Anybus® BY HMS NETWORKS

Enabling and Using OPC UA on Anybus CompactCom 40 IIoT Secure

APPLICATION NOTE

SCM-1202-169 1.0 en-US ENGLISH

HMS Connecting Devices™

Important User Information

Disclaimer

The information in this document is for informational purposes only. Please inform HMS Networks of any inaccuracies or omissions found in this document. HMS Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the 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.

Table of Contents

Page

1 Preface 3

1.1 Document History 3

1.2 Document Conventions 3

2 Setup and Configuration 4

2.1 Prerequisites 4

2.2 Update the Host Application 4

2.3 Certificates 4

2.4 Configuration 13

3 Use UaExpert 15

3.1 Connect to the Anybus CompactCom 40 15

3.2 Browse the Address Space 19

3.3 Subscribe to Monitor Application Data Instances 21

This page intentionally left blank

1 Preface

This document describes how to setup and configure an Anybus CompactCom 40 IIoT Secure device to enable OPC UA and how to connect and use the desktop client UaExpert.

More documentation and downloads can be found at www.anybus.com/support. For more info regarding OPC UA and UaExpert, please visit the manufacturer's support website.

1.1 Document History

Version	Date	Description
1.0	2020-10-xx	First release

1.2 Document Conventions

Numbered lists indicate tasks that should be carried out in sequence:

1. First do this
2. Then do this

Bulleted lists are used for:

- Tasks that can be carried out in any order
- Itemized information

► An action

→ and a result

User interaction elements (buttons etc.) are indicated with bold text.

```
Program code and script examples
```

Cross-reference within this document: *Document Conventions, p. 3*

External link (URL): www.hms-networks.com

WARNING
Instruction that must be followed to avoid a risk of death or serious injury.

Caution
Instruction that must be followed to avoid a risk of personal injury.

Instruction that must be followed to avoid a risk of reduced functionality and/or damage to the equipment, or to avoid a network security risk.

Additional information which may facilitate installation and/or operation.

2 Setup and Configuration

2.1 Prerequisites

- Download and install UaExpert from Unified Automation: www.unified-automation.com/products/development-tools/uaexpert.html
- Download and install an OPC UA Discovery server on a PC that the Anybus CompactCom 40 can access to get time synchronized.
  - Local discovery server from OPC Foundation: opcfoundation.org/developer-tools/developer-kits-unified-architecture/local-discovery-server-lds/. This server installs as a service on a Windows PC and needs no configuration.
- An Anybus CompactCom 40 series Ethernet IIoT Secure device supporting OPC UA.
- Possibility to modify and update the host application.

2.2 Update the Host Application

To enable the OPC UA server on the Anybus CompactCom 40, the OPC UA host object must be implemented in the host application. Attribute #1, OPC UA Model, must be set to the value 1. Other attributes are optional to implement to brand the identification of OPC UA on the network.

The definition of the OPC UA host object is available in the IIoT Secure Network Guide of each product (see www.anybus.com/support pages for Anybus CompactCom 40 EtherNet/IP and PROFINET).

> **!** Implementing attribute #1, OPC UA Model, of the OPC UA host object is required to enable OPC UA on Anybus CompactCom 40 devices.

2.3 Certificates

Certificates are needed in order to set up a secure OPC UA connection. Both the CompactCom and the OPC UA Client need to trust each other by installing the respective certificates in order to set up a secure connection. The following sections will deal with how to generate and install certificates in the CompactCom and in UaExpert.

2.3.1 Creating a CA Certificate

First, a CA certificate must be generated, e.g., by using the Anybus Certificate Generator. The Anybus Certificate Generator can be downloaded from www.anybus.com/support.

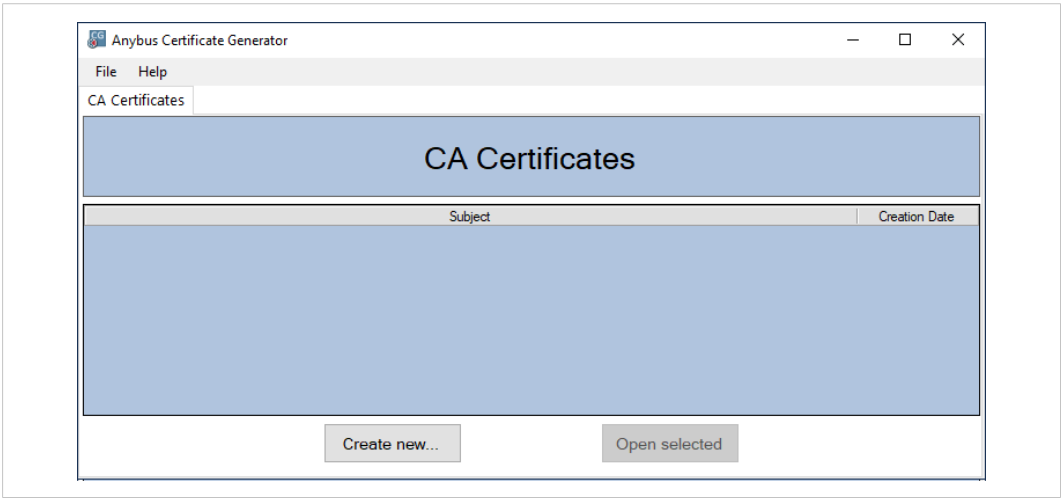


Fig. 1

1. Click the 'Create new…' button.
2. Fill out the requested fields (fields marked with * are mandatory).

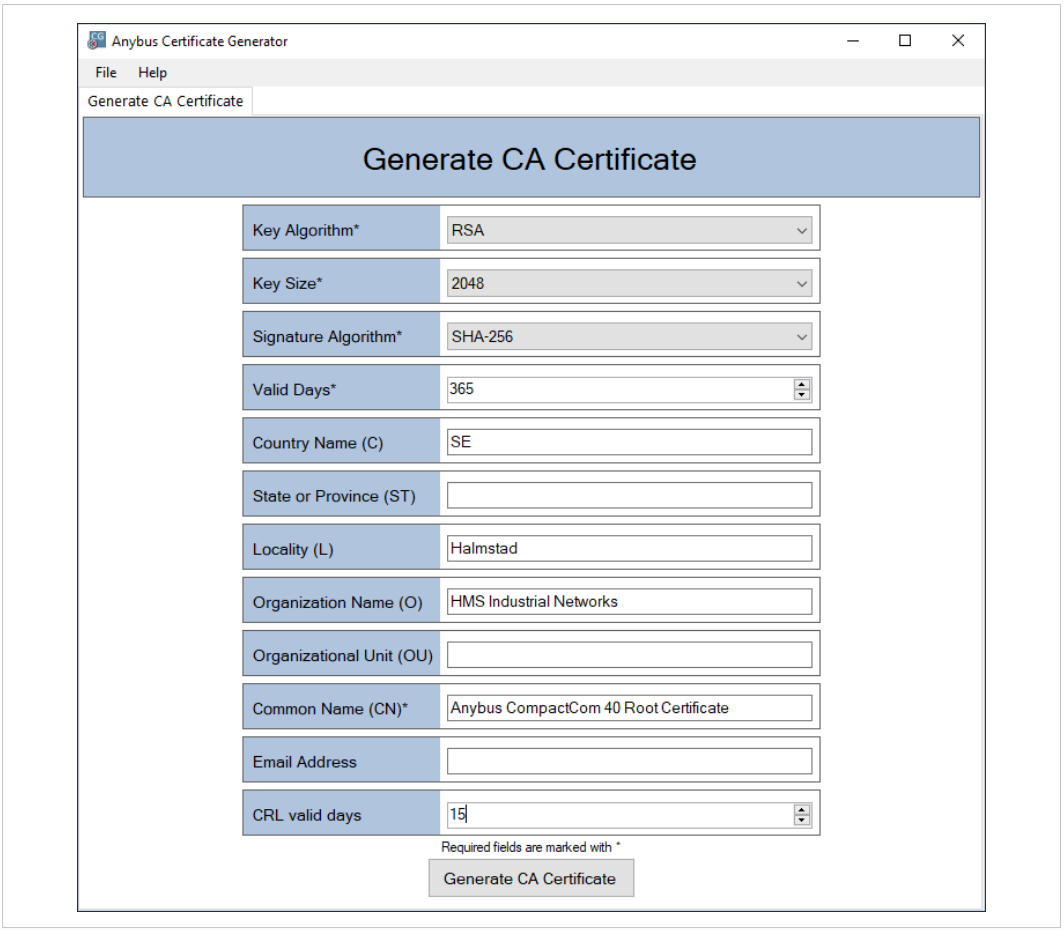


Fig. 2

3. Click ‘Generate CA Certificate’. The CA certificate is generated and can now be used to generate device certificates.

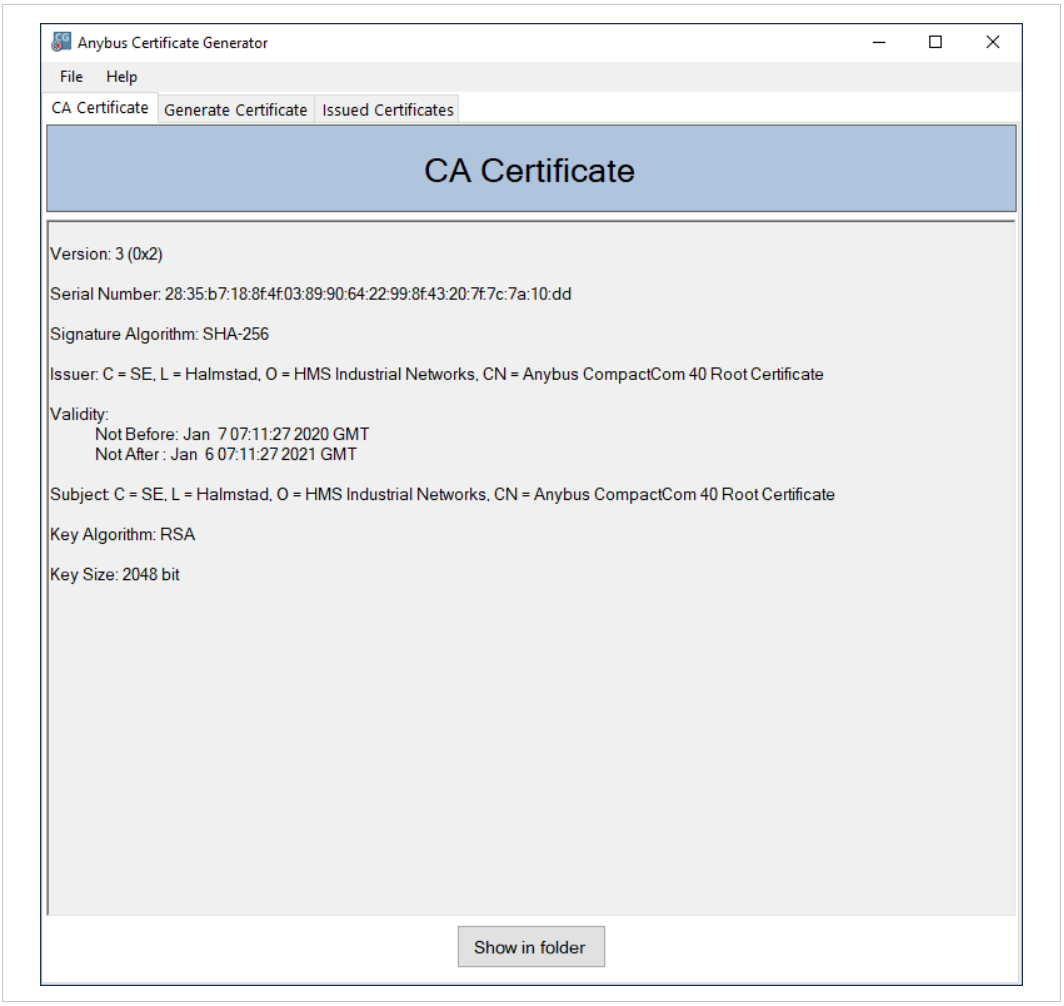
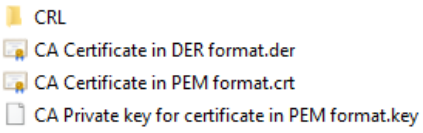


Fig. 3

4. To access the certificate, click on the ‘Show in folder’ button.

Folder contents:



- CA Certificate... is the CA certificate itself.
- CA Private key... is the private key for the CA certificate.
- The CRL-folder contains an empty Certificate Revocation List.
- Other folders hold the device certificates generated from this CA certificate.

2.3.2 Creating a Device Certificate

A Device Certificate for the CompactCom must be generated.

1. Click on the ‘Generate Certificate’ tab.
2. Fill out the requested fields (fields marked with * are mandatory).

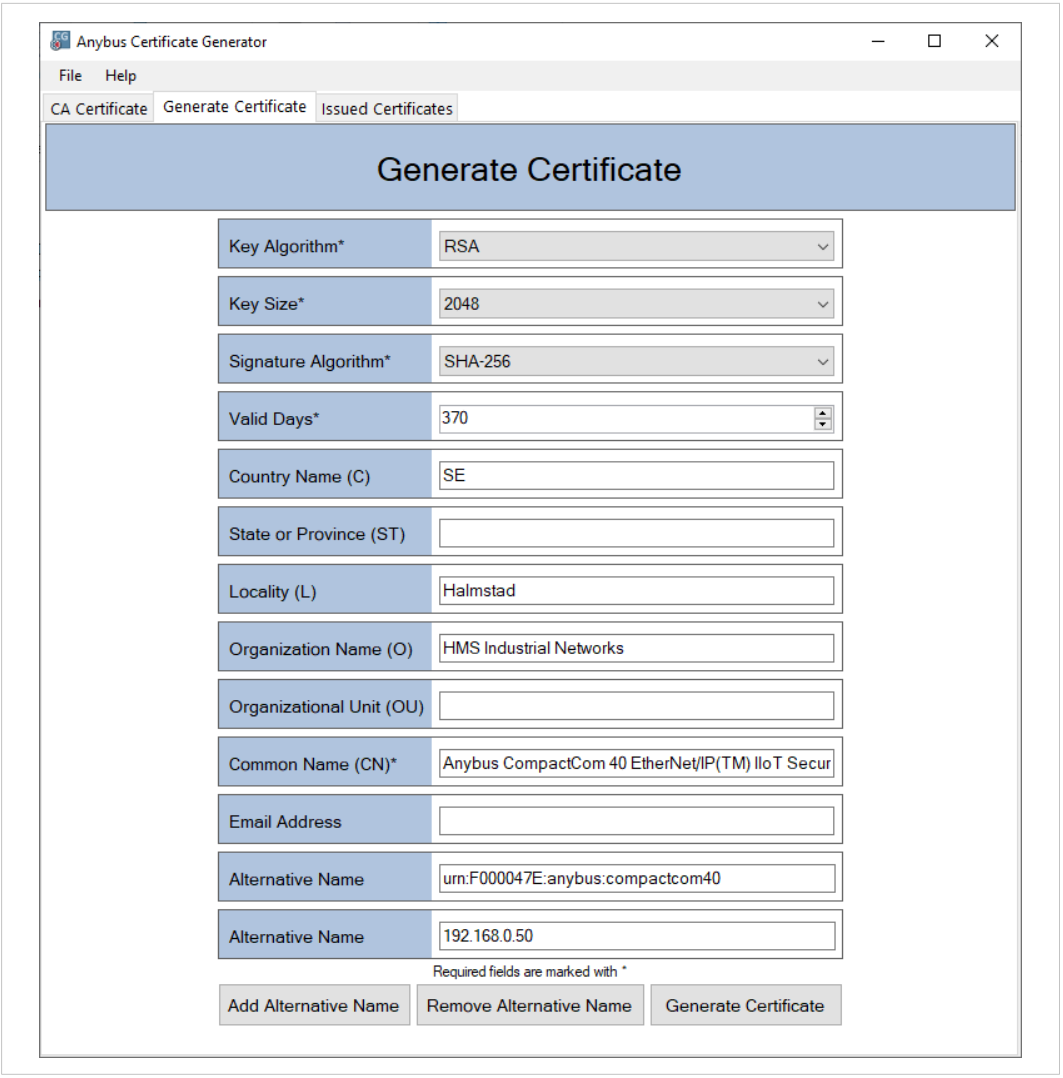


Fig. 4

For certificates intended for use with OPC UA, the following fields must be present with the specified contents.

Common Name (CN): Must match the Product Name (Application Object (FFh), Attribute 9. NOTE: Some network objects have a product name attribute that will override this attribute).

- For EtherNet/IP, the default value is ‘Anybus CompactCom 40 EtherNet/IP(TM) IIoT Secure’.
- For PROFINET, the default value is ‘Anybus CompactCom 40 PROFINET IRT IIoT Secure’.

Alternative Name: Must match the Application URI (OPC UA Object (E3h), Attribute 2).

- The default value is ‘urn:<hostname/serialnumber>:anybus:compactcom40’

Alternative Name: Must match the IP number or URL including host name, if configured.

3. Click the ‘Generate Certificate’ button.

4. The certificate is generated and is now visible on the ‘Issued Certificates’ tab.

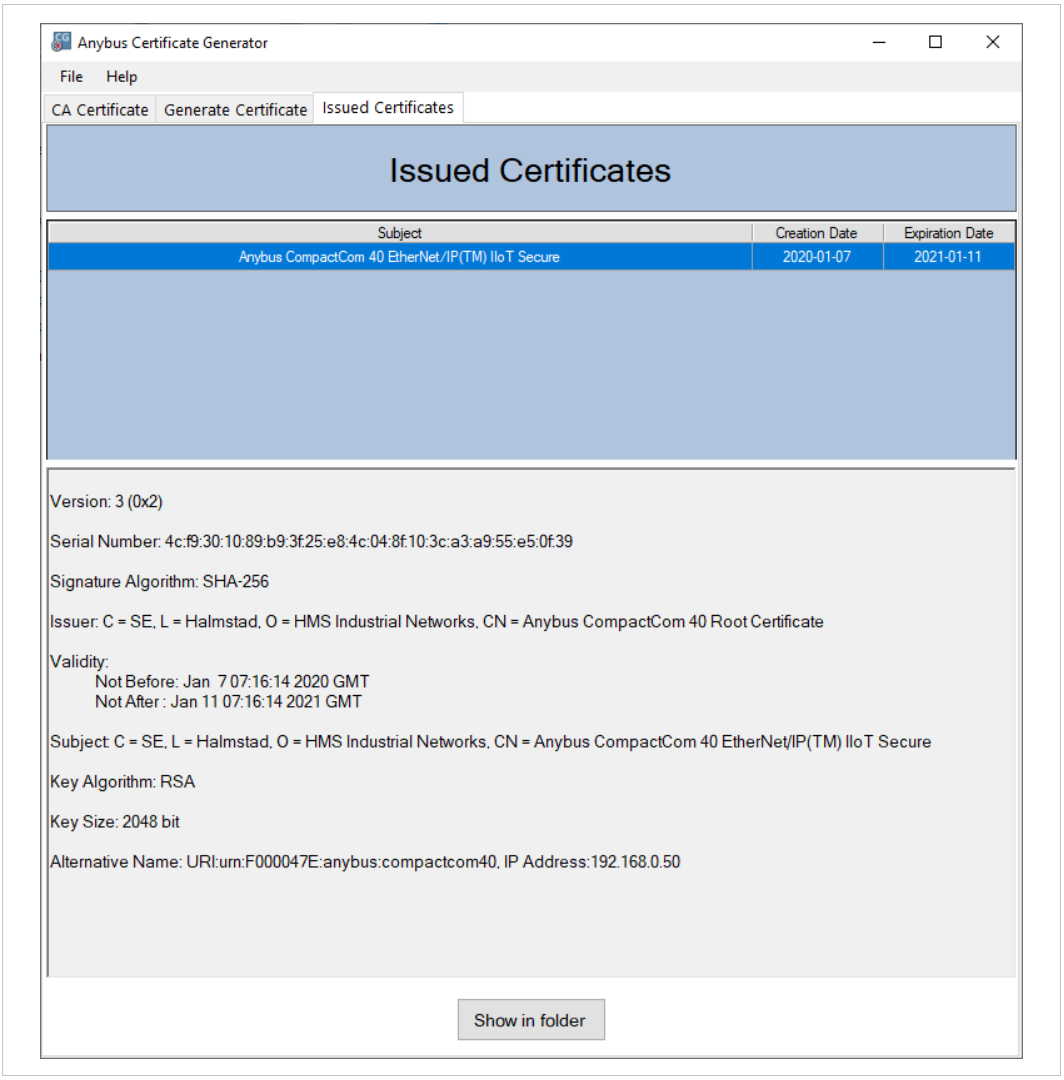
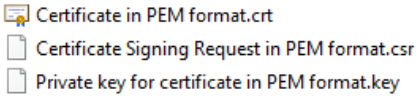


Fig. 5

5. To access the certificate, click on the ‘Show in folder’ button.

Folder contents:



2.3.3 Installing Certificates in the Anybus CompactCom

The Device Certificate shall be installed in the CompactCom device via the website. Do the following:

1. Browse to the CompactCom website and login with an account with administrator rights.
2. Install the certificate in the CompactCom – 'Certificates->Install a device certificate'.
3. Enable the certificate for use with OPC UA by checking the usage checkbox.
4. Click 'Apply'.
5. Restart the CompactCom for the changes to take effect.

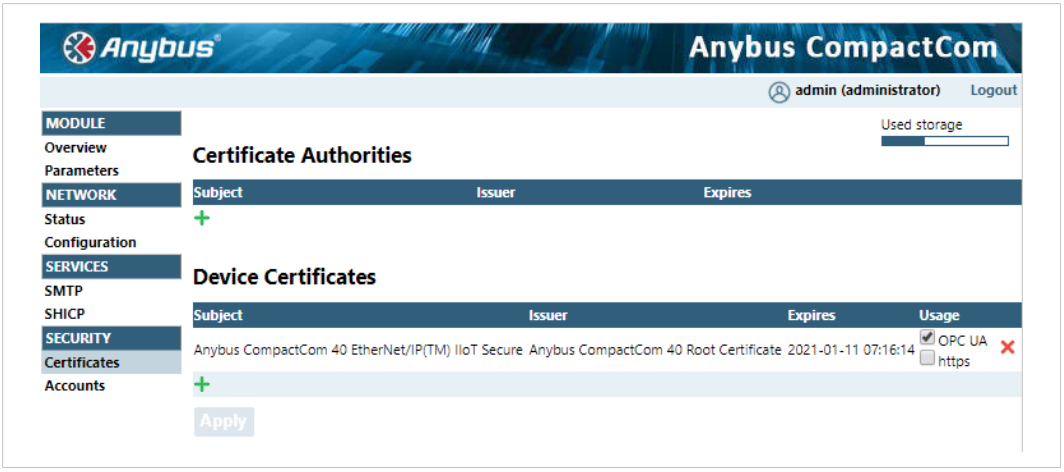
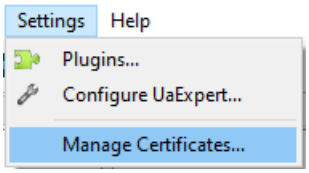


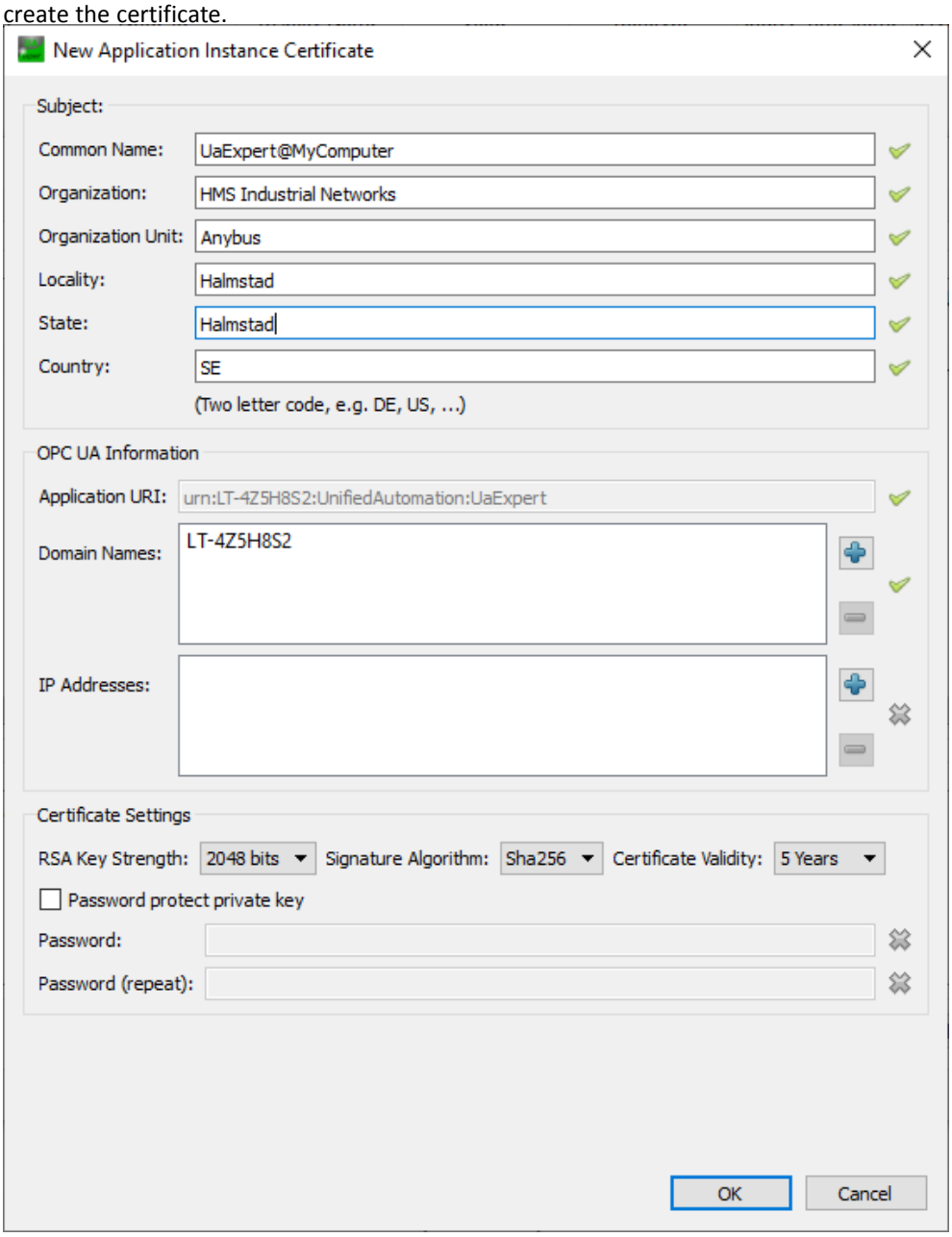
Fig. 6

The Application Certificate from UaExpert shall then be installed in the CompactCom via the website. When installing UaExpert, a dialogue will appear where the client certificate is configured and generated.

1. Start UaExpert.
2. Select 'Settings->Manage Certificates' in the menu.



3. Click ‘Create new Application Certificate…’, if the ‘Own Certificate’ was not already created when installing UaExpert. Follow the instructions and fill out the information needed to create the certificate.



4. Click ‘Copy Application Certificate To…’ to save the certificate (uaexpert.der) to a folder of your choice.
5. Convert the certificate from DER-format to PEM-format, e.g. by using the converter at https://sslshopper.com/ssl-converter.html or by using the conversion function in OpenSSL.
6. Browse to the CompactCom website and login with an account with administrator rights.
7. Install the certificate in the CompactCom – ‘Certificates->Install a CA certificate’.

8. Restart the CompactCom for the changes to take effect.

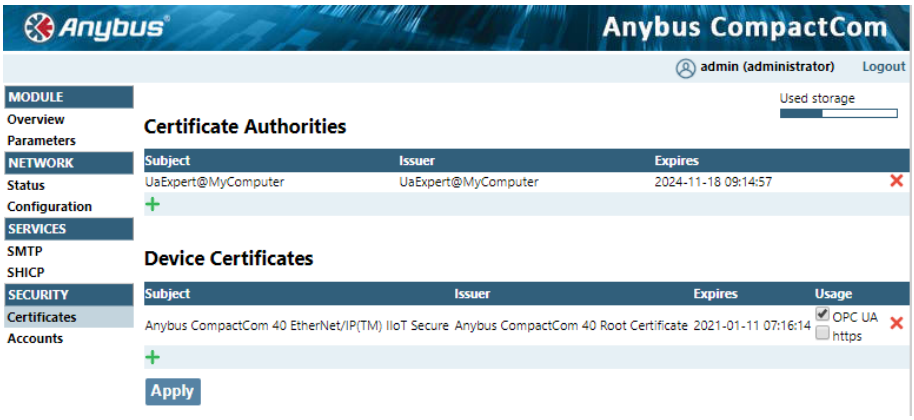


Fig. 7

2.3.4 Installing Certificates in UaExpert

The CA Certificate that was used when generating the Device Certificate to the CompactCom shall be installed in UaExpert. The easiest way to find the CA Certificate is to start the Anybus Certificate Generator, open the specific certificate, and click 'Show in folder' (the CA certificate in DER format, '.der', is the certificate to use).

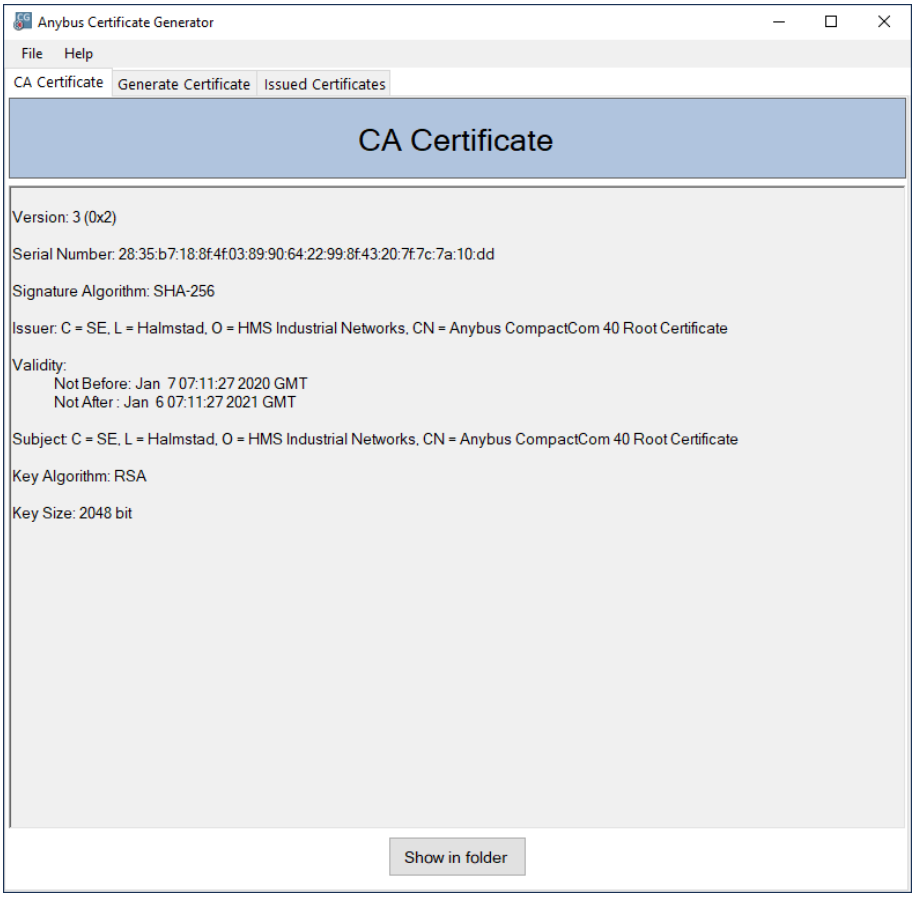
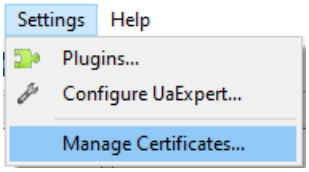


Fig. 8

1. Start UaExpert
2. Select ‘Settings->Manage Certificates’ in the menu.



3. Click ‘Open Certificate Location’.
4. Copy the CA Certificate to the folder that pops up (remember to use DER format).
5. Copy the CRL for the CA certificate to the trusted crl-folder (go back one folder).
6. Click refresh. The certificate will show up as a trusted certificate and the CRL will show up as a trusted CRL. Now, all devices with a device certificate based on this CA certificate will be trusted by UaExpert.

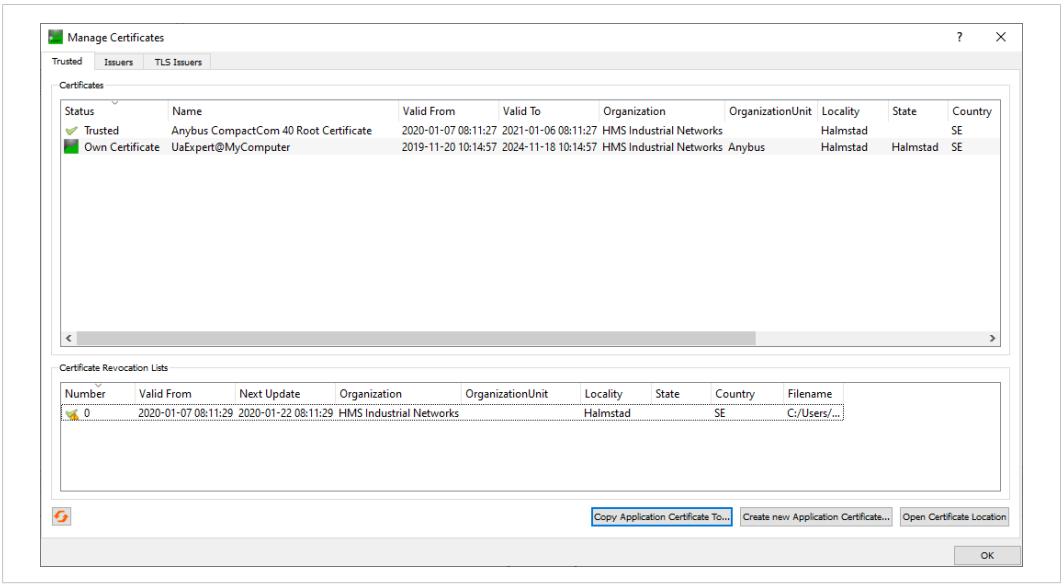


Fig. 9

2.4 Configuration

An easy check to verify that OPC UA is enabled when the module has started, is to enter the configuration web page of the module. An OPC UA Configuration section shall be present containing fields to configure the Network Configuration object instances related to OPC UA. It is possible to specify what port the OPC UA server of the CompactCom 40 device listens to and the URL to the Discovery server to be accessed to get time synchronized.

Configure the Discovery Server URL to point to the PC where the Discovery Server is installed. The format of the URL must be: `opc.tcp://<ip address or hostname>:<port>`. The port is optional. If it is absent, the default port 4840 will be used.

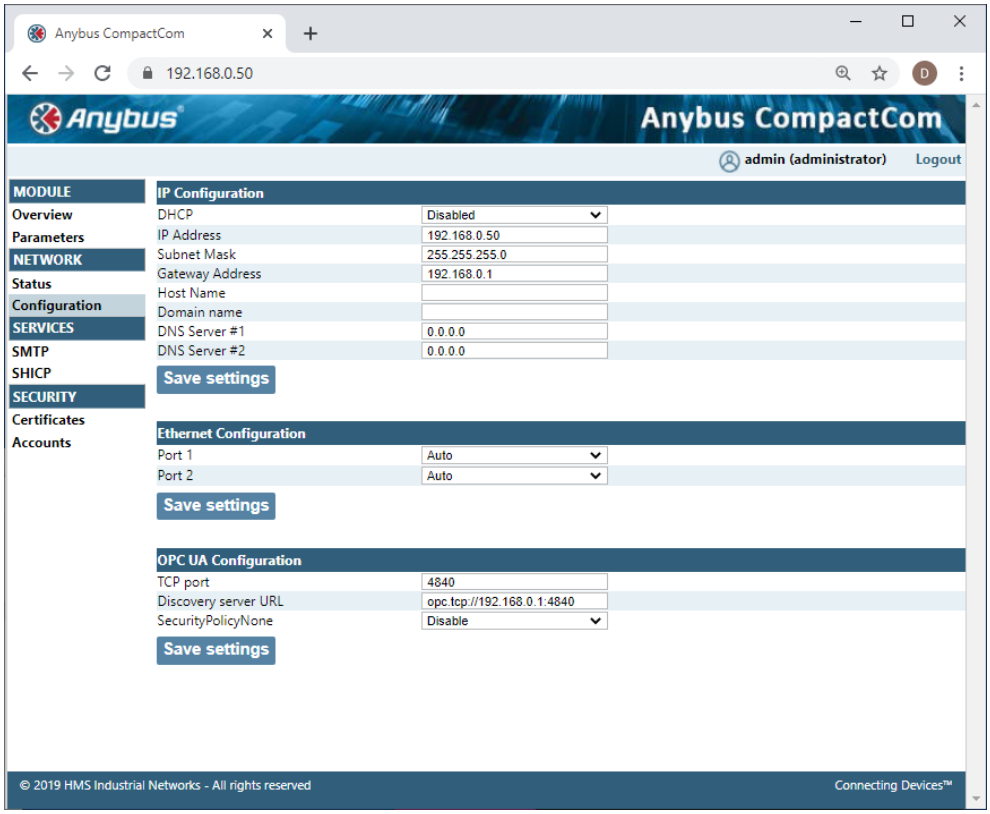


Fig. 10

> **!** To get Application Data Instance values timestamped correctly and to get valid timestamps in the responses from the Anybus CompactCom 40 device a valid Discovery Server URL must be configured.

2.4.1 Roles and Users

Roles and Users must be configured in the CompactCom according to the network guide.

By default, Admin and Operator roles have OPC UA access (stated in vfs/opcua.cfg). By adding an opcua.cfg file to the root of the file system of the CompactCom the default file will be overridden, and other roles can be configured for OPC UA access.

Default contents of vfs/opcua.cfg:

```
[Access]
administrator
operator
user:r,b
```

In order to access the entire file system with the default roles, Admin Mode must be enabled in the Ethernet Host Object (F9h), Attribute #7.

3 Use UaExpert

3.1 Connect to the Anybus CompactCom 40

When starting UaExpert a new project will be loaded automatically. To add the CompactCom 40 device to the project, right click on the Servers folder of the Project window. Select “Add…” in the drop-down menu.

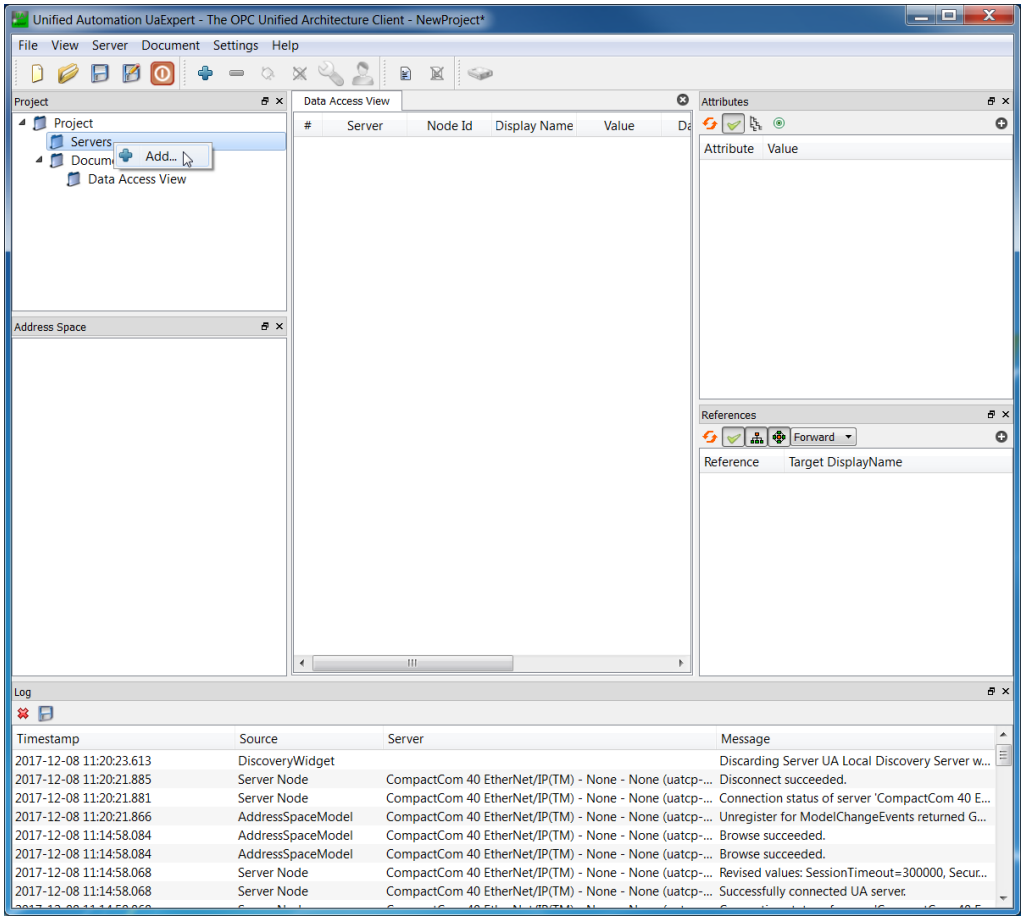


Fig. 11

A new dialog window, “Add Server”, shall pop up. On the Discovery tab, add the CompactCom 40 device in the Custom Discovery section by double clicking on the “Double click to Add Server…” option.

Enter the IP address of the device in the format `opc.tcp://<ip-address or hostname>:<port>`, e.g. `opc.tcp://192.168.0.10`. If no port is specified, UaExpert will use the default TCP port 4840.

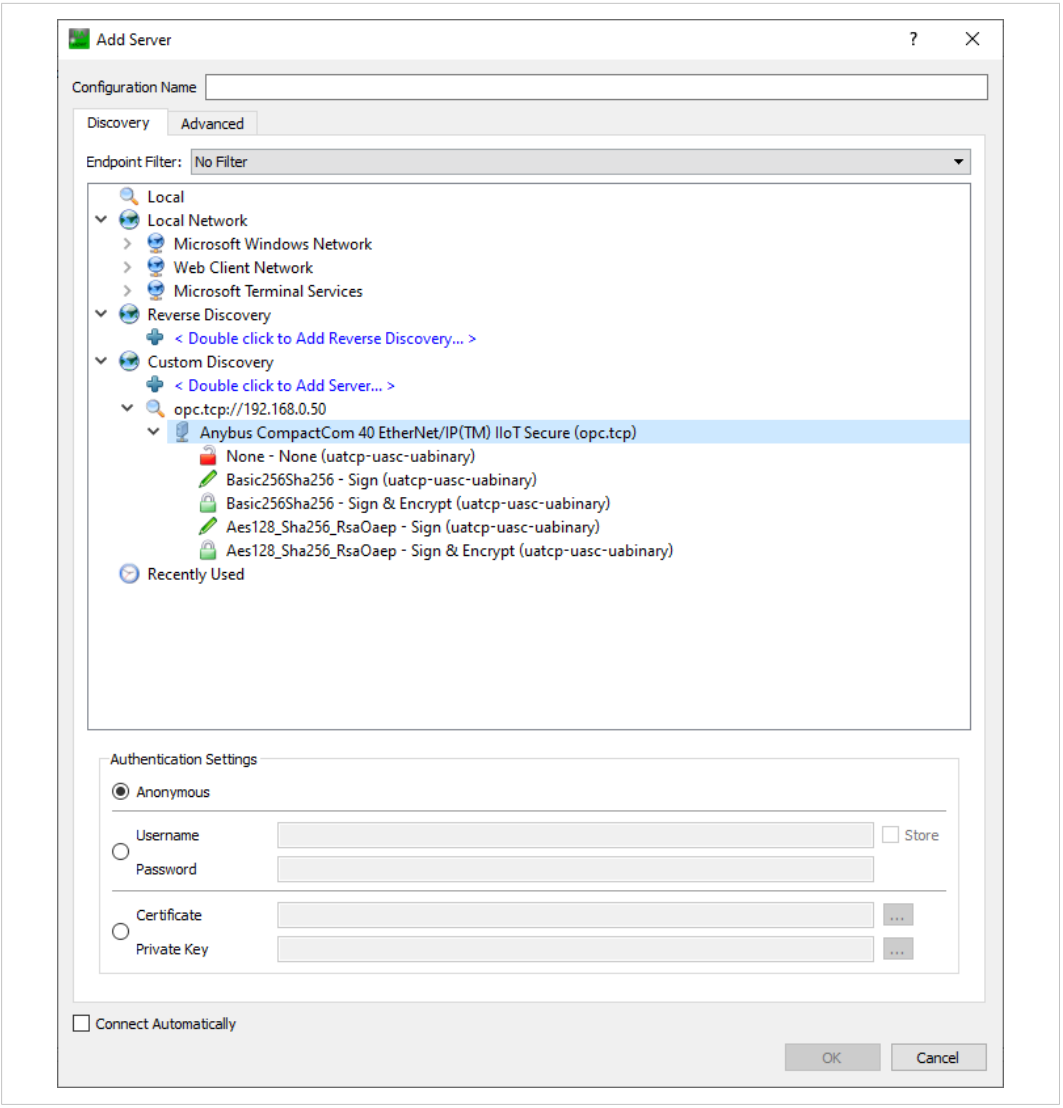


Fig. 12

When the module has been added, expand it to find the available OPC UA server on the module. Then expand the OPC UA server to see available endpoints to connect to.

Available endpoints:

Endpoint	Sign	Encrypt
None	No	No
Basic256Sha256	Yes	No
Basic256Sha256	Yes	Yes
Aes128_Sha256_RsaOaep	Yes	No
Aes128_Sha256_RsaOaep	Yes	Yes

Select the endpoint to use. Username and Password can also be entered here (if stored, the user does not have to fill it out at every connect).

*For debugging purposes, select the endpoint **SecurityPolicy - None** to be able to see the information in e. g. Wireshark.*

Press the OK button to confirm the addition of the CompactCom 40 device to the UaExpert project.

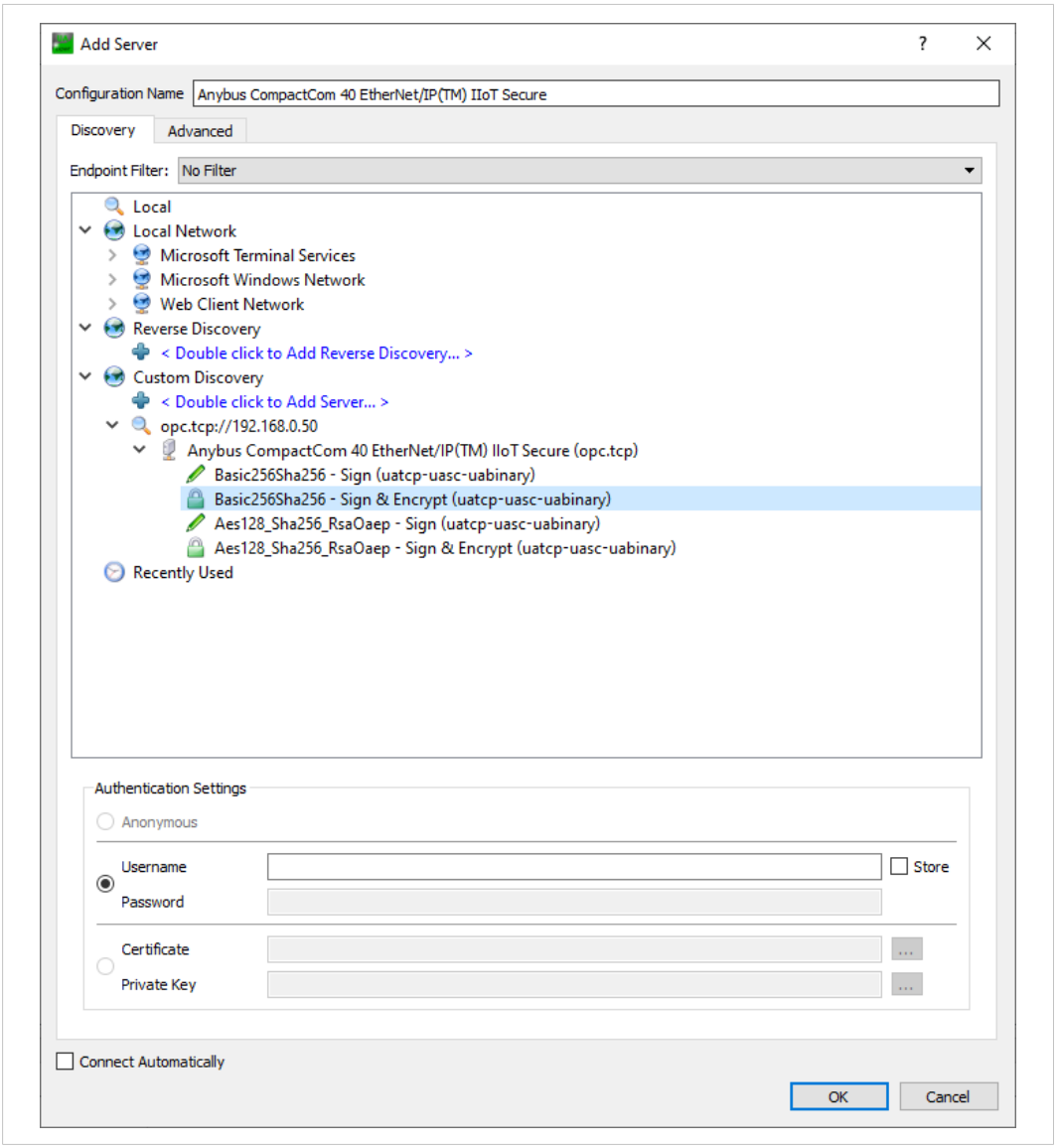


Fig. 13

When the CompactCom 40 device has been added to the UaExpert project, it is possible to right click on the entry representing the CompactCom 40 device in the Servers folder of the project view. Click on the “Connect” option in the drop-down menu to connect to the device.

If “Username/password” was not already entered in the Authentication Settings when adding the device, UaExpert will now ask for this information.

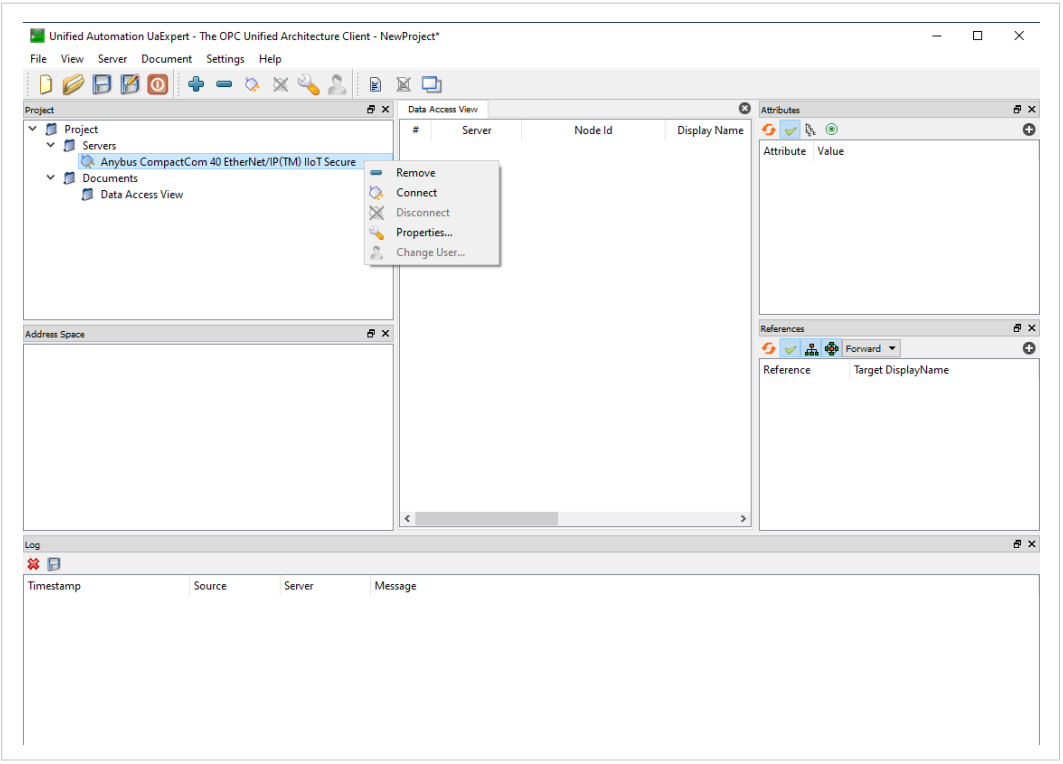


Fig. 14

3.2 Browse the Address Space

Once connected, UaExpert will present the Address space of the device in the Address Space window (1). The address space can be browsed manually by expanding the folders and objects visible in the Address Space window. At the bottom UaExpert presents a log of events (2). If it fails to connect to the device or the Address Space is not populated as expected, it is recommended to take a look at this log to figure out the problem.

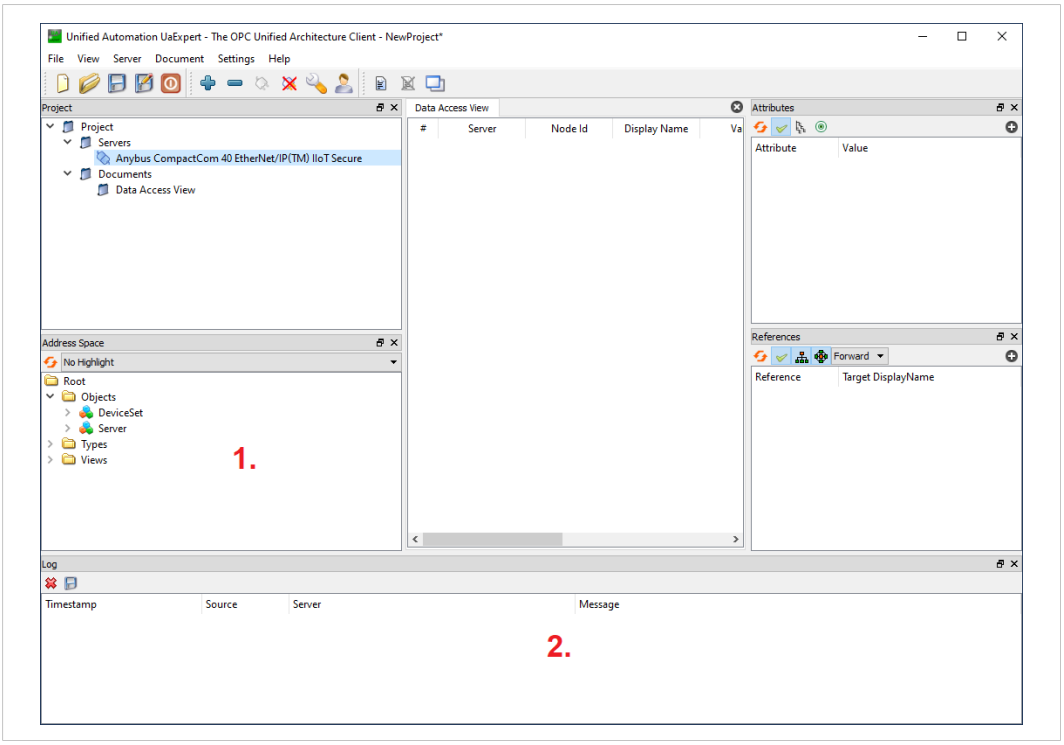


Fig. 15

When browsing the address space, it is possible to select any node to get more details about it. When a node has been selected in the Address Space window, all attributes of the node are presented in the Attributes window (1). All nodes always have a mandatory base set of attributes, then different node classes may specify additional attributes as well, both mandatory and optional ones.

The references of the selected node are presented in the References window (2). By default only forward references are shown. But there is a drop-down list that offers the possibility to show inverted references or references in both directions.

The Address Space window, the Attributes window and the References window also have a refresh button which forces UaExpert to reload the information presented in the window by requesting it from the device.

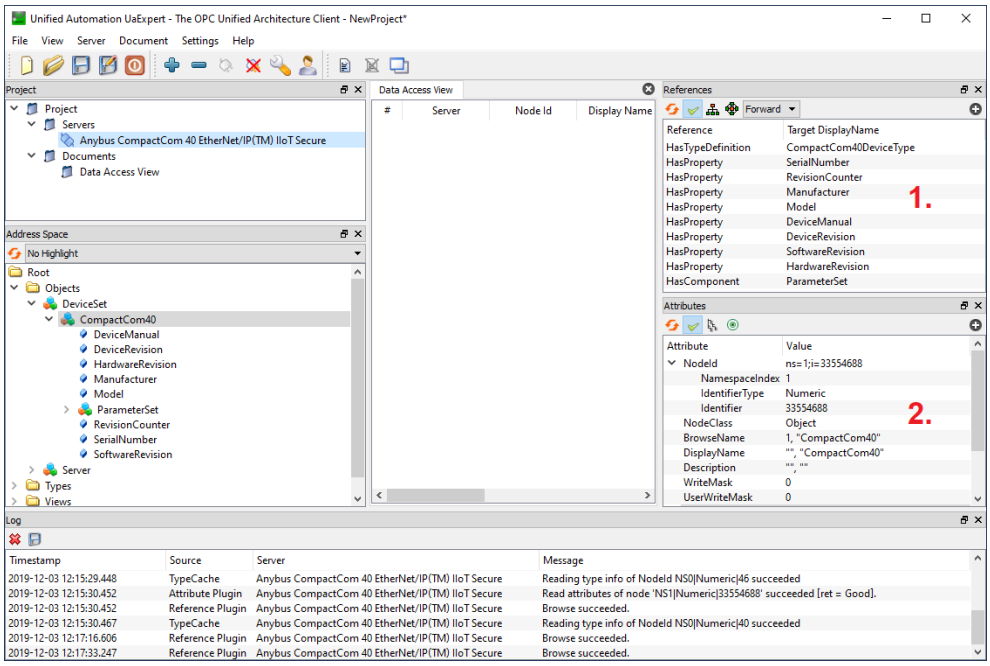


Fig. 16

3.3 Subscribe to Monitor Application Data Instances

The Application Data Instances are present in the ParameterSet of the device in the address space. By selecting the node it is possible to see the current value of the Application Data Instance in the Attributes window.

To setup a subscription and monitor the value of an Application Data Instance, drag and drop one of the variable nodes from the ParameterSet into the Data Access View tab. UaExpert will display the current value of the parameter, its data type, timestamp when latest value was received etc. The OPC UA implementation has support for 10 subscriptions with up to 100 monitoredItems in total.

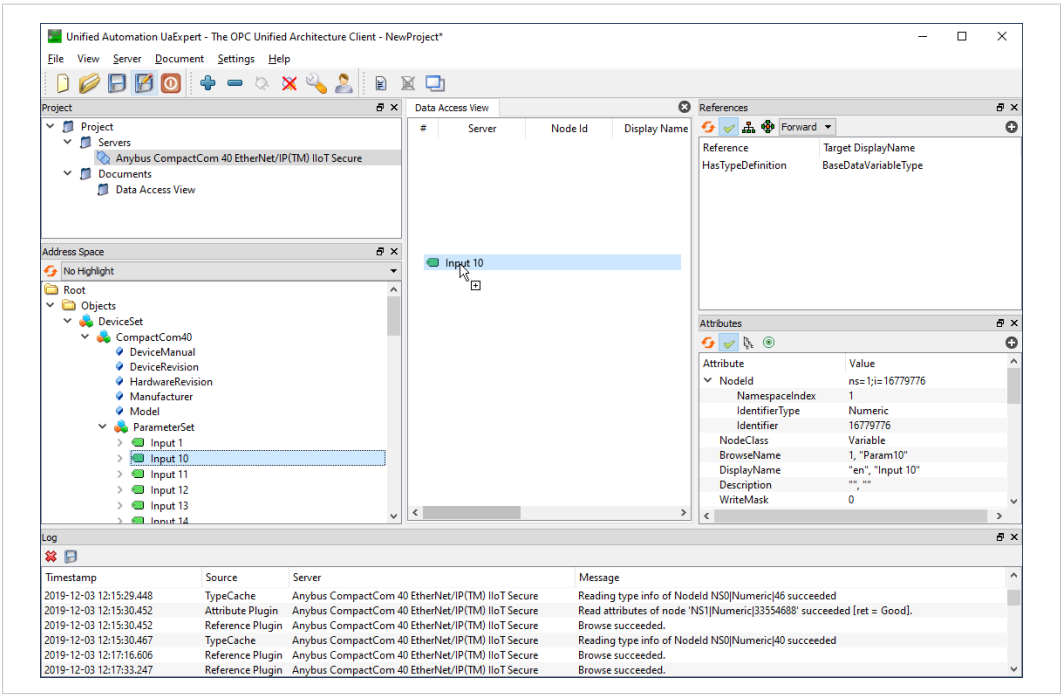


Fig. 17

© 2020 HMS Industrial Networks
Box 4126
300 04 Halmstad, Sweden

info@hms.se

SCM-1202-169 1.0 en-US / 2020-10-28 / 20471