OPC UA Server

for Win-GRAF

User Manual

(Version 2.0)

WARRANTY

All products manufactured by ICP DAS are warranted against defective materials for a period of one year from the date of delivery to the original purchaser.

WARNING

ICP DAS assumes no liability for damages consequent to the use of this product. ICP DAS reserves the right to change this manual at any time without notice. The information furnished by ICP DAS is believed to be accurate and reliable. However, no responsibility is assumed by ICP DAS for its use, nor for any infringements of patents or other rights of third parties resulting from its use.

COPYRIGHT

Copyright © 2024 by ICP DAS. All rights are reserved.

TRADEMARK

Names are used for identification only and may be registered trademarks of their respective companies.

CONTACT US

If you have any questions, please feel free to contact us via email at:
service@icpdas.com
service.icpdas@gmail.com

Revision

Revision	Date	Description	Author
2.0	08.03.2024	Description of the "K5BusOpcUaServ2" OPC UA server plug-in wizard	M.K

Contents

1 INTRODUCTION....5

2 SOFTWARE INSTALLATION....5

2.1 WORKBENCH....5

3 OPC UA SERVER CONFIGURATION....6

3.1 SERVER CONFIGURATION PROCEDURE....6

3.1.1 Start the OPC UA Server Configuration Wizard....6

3.1.2 Configure UA Endpoint....7

3.1.2.1 Discovery and Session Endpoint URL....8

3.1.2.2 Security Policies....8

3.1.2.3 Application Description....10

3.1.2.4 Identity Token....11

3.1.2.5 Security Check Option....12

3.1.2.6 User Account....13

3.1.2.7 Server Certificate....14

3.1.2.8 Publishing PLC Variables....18

3.1.2.9 Build and Download PLC Application....21

3.1.2.10 Connect Client to Server....22

4 USING UAEXPERT® CLIENT TO CONNECT TO THE WIN-GRAF OPC UA SERVER.....25

4.1 NO SECURITY POLICY AND ANONYMOUS IDENTITY TOKEN....25

4.1.1 Win-GRAF server setting....25

4.1.2 UA-Expert Client....26

4.2 SECURITY POLICY AND LOGIN ACCOUNT (USERNAME AND PASSWORD)....31

4.2.1 Win-GRAF server setting....31

4.2.2 UA-Expert Client....33

5 SERVER OPERATION ERROR....40

5.1 SERVER FAILED TO CREATE ENDPOINTS....40

5.2 COMMUNICATION ERROR MESSAGE....40

5.2.1 BadCertificateHostNameInvalid....40

5.2.2 BadSecurityModeInsufficient....43

5.2.3 BadUserAccessDenied....43

5.2.4 BadUserAccessDenied, BadSecurityCheckFailed....44

5.2.5 BadSecurityChecksFailed....44

6 APPENDIX....44

6.1 SUPPORTED FEATURES....44

6.2 Default Settings....46

1 Introduction

OPC Unified Architecture (UA) is an open standard created by the OPC Foundation and defines a platform independent interoperability standard. OPC UA offers a secure method of client-to-server connectivity and has the ability to connect securely through firewalls and over VPN connections.

For the majority of user applications, the most relevant components of the UA standard are as follows:

- Secure connections through trusted certificates for client and server endpoints.
- Robust item subscription model to provide efficient data updates between clients and servers.
- An enhanced method of discovering available information from participating UA servers.

The purpose of this manual is to introduce the main functions and configuration supported by the Win-GRAF OPC UA server. In addition configuration and testing procedure are given to familiarize yourselves with the features, functions, limitations and operating characteristics of specific settings.

2 Software Installation

2.1 Workbench

The Win-GRAF workbench setup program "Win-GRAF_Workbench_xxxx_Setup" automatically installs the necessary OPC UA plugin library and wizard for configuring the server.

C:\Program Files (x86)\Win-GRAF Workbench\Win-GRAF Wb xx.xx\IOD\K5BusOpcUaServ2.dll

3 OPC UA Server Configuration

You should be familiar with the OPC UA specification and the communication methods used for the data exchange between OPC UA servers and clients. If security plays an vital role in your application a deeper understanding of how OPC UA certificate are used by the servers and clients to securely identify and communicate with each other is being required.

This chapter gives a quick overview of the OPC UA server configuration procedure using the Win-GRAF workbench and describes the supported configuration parameters.

3.1 Server Configuration Procedure

This section provides an overview of adding and configuring an OPC UA server with the Win-GRAF Workbench and describes the essential server parameters. The server must provide information such as supported protocol, network address, and security settings in order for the client to connect.

The endpoint in OPC UA stores all the necessary information required to establish a connection client and server. The Win-GRAF supports only one endpoint.

All information which is required to establish a connection between client and server is stored in a so-called endpoint. A server can provide several endpoints, each containing

3.1.1 Start the OPC UA Server Configuration Wizard

Start the Win-GRAF workbench and create a new project.

Select '*OPC UA Server 2.0 (ICP DAS)*' wizard

1. Open the Fieldbus Configurations window by clicking on the '*Fieldbus Configuration*' button in the toolbar or double clicking the '*Fieldbus Configuration*' node in the workspace.

2. Open the plug-in selection list by clicking the '*Insert Configuration*' button on the left toolbar.
3. Select '*OPC UA Server 2.0 (ICP DAS)*' plug-in from the '*Add Configuration*' dialog.

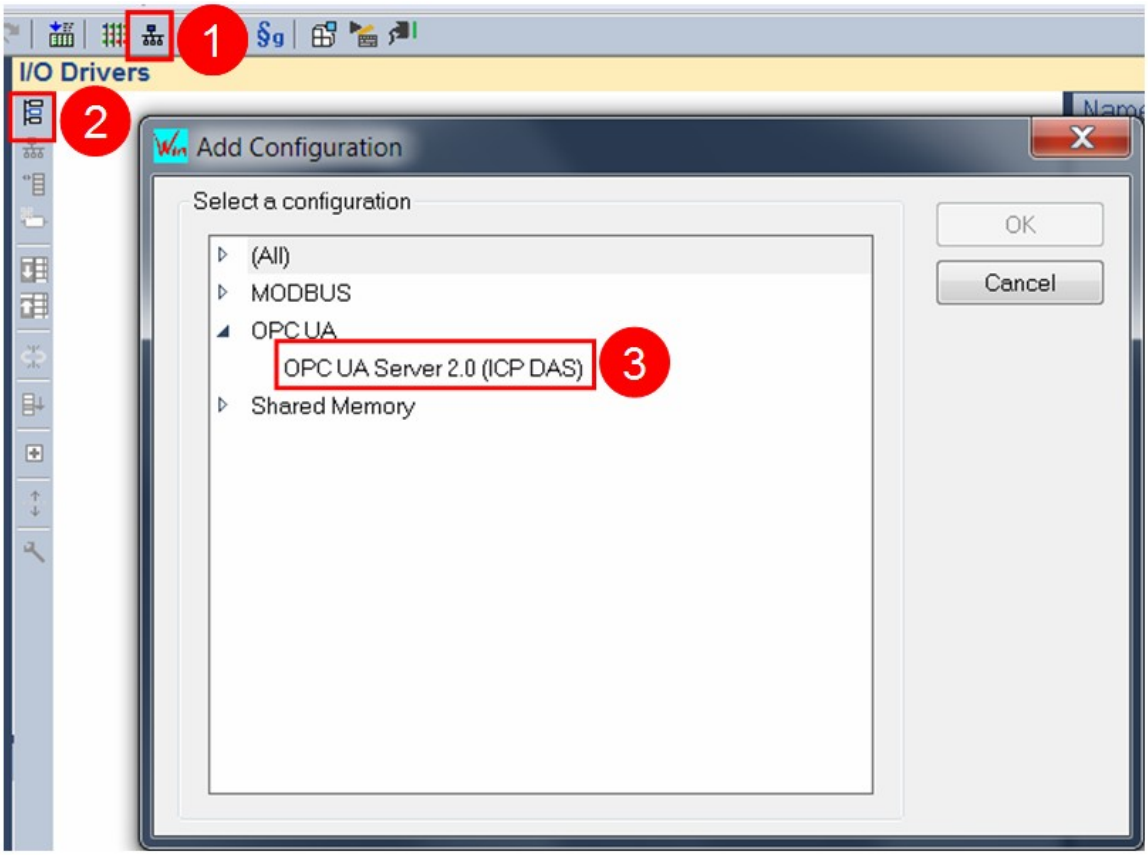


Figure 1: Start the OPC UA server wizard

3.1.2 Configure UA Endpoint

The Win-GRAF OPC UA server provides one session endpoint where clients can connect to.

The endpoint setting (Error: Reference source not found) for the OPC UA Server module determine how the server will appear on the network, as well as how OPC UA clients may communicate with it.

Click on the '*Insert Master/Port*' button on the left toolbar to open the server configuration dialog box.

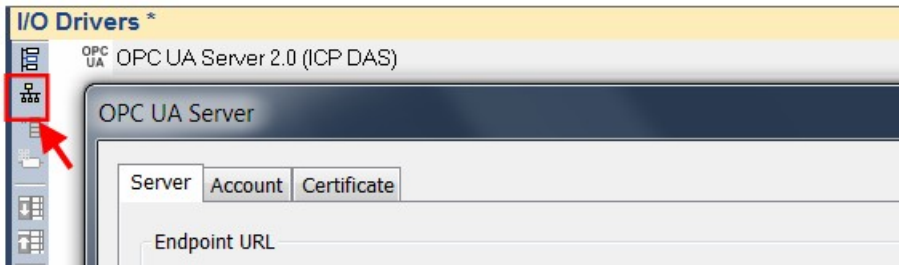


Figure 2: Essential OPC UA server configuration

3.1.2.1 Discovery and Session Endpoint URL

The Session and Discovery Endpoint URLs provides the basic information that clients need to connect to a server, including the protocol, the host name or IP address, and the port number. A Discovery Endpoint allows the client to access to Discovery Services without a Session and without message security.
For the Win-GRAF OPC UA server, the discovery URL is identical to the endpoint URL.

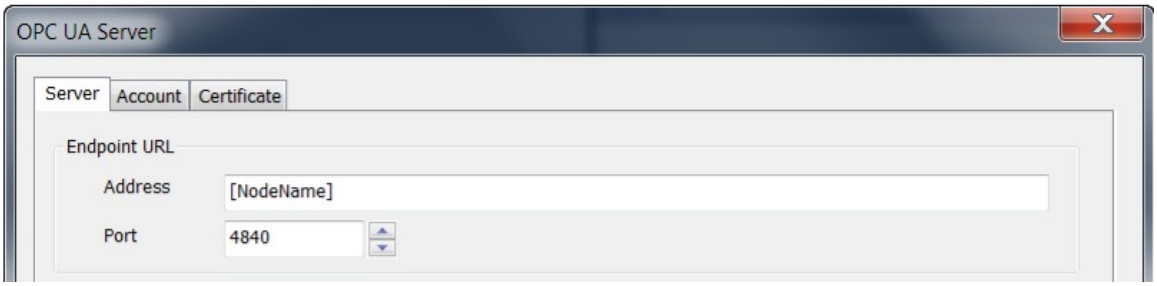


Figure 3: Discovery and Session Endpoint URL

Set the endpoint parameters such as the address and port number for the OPC UA server. Only one endpoint is supported by the Win-GRAF server. Use the key string '*[NodeName]*' to automatically retrieve the hostname of the actual computer or device.

Examples of endpoint URL:

- opc.tcp://HostNameOfDevice:4840
- opc.tcp://192.168.201.100:4840

3.1.2.2 Security Policies

In the '*Security Policies*' section, select the policies that the OPC UA server may use to communicate with OPC UA clients. In order for a server and client to communicate with

each other, they must have at least one security policy in common. More than one security options for the server can be selected. This allows clients with different security settings to access the same server.

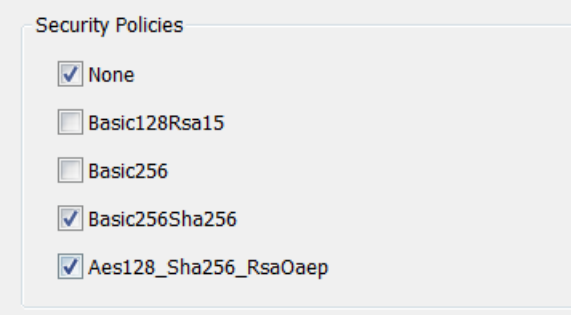


Figure 4: Encryption types (Security policies options) supported by the server

Security Policies Option	Description
None	• Communication between server and client does not need to be encrypted. Check '*None*' if your application does not need to use security certificates for encrypted communication. • Default setting: Enabled • Message Mode: None
Basic128Rsa15	• The server will use and recognize 128-bit AES encryption. • Message Mode: Sign, Sign and Encrypt • Default setting: Disabled
Basic256	• The server will use and recognize 256-bit AES encryption. • Message Mode: Sign, Sign and Encrypt • Default setting: Disabled
Basic256Sha256	• The server will use SHA256 for the signature digest and 256-bit Basic as the message encryption algorithm • Message Mode: Sign, Sign and Encrypt • Default setting: Enabled
Aes128_Sha256_RsaOaep	• The server will use and recognize Aes128-Sha256-RsaOaep encryption. • Message Mode: Sign, Sign and Encrypt • Default setting: Enabled

Table 1: Security policies options

If none of the encryption options are selected then the communication between the server and client will not be signed or encrypted. In this case, only clients whose security policy is set to '***None***' can exchange data.

Both ***Sign*** and ***Sign&Encrypt*** modes are supported for Basic128RAS1, Basic256, Basic256SHA256 etc. settings. Sign mode guarantees the authenticity of messages exchanged between client and server. The Encrypt mode uses encryption and decryption to ensure that the data exchanged cannot be read by third parties.

For all the policies option (except '*None*') both OPC UA clients and servers will have their own certificates. The server will have to trust the client's certificate and the client will have to trust the server's certificate before a client - server session can be established. This means the client's certificate file has to be in the '*%InstallDir%\OPC-UA\Server\PKI\trusted\cert*' folder of the server and the server certificate has to be in the trusted folder of the client.

The server certificate is sent to the client when a connection is being established, and the client certificate on the other hand is sent to the server rejected folder: '*%InstallDir%\OPC-UA\Server\PKI\rejected*'. Move the client certificate from the rejected folder to the '*trusted\certs*' folder: '*%InstallDir%\OPC-UA\Server\PKI\trusted\certs*'. Depending on the Win-GRAF controller type this has to be done either manually, via Certificate manager or via a web browser.

If the self-signed certificate has been enabled (Figure 9) the server will create a certificate even if the '*None*' security option has been selected. The client will receive the certificate when a connection is being created. For the '*None*' security mode the server does not need the client certificate for the client to create a session with the server because the communication data is not encrypted.

3.1.2.3 Application Description

Enter the application description:

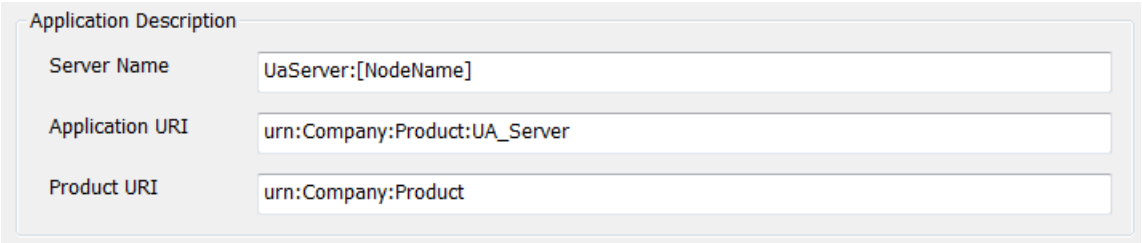


Figure 5: Application description

Server Setting	Description
Server Name (Application Name)	• The name of the server. • This name will be stored under the keyword '*[ServerName]*' which means strings containing the keyword are modified by the server by replacing the keyword with the server name. • Use the key string '[NodeName]' to automatically retrieve the hostname of the actual computer or device. - For example: If the computer name is '*DESKTOP123*'

	then the string '*UaServer:[NodeName]*' will generate the common name '*UaServer:DESKTOP123*'
Application URI (Server URI)	• Every server shall have a globally unique identifier called the server or application URI. • This URI is the unique identifier for the server application. It is also part of the server discovery information and the server certificate. This namespace contains typically server specific diagnostic nodes. • The default name is '*urn:Company:Product:UA_Server*' • The following key strings are supported: - '*[NodeName]*' - retrieves the host name of the actual computer. - '*[ServerName]*' - replaces the key string with the server name • Example: - '*urn:MyCompany:MyProduct:MyServer*' - '*urn:[NodeName]:MyProduct:[ServerName]*'
Product URI	• A globally unique identifier for the product the server belongs to. • Default name: '*urn:Company:Product*' • The following key strings are supported: - '*[NodeName]*' - gets the host name of the actual computer. - '*[ServerName]*' - replaces the key string with the server name • example: - '*urn:MyCompany:MyProduct*' - '*urn:[NodeName]:MyProduct*'

Table 2: Server information

3.1.2.4 Identity Token

When a user attempts to connect from an OPC UA client to an OPC UA server, the server must confirm the user's identity before allowing the connection from the client. The Win-GRAF server currently supports two different ways to authenticate a user during session activation:

- Anonymous Identity Token
- User Name Identity Token

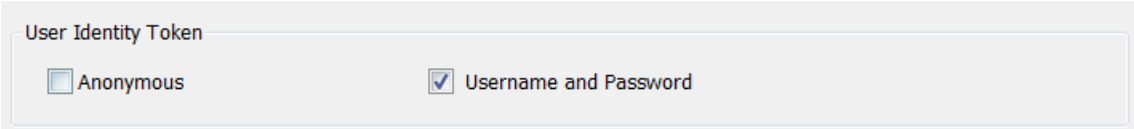


Figure 6: Identity token

Identity Token Option	Description
Username and Password	User Name Identity Token • Require clients to always enter a username and password before a session with the server can be started. • This option is only available if at least one of the encrypted security policy options is selected. • It is therefore necessary to set up a account for each user (Figure 8). The '*Account*' tab provides a list in which the user anme with the password can be entered. • Default: Enabled
Anonymous	• Application based security is disabled. No username and password is required for the client to login. • Allows the client to create a session with the server without the client certificate file to be stored in the trusted folder of the server. • It is important to remember that the server will not create an endpoint and allow any client to connect, if no server certificate with its private key exist in the directories '%InstallDir%\OPC-UA\Server\PKI\own\certs\' and '%InstallDir %\OPC-UA\Server\PKI\own\private\'. Therefore enable the self-signed certificate option to inform the server to generate a new certificate and private key if no certificate exists. • Client only has got read and no write access. PLC variables can only be read by the client and can not be changed. • Default: Disabled

Table 3: Identity token information

3.1.2.5 Security Check Option

Select the security check option:

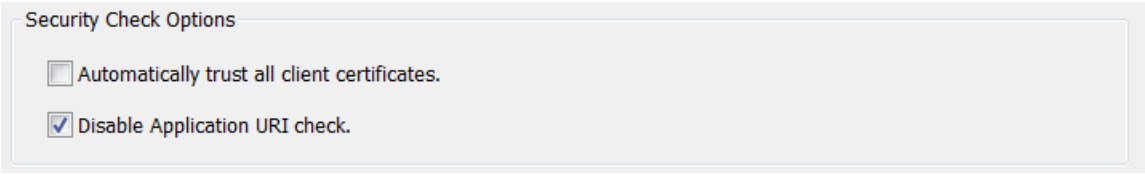


Figure 7: Security check option

Security Check Option	Description
Automatically trust all client certificates	All clients are allowed to connect • If you automatically trust all clients certificate the server mode is switching from the OPC UA double-side trust check into a

Security Check Option	Description
	single-side trust check. The OPC UA server will be public for every client and therefore user authentication should be enabled ('User and Password' option). • The client certificates will not be listed or stored in any of the client directories, such as '*%InstallDir%\OPC-UA\Server\PKI\trusted\certs*'. • Default: Disabled
Disable Application URI check	• It allows clients with a certificate whose URI does not match the server's '*Application URI*' to connect to the server. • Disables the '*Application URI*' match check between client certificate and parameter in session creation. The check is required for compliant OPC UA servers but older clients may provide a wrong '*Application URI*'. • Default: Enabled

Table 4: Security check options

3.1.2.6 User Account

Set up user accounts to give individuals access to the OPC UA server data. User accounts only needs to be created if the '*Username and Password*' option is selected as user identity token.

1. Select the '*Account*' tab
2. Click '*Add*' button to add a new user to the account list.
3. In the '*OPC UA User*' dialog enter a username with password and the access write restriction. The '*This user can write to variables*' option allows the administrator to grant the user only read access or both read and write access. After confirming the new user account with '*OK*', the new entry appears in the user account list.

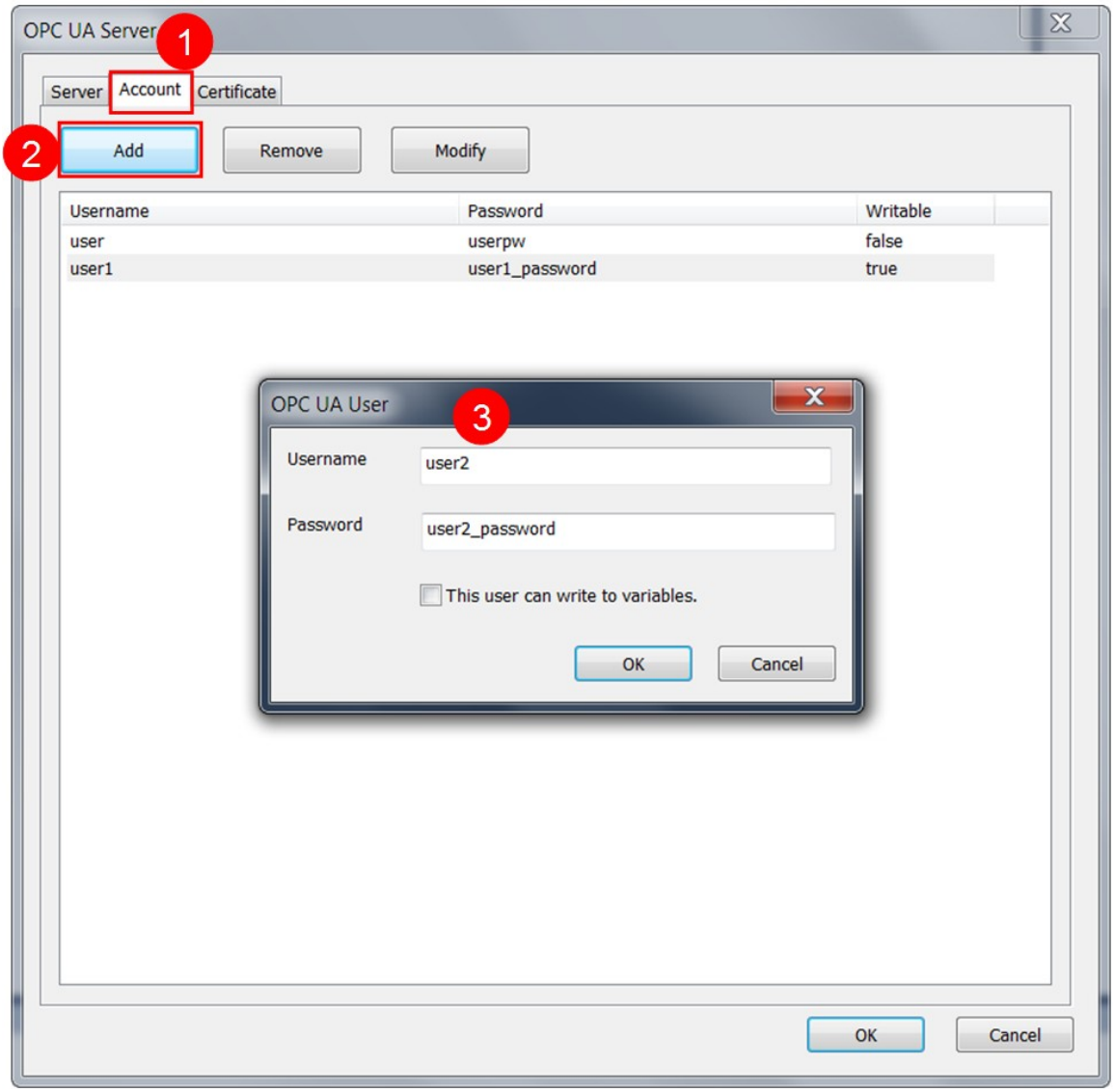


Figure 8: User account

Note:

It is important to remove the default entries provided by ICPDAS from the account list and replace them with your user login account settings otherwise the security is impacted.

3.1.2.7 Server Certificate

Fill in the server Certificate (Figure 9).

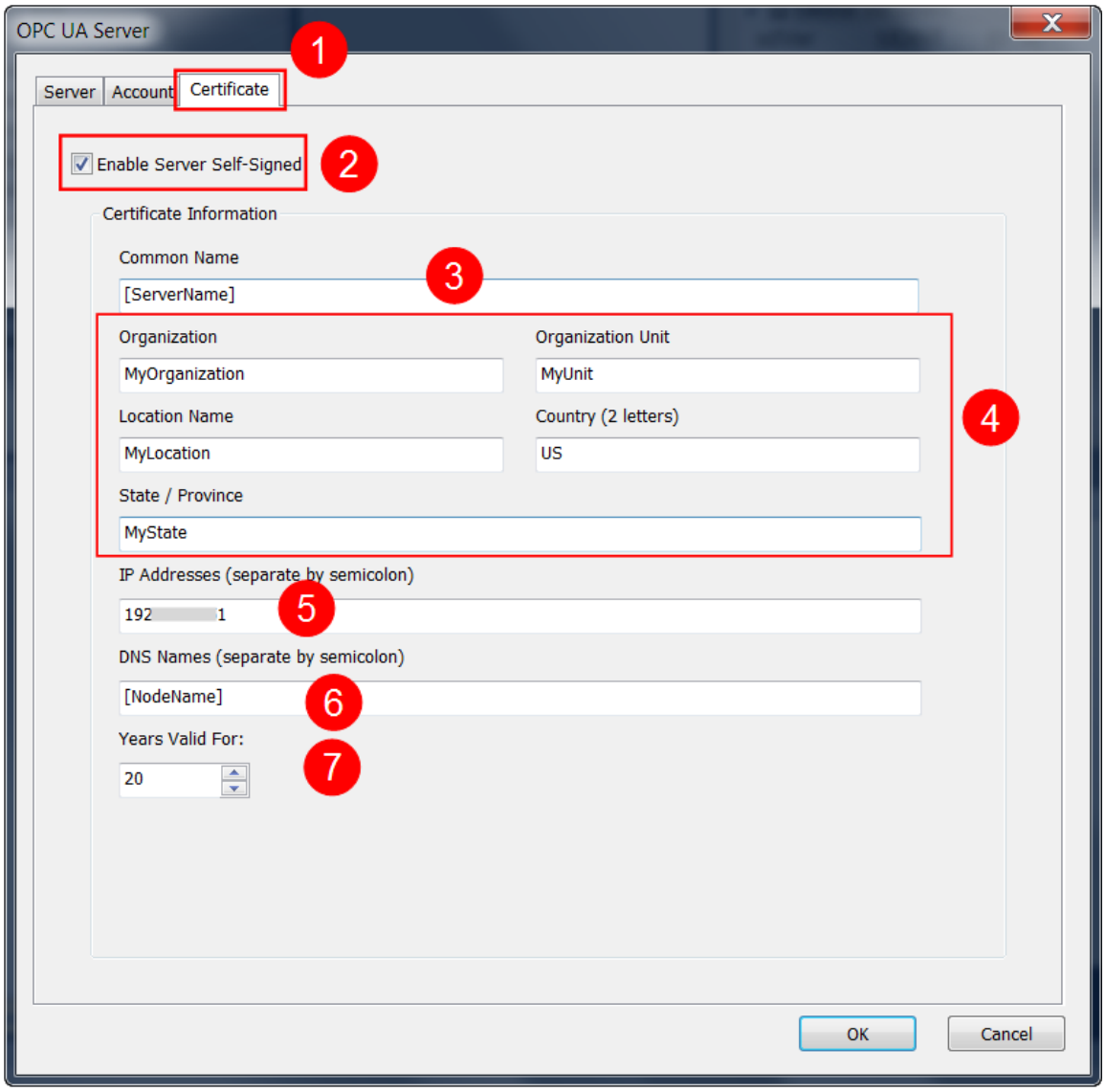
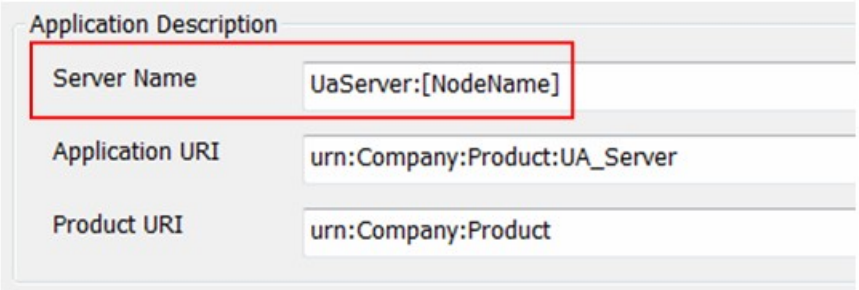


Figure 9: Self-signed security information

1. Open the '*Certificate*' tab
2. The OPC UA server enables you to create a self-signed user certificate, which means the certificate is directly generated by the Win-GRAF server using the OpenSSL toolkit.
   - Make sure that the '*Enable Server Self-Signed*' option is checked and the certificate details are filled out. The server will use all information entered into the dialog box (Figure 9) to generate a certificate with its private key. The '*Enable server self-signing*' option only needs to be selected if a server certificate with its key does not yet exist, since the server cannot be started without a certificate.
   - Uncheck the '*Enable Server Self-Signed*' option if you prefer to use a CA Signed Certificate, a certificate generated by another authority. In this case the

certification information setting will be ignored and no certificate generated.

3. Common Name:
   - The default common name is the '*Server Name*' indicated by the keyword '*[ServerName]*'. The server will automatically replace the string containing the keyword '*[ServerName]*' with the server name.
   - The server name is set in the '*Server*' tab under the category '*Application Description*'



4. Enter the organization name and its unit, location name (city name), state province and country. See Table 5 for further description.
5. Enter IP addresses listen by the OPC UA server on the Win-GRAF runtime device. Add a semicolon between IP addresses.
6. DNS name: The default name is set to the keyword '*[NodeName]*' which means the server will replace this keyword with the host name of the actual computer or device on which the WinGRAF runtime is installed.
7. Certificate's validity duration: Set the number of years the certificate is valid for.

Certificate Info Parameter	Description
Common Name	• The 'Common Name' of the OPC UA server itself, which is broadcast to the discovery server and other OPC UA clients on the network. • The default common name is *[ServerName]*. This keyword automatically assigns the '*Server Name*' set in the '*Server*' tab to the '*Common Name*'. • Default setting: *[ServerName]*
Organization	• Organization that owns the application.
Organization Unit	• Organization's division/department to which the certificate is attached. Name of the organization unit that provides the OPC UA server.
Location Name	• City in which the OPC UA server certificate is issued. Name of the city from where the OPC UA server is operated.
State/Province	• State/province in which the OPC UA Client certificate is issued.
Country	• Country in which the OPC UA Client certificate is issued. • Country code consisting of two letters that indicates the country in which the OPC UA server is operated.
IP Address	• Type all of the addresses that may be used by the actual computer or device that will host the project and present this certificate. You may leave this box empty. Doing so will not prevent the server certificate from being issued or make it not valid.
DNS Name	• Names of the domain name servers that will administer the project

Certificate Info Parameter	Description
	runtime server. The default DNS name is *[NodeName]*. • The default name *[NodeName]* automatically retrieves the host name of the actual computer or device on which the WinGRAF runtime is installed • Default: *[NodeName]*
Validity Duration	• Certificate's expiration date. Depending on the client configuration once the server certificate expires the communication between server and client may no longer be possible. - Procedure to create a new certificate: Delete the server certificate with the associated key file and restart the runtime to generate a new certificate • Default: 20 years

Table 5: Certificate information parameters

The file based certificate store on the Win-GRAF UA server has got the directory layout as shown in Table 6. If the folders do not exist then the runtime will automatically created them in the runtime working directory during the startup phase and generate a application instance certificate *'ua_server.der*' and private key '*ua_server.pem*' and place it in the '*own*' directory.

During the startup phase, the Win-GRAF runtime environment checks whether a certificate is present in the '*\OPC-UA\Server\PKI\own\certs*' folder. If there is no certificate and '*Enable Server self-Signed*' is checked, the runtime creates a new certificate and private key.

Note:
The private key ('*ua_server.pem*') has to remain secret and is used to sign and/or decrypt messages. Make sure no unauthorized person has access to the '*\OPC-UA\ Server\PKI\own\private*' folder.

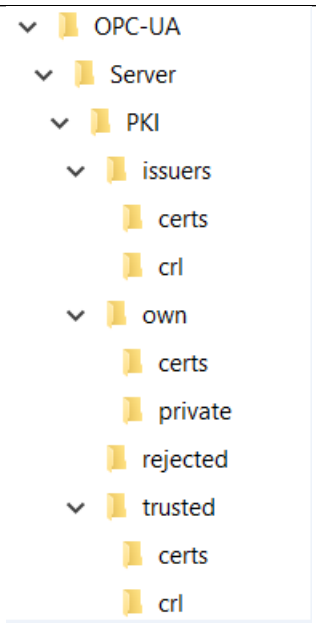
OPC-UA **\Server** **\PKI** ▪ **issuers** - certs - crl ▪ **own** - certs stores the server certificate 'ua_server.der' - private stores the private key 'ua_server.pem' ▪ **rejected** ▪ **trusted** - certs the trusted client certificate has to be stored in this folder - crl	

Table 6: File based certificate store

3.1.2.8 Publishing PLC Variables

Create a monitoring group node:

1. Activate endpoint node ('*Bind IP Address: opc.tcp://...*')
2. Click '*Insert Slave/Data Block*' command on the left toolbar. A '*Group*' dialog appears.
3. Enter a group name in the dialog by double clicking the '*Value*' column. Click '*OK*'. The new node with the group name is added to the tree view.

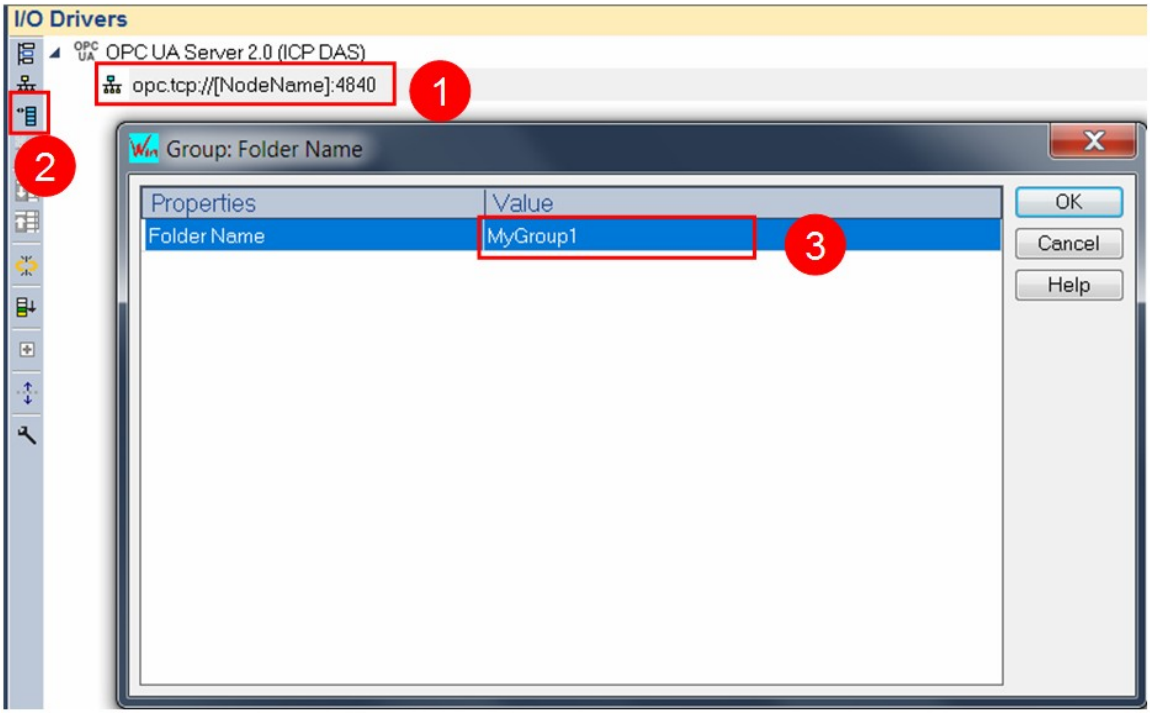


Figure 10: Add monitoring group node

Assign PLC variables to the group. Here the PLC variables are assigned to the UA server so that the client can access them.

1. Declare variables to be accessed by the client in the variable editor.
2. Activate the group node ('*Group: MyGroup1*') by clicking on it.
3. Drag and drop the PLC variables from the variable editor to the mapping area.

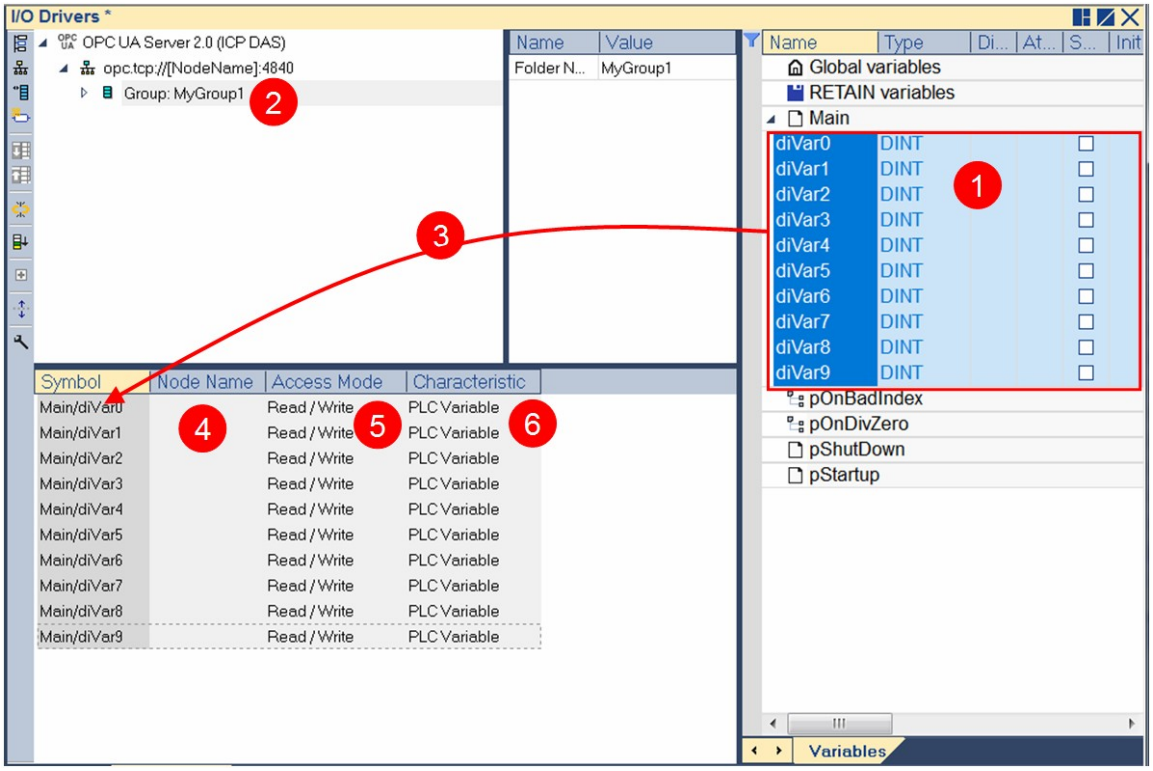
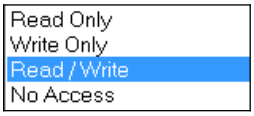


Figure 11: Mapping PLC variables to the OPC UA server

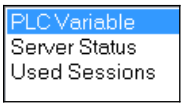
4. Enter a '*Node name*' for each variable. The node name is displayed to the client. If the '*Node name*' field is blank, the name in the '*Symbol*' column is used as the node name.

5. Select the client access mode: '*Read only*', '*Write only*', '*Read/Write*', or '*No Access*'.



If '*No Access*' is selected, the associated variable represents the OPC UA server status. The type of status to be shown has to be set in the '*Characteristic*' column.

6. The OPC UA server status type represented by the PLC variable is set in the '*Characteristic*' column.This column is only valid if the access mode '*No Access*' has been selected. Available server status types:



Message Mode	Description
Symbol	• The variable name declared inside the PLC application
Node name	• The variable node name displayed in the OPC UA Client • If the '*Tag name*' is empty then the '*Symbol*' name will be used as the variable node name. • Default: empty

Message Mode	Description
Access Mode	• Client access write: '*Read only*', '*Write only*', '*Read/Write*', '*No Access*' • The mode '*No Access*' indicates that the mapped variable is being used to indicate the server status and can not be accessed by the client. Select the status type (Type) to display • Default: '*Read/Write*'
Characteristic	• Select the server status type to read. • This parameter is only valid if the '*Access Mode*' is set to '*No Access*', which means the mapped parameter will be updated with server status information. A variety of status information are available: - '*Server Status*': OPC UA server status - '*Used Session*': number of clients connected Variables with either '*Server Status*' or '*Used Session*' characteristic can <u>not</u> read by the client. • Set the type to '*PLC Variable*' if the '*Access Mode*' is set to any mode except '*No Access*' • Default: '*PLC Variable*'.

Table 7: Variable node property setting

Supported variable types:

Data Types	
PLC	OPC UA
BOOL	Boolean
SINT	SByte
USINT	Byte
DINT	Int16
USINT	UInt16
UINT	Int32
UDINT	UInt32
LINT	Int64
ULINT	UInt64
REAL	Float
LREAL	Double
STRING	String

Table 8: Supported data types

3.1.2.9 Build and Download PLC Application

Built the program, download it to the runtime and start the application.

If no server certificate exist in the folder '*%InstallDir%\OPC-UA\Server\PKI\own\certs*' and '*%InstallDir%\OPC-UA\Server\PKI\own\private*' of the Win-GRAF controller and the '*Enable Server self-Signed*' option is checked, then when the SPS application starts, a

new server certificate with its private key is automatically created.

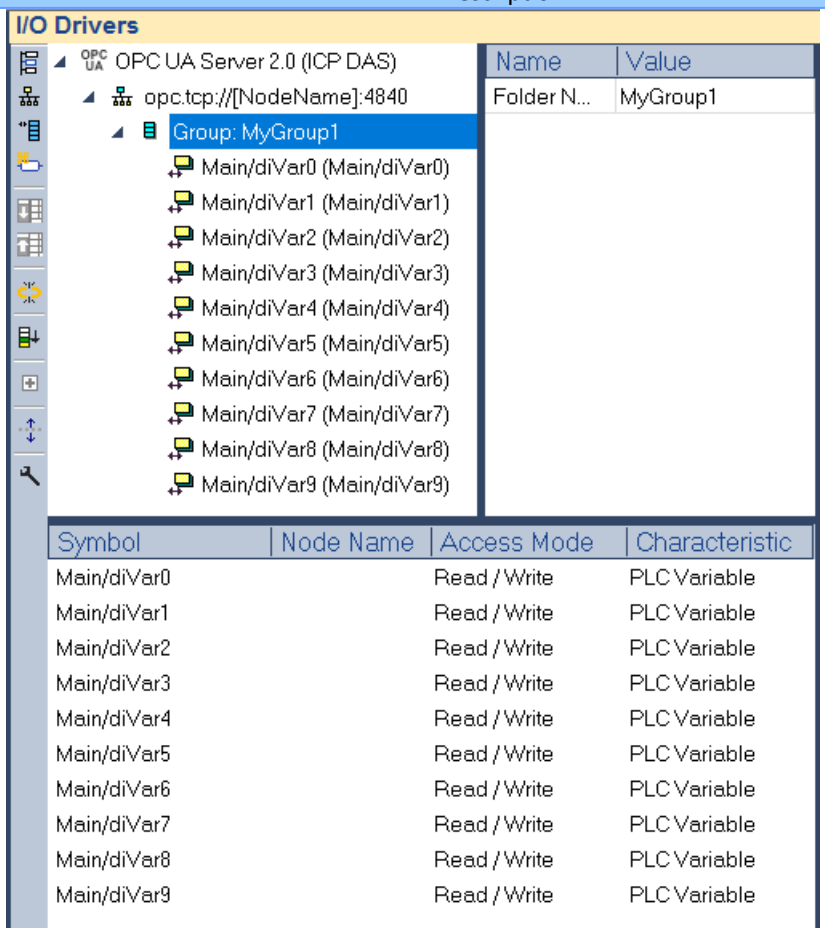
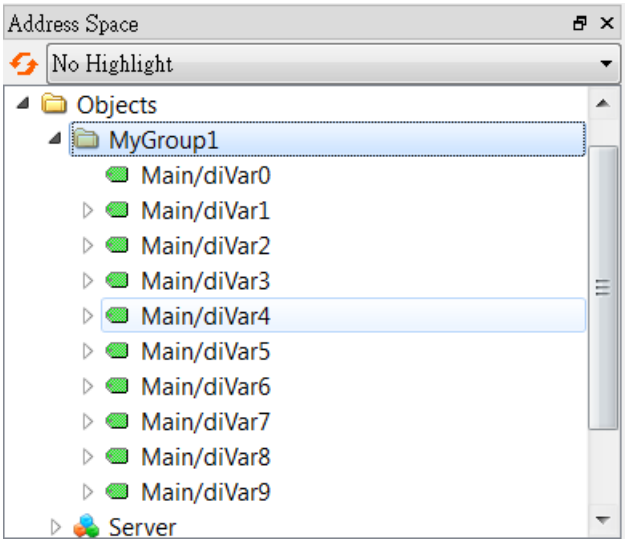
IMPORTANT:
If changes were made to the server and certificate settings, the server certificate files must be deleted from the '*%InstallDir%\OPC-UA\Server\PKI\own\certs*' and '*%InstallDir%\OPC-UA\Server\PKI\own\private*'' directory, so that the OPC UA server generates new certificate with the new setting during the PLC application start-up.

3.1.2.10 Connect Client to Server

Use a OPC UA client to connect to the server.

1. The client sends it certificate to the server 'rejected' directory: '*%InstallDir%\OPC-UA\Server\PKI\rejected*'
2. Move the client certificate from the 'rejected' to the 'trusted' directory: '%InstallDir %*OPC-UA\Server\PKI*\trusted\certs'. Depending on the Win-GRAF controller type this has to be done manually, via Certificate Manager or via a web browser.
3. The Table 9 shows the connection of the UaExpert client utility.

OPC UA	Description
Server	Win-GRAF workbench: Mapped PLC variables

OPC UA	Description
	
Client	UaExpert Client: Display of Win-GRAF mapped PLC variables  The value of each variable can be directly monitored by dragging the variables from the '*Address Space*' to the '*Data Access View*' window

OPC UA	Description
	Data Access View

#	Server	Node Id	Display Name	Value	Datatype
1	UaServer:DESKTOP-A...	NS2|String|MyGroup1.Main/diVar0	Main/diVar0	131500	Int32
2	UaServer:DESKTOP-A...	NS2|String|MyGroup1.Main/diVar1	Main/diVar1	0	Int32
3	UaServer:DESKTOP-A...	NS2|String|MyGroup1.Main/diVar2	Main/diVar2	0	Int32
4	UaServer:DESKTOP-A...	NS2|String|MyGroup1.Main/diVar3	Main/diVar3	0	Int32
5	UaServer:DESKTOP-A...	NS2|String|MyGroup1.Main/diVar4	Main/diVar4	0	Int32
6	UaServer:DESKTOP-A...	NS2|String|MyGroup1.Main/diVar5	Main/diVar5	0	Int32
7	UaServer:DESKTOP-A...	NS2|String|MyGroup1.Main/diVar6	Main/diVar6	0	Int32
8	UaServer:DESKTOP-A...	NS2|String|MyGroup1.Main/diVar7	Main/diVar7	0	Int32
9	UaServer:DESKTOP-A...	NS2|String|MyGroup1.Main/diVar8	Main/diVar8	0	Int32
10	UaServer:DESKTOP-A...	NS2|String|MyGroup1.Main/diVar9	Main/diVar9	0	Int32

Table 9: PLC variable mapping

4 Using UaExpert® Client to Connect to the Win-GRAF OPC UA Server

The UaExpert® is a full-featured OPC UA Client provide by Unified Automation®. The UaExpert is available for Windows and Linux and can be downloaded for free from the Unified Automation website. With this client you can connect to the Win-GRAF OPC UA server to test the comunication.

The following descriptions refer to the UaExpert program and demonstrate the effect of various server configurations on the connection process between client and server. To show the effects of the server parameter settings, the demo program 'SimpleDemo' is used with its server configuration.

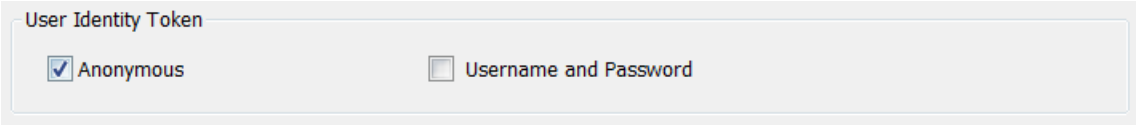
The demo program is located in the directory:
C:\Users\Public\Documents\Win-GRAF Workbench\Win-GRAF Wb xx.xx\Projects\Windows PC\OPC UA\SimpleDemo

4.1 No Security Policy and Anonymous Identity Token

4.1.1 Win-GRAF server setting

The server is configured as follows:

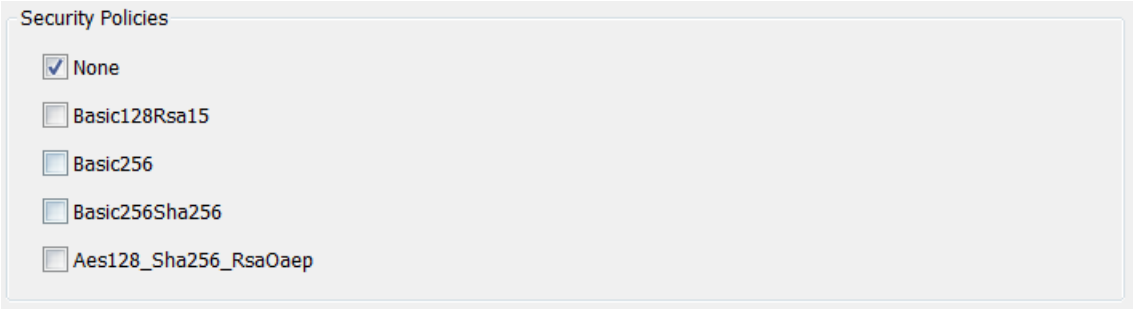
- Application based security is disabled. No login password is required for the client.



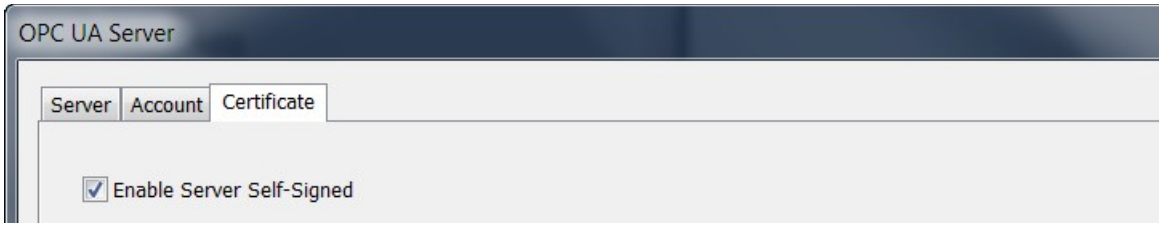
Note:
It is important to note that the '*Anonymous*' user identity only grants the client read access and not write access. PLC variables can only be read by the client and can not be changed, regardless of whether the variable's '*Access Mode*' is set to '*Read/Write*'.

- Disable security certificates for encrypted communications. This allows the client to

create a session with the server without having to store the client certificate file in the server's trusted folder.



- It is important to remember that if there is no server certificate with its private key in the directories '*%InstallDir%\OPC-UA\Server\PKI\own\certs*' and '*%InstallDir%\OPC-UA\Server\PKI\own\private*', the server will not create an endpoint and will not allow any client to connect. Therefore, check the '*Enable Server self-Signed*' option to instruct the server to generate a new certificate and private key if no certificate could be found.



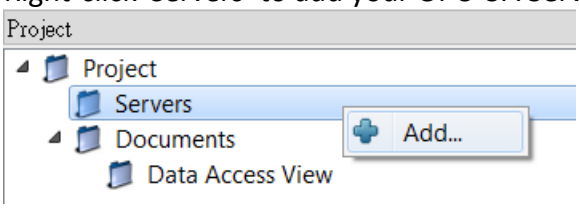
4.1.2 UA-Expert Client

After launching the UA-Expert it will ask to create a OPC-UA client certificate, press OK.

Figure 12: Client certificate generation

Add server to client:

Step 1: Right-click '*Servers*' to add your OPC-UA Server.



Step 2: Double click the '*<Double click to Add Server>*' in the '*Custom Discovery*' directory and enter the Win-GRAF server URL in the pop-up dialog.

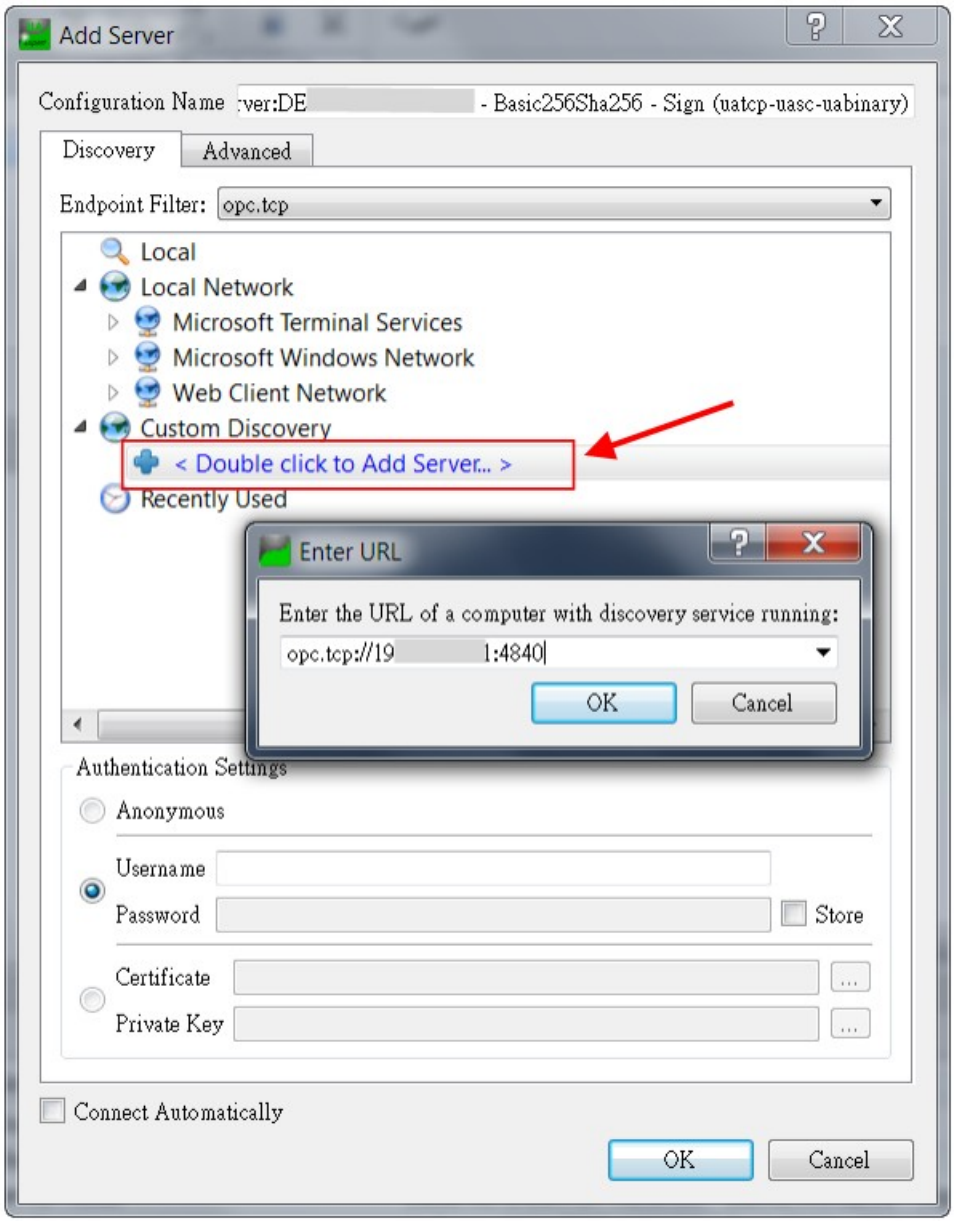


Figure 13: UaExpert server discovery

The discover directory list all the support connection security mode supported by the server. As all security policies of the server are disabled ('*None*') only the unsecured connection option is available. Double click the '*None-None(uatcp-uasc-uabinary)*' connection type.

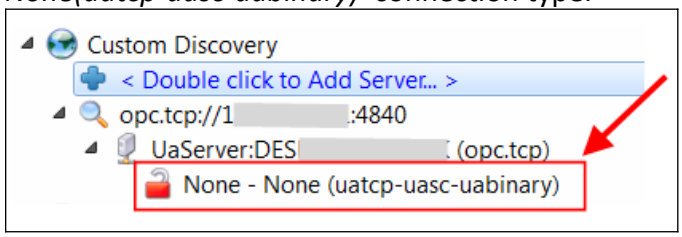
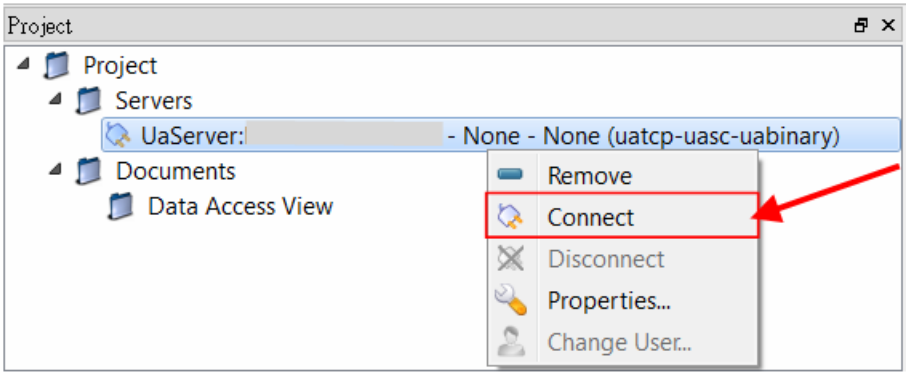


Figure 14: Server supported security policies

Step 3: Connect to the server by right clicking the server and selecting '*Connect*'.



A certification validation window pops up. Click '*Trust Server Certificate*' and '*Continue*' button. This window only appears if the server certificate has not already been added to the trusted client server.

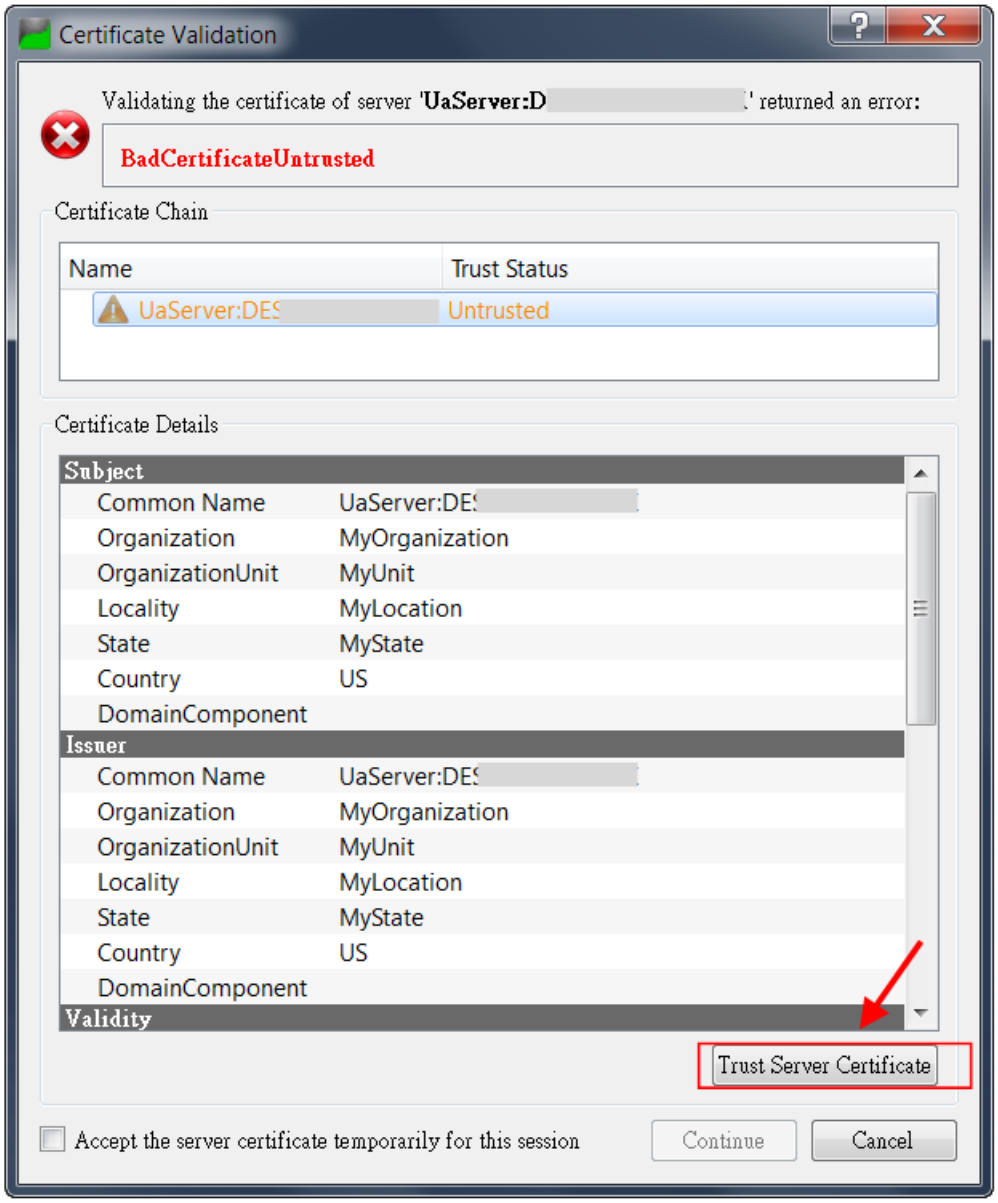


Figure 15: UaExpert client validates the server certificate

Step 4: View the PLC variable values in the UaExpert:
Select the nodes in the '*Address Space*' listed under the '*MyGroup1*' and '*MyGroup2*' and drag and drop to the '*Data Access View*'. The '*Address Space*' shows for each node its attributes such as ID, name, value, data type, etc..

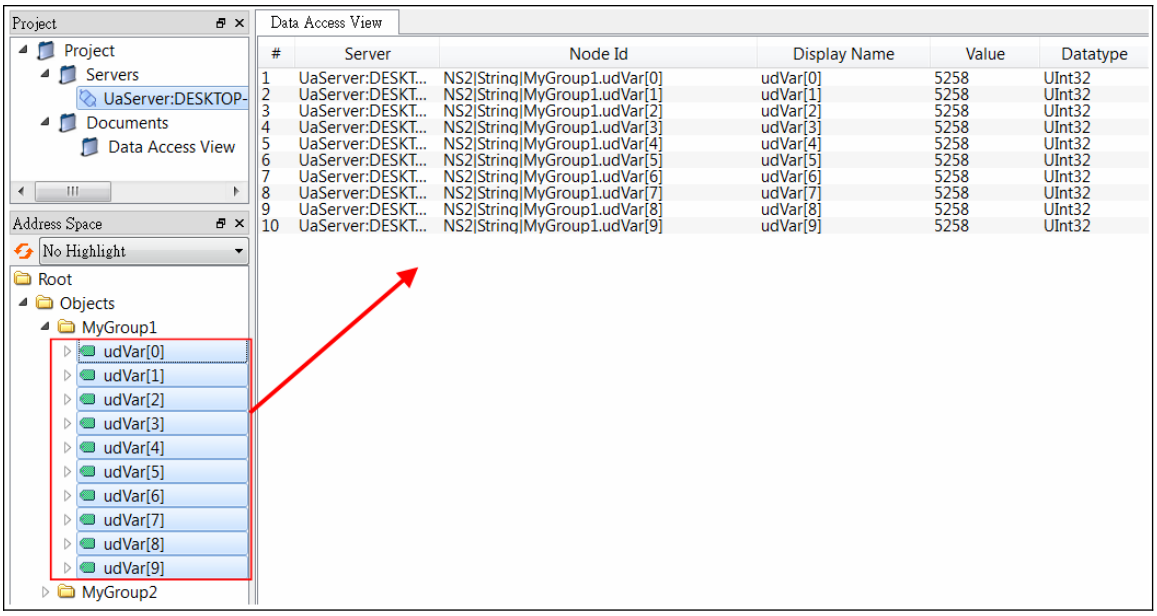


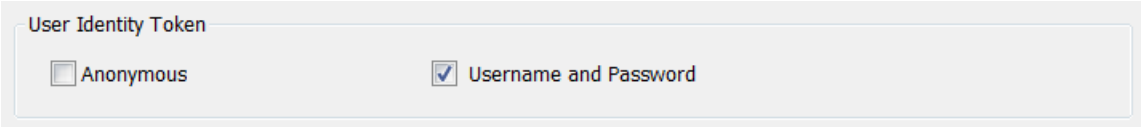
Figure 16: UaExpert client displays the PLC variables

4.2 Security Policy and Login Account (Username and Password)

4.2.1 Win-GRAF server setting

Configure the server as follows:

- Enable '*Username and Password*' option. The user on the client side must always enter a password before starting a session with the server.



- Select the following security policies options.

- Add user name with password to login account

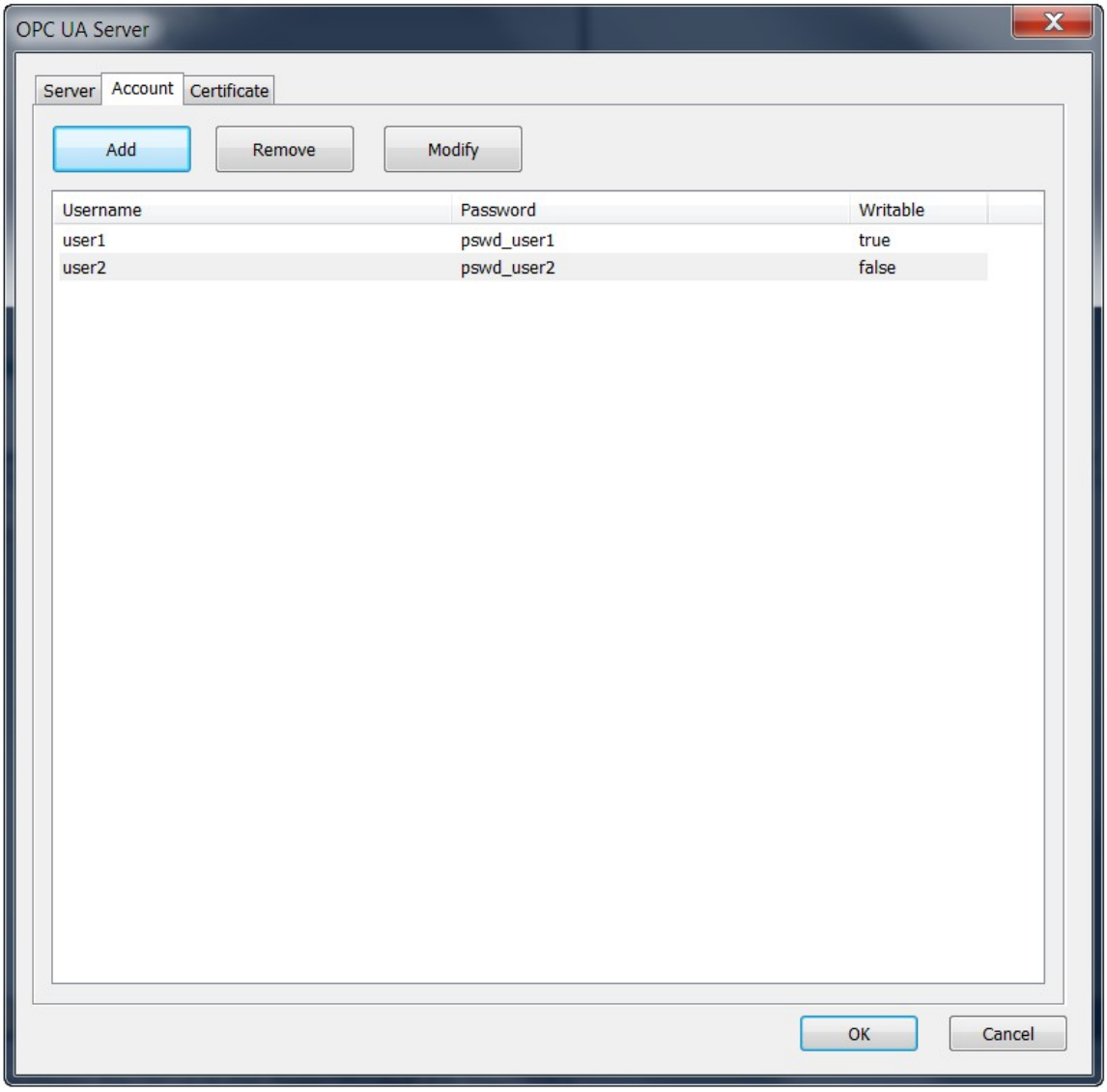


Figure 17: Win-GRAF OPC UA server user account setting

- Enable the self-signed certificate option and fill in the information

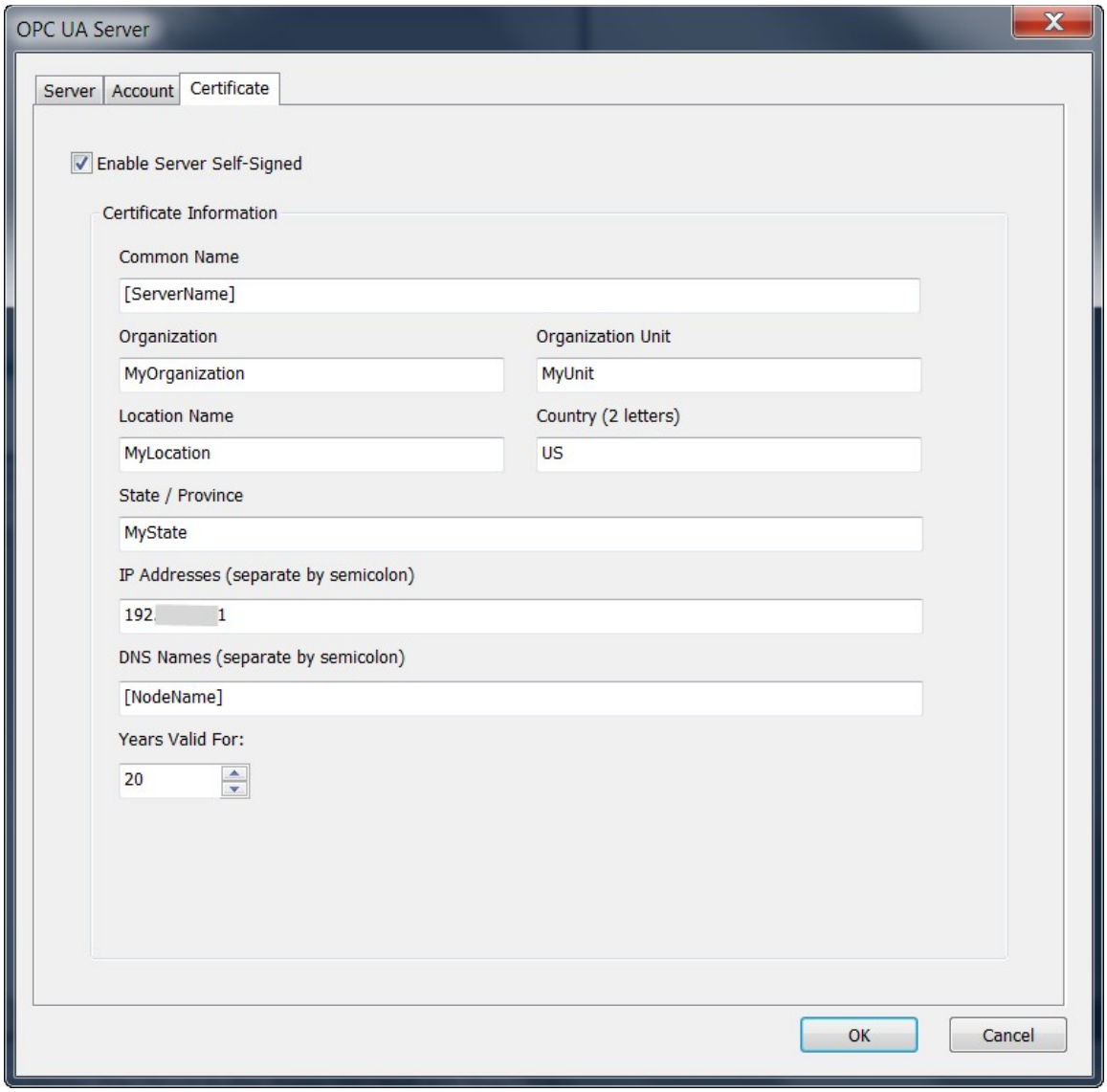
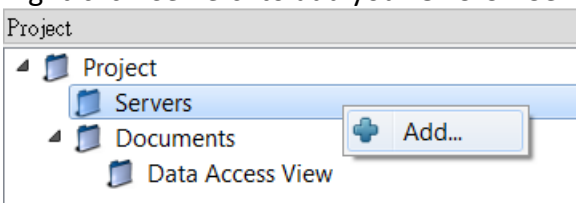


Figure 18: Win-GRAF OPC UA server certificate setting

4.2.2 UA-Expert Client

Add server to client:

Step 1: Right-click '*Servers*' to add your OPC-UA Server.



Step 2: Double click the '*<Double click to Add Server>*' in the '*Custom Discovery*'

directory and enter the Win-GRAF server URL in the pop-up dialog.

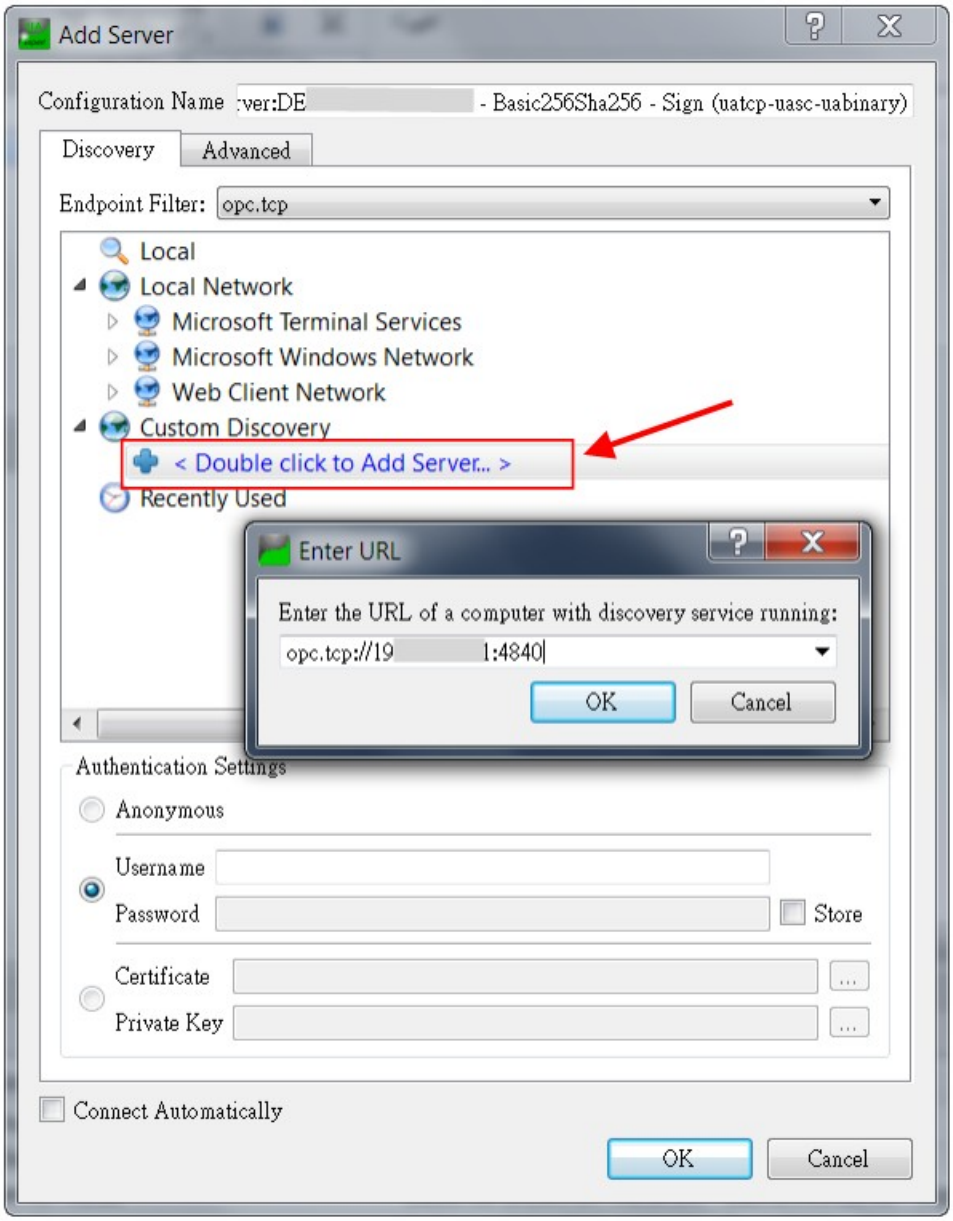


Figure 19: UaExpert server discovery

The encryption algorithm supported by the server are listed beneath the server name. The client can select any one of the available encryption options to be used for the server to client communication.

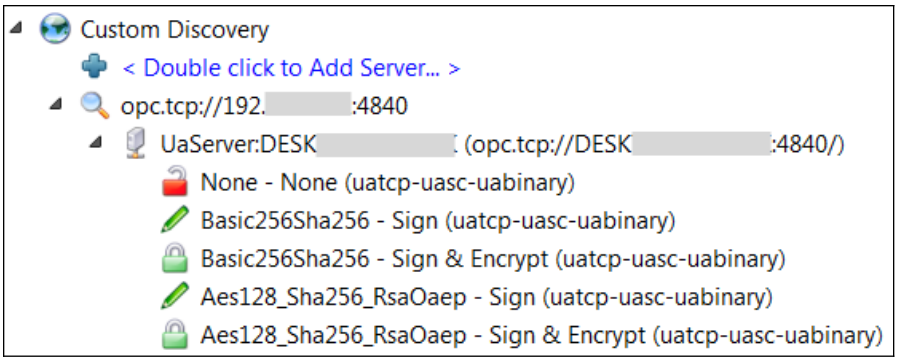
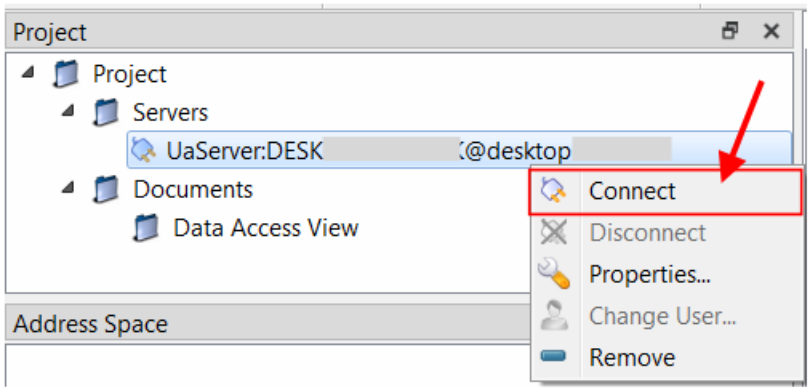


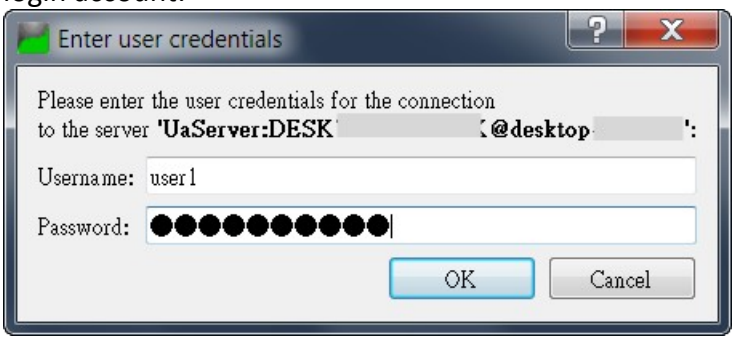
Figure 20: Server supported security policies

In this demo we select the following option:
Double click '*Basic256Sha256 -Sign&Encryp(uatcp-uasc-uabinary)*' option.

Step 3: Connect to the server by right clicking the server and selecting '*Connect*'



Enter username and password as defined by the Win-GRAF workbench for the login account:



A certification validation window pops up. Click '*Trust Server Certificate*' and '*Continue*' button.

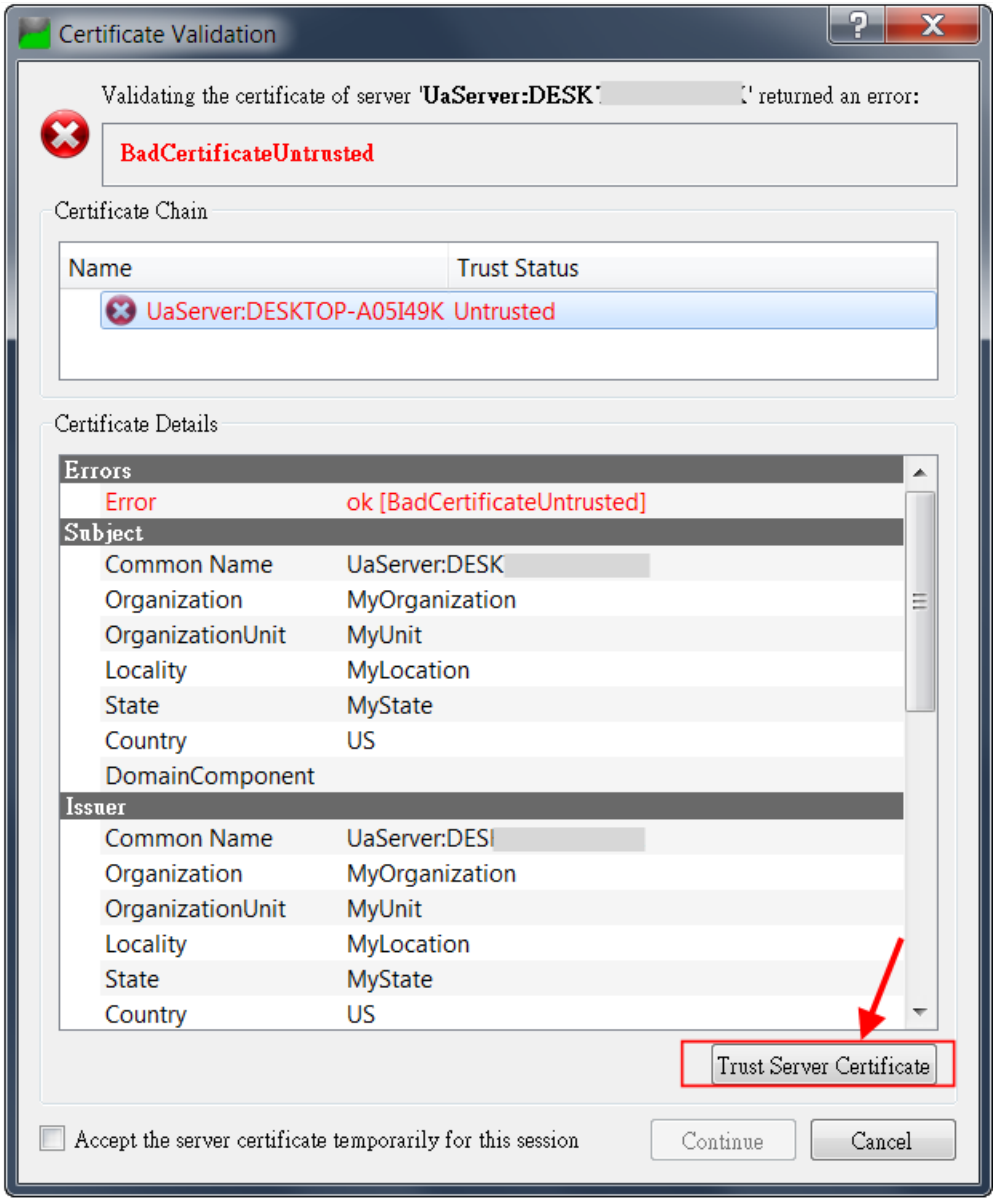


Figure 21: Server certificate before authorized by the client

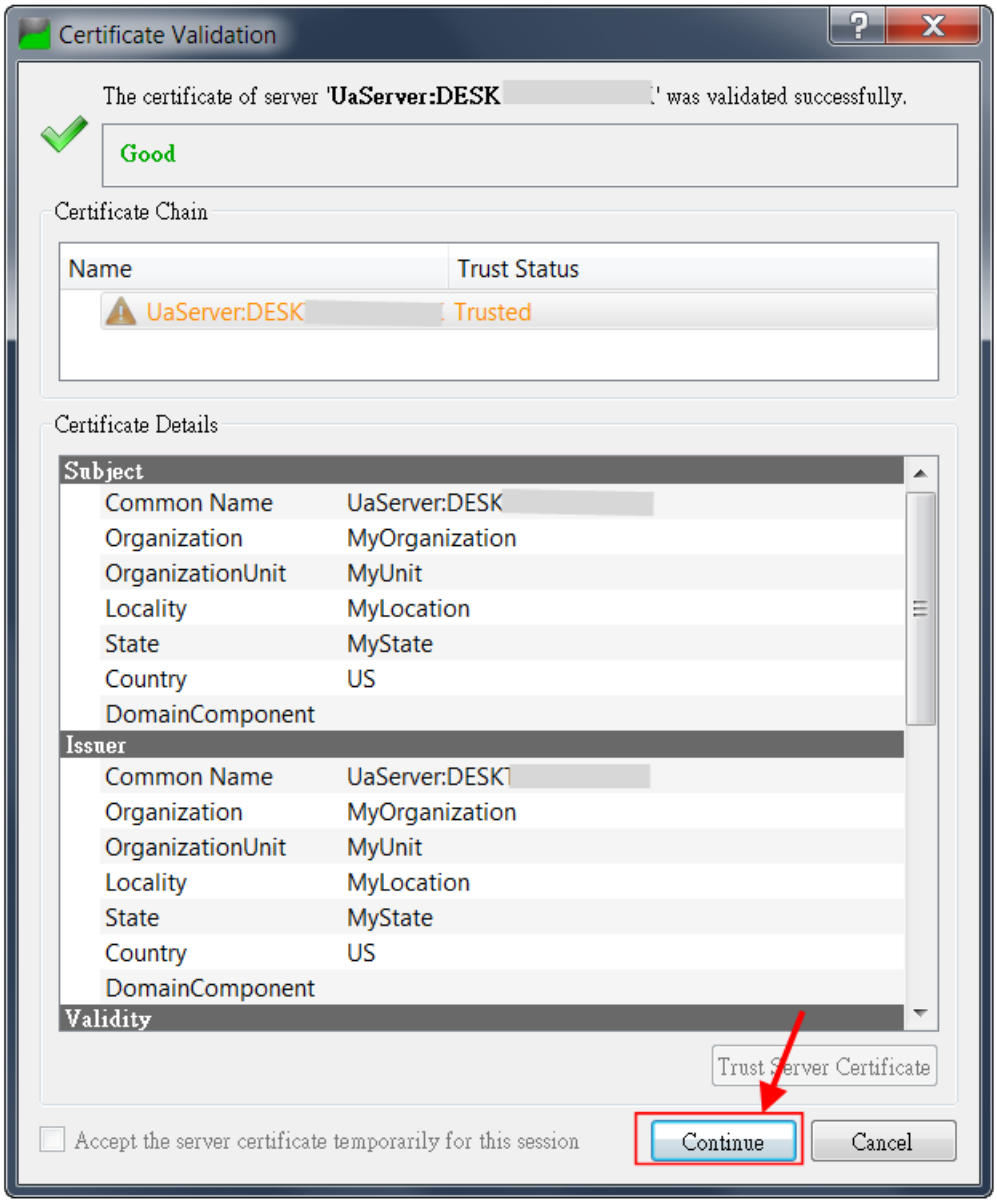


Figure 22: Server certificate after authorized by the client

Now the client certificate is send to the 'rejected' directory of the server: '*%InstallDir%\OPC-UA\Server\PKI\rejected*'

Step 4: OPC UA server needs to authorize the client communication by moving the client certificate from the directory '*%InstallDir%\OPC-UA\Server\PKI\rejected*' to the trusted directory: '*%InstallDir%\OPC-UA\Server\PKI\trusted\certs*'

The moving of the client certificate to the '*trusted\certs*' directory can be done either manually, via Certificate Manager or via web browser depending on the Win-GRAF controller.

Example using the EMP-9000 controller:
The EMP-9000 Win-GRAF runtime utility has got an integrated Certificate Manager. The certificate send by the client is added by the server to the 'Rejected' folder. Select this certificate in the 'Rejected' folder and click '*Trusted*' to move the certificate to the '*Trusted*' folder.

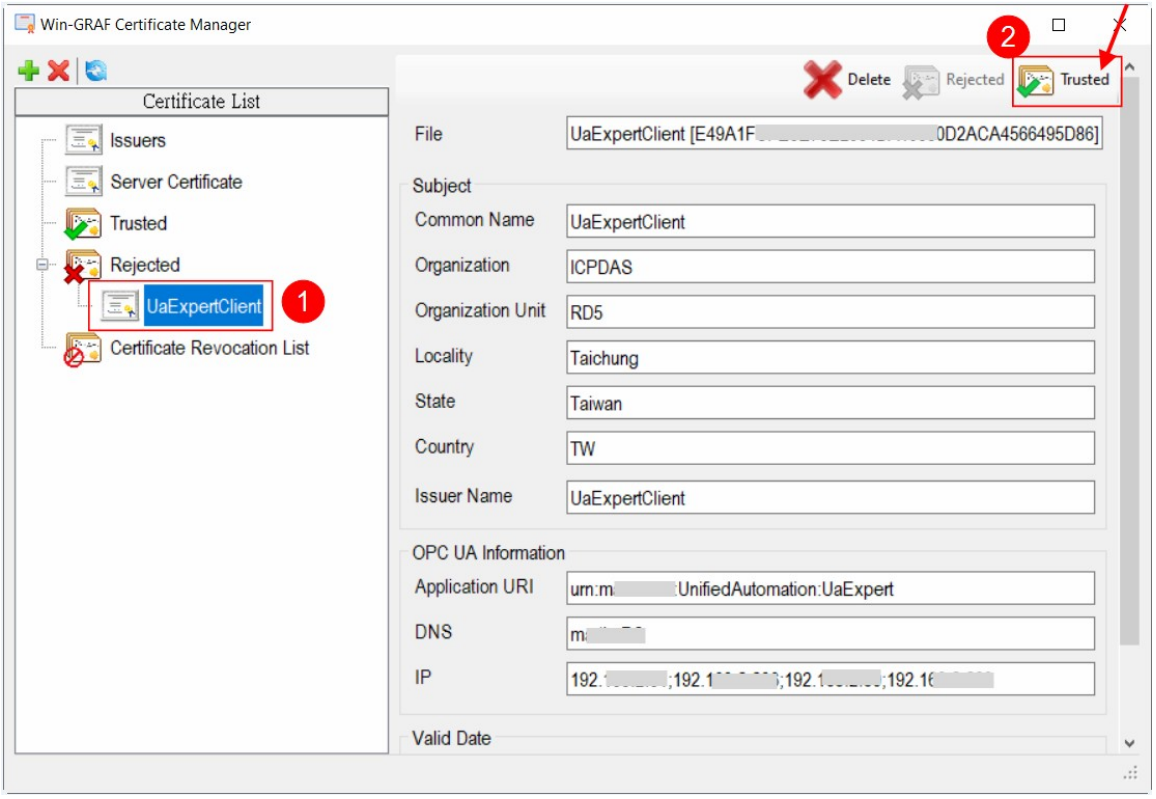


Figure 23: Client certificate before authorized by the server

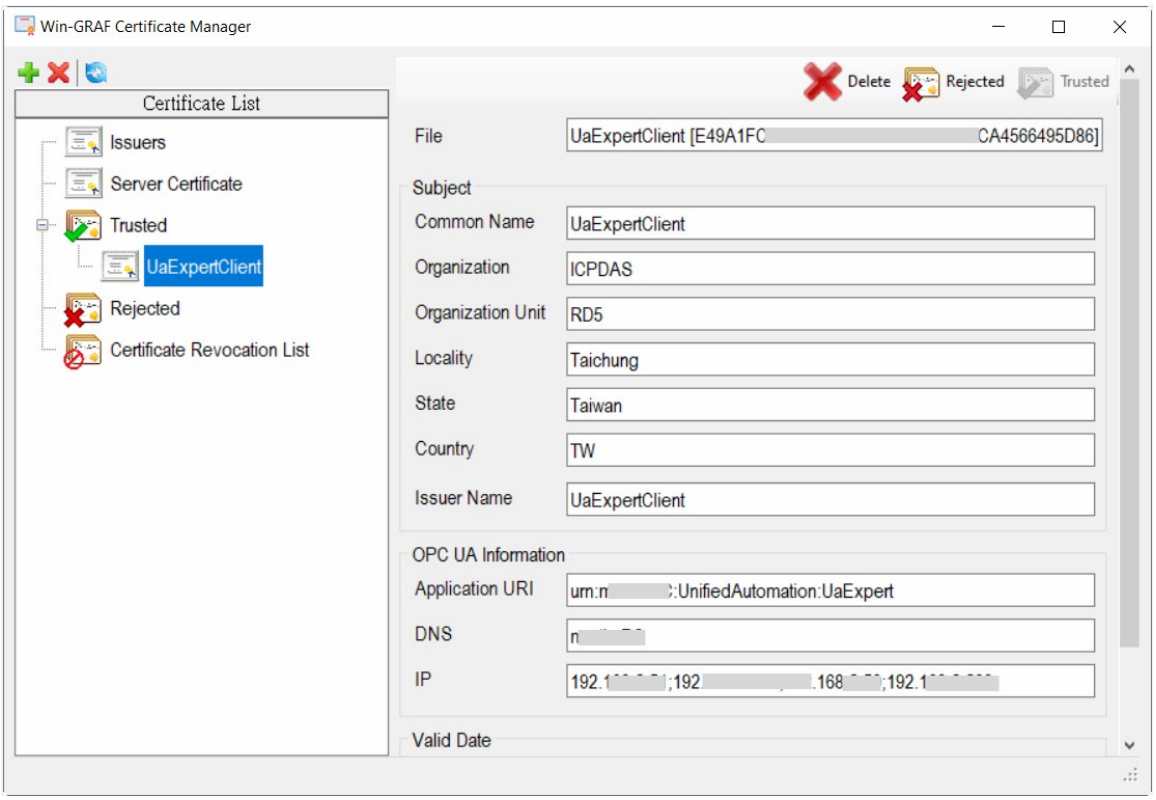


Figure 24: Client certificate after authorized by the server

Step 5: View the data values:

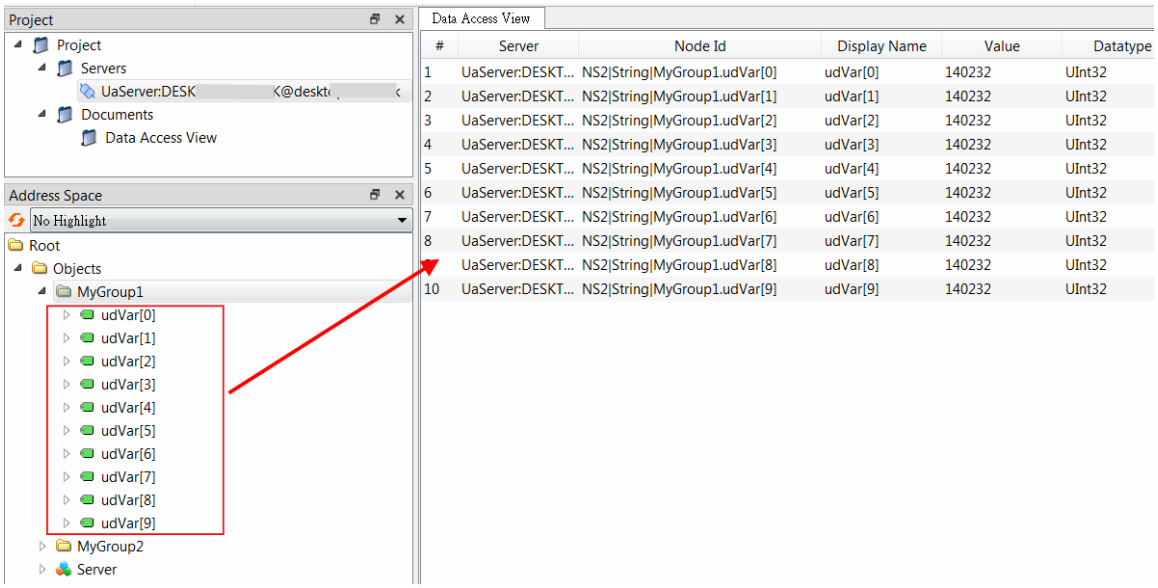


Figure 25: UaExpert client displays the published PLC variables

5 Server Operation Error

Most connection errors to an OPC UA server are due to missing or invalid certificates. Therefore, it is important to ensure that both server and client have the necessary certificates. Both communication partner (server or client) needs to have the partners certificate defined as trusted.

5.1 Server Failed to Create Endpoints

If the server does not find any server certificate in the directory '*%InstallDir%\OPC-UA\Server\PKI\own\certs*' and any private key in the directory '%InstallDir%\OPC-UA\Server\PKI\own\private\' then no endpoints will be created. This means the client will not be able to connect and returns with a connection timeout.

It is therefore important to ensure that a server certificate with its private key file exist in the corresponding directory. The certificate can either be signed by a 'Certificate Authorities (CA)' or 'self-assigned'. In case of a 'self-assigned' certificate the Win-GRAF server will generate a new certificate if no certificate already exist in the directory. To enable 'self-signed' certificate check the check box as shown in Figure 26. To force the server to generate a new certificate remove all files, certificate and private key files, from both directories: '*%InstallDir%\OPC-UA\Server\PKI\own\certs*' and '%InstallDir%\OPC-UA\Server\PKI\own\private\'.

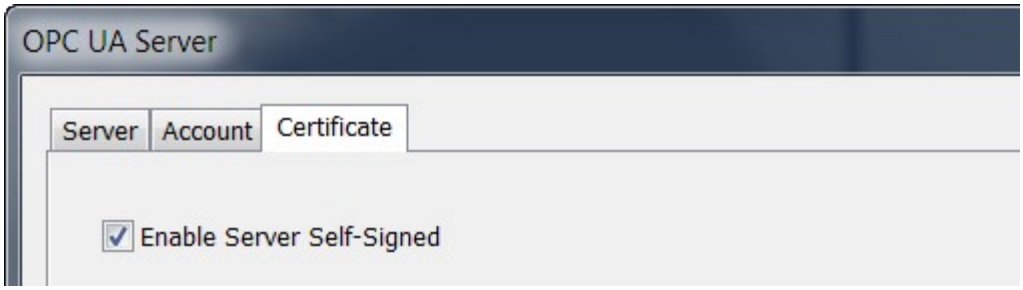
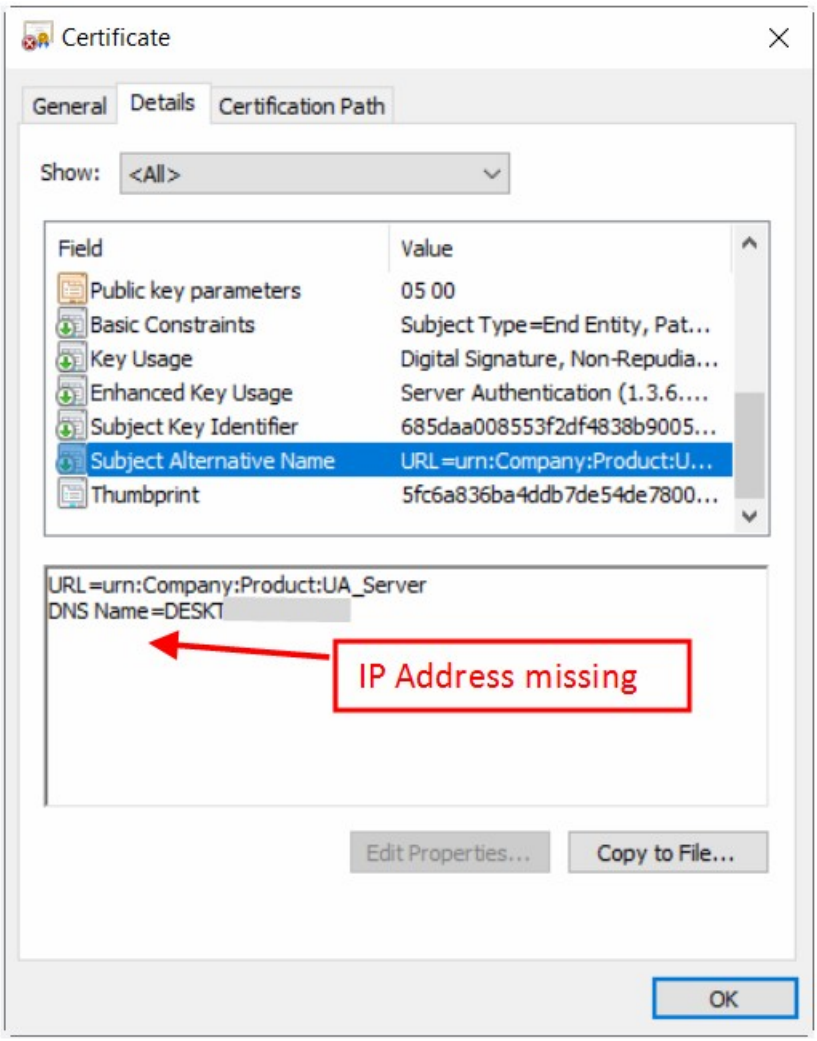


Figure 26: Create a 'Self-assigned' certificate

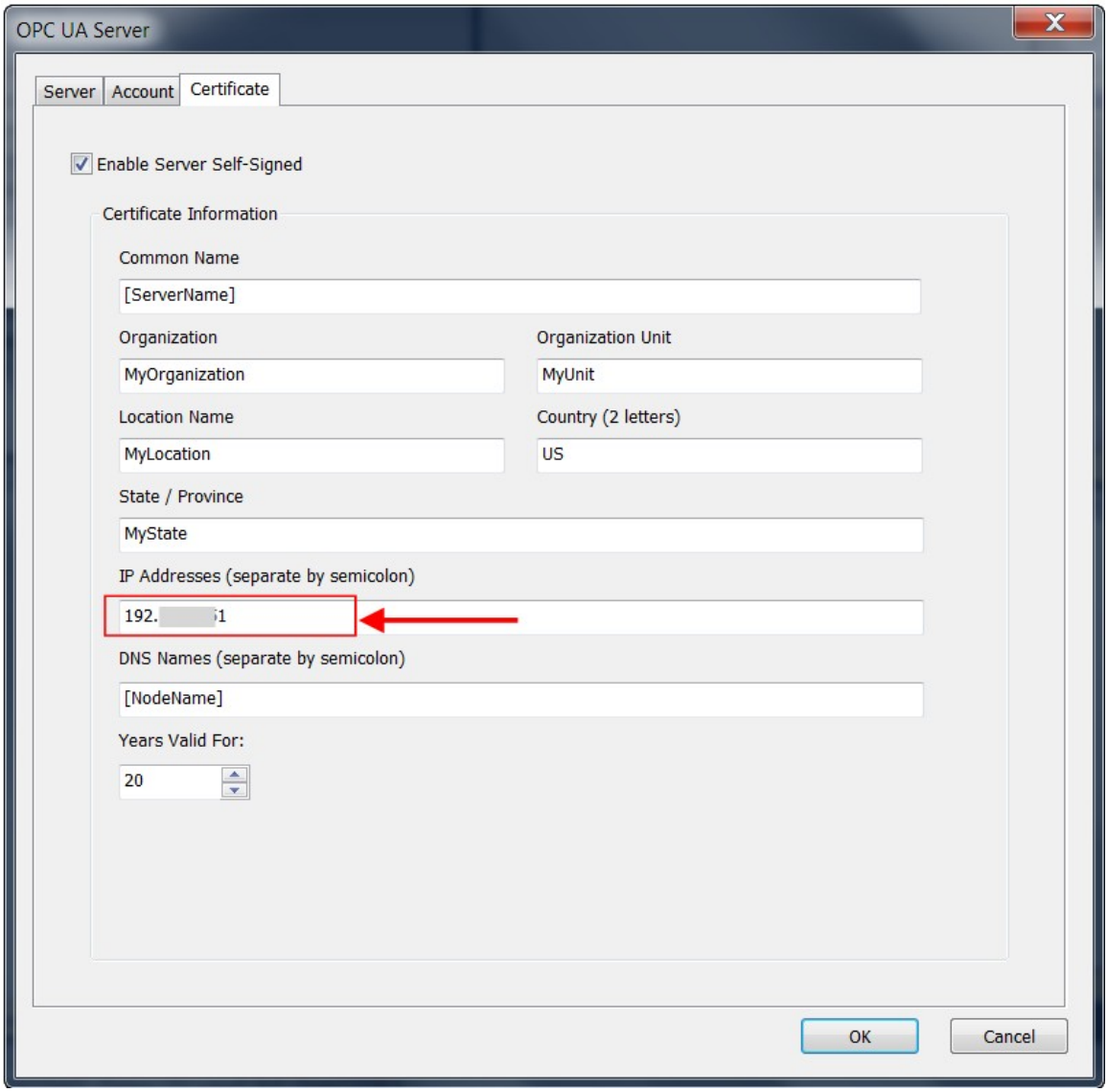
5.2 Communication Error Message

5.2.1 BadCertificateHostNameInvalid

The error relates to the '*SubjectAlternativeName*' extension, which is supposed to contain the hostname(s) and/or IP addresses of the server. If you connect to the server using its IP address and the certificate contains only the hostname (or vice versa), this error will be thrown.

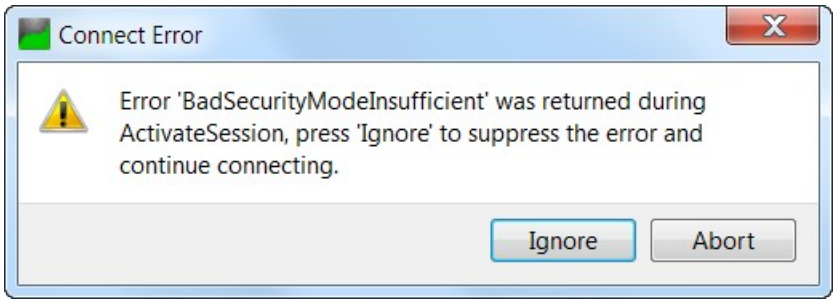


Solution:
Enter the IP address of the server as shown in the figure below:

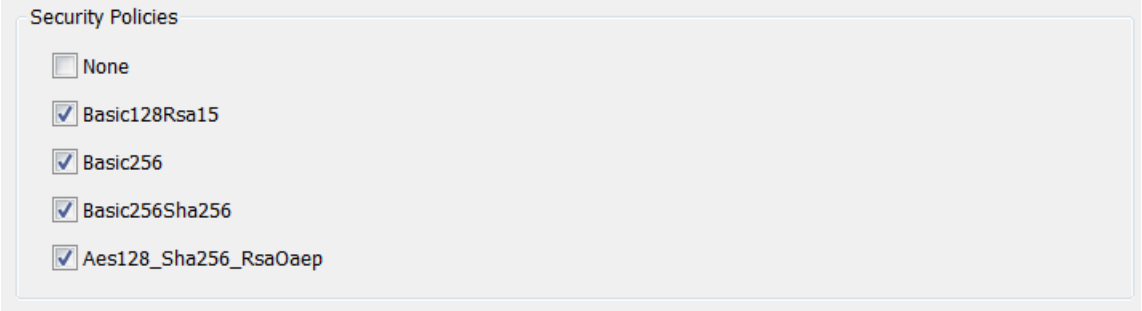

OPC UA Server
Server
Account
Certificate
Enable Server Self-Signed
Certificate Information
Common Name
[ServerName]
Organization
MyOrganization
Organization Unit
MyUnit
Location Name
MyLocation
Country (2 letters)
US
State / Province
MyState
IP Addresses (separate by semicolon)
192.
1
DNS Names (separate by semicolon)
[NodeName]
Years Valid For:
20
OK
Cancel

5.2.2 BadSecurityModeInsufficient

This error means that the client tries to establish a '*none*' encrypted communication by logging into the server. In security mode '*none*', '*Username*' and '*Password*' are sent over the Ethernet as plain text, which poses a major security risk.



Solution:
Select the '*Basic256Sha256*' or *'Basic256'* or any other security policy to encrypt the password. It is also necessary to move the client certificate from the '*%InstallDir%\OPC-UA\Server\PKI\rejected*' server directory to the '*%InstallDir%\OPC-UA\Server\PKI\trusted\certs*' directory.



5.2.3 BadUserAccessDenied

'*BadUserAccessDenied*' stands for 'User does not have permission to perform the requested operation'. It is an authorization error: That is, either the 'Username' used when creating the UA session is not authorized to perform the operation or the 'Password' is incorrect.

5.2.4 BadUserAccessDenied, BadSecurityCheckFailed

This error indicates that client can not establish a session because the server can not find a valid certificate of this client in the '*%InstallDir%\OPC-UA\Server\PKI\trusted\ certs*' directory.

Solution:
Move the client certificate from the '*%InstallDir%\OPC-UA\Server\PKI\rejected*' server directory to the '*%InstallDir%\OPC-UA\Server\PKI\trusted\certs*' directory.

5.2.5 BadSecurityChecksFailed

The server has not received the UA Client certificate, or it is in the rejected folder of the server.

Solution:

- Move the certificate from the rejected folder to the trusted folder of the server. Attempt to connect again.
- If the server has not received the certificate than manually copy the client certificate to the trusted folder of the server. Attempt to connect again.

6 Appendix

6.1 Supported Features

As part of the standard (OPC UA Part 7), the OPC UA Server will support features (Table 10):

Service Set	Service	Supported
Discovery	Find Server	Yes
	Find Server On Network	No
	GetEndpoint	Yes
	Register Server	No
	Register Server 2	No
Session	Create Session	Yes
	Activate Session	Yes
	Close Session	Yes

Service Set	Service	Supported
	Cancel	No
NodeManagment	Add node	No
	Add reference	No
	Delete node	No
	Delete reference	No
View	Browse	Yes
	Browse next	Yes
	TranslateBrowsePathToNodeIds	Yes
	Register Node	Yes
	Unregister Nodes	Yes
Query	Query First	No
	Query Next	No
Attribute	Read	Yes
	History Read	No
	Write	Yes
	History Update	No
Method	Call	No
Monitored Item	Create	Yes
	Modify	Yes
	Set Monitoring Mode	Yes
	Set Triggering	No
	Delete Monitoring Items	Yes
Subscription	Create	Yes
	Modify	Yes
	Set Publishing Mode	Yes
	Publish	Yes
	Republish	Yes
	Transfer Subscription	No
	Delete Subscription	Yes

Table 10: Supported OPC UA service set

	Feature	Supported
Encryption	None	Yes
	Basic128Rsa15	Yes
	Basic256	Yes
	Basic256Sha256	Yes
	Aes256Sha256RsaPss	Yes
Authentication	Anonymous	Yes
	User Name Password	Yes
	X509 Certificate	No

Table 11: Supported OPC UA stack

	Feature	Supported
Subscription	DataChange MonitoredItems	Yes
	DataChange Filters	Yes
	Event MonitoredItems	Yes
	Event Filters	Yes

Table 12: Supported subscription

	Feature	Supported
Discovery	Local Discovery Server	Yes
	Local Discovery Server Multicast Ext.	Yes
	Global Discovery Server	No

Table 13: Supported discoveries modes

	Feature	Supported
Access Type Specifications	Data Access (DA)	Yes
	Alarms & Events	No
	Historical Data Access (HDA)	No

Table 14: Supported access types

6.2 Default Settings

	Setting	Default Value
Server	maxSessions	100
	maxSessionTimeout	1 Hour
	maxSecureChannels	40
	maxSecurityTokenLifetime	10 Minute
Subscriptions	publishingIntervalLimits	0.1 sec ~ 3600 sec
	lifeTimeCountLimits	3 ~ 15000
	keepAliveCountLimits	1 ~ 100
	maxNotificationsPerPublish	1000
	enableRetransmissionQueue	True
	maxRetransmissionQueueSize	Unlimited
	maxEventsPerNode	Unlimited
Monitored Items	samplingIntervalLimits	0.05 sec ~ 24 Hour
	queueSizeLimits	1 ~ 100
	maxMonitoredItems	0 (Unlimited)
	maxMonitoredItemsPerSubscription	0 (Unlimited)
	maxPublishReqPerSession	0 (Unlimited)

Table 15: Default settings