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 <u>MUST</u> 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.



ROCK SOLID PERFORMANCE. TIMELESS COMPATIBILITY.

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.



100			
Ē	∞ OPC UA Server	Name	Value
*B		Name	T5 OPC-UA Server
÷		Max. sessions	2
		Max. Subscriptions per session	5
		Max. Monitored Item per subscription	100
<u>*</u>		Max. PublishRequest per session	10
H		Max. DataChangedValue per MonitoredItem	10
		Trace level	No tracing
<u></u>		Use certificates	
		Certificates path	PKI/CA
		Server certificate	t5opcua.der
		Server private key	t5opcua.pem
		URI	
		Security Check	0

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.

Endpoint				×
TCP/IP Address:	10.25.1.20	9		
Port:	4840	•		
Security Policies				
Basic128Rsa	15			
Basic256				
Basic256Sha	256			
		Default	ОК	Cancel

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.

ŀ		4	or C	PC UA Server	Name	Value			
+ +	話 日		Þ	apc.tcp://172.18.69.101:	TCP/IP Address	172.18.69.101			
-0	-				Port	4840			
1	ļ.				Security settings	1			
1									
Ģ	\$								



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.

		-/
BoolArray	BOOL	[01]
IntArray	INT	[01]

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.

(Group:		×
Properties	Value	OK
Name	Group1	Cancel
		Help

Click OK to add the group.

 CPC UA Server 	Name	Value
# opc.tcp://10.25.1.209:4840	Name	Group1
Group: Group1		
	1	

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:

5	🔺 🖛 OPC UA Server		Name			
*B	 # opc.tcp://10.25.1 	.209:4840	Name			
Ð	Group: Group	01				
4						
1						
¢						
8						
+						
100						
4	Symbol	TAG Name	e Mo	de	TAG	
4	Symbol IntArray[0]	TAG Name	e Mo Rea	de dOnly	TAG BOOL	
· 4	Symbol IntArray[0] IntArray[1]	TAG Name	e Mo Rea Rea	de dOnly dOnly	TAG BOOL BOOL	
· 4	Symbol IntArray[0] IntArray[1] BoolArray[0]	TAG Name	e Mo Rea Rea Rea	de dOnly dOnly dOnly	TAG BOOL BOOL BOOL	
* *	Symbol IntArray[0] IntArray[1] BoolArray[0] BoolArray[1]	TAG Name	e Mo Rea Rea Rea Rea	de dOnly dOnly dOnly dOnly	TAG BOOL BOOL BOOL BOOL	
	Symbol IntArray[0] IntArray[1]	TAG Name	e Mo Rea Rea	de dOnly dOnly	TAG BOOL BOOL	

1.1.6 Add Tagnames

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

IntArray[0] Int1 ReadOnly B IntArray[1] Int2 ReadOnly B BoolArray[0] Bool1 ReadOnly B	TAG	
IntArray[1] Int2 ReadOnly B BoolArray[0] Bool1 ReadOnly B	BOOL	
BoolArray[0] Bool1 ReadOnly B	BOOL	
	BOOL	
BoolArray[1] Bool2 ReadOnly B	BOOL	

1.1.7 *Set the Mode*

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

I	٩	Symbol	TAC Name	Mode	TAC Type
I		Symbol	TAGINAIIIe	Wode	TAG Type
I		IntArray[0]	Int 1	ReadWri	BOOL
I		IntArray[1]	Int2	ReadWri	BOOL
I		BoolArray[0]	Bool1	ReadWri	BOOL
I		BoolArray[1]	Bool2	ReadWri	BOOL
I					

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".

٩	Symbol	TAG Name	Mode	TAG Type
	IntArray[0]	Int1	ReadWrite	INT16
	IntArray[1]	Int2	ReadWrite	INT16
	BoolArray[0]	Bool1	ReadWrite	BOOL
	BoolArray[1]	Bool2	ReadWrite	BOOL

That completes the OPC Server setup.

1.2 UaExpert Configuration

Download UaExpert from the Unified Automation website at <u>https://www.unified-automation.com/downloads/opc-ua-clients.html</u>. 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.

💹 New Application	n Instance Certificate	\times
Subject:		
Common Name:	UaExpert@RocketMINI	¥
Organization:	сп	~
Organization Unit:		*
Locality:		*
State:	TN	~
Country:	US	*
	(Two letter code, e.g. DE, US,)	
OPC UA Information	n	
Application URI: U	ırn:RocketMINI:UnifiedAutomation:UaExpert	*
Domain Names:	RocketMINI	
		*
IP Addresses:	•	
		*
	-	
Certificate Settings		
RSA Key Strength:	2048 bits 🗸 Signature Algorithm: Sha256 🗸 Certificate Validity: 5 Years	~
Password prote	ect private key	
Password:		8
Password (repeat)	:	*
	QK Cance	

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



Unified Automation UaExp	ert - The OPC Uni	fied Architecture C	lient - NewProject												-	ð ×
Eile View Server Docur	ment Settings	Help														
0 🤌 🖯	1		0 ×	2 2		< 🔁										
Deplect		Data Access Viev											6	3 Autobutes		8 V
Fioject			Canada		Mada Id		Diselau Mama	Malue	Datatura	Course Timestame		our Treatmen		Accilouces		
✓			Jerver		Node la		Display Name	value	Datatype	source ninestamp	36	aver ninestamp		ាំ 😏 🧹 💱	۲	0
D Servers														Attribute		Value
✓	ts .															
Address Space														References	Porwar	e × d ∨ O Target DisplayNam
Log																e ×
#																
Timestamp	Source		Server	M	lessage											
10/14/2024 3:11:06.182 PM	UaExpert			Le	aded Server Diagno	stic Plugin (Sta	atic Plugin)									
10/14/2024 3:11:06.182 PM	UaExpert			Lo	aded Data Logger P	lugin (Static P	lugin)									
10/14/2024 3:11:06.182 PM	UaExpert			Le	aded GDS Push Plu	gin (Static Plug	gin)									
10/14/2024 3:11:06.182 PM	UaExpert			Le	oaded File Transfer Pl	lugin (Static Pl	lugin)									
10/14/2024 3:11:06.182 PM	UaExpert			Le	aded XML Nodeset	Export Plugin	(Static Plugin)									1
10/14/2024 3:11:06.182 PM	UaExpert			Lo	aded PubSub Confi	g Plugin (Stati	c Plugin)									
10/14/2024 3:11:06.229 PM	UaExpert			Le	aded UaExpert's cer	tificate.										
10/14/2024 3:11:06.260 PM	CertificateMan	ager		Ci	reate CertificateMan	ager managed	i by GDS									
10/14/2024 3:11:06.260 PM	UaExpert			Le	aded UaExpert's cer	tificate.										
10/14/2024 3:11:06.277 PM	UaExpert			Ui	aExpert is ready to u	se.										

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.

📰 Unified /	Automatio	on UaExpert - T	he 🗘 🗸 U	nified Ar	chitect	ure
File View	Server	Document	ngs	Help		
	BF	1 💽 🔶		> ×	2	2
Address Space					5	×

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.

Mdd Server		?	×
Configuration Name Janus OPC Server PKI Store Default	click on "Advanced tab		~
Discovery Advanced			
Server Information			
Endpoint Url opc.tcp://10.25.1.20		the ID (addroc
Reverse Connect	you se	t in Wo	rkben
Security Settings	serv	er in Se	ection
Security Policy None		1.1.2	
Message Security Mode		~	
Authentication Settings Anonymous Username Password		Store	-
Certificate			
Private Key			
Session Settings			
Session Name Session1			
Connect Automatically			
	ОК	Cano	



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.





Unified Automation UaExpert - The OPC Unified	d Architecture Client - Ne	ewProject*						
<u>File</u> View <u>Server</u> <u>D</u> ocument <u>Settings</u> <u>H</u> elp								
D 💋 🗗 🙆 🔕 单 🗢 🗙	🔌 🤰 🖻 🕿 🕻	2						
Project & ×	Data Access View							٥
 Project Servers Janus OPC Server@10.25.1.209 Documents Data Access View 	 # Server 1 Janus OPC 2 Janus OPC 3 Janus OPC 4 Janus OPC 	Node Id NS1 String NS1 String NS1 String	Display Name Group1/Bool2 Group1/Bool2 Group1/Int1 Group1/Int2	Value false false 0 0	Datatype Boolean Boolean Int16 Int16	Source Timestamp 6:03:09.175 PM 6:03:09.175 PM 6:03:09.175 PM 6:03:09.175 PM	Server Timestam; 6:03:09.175 PM 6:03:09.175 PM 6:03:09.175 PM 6:03:09.175 PM	3 S Good Good Good
Address Space 🗗 🗙	tags in Acc	ito the Data ess View						
 No riigniight Root © Objects © Objects © Group1/Bool1 > © Group1/Bool2 > © Group1/Int1 > © Group1/Int2 > © Server > © Types > © Views 								

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.

E Subscription Settings	? X
Publishing Interval:	500
Life Time Count:	2400
Max Keep Alive Count:	10
Max Notifications Per Publish:	0
Priority:	0
Show count values	○ Show counts as ms
Ok	Cancel



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

💹 Monitored Item Set	tings	?	×
Sampling Interval:	250.00		^
Queue Size:	1		▲ ▼
Discard Oldest:			
Data Change Trigger:	Status/Value		\sim
Deadband Type:	None		~
Deadband Value:	0.00		▲ ▼
	ОК	Car	ncel

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 <u>authenticate</u> 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 <u>encrypt</u> 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: <u>https://hohnstaedt.de/xca/index.php</u>.

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.



X Certif ile Impo	ficate and Ke ort Token	y manag Extra	gement Help						_)
Private Ke	eys Certif	icate sign	ning requ	ests Cert	ificates	Templates	Revocati	on lists			
	nternal nam	e R	Type RSA	Size 2048 bit	Use t 1	Password Common			New Key		
									Export		
									Import		
								Im	port PFX (PKCS#	12)	
									Show Details		
									Delete		

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.

🕅 X Certifi	cate and Key management	?	\times
New Ke	ey .		
Please give a	name to the new key and select the desired keysize		
Key proper	ties		
Name	MyServerKey		
Keytype	RSA		\sim
Keysize	2048 bit		~
Rememb	er as default Create Cancel	He	lp

Confirm that key was successfully created.

X Certificate	e and Key manag	ement						
File Import	Token Extra	Help						
Private Keys	Certificate signi	ing reque	ests	Certifi	cates	Templates	Revocation lists	
Interr	nal name	Туре	9	Size	Use	Password		
0=	SERVER	RSA	204	8 bit	1	Common		
	MyServerKey	RSA	204	8 bit	0	Common		
	А	🔶 X Ce	rtifica	te and k	ey mar	agement		×
			Suc	ccessful	y create	ed the RSA p	rivate key 'MyServe	'Key'
							ОК	

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 button is selected.

2					~
13				a) Consider	- 72m
Netscape A	dvanced Com	ment			
					~
		Show request			
					~
	SHA 256				~
					~
		Apply extensions Apply	subject	Apply all	
		ОК	Cancel	He	lp
	Netscape A	Netscape Advanced Com	Netscape Advanced Comment Show request Show request	Netscape Advanced Comment Show request Show request Show request Show request Show request Show request Show request Show request Apply extensions Apply subject OK Cancel	Netscape Advanced Comment Show request Show request Show request Show request SHA 256 Apply subject Apply all OK Cancel He



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.

X Certificate and Key	management							?	Х
Create x509 Ce	ertificate								- 7in
Source Subject E	Extensions Key	/ usage	Netscape	Advanced	Comment				
Internal Name <mark>MyServer</mark>	rCert								
Distinguished name									
countryName				organizat	ionalUnitName				
stateOrProvinceName				commonN	ame	MyServerCert			
localityName				emailAdd	ess				
organizationName									
Туре	2			C	ontent			Add	
							1	Delete	
									-
Private key									
	10 1 11						-		_
MyServerKey (RSA:20	48 DIT)					✓ Used keys to	Gener	ate a new k	ey
						ОК	Cancel	He	elp



When finished, Select the EXTENSIONS tab.

X Certificate and Key managem	lent	?	×
Create x509 Certifica	e	Premiande Relative", 74	
Source Subject Extensions	Key usage Netscape Advanced Comment		
X509v3 Basic Constraints	Key identifier		
Type End Entity	V X509v3 Subject K	ey Identifier	
Path length	Critical X509v3 Authority	Key Identifier	
Not after	2023-04-05 14:37 GMT V Midnight Local time No well-defined	expiration	
X509v3 Subject Alternative Name	URI:um:janusobcuaserver,IP:172.18.74.26	Edit	
X509v3 CRL Distribution Points		Edit	1
Authority Information Access		Edit	1
	OCSP Must Staple		1
	OK Cancel	Help	

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) <u>exactly</u> 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.

💓 X Certificate and Key management				- 🗆 X
File Import Token Extra Help				
Private Keys Certificate signing requests	Certificates Templates	Revocation lists		
Internal name common MyServerCert MyServe SERVER SERVER	Name CA Se irCert No 3F6F42AC No 3EB707F6	rial Expiry date DD5DE10D 4/5/2023 2CB21520 3/31/2023	CRL Expiration	New Certificate Export Import Show Details Delete
Successfully created	the certificate 'MyServerCert	, 1		Import PKCS#12 Import PKCS#7 Plain View
Database: C:\Users\ceskew\Documents\XCA	CertDatabase.xdb	Search		



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.

📌 X Certificate and Key management				- [) X
File Import Token Extra Help					
Private Keys Certificate signing request	ts Certificates Templates	Revocation lists			
Internal name comm	nonName CA Ser	rial Expiry date	CRL Expiration	New Certificate	
MyServerCert MySer	verCert No 3F6F42AC CR No 3EB707F6	DD5DE10D 4/5/2023 2CB21520 3/31/2023		Export	
				Import	
				Show Details	
				Delete	
				Import PKCS#12	
				Import PKCS#7	
				Plain View	
				Franinata Mindone Jine	
Database: C:\Users\ceskew\Documents\XCACertDatabase.xdb Search					

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

₩ X Certificate and Key management	? ×	
Certificate export	(a) Promised (Construction of the Construction	
Name MyServerCert		
Filename C:\Users\ceskew\Desktop\MyServerCert\der		
Binary DER encoded file	A A A A A A A A A A A A A A A A A A A	
Export comment into PEM file	Export Format DER (*.cer)	,
	OK Cancel Help	

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.

N Certificate and Key management		– 🗆 X
File Import Token Extra Help		
Private Keys Certificate signing requests	Certificates Templates Revoc	ation lists
Internal name Type S	Size Use Password	New Key
MyServerKey RSA 204	8 bit 1 Common	Export
		Import
		Import PFX (PKCS#12)
		Show Details
		Delete
		o Hox
Database: C:\Users\ceskew\Documents\XCAC	CertDatabase.xdb	Search

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

₩ X Certificate and Key management		?	×
Export private key [RSA]			
Name MyServerKey			
Filename C:\Users\ceskew\Desktop\MyServerKey.pem			
Unencrypted private key in text format			
Export comment into PEM file	Export Format	PEM private (*.pem)	~
	ОК	Cancel	Help

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.

Product Information			
Application Information	Product Information		
Configuration	General Settings		
Event Log	Network Settings		
Statistics	Security Settings		
Error Descriptions & Status	Clock Settings		
Display All Pages	FileManagement		
Custom HTML (graphics)	Firmware Update		
Acknowledgements	Product Reset		
Product Support	Clock Synchronization Mode		

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

l⊊ile Management
Select the file operation to perform: Import Public Certificate from Computer
Select the Public Certicate you want to Import.
Certificate File No file chosen
Import
File Manager Idle

- 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.

File Management	
Select the file operation to perform: Import Private Key from Computer Refresh	~
Select the Private Certicate you want to Import. Certificate File Choose File No file chosen	
Import File Manager Idle	

- 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.

File Management
Select the file operation to perform: Delete Files from System SD Card Refresh File Lists
Click on the files or folders you want to delete.
Deletable Files/Folders

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.

```
comation UaExpert - The OPC Unified Architecture Client - U,
```

rver Document	Settings Help								
9 🛛 🖸	Plugins			R					
	& Configure UaExpert			s View		C			
		Man	age Cert	tifi	cat	es			
vers	_				1	Server0	1		
server01					2	Server0	1		

The Manage Certificates dialog will come up.

efault certii	ficate Stor	e GDS Ser	ver 1 ned certificate					
Certific	cates	120 13300						
State	us Own C	Name UaExpert	Valid From 10/14/2024 4:11 PM	Valid To 10/13/2029 4:	Organization CTI	OrganizationUnit	Locality	State TN
_						_		
Certific	cate Revoo	cation Lists Valid Fro	m Next Up	odate	Organization	OrganizationUnit	Locality	State

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.



Product Information Application Information	Product Information		
Configuration	General Settings		
Event Log	Network Settings		
Statistics	Security Settings		
Error Descriptions & Status	Clock Settings		
Display All Pages	FileManagement		
Custom HTML (graphics)	Firmware Update		
Acknowledgements	Product Reset		
Product Support	Clock Synchronization Mode		

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

ÿ File Management
Select the file operation to perform: Import Public Certificate from Computer
Select the Public Certicate you want to Import.
Choose File No file chosen
Import
File Manager Idle

- 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.

File Management	
Select the file operation to perform: Delete Files from System SD Card Refresh File Lists	~
Click on the files or folders you want to delete. Deletable Files/Folders	
<pre>> graphics > certs MyServerCert.der Uaexpert.der > mrvate MyServerKey.pem > User</pre>	



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.

😨 Server				×	
Name:	T5 OPC-UA Server				
URI:	urn:janusopcuaserv	er			
Settings					
Max. sessions		10	(1 - 10)		
Max. Subscriptions per session	on:	10 🗘	(0 - 20)		
Max. Monitored Item per sul	oscription:	3000 🗘	(0 - 10000)		
Max. PublishRequest per ses	sion:	10 🗘	(1 - 20)		
Max. DataChangedValue per	MonitoredItem:	10	(1 - 10)		
			. ,		
	DKT/CA				
Certificates path:				-	
Server certificate:	RobertJPLC206	o.der	-	_	
Server private key:	RobertJPLC206	5.pem		_	
Authentication settings				certifica	te an
Anonymous				kev nam	ies vo
User name				imported	go he
Password					
1 donord					
Trace level: No tracing	~				
Default		OK	Cano	cel	

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

//O Drivers *	double-click here to bring up Endpoint dialog	Name TCP/IP Addre Port Security settin
 P TstINTs006 (TstINTs006) P TstINTs005 (TstINTs005) P TstINTs004 (TstINTs004) P TstINTs002 (TstINTs003) P TstINTs002 (TstINTs002) P TstINTs001 (TstINTs001) P TstINTs001 (TstINTs000) Group: Group2 Group: Group3 Group: ClientWrOnly ClientWriteOnly (ClientWriteOnly) 	Endpoint TCP/IP Address: 10.25.1.206 Port: 4840 - Security Policies © None © Basic128Rea15 © Basic256 © Basic256Sha256	enable all security policies (or only the ones you want, if you prefer)



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.

Server Setting	s - Server01		?
onfiguration			
Configuration Na	me Server01		
KI Store	Default		· · · · · · · · · · · · · · · · · · ·
Server Informa	tion		
Endpoint Url	opc.tcp://10.25.1.206:4840/	1	
Reverse Connect			
Security Setting	IS		
Security Policy	Basic256Sha256		~
Message Security Mode	Sign & Encrypt		~
Authentication	Settings	select one of the	
Username		enabled on the	Store
Password		server	
Certificate			
Private Key			
Session Setting	s		
Session Name	urn:BUGBOMB:UnifiedAuton	nation:UaExpert	



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".

returned an error:		
BadCertificateUn	trusted	
ificate Chain		
ame	Trust Status	
RobertJPLC200	5 Untrusted	
RobertJPLC200	5 Untrusted ok (BadCertificateUntrusted]
RobertJPLC200	5 Untrusted ok [BadCertificateUntrusted Bobert IPI C206]
RobertJPLC200 ificate Details rors Error bject Common Name Organization	5 Untrusted ok [BadCertificateUntrusted RobertJPLC206]
RobertJPLC200 ificate Details rors Error bject Common Name Organization OrganizationUnit	5 Untrusted ok [BadCertificateUntrusted RobertJPLC206]
RobertJPLC200 ificate Details rors Error bject Common Name Organization OrganizationUnit Locality	5 Untrusted ok [BadCertificateUntrusted RobertJPLC206]

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





ROCK SOLID PERFORMANCE. TIMELESS COMPATIBILITY.

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

Filter:				
Parameter		Valu	e	
General.AutomaticReconnect	true			
General.BrowseTimeout	10000			
General.CallTimeout	10000			
General.ConnectTimeout	10000			
General.DisableError.CertificateHostNameInvalid	false			
${\tt General.Disable Error.Certificate {\tt IssuerRevocation Unknown}}$	false			
General. Disable Error. Certificate Issuer Time Invalid	false			
General.DisableError.CertificateRevocationUnknown	false			
General:DisableEnor.CertificateTimeInvalid	false			
General.DisableError.CertificateUsage	true			
General:DiscoveryTimeout	10000			
General.ForceSendClientCertificate	false			
General.InternalServiceCallTimeout	5000			
General.LocaleId	en-US			
General Logi evel	ALL			

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

Unified Automation UaExpert - The OPC U	nified Architecture Clien	t - UAExpert_OPCS_Dat	VerfHOME*						
ile View Server Document Settings Help	5								
) 🖉 🗟 💆 🍖 🕤	🗙 🔌 🤶 🖹	M 🗖							
roject d	× Data Access View	Data Access View-1	Data Access View-2						
 Moject 	#	Server	Node Id	Display Name	Value	Datatype	e Source Timestam	rver Timestar	Statuscod
✓	1 Server01		NS1 String Group3/TstSINTs0[0]	Group3/TstSINTs0[0]	0	SByte	3:23:35.840 PM	3:23:35.840	Good
Server01	2 Server01		NS1 String Group3/TstSINTs0[1]	Group3/TstSINTs0[1]	0	SByte	3:23:35.840 PM	3:23:35.840	Good
Documents	3 Server01		NS1 String Group3/TstSINTs0[2]	Group3/TstSINTs0[2]	0	SByte	3:23:35.840 PM	3:23:35.840	Good
Data Access View	4 Server01		NS1[String]Group3/TstSINTs0[3]	Group3/TstSINTs0[3]	0	SByte	3:23:35.840 PM	3:23:35.840	Good
Data Access View-1	5 Server01		NS1 String Group3/TstSINTs0[4]	Group3/TstSINTs0[4]	0	SByte	3:23:35.840 PM	3:23:35.840	Good
Data Access view-2	6 Server01		NS1[String]Group3/TstSINTs0[5]	Group3/TstSINTs0[5]	0	SByte	3:23:35.840 PM	3:23:35.840	Good
	7 Server01		NS1 String Group3/TstSINTs0[6]	Group3/TstSINTs0[6]	0	SByte	3:23:35.840 PM	3:23:35.840	Good
	8 Server01		NS1[String]Group3/TstSINTs0[7]	Group3/TstSINTs0[7]	0	SByte	3:23:35.840 PM	3:23:35.840	Good
	9 Server01		NS1[String]Group3/TstSINTs0[8]	Group3/TstSINTs0[8]	0	SByte	3:23:35.840 PM	3:23:35.840	Good
	10 Server01		NS1[String]Group3/TstSINTs0[9]	Group3/TstSINTs0[9]	0	SByte	3:23:35.840 PM	3:23:35.840	Good
	11 Server01		NS1[String]Group2/TstDINTs000[0]	Group2/TstDINTs000[0]	0	Int32	3:23:35.840 PM	3:23:35.840	Good
	12 Server01		NS1 String Group2/TstDINTs000[1]	Group2/TstDINTs000[1]	0	Int32	3:23:35.840 PM	3:23:35.840	Good
	13 Server01		NS1 String Group2/TstDINTs000[2]	Group2/TstDINTs000[2]	0	Int32	3:23:35.840 PM	3:23:35.840	Good
	14 Server01		NS1 String Group2/TstDINTs000[3]	Group2/TstDINTs000[3]	0	Int32	3:23:35.840 PM	3:23:35.840	Good
	15 Server01		NS1 String Group2/TstDINTs000[4]	Group2/TstDINTs000[4]	0	Int32	3:23:35.840 PM	3:23:35.840	Good
	16 Server01		NS1 String Group2/TstDINTs000[5]	Group2/TstDINTs000[5]	0	Int32	3:23:35.840 PM	3:23:35.840	Good
	17 Senver01		NS1IString/Group2/TetDINTe00061	Group2/TetDINITe000161	0	Int22	2-72-25 SAD DM	2-22-25 840	Good

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.

