OPC UA Server

APPLICATION NOTE

AUG-0064-00 EN 1.1 ENGLISH

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 server and explains how to publish 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	2016-06-07	First release
1.1	2018-08-28	Added:Certificates Management Changed: OPC UA Client configuration Changed: General Template

1.3 Related Documents

Document	Author	Document ID
Flexy	HMS	RG-0008-00

1.4 Trademark Information

eWON® is a registered trademark of HMS Industrial Networks SA. All other trademarks mentioned in this document are the property of their respective holders.

2 Introduction

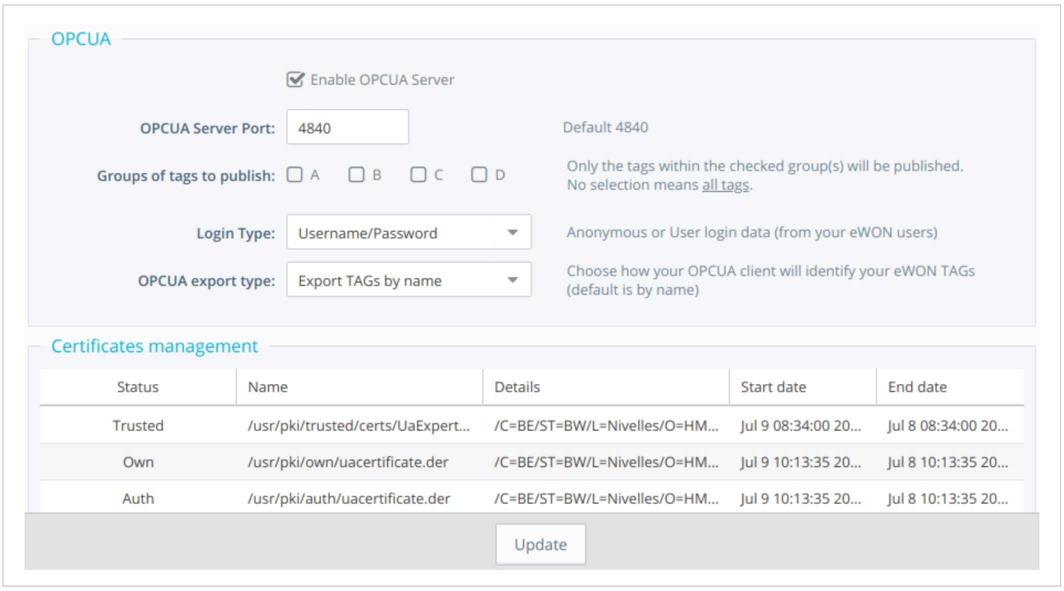
As of firmware version 11.2, the Flexy features an OPC UA server that allows the access to your tags through a third-party OPC UA client.

Only the instantaneous tag values are accessible in read & write through OPC UA. The historical logging or the alarms cannot be retrieved.

3 Configuration

To enable the functionality, go to **Setup** > **System** > **Main** > **Net services** > **OPCUA**.

The configuration page of the OPC UA server is divided in two tables.



OPCUA

☑ Enable OPCUA Server

OPCUA Server Port: 4840 — Default 4840

Groups of tags to publish: □ A □ B □ C □ D — Only the tags within the checked group(s) will be published. No selection means all tags.

Login Type: Username/Password — Anonymous or User login data (from your eWON users)

OPCUA export type: Export TAGs by name — Choose how your OPCUA client will identify your eWON TAGs (default is by name)

Certificates management

Status	Name	Details	Start date	End date
Trusted	/usr/pki/trusted/certs/UaExpert...	/C=BE/ST=BW/L=Nivelles/O=HM...	Jul 9 08:34:00 20...	Jul 8 08:34:00 20...
Own	/usr/pki/own/uacertificate.der	/C=BE/ST=BW/L=Nivelles/O=HM...	Jul 9 10:13:35 20...	Jul 8 10:13:35 20...
Auth	/usr/pki/auth/uacertificate.der	/C=BE/ST=BW/L=Nivelles/O=HM...	Jul 9 10:13:35 20...	Jul 8 10:13:35 20...

Fig. 1 Flexy OPC UA Server Web Interface

3.1 General settings

Parameters	Description
Enable OPCUA Server	Check the box to enable the OPC UA server of the Flexy.
OPCUA Server Port	The port the Flexy OPC UA server will listen to. Default : 48020. The server is accessible regardless the IP interface : VPN, LAN or WAN.
Groups of tags to publish	The group(s) of tags the OPC UA server will publish. One group at least must be selected.
Login Type	The access to your eWON OPC UA server can be opened to any clients (anonymous access), 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 an eWON user for which the right *Force Outputs* has been granted. The certificates are explained in *Certificates Management, p. 6*
OPCUA export type	How the 3rd-party OPC UA client should identify the tags send by the Flexy OPC UA server. Default: Export TAGs by name.

! The OPC UA server can be accessed from all network interfaces. The use of the “Anonymous” authentication is therefore not recommended if your Flexy is accessible from an untrusted network.

3.2 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.

ℹ *Security modes are available for compatibility purpose.*

The recommended setup would be:

- Basic256Sha256.
- Sign and encrypt.

3.2.1 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.

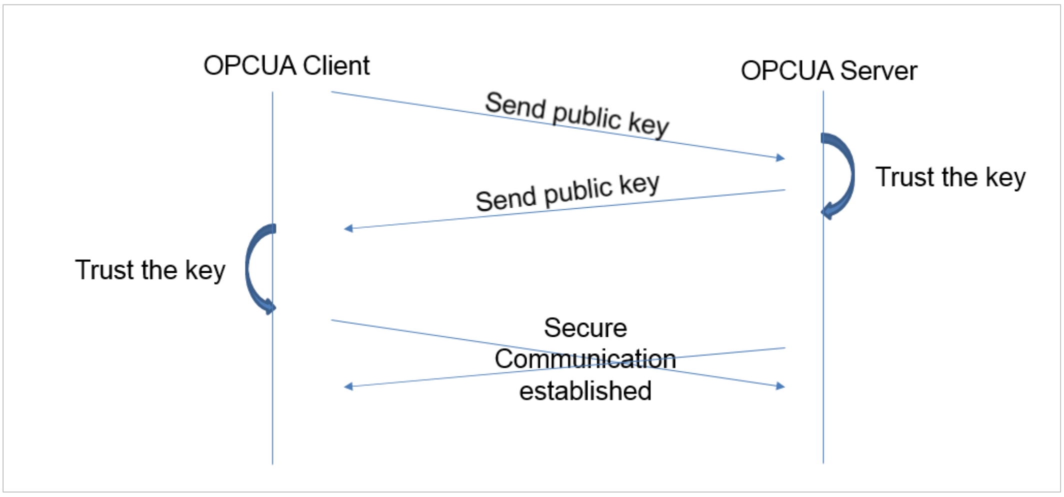


Fig. 2 OPC UA Secure Communication Exchange

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.

3.2.2 Certificates Setup

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

- encrypt
- sign
- authenticate

If the security policy requires to sign, the first connection will be a failure but will allow the Flexy to list the certificate that is not yet trusted, and so rejected. Once the certificate has been marked as trusted, the connection can then be established.

You dispose of 3 ways to log in to the Flexy OPC UA server:

- Anonymous: no credential required.
- Username/Password: one of the Flexy user credentials.
- Certificate: one of the listed certificate

If you chose the third option (certificate), the certificate exchange is automatic. You will have to trust the Flexy certificate, but the authentication certificate exchange is automatic.

If it is not the case (depending on your OPC UA client), you can download it from your Flexy through FTP or the GUI to paste it to your OPC UA client PKI.

These certificates are divided in 3 categories:

- Own: the server 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.

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

The certificates can be managed through FTP. All the operations (the PKI) can be done by switching certificates/keys from one folder to another one.

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.

> **!** If you are generating your own certificates (i.e.: because of facility network policy), the “urn” string must be included in the server certificate which value is “urn: localhost:ewon:ewontags”. If the “urn” is not provided the following error will be generated in the logs: *opcuasrv-Connect fail (BadCertificateUriInvalid)*.

3.3 OPC UA Client

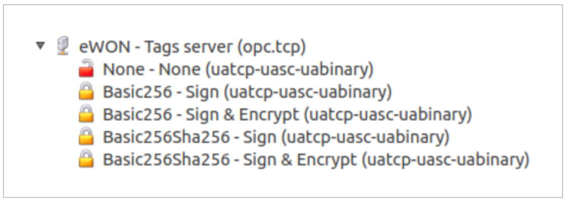
With OPC UA, there is no need to define and maintain a map of addresses for the tags you publish. The OPC UA protocol allows the client to simply browse the list of the available tags and the user only needs to pick up the tags he wants to monitor.

There is a limitation regarding the number of simultaneous clients that can connect to the same Flexy which is limited to 10 OPC UA clients.

3.3.1 UA Expert

The following configuration describes the steps to follow to get the “UA Expert” software, communicating with your Flexy and retrieving tag values through OPC UA.

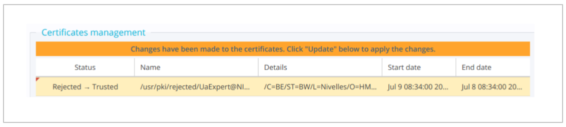
1. When configuring the communication from the UA Expert software to the Flexy, you will need to select the security policy that will be used



eWON - Tags server (opc.tcp)
- None - None (uatcp-uasc-uabinary)
- Basic256 - Sign (uatcp-uasc-uabinary)
- Basic256 - Sign & Encrypt (uatcp-uasc-uabinary)
- Basic256Sha256 - Sign (uatcp-uasc-uabinary)
- Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary)

Fig. 3 Selection of Security Policy

2. If you chose to sign, a first connection must be made. This first connection will be rejected by the Flexy.



Certificates management

Changes have been made to the certificates. Click "Update" below to apply the changes.

Status	Name	Details	Start date	End date
Rejected → Trusted	/usr/pki/rejected/UaExpert@NI...	/C=BE/ST=BW/L=Nivelles/O=HM...	Jul 9 08:34:00 20...	Jul 8 08:34:00 20...

Fig. 4 Trusting an Uploaded Certificate

This is the normal behavior: the first certificate exchange will always be rejected. You must go to the OPCUA server configuration page and use the PKI management tool to trust the certificate from UA Expert client.

Once the certificate has been accepted, perform once again a connection.

3. The OPC UA server can be reached through 3 ways

- Anonymous: no credentials required.
- Username/Password: use the credentials of a Flexy user.

- Certificate: use certificate to log in.

  If the third option (certificate) is chosen, the certificate exchange is automatic but not acceptance. You will still have to trust the certificate in the *Certificates management* frame, but the authentication certificate download is automatic.

  If the automatic exchange doesn’t occur (depending on your client), you can download the certificate from your Flexy via FTP or the GUI to copy it to your OPC UA client PKI.

Box 4126
300 04 Halmstad, Sweden

info@hms.se