New Features in ibaLogic v5.1.0

Author: iba AG Fürth

Date: 20/01/2017

Content

1 OPC UA

OPC UA is the new standard of the OPC Foundation. It allows a simpler and faster connection than the older OPC DA standard.

IbaLogic provides an OPC UA server. Thus, data with an OPC UA client, e.g. IbaPDA are exchanged.

OPC UA data can be transmitted encrypted, but will always be signed (= sender recognition).

For the security (signing) so-called certificates are used. These are encrypted security files that are exchanged between the server and the client to allow data traffic.

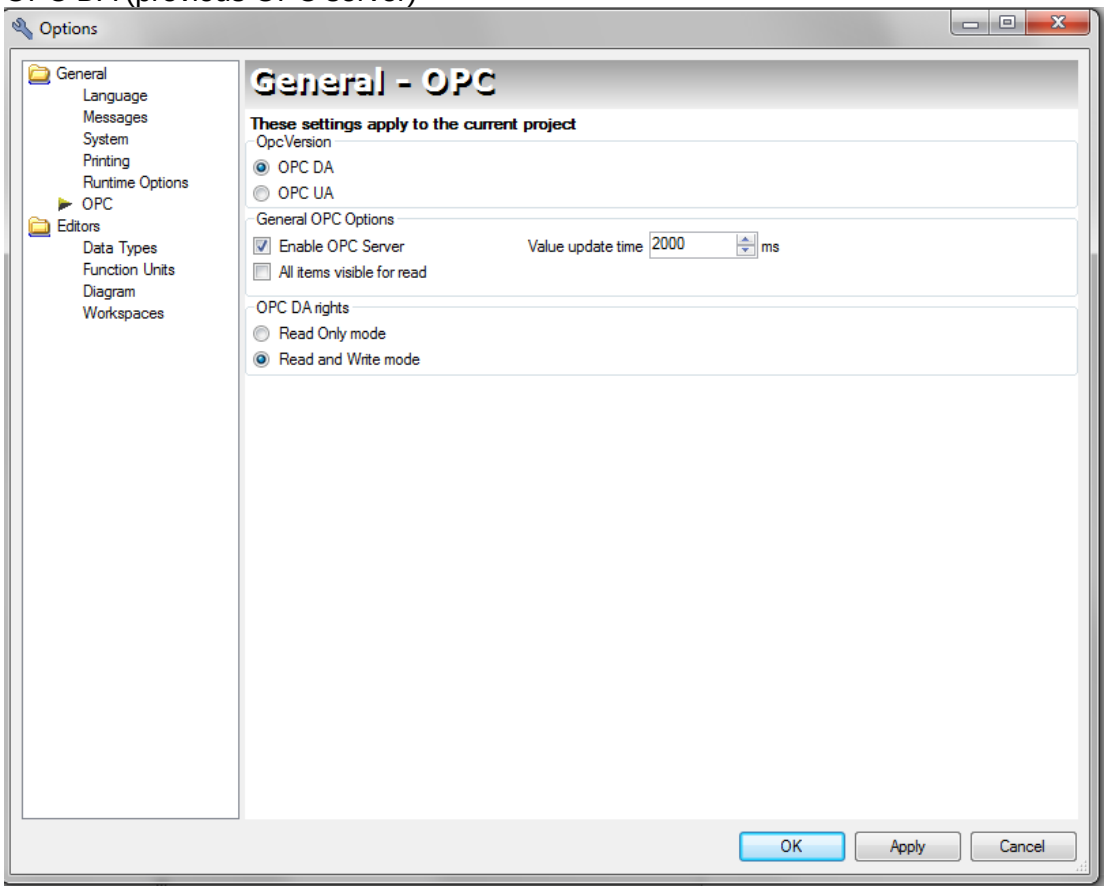
In addition to this signature, the transmitted data can then also be encrypted by various methods.

1.1 Selection between OPC UA and OPC DA Server

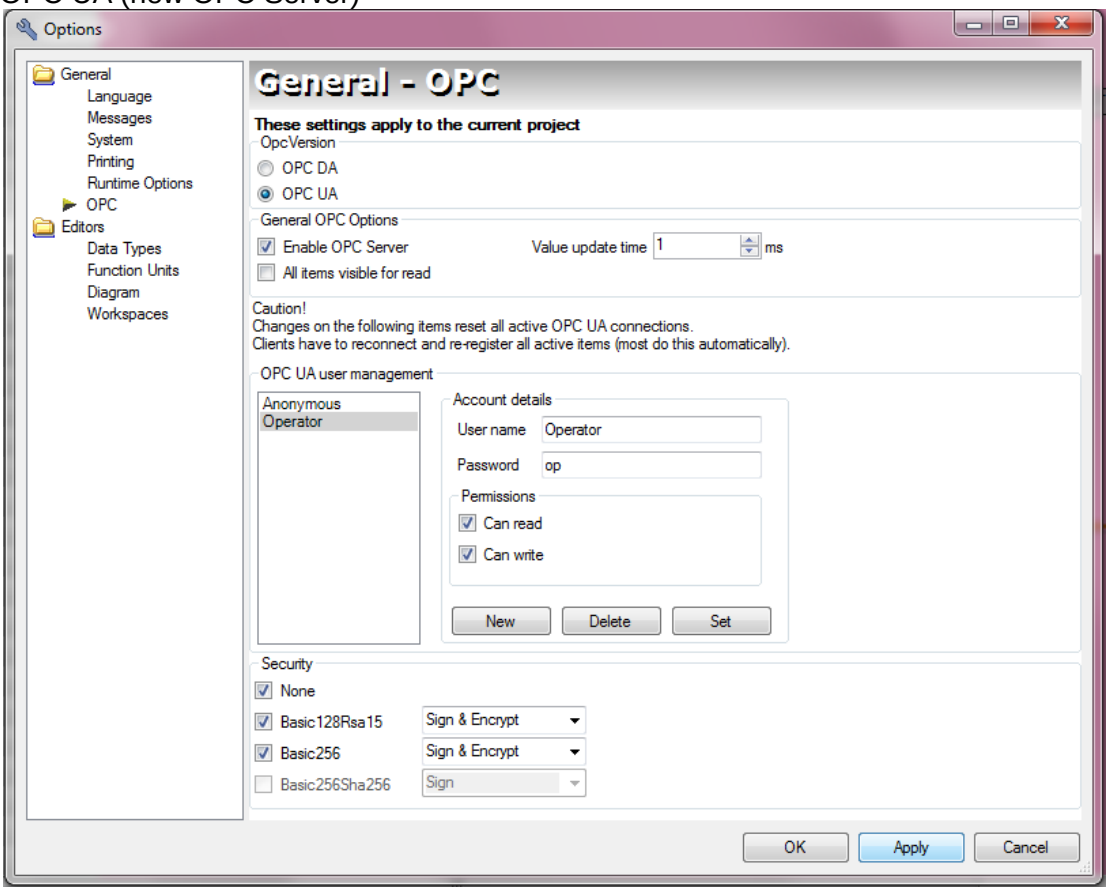
It is possible to choose between the previous OPC-DA servers and the new OPC-UA server.
It is either one or the other selectable. Both are not available in parallel.

The selection is made via the menu CONFIGURATION-> OPTIONS -> OPC

OPC DA (previous OPC server)



OPC UA (new OPC Server)



Enable OPC Server: Enable OPC UA

All items visible for read: Not only the OTCs marked as available for OPC, but all internal variables, e.g. all inputs and outputs of a block and also internal variables of the block.

Value Update Time: 20ms…x ms Transfer time of the data. 20ms is the fastest transfer rate (depends also on the amount of data)

OPC UA user management

Any user can be created for the OPC UA connection and their rights can be set.

Anonymous is a standard user without a password.

Permissions

Can browse: Browsing is allowed. Than means a client can read out all the OPC variables that have been created in order to make them available to the user as a selection..

Can read: Read access to the OPC data

Can write: Write access to the OPC data

New/Delete/Set: Create / delete a user and apply the changes

Security: Security - Settings

OPC UA has different security settings. The OPC UA server (here: ibaLogic) specifies which types of security settings are allowed for a connection. Only these types can then used by an OPC UA client for a connection.

There are the security guidelines and the message security mode:

Security guidelines are:

- **None** no security guidelines
- **Basic128Rsa15** 128 is the bit width of the encryption and RSA15 is the encryption method used (with certificates). (RSA = Rivest, Shamir, Adleman)
- **Basic256** Encryption on a bit-width of 256 (without certificates)
- *Basic256Sha256* (Not yet implemented) 256 is the bit width of the encryption and SHA256 is the encryption method (with certificates) (SHA = Secure Hash Algorithm)

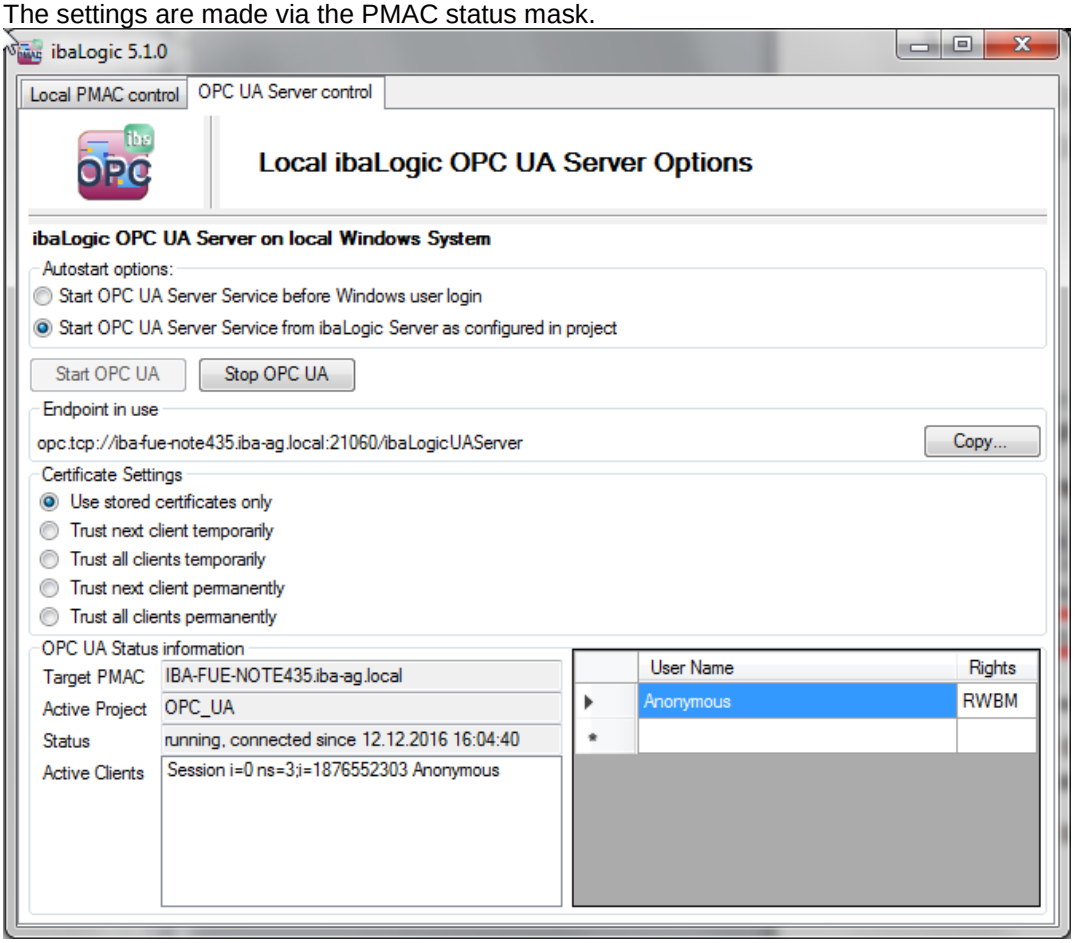
Message-SecurityMode: (Depending on selected safety guidelines)

- **None** nothing
- **Sign** The message transmission is signed so that the sender is clear
- **Sign&Encrypt** The message is encrypted in addition to "Sign".
- **Sign,Sign&Encrypt**: allows all encryption, so only "Sign" as also "Sign&Encrypt”.

1.2 OPC UA Server

The OPC UA server in ibaLogic is available as a service.

The settings are made via the PMAC status mask.



Autostart Options: Set when to start the service

Manual Start/Stop:

Endpoint in use:

The OPC UA endpoint is displayed. This endpoint is important for the connection to the OPC UA client.

The end point can easily copy to the clipboard (COPY) and can easily be inserted into the OPC UA client.

Example: opc.tcp://iba-fue-note435.iba-ag.local:21060/ibaLogicUAServer

Ceritficate Settings:

(See below: exchange of certificates)

OPC UA Status Information:

Display of connected OPC UA clients with users.

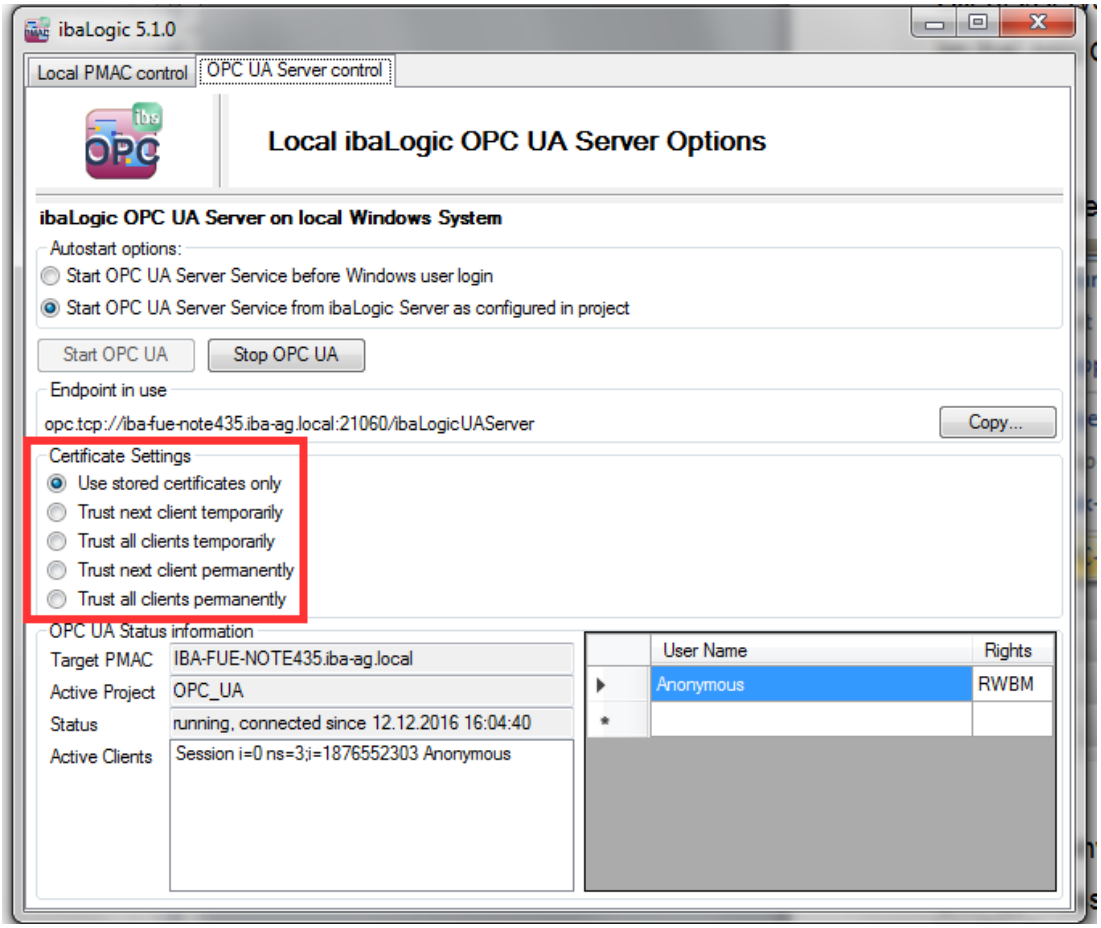
1.3 Exchange of certificates

Since secure OPC UA connections only work via certificates, they must be exchanged.

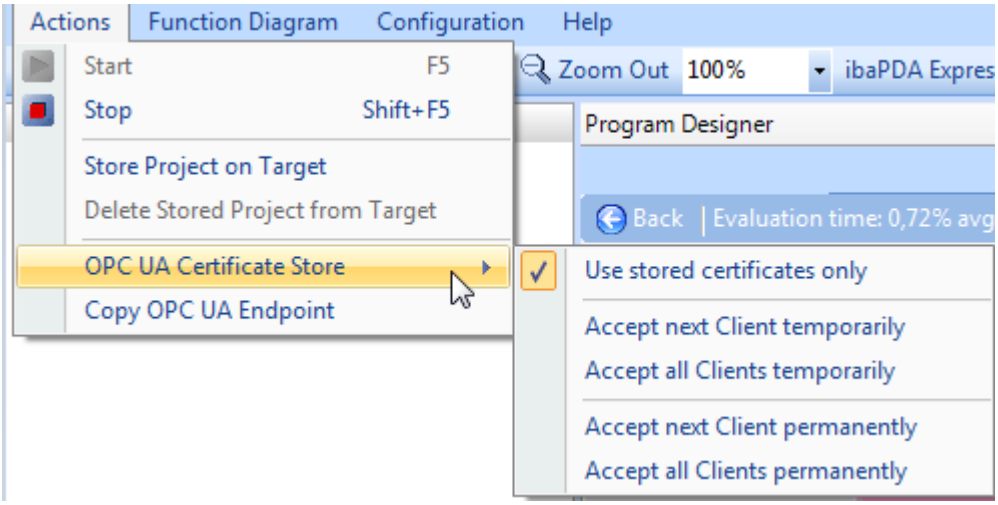
For this purpose, each OPC UA server and OPC UA client has a directory for placing its own certificate and that of its connection partners so that a connection can be made securely.

This exchange of the certificates can be done manually by copying. Most OPC UA clients / servers also offer an automated option.

In the ibaLogic PMAC Control and also directly in the ibaLogic Client you have the following selection:



ibaLogic Client



That is, that the necessary certificates have to exist on both sides, otherwise no connection to the state will occur.

If you now want to connect an OPC UA client to ibaLogic, you must select one of the following 4 options **before** making a connection setup from an OPC UA client.

Trust next one temporarily: When an OPC UA client attempts to establish a connection to the ibaLogic OPC UA server, its certificate is classified as "safe" and stored with the ibaLogic OPC UA server. Afterwards, the selection automatically reverts to "Do not trust". However, as soon as you close this OPC connection, these certificates are deleted again.

Trust ALL temporarily: : All attempts made by one or more OPC UA clients to establish a connection to the ibaLogic OPC UA server is classified as "safe" and its certificates are stored with the ibaLogic OPC UA server. However, as soon as you close this OPC connection, these certificates are deleted again.

Trust next one PERMANENTLY: When an OPC UA client attempts to establish a connection to the ibaLogic OPC UA server, its certificate is classified as "safe" and stored with the ibaLogic OPC UA server. Afterwards, the selection automatically reverts to "Do not trust". This connection can then be set up again and again without the need for any further certificates to be exchanged.

Trust ALL PERMANENTLY: All attempts made by one or more OPC UA clients to establish a connection to the ibaLogic OPC UA server are classified as "safe" and their certifications are stored with the ibaLogic OPC UA Server. The certificates are retained even when the connection is disconnected.

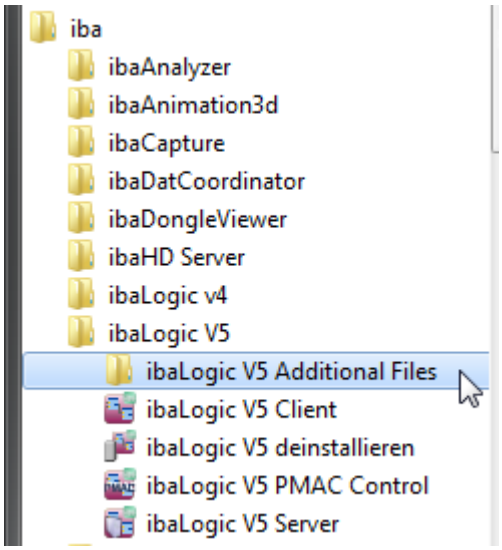
! Make sure that a **TRUST ALL PERMANENTLY** setting can also be a security risk, as all incoming connections are running during the ibaLogic OPC UA server, are automatically classified as secure, and a permanent certificate for each of these incoming connections is stored. This allows these clients to connect without problems after restarting. This mode should therefore only be used for test purposes!

1.4 Certificate storage and control

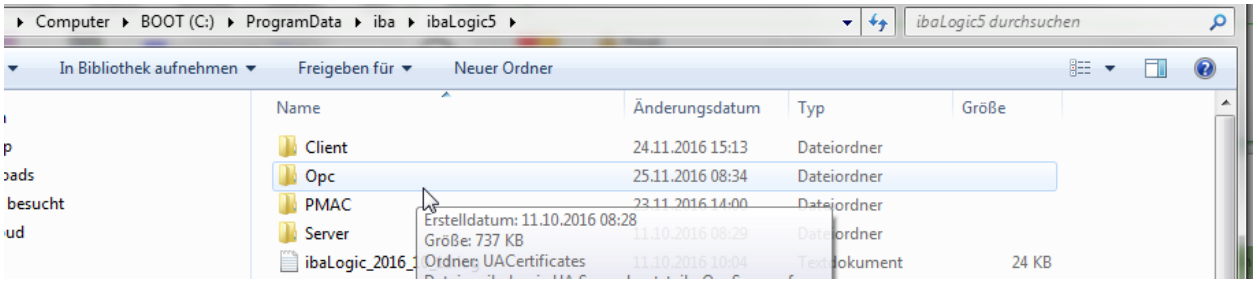
IbaLogic stores all certificates in a separate folder.

This can be found as follows:

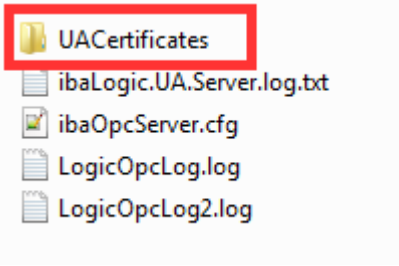
Über START-ALL PROGRAMS-IBA- ibaLogic V5 Additional Files

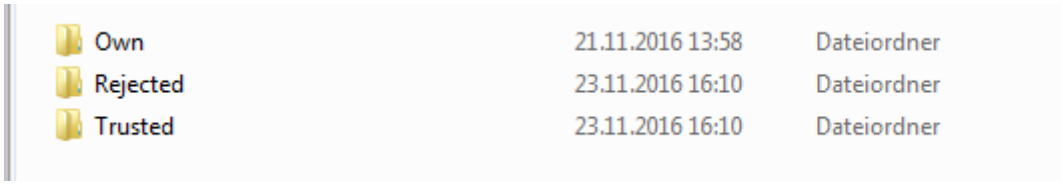


Go to this directory and select OPC



Select the UACertificates





Here you can find now

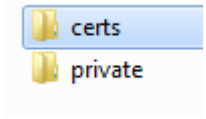
Own: own certificates from ibaLogic

Rejected: rejected certificates of unauthorized connections.

Trusted: allowed and accepted certificates

If you delete these folders, all OPC UA connections are no longer valid.

Under OWN, there are the subfolders

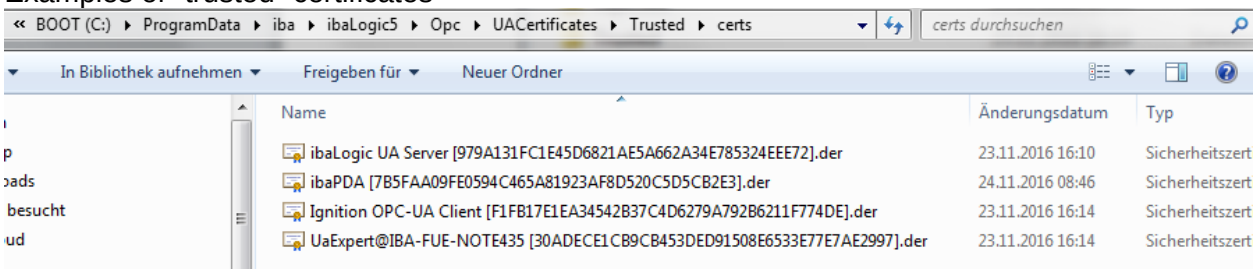


There is always a private and a public certificate for OPC UA. The private can not be passed on. The public (here, under CERTS) is that which is sent to the opponent, so that a connection can be established if it accepts the opposing.

You can also copy this certificate simply at the opposing place into the appropriate "Trusted" directory and thus it is also a permitted connection.

And also you can enter an originally rejected connection (see the folder Rejected) by moving to the Trusted folder as a valid connection.

Examples of "trusted" certificates

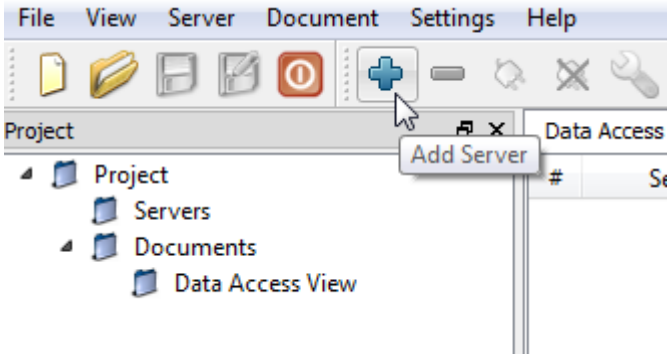


Caution: All certificates have a runtime and are invalid after the runtime. The ibaLogic certificate is set for a term of 50 years. In the next versions, corresponding display options and handling for the expiry warning will be included here.

2 Examples: Establishing a connection to the UAExpert client

Example of a connection via the freely available OPC UA client UAExpert

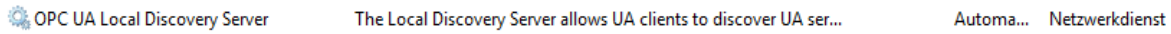
First you have to integrate the OPC UA server from ibaLogic



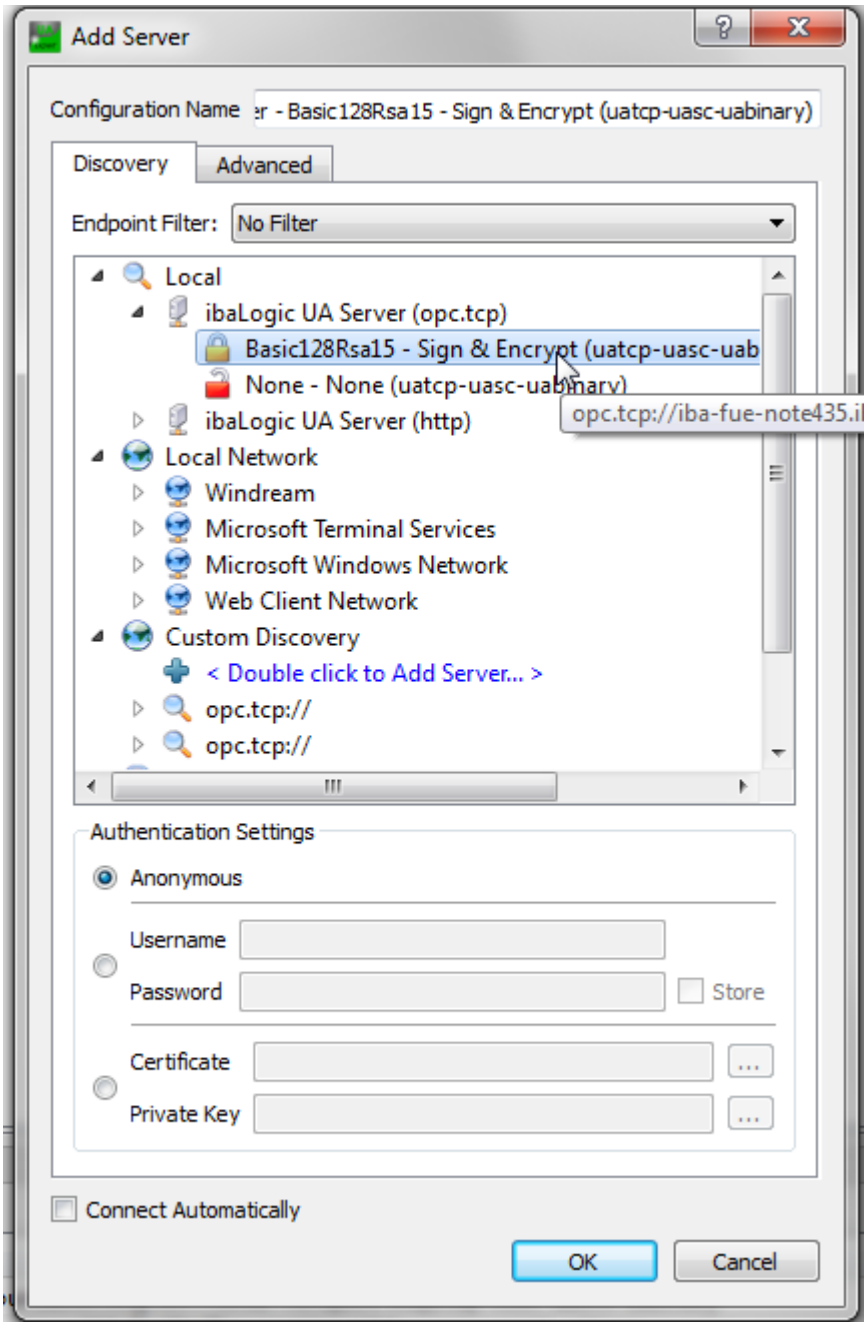
Normaly the ibaLogic UA server can be found there.

If not, then see if
A) ibaLogic is online and the OPC server is running (see tab in PMAC control)
B) the Discovery service is started

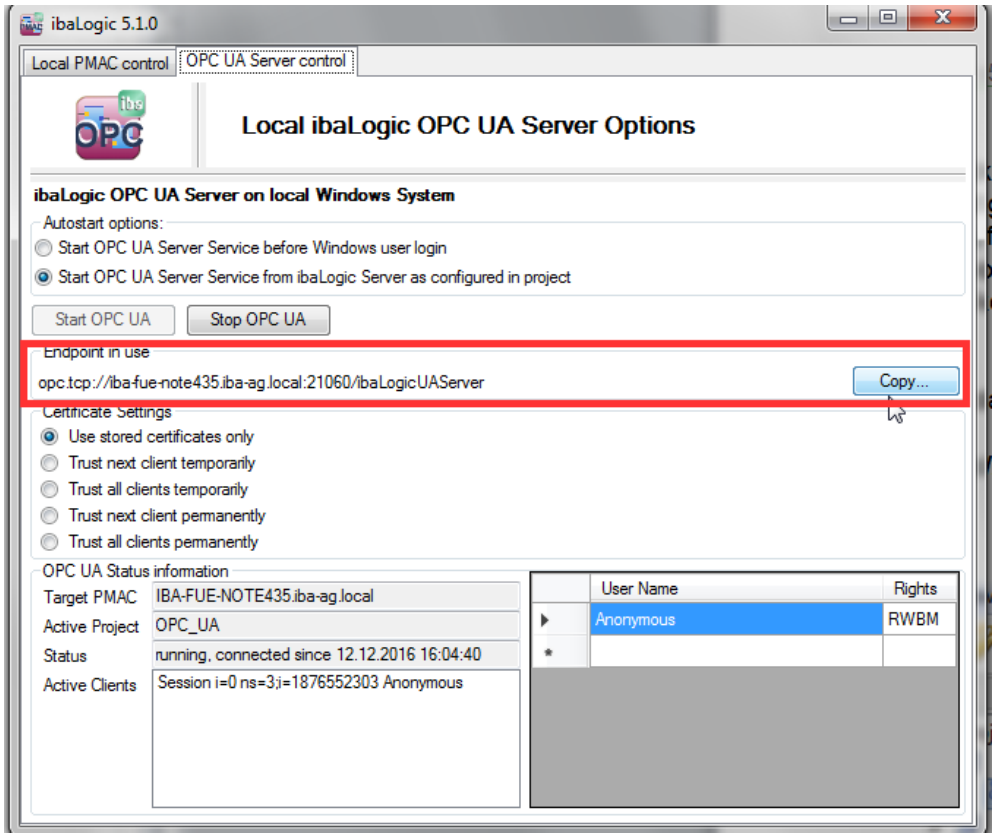
For searching the existing OPC UA server the OPC UA Discovery Server must be existing and running.



You can see here also with what kind of access ibaLogic works (Basic128Rsa15)

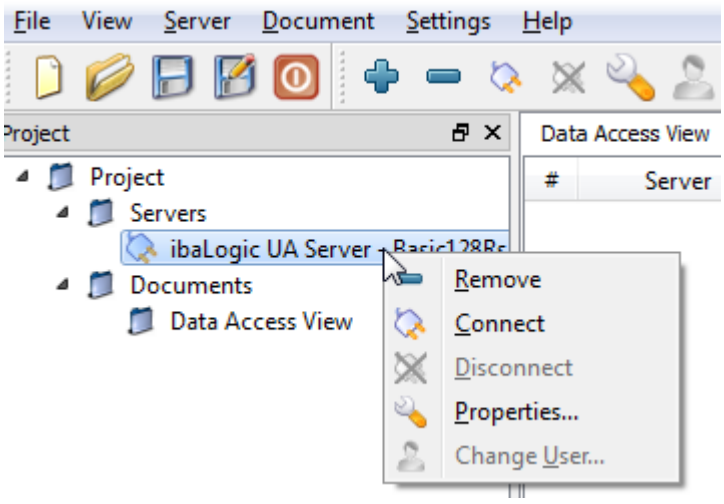


Double-click on the selected connection set this URL which is necessary for the connection automatically and closes the dialog.
The URL can also be found under ADVANCE and could also be copied from the OPC UA server of ibaLogic.
For copying, the ibaLogic UA Server has the following entry:

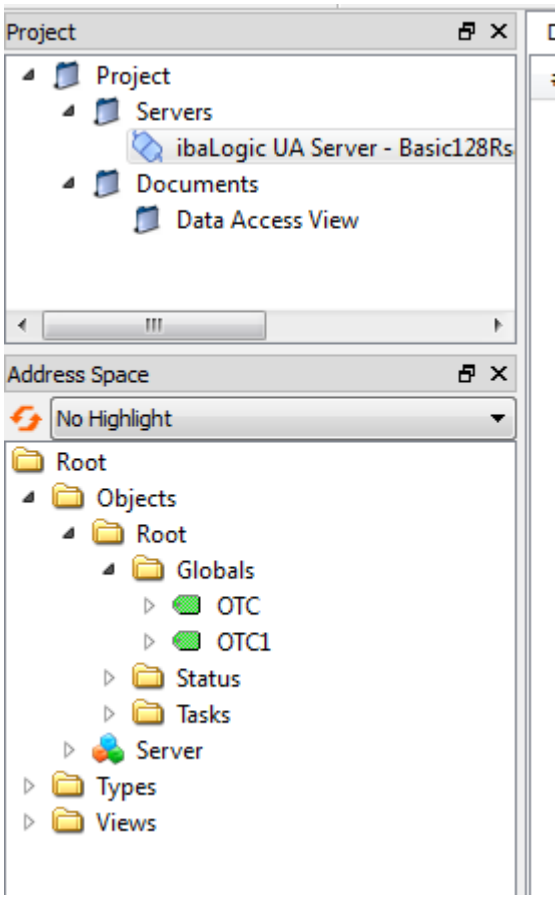


This is then the connection address (example)

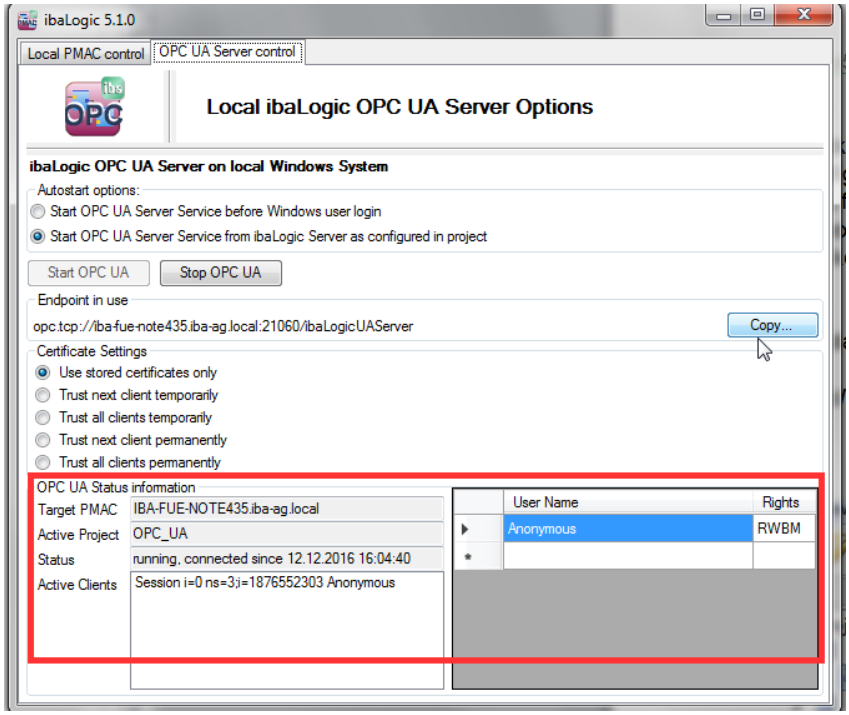
opc.tcp://iba-fue-note435.iba-ag.local:21060/ibaLogicUAServer



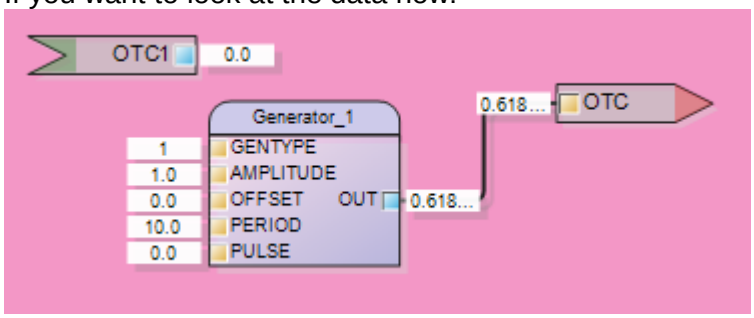
Now you can connect to the ibaLogic OPC UA Server (Connect) and access the variables below.



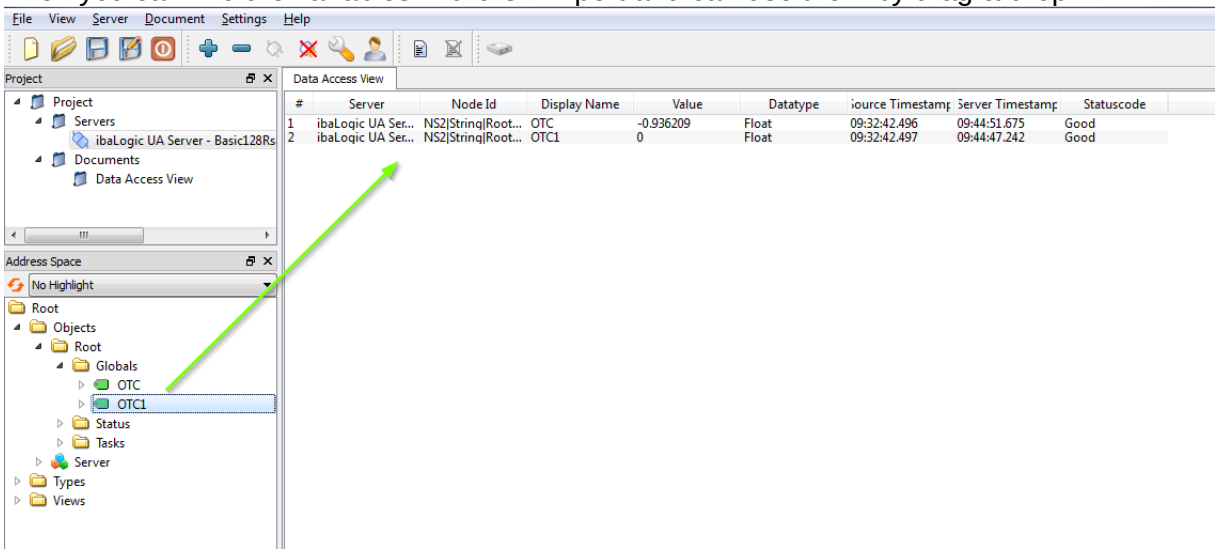
In the ibaLogic OPC UA server display in the PMAC Control you can also find the current user with which you are logged in.



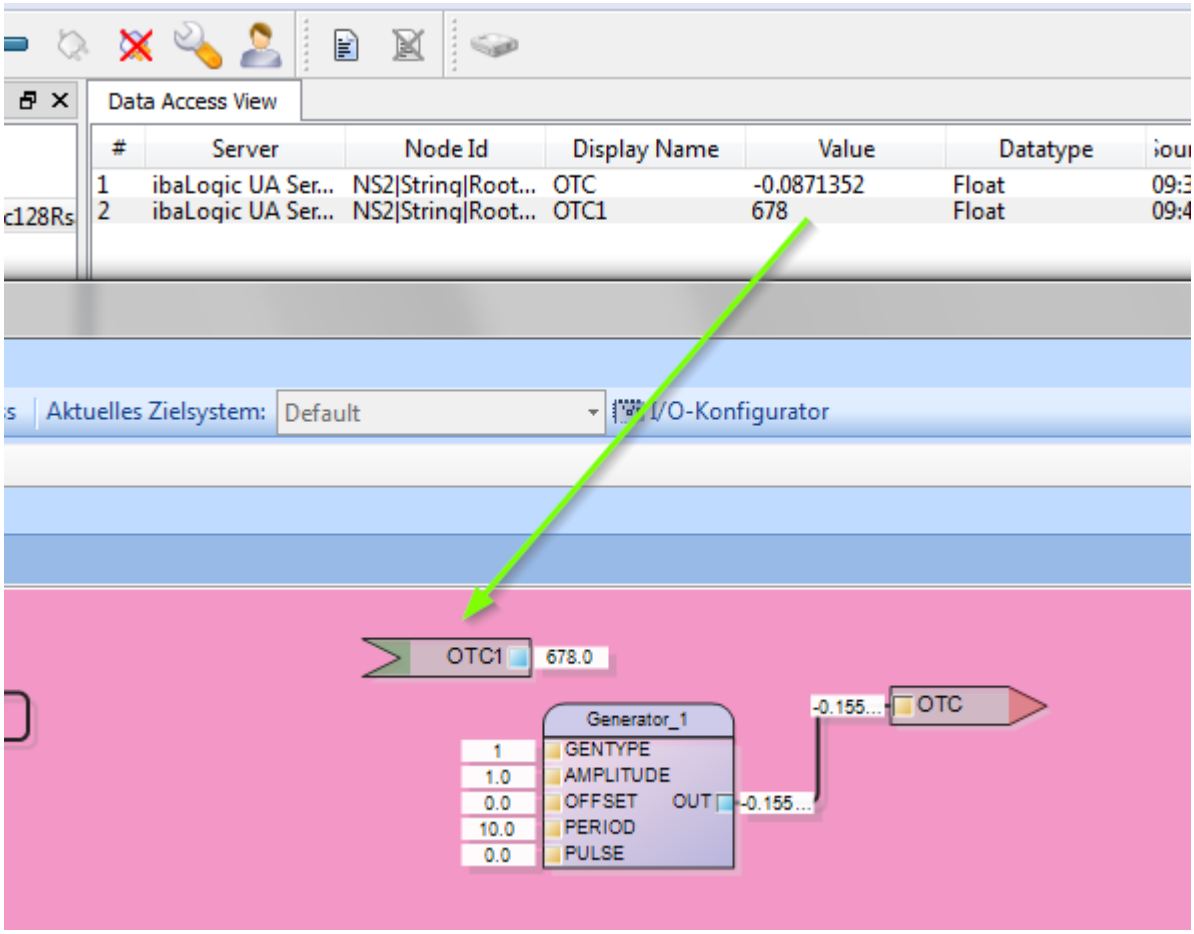
If you want to look at the data now:



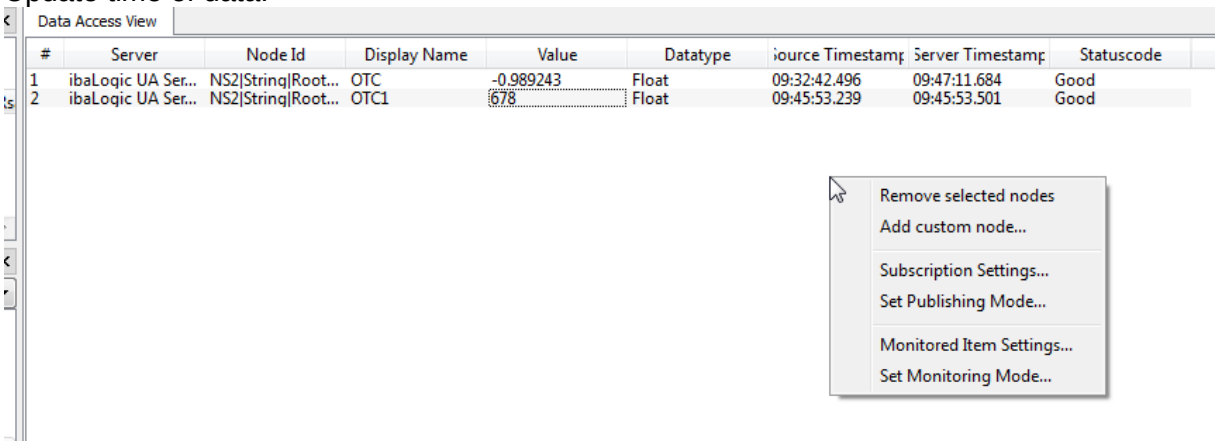
Then you can find the variables in the UAExpert and can use them by drag & drop.



Input values can be entered directly in the VALUE field. ! If the user has the right to write!

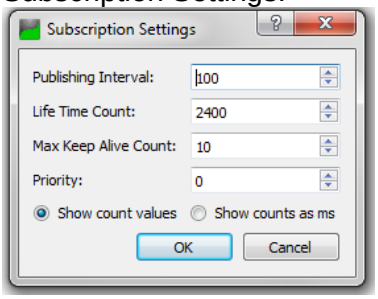

Data Access View
Server Node Id Display Name Value Datatype
1 ibaLogic UA Ser... NS2|String|Root... OTC -0.0871352 Float
2 ibaLogic UA Ser... NS2|String|Root... OTC1 678 Float
Aktuelles Zielsystem: Default
I/O-Konfigurator
OTC1
678.0
Generator_1
1 GENTYPE
1.0 AMPLITUDE
0.0 OFFSET
10.0 PERIOD
0.0 PULSE
OUT
-0.155...
-0.155...
OTC

Update time of data:



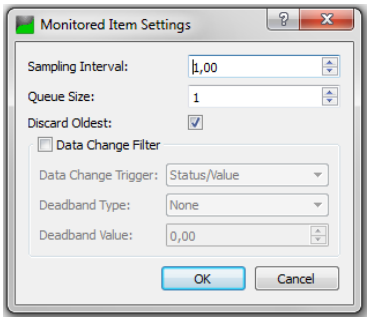
With the right mouse button this menu is displayed.
The most important points are here

Subscription Settings:



A publishing interval is possible up to 100ms

Each individual item has a setting:



The sampling interval can be used here, eg. could be set to 1ms.

Interesting is the queue size. It tells how many values in the samling intervall arrive.

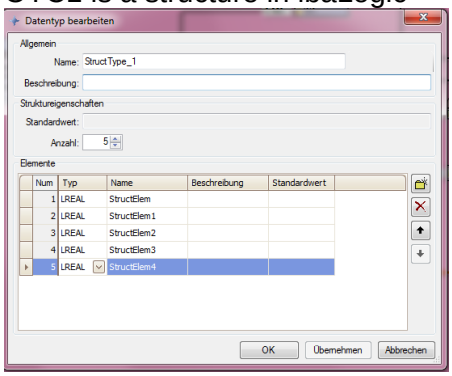
This can be seen as the buffered values of iba.

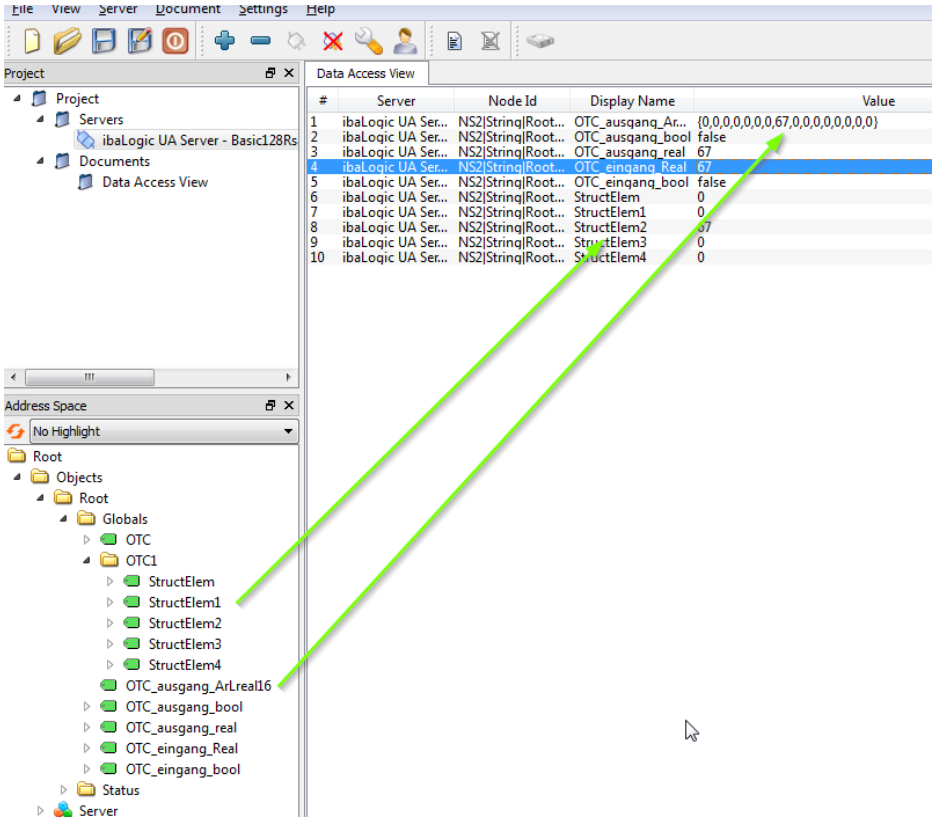
An array of data is sent at all x intervals.

This function is supported by the ibaLogic OPC UA server. It allows HMI to display more detailed curves, despite a slower pick-up rate.

Data types: (examples)

Here is just an example of arrays and structures
OTC1 is a structure in ibaLogic

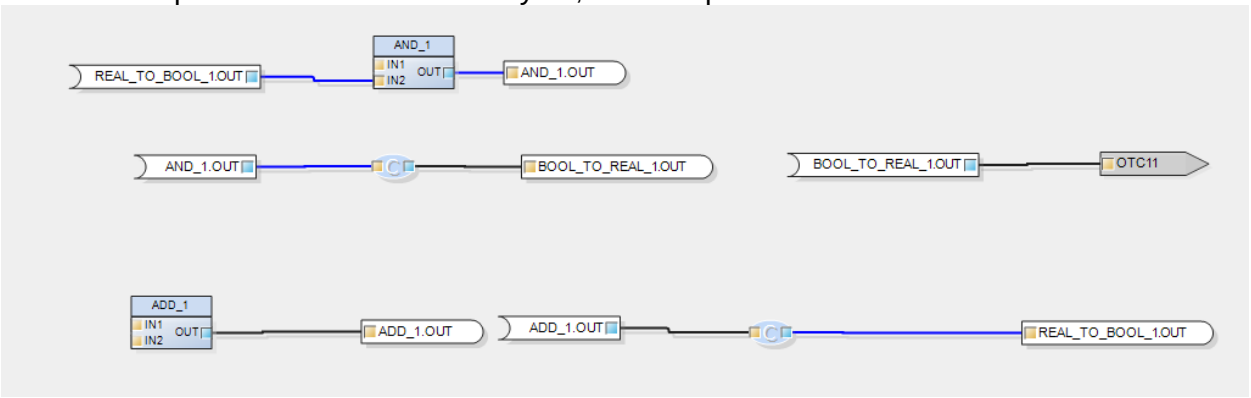




3 Template Export/Import for external generated programs

A reduced import was implemented from the request that it should be possible to automatically generate ibaLogic plan by external programs.

A reduced import then creates such a layout, for example.



All connections are replaced by IntraPageConnectors (IPCs). Thus, as a user, it is not necessary to provide exact information about the "connection path", ie the path of the connection.

Also other unnecessary information was removed from this reduced import.

Using an export, you can create a template for such an import file.

As a user you could now generate such a file with reduced information via an own written program (e.g. an C# programm).
That can be imported and so an automatically generated ibaLogic program can be build.

Example: An export has been generated for a plant part. This is however required depending on the customer 1..x times. You can now take the export as a base and copy the program over and over again.

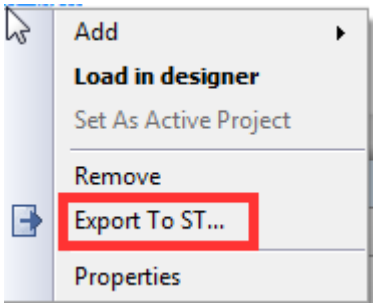
The export template contains GUIDs. These must then be adapted accordingly when copying. This means that if a template is to be used multiple times in the target, the GUIDs used must be modified for each copy so that the same GUIDs of the original are put together on new GUIDs, that the references between the connections are retained, but all GUIDs per se are unique.

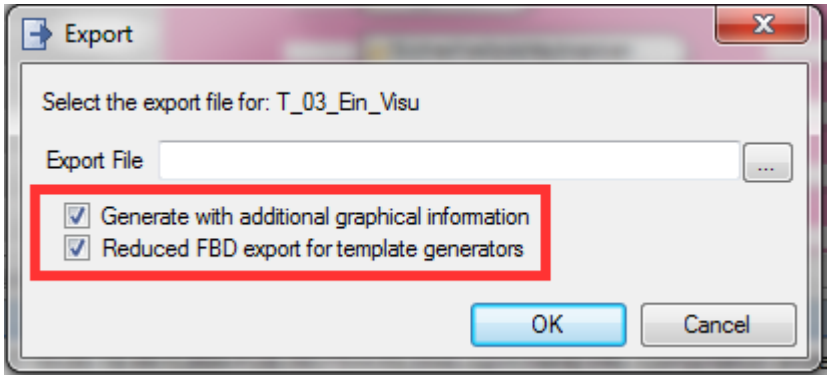
For the placement of inputs and outputs, note that these have a height of 22.03 and an offset of 3.01. Thus, the position of a connector can be easily calculated using (Index * 22.03) +3.01.

The naming of the inputs and outputs depends on which hardware is used.

Reduced Export:

It is called up in the context menu of the project, the individual program ... ..

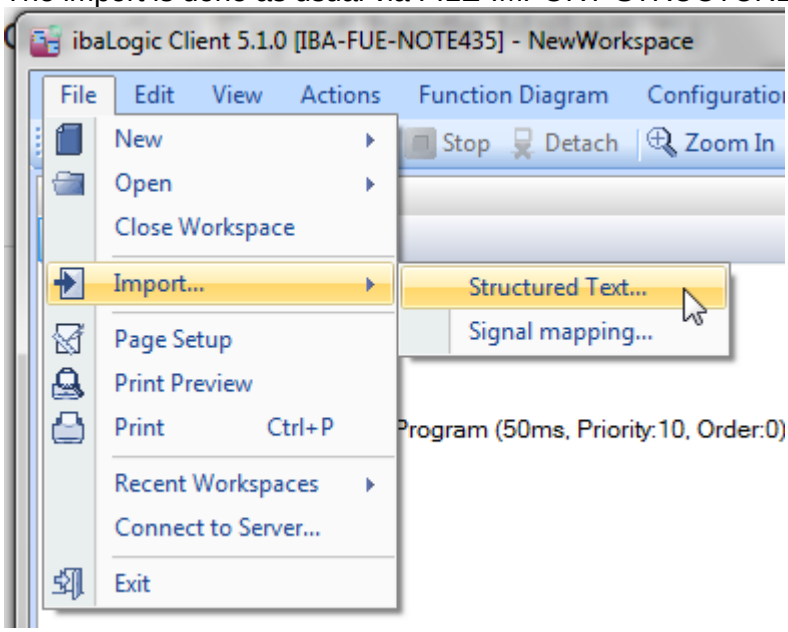


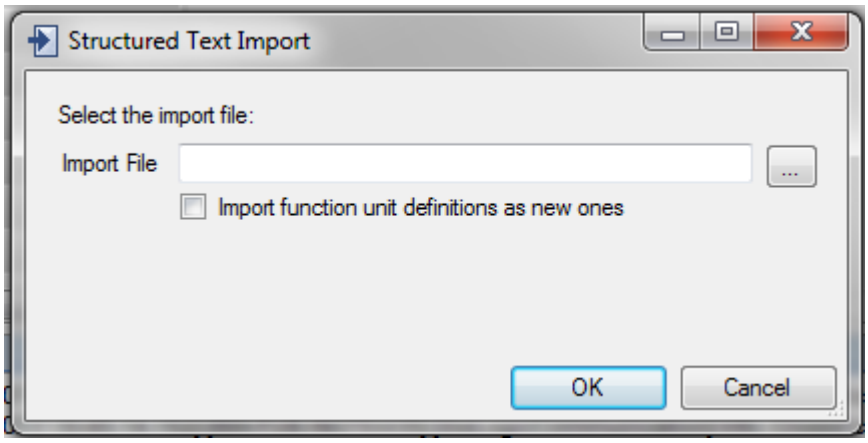


There are two hooks for a reduced export.

Reduced Import:

The import is done as usual via FILE-IMPORT-STRUCTURED TEXT ...

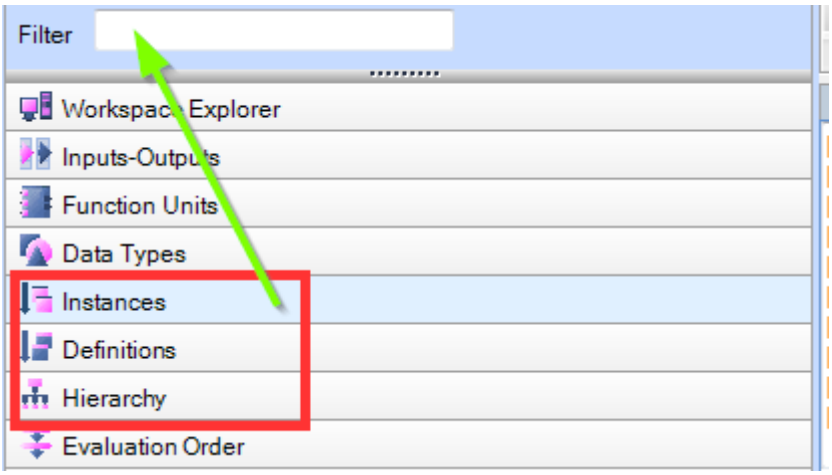




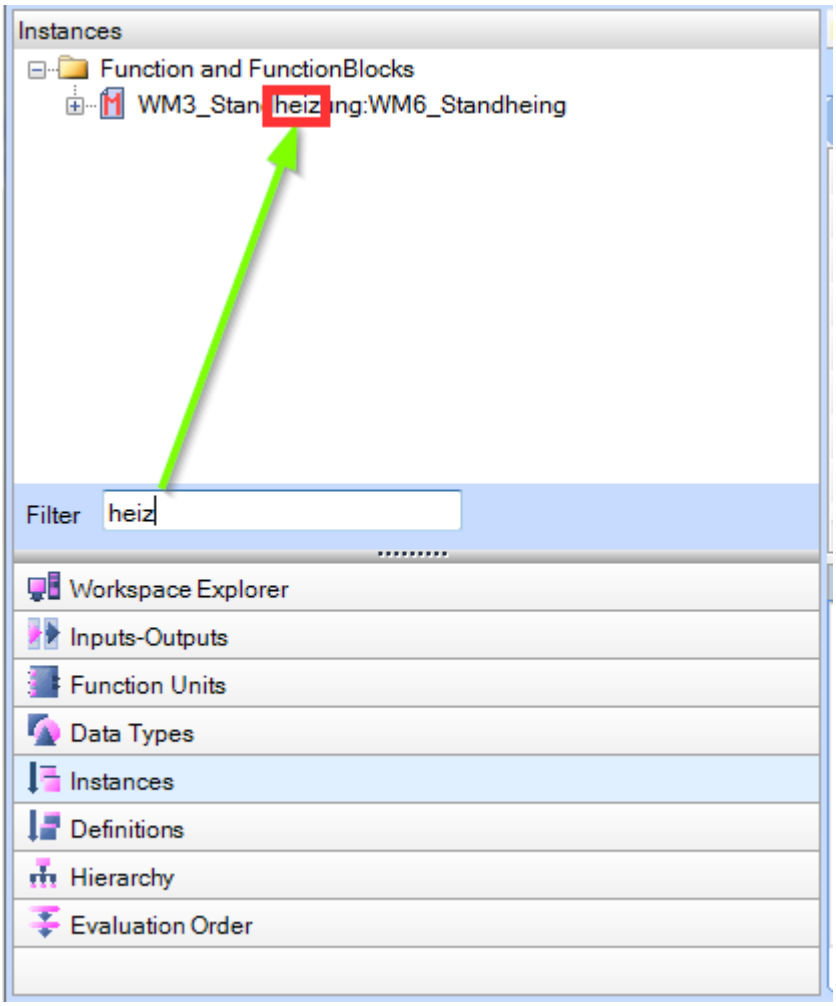
A reduced import is then automatically detected.

4 Filter in Instanz-/Definitions-/ Hirarchie-Tree

In the tree structure of instance view / definition view / hierarchy, a filter field is now available



This filter field is a text search. This allows you to limit the number of blocks you need to find them more quickly. Example:



5 Support of Windows10

Now Windows10 is supported as a platform.