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

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
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 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 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.

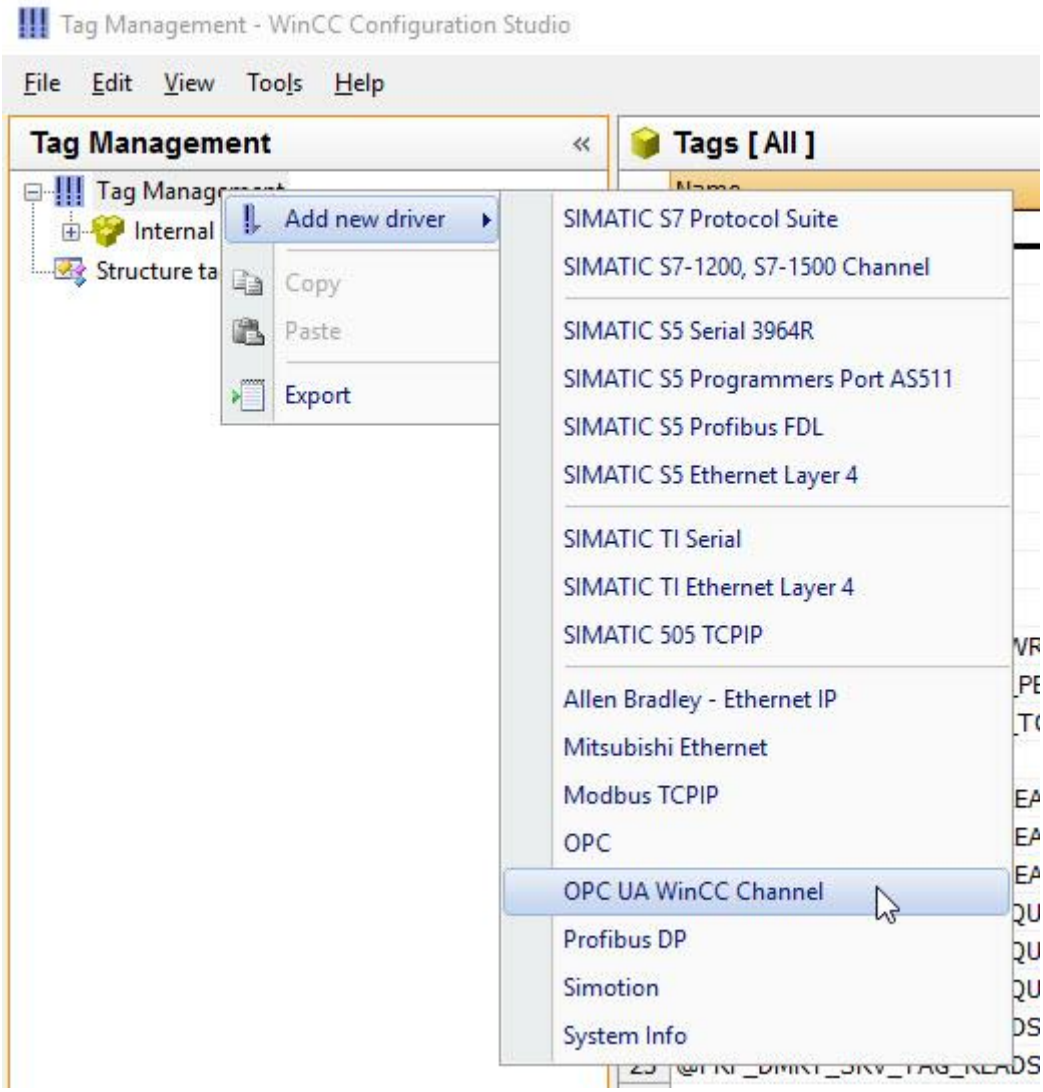
1.1.2 Configure the OPC UA Client

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.

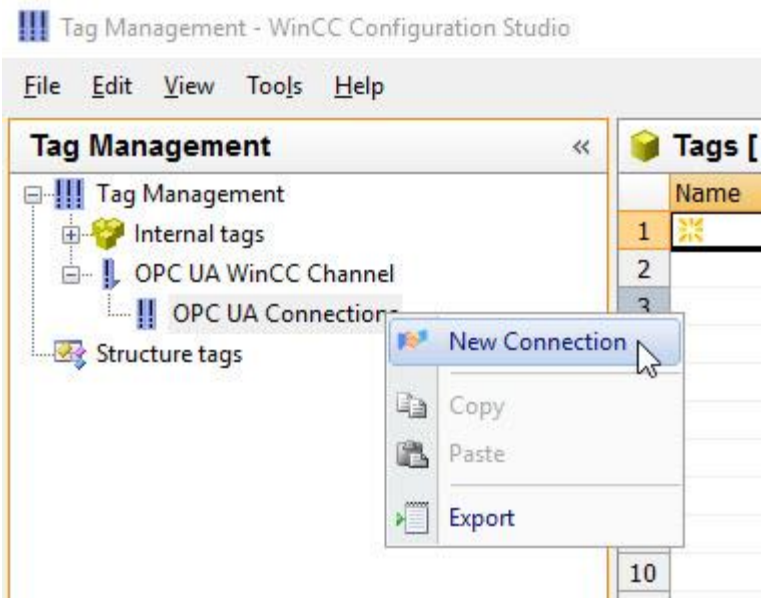
Figure 1-1



1.1.2.2 Create a New Connection

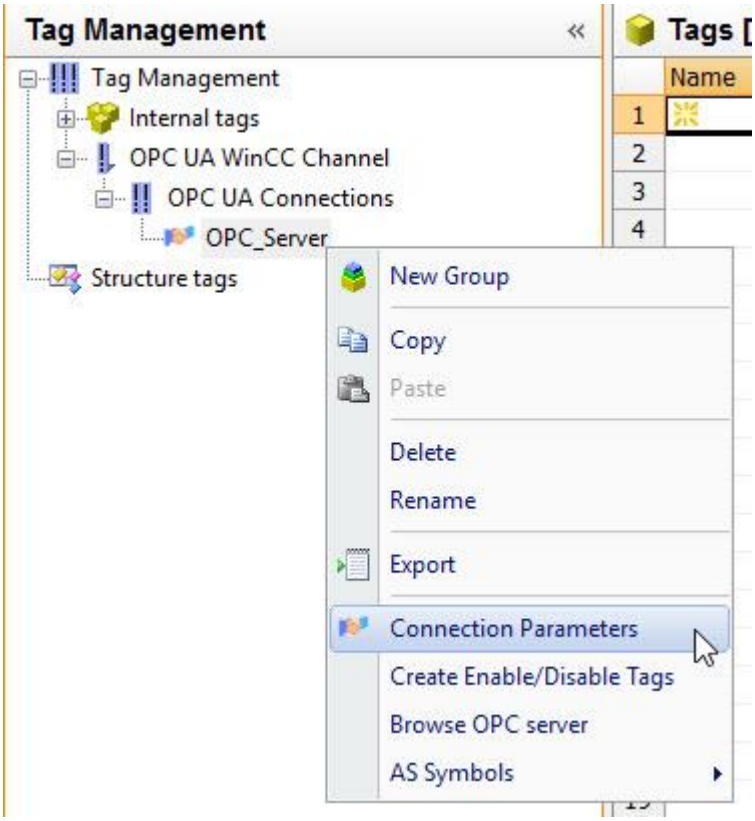
Add a new connection via the "New Connection" pop-up menu and assign it the name "OPC_Server".

Figure 1-2



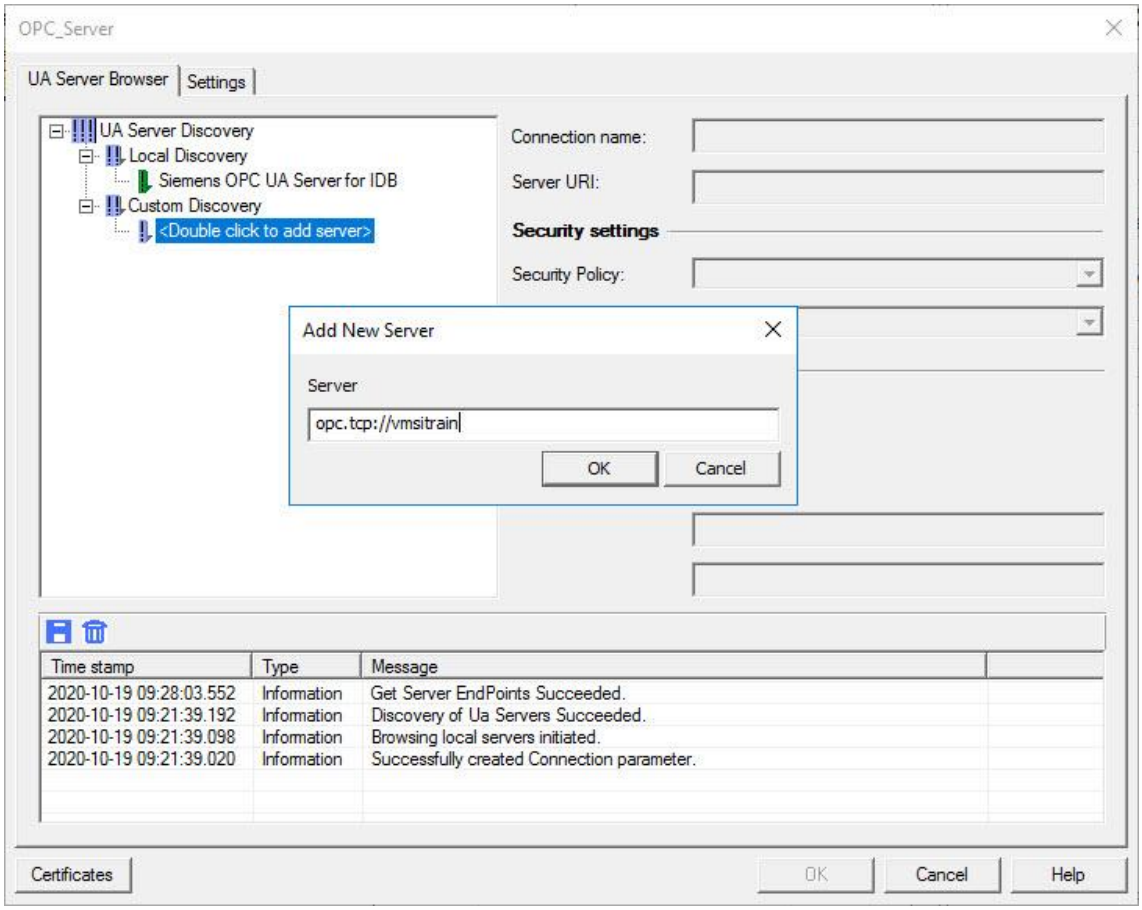
Select the menu item "Connection Parameters".

Figure 1-3



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.

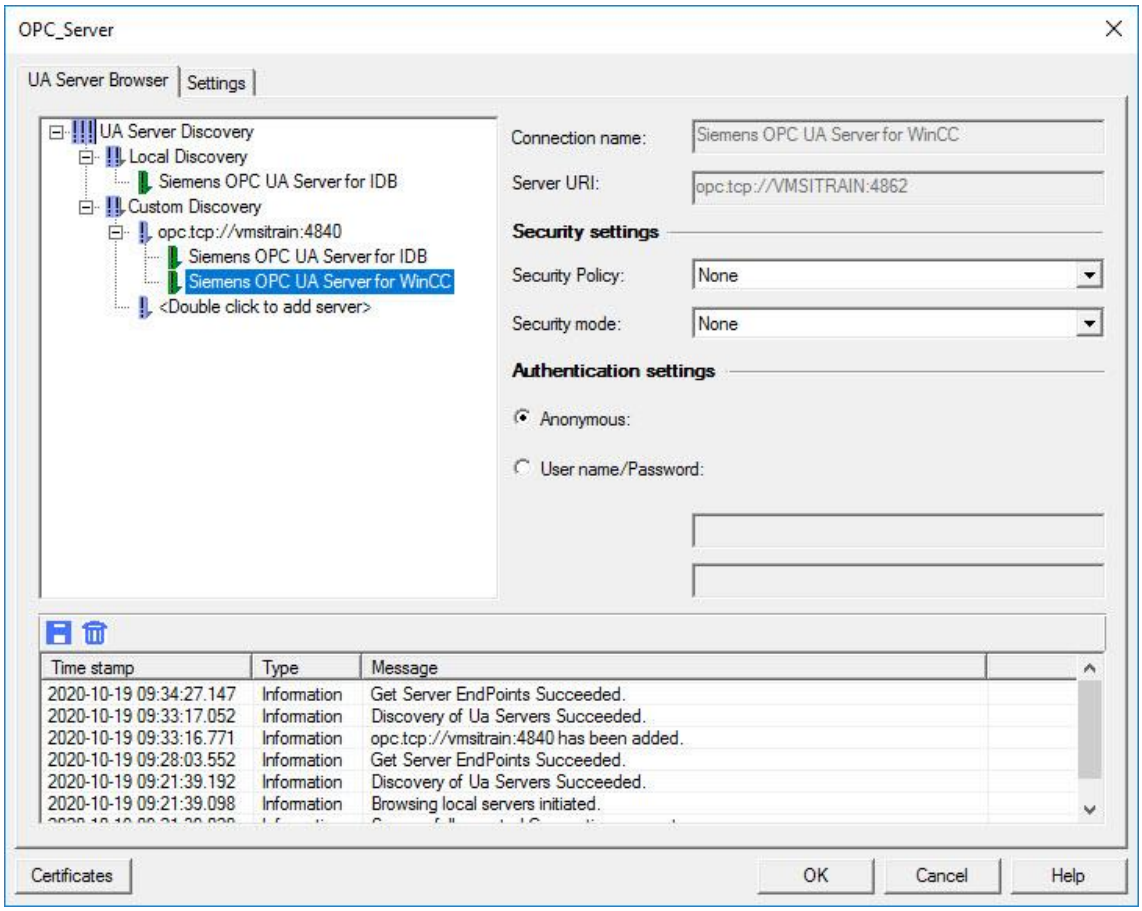
Figure 1-4



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

Figure 1-5



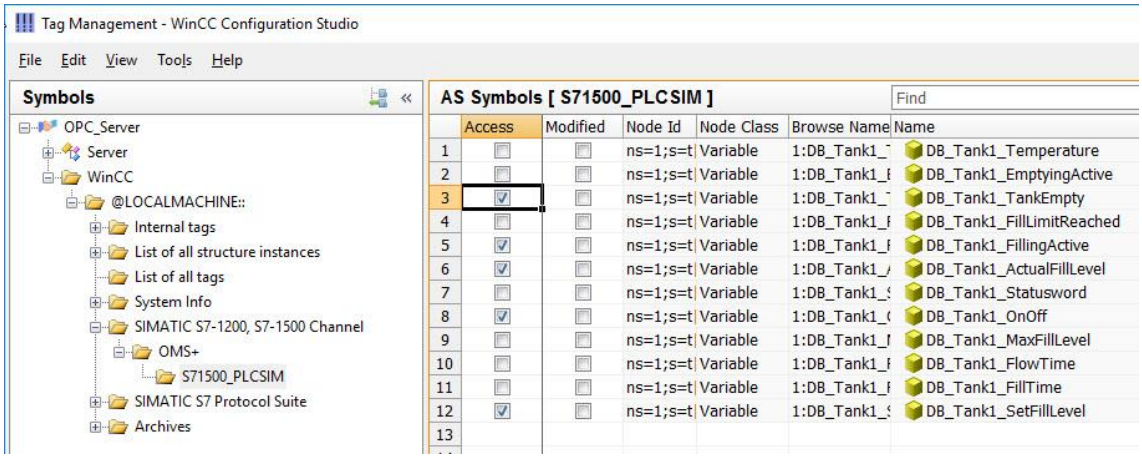
Initially, we will leave the security settings and authentication settings unchanged. These will then be enabled in section 1.2 "Additional Steps for Secure Communication".

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".

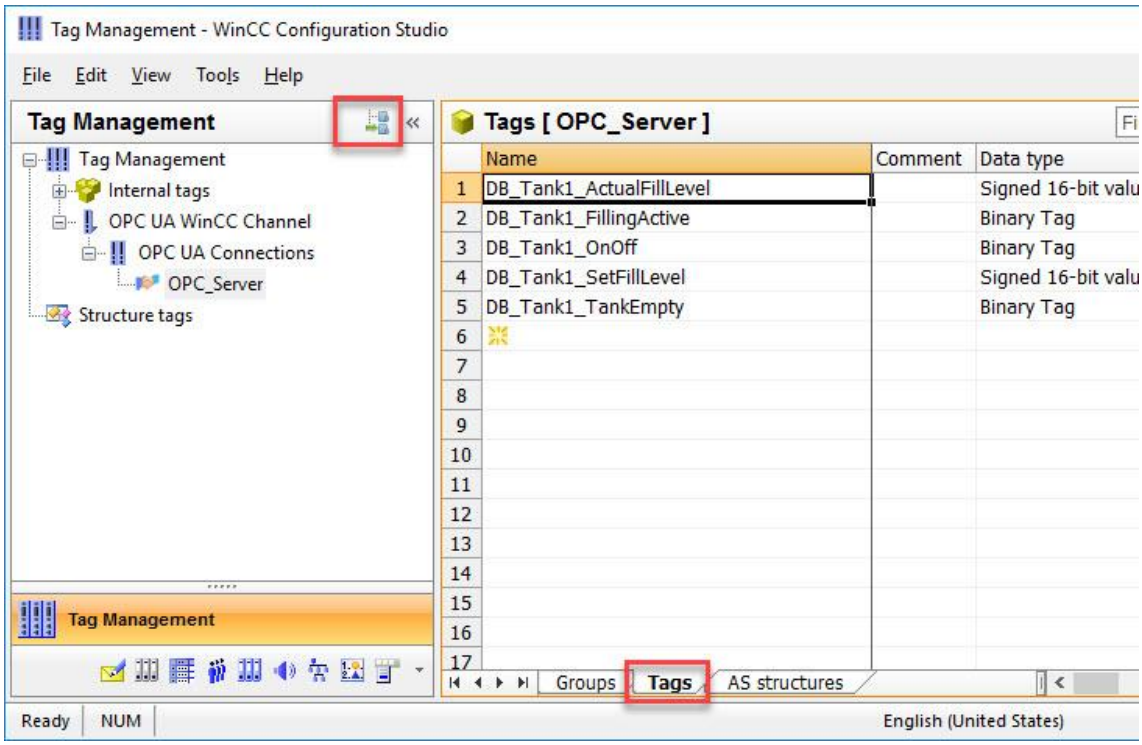
Figure 1-6



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".

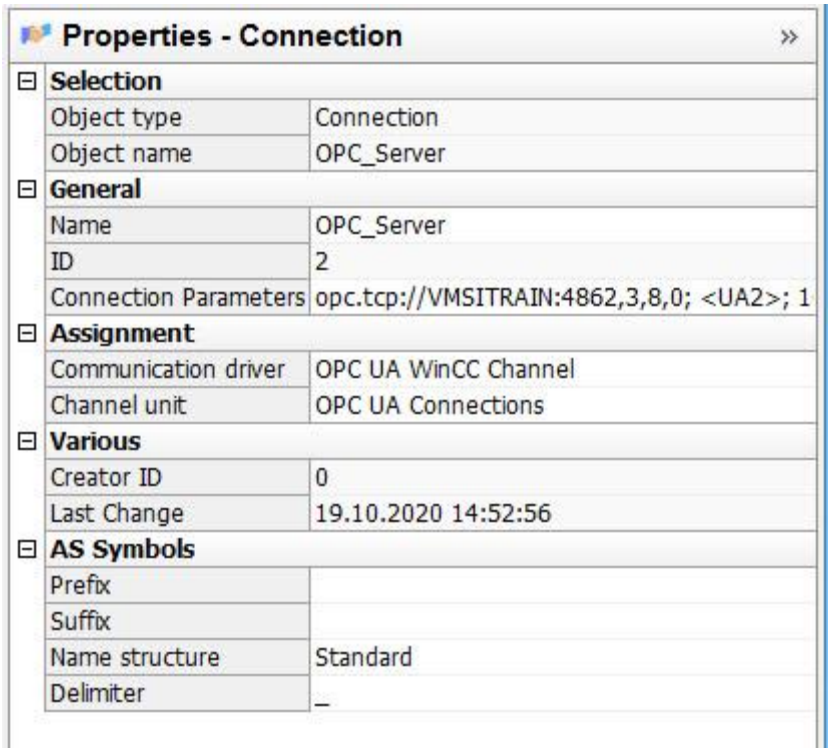
Figure 1-7



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.

Figure 1-8

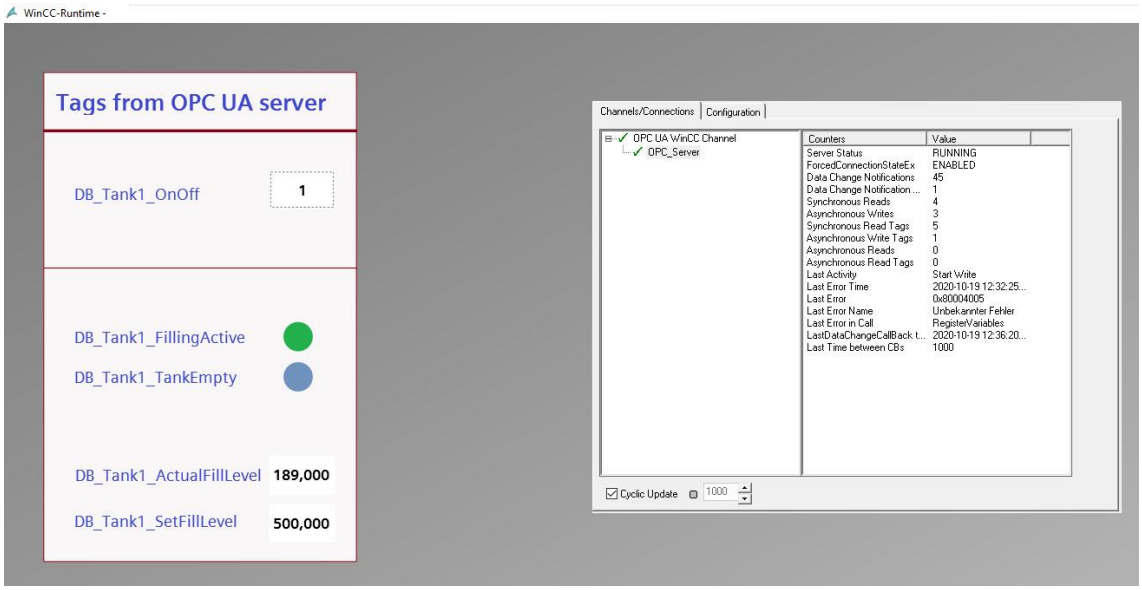


Properties - Connection

Selection	
Object type	Connection
Object name	OPC_Server
General	
Name	OPC_Server
ID	2
Connection Parameters	opc.tcp://VMSITRAIN:4862,3,8,0; <UA2>; 1
Assignment	
Communication driver	OPC UA WinCC Channel
Channel unit	OPC UA Connections
Various	
Creator ID	0
Last Change	19.10.2020 14:52:56
AS Symbols	
Prefix	
Suffix	
Name structure	Standard
Delimiter	_

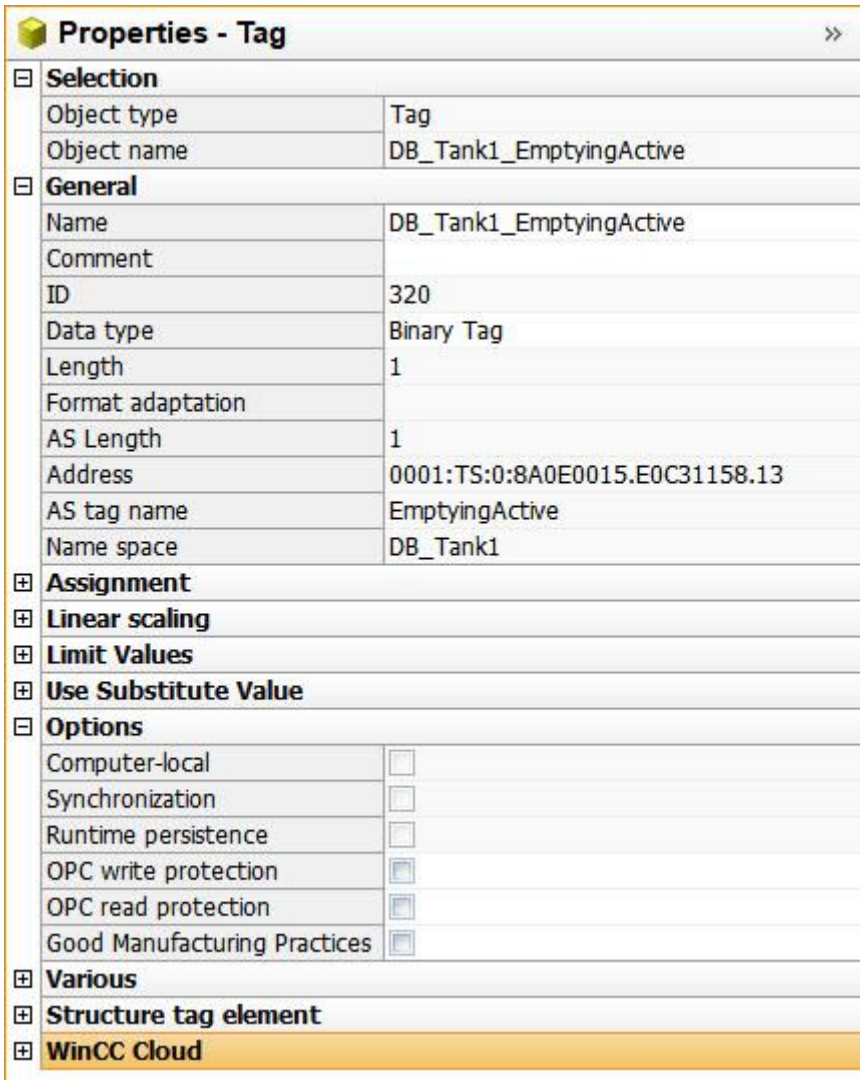
Now you can use the OPC tags in screens, for example.
Start Runtime and check whether the connection is established.

Figure 1-9



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.

Figure 1-10



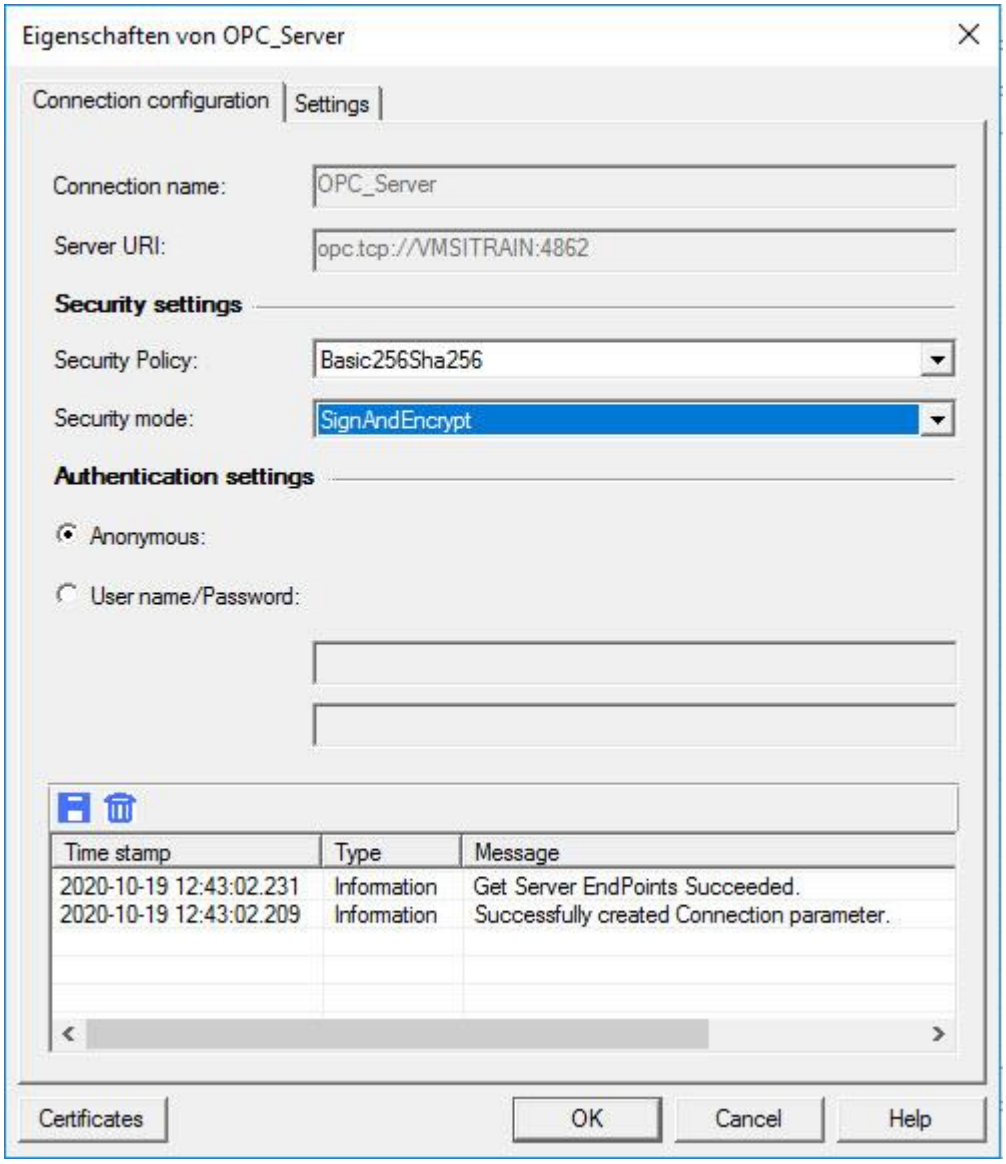
1.2 Additional Steps for Secure Communication

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.

Figure 1-11



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.

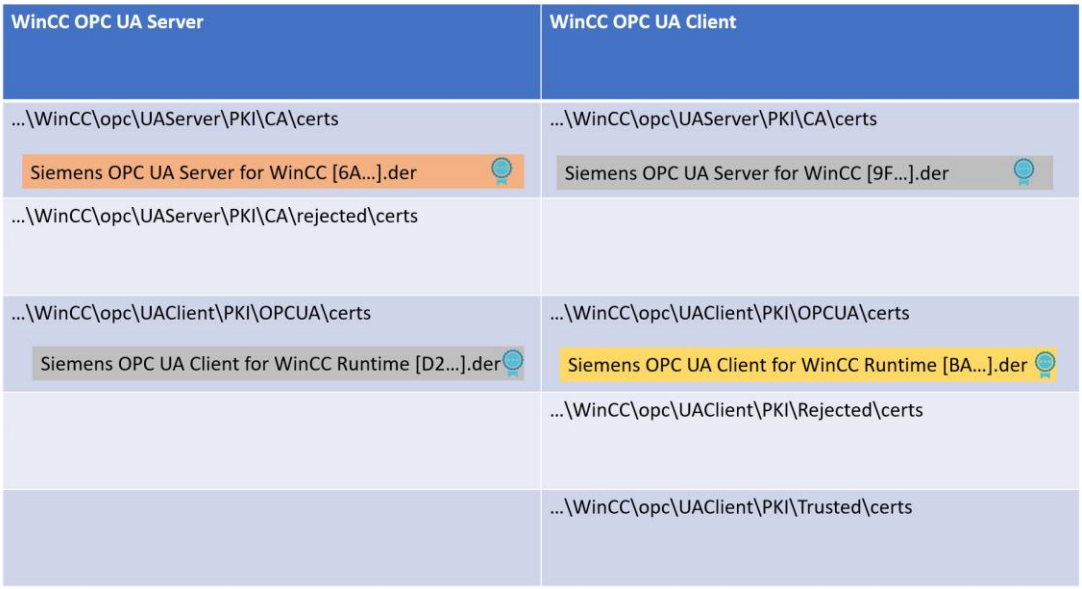
The situation prior to the enabling of secure communication is as follows with regard to certificates.

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

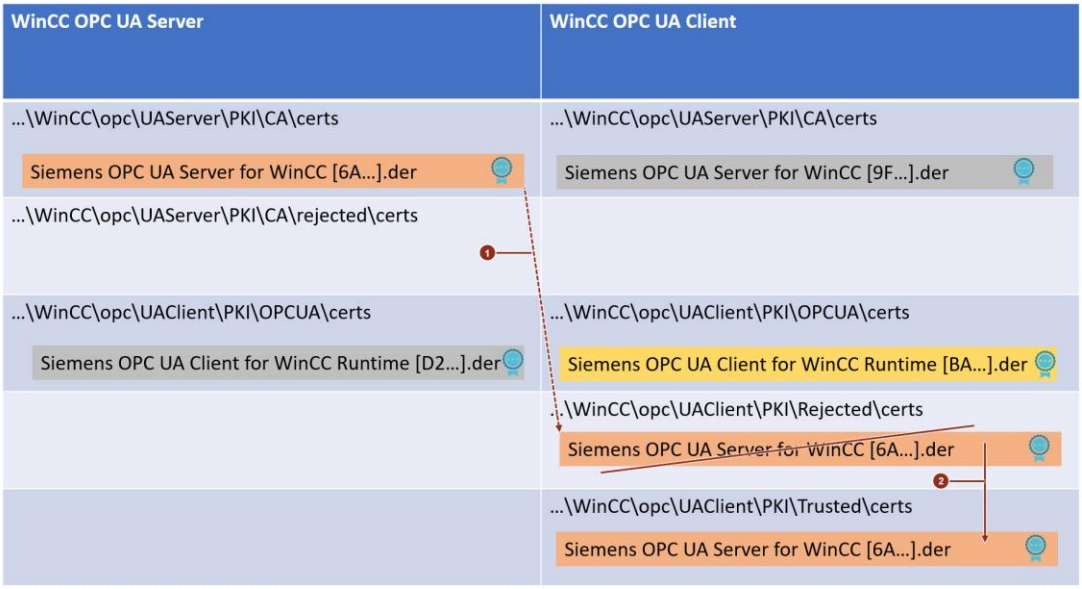


The following steps are necessary after enabling secure communication.

(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



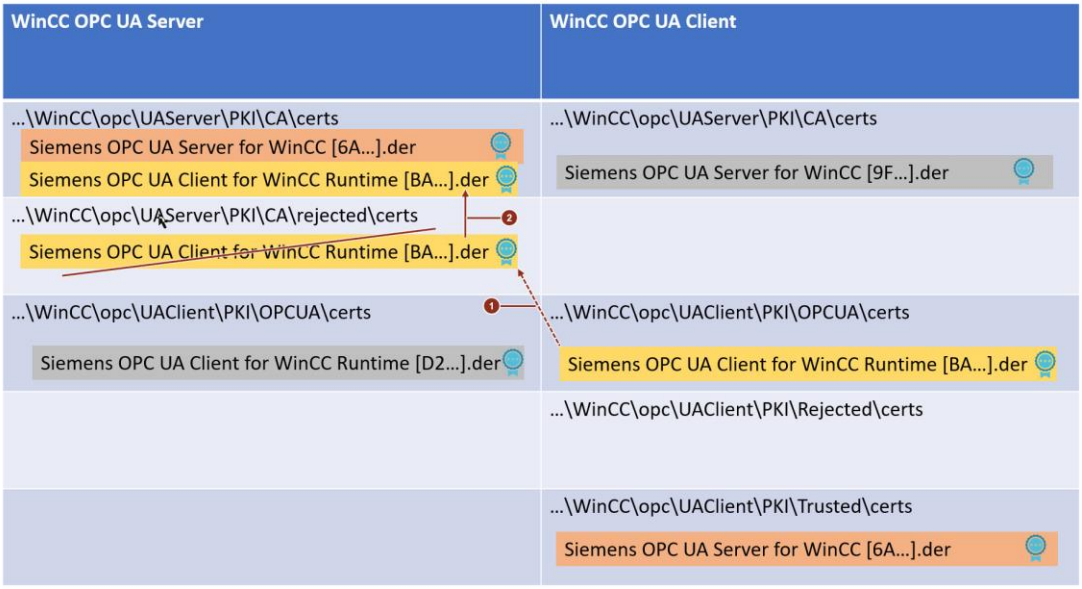
Tip:
On the OPC UA client, in the Connection Parameters mask, if you click the "Certificates" button (see Figure 1-11), you jump directly to the folder `C:\Programs (x86)\Siemens\WinCC\opc\UAClient\PKI`.

After these two steps further steps are necessary.

(1) The certificate of the OPC UA client was automatically 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).

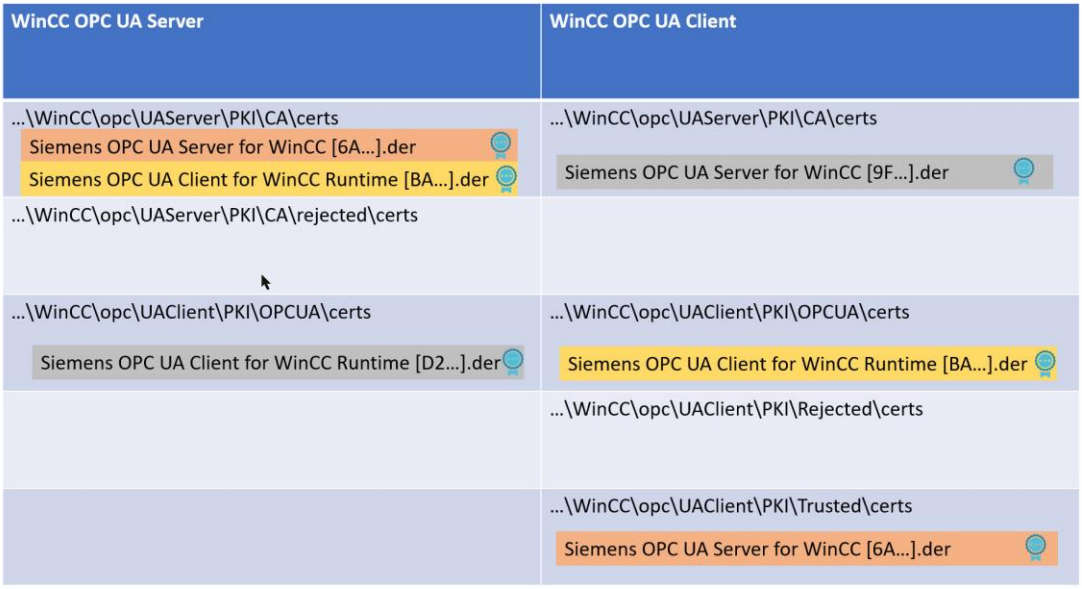
(2) Then you have to manually move the certificate on the OPC UA server from `…\WinCC\opc\UAServer\PKI\CA\rejected\certs` to `…\WinCC\opc\UAServer\PKI\CA\certs`.

Figure 1-14



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

Figure 1-15



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

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.