OPC UA Client Communication Driver

This document has the specific information related to the driver configuration. For a generic explanation on Devices, Channels, Nodes and Points configuration, please refer to the reference guide.

Contents

Section 1 – Summary Information

Communication Driver Name: OPC UA Client

Implementation DLL: T.ProtocolDriver.OPCUA.dll

Protocol: OPC proprietary

Interface: OPC proprietary

Description: OPC UA Client implements communication with local and remote OPC servers. The communications blocks are dynamically created according the pooling cycle defined on the Access Type for each Device Point.

OPC servers supported: Any OPC server compatible with OPC UA specifications

Protocol Options: None

Max number of nodes: user defined

PC Hardware requirements: none

PC Software requirements: OPC Core components

> ✍Note:
> You can find the OPC Core components in the OPC Foundation web site.
> http://www.opcfoundation.org/

Section 2 – OPC UA Certificate Configuration

The UA security bases on X509 Certificates.
Each UA server and client application requires a certificate with the ApplicationUri of the application. UA servers typically can be configured for the certificate validation to be disabled. In this mode any proper certificate is accepted. It doesn't have to match the application.

Self-signed certificates can be created with the uaPLUS **UaClientConfigHelper** utility.
OPC UA maintains certificates in the Windows Certificates Store. The certificates are by default in the stores LocalMachine\UA Applications and LocalMachine\Trusted UA Applications
The stores are defined in the application UA configuration and can be changed if necessary.

The **UaClientConfigHelper** utility creates and imports certificates into the stores defined in the configuration.

Follow are steps to create certificates so that “Manager” and “Device module” work with OPC UA:

1) In Windows Explorer, open the installation folder

2) Run "UaClientConfigHelperNet4.exe" utility (right button and choose "Run as Administrator" command);

3) Inside “UA Client Configutaration Helper”, click “Browse" button and select the file TManager.exe into the product installation folder.

3.1) Click "Create UA Configuration" button;

3.2) Click "Edit UA Configuration" button;

3.3) Click "Certificates" button;

3.4) Click "Create" button and after clicking "OK" button;

3.5) Click "Save and Close" button;

3.6) Click "Done" button to close;

Note: Repeat the same steps to "TRunModule.exe" application.

- Server and Client on the same machine: the certificates are in the right place when created or imported with the **UaClientConfigHelper** utility.
- Server and Client on different machine: the following steps are required:

1. On the client machine create a certificate for the client application with the **UaClientConfigHelper** utility. The created certificate is automatically exported into a .DER file in the directory of the utility.

2. Copy the client certificate .DER file to the server machine and import it according the UA server documentation.

3. Copy the server .DER certificate file to the client machine and import it with the **UaClientConfigHelper** utility.

Note: The Windows Certificates manager can be used to check and maintain the certificates beyond the capabilities of the **UaClientConfigHelper** utility.

Section 3 – Channel Configuration

There is no channel configuration for OPC UA Client channels.

Section 4 – Node Configuration

Station Configuration

Service URL: Defines the location of the OPC Server. Example: ua:opc.tcp://127.0.0.1:62841/Advosol/uaPLUS

Refresh Rate: Server update rate.

AllItemsSameGroup: Flag indicating whether driver should add all items at the same OPC group and only one connection is created with OPC Server.

EnableReadPolling: Flag indicating whether reading is by polling.

WindowsAuthentication: Flag indicating whether it should use Windows Authentication security.

DisableSecurity: Flag indicating whether security is disabled.

UserName: String containing user name as security credentials.

Password: String containing user password as security credentials.

Domain: String containing domain as security credentials.

ReadFromDevice: Force all reads made from device.

UseTimestampFromComputer: Use timestamp from computer instead of device.

Section 5 – Point Configuration

Choose the OPCServer item that will communicate with the tag.

You can type the OPC Server item name into the textbox, or you can browse the OPC Server items with the cell editor.

OPC Arrays: You should configure the Array field in Modifiers column.

Section 6 – Troubleshoot

The status of the driver execution can be observed through the diagnostic tools, which are:

- Trace window
- Property Watch
- Module Information

The above tools indicate if the operations have succeeded or have failed, where the status 0 (zero) means success. Negative values are internal error codes and positive values are protocol error codes.

Please, consult your OPC Server documentation for the protocol specific error codes.

Revision History

Revision	Description	Date
A	Initial	1-sep-2014
B	Created new option “UseTimestampFromDevice”	14-nov-2014