OPC UA Client

APPLICATION NOTE

AUG-0074-00 EN 1.2 ENGLISH

Connecting Devices™

Important User Information

Liability

Every care has been taken in the preparation of this document. Please inform HMS Industrial Networks SA of any inaccuracies or omissions. The data and illustrations found in this document are not binding. We, HMS Industrial Networks SA, reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be considered as a commitment by HMS Industrial Networks SA. HMS Industrial Networks SA assumes no responsibility for any errors that may appear in this document.

There are many applications of this product. Those responsible for the use of this device must ensure that all the necessary steps have been taken to verify that the applications meet all performance and safety requirements including any applicable laws, regulations, codes, and standards.

HMS Industrial Networks SA will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features, timing, or functional side effects found outside the documented scope of this product. The effects caused by any direct or indirect use of such aspects of the product are undefined, and may include e.g. compatibility issues and stability issues.

The examples and illustrations in this document are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular implementation, HMS Industrial Networks SA cannot assume responsibility for actual use based on these examples and illustrations.

Intellectual Property Rights

HMS Industrial Networks SA has intellectual property rights relating to technology embodied in the product described in this document. These intellectual property rights may include patents and pending patent applications in the USA and other countries.

Table of Contents

Page

This page intentionally left blank

1 Preface

1.1 About This Document

The present document describes the eWON Flexy used as an OPC UA client and explains how to retrieve tags using this OPC UA protocol.

For additional related documentation and file downloads, please visit www.ewon.biz/support.

1.2 Document History

Version	Date	Description
1.0	2018-03-30	First release
1.1	2018-05-03	Changed: Firmware version
1.2	2018-09-04	Changed: Previously named KB-1502 Added: Certificates

1.3 Related Documents

Document	Author	Document ID
Flexy	HMS	RG-0008

1.4 Trademark Information

2 Introduction

As of firmware version 13.0, the Flexy features an OPC UA client capable of retrieving values from an OPC UA server embedded in to PLCs, HMIs, ...

The retrieval of such values is done thanks to the Flexy IO server called “OPCUA”.

This IO server allows the Flexy to connect to a maximum of 3 different OPC UA devices/servers.

3 Configuration

To enable the functionality, go to the IO Servers section located at:**Tags** > **IO Servers** > **OPCUA**.

The configuration page of the OPC UA client is divided in two sections.

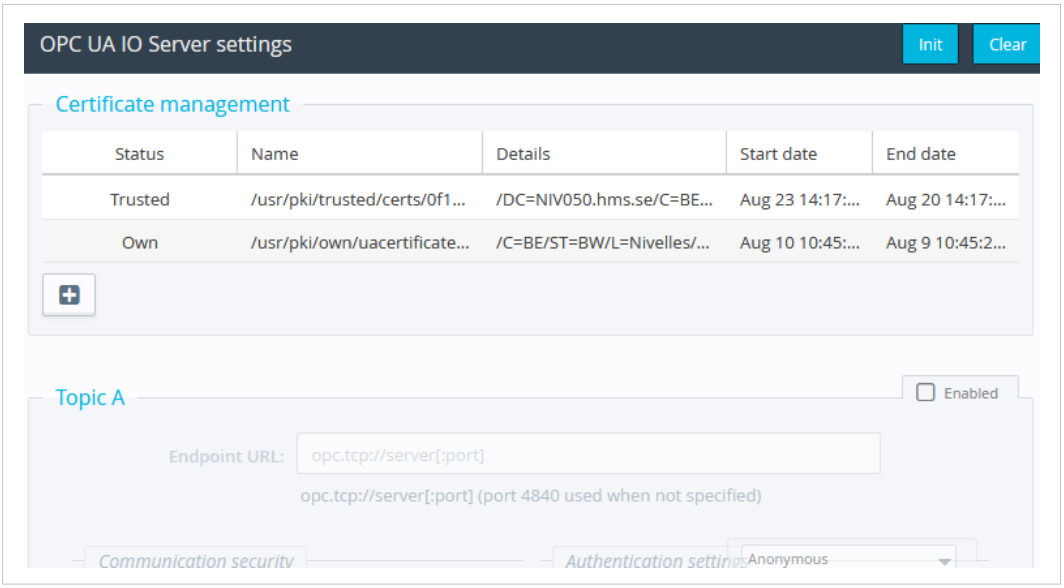

Fig. 1 Flexy OPC UA Client Web Interface

3.1 Certificates Management

As of firmware version 13.1s0, the Flexy makes its OPC UA protocol compatible with certificates.

This allows the encryption and the authentication with certificates for the OPC UA server of the Flexy.

The Flexy is capable of handling different:

- Security policy:
  - None: no encryption.
  - Basic256.
  - Basic256Sha256.
- Security mode:
  - None: no encryption.
  - Sign: the access control, which allows to trust or reject the connection on both sides.
  - Sign and encrypt: the access control and encryption.

Security modes are available for compatibility purpose.

The recommended setup would be:

- Basic256Sha256.
- Sign and encrypt.

3.1.1 Certificates Usefulness

The certificates help in:

- Securing the communication, by providing a secure channel where messages are signed and/or encrypted.
- Authenticating the user, by providing an access to a server as well as an easy (standard) way of managing accesses (process of identify – approve – revoke).

This is done through a process:

- Certificates are stored in a “PKI”: one for the OPC UA client and another one for the OPC UA server.
- Users or devices possess a key pair: private & public.
  - If none is provided, they will be generated automatically (by the Flexy OPC UA server).
  - Commissioning possibility: GUI, FTP, SD card, USB.
  - Managing possibility (trust, revoke, upload & download) through the GUI or the FTP.

The following procedure occurs when an OPC UA client and an OPC UA server try to communicate in a secure way.

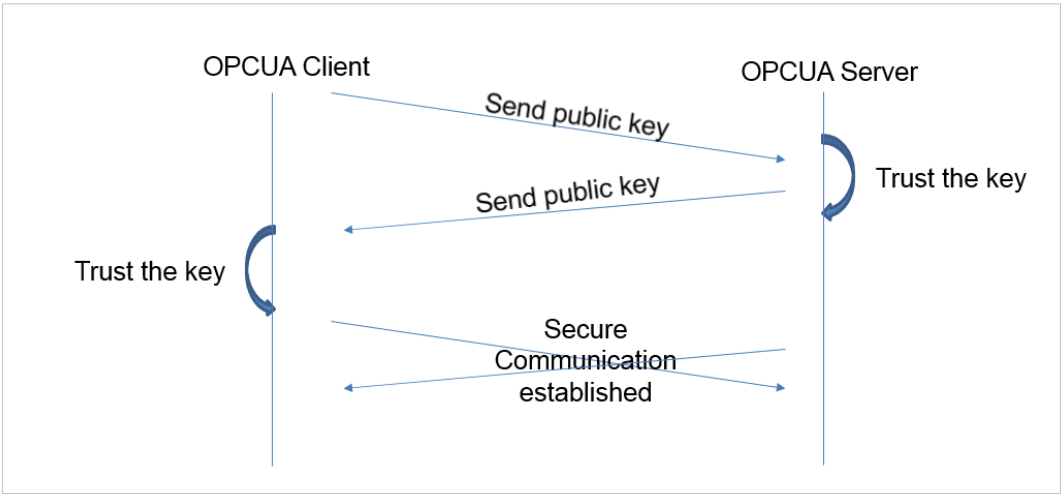

Fig. 2 OPC UA Secure Communication Exchanges

They exchange their certificates (from the PKI) and on each side, an operation occurs consisting in approving/rejecting the key. Once it’s done, they can encrypt/decrypt the communication.

This is the “Sign and Encrypt”: both parts know each other (trusted the keys) and they communicate over an encrypted channel.

3.1.2 Certificates Setup

When using certificates, through the GUI or FTP, you will be able to:

- encrypt
- sign
- authenticate

The list of certificates managed by the Flexy is displayed at the top of the OPCUA IO client web page.

Certificates can be manually added by clicking the “+” icon which makes it possible to upload new certificates/private key for the authentication part.

These certificates are divided in 3 categories:

- Own: the client certificate, used for signing/encryption.
- Auth: the authentication certificate, used to log in with a certificate.
- Trusted/Rejected: this is used to control the access (signing procedure) and ensure to know who can and cannot connect from/to.

Only certificates tagged as “own”, “auth” and “trusted” will be used. Certificates tagged as “rejected” will be listed but ignored.

> **!** When a certificate is added to the list for the first time, it will automatically be tagged as “rejected” and can’t be used yet to connect. You will need to right-click on the certificate row and switch its status to “trust”. By applying this configuration, the certificate will become usable.

If the certificates can be dealt via the GUI, it can also be managed through FTP. All the operations (the PKI) can be done by switching certificates/keys from one folder to another one.

Each PKI is stored in the */usr* dir of your Flexy. The default folder for the OPC UA client is */usr/pki_cli*.

In the PKI directory, there are 4 subdirectories:

auth	the storage of the certificates and private keys used for authentication.
own	the storage of its own certificates (identity) for signing purpose.
rejected	the storage of the rejected certificates (default folder).
trusted	The storage of the accepted/trusted certificates.

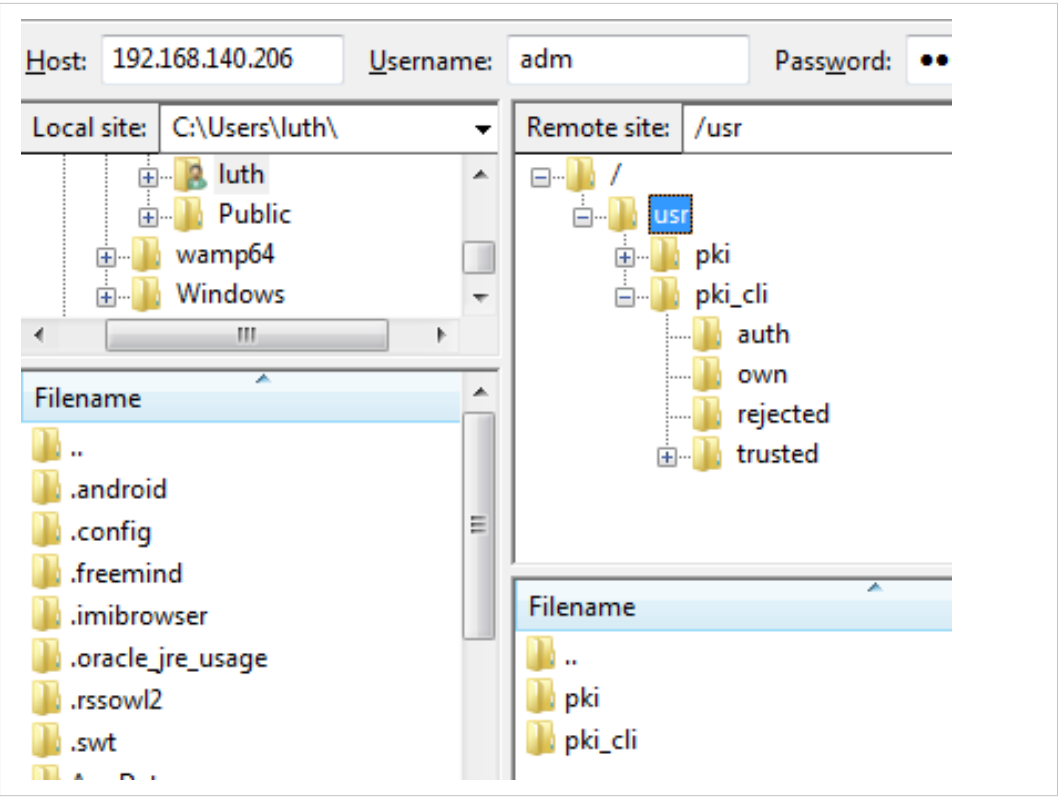

Fig. 3 FTP Interface for OPC UA Client.

The trust operation is a simple file move from "rejected" to "trusted/certs/" directory.

If you are generating your own certificates (i.e.: because of facility network policy), the "urn" string must be included in the client certificate which value is "urn:HMS: IOServer:Client:C0". If the "urn" is not provided the following error will be generated in the logs: *opcuasrv-Connect fail (BadCertificateUriInvalid)*.

3.2 Topics settings

There are 3 sections representing each topic (A, B and C) and allowing the configuration of corresponding topic.

Parameters	Description
Enable Topic	By checking the box, you enable the topic to be published.
Endpoint URL	The address of the OPC UA device you want to retrieve tags from, which must follow the syntax: opc.tcp://[server]:[port]. This address must be in the same range than the IP address of your Flexy.
Security policy	The level of security policy.

Parameters	Description
Security mode	The security method applied to the communication: • None: no security • Sign: will allow you to sign the communication to ensure both sides (client and server) know each other. • Sign and encrypt: will do the same as *Sign* and encrypt your communication in a secure way.
Authentication settings	The authentication to be able to publish to the eWON OPC UA server can be anonymous (server widely open), protected by a combination of user/password or by a certificate. In the case of a user/password combination, the OPC UA client will have to log in with credentials accepted by the OPC UA server. In case of certificates, you will need to select a certificate (.der file) and a private key (.pem file). These files will need to be uploaded in the PKI frame first. The certificates are explained in *Certificates Management, p. 5*

3.3 Tag Configuration

When configuring a Flexy tag which uses the *OPCUA* IO server, you have the possibility to browse a list of tags retrieved from the OPC UA server.

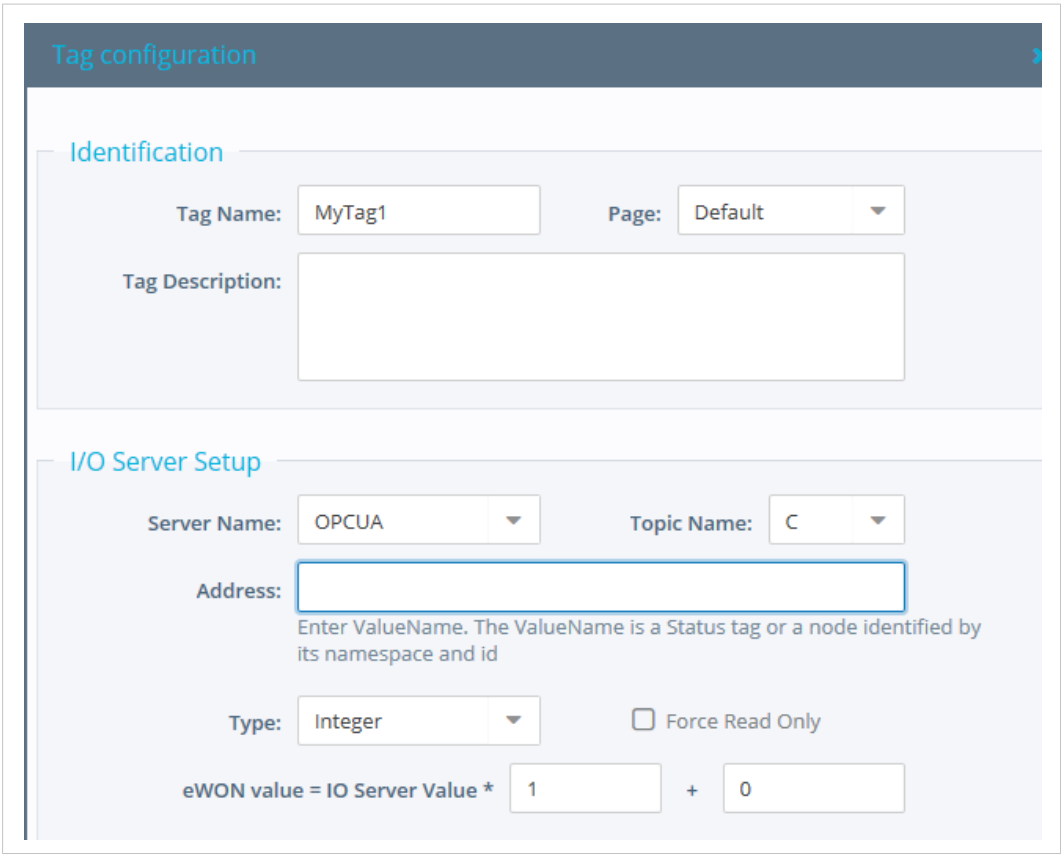

Fig. 4 Tag Setup Window

Create a tag by specifying a *Tag Name* and select for the *Server Name* “OPCUA”. For the *Topic Name*, select the one you just enabled and configured (A, B or C). This will link the Tag to the OPC UA device you want to reach.

To specify the address, click on the *Address* field and the *Tag Helper* will provide 2 choices:

- Status: indicates the current status of the tag.

- OPCUA Node: will link the Flexy tag to one of the OPC UA device value.

A new window will open which allows the discovery of all nodes from the OPC UA server.

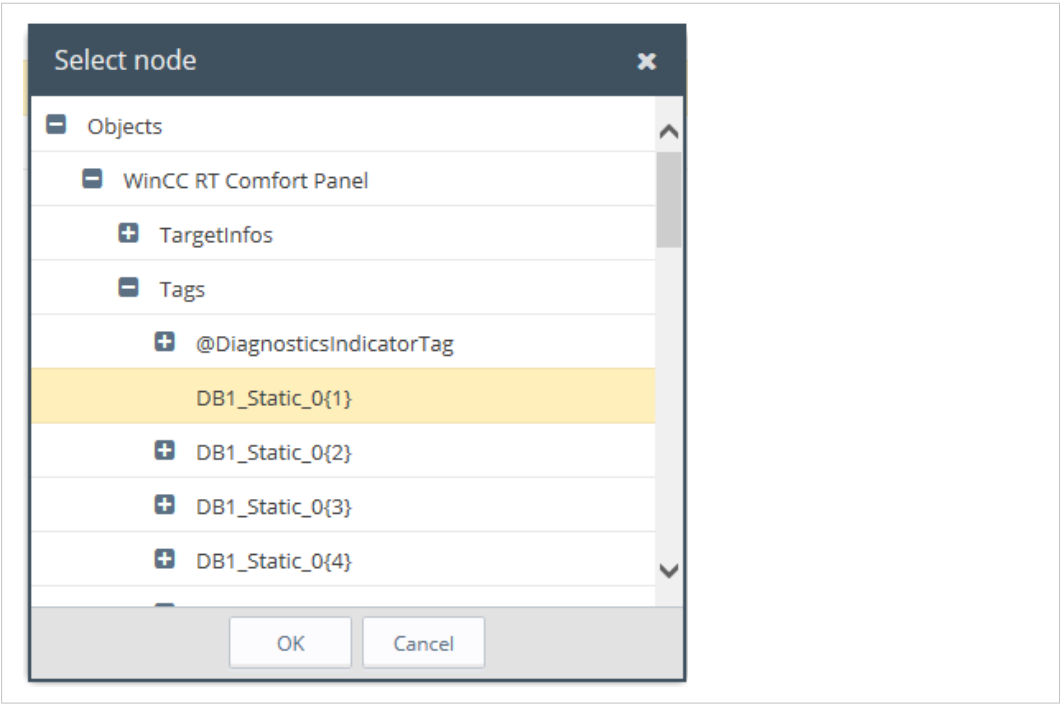

Fig. 5 Node List from OPC UA Server

The list is in a dynamic mode and will refresh each time a “+” icon is clicked.

You will never have a complete view of the node architecture because it can sometimes very long. The structure is not a tree-based one, it’s a graph and can contain cycles.

Once you found your OPC UA node on your OPC UA server, click on it and hit the “OK” button to validate the IO address.

The *Tag Address* field is now filled with the correct syntax of the OPC UA node.

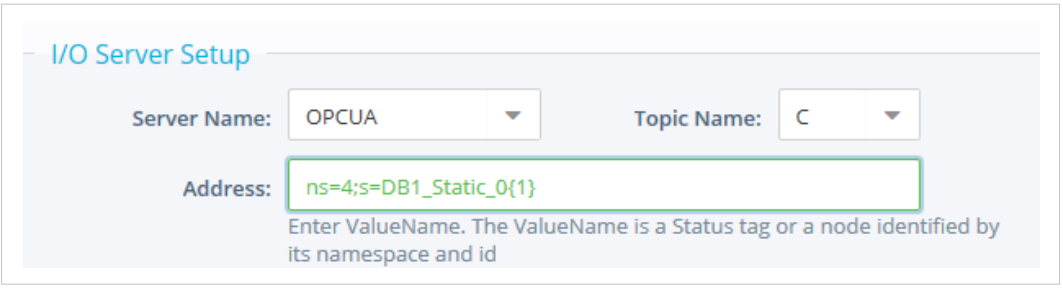

Fig. 6 Address of an OPC UA Node.

The tag type field is automatically updated with the corresponding type based on the provided OPC UA node.

Fill in the other tag parameters if required (alarm setting, historical settings, etc.) and click on *Add Tag* to create the tag.

If you switch to the “View mode”, the tag should now reflect the value of the corresponding OPC UA node.

> **!** Strings data type are currently in ASCII format and it is supported by OPCUA I/O server. UTF-8 is not supported yet.

Box 4126
300 04 Halmstad, Sweden

info@hms.se

AUG-0074-00 EN 1.2 / 2018-11-20 / 10606