OPC-UA Client

straton user guide – Rev. 3

sales@straton-plc.com

CP_R31_006_H

straton

Content

1. Overview

This document describes how to start with the straton OPC UA Client.

Note: This tutorial concerns the OPC UA configurator from the version 10.0 of straton and is not definitive (especially the part about security and authentication).

The OPC UA Client driver implementation uses the open62541 stack version "v1.0.1". The stack is a Single-file release available at: https://open62541.org/releases/

Additionally, the security implementation uses mbedtls version "mbed TLS 2.16.5". Library can be found here: https://tls.mbed.org/

2. Requirement and setup

For straton Editor: copy "K5BusOPCUA_client.dll" in the IOD folder of straton (if not already available).

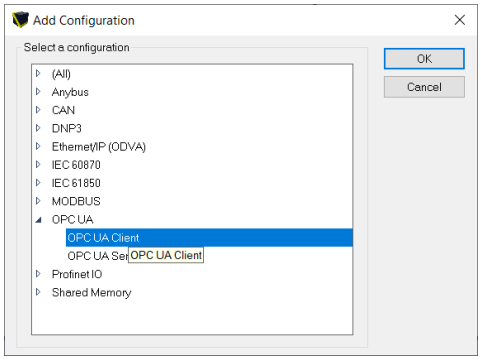
For straton Windows runtime, copy "T5BusExopcua_c.dll" with the runtime (if not already available).

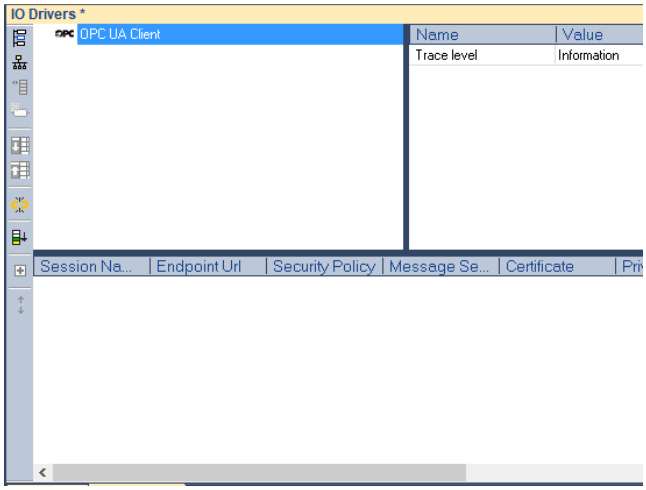
3. Create and configure an application

1.1. Create the configuration

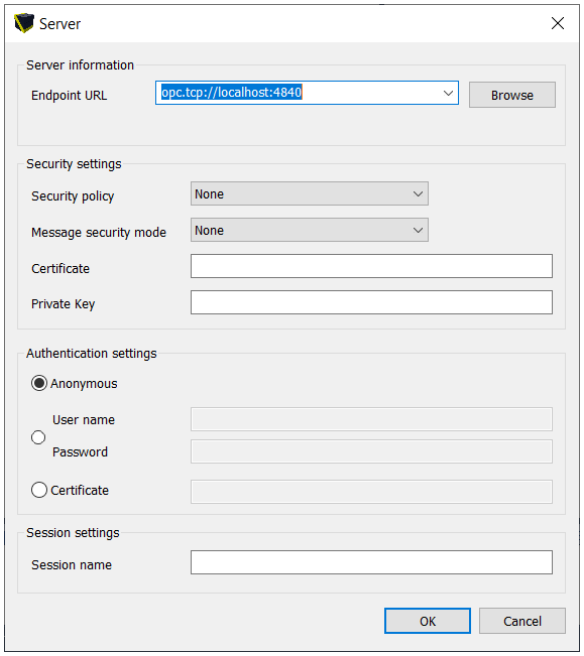
1.1.1. Add bus and server nodes

- Open the Fieldbus Configurations ( ) and add an “OPC UA Client” configuration.

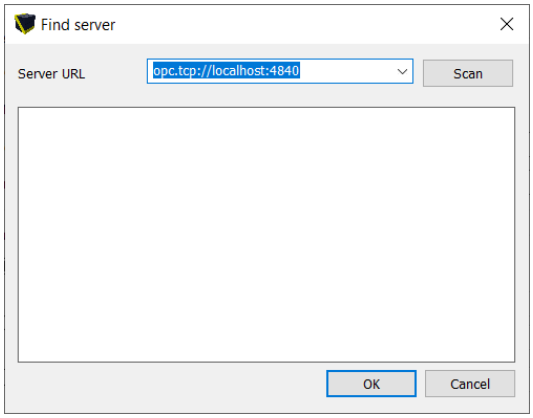




- Add a server node using the “Insert Master/Port” button:



Browse button: if you do not want to set all parameters manually, use the "Browse" button to scan all available servers/endpoints at chosen Endpoint URL. The dialog below will be displayed:



Using the "Scan" button, all available endpoints will appear in the list. Select one and click on OK.

Endpoint parameters will be automatically set in the dialog "Server".

1.1.2. Bus and Server parameters

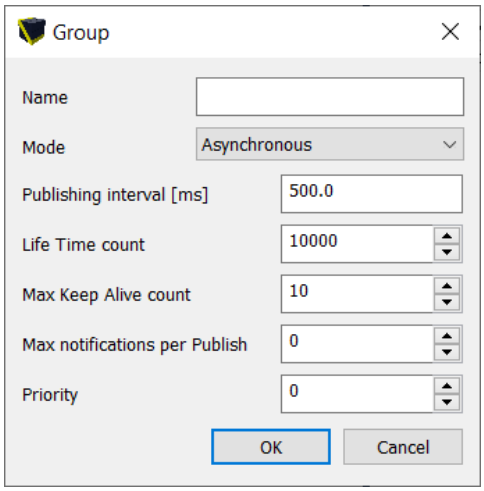
Level	Parameter	Description
Bus	Trace Level	Indicates which trace level user want to display (None, Information or Debug)
Server	Session Name	The session name. Not used
	Endpoint URL	The URL of the server where to connect with our client
	Security Policy	One of the security policies in this list: - None - Basic128Rsa15 - Basic256 - Basic256Sha256
	Message Security Mode	The security mode to use in this list: - None - Sign - Sign & Encrypt
	Certificate	If you choose 'Sign' or 'Sign & encrypt' as Message Security Mode, you must provide the name of the client certificate file to be used. *(part 1/2)*

Level	Parameter	Description
		(part 2/2) The certificate file must be in the PKI\CA\certs subfolder of the runtime folder. The certificate file must be in a DER binary format.
	Private Key	If you choose 'Sign' or 'Sign & encrypt' as Message Security Mode, you must provide the name of the private key file to be used. The private key file must be in the PKI\CA\private subfolder of the runtime folder. The private key file must be in a PEM format.
	Authentication	Authentication when connecting to the server: - Anonymous - User Name: a User name & password are required - Certificate: you must provide the name of the certificate file to be used for authentication. The certificate file must be in the PKI\CA\certs subfolder of the runtime folder. The certificate file must be in a DER binary format.
	User Name	If user has chosen Authentication with "User Name" he will have to set this parameter
	Password	If user has chosen Authentication with "User Name" he will have to set this parameter
	Certificate	If user has chosen Authentication with "Certificate" he will have to set this parameter The certificate file must be in the PKI\CA\certs subfolder of the runtime folder. The certificate file must be in a DER binary format.

1.2. Add group

When endpoint(s) have been chosen and configured, you can add groups and tags.

Click on button "Insert Slave/Data Block" in the left toolbar:



Level	Property	Description
Group	Name	The group name. Used to describe collection of tags below
	Mode	Synchronous: all variable will be read each runtime cycle with blocked call Asynchronous: variables will be read on event only
	Publishing Interval (ms)	This interval defines the cyclic rate that the Subscription is being requested to return Notifications to the Client. This interval is expressed in milliseconds. The negotiated value for this parameter returned in the response is used as the default sampling interval for MonitoredItems assigned to this Subscription.If the requested value is 0 or negative, the Server shall revise with the fastest supported publishing interval.
	Life Time Count	Requested lifetime count. The lifetime count shall be a minimum of three times the keep-alive count. When the publishing timer has expired this number of times without a *Publish* request being available to send a *NotificationMessage*, then the *Subscription* shall be deleted by the *Server*.
	Max Keep Alive Count	Requested maximum keep-alive count. When the publishing timer has expired this number of times without requiring any *NotificationMessage* to be sent, the *Subscription* sends a keep-alive *Message* to the *Client*. The negotiated value for this parameter is returned in the response.If the requested value is 0, the *Server* shall revise with the smallest supported keep-alive count.

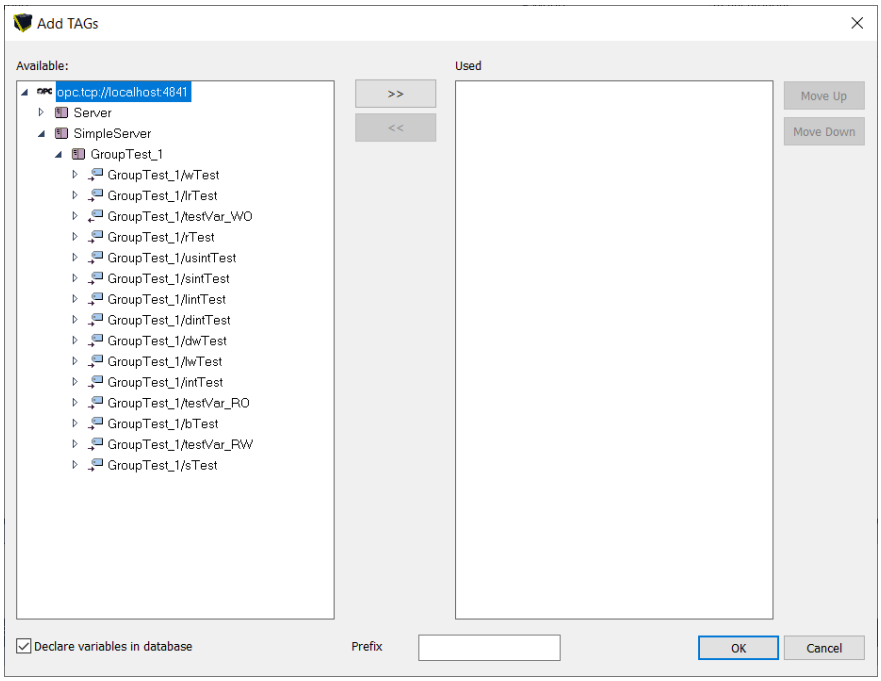
Level	Property	Description
	Max Notifications Per Publish	The maximum number of notifications that the Client wishes to receive in a single Publish response. A value of zero indicates that there is no limit
	Priority	Indicates the relative priority of the Subscription. When more than one Subscription needs to send Notifications, the Server should de-queue a Publish request to the Subscription with the highest priority number. For Subscriptions with equal priority the Server should de-queue Publish requests in a round-robin fashion. A Client that does not require special priority settings should set this value to zero.

Note: Groups can be created to have a clear overview of the overall configuration.

1.3. Add tags

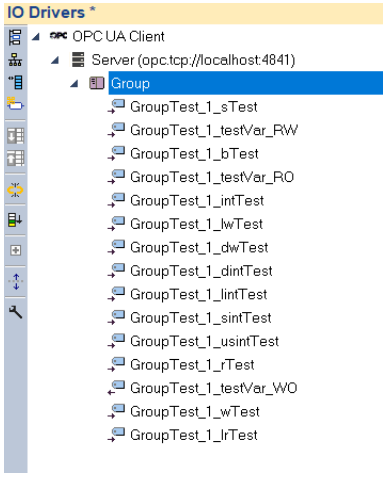
Once group has been added, right click on group and click on command "Add Tags…".

Note: to use this dialog you should have set the endpoint URL to connect to an existing server with correct authentication.



A popup window opens, simply map your variables from the left area to the right area, using the '>>'.

After validating, the configuration tree is automatically created:



Variable properties:

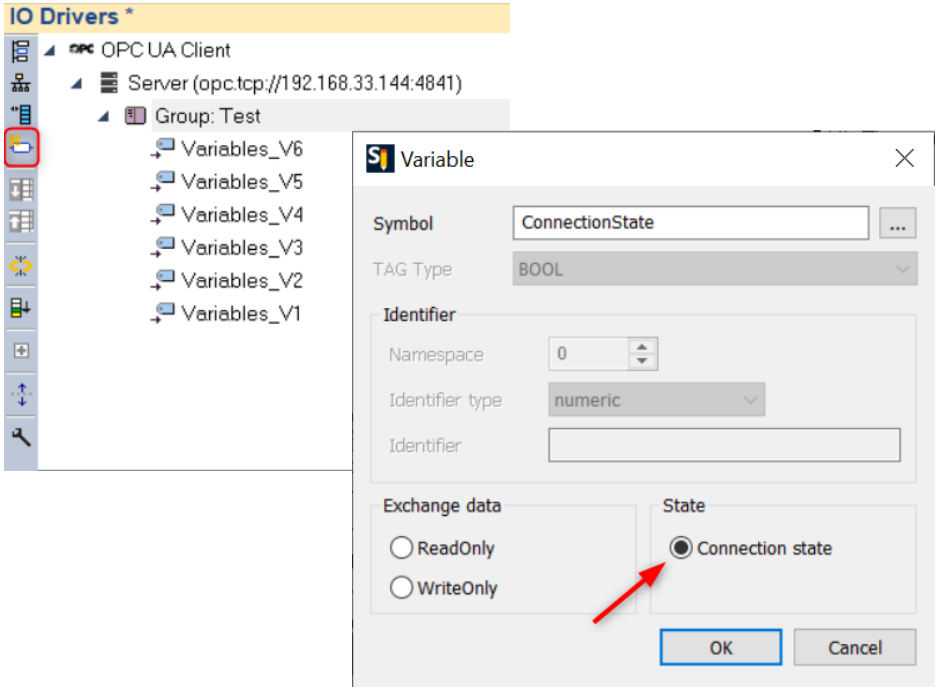
Level	Parameter	Description
Variable	Symbol	The straton variable associated to the OPC UA tag
	Namespace	The name space where the tag belongs
	Identifier Type	The tag identifier type. Can be: - numeric - string - GUID - bytestring
	Identifier	The tag identifier value
	Tag Type	The OPC UA tag type: - BOOL - INT8, UINT8 - INT16, UINT16 - INT32, UINT32 - INT64, UINT64 - FLOAT32, FLOAT64 - STRING256 - BYTESTRING256 - GUID - STATUSCODE - XMLELEMENT

Level	Parameter	Description
	Mode	The mode of the variable. Can be: - ReadOnly - WriteOnly - Connection Status

1.4. Add the Connection State

The "Connection State" is a Boolean variable, which show you if you are connected to the Server or not.

Click on "Insert Variable" and select "Connection State"



Values matching:

ConnectionState = TRUE

➔ The Client is connected to the Server

ConnectionState = FALSE

➔ The Client is not connected to the Server (connection lost,…)

1.5. Building and downloading the application

Download the application to the runtime:

- Select the communication parameters in menu Tools/Communication Parameters
- Establish the connection through menu Project/Online

RESULT IS:

The download is successful and application starts correctly.

The runtime is not started or communication parameters are wrong.

The application is not yet downloaded or an error occurs during startup. More detail can be found in the output view.

4. Frequently Asked Questions

The OPC UA Client does not want to connect to the Server…

If no certificates are used, check the Client's Endpoint URL parameter. For example if your Server is on another PC than the Client, the URL can't be 'opc.tcp://localhost:4840', it must be something like 'opc.tcp://192.168.33.136:4840' with the Server's IP address and port.

Check that the port is well opened on the Server side.

Check that the Server can be reached using a 'ping' command, for example.

Check that the Client certificate (*.der file) is copied in the Server certificate folder.

If a Password is used by the Server ('Password' field not empty), check that the Client's matches: the security policy must be different than 'None' and passwords must match.

How to check that a Server is available?

From the second level of the configuration (Server level) the "Browse" button already give an idea about available Servers.