

Industry Online Support

NEWS

0

OPC UA Connection between two WinCC V7.5 Computers

WinCC / V7.5

https://support.industry.siemens.com/cs/ww/en/view/109479664

Siemens Industry Online Support



This entry is from the Siemens Industry Online Support. The general terms of use (<u>http://www.siemens.com/terms_of_use</u>) apply.

Security Siemens provides products and solutions with industrial security functions that support the informasecure operation of plants, systems, machines and networks. tion In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement - and continuously maintain - a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to

secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Table of content

1

OPC L	JA Connection between two WinCC V7.5 Computers	3
1.1	General Configuration Steps	3
1.1.1	Start the OPC UA Server.	3
1.1.2	Configure the OPC UA Client	3
	1.1.2.1 Add the OPC UA Channel	4
	1.1.2.2 Create a New Connection	4
	1.1.2.3 Security Settings	7
	1.1.2.4 Create OPC UA Tags	7
1.2	Additional Steps for Secure Communication	10
1.2.1	Enable Security Settings	10
1.2.2	Exchange of Certificates	
1.2.3	Validity of Certificates	
1.2.4	Change the Port Number on the OPC UA Server	16
1.3	Necessary WinCC Licenses	16

Siemens 2020 All rights reserved

0

1 OPC UA Connection between two WinCC V7.5 Computers

The procedures for configuring an OPC UA connection between two WinCC V7.5 stations are described in the following. Here, current process values are to be exchanged, this means that only the DA (Data Access) part of the OPC UA specification is used here.

First, we show the general configuration steps for unsecured communication. In the second step we secure the communication.

1.1 General Configuration Steps

A WinCC station is to be operated as an OPC UA server. The computer name of the station in this example is "VMSITRAIN".

A second WinCC station is supposed to access tags from the OPC UA server and is therefore the OPC UA client. The computer name of the second station in this example is "VCLIENT02".

1.1.1 Start the OPC UA Server

In order for the OPC UA server to run, the WinCC Runtime must be enabled on the PC "VMSITRAIN". This is necessary so that the OPC UA client can later access the tags and also so that the OPC UA client can search the OPC UA server for tag names.

1.1.2 Configure the OPC UA Client

The further configuration steps are executed on the PC that is to run as OPC UA client. In our example "VCLIENT02".

1.1.2.1 Add the OPC UA Channel

In the WinCC project of the OPC UA client you open the Tag Management. Via "Add new driver" you add the channel named "OPC UA WinCC Channel" to your project.

Figure	1-1
--------	-----

....

ag Managem	ent		~	📦 Tags [All]
III Tag Manage	ŀ	Add new driver 🔸	SIMA	ATIC S7 Protocol Suite
Structure ta		Copy Paste	SIMA	ATIC S5 Serial 3964R
	*	Export	SIMA SIMA	ATIC S5 Programmers Port AS511 ATIC S5 Profibus FDL ATIC S5 Ethernet Laver 4
			SIM/ SIM/ SIM/	ATIC TI Serial ATIC TI Ethernet Layer 4 ATIC 505 TCPIP
			Aller Mits Mod	n Bradley - Ethernet IP ubishi Ethernet Ibus TCPIP
			OPC	UA WinCC Channel
			Profi Simo	bus DP otion

1.1.2.2 Create a New Connection

Add a new connection via the "New Connection" pop-up menu and assign it the name "OPC_Server".

File	Edit	View	Too <u>l</u> s	<u>H</u> elp			
Тас	g Man	agem	ent		«		Tage
-	Tag l	Manage	ment				Nam
G	- 🤫 lı	nternal t	ags			1	派
E	- J. C	PC UA	WinCC (Channel		2	
	L.	OPC	UA Con	nection	11	3	5
	Struc	ture tag	ļs	101	New Connectio	n	
					Сору	- 00	
					Paste		
					88		

Select the menu item "Connection Parameters".

Figure 1-3

Tag Management		~		Tags [
- Tag Management				Name
🗄 💝 Internal tags			1	派
🖃 📙 OPC UA WinCO	Channe	el	2	
🗄 - 👖 OPC UA Co	nnectior	ıs	3	
OPC_Se	rver		4	
Structure tags	8	New Group		
	-	Сору		
	8	Paste		
		Delete		
		Rename		
	*	Export		
	P	Connection Paramet	ers	N
		Create Enable/Disabl	le Tag	IS
		Browse OPC server		
		AS Symbols		

In the mask that opens you must enter a new OPC UA server under "Custom Discovery". Only the local OPC UA servers are displayed directly. This step is necessary because the OPC UA server in our example is running on another PC.

Figure 1-4

⊡ III UA Server Discover □ III Local Discovery □ III Local Discovery □ III Custom Discover □ III Custom Discover □ III Custom Discover	y C UA Server fo ay sk to add serve	or IDB	Connection name: Server URI: Security settings – Security Policy:		
	Add N Server opc.t	ew Server cp://vmsitrain	OK	Cancel	
Time stamp	Type	Message			
2020-10-19 09:28:03.552 2020-10-19 09:21:39.192 2020-10-19 09:21:39.098 2020-10-19 09:21:39.020	Information Information Information Information	Get Server En Discovery of L Browsing local Successfully c	dPoints Succeeded. Ja Servers Succeeded. servers initiated. reated Connection paramet	er.	

Here you enter "opc.tcp://vmsitrain" and close the mask with OK.

It is not necessary to enter the port number 4840, it is added by the system. You can see the result in Figure 1-5.

1.1.2.3 Security Settings

Figu	re 1	-5
i iyui	6 1	-0

	•		None None ttings vord:	Security Policy: Security mode: Authentication set Authentication set Anonymous: User name/Passw	er for IDB er for WinCC >	nsitrain:4840 OPC UA Serve OPC UA Serve k to add server	E. , opc.tcp://w Siemens Siemens Couble clic
The stars		1			Massaga	Tune	E 💼
2020-10-19 09:34:27.147 Information Get Server EndPoints Succeeded.	- î		Message Get Server EndPoints Succeeded.			Information	2020-10-19 09:34:27.147
2020-10-19-09:33:17.052 Information Discovery of Us Servers Succeeded.			d.	a Servers Succeeded. rain:4840 has been addeo	Discovery of Ua opc.tcp://vmsit	Information Information	2020-10-19 09:33:17.052 2020-10-19 09:33:16.771
ZUZU-TU-TO-US.SS.TO.771 Information Opc.tcp.//vmsitrain.4640 has been added.			opc.tcp://vmsitrain:4840 has been added. Get Server EndPoints Succeeded.				2020-10-19 09:28:03.552
2020-10-19 09:28:03.552 Information Get Server EndPoints Succeeded.					Discovery of Us	Indiana and in an	-NUNUER 10 00.01.00 100

Initially, we will leave the security settings and authentication settings unchanged. These will then be enabled in section 1.2 "Additional Steps for Secure Communication".

With the server URL, the standard port "4862" is added automatically. "opc.tcp://vmsitrain:4862".

1.1.2.4 Create OPC UA Tags

In the pop-up menu of the connection you select "Browse OPC server".

Figure 1-6

Tag Management - WinCC Configuration Studio							
<u>F</u> ile <u>E</u> dit <u>V</u> iew Too <u>l</u> s <u>H</u> elp							
Symbols 📮 <	< A	S Symbo	ls [S7150	Find			
⊡#9 OPC_Server		Access	Modified	Node Id	Node Class	Browse Name	Name
🗄 🏘 Server	1			ns=1;s=t	Variable	1:DB_Tank1_	DB_Tank1_Temperature
🗄 🇁 WinCC	2		(m)	ns=1;s=t	Variable	1:DB_Tank1_B	DB_Tank1_EmptyingActive
DCALMACHINE::	3	1		ns=1;s=t	Variable	1:DB_Tank1_T	B_Tank1_TankEmpty
internal tags	4		Ē	ns=1;s=t	Variable	1:DB_Tank1_F	😝 DB_Tank1_FillLimitReached
Hold List of all structure instances	5	V		ns=1;s=t	Variable	1:DB_Tank1_F	DB_Tank1_FillingActive
List of all tags	6			ns=1;s=t	Variable	1:DB_Tank1_/	😝 DB_Tank1_ActualFillLevel
	7			ns=1;s=t	Variable	1:DB_Tank1_S	📦 DB_Tank1_Statusword
SIMATIC S7, 1200, S7, 1500 Chapped	8	V		ns=1;s=t	Variable	1:DB_Tank1_0	DB_Tank1_OnOff
SIMATIC 37-1200, 37-1300 Channel	9		1	ns=1;s=t	Variable	1:DB_Tank1_M	😝 DB_Tank1_MaxFillLevel
	10			ns=1;s=t	Variable	1:DB_Tank1_F	DB_Tank1_FlowTime
S/1500_PLCSIM	11			ns=1;s=t	Variable	1:DB_Tank1_F	😝 DB_Tank1_FillTime
Ima SIMATIC S/ Protocol Suite	12	V	Ē	ns=1;s=t	Variable	1:DB_Tank1_S	😝 DB_Tank1_SetFillLevel
	13						

Here you can see all the tags of the WinCC project on the OPC UA server. Navigate to the tags that you want to show on the OPC UA client and enable the corresponding option fields in the "Access" column. In the example above we have selected tags from an S7-1500 connection.

If you wish to see only those tags just created, you switch from the Symbols view back to the Tag Management and go to "Tags".

Figure 1-7

1 2 3 4	Name DB_Tank1_ActualFillLevel DB_Tank1_FillingActive DB_Tank1_OnOff	Comment	Data type Signed 16-bit valu Binary Tag
1 2 3 4	DB_Tank1_ActualFillLevel DB_Tank1_FillingActive DB_Tank1_OnOff		Signed 16-bit valu Binary Tag
2 3 4	DB_Tank1_FillingActive DB_Tank1_OnOff		Binary Tag
3	DB_Tank1_OnOff		
4			Binary Tag
-	DB_Tank1_SetFillLevel		Signed 16-bit val
5	DB_Tank1_TankEmpty		Binary Tag
6	*		
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
- <u>17</u>	► H Groups Tags AS structures	ļ	
	6 7 8 9 10 11 12 13 14 15 16 16 7 17	6 7 8 9 10 11 12 13 14 15 16 ↓ 17 H ↓ ▶ H Groups Tags AS structures	6 ₩ 7 8 9 10 10 11 12 13 13 14 15 16 17 H ← H Groups Tags AS structures English (Ur

Tip:

You have the option of defining a prefix for the newly created tags. This is useful, for example, if the tag names in the WinCC projects are to have the same name on multiple OPC UA servers. You can define the prefix in the Properties of the connection.

10	Properties - Conn	ection »					
Ξ	Selection						
	Object type	Connection					
	Object name	OPC_Server					
Ξ	General	AP BARAN					
	Name	OPC_Server					
	ID	2					
	Connection Parameters	opc.tcp://VMSITRAIN:4862,3,8,0; <ua2>; 1</ua2>					
Ξ	Assignment	1969 - 1969 - 1969 - 1960 - 1960 - 1960 - 1960 - 1960 - 1960 - 1960 - 1960 - 1960 - 1960 - 1960 - 1960 - 1960 -					
	Communication driver	OPC UA WinCC Channel					
	Channel unit	OPC UA Connections					
Ξ	Various						
	Creator ID	0					
	Last Change	19.10.2020 14:52:56					
Ξ	AS Symbols						
	Prefix						
	Suffix						
	Name structure	Standard					
	Delimiter						

Now you can use the OPC tags in screens, for example. Start Runtime and check whether the connection is established.



ags from OPC UA s	server	Channels/Connections Configuration		
DB_Tank1_OnOff		B-√ OPC UA WinCC Channel └ √ OPC_Server	Counters Server Status ForceConnectionStateEx Data Change Notifications Data Change Notification Synchronous Read Asynchronous Weles Synchronous Read Tags Asynchronous Read Asynchronous Read Asynchronous Read	Value FUNNING ENABLED 45 1 4 3 5 1 0 0 0 5 5 0 0 0 5 5 5 5 5 5 5 5 5 5
DB_Tank1_FillingActive DB_Tank1_TankEmpty	:		Last Activity Last Error Time Last Error Name Last Error in Call LastDataChangeCallBack L. Last Time between CBs	2481 WHEP 2220-10-19 12:32:25 0x80004005 Unbekarnets Fehler Registe/Variables 2220-10-19 12:36:20 1000
DB_Tank1_ActualFillLevel	189,000			

Tip:

On the OPC UA server you have the option of defining write protection for access to the OPC UA client. You do this in the Properties of the tags.

Read and write protection is also possible. In this way you can prevent the tag value from being read by the OPC UA client.

	Properties - Tag		>>
Ξ	Selection	<i>n</i>	
	Object type	Tag	
	Object name	DB_Tank1_EmptyingActive	
Ξ	General		
	Name	DB_Tank1_EmptyingActive	
	Comment		
	ID	320	
	Data type	Binary Tag	
	Length	1	
	Format adaptation		
	AS Length	1	
	Address	0001:TS:0:8A0E0015.E0C31158.13	
	AS tag name	EmptyingActive	
	Name space	DB_Tank1	
Ð	Assignment		
Ŧ	Linear scaling		
Ŧ	Limit Values		
Ŧ	Use Substitute Value		
Ξ	Options		
	Computer-local		
	Synchronization		
	Runtime persistence		
	OPC write protection		
	OPC read protection		
	Good Manufacturing Practices		
Ŧ	Various		
Ŧ	Structure tag element		

1.2 Additional Steps for Secure Communication

1.2.1 Enable Security Settings

You enable the security settings on the OPC UA client as follows.

Enable the Runtime on both computers. In this way both the OPC UA server and the OPC UA client are running.

genschaften von OPC_Sen	ver		
onnection configuration Se	ettings		
Connection name:	OPC_Server		
Server URI:	opc.tcp://VMS	SITRAIN:4862	
Security settings			
Security Policy:	Basic256Sha2	256	•
Security mode:	SignAndEncry	pt	-
Authentication settings Anonymous: User name/Password:			
Authentication settings Anonymous: User name/Password:			
Authentication settings Anonymous: User name/Password:	Туре	Message	
Authentication settings Anonymous: User name/Password: User name/Password: Time stamp 2020-10-19 12:43:02.231 2020-10-19 12:43:02.209	Type Information Information	Message Get Server EndPoints Succeeded. Successfully created Connection param	eter.

In this example we have selected "Basic256Sha256" as "Security Policy" and "SignAndEncrypt" as "Security mode". This is the highest security level available.

Alternatively you can select "None", "Basic128Rsa15" or "Basic256" as security policy.

You can also select "Sign" instead of "SignAndEncrypt" for the security mode. Signing protects data from manipulation. Encrypting protects against spying because you cannot gain knowledge of the content if you are not authorized.

Tip:

The FAQ response entitled "How do SIMATIC and SITOP products support communication via OPC UA?" gives you an overview of which products support which features of OPC UA communication (security policy, for example): https://support.industry.siemens.com/cs/en/en/view/109763315

After the above changes, the connection between OPC UA server and client is terminated. Further steps are necessary to re-establish the connection.

1.2.2 Exchange of Certificates

For secure communication, security certificates must be exchanged between the OPC UA server and the OPC client.

The situation prior to the enabling of secure communication is as follows with regard to certificates.

The paths all refer to the installation directory of WinCC. By default this is C:\Programs (x86)\Siemens\WinCC\....

The certificates have the ending *.der and were generated during the installation of WinCC. The complete name of the certificate is, for example, "Siemens OPC UA Server for WinCC [6AEEEC2EDBDA591A5F9E7F703B8C18785DB0689C].der". The square brackets show the so-called fingerprint (40 characters) of the certificate. This is unique and will look different on your installation. In the following figures the names of the certificates have been shortened.

The two certificates marked in gray are available, but are not relevant in this configuration.

Figure 1-12

WinCC OPC UA Server	WinCC OPC UA Client
\WinCC\opc\UAServer\PKI\CA\certs	\WinCC\opc\UAServer\PKI\CA\certs
Siemens OPC UA Server for WinCC [6A].der	Siemens OPC UA Server for WinCC [9F].der
\WinCC\opc\UAServer\PKI\CA\rejected\certs	
\WinCC\opc\UAClient\PKI\OPCUA\certs	\WinCC\opc\UAClient\PKI\OPCUA\certs
Siemens OPC UA Client for WinCC Runtime [D2].der	Siemens OPC UA Client for WinCC Runtime [BA].der
	\WinCC\opc\UAClient\PKI\Rejected\certs
	\WinCC\opc\UAClient\PKI\Trusted\certs

The following steps are necessary after enabling secure communication.

(1) The certificate of the OPC UA server was automatically copied from

C:\Programs (x86)\Siemens\WinCC\opc\UAServer\PKI\CA\certs to the OPC UA client C:\Programs (x86)\Siemens\WinCC\opc\UAClient\PKI\Rejected\certs.

(2) Then you have to manually move the certificate on the OPC UA client from

...\WinCC\opc\UAClient\PKI\Rejected\certs to

...\WinCC\opc\UAClient\PKI\Trusted\certs.

Figure 1-13

WinCC OPC UA Server	WinCC OPC UA Client
\WINCC\opc\UAServer\PKI\CA\certs	\WINCC\opc\UAServer\PKI\CA\certs
Siemens OPC UA Server for WinCC [6A].der	Siemens OPC UA Server for WinCC [9F].der
\WinCC\opc\UAServer\PKI\CA\rejected\certs	
\WinCC\opc\UAClient\PKI\OPCUA\certs	\WinCC\opc\UAClient\PKI\OPCUA\certs
Siemens OPC UA Client for WinCC Runtime [D2].der	Siemens OPC UA Client for WinCC Runtime [BA].der
	.\WinCC\opc\UAClient\PKI\Rejected\certs
	Siemens OPC UA Server for WinCC [6A].der
	(WinCC) onc) LIAClient' BKI) Tructed Corts
	wince tope to Achenic (FRI) indiced (certs
	Siemens OPC UA Server for WinCC [6A].der

Tip:

On the OPC UA client, in the Connection Parameters mask, if you click the "Certificates" button (see Figure 1-11), you jump directly to the folder C:\Programs (x86)\Siemens\WinCC\ opc\UAClient\PKI. After these two steps further steps are necessary.

(1) The certificate of the OPC UA client was <u>automatically</u> copied from ...\WinCC\opc\UAClient\PKI\OPCUA\certs to the OPC UA server ...\WinCC\opc\UAServer\PKI\CA\rejected\certs. This only happens if the OPC UA server and the OPC UA client are running (Runtime is running on both computers).

(2) Then you have to <u>manually move</u> the certificate on the OPC UA server from ...\WinCC\opc\UAServer\PKI\CA\rejected\certs to ...\WinCC\opc\UAServer\PKI\CA\certs.

Figure 1-14

WinCC OPC UA Server	WinCC OPC UA Client
\WinCC\opc\UAServer\PKI\CA\certs Siemens OPC UA Server for WinCC [6A].der Siemens OPC UA Client for WinCC Runtime [BA].der	\WinCC\opc\UAServer\PKI\CA\certs Siemens OPC UA Server for WinCC [9F].der
\WinCC\opc\U&Server\PKI\CA\rejected\certs	
\WinCC\opc\UAClient\PKI\OPCUA\certs	\WinCC\opc\UAClient\PKI\OPCUA\certs Siemens OPC UA Client for WinCC Runtime [BA].der
	\WinCC\opc\UAClient\PKI\Rejected\certs
	\WinCC\opc\UAClient\PKI\Trusted\certs Siemens OPC UA Server for WinCC [6A].der

After these steps the distribution of the certificates looks like this:

Figure 1-15

WinCC OPC UA Server	WinCC OPC UA Client
\WinCC\opc\UAServer\PKI\CA\certs Siemens OPC UA Server for WinCC [6A].der	\WinCC\opc\UAServer\PKI\CA\certs
Siemens OPC UA Client for WinCC Runtime [BA].der	Siemens OPC UA Server for WinCC [9F].der
\WinCC\opc\UAServer\PKI\CA\rejected\certs	
\WinCC\opc\UAClient\PKI\OPCUA\certs	\WinCC\opc\UAClient\PKI\OPCUA\certs
Siemens OPC UA Client for WinCC Runtime [D2].der	Siemens OPC UA Client for WinCC Runtime [BA].der 🥥
	\WinCC\opc\UAClient\PKI\Rejected\certs
	\WinCC\opc\UAClient\PKI\Trusted\certs
	Siemens OPC UA Server for WinCC [6A].der

After these steps the OPC connection is established.

1.2.3 Validity of Certificates

All the certificates shown above are created new when WinCC is installed. They are valid for 5 years.

You can easily check how long a certificate is still valid by double-clicking the *.der file in Windows Explorer.

Figure 1-16

Details Zertifizierungspfad
Zertifikatsinformationen
s Zertifizierungsstellen-Stammzertifikat ist nicht auenswürdig. Installieren Sie das Zertifikat in peicher vertrauenswürdiger mzertifizierungsstellen, um die auensstellung zu aktivieren.
Ausgestellt für: Siemens OPC UA Server for WinCC
Ausgestellt von: Siemens OPC UA Server for WinCC
Gültig ab 07.02.2019 bis 12.01.2024

You can ignore the statement "This certification authority root certificate is not trustworthy" shown above because the OPC UA server uses its own certificate directory and is independent of the Windows certificate management. For the same reasons you should not use the "Install certificate..." button.

You must renew a certificate before it expires, otherwise the communication will no longer work. More information about this is available in the FAQ response entitled "How do you create or delete CA certificates of the OPC UA server and client in WinCC?"

https://support.industry.siemens.com/cs/ww/en/view/109765628

1.2.4 Change the Port Number on the OPC UA Server

The default port on the OPC UA server with WinCC is "4862" (for example "opc.tcp://vmsitrain:4862").

If it is necessary to change the port number, you can do this in the file "OPCUAServerWinCC.xml" in the directory <WinCC Project Folder>\OPC\UAServer. Further information about this is available in the WinCC Help under "Interfaces > OPC Open Connectivity > WinCC OPC UA Server > Configuration of the WinCC OPC UA Server".

Make sure that your firewall does not hinder communication between server and client. The relevant settings are made automatically when WinCC is installed.

1.3 Necessary WinCC Licenses

If you are using WinCC V7.5 as OPC UA server, you need a "WinCC Connectivity Pack" license in addition to the other licenses (WinCC RT 2048, for example). Without this license an OPC UA client cannot establish a connection.

If you are using WinCC V7.5 as OPC UA client, you do not need any additional license.