Tech Tips

Setting Up Secure OPC Communications Between Janus OPC Server and UaExpert

Janus OPC Servers support the use of security certificates for implementing secure OPC communications with external OPC Clients. This Tutorial will outline the process for setting up certificate-based secure communications between a Janus OPC Server and UaExpert.

The basic steps are:

1. First, set up “non-secure” communications with UaExpert and Janus OPC Server
2. Creating self-signed certificates for the Janu OPC Server
3. Import the self-signed certificate and key to the Janus product
4. Create a certificate for UaExpert
5. Import the UaExpert certificate to the Janus product

UaExpert® is designed as a general-purpose test client that allows you to test various OPCUA capabilities. In this use case UaExpert will be used to test Data Access capabilities. UaExpert can be downloaded from the Unified Automation web site. It is available as a royalty free license. Refer to the license agreement for terms and conditions. United Automation is a supplier of OPCUA development software.

*IMPORTANT NOTE: When implementing certificate-based secure communications, you will be creating certificates with a specific date/time validity range. Accordingly, you **MUST** set the real time clock in the Janus product to the correct time using the product web page, as this real time clock is used by the OPC server to determine the validity of certificates. If the clock is not set properly, you may not be able to create a connection due to invalid certificates.*

1. Set Up “Non-secure” Communications with Janus OPC Server and UaExpert

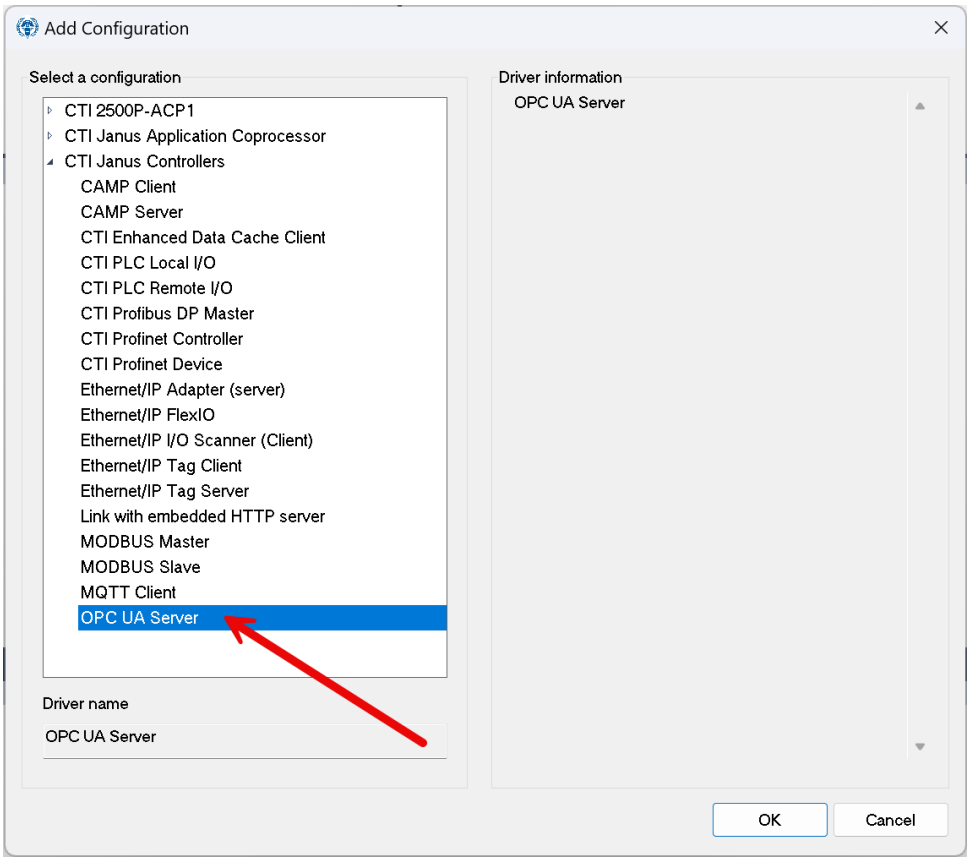
UaExpert® is designed as a general-purpose test client that allows you to test various OPCUA capabilities. In this use case UaExpert will be used to test Data Access capabilities. UaExpert can be downloaded from the Unified Automation web site. It is available as a royalty free license. Refer to the license agreement for terms and conditions. United Automation is a supplier of OPCUA development software.

1.1 Janus OPC Server Configuration

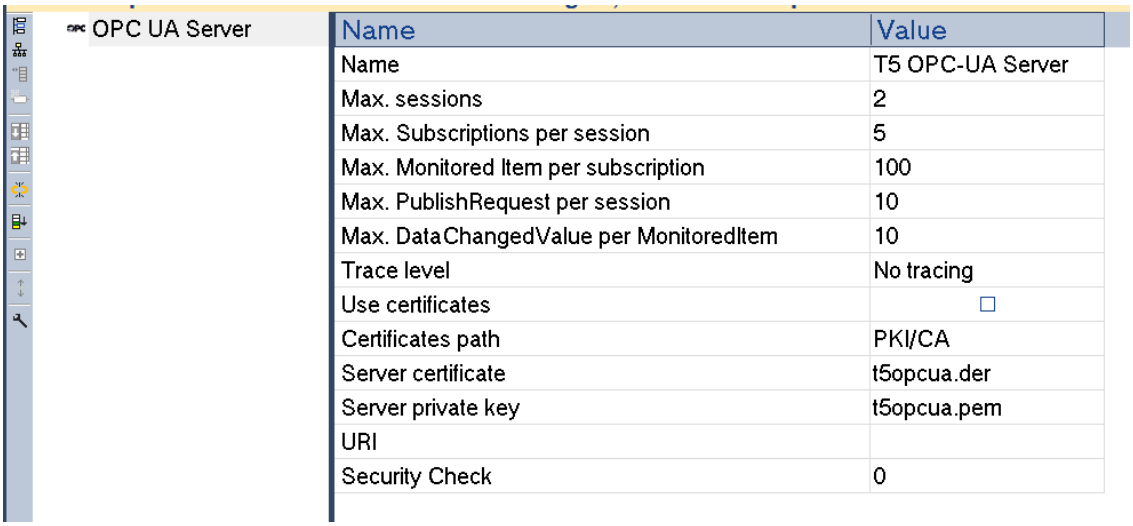
This section shows how to configuration the OPC UA Server Fieldbus for Janus products in Workbench. It assumes you are familiar with Workbench.

1.1.1 *Add the OPC UA Server Protocol*

Create a new project in Workbench. In your Workbench project, open the Fieldbus Configuration screen. Using the toolbar on the left, click the “Insert Configuration” icon. Select and expand the list for your Janus product.



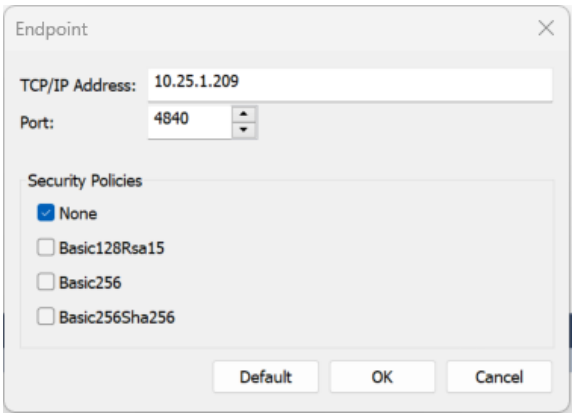
Select OPC UA Server and click OK. The OPC UA Server will be added.



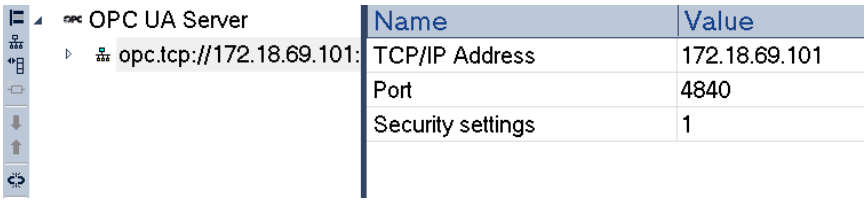
Server parameters can be edited on the right, or by double-clicking the OPC UA Server. The default values work for most applications. See Workbench HELP for information on parameters.

1.1.2 *Add the Endpoint*

Next, use the Insert Master/Port icon on the left to insert the Endpoint.

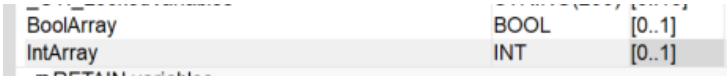


Enter the IP address of your Janus product. For now, leave all the security policies unchecked except “None”. Click OK and the Endpoint will be added.



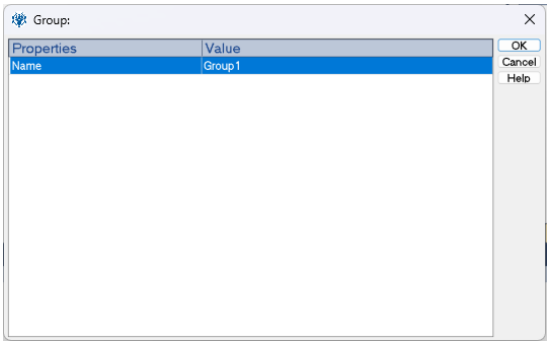
1.1.3 *Create Variables*

Next, create some variables to be served by the OPC Server. For this example, we will use two arrays to make things easier. Create a Boolean array of dimension 2 and an Integer array of dimension 2.

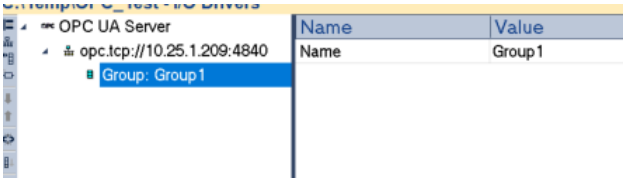


1.1.4 *Add a Variable Group to the Server*

Next, use the Insert Slave/Data Block icon on the left to insert a group. We'll call it Group1. Remember that you have to press the <Enter> key to keep the name after editing.

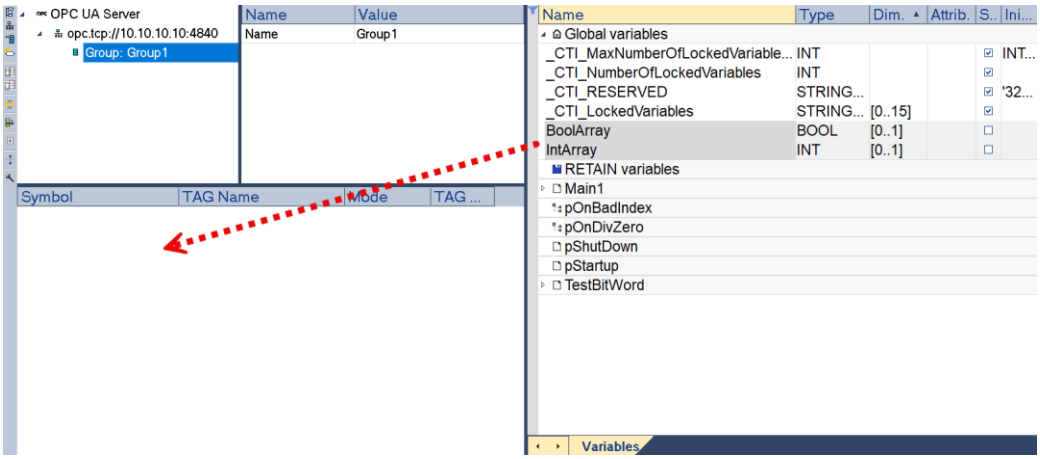


Click OK to add the group.

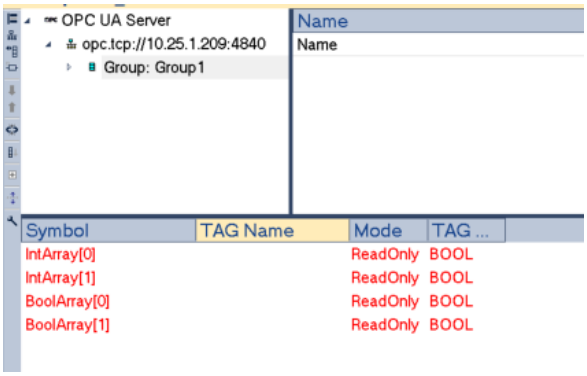


1.1.5 *Add Variables to the Group*

Now, with the group highlighted as shown above, drag and drop the desired variables from the variable pane to the pane below the OPC server configuration.

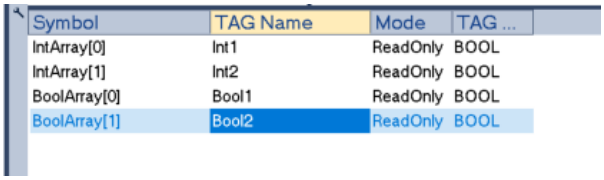


When completed, it should look like this:



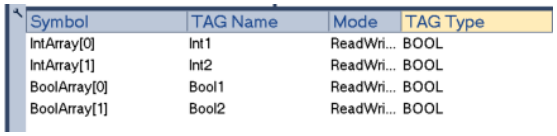
1.1.6 *Add Tagnames*

Now click in the "TAG Name" column of each variable and add a Tagname for your variables.



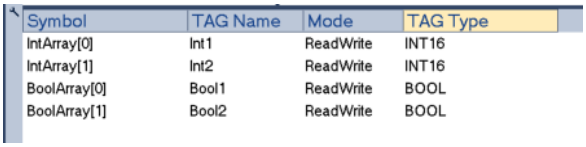
1.1.7 *Set the Mode*

There are 3 modes available: ReadOnly, WriteOnly, Read/Write. We'll set ours to Read/Write.



1.1.8 *Set the Tag Type*

The default Tag Type is BOOL. We'll need to change the Tag Type on our Integer tags to "INT16".

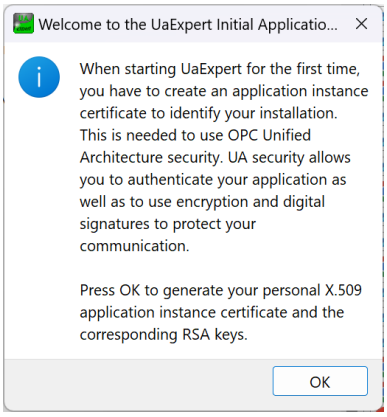


That completes the OPC Server setup.

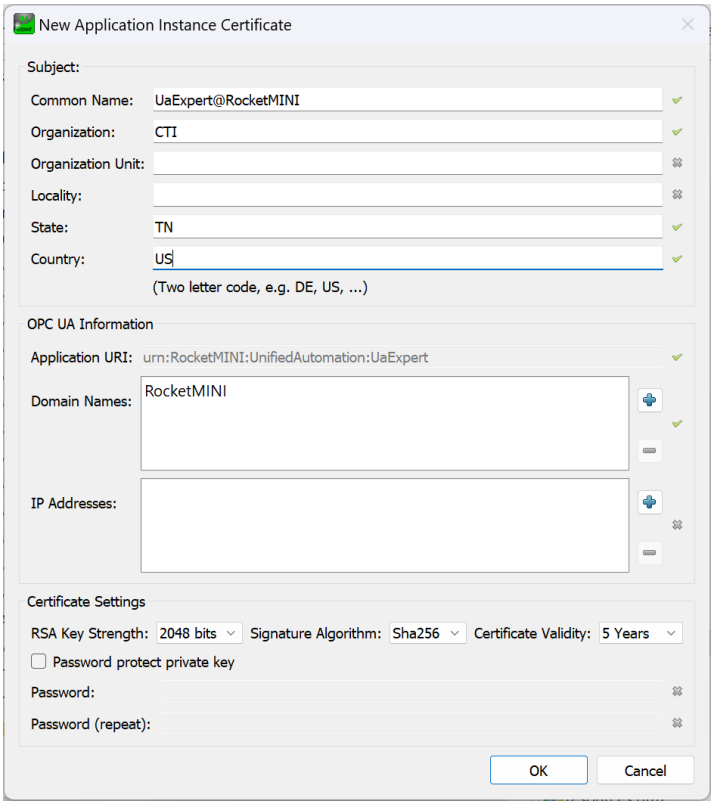
1.2 UaExpert Configuration

Download UaExpert from the Unified Automation website at https://www.unified-automation.com/downloads/opc-ua-clients.html. You will need to register and create an account before downloading.

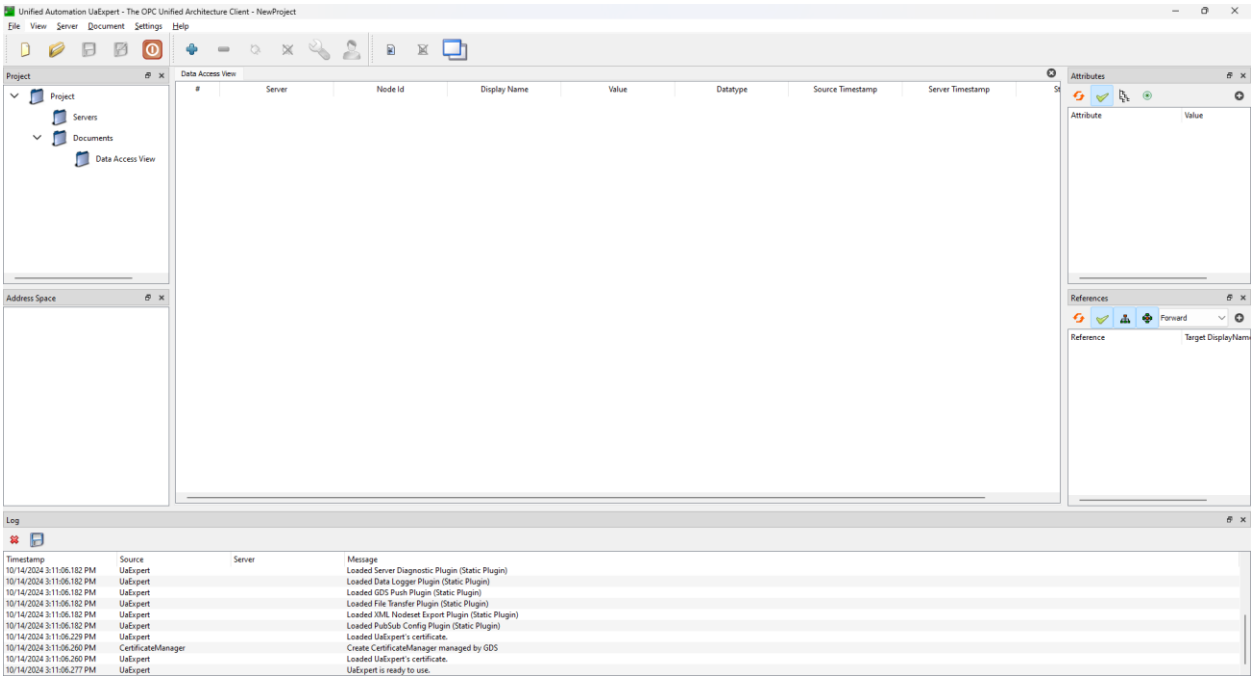
After installing and launching UaExpert for the first time, it will prompt you to create a certificate and related RSA keys for UaExpert. Click on OK to continue. The certificate will be needed later when you are implementing secure communications.



The *New Application Instance Certificate* dialog will come up. It should be pre-filled with Common Name and Domain Names based on your PC name. The Organization field is required, and you can complete the location fields if you like. Leave the certificate settings at their default values. Set the validity as desired.

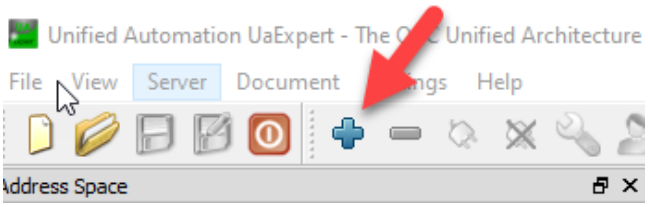


Click OK. The certificate will be created, and the main program window will come up.



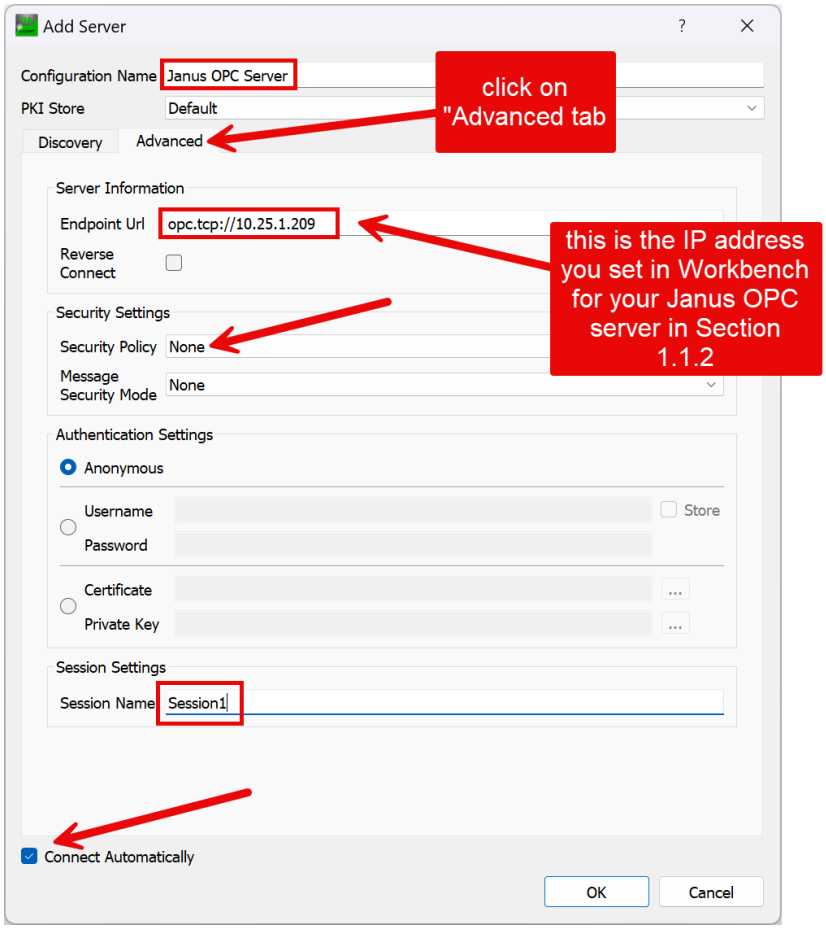
1.2.1 *Add the Server Session*

To configure a server session, click on the  icon in the main tool bar to add your OPCUA server.

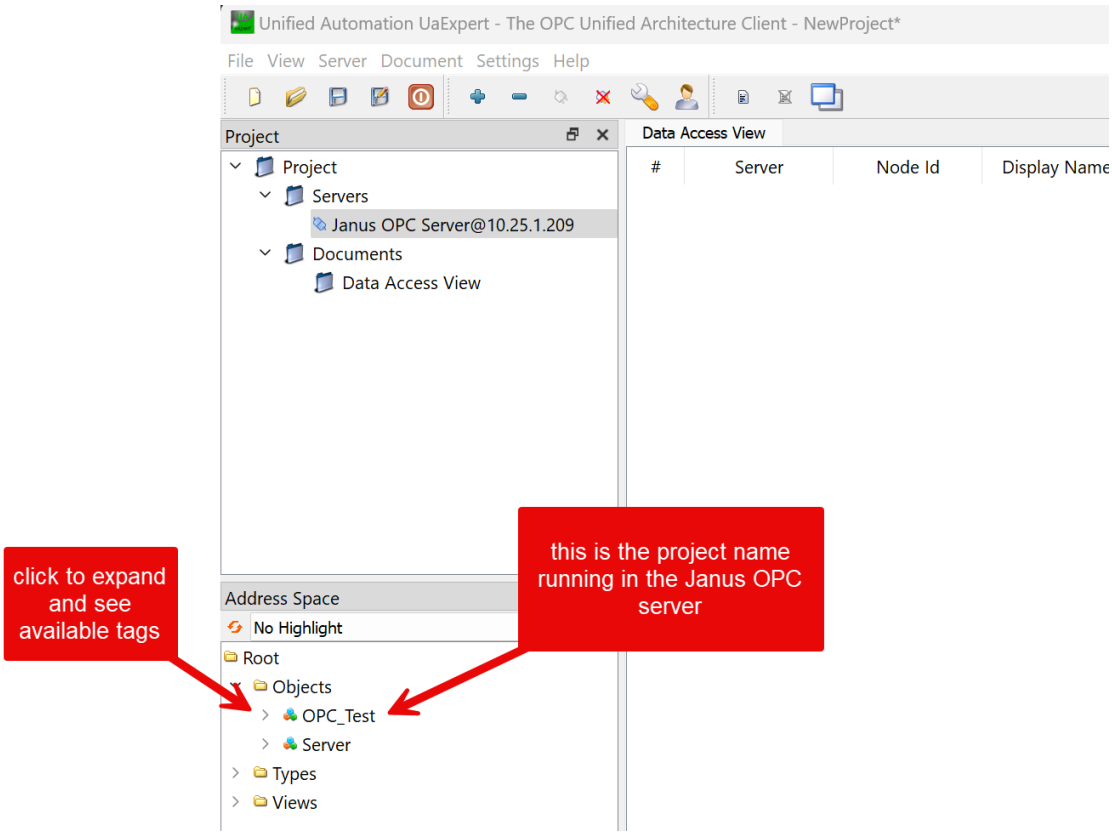


This will open the ADD SERVER window.

Click on the “Advanced” tab, then complete the “Configuration Name”, “Endpoint Url” and “Session Name” fields as shown (you can use your own Configuration and Session names, and your IP address may be different). Be sure the Security Policy is set to “None”. Tick the “Connect Automatically” box.

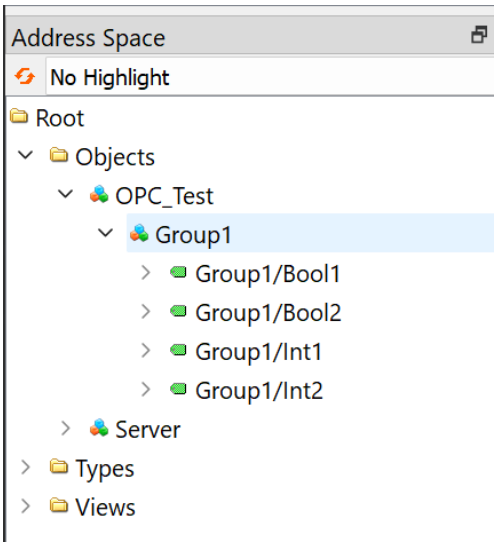


Once connected, the server will appear in the Address Space pane as shown below. The name of the Janus OPC Server project will be shown ("OPC_Test" in this case).

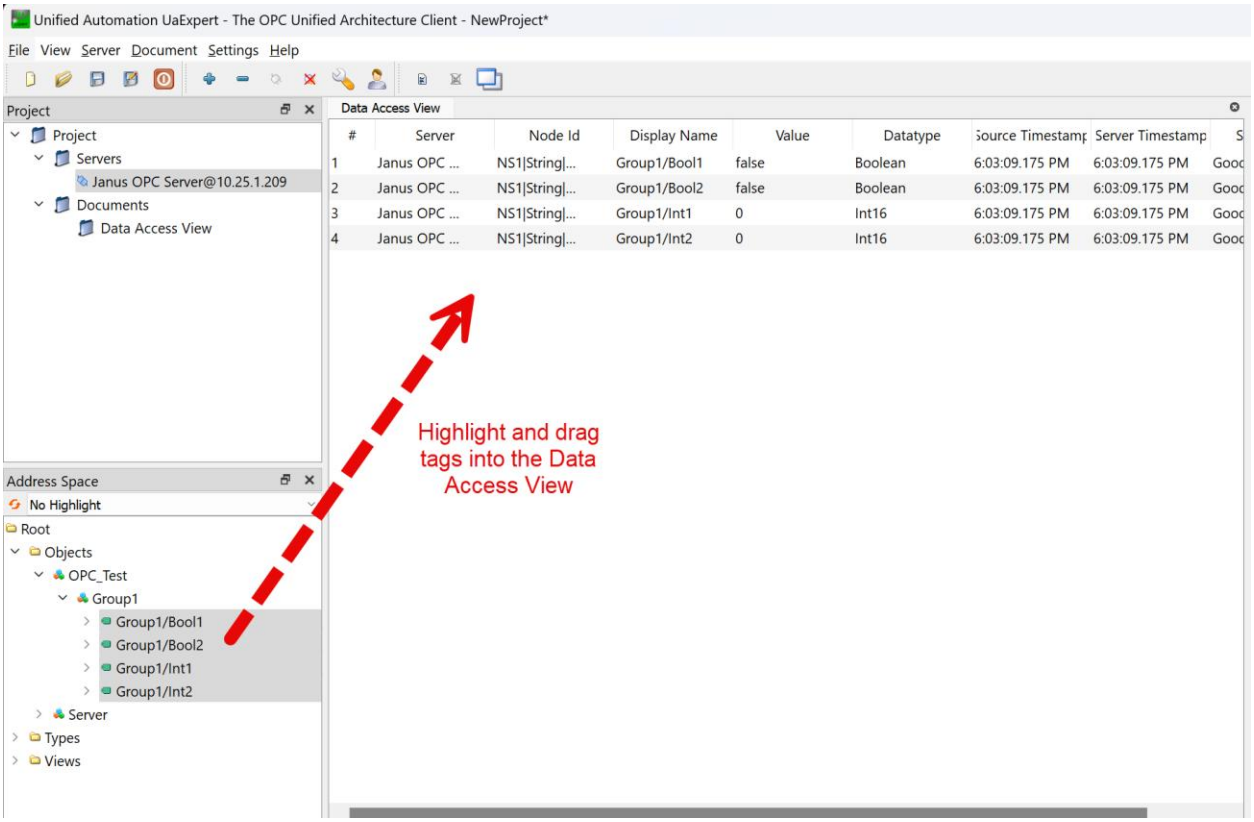


1.2.2 *Configure the Data Access View*

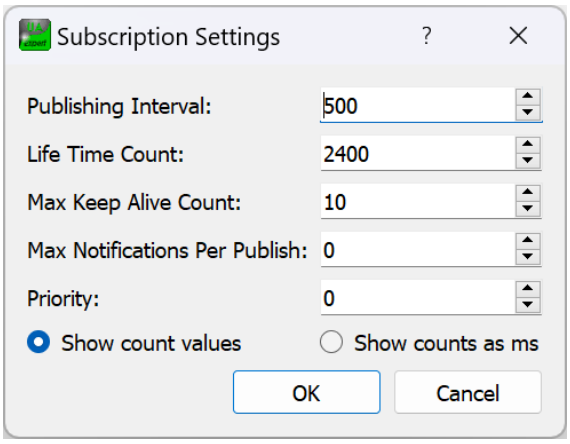
Expand the Server name to see the available tags.



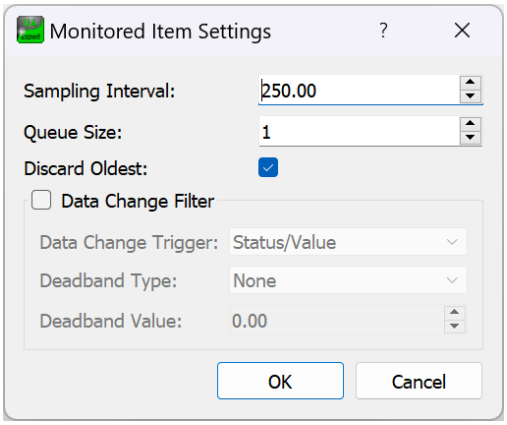
Highlight the desired tag(s) and drag them into the Data Access View.



Default settings for subscriptions and monitored items are applied. You can change the Subscription settings by right-clicking in the Data Access view.



You can change Monitored items settings by selecting one or more tags in the Data access view and right-clicking.



See UaExpert help for more information regarding the data access view. All items in a Data Access view belong to a single subscription. You can add another subscription by adding a Data Access view.

Values can be written to monitored items that are not "read-only" by double-clicking on the value and entering a new value.

If problems occur, selecting the log view will help you determine the cause of the problem.

2. Set Up Secure Communications

To implement OPCUA Security Features, the following steps are required:

1. Create a certificate and private key for your Janus OPC Server
2. Import the certificate and private key to the Janus product
3. Create the UaExpert certificate
4. Import the UaExpert certificate to the Janus product
5. Configure certificates in the Janus OPC server
6. Enable Security Policies on the Janus OPC server
7. Enable Security Policies on UaExpert

2.1 Creating Self-Signed Certificates for your Janus OPC Server

In order to implement the security features of the Janus OPCUA server, a self-signed X.509 Certificate that specifically identifies the server installation must be used. Part 1 describes how to create a basic certificate (and corresponding private key) that that will work with your server application.

The X.509 certificate contains information that allows the OPCUA client to authenticate the server (ensure the server can be trusted). It also contains a public key (derived from the server's private key) that the client can use to encrypt messages sent to the client. For more information, see the USING X.509 CERTIFICATES topic in the CTI Janus Workbench help system.

2.1.1 *Get the Certificate Creation Tool*

The creation tool used in this example is open-source software named XCA. It allows you to create and manage X.509 certificates and provides a password protected database for certificate and private key storage. You can download the software at the following URL: https://hohnstaedt.de/xca/index.php.

If you prefer another tool, this example should provide enough information to create an acceptable certificate.

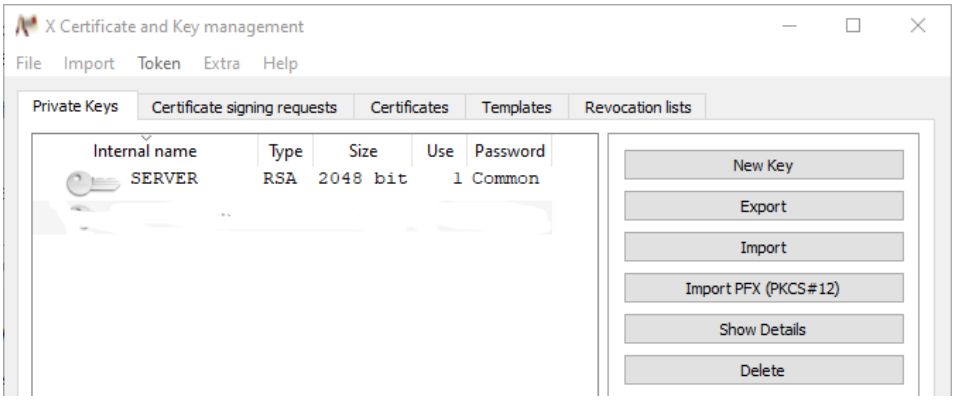
After downloading, installe the application using "Typical" options, Then open the XCA application and create a database. SELECT FILE: NEW DATABASE to choose the data base location and password (or no password).

2.1.2 *Create a Certificate and Private Key*

The following steps describe how to create a certificate and associated private key

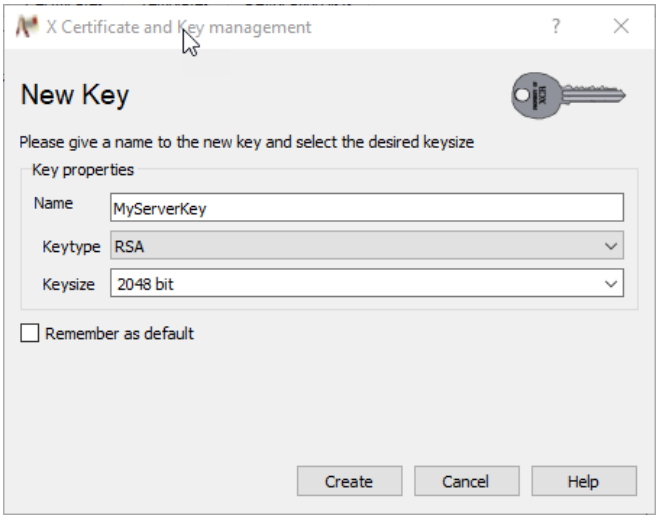
2.1.2.1 Create a Private Key

Select the PRIVATE KEYS tab and click on the NEW KEY button.

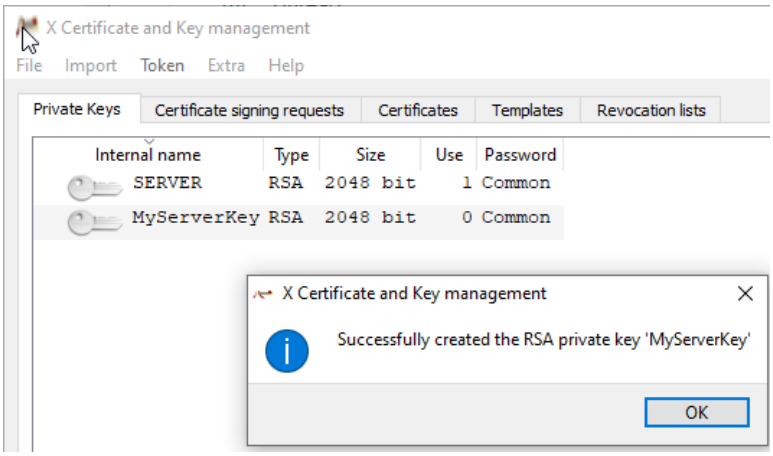


NOTE: The database in this example already contains a previously generated key named SERVER

Enter a name for the key and click on the CREATE button.



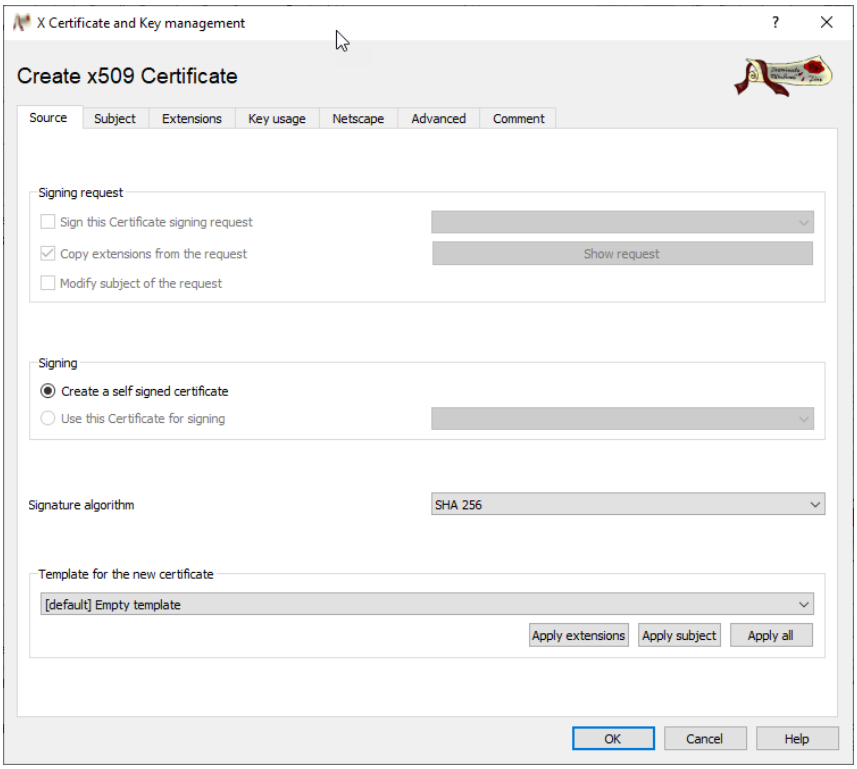
Confirm that key was successfully created.



Next, select the CERTIFICATES Tab, then click on the NEW CERTIFICATES button.

2.1.2.2 Create the Certificate

Confirm that the SOURCE tab is selected and that the CREATE A SELF-SIGNED CERTIFICATE radio button is selected.

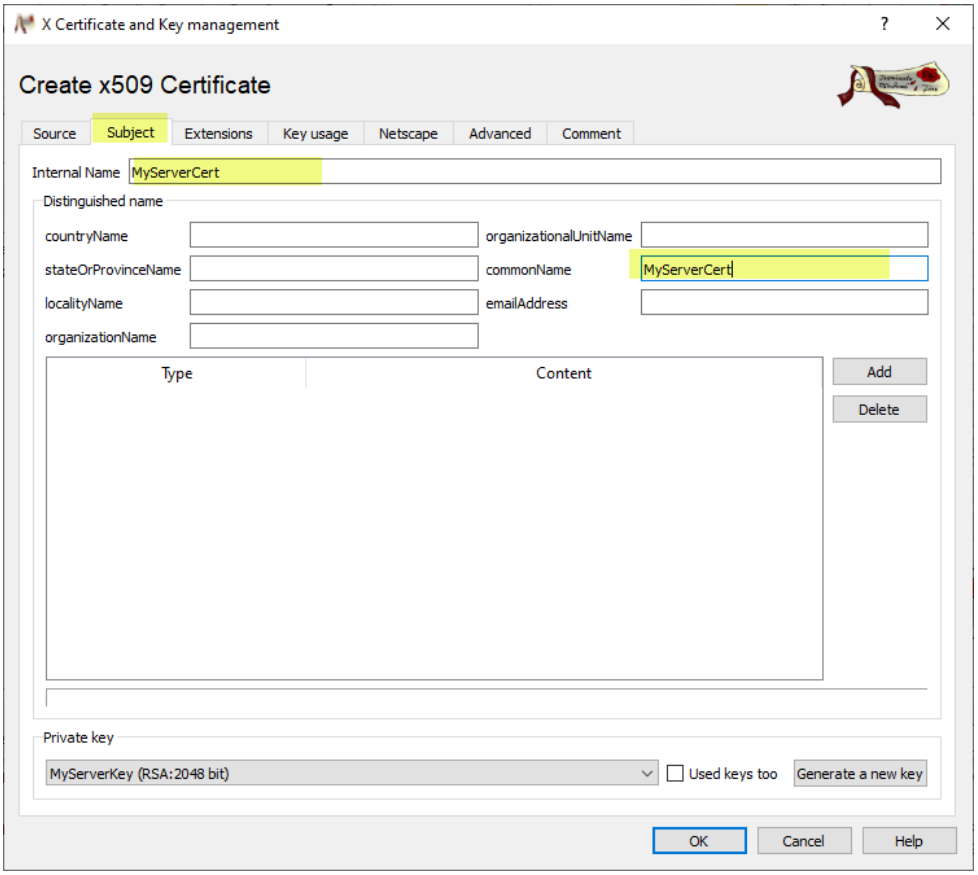


Next, select the SUBJECT tab.

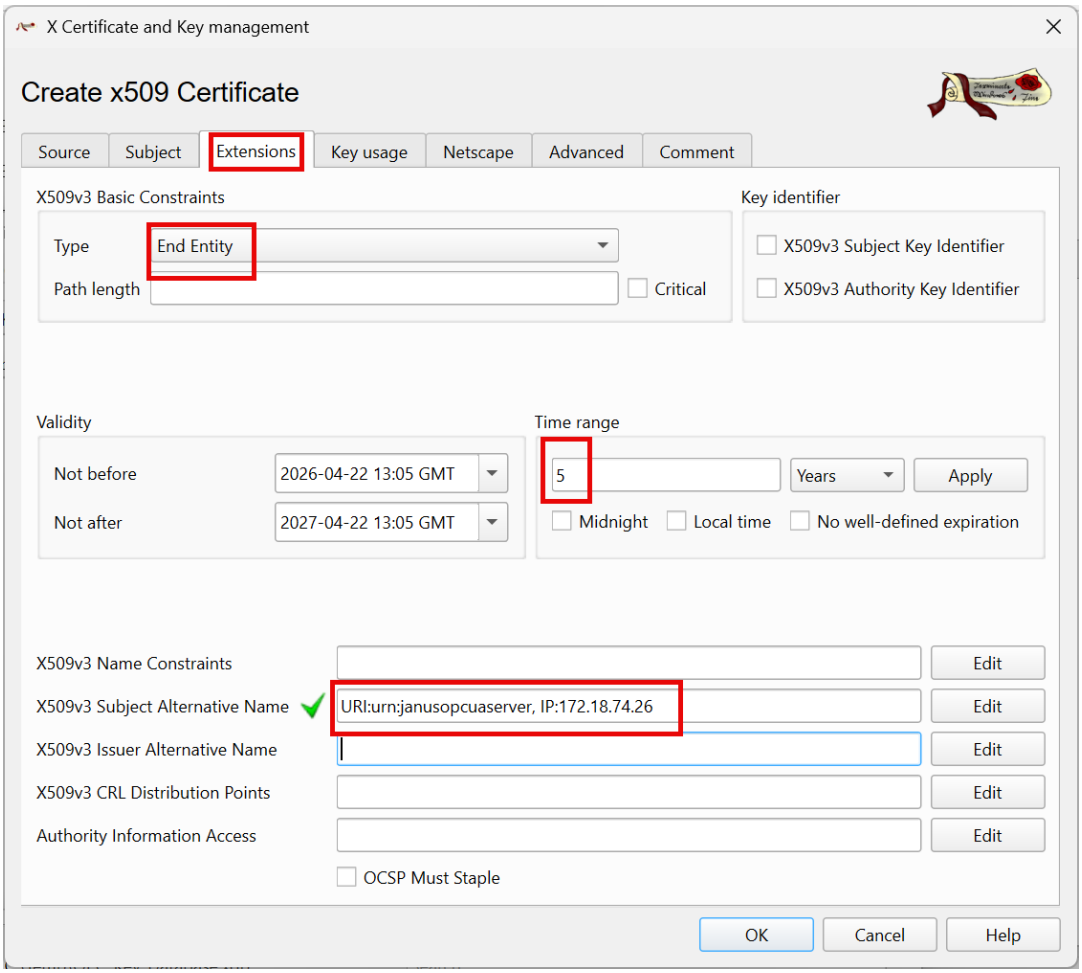
Enter a name in the INTERNAL NAME box. This name is not included in the certificate but will be used as the name of the certificate file.

Enter a name in the COMMON NAME box. Although this name is not required to be the same as the internal name, using the same name is recommended since it makes it easier to administer the certificate.

Verify that the private server key that you previously created appears in the Private Key selection at the bottom of the window. If not, you can change the selection using the drop-down menu.



When finished, Select the EXTENSIONS tab.



In the TYPE dropdown menu, select END ENTITY. Since this is a self-signed certificate, there is no higher certificate authority.

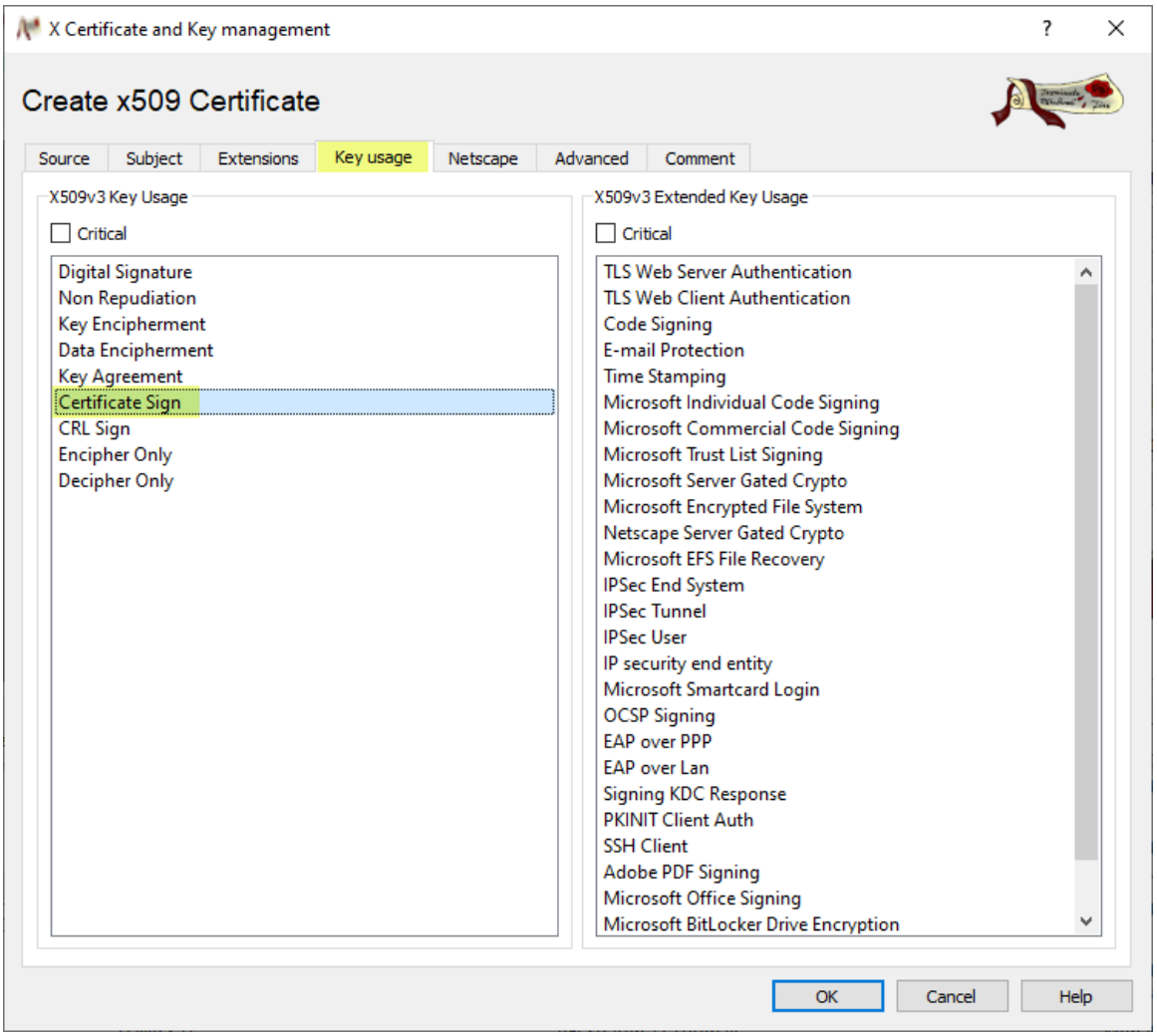
Set the Validity time range or accept the default of one year from now. *NOTE: once the "Not After" Date/Time expires, the certificate will not work.*

Enter the required information for the SUBJECT ALTERNATIVE NAME. This field identifies the server application and the network address of the product running the server.This is verified when connecting to the server. In the example below, the term URI: (Uniform Resource Identifier) is always required. The "urn:janusopcuaserver" portion identifies the server application, where urn: designates the following characters are a Uniform Resource Name. You can create any name you wish as long as the entire string (including the urn: designator) exactly matches the entry in the URI field for the OPC UA server configuration, Using the example urn, the configuration would appear as shown below.

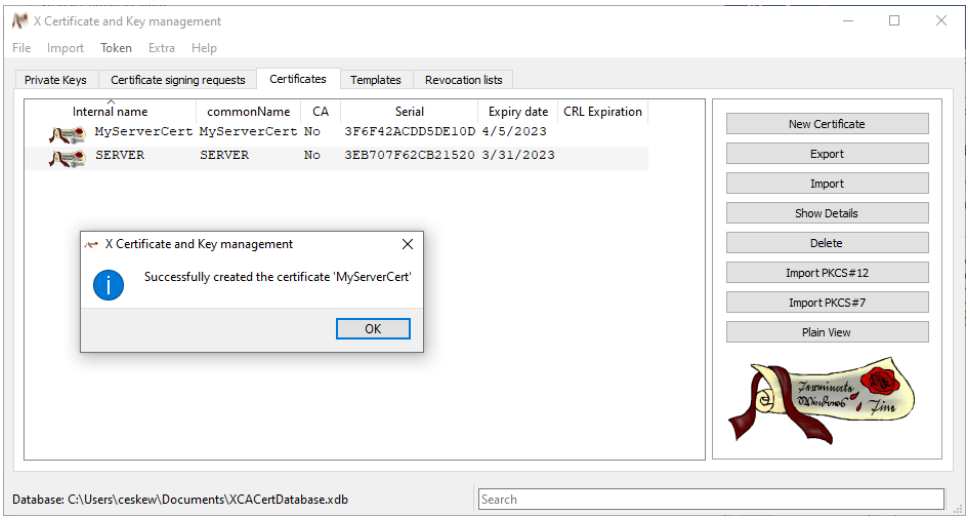
URI	urn:janusopcuaserver

The "IP: 172.18.74.26" portion is the IP address of product the server is running on in the example. You should enter the IP address of your host This must be separated from the urn string by a comma. The digits following the "IP:" designator must be expressed in dotted decimal format. Alternatively, a DNS name can be entered by using the "DNS:" designator instead of "IP:"

Next, select the Key Usage tab. Select CERTIFICATE SIGN as the key usage



Click on the OK button to complete the process.

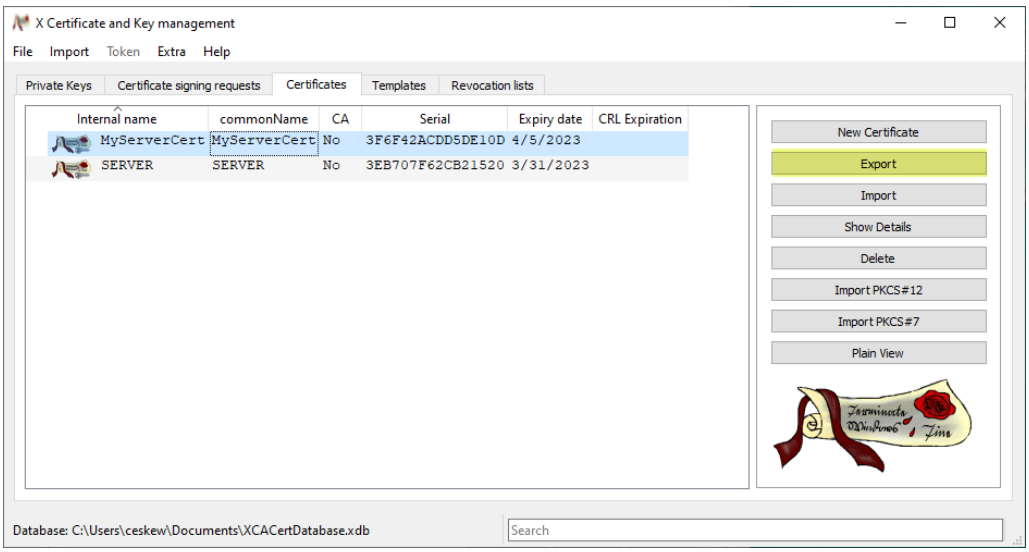


2.1.3 *Export the Certificate and Key*

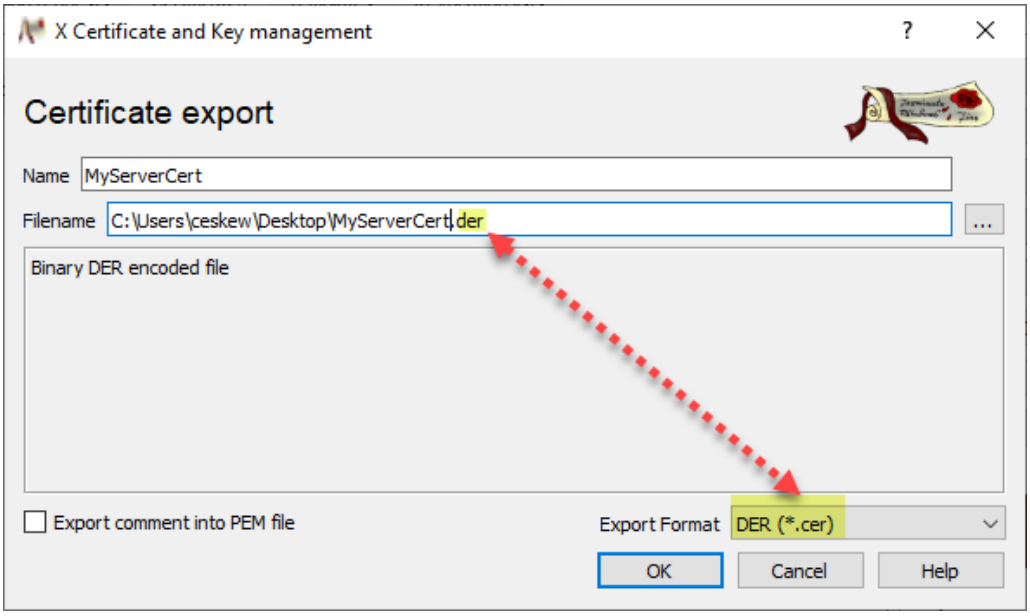
The Certificate and associated private key must be exported before they can be imported to the product.

2.1.3.1 Export the certificate

Select the desired certificate and click on the EXPORT button.



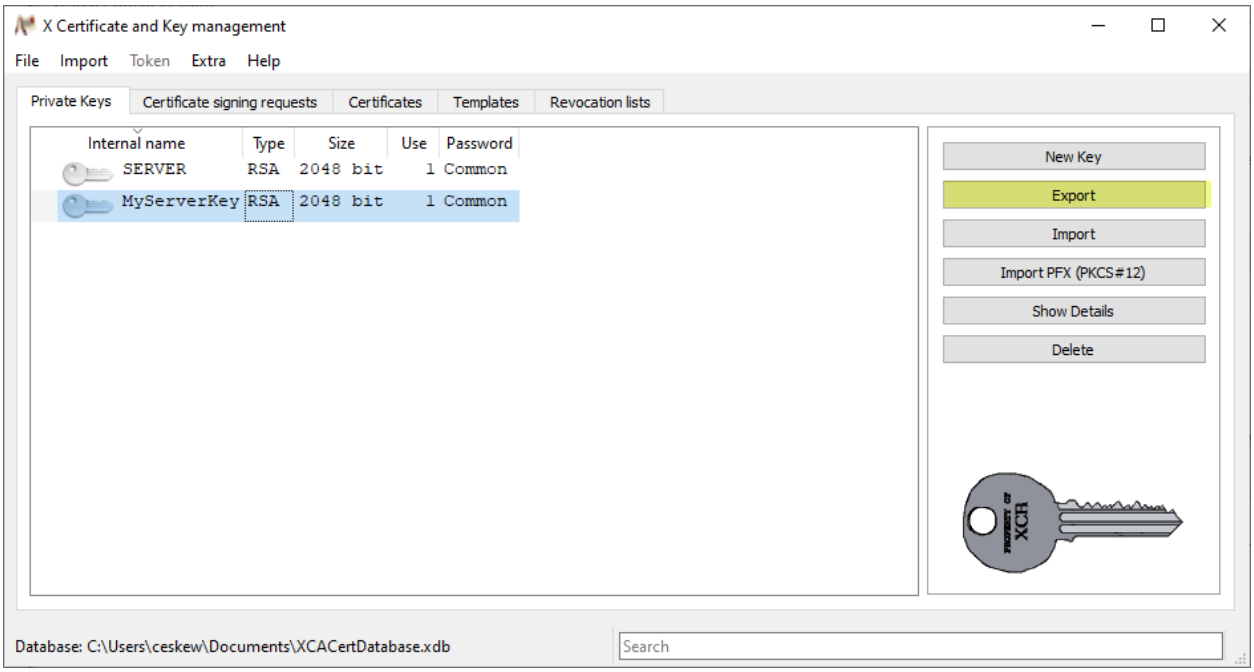
Set the Export Format to DER(*.cer). ***The XCA application will set the file extension to .cer. You must change this to .der before clicking on the OK button, since the OPCUA server does not support the .cer prefix***



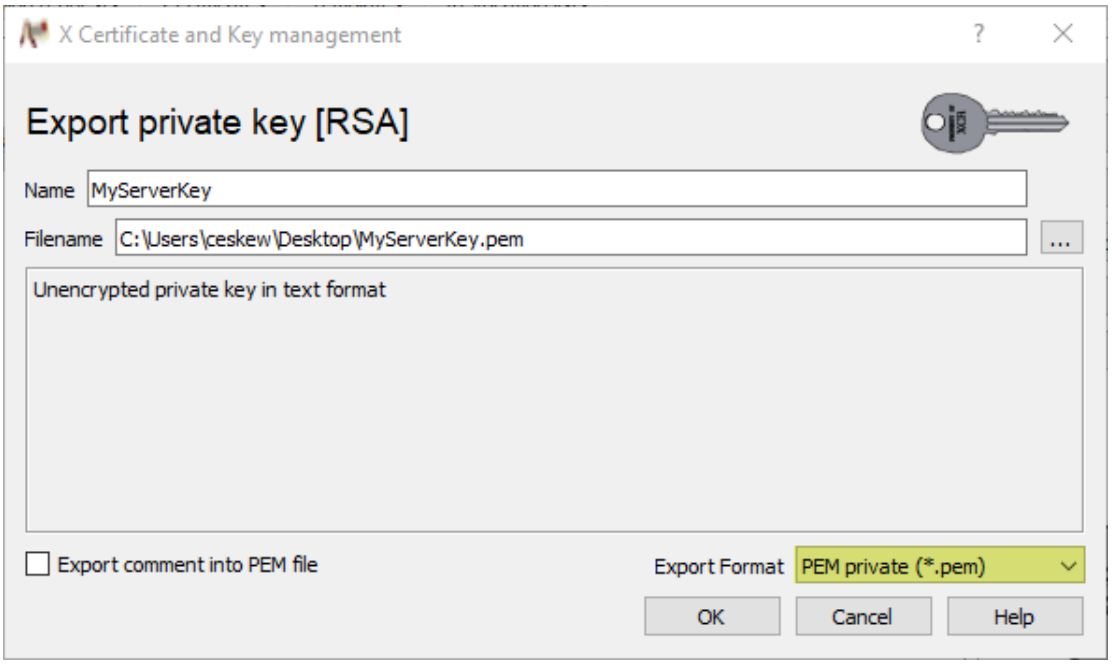
Take note the path of the exported file. This information will be required when importing the certificate to the CTI Janus product.

2.1.3.2 Export the Private Key

Select the desired key and click on the Export button.



Verify that the Export Format is PEM private (*pem). Click on the OK button to export the key.



Take note the path of the exported file. This information will be required when importing the key to the CTI Janus product.

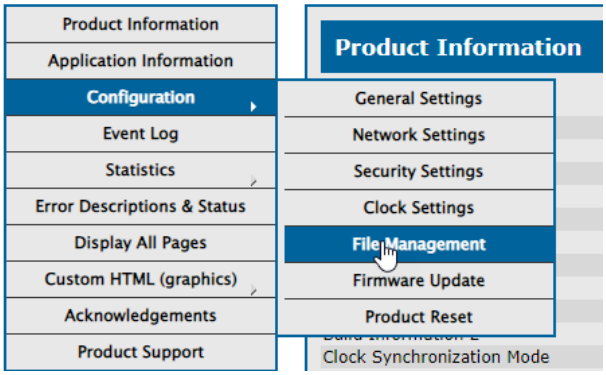
2.2 Import the Certificate and Private Key to the Janus Product

The certificate and associated private key must be stored on the internal SD card of the Janus product before they can be used. This can be accomplished using the File Manager page accessible from the product web server.

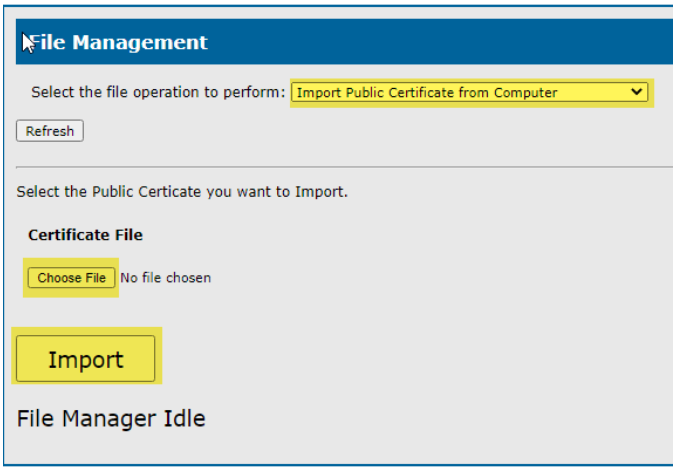
2.2.1 *Import the Server Certificate*

The certificate can be imported to the CTI Janus product using the following steps:

1. Open the Product web server.
2. Select the CONFIGURATION/ FILE MANAGEMENT menu item to open the File Management page.



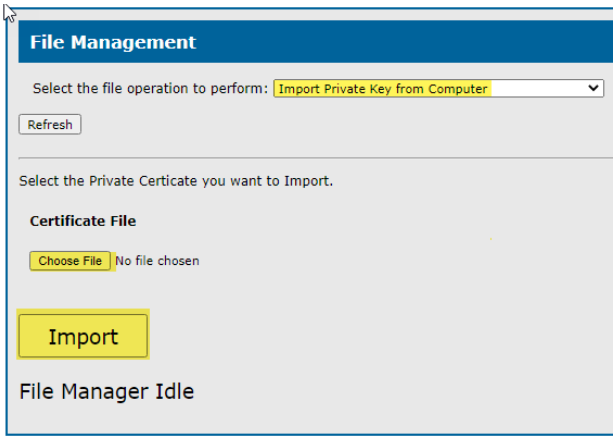
3. Select IMPORT PUBLIC CERTIFICATE FROM COMPUTER option from the dropdown menu.



4. Click on the CHOOSE FILE button, navigate to the location of the certificate file, and select it.
5. Once the file has been selected, click on the IMPORT button to copy the certificate file to the product.

2.2.2 *Import the Private Key*

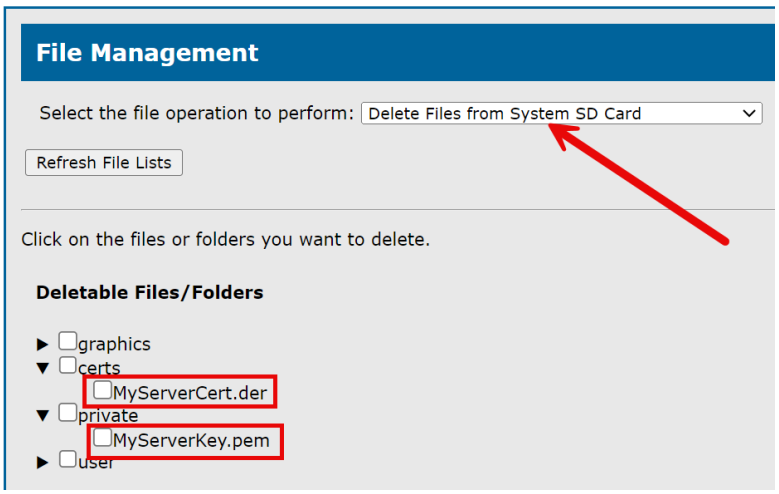
1. From the File Management page, select the IMPORT PRIVATE KEY FROM COMPUTER option from the dropdown menu.



2. Click on the CHOOSE FILE button, navigate to the location of the key file, and select it.
3. Once the file has been selected, click on the IMPORT button to copy the key file to the product.

2.2.3 *Displaying/Deleting files*

1. From the File Management pane, select DELETE FILES FROM SYSTEM SD CARD.



2. Expand the *Certs* and *Private* folders to list file content.

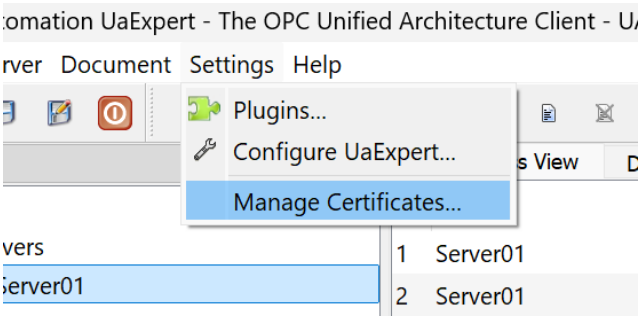
If necessary, select the files you want to delete and click the DELETE button to erase files.

2.3 Copy the UaExpert Application Instance Certificate to Janus

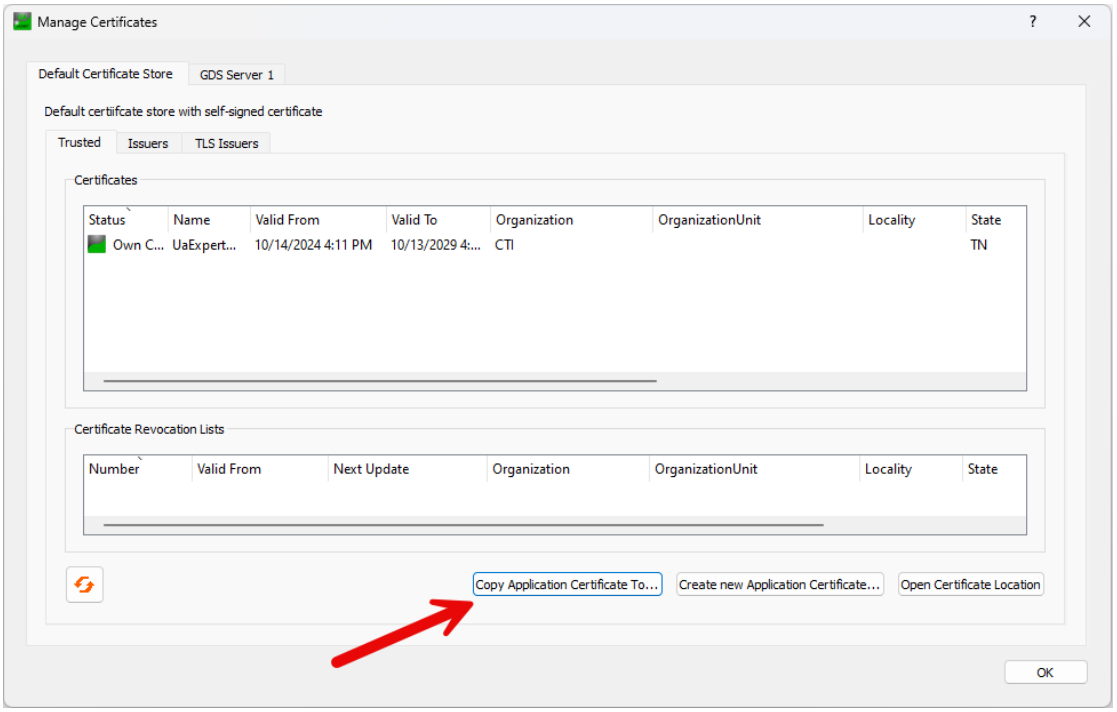
Next, we must manually copy to the UaExpert Application Instance Certificate to the Janus product runtime PKI/CA/certs folder.

2.3.1 *Save the Certificate in UaExpert*

Click on the UaExpert "Settings" menu item, and Select "Manage Certificates" from the pop-up menu.



The *Manage Certificates* dialog will come up.

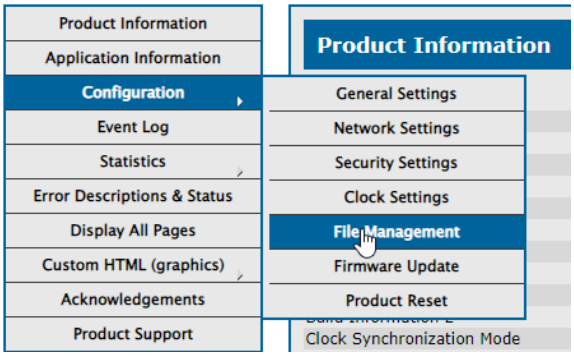


Click on the *Copy Application Certificate To* button. A *File Explorer* window will open. Navigate to a temporary folder where you want to copy the certificate and click *Save*.

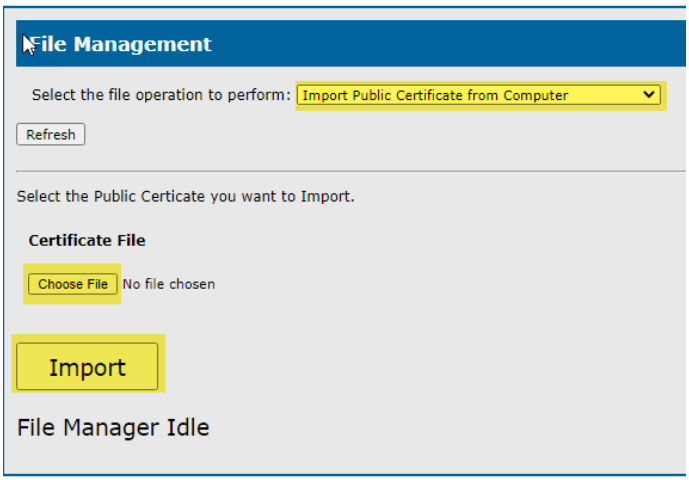
2.3.2 *Import the UaExpert Certificate to the Janus Product*

The certificate can be imported to the CTI Janus product using the following steps:

1. Open the Product web server.
2. Select the CONFIGURATION/ FILE MANAGEMENT menu item to open the File Management page.

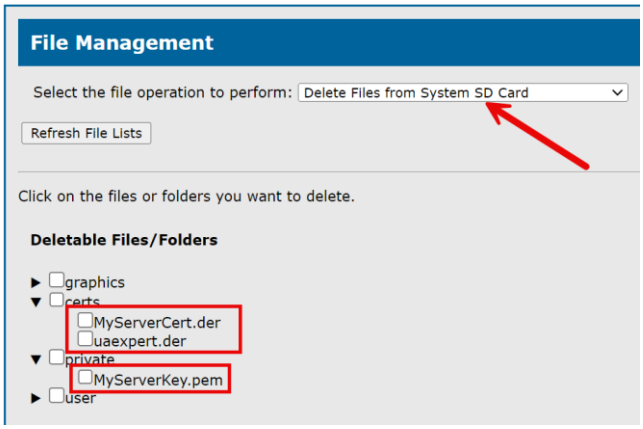


3. Select IMPORT PUBLIC CERTIFICATE FROM COMPUTER option from the dropdown menu.



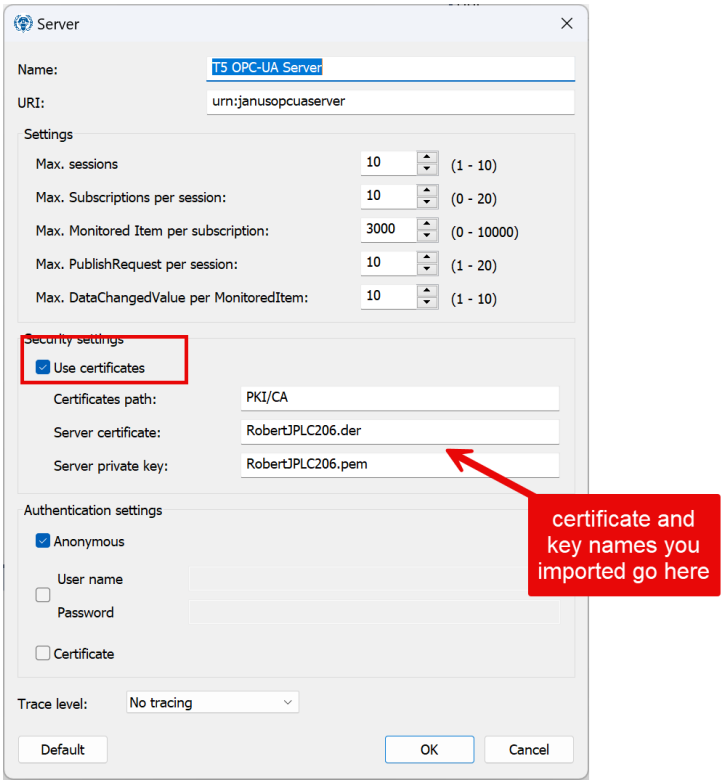
4. Click on the CHOOSE FILE button, navigate to the location where you saved the UaExpert certificate file, and select it.
5. Once the file has been selected, click on the IMPORT button to copy the certificate file to the Janus product.

Now you should have 2 certificates (in the *certs*) folder and 1 key (in the *private* folder) imported to the Janus product as shown below.



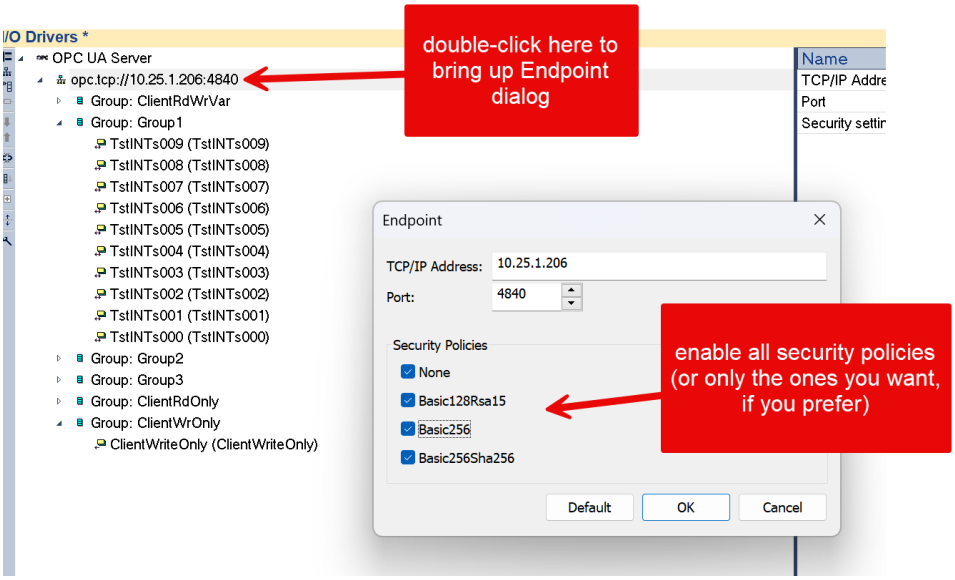
2.4 Configure Secure Communications in the Janus OPC Server

After uploading certificates, the OPC Server Configuration in Workbench needs to be configured for the certificates. First, edit your Janus PLC OPC server configuration in Workbench to turn on certificates.



Next, edit the Endpoint in Workbench to turn on security policies.

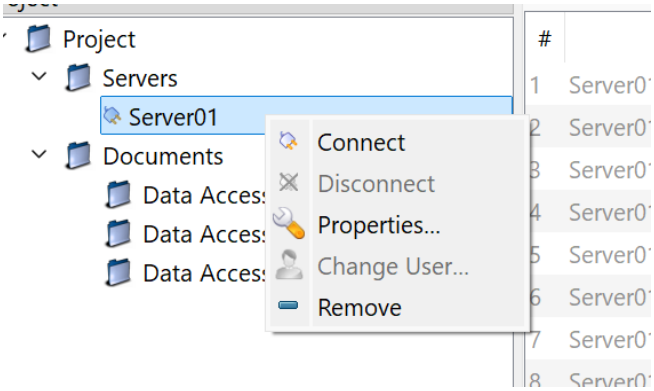
NOTE: The Basic Rsa15 and Basic 256 policies have been deprecated in the latest OPCUA version (V1.4). With the increase in available processing power, the SHA1 hash algorithm included in these policies (used when encrypting signatures) is no longer considered completely secure. They are offered to provide compatibility with clients that do not support the 256Sha256 security policy or don't have enough processing power to service this policy.



Then recompile and download your project to Janus PLC.

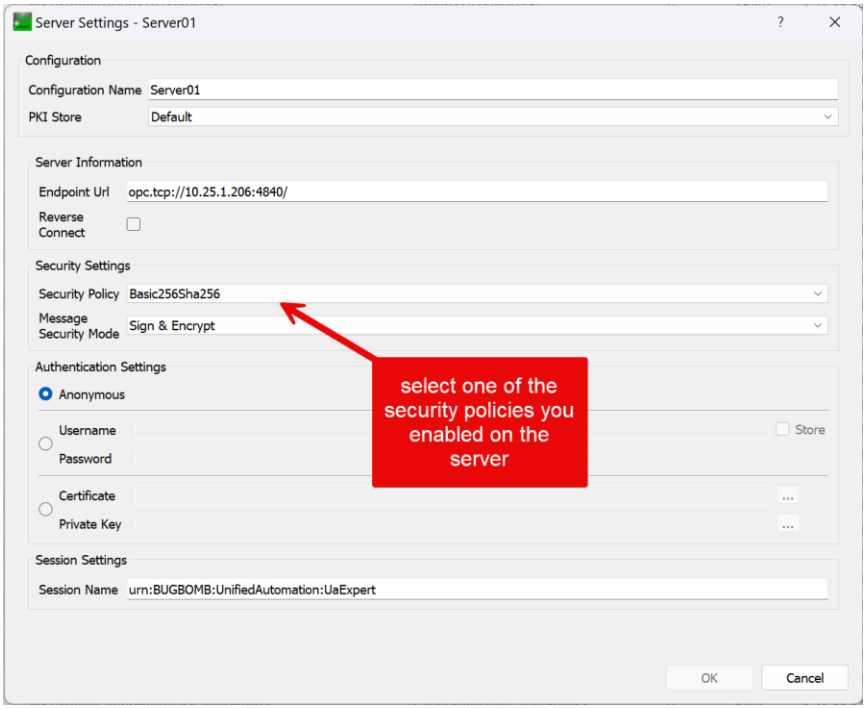
2.5 Configure Secure Communications in UaExpert

In UA-Expert, make sure the server is disconnected, then right-click on it and select *Properties*.

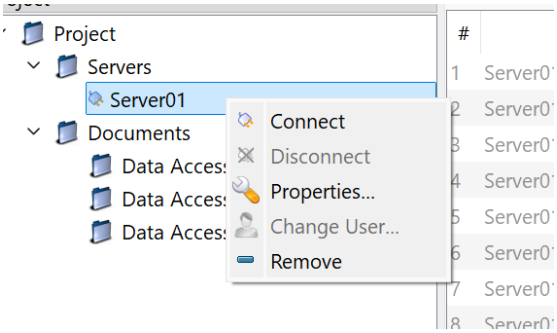


The Server Settings box will come up.

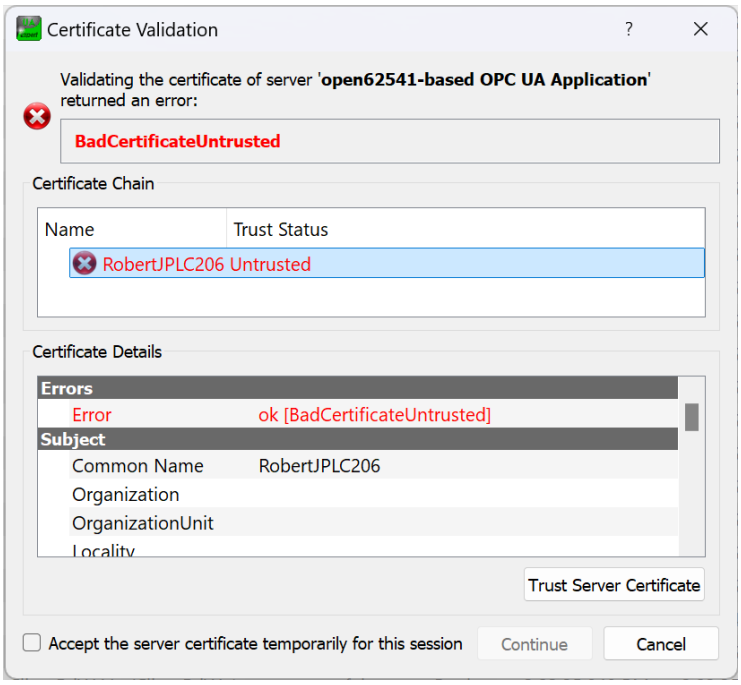
Select the security policy from the dropdown. It must be one of the ones you enabled in the Janus OPC Server configuration in Section 2.4 above. Click OK when done.



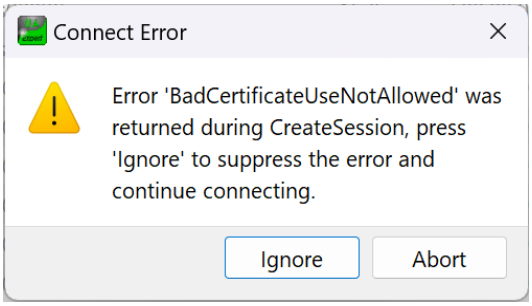
Right-click on the server again and select “Connect”.



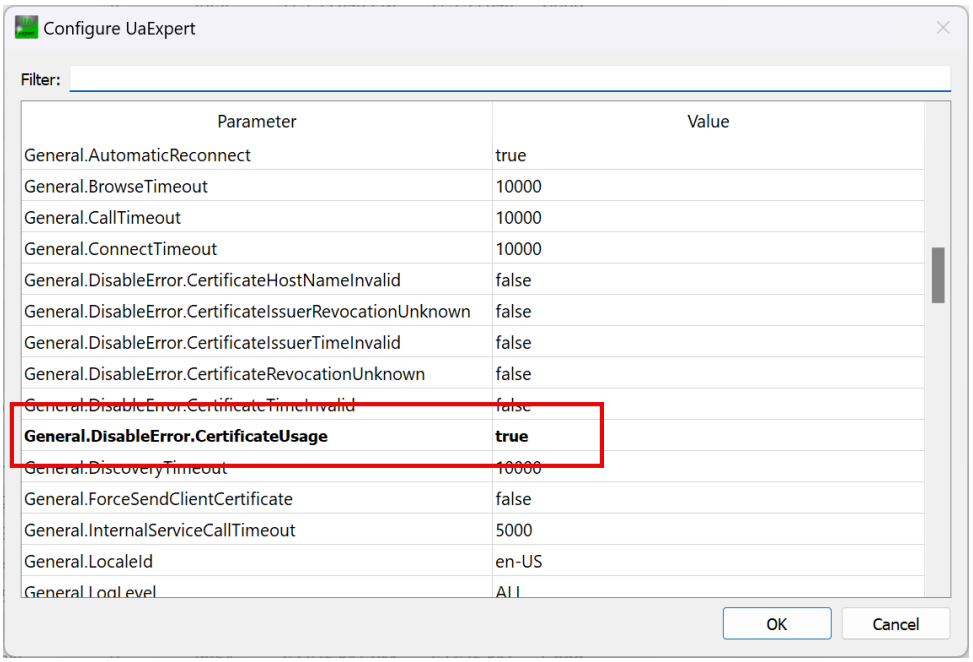
UA-Expert will connect to the Janus OPC server and you will get this prompt, because Janus has sent it’s certificate and you need to trust it. Click “Trust Server Certificate” and “Continue”.



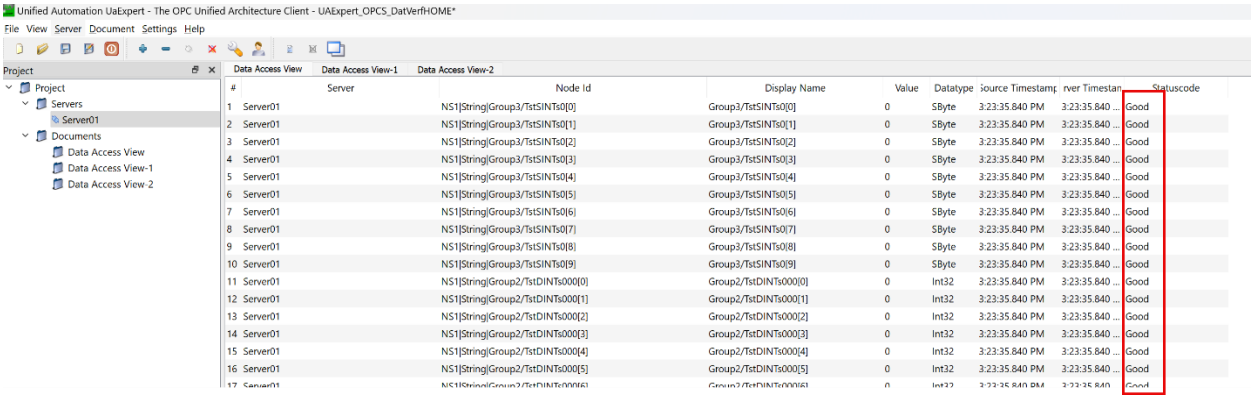
You will probably get this error. Click Ignore. This will happen on every connection.



You can disable checking this error by going to Settings – Configure UaExpert and modifying this setting to TRUE.



If everything worked right, you should now get “Good” data on UA-Expert.



MPORTANT NOTE: The X509 certificate you create using the “XCA” application contains the IP address of the Janus PLC OPC Server (see Section 2.1.2.2 above). Therefore, that certificate and the private key is only good for <u>that</u> IP address. If you use another Janus PLC or JACP with a different IP address, you will need to create a new X509 certificate for that module.