐 Virtual Machine 1 🛛 🗸 Edit Connect Disconn	ect	Connection state: o	connected		
Da	ata Acces	s H	Historical Access Alarms & Conditions Security Server Settings Online Panel	ī				
	Endpoint							
	Genera	lsett	ings		Ovenides			
	General settings				ovendes			
	Server port: 4840				Disable Application URI check			
					Allow deprecated security policies			
					Automatically t			
	Security	setti	ings					
			SecurityPolicy					
	•		http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256	_		1		
		<u> </u>	http://opcfoundation.org/UA/SecurityPolicy#Aes256_Sha256_RsaPss		Add			
			http://opcfoundation.org/UA/SecurityPolicy#Aes128_Sha256_RsaOaep		Remove			
		-	http://opcioundation.org/ 0/v/Security/ oncy#/les/120_Sha230_hsa0aep		Edit			- 11
					Move up			
					Move down			
				_		·		

4.4.10 Trust relationship for certificates

The trust relationships for client certificates on the TwinCAT OPC UA Server can be configured via the **Online Panel** tab and the **Certificates** section there. By selecting a client certificate in the respective TrustStore (Rejected/Accepted), certificate details can be displayed and moved between the TrustStores.

TwinCAT OPC UA Configurator	— C	x c
File Server		
🗋 📴 🛃 📔 😭 Virtual Machine 1 🛛 🗸 Edit 🛛 Connect 🛛 Disconnect 🖉 Connection state: connect	nected	
Data Access Historical Access Alarms & Conditions Security Server Settings Online Panel		
Server information Device States Certificates Logging		
Trust store for client certificates Rejected client certificates: Accepted client certificates:	Server certificate	
UaExpert@SvenG-NB06 [AAC6E3C0C3619211AC879929 > TcOpcUaConfiguratorV3 [703D5A5153DE45713A54987.	Common name: TcOpcUaServer@DESKTOP-PDTN3	
COpcUaGateway@DESKTOP-PDTN351 [8874FC8B7F1	Thumbprint: 5CE0BC7831D03147D2EA26A3AE36	
<	Application URI: um:BeckhoffAutomation:TcOpcUaSer	
	Valid from: 13.12.2021 14:11:46	
ο	Valid to: 08.12.2041 14:11:46	
	Delete server certificate	
< > × < >		
Selected certificate		
Common name: TcOpcUaGateway@DESKTOP-PDTN Valid from: 13.12.2021 14:12:10		
Thumbprint: 8874FC8B7F7351827F8D414C9D5FE Valid to: 08.12.2041 14:12:10		
Application URI: um:BeckhoffAutomation:TcOpcUaGat		
Application URI: um:BecknotrAutomation:1cupcuaGat		
Date/Time Message		^
In 16.12.2021 07:44:14 Successfully refreshed certificate list		
0 16.12.2021 07:44:14 Successfully moved certificate to rejected list		
16.12.2021 07:43:32 Successfully refreshed certificate list 16.12.2021 07:43:20 Successfully connected to server!		
16.12.2021 07:43:20 Successfully connected to serven 16.12.2021 07:40:08 Successfully refreshed certificate list		
16.12.2021 07:39:09 Successfully refreshed certificate list		
16 12 2021 07:39:08 Successfully refreshed certificate list		~
Logging Target Browser		

4.4.11 Configuring security settings

Security settings can be made on the server via the **Security** tab. These security settings may include the following items:

- Users and groups
- Access rights for groups to namespaces
- · Access rights for groups to individual nodes

R	TwinCAT OPC UA Conf	figurator				-		\times
Fil	e Server							
1	📔 🛃 💕 🔛 Vii	tual Machine 1	ana stina stata					
_			innection state: c	onnected				
Dat	ata Access Historical Access Alarms & Conditions Security Server Settings Online Panel							
U	Users/Groups Node permissions							
	Users							
ΙI	-			_				
	-							
	Sven		Guests	Users	Administrators			
	Anonymous user							
	A statistic statistics							
	Operating system	user						
	Server user							
	Date/Time	Message						^
		Successfully read configuration from server						
		Successfully connected to server!						
		Successfully refreshed certificate list						
		Found device http://Beckhoff.com/TwinCAT/TF6100/Server/Configuration						_
		Found device um:BeckhoffAutomation:Ua:AC Found device um:BeckhoffAutomation:Ua:HA						_
Ğ		Found device um:BeckhoffAutomation:Ua:HA Found device um:BeckhoffAutomation:Ua:Types:GlobalTypes						~
_		Found device unit becknoll automation 10a. Types Global Types	1					
Log	ging Target Browser							

Users and groups

To configure access rights, users and user groups must first be created. Some groups are already predefined when the server is delivered. New users or groups can be added to the configuration via the context menu.

A user can be either the anonymous user, an operating system user or a server user. In any case, we recommend the configuration of operating system users.

A user group can have a so-called **default access** configured. These are access rights to a specific namespace.

Access rights to namespaces

Access rights to certain namespaces can be defined at a user group. In the settings of the group there is a corresponding configuration area, which can be edited via the context menu.

GroupDetails					×	
Group details			Namespace access			
Name:	Users		NamespaceName		Access	
Member of group(s):	Guests	•	um:BeckhoffAutoma	ation:TcOpcUaServer	UA_ATTRREADABLE, UA_READABLE, UA_BROWSEABLE	
	Users Administrators		http://opcfoundation	n.org/UA/DI/	UA_ATTRREADABLE, UA_READABLE, UA_BROWSEABLE	
	Administrators		http://PLCopen.org/OpcUa/IEC61131-3/		UA_ATTRREADABLE, UA_READABLE, UA_BROWSEABLE	
			um:BeckhoffAutomation:Ua:Types:GlobalTypes		UA_ATTRREADABLE, UA_READABLE, UA_BROWSEABLE	
			http://Beckhoff.com/TwinCAT/TF6100/Server/Configuration		UA_ATTRREADABLE, UA_READABLE, UA_BROWSEABLE	
			um:BeckhoffAutomation:Ua:AC		UA_ATTRREADABLE, UA_READABLE, UA_BROWSEABLE	
			Add	n:Ua:HA	UA_ATTRREADABLE, UA_READABLE, UA_BROWSEABLE	
			Remove	noffAutomation:Ua:PLC1	UA_PERMISSION_ALL	
			Edit			
	Ok Cancel	l	Luit			

Configure DefaultAcce	Configure DefaultAccess X							
DefaultAccess details								
Available namespaces:	http://opcfoundati	on.org/UA/	~]				
NamespaceName:	um:BeckhoffAutomation:TcOpcUaServer]				
Permissions								
🗌 Ali	Read attribute	Browse	History modify	Method call				
	Read value	✓ History read	History delete	Write attribute				
	Write value	History insert	Receive events					
	Ok Ca	ancel						

Access rights to individual nodes

The **Node permissions** tab can be used to define access rights to individual nodes and their child elements. You can configure the nodes manually via the context menu or conveniently add them to the configuration by dragging and dropping them from the **Target Browser**, provided you are connected to a server.

TwinCAT OPC UA Configurator	_	×
File Server		
🗄 🗋 🚰 🛃 📂 🔐 Virtual Machine 1 💎 Edit Connect Disconnect Connection state: connected		
Data Access Historical Access Alarms & Conditions Security Server Settings Online Panel		
Users/Groups Node permissions		
Pemissions NamespaceName		
NouerD NamespaceName		
AamsConditions		^
- ServerStatus		
BuildInfo CurrentTime		
Seconds Till Shutdown ShutdownReason		
B-G StartTime		
AdmsConditions		 ~
Logging Target Browser		

The user groups and access rights of the respective group can then be defined in the node configuration dialog.

Noden	ermission		_		×	
					^	
Genera	l settings					
Nodel	D:	i=2258				
Name	spaceName:	http://opcfounda	tion.org/UA/			
Depth:		-1				
Groups	Groups					
	Name		Access			
		Add				
		Remove				
		Edit				
		Edit				
C)k	Cancel				

You can use the parameter **Depth** to set whether the permissions should be inherited by child elements. The value "-1" indicates that all child elements should inherit the permissions.

4.4.12 Restarting the server

A TwinCAT OPC UA Server can be restarted via the **Server** menu. Usually you want to restart the server that is just connected via OPC UA. Alternatively, you can trigger the restart via ADS if you have established an ADS route to the server system.

😭 Twin	🔛 TwinCAT OPC UA Configurator						
File	Server		N				
i 🗋 💕	Open from target	1	onnect Connection state: connected				
Data Ac Setting	Symbol Files	Conditions Security Server Settings Online Pa	anel				
Devi							
	Shutdown	AmsNetId	AdsPort				
•	Restart via ADS	127.0.0.1.1.1	851				
	Shutdown via ADS						

4.4.13 Logging

For an advanced diagnostics you can activate the logging function of the OPC UA Server.



Writing the log file

Activating the logging function on the server causes a log file to be written on the file system. Make sure that there is sufficient storage space available and set the logging parameters accordingly (number of log files, size per log file).

Performance and timing behavior

Activation of the logging function will change the timing behavior of the OPC UA Server. As a result there may be losses of speed, depending on the platform and project.

The server logging functions can be activated via the **Online Panel** tab and the **Logging** section there.

TwinCAT OPC UA Configurator	– 🗆 X									
File Server										
🗄 🗋 💕 🛃 📂 🔛 Virtual Machine 1 🤍 Edit Connect 🛛 Disconnect	Connection state: connected									
Data Access Historical Access Alarms & Conditions Security Server Settings Online Panel	Data Access Historical Access Alarms & Conditions Security Server Settings Online Panel									
Server information Device States Certificates Logging	Server information Device States Certificates Logging									
General settings										
Trace file: C:\TwinCAT\Functions\TF6100-OPC										
Number of trace files: 5										
Number of entries per file: 100000										
AppTrace	StackTrace									
App Trace level: 7	StackTrace level: 7									
AppTrace enabled: False	Stack Trace enabled: False									
Activate Deactivate	Activate Deactivate									

Trace Level

In general, the higher the trace level, the more detailed (and more) data is written, but the more load is also placed on the server application, which changes the timing behavior accordingly. Please therefore only activate logging in the event of diagnostics and in consultation with Beckhoff Support.

Activate App Trace

In most cases it is sufficient to create a so-called "AppTrace". This logs information from the server application. To activate the AppTrace, please enter the number of TraceFiles and the number of entries per TraceFile in the corresponding text fields. Then select a trace level and click the button to activate the AppTrace. The values in the gray text boxes represent the current settings on the server.

Activate Stack Trace

In a few cases it is also necessary to create a so-called "StackTrace", whereby information from the OPC UA stack is logged. To activate the StackTrace please enter the number of TraceFiles as well as the number of entries per TraceFile into the corresponding text boxes. Then select a trace level and click on the button to activate the StackTrace. The values in the gray text boxes represent the current settings on the server.

5 Appendix

5.1 ADS Return Codes

Grouping of error codes:

Global error codes: <u>ADS Return Codes</u> [▶ <u>60</u>]... (0x9811_0000 ...) Router error codes: <u>ADS Return Codes</u> [▶ <u>60</u>]... (0x9811_0500 ...) General ADS errors: <u>ADS Return Codes</u> [▶ <u>61</u>]... (0x9811_0700 ...) RTime error codes: <u>ADS Return Codes</u> [▶ <u>63</u>]... (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 INVALID//COESC	Parameter size not correct.
0x705	1798	0x98110706	ADSERR DEVICE INVALIDBATA	Invalid data values.
0x707	1799	0x98110707	ADSERR DEVICE NOTREADY	Device is not ready to operate.
0x707	1800		ADSERR DEVICE BUSY	Device is hor ready to operate.
0x708	1800	0x98110708		,
0x709	1001	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.
0x71A	1819	0x9811071B	ADSERR DEVICE INVALIDINTERFACE	Wrong interface requested.
0x71C	1820			Class ID is invalid.
0x71C	1821	0x9811071C 0x9811071D		
0x71E	1822	0x9811071E		Object ID is invalid.
	1823	0x9811071E		Request pending.
0x71F				Request is aborted.
0x720	1824	0x98110720		Signal warning.
0x721	1825	0x98110721		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 INVALIDENCID	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.
07120	1040	0790110130		

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			

5.2 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 <u>download finder</u> 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 <u>local support and service</u> on Beckhoff products!

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

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/TS6100

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

