

# **OPC UA Server**

**for Win-GRAF**

## **User Manual**

**(Version 1.0)**



### **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 © 2022 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](mailto:service@icpdas.com)

[service.icpdas@gmail.com](mailto:service.icpdas@gmail.com)

## Revision

Revision	Date	Description	Author
1.0	30.06.2022	Initial version	M. K.

# Contents

1	INTRODUCTION.....	6
2	SOFTWARE INSTALLATION.....	6
2.1	WORKBENCH.....	6
2.2	RUNTIME.....	6
3	OPC UA SERVER CONFIGURATION.....	8
3.1	SERVER CONFIGURATION PROCEDURE.....	8
3.2	SERVER CONFIGURATION PARAMETERS.....	14
3.2.1	<i>Server Information</i> .....	14
3.2.2	<i>Session Settings</i> .....	16
3.2.3	<i>Server Subscription Setting</i> .....	16
3.3	USER AUTHENTICATION CONFIGURATION.....	18
3.3.1	<i>Anonymous Identity Token</i> .....	19
3.3.2	<i>User Name Identity Token</i> .....	20
3.3.3	<i>X509 Identity Token</i> .....	21
3.4	ENDPOINT SETTING.....	25
3.5	SECURITY POLICIES SETTING.....	27
3.6	SELF-SIGNED SECURITY INFORMATION.....	28
3.6.1	<i>Manual Certificate Handling</i> .....	30
3.6.2	<i>Create New Security Certificate</i> .....	32
3.7	VARIABLE NODE ASSIGNMENT.....	33
4	UA EXPERT CLIENT - WINGRAF UA SERVER.....	35
4.1	NO SECURITY POLICY AND ANONYMOUS IDENTITY TOKEN.....	35
4.1.1	<i>Win-GRAF server</i> .....	35
4.1.2	<i>UA-Expert Client</i> .....	36
4.2	SECURITY POLICY AND LOGIN ACCOUNT (USERNAME AND PASSWORD).....	40
4.2.1	<i>Win-GRAF server</i> .....	40
4.2.2	<i>UA-Expert Client</i> .....	42
4.3	SECURITY POLICY AND IDENTITY CERTIFICATE.....	47
4.3.1	<i>Win-GRAF server</i> .....	47
4.3.2	<i>UA-Expert Client</i> .....	50
4.4	SUBSCRIPTION SETTING.....	53
4.4.1	<i>Win-GRAF server</i> .....	53
4.4.2	<i>UA-Expert Client</i> .....	53
5	SERVER OPERATION ERROR.....	56
5.1	TRACE LOG.....	56
5.1.1	<i>Server Failed to Create Endpoints</i> .....	57
5.2	COMMUNICATION ERROR MESSAGE.....	57
5.2.1	<i>BadCertificateHostNameInvalid</i> .....	57
5.2.2	<i>BadSecurityModeInsufficient</i> .....	60
5.2.3	<i>BadUserAccessDenied</i> .....	60
5.2.4	<i>BadUserAccessDenied, BadSecurityCheckFailed</i> .....	61
6	APPENDIX.....	61
6.1.1	<i>Combination of User Identity, Self-Assigned Certificate and Security Policies</i> .....	61

6.1.2 *Supported Features*..... 64  
6.1.3 Default Settings..... 65

---

# 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 for configuring the server.

*C:\Program Files (x86)\Win-GRAF Workbench\Win-GRAF Wb xx.xx\IOD\K5BusOpcUaServ.dll*

### 2.2 Runtime

By default the OPC UA server runtime DLL ("*ddkc\_opcuaserv.dll*") is being installed by the runtime setup program in the directory of the runtime execution file "*WinGrafRuntime.exe*". If you manually move the runtime execution file to a different

directory make always sure that the server DLL is being placed in the runtime directory.

---

## 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 a vital role in your application a deeper understanding of how OPC UA certificates are used by the servers and clients to securely identify and communicate with each other is being required.

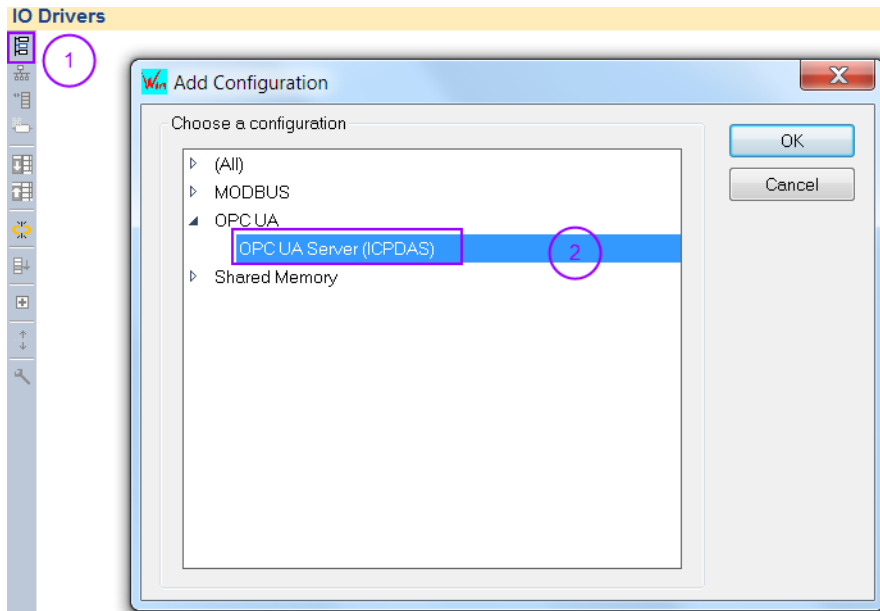
This chapter gives a quick overview of the OPC UA server configuration procedure using the Win-GRAF workbench and describes the supported configuration parameters.

### 3.1 Server Configuration Procedure

This section provides a quick overview how to add and configure a OPC UA server with the Win-GRAF workbench. The next chapter describes the server parameters in more details.

- Step 1:** Start the Win-GRAF workbench and create a new project
- Step 2:** 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.
- Step 3:** Open the 'OPC UA Server' plug-in: Click 'Insert Configuration'  button on the left toolbar and select 'OPC UA Server (ICPDAS)' from the 'Add Configuration' dialog.



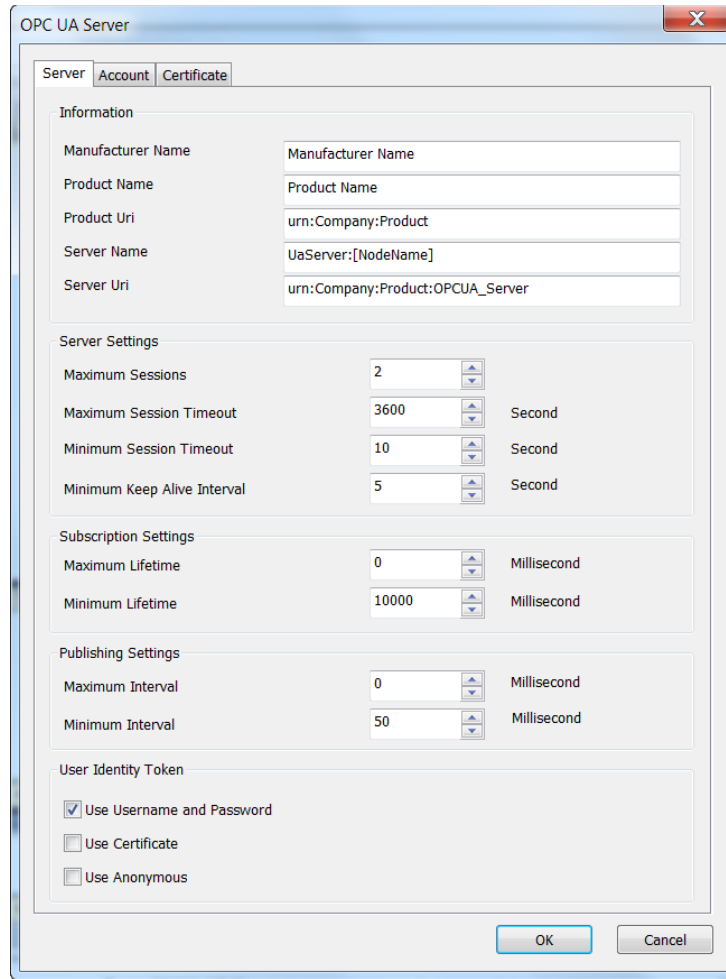


**Step 4:** Basic configuration parameters setting:

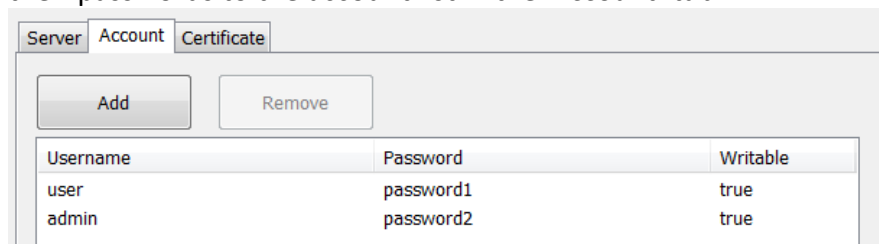
- Click on the "OPC UA Server (ICPDAS)" node to show a list of basic configuration parameters with their default values. Double click a parameter entry in the 'Value' column to modify the setting.

IO Drivers		Name	Value
opc	OPC UA Server (ICPDAS)	Server Name	UaServer:[NodeName]
		Server URI	urn:Company:Product:OPCUA_Server
		Product Name	Product Name
		Product URI	urn:Company:Product
		Manufacturer Name	Manufacturer Name
		Max Session	2
		Max Session Timeout	3600
		Min Session Timeout	10
		Min Keep Alive Interval	5
		Max Publish Interval	0
		Min Publish Interval	50
		Max Subscription Lifetime	0
		Min Subscription Lifetime	10000
		Use Username and Pass...	True
		Use Anonymous	False
		Use Certificate	False

- Double click the 'OPC UA Server (ICPDAS)' node (left hand side) to open a separate dialog which beside the basic parameter allows you to do additional setting (e.g. user identity token, user login account).



- If 'Use Username and Password' is selected, add the usernames with their passwords to the account list in the 'Account' tab



- Under the 'Certificate' tab make sure that the 'Enable Server Self-Signed' option is enabled and the other detailed as shown below a filled in. The server will use this information to generate a certificate with its private key and store it in the directories '*pkiserver\own\certs\*' and '*pkiserver\own\private\*'. The 'Enable Server Self-Signed' option only needs to be selected if no server certificate with its key already exist in the directories, because the server can not start without having a certificate.

Server Account Certificate

Enable Server Self-Signed

Certificate Information

Common Name  
[ServerName]

Organization  
Organization

Organization Unit  
Unit

Location Name  
Location Name

Country (2 letters)  
US

State / Province

Machine  
[NodeName]


IP Addresses (separate by semicolon)  
192.168.2.51

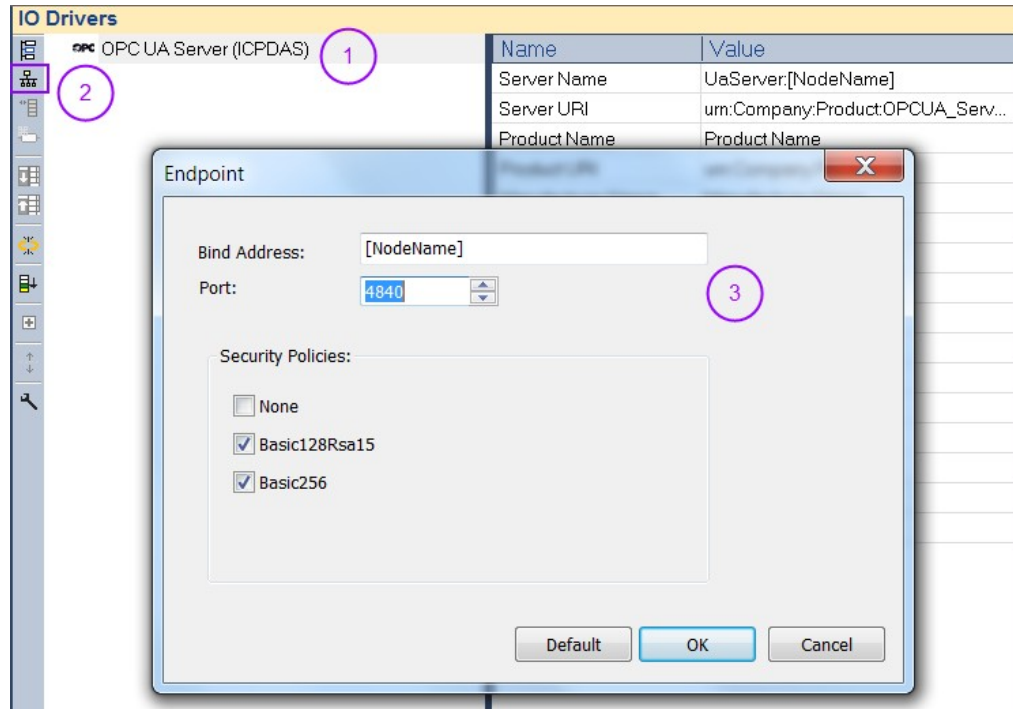
DNS Names (separate by semicolon)  
[NodeName]

Years Valid For:  
20


**Step 5:** Endpoint setting:

- Add a endpoint node to the server:

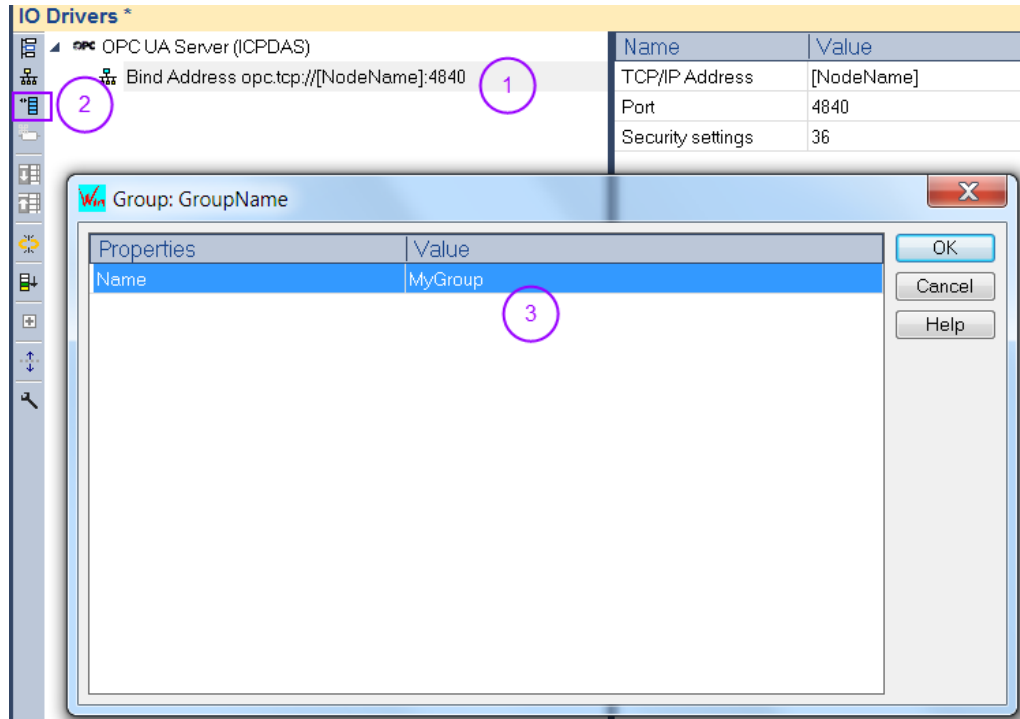
1. Activate the '*OPC UA Server (ICPDAS)*' node by clicking on the node
2. Click on the 'Insert Master/Port' button  on the left toolbar. A '*Endpoint*' dialog pops up.
3. Set the endpoint parameters. Only one endpoint is supported by the Win-GRAF server. Confirm the setting with 'OK'.



**Step 6:** Create a monitoring group node:

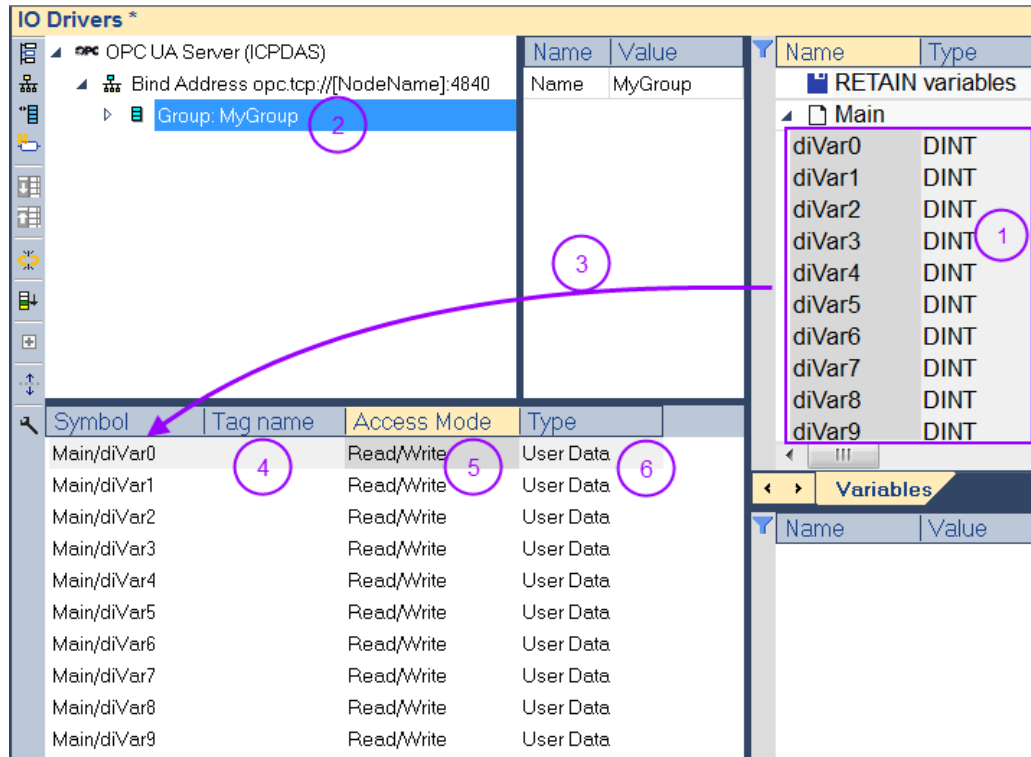
1. Activate endpoint node ('Bind IP Address: *opc.tcp://...*')
2. Click '*Insert Slave/Data Block*' command  on the left toolbar. A 'Group' dialog will be displayed
3. Enter a group name in the dialog by double clicking the '*Value*' column. Click 'OK'

The new node with the group name will added to the tree view.



**Step 7:** Assign PLC variable to the group. Here the PLC variables are assigned to the UA server for the client to access.

1. Declare variables to be accessed by the client
2. Select the group node by clicking on it
3. Drag and drop the variables to the mapping area
4. Enter a '*Tag name*' for each variable. The tag name will be shown to the client. If the tag name is empty then the '*Symbol*' name will use for the node name.
5. Select the client access mode: '*Read only*', '*Write only*' or '*Read/Write*', '*No Access*'. If '*No Access*' has been selected then the variable represents the OPC UA server status. The type of status to be shown has to be set in the '*Type*' column.
6. In the '*Type*' column the OPC UA server status type represented by the variable is set. The '*Type*' column is only valid if the access mode '*No Access*' has been selected. Available server status type:
  - Server Status
  - Used Sessions
  - Used Subscription
  - Used Monitored Items



- Step 8:** Built the program, download it to the runtime and start the application. If no certificate exist in the folder '*.\pkiserver\own\certs*' of the runtime execution file directory then a new certificate with its private key will be automatically created.
- Step 9:** Use a OPC UA client to connect to the server.

## 3.2 Server Configuration Parameters

The communication settings 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.

### 3.2.1 Server Information

Information	
Manufacturer Name	Manufacturer Name
Product Name	Product Name
Product Uri	urn:Company:Product
Server Name	UaServer:[NodeName]
Server Uri	urn:Company:Product:OPCUA_Server

Server Setting	Description
Server Name	<ul style="list-style-type: none"> <li>The name of the server. The default common name is 'Server'.</li> <li>This name will be stored under the keyword '<i>[ServerName]</i>' which means strings containing the keyword are modified by the server by replacing the keyword with the server name. For example by default the keyword '<i>[ServerName]</i>' is assigned to the '<i>Common Name</i>' of the self-signed certificate (Figure 12), which means the server name will be used as a '<i>Common Name</i>'.</li> <li>Use the key string '<i>[NodeName]</i>' to automatically gets the host name of the actual computer. <ul style="list-style-type: none"> <li>For example: If the computer name is '<i>DESKTOP123</i>' then the string '<i>MyName@[NodeName]</i>' will generate the common name '<i>MyName@DESKTOP123</i>'</li> </ul> </li> </ul>
Server Uri	<ul style="list-style-type: none"> <li>Every Server shall have a globally unique identifier called the ServerUri.</li> <li>if a UA server is selected, the server URI will be displayed. The server URI can be used as a reference to filter the discovery result.</li> <li>The default name is '<i>urn:Company:Product:OPCUA_Server</i>'</li> <li>The following the key strings are supported: <ul style="list-style-type: none"> <li><i>'[NodeName]</i>' - gets the host name of the actual computer.</li> <li><i>'[ServerName]</i>' - replaces the key string with the server name</li> </ul> </li> <li>example: <ul style="list-style-type: none"> <li><i>'urn:MyCompany:MyProduct:MyServer'</i></li> <li><i>'urn:[NodeName]:MyProduct:[ServerName]'</i></li> </ul> </li> </ul>
Manufacturer Name	<ul style="list-style-type: none"> <li>The name of the manufacturer. This name will be used for the PLC application program build information and is shown in the trace log file.</li> </ul>
Product Name	<ul style="list-style-type: none"> <li>The name of this application. Same as the manufacturer name it is being used as internal data to identify the build program and the trace log file. Appears as a header in the trace log file.</li> </ul>
Product URI	<ul style="list-style-type: none"> <li>A globally unique identifier for the product the server belongs to.</li> <li>Default name: '<i>urn:Company:Product</i>'</li> <li>The following the key strings are supported: <ul style="list-style-type: none"> <li><i>'[NodeName]</i>' - gets the host name of the actual computer.</li> <li><i>'[ServerName]</i>' - replaces the key string with the server name</li> </ul> </li> <li>example: <ul style="list-style-type: none"> <li><i>'urn:MyCompany:MyProduct'</i></li> <li><i>'urn:[NodeName]:MyProduct'</i></li> </ul> </li> </ul>

Table 1: Server information

### 3.2.2 Session Settings

Server Settings		
Maximum Sessions	2	
Maximum Session Timeout	3600	Second
Minimum Session Timeout	10	Second
Minimum Keep Alive Interval	5	Second

Descriptions of the parameters are as follows:

Server Setting	Description
Maximum Sessions	<ul style="list-style-type: none"> <li>This parameter specifies the limit of supported connections. The valid range is 1 to 128. The default setting is 2.</li> </ul>
Session Timeouts	<ul style="list-style-type: none"> <li>This parameter specifies the UA client's timeout limit for establishing a session. Values may be changed depending on the needs of the application. The default values are 10 to 3600.</li> <li><b>Minimum:</b> This parameter specifies the UA client's minimum timeout limit. The default setting is 10 seconds.</li> <li><b>Maximum:</b> This parameter specifies the UA client's maximum timeout limit. The default setting is 3600 seconds</li> </ul>
Keep Alive Interval	<ul style="list-style-type: none"> <li>Subscriptions have a keep-alive counter that counts the time in which there have been no Notifications to report to the Client. When the Keep Alive timeout is reached, a Keep Alive Message informs the Client that the Subscription is still active.</li> <li>In case that there is nothing to report (e.g. no values have changed) the server will send a Keep Alive notification to the Client, which is an empty Publish, to indicate that the server is still alive.</li> </ul>

Table 2: Server Settings

### 3.2.3 Server Subscription Setting

OPC UA supports polling and subscription mode.

- In polling mode the client is continuously updating the objects at a defined interval. This creates a higher communication loading and is therefore only recommended for a few symbols.
- In subscription mode the server monitors a selected number of nodes. Only when the nodes value changes will the server notify the client about the changes. This



mechanism reduces the amount of transferred data immensely and is therefore the recommended mode for reading information from a OPC UA server.

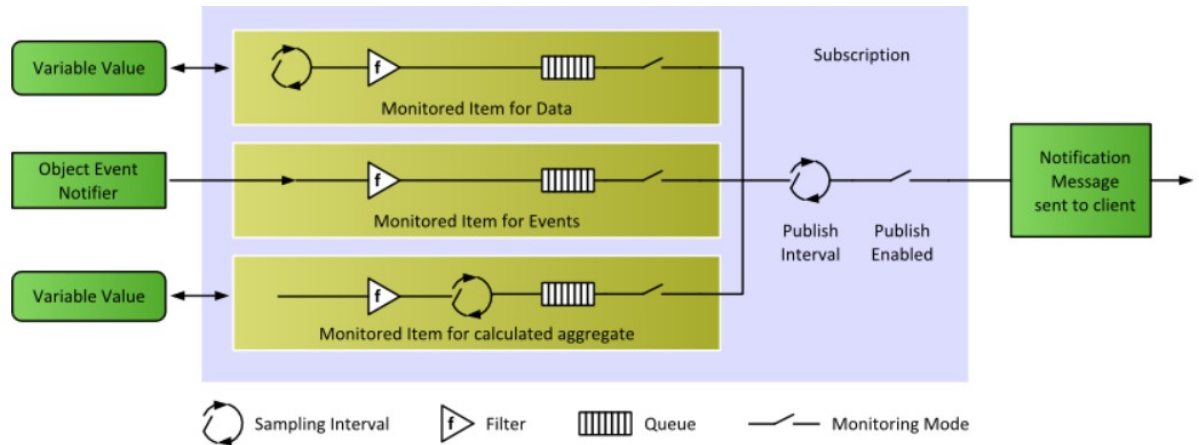


Figure 1: Subscription mode setting

In the following the subscription setting is described.

Subscription Settings		
Maximum Lifetime	10000	Millisecond
Minimum Lifetime	0	Millisecond
Publishing Settings		
Maximum Interval	1000	Millisecond
Minimum Interval	0	Millisecond

Server Setting	Description
Lifetime	<ul style="list-style-type: none"> <li>Interval, in which server publish data to Client</li> <li>The server will modify the 'Minimum Interval' interval to protect the source from extensive load that may be caused by a high sampling rate.</li> <li><b>Maximum:</b> The maximum Subscription lifetime (in milliseconds) the server allows. (Default: 10000)</li> <li><b>Minimum:</b> The minimum subscription lifetime (in milliseconds) the server allows; 0 is no limitation. (Default: 0)</li> </ul>
Interval	<ul style="list-style-type: none"> <li>Interval for sampling (and storing) data at server and send in each publishing interval. The sampling interval defines is the time interval at which the server checks the Monitored Item for data changes. The interval can be set to a faster than the notification interval (Lifetime) to the Client, in which case the server may queue the sampled data and publish the complete queue.</li> </ul>

Server Setting	Description
	<ul style="list-style-type: none"> <li>• <b>Maximum:</b> The maximum publishing interval (in milliseconds) the server allows. (Default: 1000).</li> <li>• <b>Minimum:</b> The minimum publishing interval (in milliseconds) the server allows. (Default: 50).</li> </ul>

Table 3: Subscription parameter

### 3.3 User Authentication Configuration

When a user is trying to connect from an OPC UA Client to an OPC UA Server, the OPC UA server needs to confirm the identity of the user before allowing the connection from the OPC UA client. The Win-GRAF server currently supports three different ways to authenticate a user during the activation of a session:

- Anonymous Identity Token
- User Name Identity Token
- X509 Identity Token

The '*User Identity Token*' area determines the identity types of the client that will be allowed to log on to the OPC UA server (Figure 2).

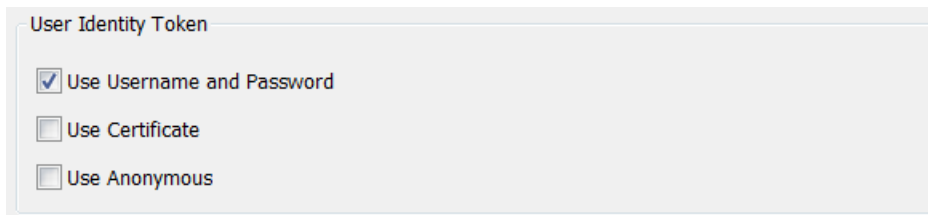


Figure 2: User Identity Token

Identity Token Option	Description
Use Username and Password	<p>User Name Identity Token</p> <ul style="list-style-type: none"> <li>• Require clients to enter a username and password that a match a user in your project's security system. This option is available only if the security system has been enabled.</li> <li>• If this option has been selected it is necessary to enter the username and password. The '<i>Account</i>' tab (Figure 6) provides a list in which the user with the password can be entered.</li> <li>• Default: Enabled</li> </ul>
Use Certificate	<p>X509 Identity Token</p> <ul style="list-style-type: none"> <li>• Instead of using a username and password to login into the server a separate X509 certificate is being used for each user.</li> </ul>

Identity Token Option	Description
	<ul style="list-style-type: none"> <li>The common name of the X509 certificate acts as the user name and its private key functions as a password.</li> <li>Default: Disabled</li> </ul>
Use Anonymous	<ul style="list-style-type: none"> <li>Allow clients to log on to the server without entering a username or password.</li> <li>Default: Disabled</li> </ul>

**Table 4: Identity token description**

Note:

- At least one of the available options have to be set. If none of the identity options have been selected then the client will not be able to connect to the server.
- The options are not exclusive; more than one option can be selected

In the following the three application based security configuration is explained.

### 3.3.1 Anonymous Identity Token

The anonymous identity token does not perform any authentication (Figure 3). That means

- Every client which certificate has been added to the '*pkiserver/trusted/certs*' directory can establish a connection with the server without having to enter a user name and password
- If the '*Security Policy*' of the server is set to '*None*' (Figure 4) then all clients regardless whether they are trusted by the server or not can create a session with the server.

For security reasons it is recommended to use anonymous identity token.

The screenshot shows a configuration window titled "User Identity Token". It contains three radio button options: "Use Username and Password", "Use Certificate", and "Use Anonymous". The "Use Anonymous" option is selected, indicated by a checkmark in the box next to it.

**Figure 3: Anonymous identity token setting**

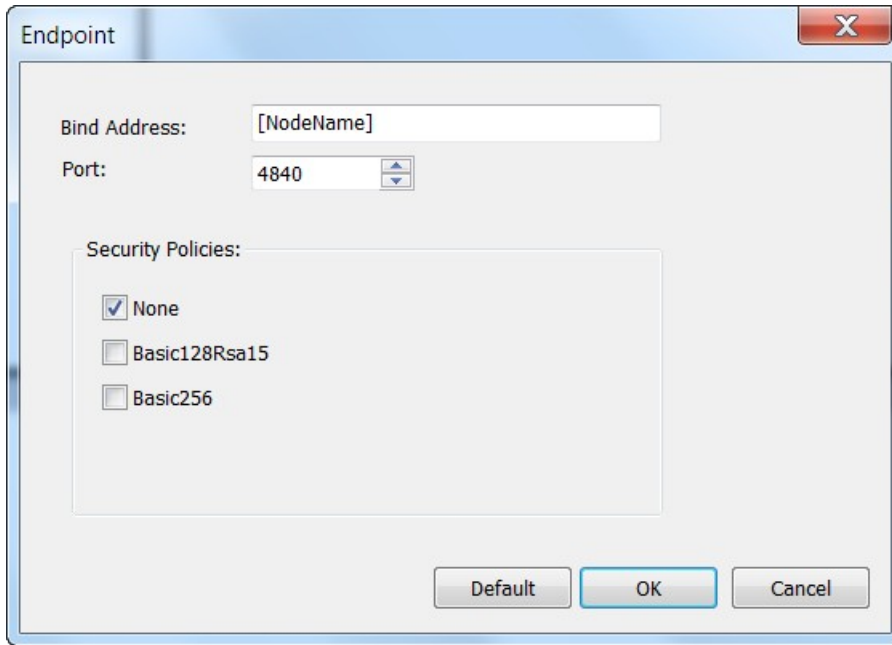


Figure 4: Security policy disabled

### 3.3.2 User Name Identity Token

This token type configuration (Figure 5) allows to authenticate the user using an username and password. The password is passed to the UA Server in encrypted form, even when using a none secure channel. The password is never stored in the memory as a plain text so it is always protected.

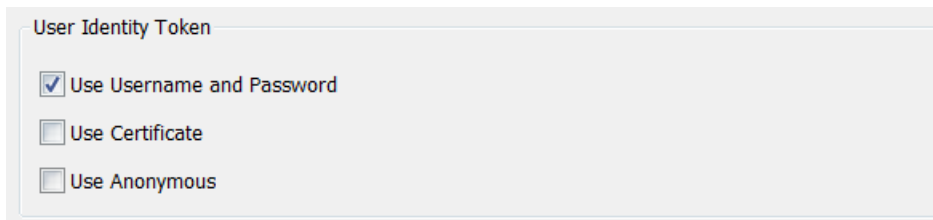


Figure 5: User name identity token setting

The user account list (Figure 6) allows you enter a number of usernames with the corresponding password. In addition the access right for each user can be limited to only read access by disabling the '*Write Authorization*' checkbox.

The default account entries are shown in Figure 6.

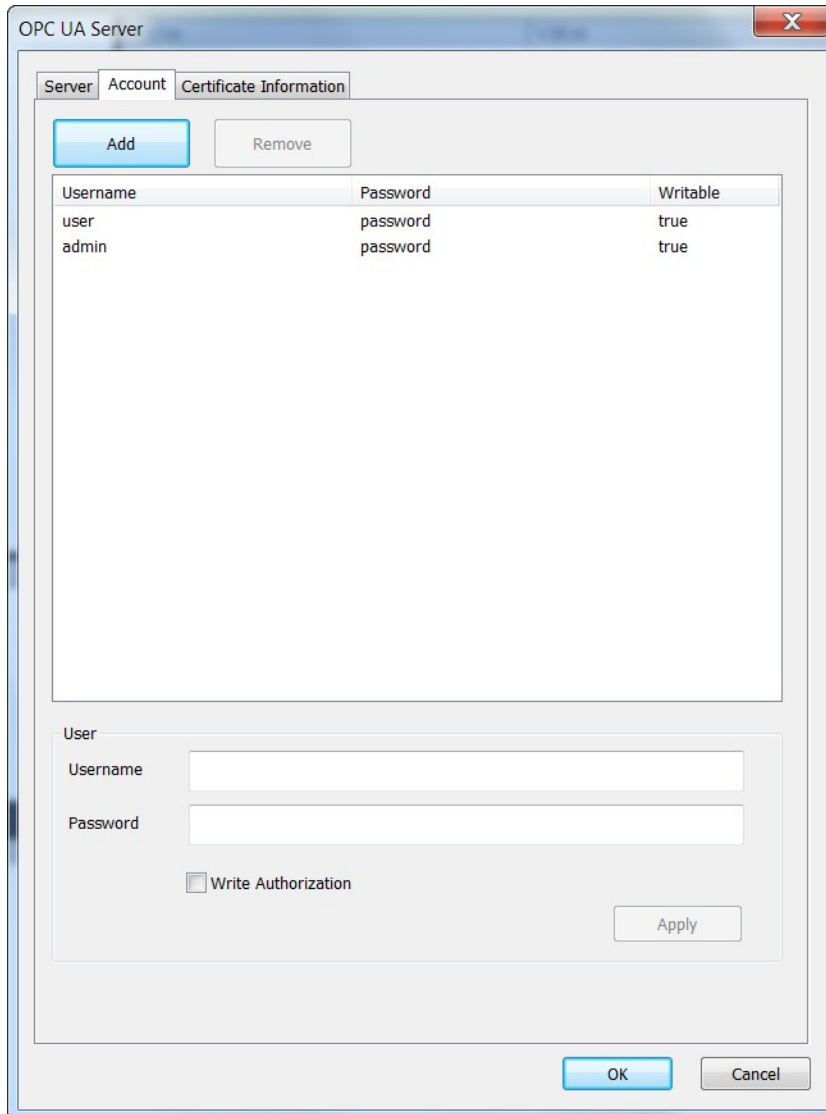


Figure 6: User account

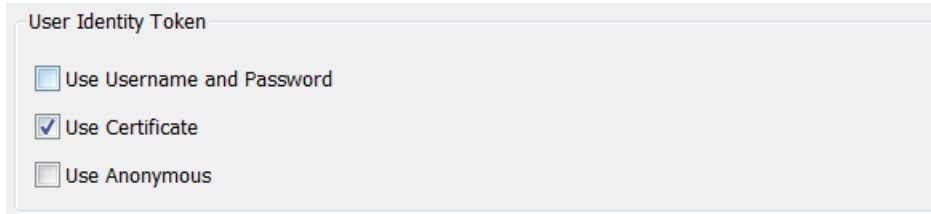
**Note:**

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

### 3.3.3 X509 Identity Token

This allows authenticating users using X509 certificates (Figure 7). The system administrator has to provide for each user with a separate authentication certificate together with its private key which can either be stored on a smart card or on the client itself which is less secure. In addition the system administrator has to add the authentication certificate file without its private key to the Win-GRAF server directory '\

*pkiserver\trusted\certs\*' which contains all the trusted OPC UA clients certificates. The client generates a signature using the private key of the X509 certificate and the server uses the public key of the same certificate to verify the received cryptographic signature.



**Figure 7: Enabling the X509 identity token mechanism**

This identity token authorization mechanism is similar to the password authentication where the '*Common Name*' (CN) field of the X509 certificate is mapped to a username and instead of a password the private key of the certificate is being used to authenticate the user. In the same way as for the password authentication the '*Common Name*' has to be added to the '*Username*' column of the user account list.

In the following the procedure for configuring the server to support X509 authentication is shown:

- Step 1:** Set the identity token to X509  
Double click the '*OPC UA Server (ICPDAS)*' node in the '*IO Driver*' window to open the main OPC UA configuration interface. Enable '*Use Certificate*' option as shown in Figure 7.
- Step 2:** Add the '*Common Name*' (CN) to the user account list.
1. Click the '*Account*' tab of the main configuration interface to display the account list.
  2. Click '*Add*' to add a new entry.
    - Enter the '*Common Name*' (CN) of the X509 certificate (Figure 9) to the '*Username*' edit box (Figure 8).
    - The password setting will be ignored if only the '*Use Certificate*' option is enabled (Figure 7). If the '*Use Username and Password*' option is selected as well then enter a secure password.
    - Determine whether the user should have both read and write access rights by selecting the '*Write Authorization*' option.
    - Click '*Apply*' and '*OK*' to confirm the setting

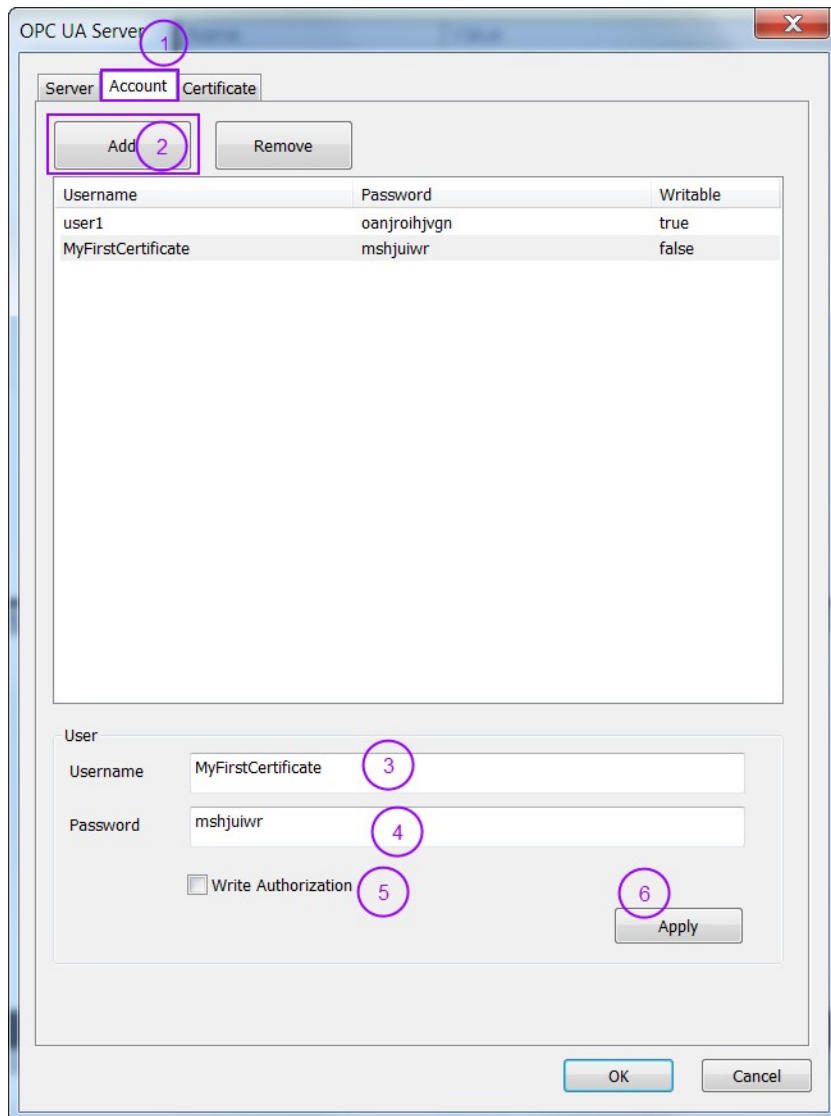


Figure 8: Add a 'Common Name'

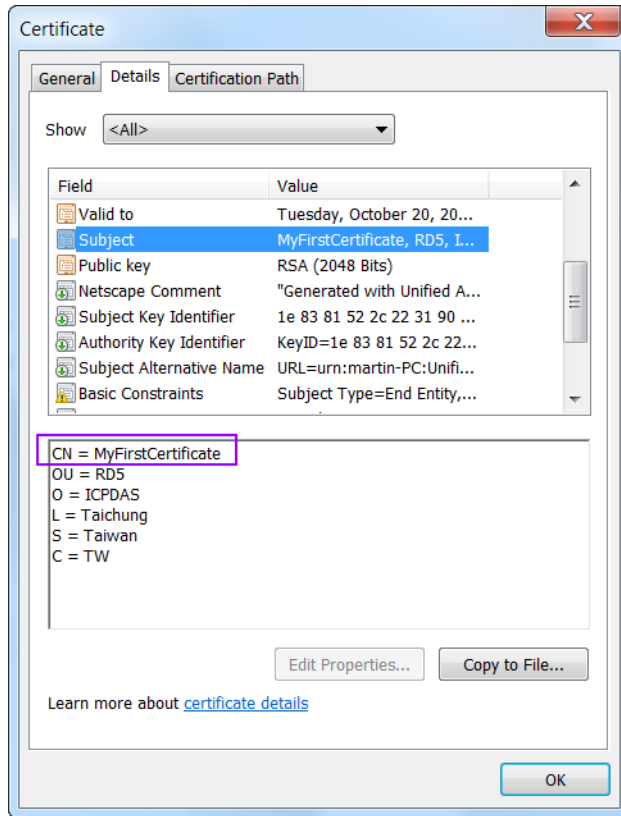
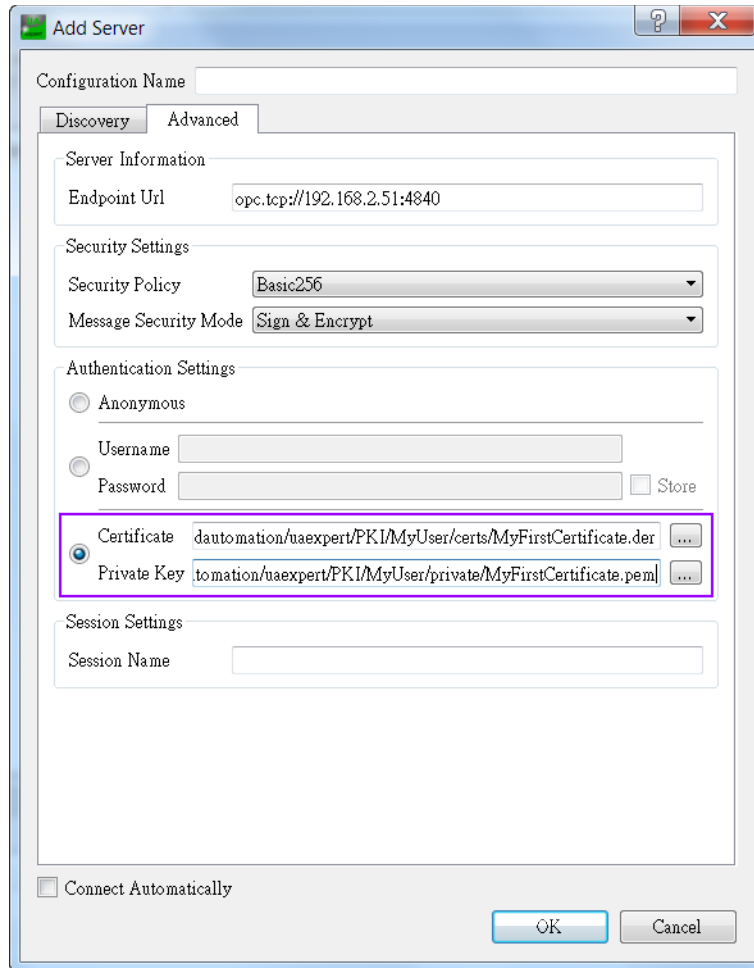


Figure 9: Example of a user authentication X509 certificate

- Step 3:** Copy the user authentication X509 certificate and the client certificate file to the trusted folder of the server '`\pkiserver\trusted\certs\`'.
- Note:
- If the client certificate is used also for user authentication then only the client certificate needs to be added to the trusted folder. In this case it is necessary to add the '*Common Name*' of the client certificate to the user account list of the server (Figure 8).
- Step 4:** Compile, download and run the PLC application.
- Step 5:** Use the UaExpert client tool to connect to the server. The '*Authentication Setting*' of the client has to be linked to the X509 certificate and its private key file so that the client can use the private key of the certificate to generate a encrypted signature.





### 3.4 Endpoint Setting

The endpoint stores all information which is required to establish a connection between client and server. The Win-GRAF OPC UA server supports only one endpoint. The endpoint contains the following information:

- Endpoint URL: protocol and network address (e.g. 'opc.tcp://<hostname>:<port>').
- Security Policy: name for a set of security algorithms and encryption key length (chapter 3.5). The key provided by the certificate is used for the encryption and for the Win-GRAF runtime its length is fixed to 1024.
- Message Security Mode: security level for exchanged messages (3.5)
- User Token Type (types of user authentication supported by the server) (3.3)

To access the endpoint configuration dialog double click the 'Bind IP Address' node.

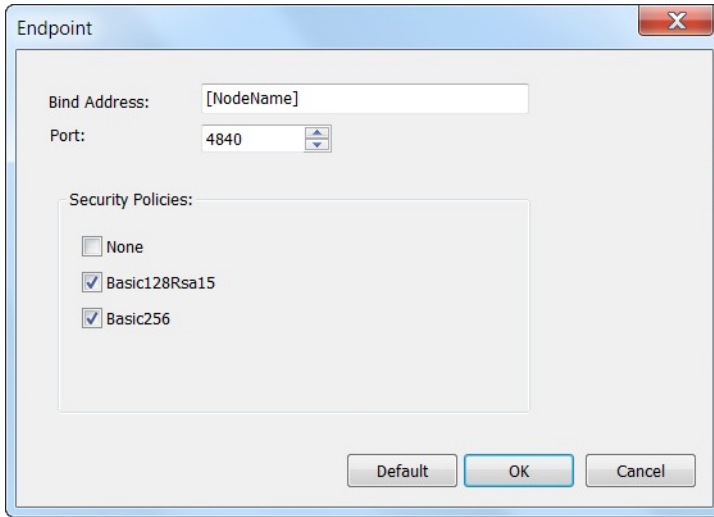


Figure 10: Endpoint configuration interface

Description of the parameters are as follows:

Endpoint Configuration Parameters	Description
Bind IP Address	<ul style="list-style-type: none"> <li>Define a specific IPv4 address the stack should use to bind to. It can be used to bind the endpoint to a specific network card or to local host only. The address is used for discovery and to open the Endpoints by the client. <ul style="list-style-type: none"> <li>'[NodeName]' or '0.0.0.0' can be used as placeholder for the host IP address(es). Server will listen to all interfaced on host. The stack binds to all IP addresses (on all network interfaces) of the host. Some OPC UA clients do not support 0.0.0.0 as endpoint or will issue a warning. In this case the place holder can not be used a the host IP address has to entered.</li> </ul> </li> <li>Default: [NodeName]</li> </ul>
Port Number	<ul style="list-style-type: none"> <li>This parameter specifies the port number.</li> <li>Default: 4840</li> </ul>
Security Policies	<ul style="list-style-type: none"> <li>Three security policies option are provided: <ul style="list-style-type: none"> <li>'None', Basic128Rsa15, Basic256 .</li> </ul> </li> <li>Default: 'Basic128RSA15' + 'Basic256'</li> </ul>

Example of typical endpoint setting:

Endpoint 1	Endpoint 2
<b>Endpoint URL:</b> <i>opc.tcp://192.168.5.68:4840</i>	<b>Endpoint URL:</b> <i>opc.tcp://[NodeName]:4840</i>
<b>Security Policy:</b> Basic256	<b>Security Policy:</b> Basic128Rsa15
<b>Message Security Mode</b> Sign, Sign and Encrypt	<b>Message Security Mode</b> Sign, Sign and Encrypt
<b>User Token</b>	<b>User Token</b>

Username	Username
----------	----------

Table 5: Endpoint setting example

### 3.5 Security Policies Setting

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 master. If none of the encryption options are selected then the communication between the server and client will not be encrypted. In this case only clients which security policy has been set to 'None' will be able to exchanged data.

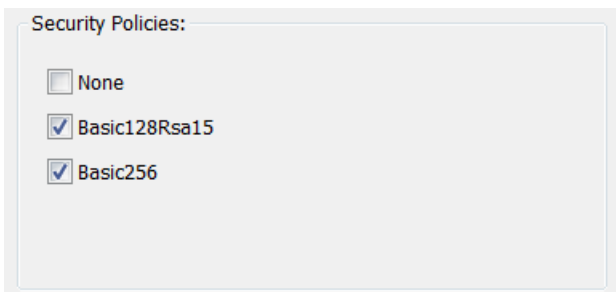


Figure 11: Encryption types (Security policies options) supported by the server

Security Policies Option	Description
None	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Default setting: Disabled</li> <li>• Message Mode: None</li> </ul>
Basic128Rsa15	<ul style="list-style-type: none"> <li>• The server will use and recognize 128-bit AES encryption.</li> <li>• Message Mode: Sign, Sign and Encrypt</li> <li>• Default setting: Enabled</li> </ul>
Basic256	<ul style="list-style-type: none"> <li>• The server will use and recognize 256-bit AES encryption.</li> <li>• Message Mode: Sign, Sign and Encrypt</li> <li>• Default setting: Enabled</li> </ul>

Table 6: Security policies options

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 '*pkiserver\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, the client certificate on the other hand has to be manually copied to the server trusted folder. The server needs the public key of the client certificate to decrypt the data package received by the client.

If the self-signed certificate has been enabled (Figure 12) 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.

*Message Mode:*

This parameter specifies the mode of encryption that will be used when messages between the client and server are exchanged. There are three options (Table 7): 'None', 'Sign' and 'Sign and Encrypt'. Win-GRAF runtime automatically selects the message mode according to security policies setting as shown in Table 6. The message mode can not be selected separately.

Message Mode	Description
None	<ul style="list-style-type: none"> <li>This mode is the least secure, but is also the fastest.</li> <li>Default setting: enabled</li> </ul>
Sign	<ul style="list-style-type: none"> <li>A checksum is added to the end of the message to ensure that the contents arrive clear and unaltered.</li> <li>This mode is more secure but can slow down communications.</li> </ul>
Sign and Encrypt	<ul style="list-style-type: none"> <li>A checksum that has been encrypted using the encryption method selected in Security Policy is added to the end of the message to ensure that the contents arrive clear and unaltered.</li> <li>This mode is more secure but can slow down communications.</li> </ul>

Table 7: Message mode

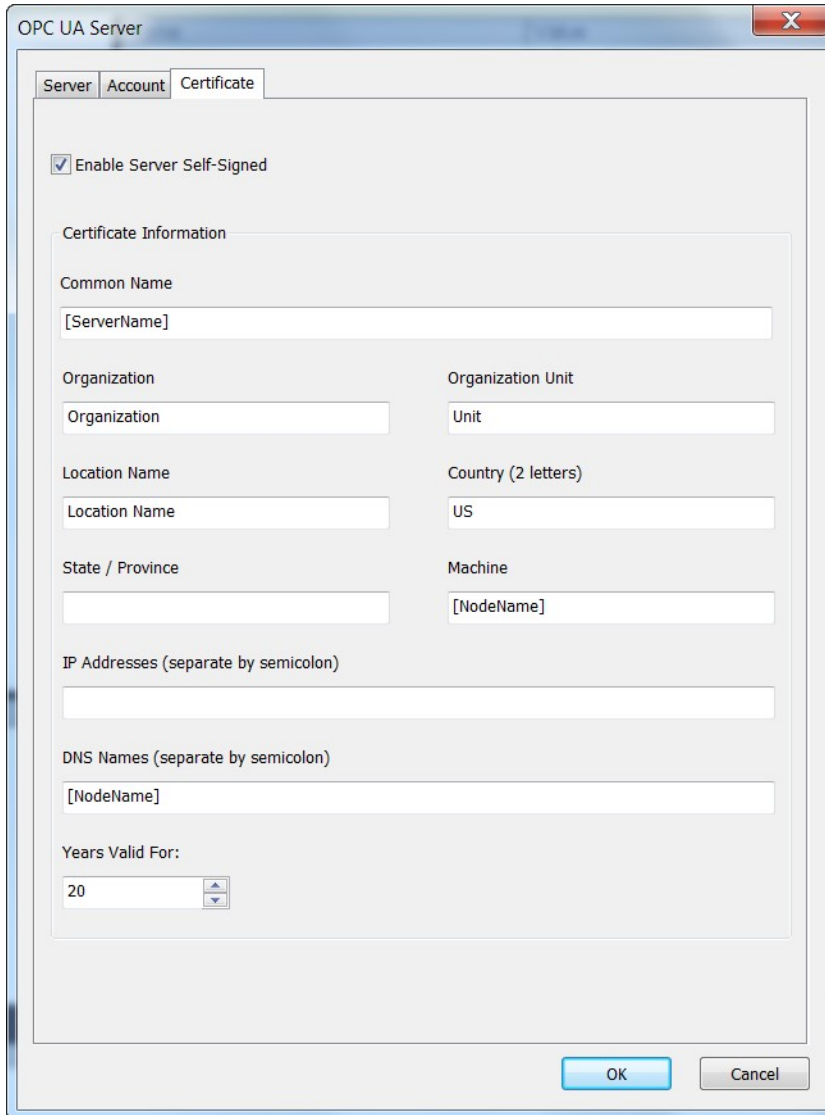
### 3.6 Self-Signed Security Information

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.

Double click the 'OPC UA server (ICPDAS)' node to open the dialog box and select the 'Certificate' tab to enter the information for the self signed certificate (Figure 12). All information entered in the dialog box will be used to create the certificate. Make sure that the 'Enable Server Self-Signed' option is enabled. Uncheck this 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.

**Note:**

It is important that there is a server certificate with its private key in the server directories 'pkiserver\own\certs\' and 'pkiserver\own\private\' otherwise the server will not configure an endpoint and can not be accessed by any client.



**Figure 12: Self-signed security information**

Certificate Info Parameter	Description
Common Name	<ul style="list-style-type: none"><li>The '<i>Common Name</i>' 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 <i>[ServerName]</i>. This keyword automatically assigns the server name set in the 'Server' tab to the '<i>Common Name</i>'.</li><li>Default setting: <i>[ServerName]</i></li></ul>
Organization	<ul style="list-style-type: none"><li>Organization that owns the application.</li></ul>

Certificate Info Parameter	Description
Organization Unit	<ul style="list-style-type: none"> <li>Organization's division/department to which the certificate is attached.</li> </ul>
Location Name	<ul style="list-style-type: none"> <li>City in which the OPC UA Client certificate is issued.</li> </ul>
State/Province	<ul style="list-style-type: none"> <li>State/province in which the OPC UA Client certificate is issued.</li> </ul>
Country	<ul style="list-style-type: none"> <li>Country in which the OPC UA Client certificate is issued.</li> </ul>
Machine	<ul style="list-style-type: none"> <li>The name of the computer or device that will host the project runtime server. The default machine name is <i>[NodeName]</i> which automatically gets the host name of the actual computer or device on which the Win-GRAF runtimes is installed</li> <li>Default: <i>[NodeName]</i></li> </ul>
IP Address	<ul style="list-style-type: none"> <li>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.</li> </ul>
DNS Name	<ul style="list-style-type: none"> <li>Names of the domain name servers that will administer the project runtime server. The default DNS name is <i>[NodeName]</i>.</li> <li>Default: <i>[NodeName]</i></li> </ul>
Validity Duration	<ul style="list-style-type: none"> <li>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. <ul style="list-style-type: none"> <li>Procedure to create a new certificate: Delete the certificate with the associated key file and restart the runtime to generate a new certificate</li> </ul> </li> <li>Default: 20 years</li> </ul>

**Table 8: Certificate information parameters**

### 3.6.1 Manual Certificate Handling

The file based certificate store on the Win-GRAF UA server has got the directory layout as shown in Table 9. 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 '*uaserver.der*' and private key '*uaserver.pem*' and place it in the '*own*' directory.

During the startup phase the Win-GRAF runtime checks whether a certificate in the folder '*\pkiserver\own\certs*' exist, if no certificate exist then a new certificate and private key is being created by the runtime. Make sure that the '*Enable Server self-Signed*' option is selected (Figure 12) to force the server to create a new certificate if none exists.

***Note:***

The private key ('*uaserver.pem*') has to remain secret and is used to sign and/or decrypt messages. Make sure no unauthorized person has access to the '*\pkiserver\own\private*'

folder.

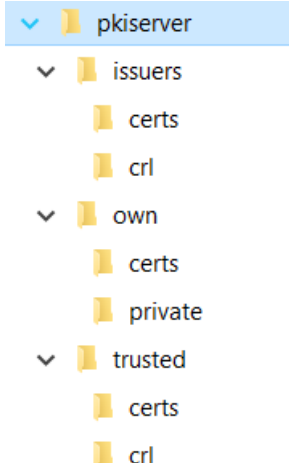
<p><b>pkiserver</b></p> <ul style="list-style-type: none"><li>▪ <b>issuers</b><ul style="list-style-type: none"><li>- certs</li><li>- crl</li></ul></li><li>▪ <b>own</b><ul style="list-style-type: none"><li>- certs stores the server certificate 'uaserver.der'</li><li>- private stores the private key 'uaserver.pem'</li></ul></li><li>▪ <b>trusted</b><ul style="list-style-type: none"><li>- certs the trusted client certificate has to be stored in this folder</li><li>- crl</li></ul></li></ul>	 <p>A folder tree diagram showing the structure of the 'pkiserver' directory. The root folder is 'pkiserver', which is expanded to show four sub-folders: 'issuers', 'own', 'trusted', and 'private'. Each of these sub-folders is further expanded to show its contents: 'issuers' contains 'certs' and 'crl'; 'own' contains 'certs' and 'private'; 'trusted' contains 'certs' and 'crl'; and 'private' contains 'certs' and 'crl'.</p>
---	--

Table 9: File based certificate store

### 3.6.1.1 Client Certificate

For the security policies (Basic128Rsa15, Basic256) the server requires the client certificate to encrypt the communication. The client certificate has to be copied to the trusted folder of the server '`\pkiserver\trusted\certs\`'. If the server does not find the client certificate or detects that it has expired, then the server will prevent any communication with this client. Data exchange with other clients with valid certificates still continues.

Users with administrative rights have to manually place a copy of the UA client certificate into the trusted folder of the server before the client can access the UA server.

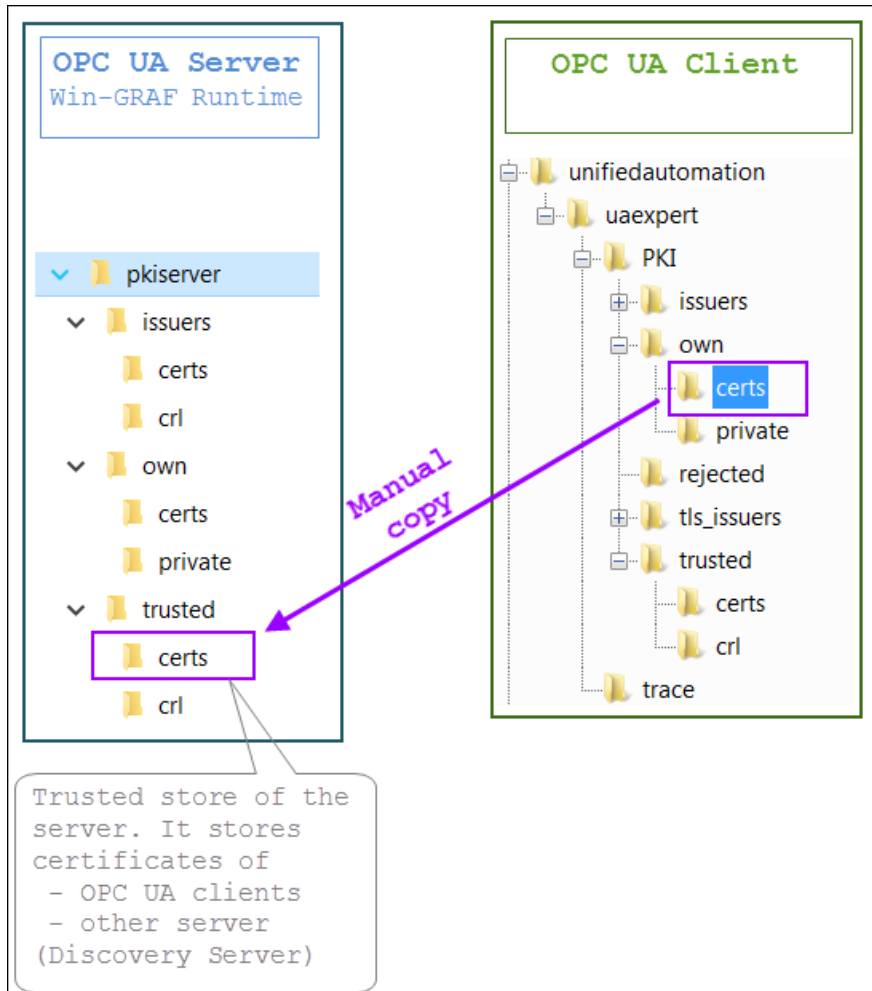


Figure 13: Trusted store folder of OPC UA server

### 3.6.2 Create New Security Certificate

A new server certificate will be generated only if the certificate and its associated key file do not exist in the following directories:

```
<WinGrafRuntime>\pkiserver\own\cert\userver.der
<WinGrafRuntime>\pkiserver\own\private\userver.pem
```

It is important to always delete both the certificate '*userver.der*' and the key file '*userver.pem*' together, to force the runtime to create a new certificate directly after startup. If the certificate and key are deleted while the runtime is running, a restart of the runtime is required to create a new certificate. It is important that the '*Enable Server self-Signed*' option is selected (Figure 12) to enable the server to create a new server



certificate if none exists.

**Hint:**

Just delete the 'Own' folder with it subfolder to quickly remove the certificate and key files together. The runtime will create the folders again after startup.

### 3.7 Variable Node Assignment

Map the PLC variable to the server node by either declaring a new PLC variable or selecting an existing variable from the variable editor. By mapping a new variable to the 'Group' directory in the OPC UA tree a new server variable node is being created. Assign the server node a name by either using the PLC declared variable name (empty 'Tag name' field) or defining a new name which has to be entered in the 'Tag name' field.

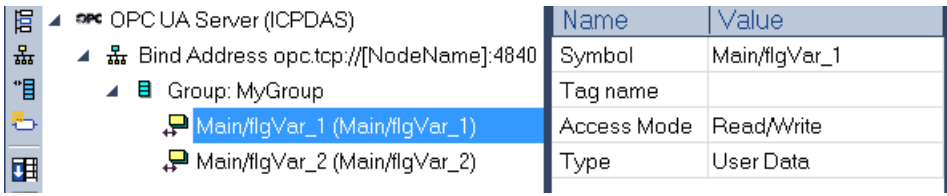
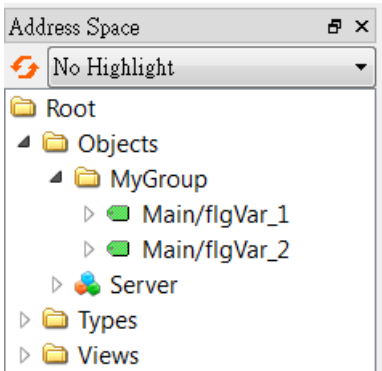
OPC UA	Description
<b>Server</b>	Win-GRAF workbench: Mapped PLC variables 
<b>Client</b>	UaExpert Client: Display of Win-GRAF mapped PLC variables 

Table 10: PLC variable mapping

Message Mode	Description
Symbol	<ul style="list-style-type: none"> <li>The variable name declared inside the PLC application</li> </ul>

Message Mode	Description
Tag name	<ul style="list-style-type: none"> <li>The variable node name displayed in the OPC UA Client</li> <li>If the '<i>Tag name</i>' is empty then the '<i>Symbol</i>' name will be used as the variable node name.</li> <li>Default: empty</li> </ul>
Access Mode	<ul style="list-style-type: none"> <li>Client access write: '<i>Read only</i>', '<i>Write only</i>', '<i>Read/Write</i>', '<i>No Access</i>'</li> <li>The mode '<i>No Access</i>' 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</li> <li>Default: '<i>Read/Write</i>'</li> </ul>
Type	<ul style="list-style-type: none"> <li>Select the server status type to read.</li> <li>This parameter is only valid if the '<i>Access Mode</i>' is set to '<i>No Access</i>', which means the mapped parameter will be updated with server status information. A variety of status information are available. Select one of them: '<i>Server Status</i>', '<i>Used Session</i>', '<i>Used Subscriptions</i>', '<i>Used Monitored Items</i>'</li> <li>Set the type to '<i>User Data</i>' if the '<i>Access Mode</i>' is set to any mode except '<i>No Access</i>'</li> <li>Default: '<i>User Data</i>'.</li> </ul>

**Table 11: 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 12: Supported data types**

---

## 4 UA Expert Client - WinGRAF 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. Using this client, you can connect to the Win-GRAF OPC UA server.

The following descriptions refers to the UaExpert program and demonstrate the effect of different server configurations on the client to server connection procedure. The demo program '*SimpleDemo*' with its server configuration will be used to show the effects of the server parameter settings.

The demo program is in the directory:

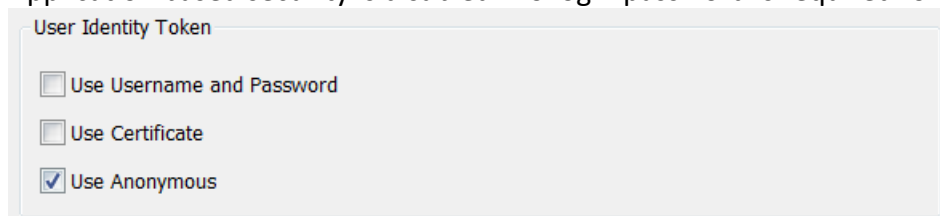
*C:\Users\Public\Documents\Win-GRAF Workbench\Win-GRAF Wb 10.0\Projects\OPC UA\ SimpleDemo*

### 4.1 No Security Policy and Anonymous Identity Token

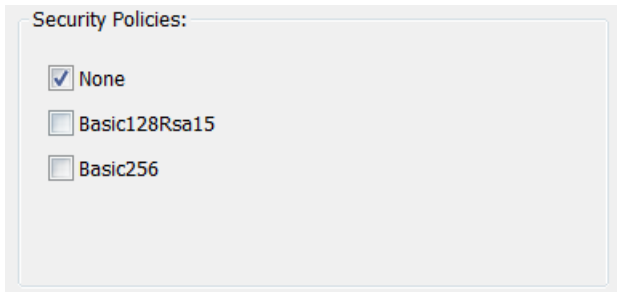
#### 4.1.1 Win-GRAF server

The server has been configured as follows:

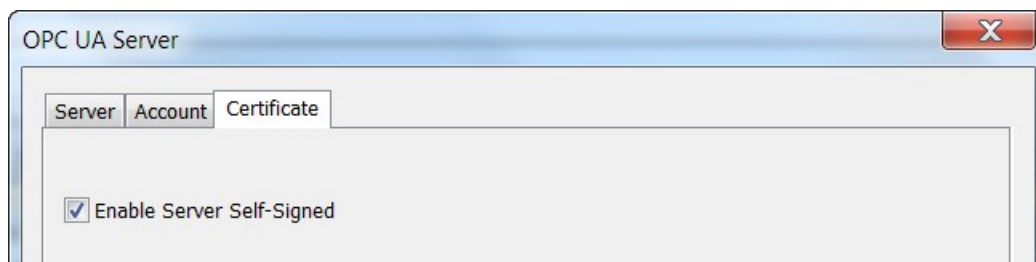
- Application based security is disabled. No login password is required for the client



- Disable security certificates for encrypted communication. This 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 'pkiserver\own\certs\' and 'pkiserver\own\private\''. Therefore enable the self-signed certificate option to inform the server to generate a new certificate and private key if no certificate could be found.



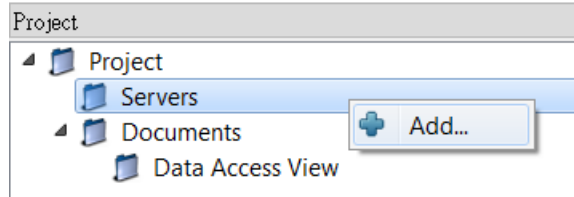
### 4.1.2 UA-Expert Client

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

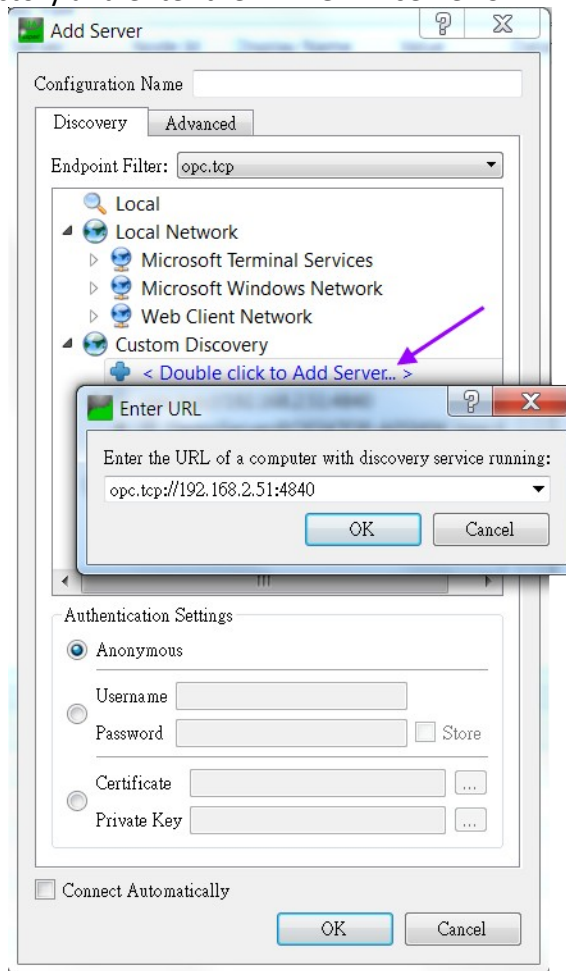


Add server to client:

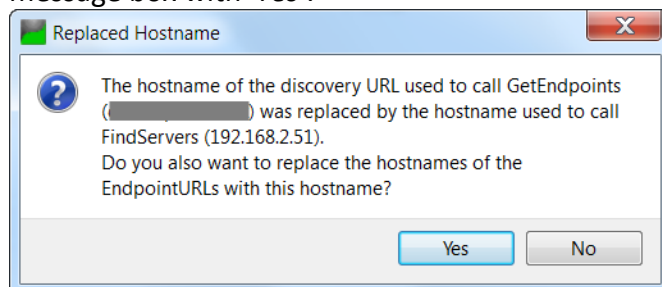
**Step 1:** Right-click on the 'Servers' to add your OPC-UA Server.



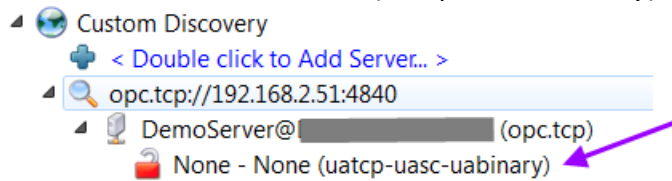
**Step 2:** Double click the '<Double click to Add Server>' in the 'Custom Discovery' directory and enter the Win-GRAF server URL in the pop-up dialog.



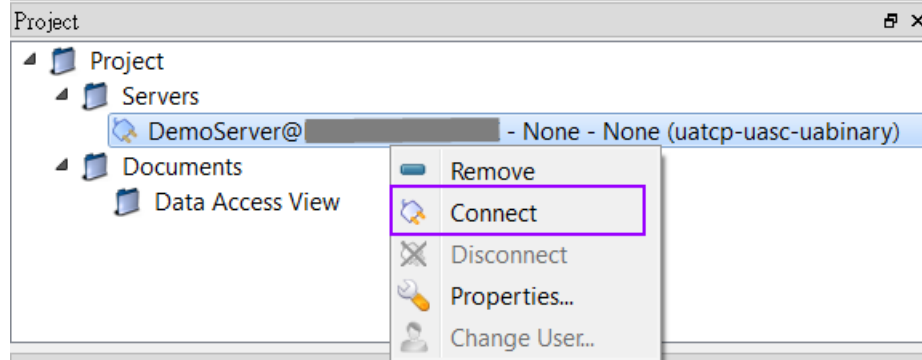
Open the 'Custom Discovery' tree node. Confirm the 'Replace Hostname' message box with 'Yes'.



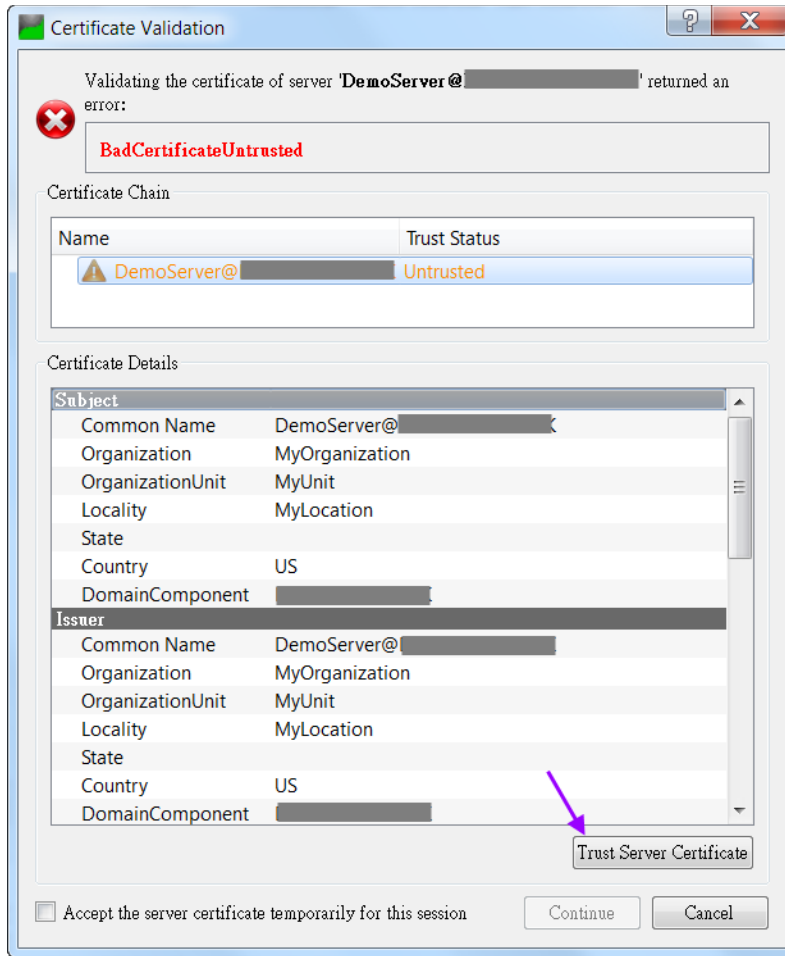
The discover directory shows that no decryption has been disabled ('None'). Double click the 'None-None(uatcp-uasc-uabinary)' connection type.



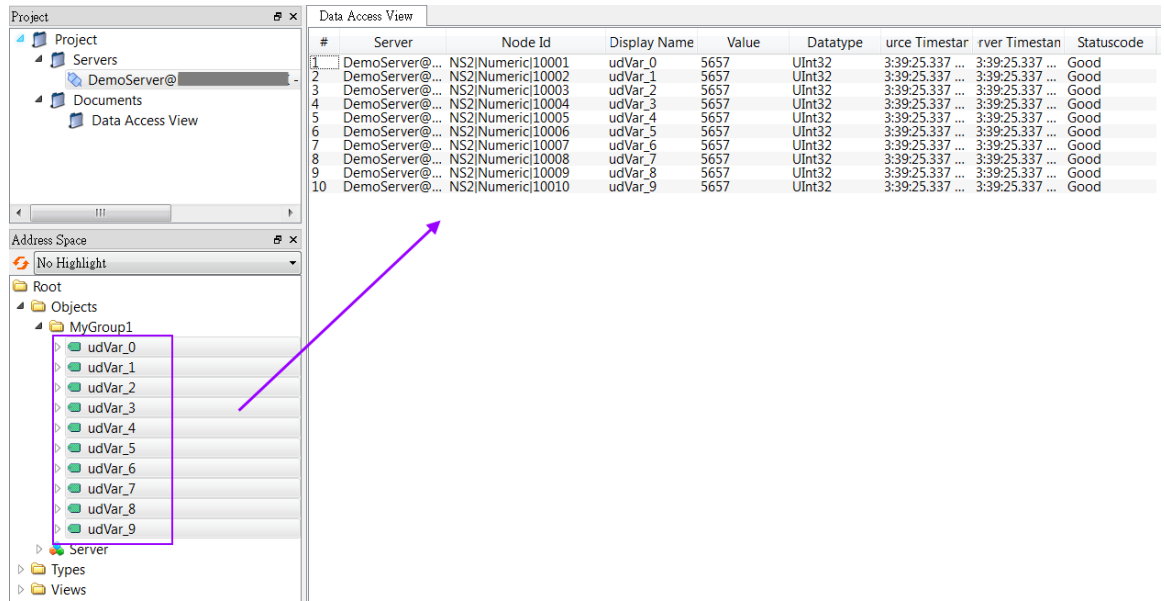
**Step 3:** Connect to the server by right clicking the server and selecting 'Connect'



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



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

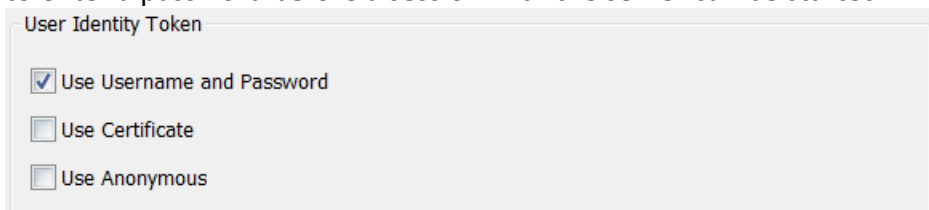


## 4.2 Security Policy and Login Account (Username and Password)

### 4.2.1 Win-GRAF server

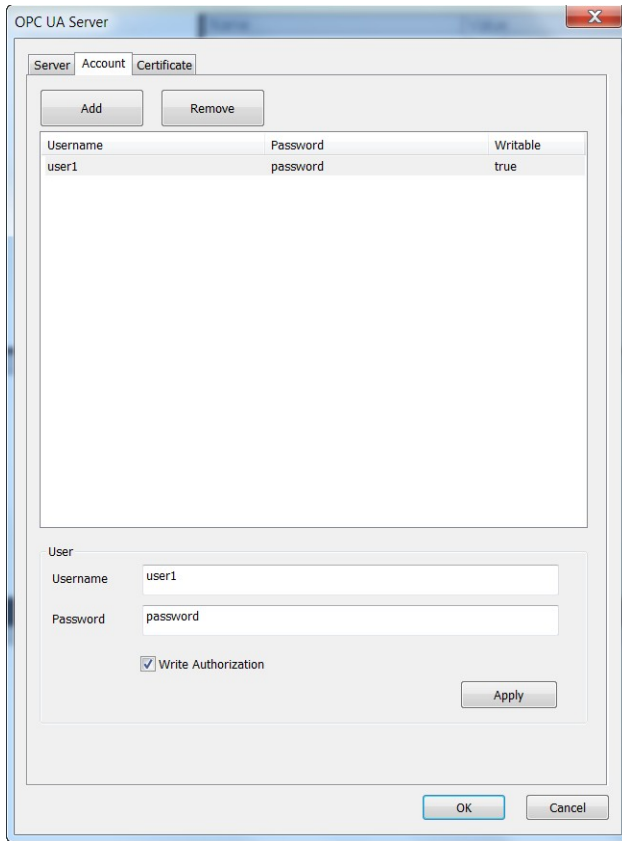
Configure the server as follows:

- Enable 'Use Username and Password' option. The user on the client side always has to enter a password before a session with the server can be started.

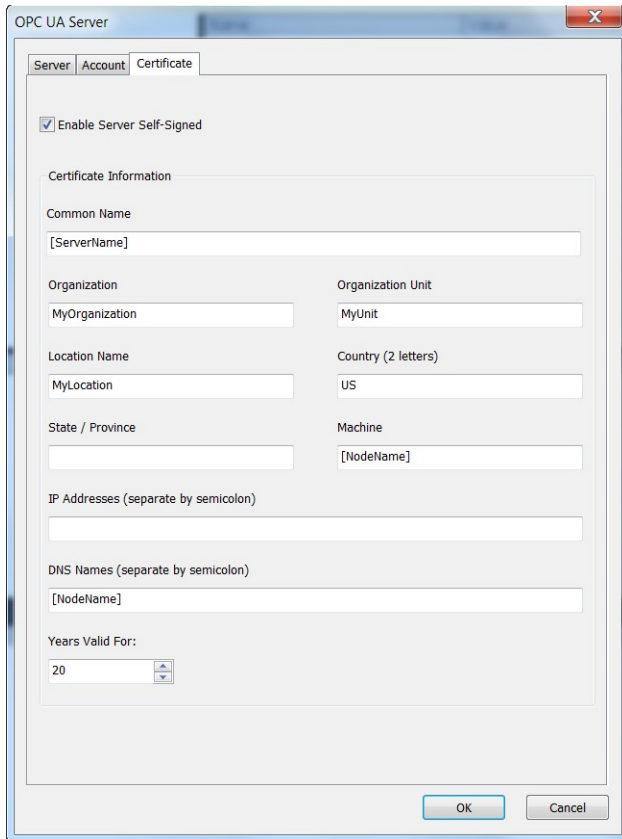


- Add user to login account

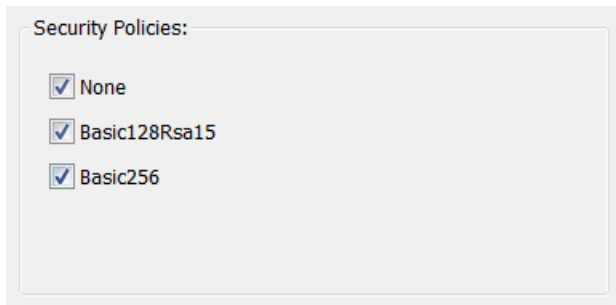




- Enable the self-signed certificate option and fill in the information



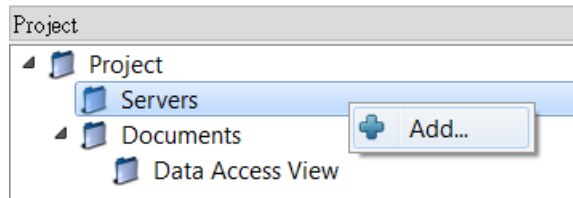
- Select all security policies options.



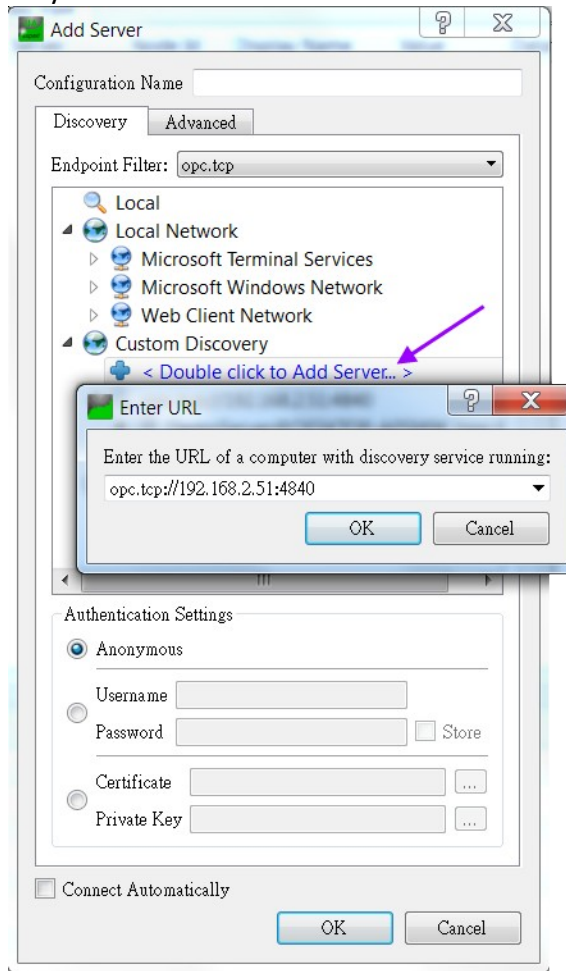
## 4.2.2 UA-Expert Client

Add server to client:

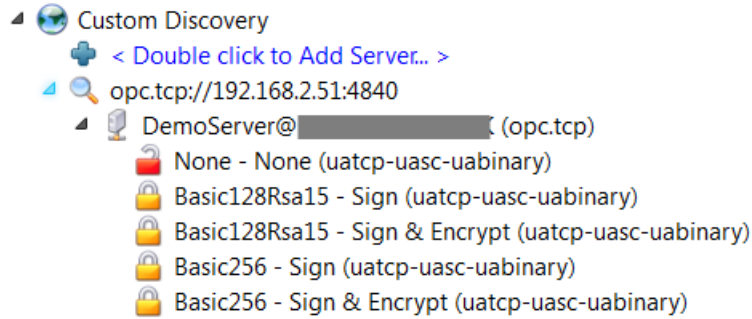
**Step 1:** Right-click on the 'Servers' to add your OPC-UA Server.



**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.



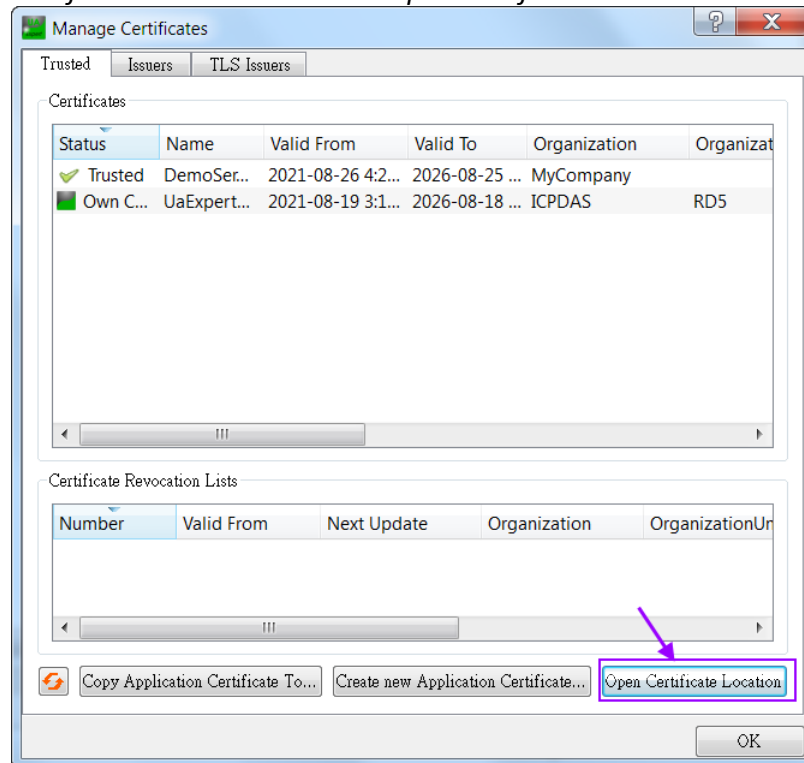
The encryption algorithm supported by the server are listed beneath the server name. The client can select any one of the available encryption options to be used for the server to client communication. Make sure that the client certificate file is in the trusted folder before establishing a connection with a encrypted security policy (not necessary for the 'None' security).



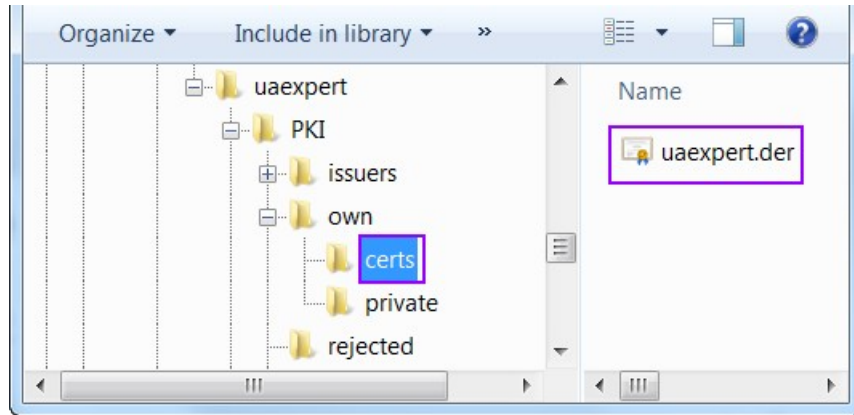
In this demo we select the following option:  
 Double click on the '*Basic256 -Sign&Encryp(uatcp-uasc-uabinary)*' option.

**Step 3:** Copy the client application certificate to the '*\pkiserver\trusted\certs*' of the Win-GRAF runtime folder:

1. Copy the UaExpert client certificate: open the '*Settings / Manage certificates*' and click on the '*Open certificates location*' button

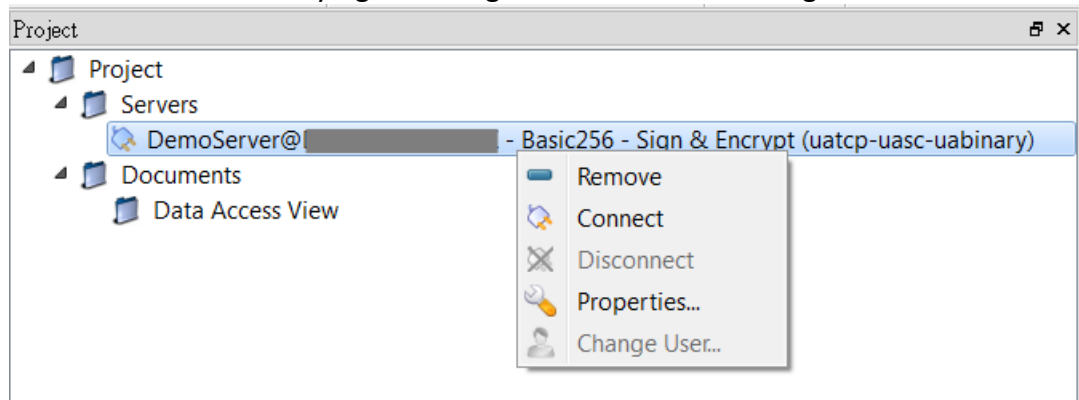


Locate the '*\pkiserver\own\certs*' folder and copy the UaExpert client certificate '*uaexpert.der*'.



2. Paste the client certificate 'uaexpert.der' to the '\pkiserver\trusted\certs' folder of the Win-GRAF runtime.

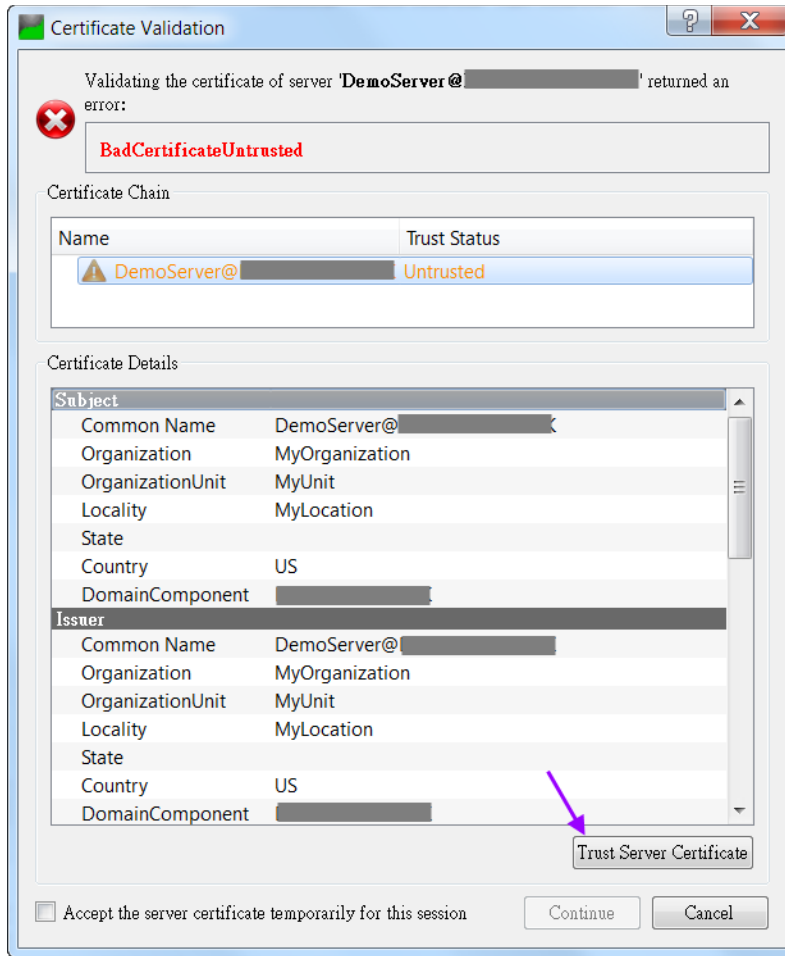
**Step 4:** Connect to the server by right clicking the server and selecting 'Connect'



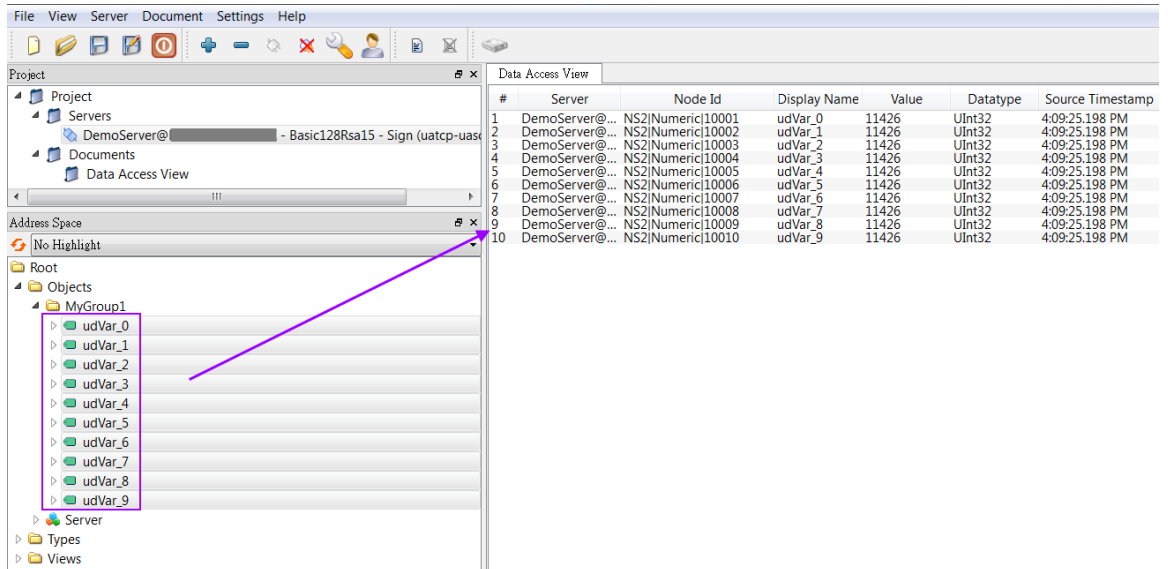
Enter username and password as defined for the login account by the Win-GRAF workbench:



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



**Step 5: View the data values:**

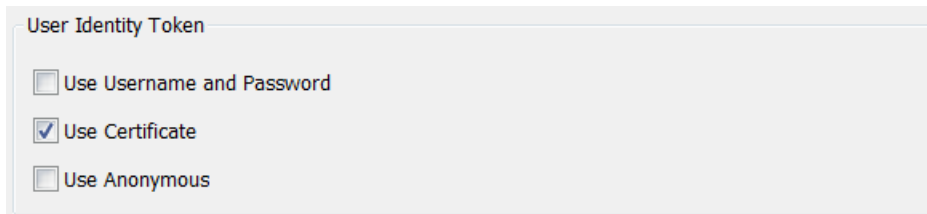


## 4.3 Security Policy and Identity Certificate

### 4.3.1 Win-GRAF server

Configured the server as follows:

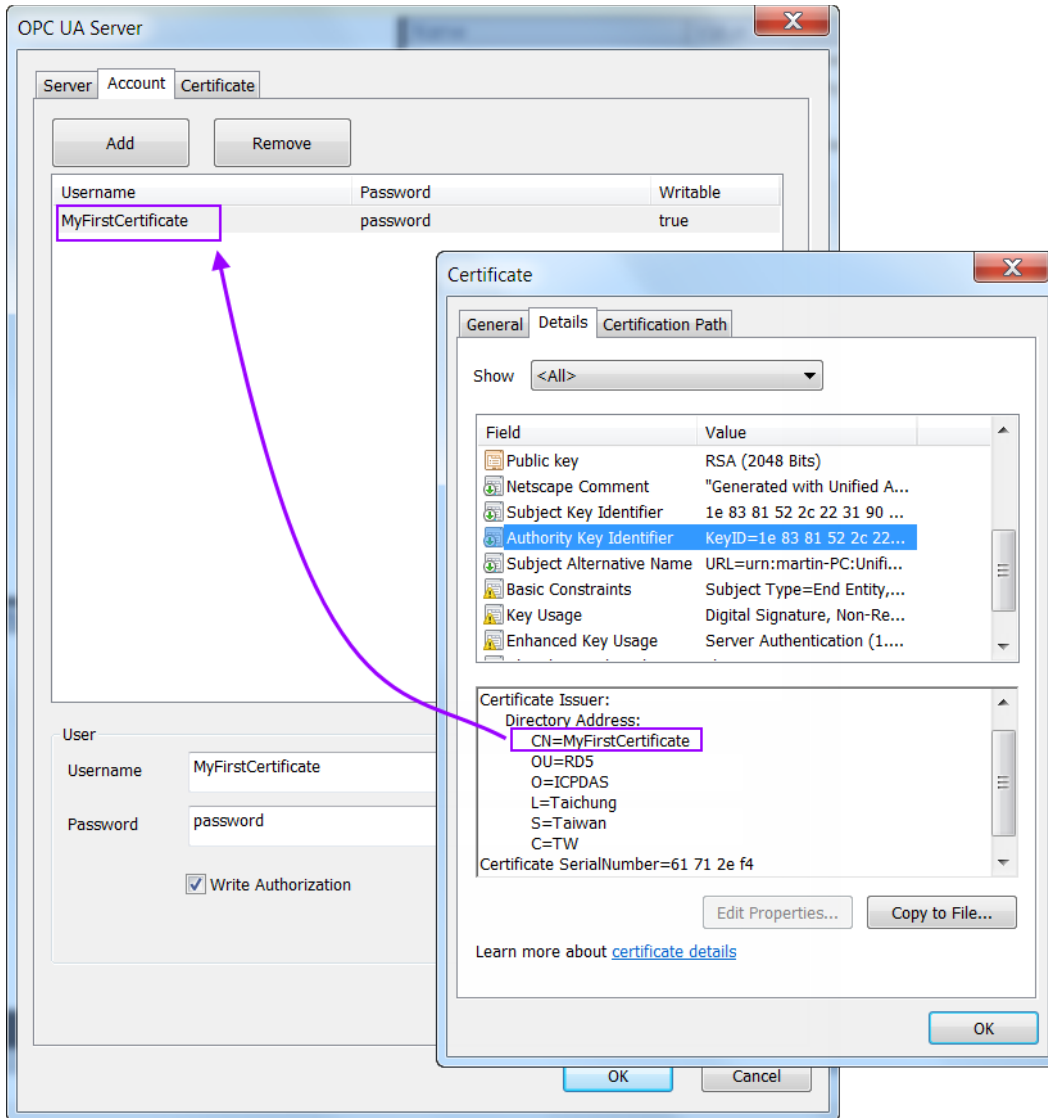
- Enable the X509 identity token. User has to use a X509 certificate to log into the server.



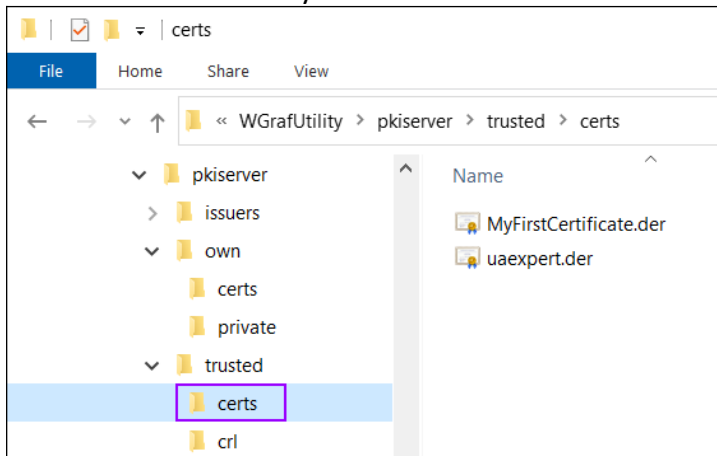
The screenshot shows a dialog box titled "User Identity Token" with three radio button options:

- Use Username and Password
- Use Certificate
- Use Anonymous

- Add the common name of the user certificate to the account list



Copy the user '*MyFirstCertificate.der*' and client '*uaexpert.der*' certificate to the server trusted directory:





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

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 Machine [NodeName]

IP Addresses (separate by semicolon)

DNS Names (separate by semicolon) [NodeName]

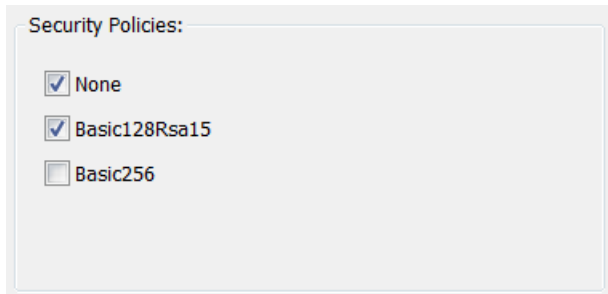
Years Valid For: 20

OK Cancel

**Attention:**

It is important to first delete the existing server certificate before a new certificate with the modified information is created. This action has to be done manually and is not automatically being done by the Win-GRAF runtime. The runtime will only create a new certificate if no certificates exist. Delete the 'own' directory ('\pkiserver\own') to remove both the 'uaserver.der' certificate and its associated 'uaserver.pem' key file.

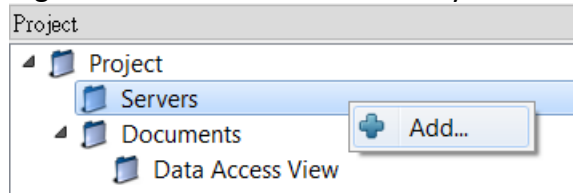
- Select both 'None' and 'Basic128Rsa15' security policies for encrypted communication



### 4.3.2 UA-Expert Client

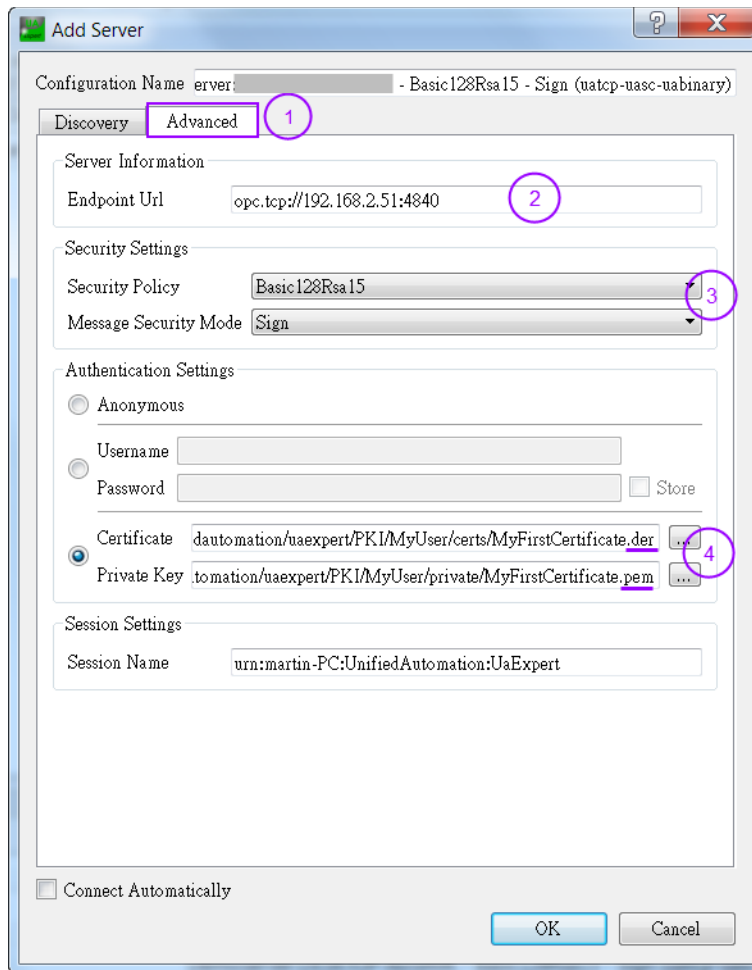
Add server to client:

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

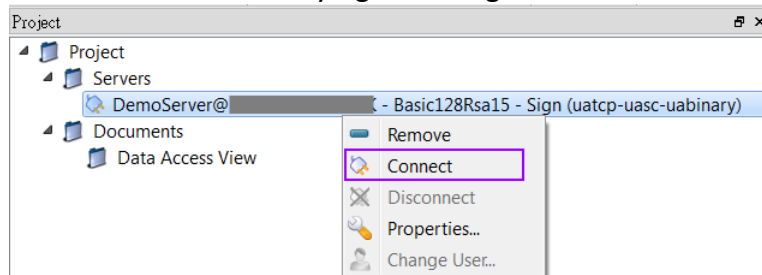


**Step 2:** Set the server endpoint Url and authentication method:

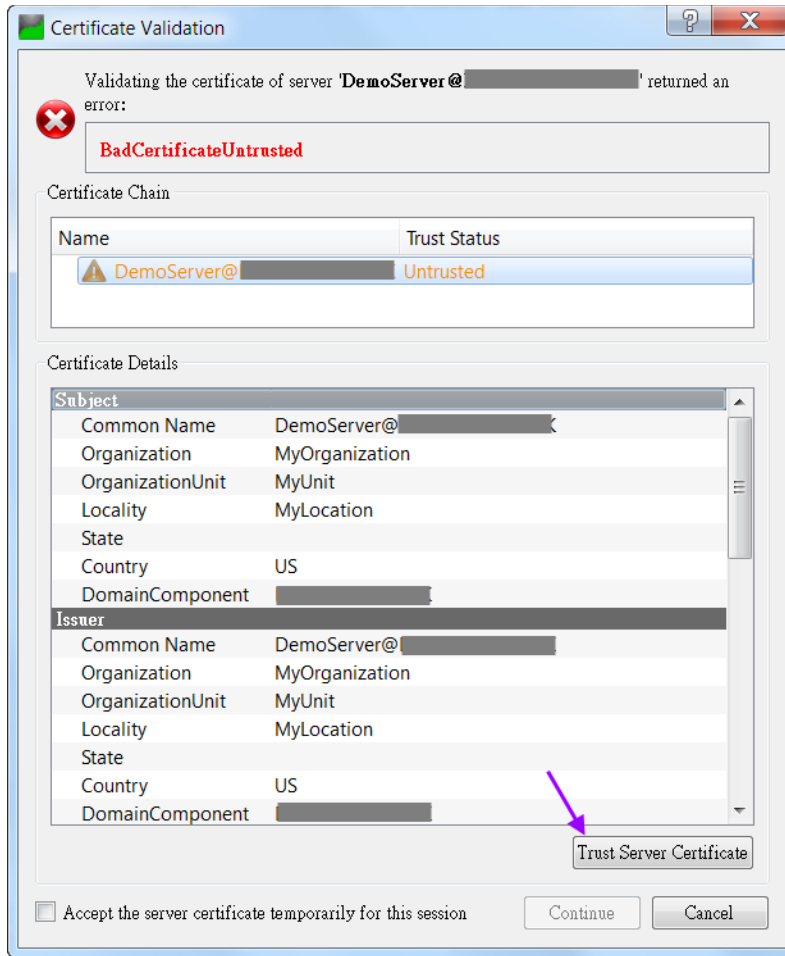
1. Select the '*Advanced*' tab.
2. Enter the server endpoint Url
3. Select the encryption options to be used for the server to client communication. In this example the '*Basic128Rsa15 -Sign(uatcp-uasc-uabinary)*' option is selected.
4. Set the authentication to user certificate and tell the client in which directory to find the user certificate and its private key.



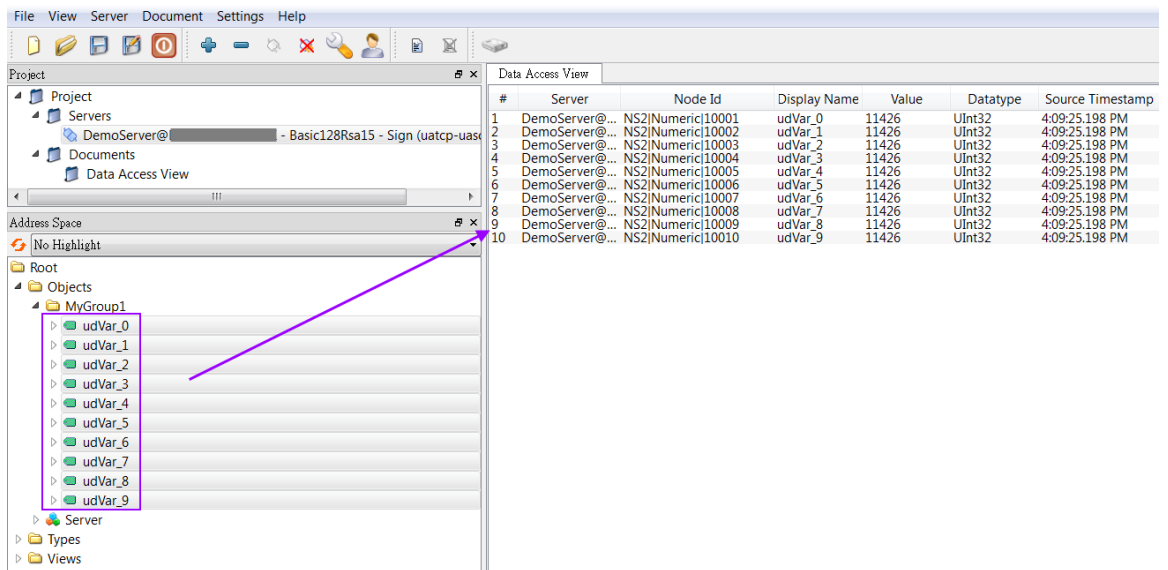
**Step 3:** Connect to the server by right clicking the server and selecting 'Connect'



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



**Step 4: View the data values:**



## 4.4 Subscription Setting

### 4.4.1 Win-GRAF server

The server has been configured as follows:

- Subscription and publishing setting

The screenshot shows a dialog box with two sections: 'Subscription Settings' and 'Publishing Settings'. Each section contains two rows of settings, each with a numeric input field and a unit dropdown menu.

Section	Setting	Value	Unit
Subscription Settings	Maximum Lifetime	10000	Millisecond
	Minimum Lifetime	0	Millisecond
Publishing Settings	Maximum Interval	1000	Millisecond
	Minimum Interval	0	Millisecond

### 4.4.2 UA-Expert Client

#### 4.4.2.1 Subscription Setting

**Step 1:** Select one or more nodes in the 'Data Access View' of the UaExpert and right-click to open the popup menu.

The screenshot shows the 'Data Access View' window with a table of nodes. A context menu is open over the table, and the 'Subscription Settings...' option is highlighted with a purple box.

#	Server	Node Id	Display Name	Value	Datatype
1	DemoServer@...	NS2 Numeric 10001	udVar_0	38779	UInt32
2	DemoServer@...	NS2 Numeric 10002	udVar_1	38779	UInt32
3	DemoServer@...	NS2 Numeric 10003	udVar_2	38779	UInt32
4	DemoServer@...	NS2 Numeric 10004	udVar_3	38779	UInt32
5	DemoServer@...	NS2 Numeric 10005	udVar_4	38779	UInt32
6	DemoServer@...	NS2 Numeric 10006	udVar_5	38779	UInt32
7	DemoServer@...	NS2 Numeric 10007	udVar_6	38779	UInt32
8	DemoServer@...	NS2 Numeric 10008	udVar_7	38779	UInt32
9	DemoServer@...	NS2 Numeric 10009	udVar_8	38779	UInt32
10	DemoServer@...	NS2 Numeric 10010	udVar_9	38779	UInt32

Context Menu Options:

- Remove selected nodes
- Add custom node...
- Subscription Settings...**
- Set Publishing Mode...
- Monitored Item Settings...
- Set Monitoring Mode...

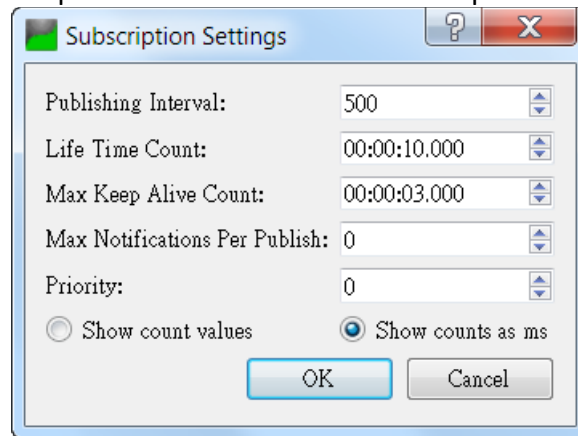
**Step 2:** Set the Publish Interval

- Publish Interval:** The client must ensure that the publishing interval is set to a value equal or greater than the sampling interval of the

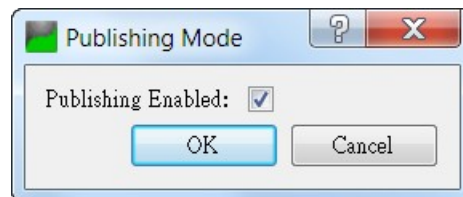
server to enable the server to execute at least one data sampling period, to ensure whenever the 'Publish Interval' elapsed sampled data is available for the client.

In case that there is nothing to report (e.g. no values have changed) the server will send a keep alive notification to the client, to indicate that the server is still alive.

2. **Life Time Count:** Number of 'Publish Interval' in which client must send publish requests to the Server. If the client does not send a request within the period the server will delete the subscription.
3. **Max Keep Alive Count:** If there are no new sampling data available. the server can skip an 'Publish Interval'. In this case the must send a keep alive notification after the keep alive time counter has elapsed.

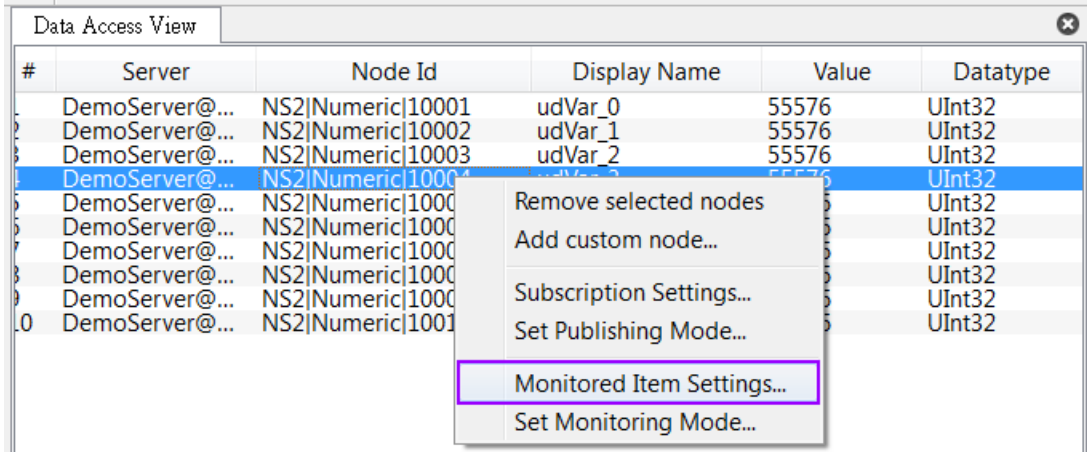


**Step 3:** Enable publish mode by right clicking the node and selecting 'Set Publishing Mode...'



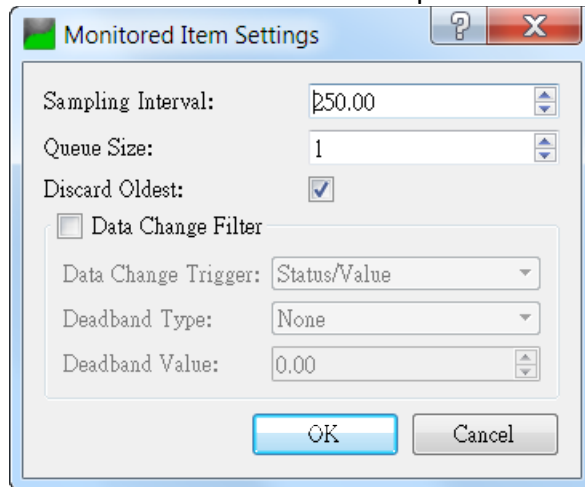
#### 4.4.2.2 Sampling Rate

**Step 1:** Set monitoring interval



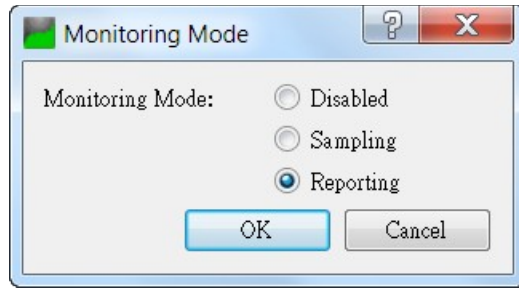
**Step 2:** Set monitored items

1. **Sampling Interval:** This is the rate at which the server scans the PLC data source for changes. The interval should not be set at a faster rate than the cycle time of the PLC task in which the server runs to enable the task to execute and update its variable at least once each period. The sampling can be set at a faster rate than the publishing interval, in which case the server may queue the sampled data and publish the complete queue.
2. **Queue Size:** Set the number sample cycle data the queue can store.
  - Queue size of '1' stores the data collected in one cycle time. If the 'Discard Oldest' has been enabled then the queue contains the information of the last sample.



**Step 3:** Monitoring mode:

1. **Sampling:** subscribe to aggregated values. Sampled values are stored in a queue and sent to the client at each subscription interval.
2. **Reporting:** subscribe to data changes of data source. Enable the 'Data Change Filter' of the previous step and set the 'Data Change Trigger'



## 5 Server Operation Error

Most failures to connect to an OPC UA are because of certificates. It is therefore 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 Trace Log

The OPC UA server does not reported in detail to the PLC application the errors encountered during the start up or operation phase. Instead it creates a trace log file and which contains all the errors with description. The log file is called '*UATrace.log*' and saved in the directory of the runtime execution file '*WinGrafRuntime.exe*'. Its content can be read with any standard text editor.

```

1. UATrace.log
0      10      20      30      40      50      60      70      80      90      100     110     120
1 |** urn:Company:Product:OPCUA_Server: start trace
2 ** Product version: Manufacturer Name Product Name 1.0.0.1
3 ** Date:      2021-10-15
4 **
5 06:15:26.555Z|4|1C5C* ==> UaServerApplication::start
6 06:15:26.555Z|1|1C5C* [uastack] OpcUa_P_ParseUrl: Hostname detected!
7 06:15:26.555Z|1|1C5C* [uastack] OpcUa_P_ParseUrl: Allowing connections to any ip!
8 06:15:26.555Z|1|1C5C* [uastack] OpcUa_P_ParseUrl: Trying to resolve host " " port "4840" to address family 0.
9 06:15:26.555Z|1|297C* [uastack] NetworkThread: Message Loop started...
10 06:15:26.555Z|1|1C5C* [uastack] OpcUa_P_ParseUrl: 0: Resolved to IPv6 address family.
11 06:15:26.555Z|1|1C5C* [uastack] OpcUa_P_ParseUrl: 0: Numeric representation of resolved address is :.
12 06:15:26.571Z|1|1C5C* [uastack] OpcUa_P_ParseUrl: 1: Resolved to IPv4 address family.
13 06:15:26.571Z|1|1C5C* [uastack] OpcUa_P_ParseUrl: 1: Numeric representation of resolved address is 0.0.0.0.
14 06:15:26.571Z|1|1C5C* [uastack] OpcUa_P_RawSocket_Create: Dual protocol stack enabled.
15 06:15:26.571Z|1|1C5C* [uastack] OpcUa_P_Socket_Delete: Closing socket 0x06279400!
16 06:15:26.571Z|1|1C5C* [uastack] OpcUa_SecureListener_OnNotify: Transport Open
17 06:15:26.571Z|1|1C5C* [uastack] OpcUa_Endpoint_OnNotify: Underlying listener raised open event!
18 06:15:36.553Z|1|2F38* [uastack] OpcUa_SecureListener_ChannelManager_TimerCallback: Checking Channels for lifetime expiration!
19 06:15:46.566Z|1|2F38* [uastack] OpcUa_SecureListener_ChannelManager_TimerCallback: Checking Channels for lifetime expiration!
20 06:15:56.595Z|1|2F38* [uastack] OpcUa_SecureListener_ChannelManager_TimerCallback: Checking Channels for lifetime expiration!
  
```

Figure 14: UATrace.log file



## 5.1.1 Server Failed to Create Endpoints

If the server does not find any server certificate in the directory '*pkiserver/own/certs*' and any private key in the directory '*pkiserver/own/private*' then no endpoints will be created (Figure 15). This means the client will not be able to connect and return with a connection timeout.

```
UATrace.log - Notepad
File Edit Format View Help
** urn:Company:Product:OPCUA_Server: start trace
** Product version: Manufacturer Name Product Name 1.0.0.1
** Date: 2021-10-19
**
09:25:25.988Z|411418* ==> UaServerApplication::start
09:25:25.992Z|111418* Error: UaServer::startUp [ret=OpcUa_BadConfigurationException] - No Endpoints configured
09:25:25.993Z|111418* <=< UaServerApplication::start - afterStartUp() failed on derived class [status=0x80020000]
```

Figure 15: No Endpoints configured

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 16. To force the server to generate a new certificate remove all files, certificate and private key file, from both directories: '*pkiserver/own/certs*' and '*pkiserver/own/private*'.

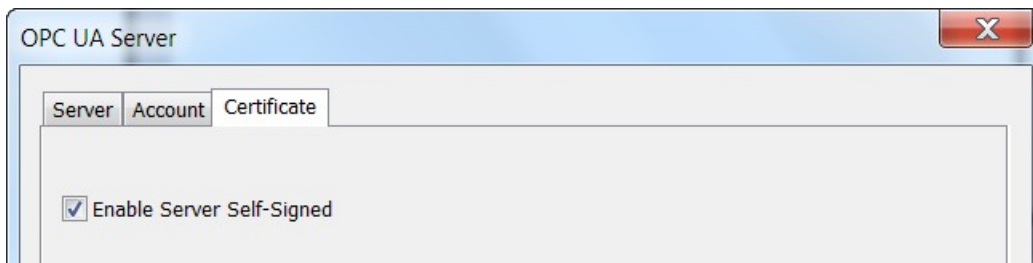


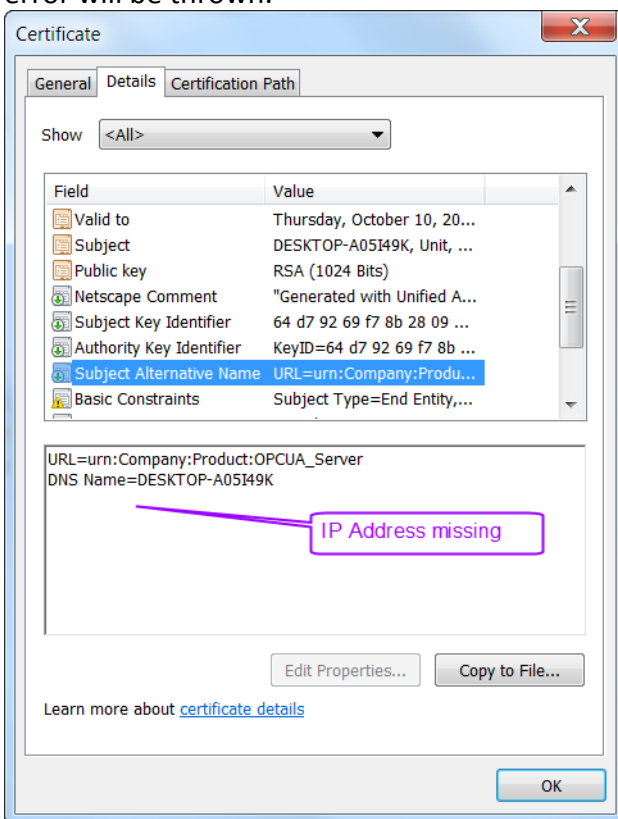
Figure 16: Create a 'Self-assigned' certificate

## 5.2 Communication Error Message

### 5.2.1 BadCertificateHostNameInvalid



The error refers to the SubjectAlternativeName extension, which shall contain the server's hostname(s) and/or IP addresses. If you connect to the server using its IP address and the certificate only contains the hostname (or the other way round), 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  
Organization

Organization Unit  
Unit

Location Name  
Location Name

Country (2 letters)  
US

State / Province

Machine  
[NodeName]

IP Addresses (separate by semicolon)  
192.168.2.51

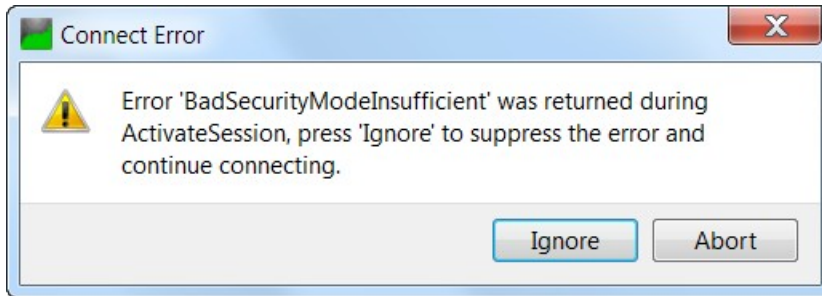
DNS Names (separate by semicolon)  
[NodeName]

Years Valid For:  
20

OK Cancel

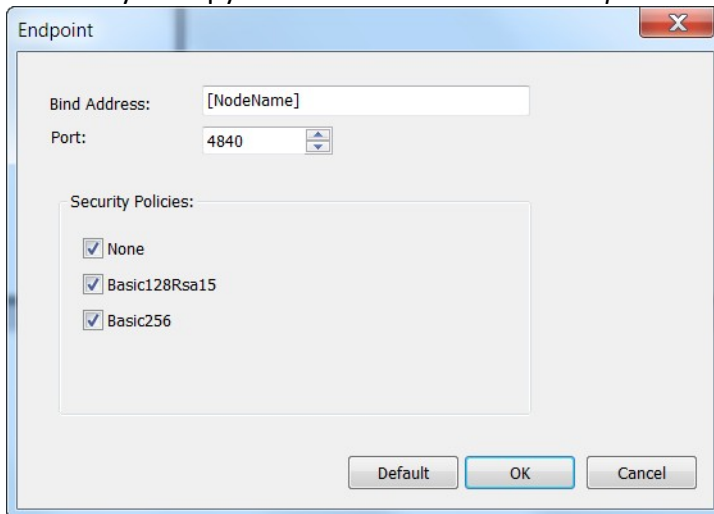
## 5.2.2 BadSecurityModeInsufficient

This error means that the client tries to establish a *'none'* encrypted communication by logging into the server. In *'none'* security mode the *'UserName'* and *'Password'* is send to as a clear text over the wire which poses a great security threat.



Solution:

Select the *'Basic128Rsa15'* or *'Basic256'* to policy to encrypt the password. It is also necessary to copy the client certificate to the *'pkiserver/trusted/certs'* server 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 '*pkiserver/trusted/certs*' directory.

Solution:

Copy the client certificate to the '*pkiserver/trusted/certs*' directory.

---

## 6 Appendix

---

### 6.1.1 Combination of User Identity, Self-Assigned Certificate and Security Policies

User Identity Token	Self-assigned	Security Policies Option	Description
Use Anonymous	Disabled	None	<ul style="list-style-type: none"><li>• The certificate and private key files have to be added manually to the corresponding directory '<i>pkiserver/own/certs</i>' and '<i>pkiserver/own/private</i>'</li><li>• If no certificate and key file exists then<ul style="list-style-type: none"><li>- Client can not connect to server</li><li>- No endpoints are configured</li></ul></li></ul>
		Basic128Rsa15	
		Basic256	
Use Anonymous	Enabled	None	<ul style="list-style-type: none"><li>• Server does <u>not</u> require the client certificate file in the directory '<i>pkiserver/trusted/certs</i>'</li><li>• Client setting:<ul style="list-style-type: none"><li>- Security Setting:<ul style="list-style-type: none"><li>- Security Policy: None</li><li>- Message Security Mode: None</li></ul></li><li>- Authentication Settings:<ul style="list-style-type: none"><li>- Anonymous</li></ul></li></ul></li></ul>
		Basic128Rsa15	<ul style="list-style-type: none"><li>• Client certificate needs to be added to the server directory '<i>pkiserver/trusted/certs</i>'.</li></ul>

User Identity Token	Self-assigned	Security Policies Option	Description
			<ul style="list-style-type: none"> <li>Client setting: <ul style="list-style-type: none"> <li>Security Setting: <ul style="list-style-type: none"> <li>Security Policy: Basic128Rsa15</li> <li>Message Security Mode: Sign &amp; Encrypt</li> </ul> </li> <li>Authentication Settings: <ul style="list-style-type: none"> <li>Anonymous</li> </ul> </li> </ul> </li> </ul>
		Basic256	<ul style="list-style-type: none"> <li>Client certificate needs to be added to the server directory '<i>pkiserver/trusted/certs</i>'.</li> <li>Client setting: <ul style="list-style-type: none"> <li>Security Setting: <ul style="list-style-type: none"> <li>Security Policy: Basic256</li> <li>Message Security Mode: Sign &amp; Encrypt</li> </ul> </li> <li>Authentication Settings: <ul style="list-style-type: none"> <li>Anonymous</li> </ul> </li> </ul> </li> </ul>
Use Certificate	Disabled	None	<ul style="list-style-type: none"> <li>The certificate and private key files have to be added manually to the corresponding directory '<i>pkiserver/own/certs</i>' and '<i>pkiserver/own/private</i>'</li> <li>If no certificate and key file exists then <ul style="list-style-type: none"> <li>Client can not connect to server</li> <li>No endpoints are configured</li> </ul> </li> </ul>
		Basic128Rsa15	
		Basic256	
	Enabled	None	<ul style="list-style-type: none"> <li>Copy the user certificate to the server trusted directory '<i>pkiserver/trusted/certs</i>' and add the common name to the account list</li> <li>Server does <u>not</u> require the client certificate file in the directory '<i>pkiserver/trusted/certs</i>'</li> <li>Client setting: <ul style="list-style-type: none"> <li>Security Setting: <ul style="list-style-type: none"> <li>Security Policy: None</li> <li>Message Security Mode: None</li> </ul> </li> <li>Authentication Settings: <ul style="list-style-type: none"> <li>Certificate: user certificate file</li> <li>Private key: user private key file</li> </ul> </li> </ul> </li> </ul>
	Basic128Rsa15	<ul style="list-style-type: none"> <li>Copy the user certificate to the server trusted directory '<i>pkiserver/trusted/certs</i>' and add the common name to the account list</li> <li>Client certificate needs to be added to the server directory '<i>pkiserver/trusted/certs</i>'.</li> <li>Client setting: <ul style="list-style-type: none"> <li>Security Setting: <ul style="list-style-type: none"> <li>Security Policy: Basic128Rsa15</li> <li>Message Security Mode: Sign &amp; Encrypt</li> </ul> </li> <li>Authentication Settings:</li> </ul> </li> </ul>	

User Identity Token	Self-assigned	Security Policies Option	Description
			<ul style="list-style-type: none"> <li>- Certificate: user certificate file</li> <li>- Private key: user private key file</li> </ul>
		Basic256	<ul style="list-style-type: none"> <li>• Copy the user certificate to the server trusted directory '<i>pkiserver/trusted/certs</i>' and add the common name to the account list</li> <li>• Client certificate needs to be added to the server directory '<i>pkiserver/trusted/certs</i>'.</li> <li>• Client setting: <ul style="list-style-type: none"> <li>- Security Setting: <ul style="list-style-type: none"> <li>- Security Policy: Basic256</li> <li>- Message Security Mode: Sign &amp; Encrypt</li> </ul> </li> <li>- Authentication Settings: <ul style="list-style-type: none"> <li>- Certificate: user certificate file</li> <li>- Private key: user private key file</li> </ul> </li> </ul> </li> </ul>
Use Username and Password	Disabled	None	<ul style="list-style-type: none"> <li>• The certificate and private key files have to be added manually to the corresponding directory '<i>pkiserver/own/certs</i>' and '<i>pkiserver/own/private</i>'</li> <li>• If no certificate and key file exists then <ul style="list-style-type: none"> <li>- Client can not connect to server</li> <li>- No endpoints are configured</li> </ul> </li> </ul>
		Basic128Rsa15	
		Basic256	
	Enabled	None	<ul style="list-style-type: none"> <li>• Server does <u>not</u> require the client certificate file in the directory '<i>pkiserver/trusted/certs</i>'</li> <li>• Add username and password to the server account list</li> <li>• Client setting: <ul style="list-style-type: none"> <li>- Security Setting: <ul style="list-style-type: none"> <li>- Security Policy: None</li> <li>- Message Security Mode: None</li> </ul> </li> <li>- Authentication Settings: <ul style="list-style-type: none"> <li>- Username:</li> <li>- Password:</li> </ul> </li> </ul> </li> </ul>
		Basic128Rsa15	<ul style="list-style-type: none"> <li>• Client certificate needs to be added to the server directory '<i>pkiserver/trusted/certs</i>'.</li> <li>• Add username and password to the server account list</li> <li>• Client setting: <ul style="list-style-type: none"> <li>- Security Setting: <ul style="list-style-type: none"> <li>- Security Policy: Basic128Rsa15</li> <li>- Message Security Mode: Sign &amp; Encrypt</li> </ul> </li> <li>- Authentication Settings: <ul style="list-style-type: none"> <li>- Username:</li> <li>- Password:</li> </ul> </li> </ul> </li> </ul>

User Identity Token	Self-assigned	Security Policies Option	Description
		Basic256	<ul style="list-style-type: none"> <li>• Client certificate needs to be added to the server directory '<i>pkiserver/trusted/certs</i>'.</li> <li>• Add username and password to the server account list</li> <li>• Client setting: <ul style="list-style-type: none"> <li>- Security Setting: <ul style="list-style-type: none"> <li>- Security Policy: Basic256</li> <li>- Message Security Mode: Sign &amp; Encrypt</li> </ul> </li> <li>- Authentication Settings: <ul style="list-style-type: none"> <li>- Username:</li> <li>- Password:</li> </ul> </li> </ul> </li> </ul>

## 6.1.2 Supported Features

As part of the standard (OPC UA Part 7), the OPC UA Server will support features (Table 13):

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
	Cancel	No
NodeManagment	Add node	No
	Add reference	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	Yes
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 13: Supported OPC UA server features**

Server limitations are :

- Maximum number of parallel sessions: 100
- Maximum number of subscriptions per session: 100
- Maximum number of MonitoredItem per subscription: 65535
- Maximum number of Publish Request per session: 100
- Maximum DataChangeValue per MonitoredItem: 100
- Allowed number of security policies: 16

### 6.1.3 Default Settings

Property	Default	Description
maxRequestAge	0	
maxSessionCount		User Setting
maxSessionsPerClient	0	
minSessionTimeout		User Setting
maxSessionTimeout		User Setting
maxBrowseContinuationPoints	0	
maxBrowseResults	0	
iMaxNodesPerHistoryReadData	0	
iMaxNodesPerHistoryReadEvents	0	
iMaxNodesPerHistoryUpdateData	0	
iMaxNodesPerHistoryUpdateEvents	0	
maxHistoryContinuationPoints	0	
minPublishingInterval		User Setting
maxPublishingInterval		User Setting
minKeepAliveInterval		User Setting
minSubscriptionLifetime		User Setting
maxSubscriptionLifetime		User Setting
maxRetransmissionQueueSize	10	
maxNotificationsPerPublish	0	

maxSubscriptionCount	0	
maxSubscriptionsPerSession	0	
maxMonitoredItemCount	0	
maxMonitoredItemPerSubscriptionCount	0	
maxMonitoredItemPerSessionCount	0	
iMaxDataQueueSize	100	
iMaxEventQueueSize	1000	
minSupportedSampleRate	0	
availableSamplingRates[0]	50	
availableSamplingRates[1]	100	
availableSamplingRates[2]	250	
availableSamplingRates[3]	500	
availableSamplingRates[4]	1000	
availableSamplingRates[5]	2000	
availableSamplingRates[6]	5000	
availableSamplingRates[7]	10000	
sProductUri		User Setting
sManufacturerName		User Setting
sProductName		User Setting
sSoftwareVersion	1.0.0	
sBuildNumber	1	
sServerUri		User Setting
sServerName		User Setting
bEnableAnonymous		User Setting
bEnableUserPw		User Setting
bEnableCertificate	FALSE	User Setting
bEnableKerberosTicket	FALSE	
Default SDK thread pool settings		
minSizeTransactionManager	1	
maxSizeTransactionManager	10	
minSizeSubscriptionManager	1	
minSizeSubscriptionManager	10	
Default UA Stack thread pool settings		
bStackThreadPoolEnabled	FALSE	
iMinStackThreads	5	
iMaxStackThreads	5	
iMaxStackThreadJobs	20	
bStackThreadBlockOnAdd	TRUE	
nStackThreadTimeout	OPCUA_INFINITE	
nRejectedCertificatesCount	100	
Discover server registration settings		
nRegistrationInterval	30000	

bAutomaticCertificateExchange	FALSE	User has to manually copy the client certificate to the trusted directory
<b>Trace Setting</b>		
bTraceEnabled	TRUE	
uTraceLevel	0xFFFFFFFF	
bSdkTraceEnabled	TRUE	
uSdkTraceLevel	Errors	Only errors messages are written to the trace file
uMaxTraceEntries	100000	
uMaxBackupFiles	2	
sTraceFile	'UATrace.log'	
uTraceEventLevel	1	History
<b>isAuditActivated</b>		
isAuditActivated	FALSE	
redundancySupport	None	
m_uaEndpointArray[0]	1	