UC20-SL2000-OLAC

2638920000

Quick Start Guide secure connection via OPC-UA

Establishing a secure connection between an OPC-UA test client and the controller

QSG0017v-02-UC20

Revision history

Version	Date	Change log
01	2019-11	First released version
02	2020-07	Review before web launch

Contact

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14-292083
info@weidmueller.com
www.weidmueller.com

For further support please contact your local sales representative.

Author: w010485

1. Content

2. Warning and disclaimer

Warning
Controls may fail in unsafe operating conditions, causing uncontrolled operation of the controlled devices. Such hazardous events can result in death and / or serious injury and / or property damage. Therefore, there must be provide safety equipment/ electrical safety design or other redundant safety features that are independent from the automation system.

Disclaimer
This Example / Application Note does not relieve you of the obligation to handle it safely during use, installation, operation and maintenance. Each user is responsible for the correct operation of his control system. By using this program example / application note prepared by Weidmüller, you accept that Weidmüller cannot be held liable for any damage to property and / or personal injury that may occur because of the use.

Note
The application examples do not represent customer-specific solutions, they are simply intended to help for typical tasks. The user is responsible for the proper operation of the described products. This application example does not relieve you of the obligation of safe use, installation, operation and maintenance. Application examples are not binding and do not claim to be complete in terms of configuration as well as any contingencies.
By using this Application Example, you acknowledge that we cannot be held liable for any damages beyond the described liability regime. We reserve the right to make changes to this sample application at any time without notice.
In case of discrepancies between the proposals in the application example and other Weidmüller publications, like manuals, such contents always have more priority to the examples.
We assume no liability for the information contained in this document. Our liability, for whatever legal reason, for damages caused by the use of the examples, instructions, programs, project planning and performance data, etc. described in this application example is excluded.

Security notes
In order to protect equipment, systems, machines and networks against cyber threats, it is necessary to implement (and maintain) a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorized access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards (such as firewalls and network segmentation) have been taken.

3. Abstract

The scope of this document is to show how a secure connection between the u-control SL2000 and an OPC-UA test client can be established. This quick start guide uses the Unified Automation UaExpert client, that can be downloaded here:

https://www.unified-automation.com/products/development-tools/uaexpert.html

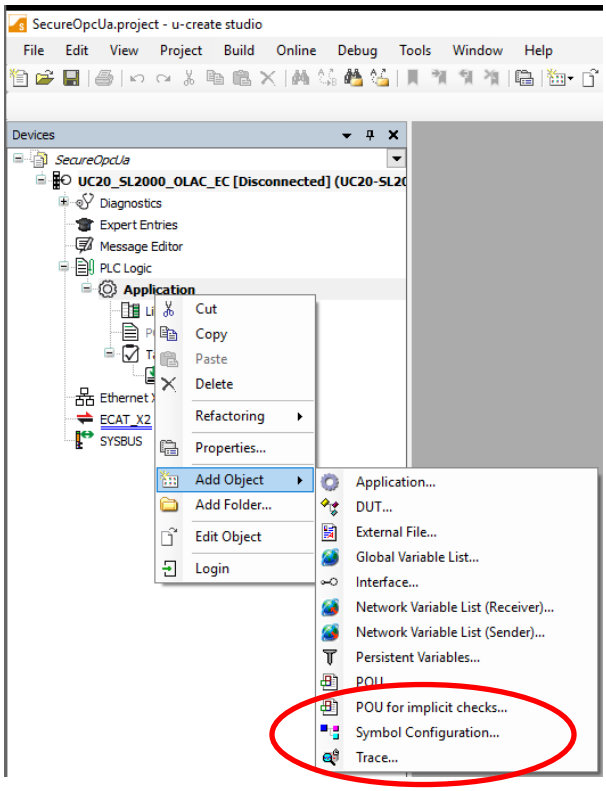
To understand the content of this document, basic knowledge about handling projects in u-create studio is required. All programming snippets are written in structured text. Basic knowledge about Linux operating systems is also required.

4. Setting up the OPC-UA server

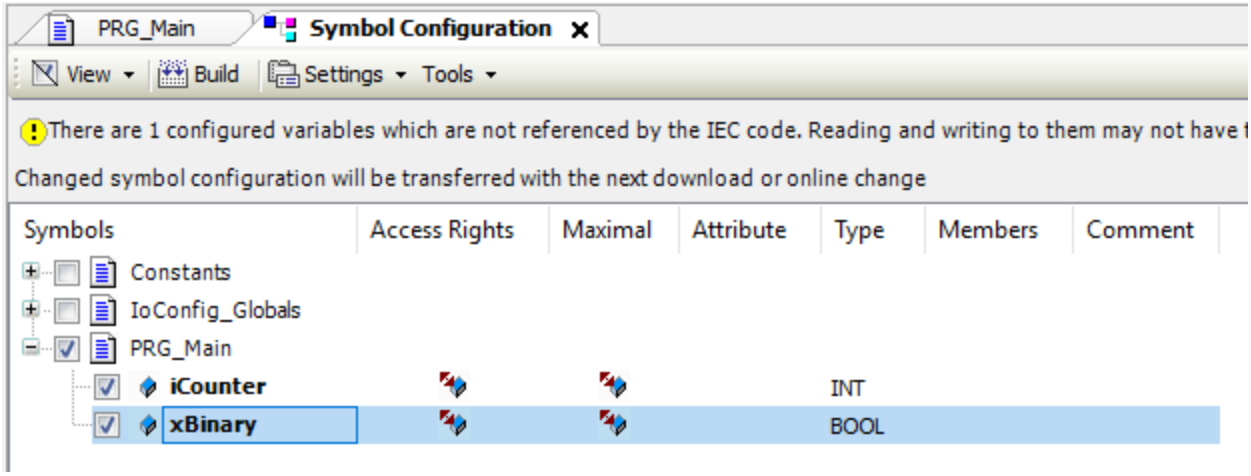
The server is not part of the plc runtime by default. It must be installed and configured by the user. Once it is installed, it is also required to add plc variables to it. The following section guides the reader through this process.

4.1. Adding PLC variables to the server

Variables that shall be exchanged via OPC-UA must be added to the symbol configuration. The picture below shows how a symbol configuration is added to a controller in a new project.

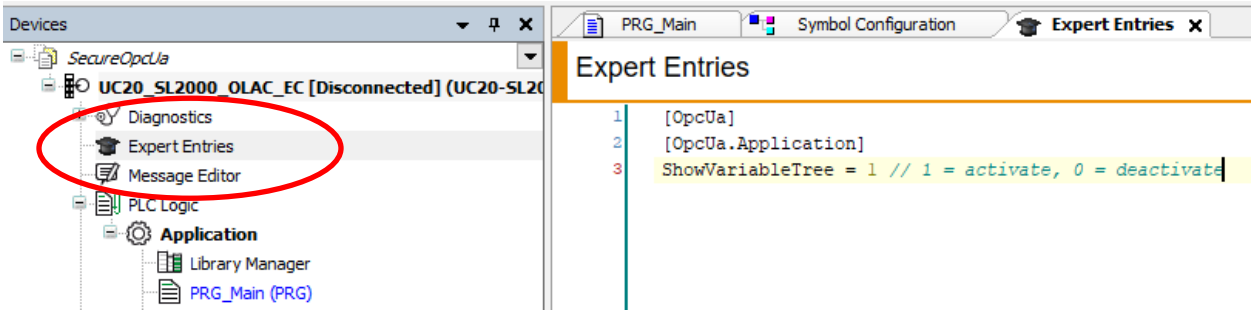


The picture below shows how variables are added to the symbol configuration. In this scenario, two variables from the program “PRG_Main” are added.



4.2. Allowing to browse the variable server through OPC-UA

There are two possible ways to make the variables available for the client. The first and most secure is to create an own information model. However, sometimes there are too many variables needed, which makes this very time consuming for the programmer. In this case, u-create studio offers the possibility to make the complete variable server available via OPC-UA.

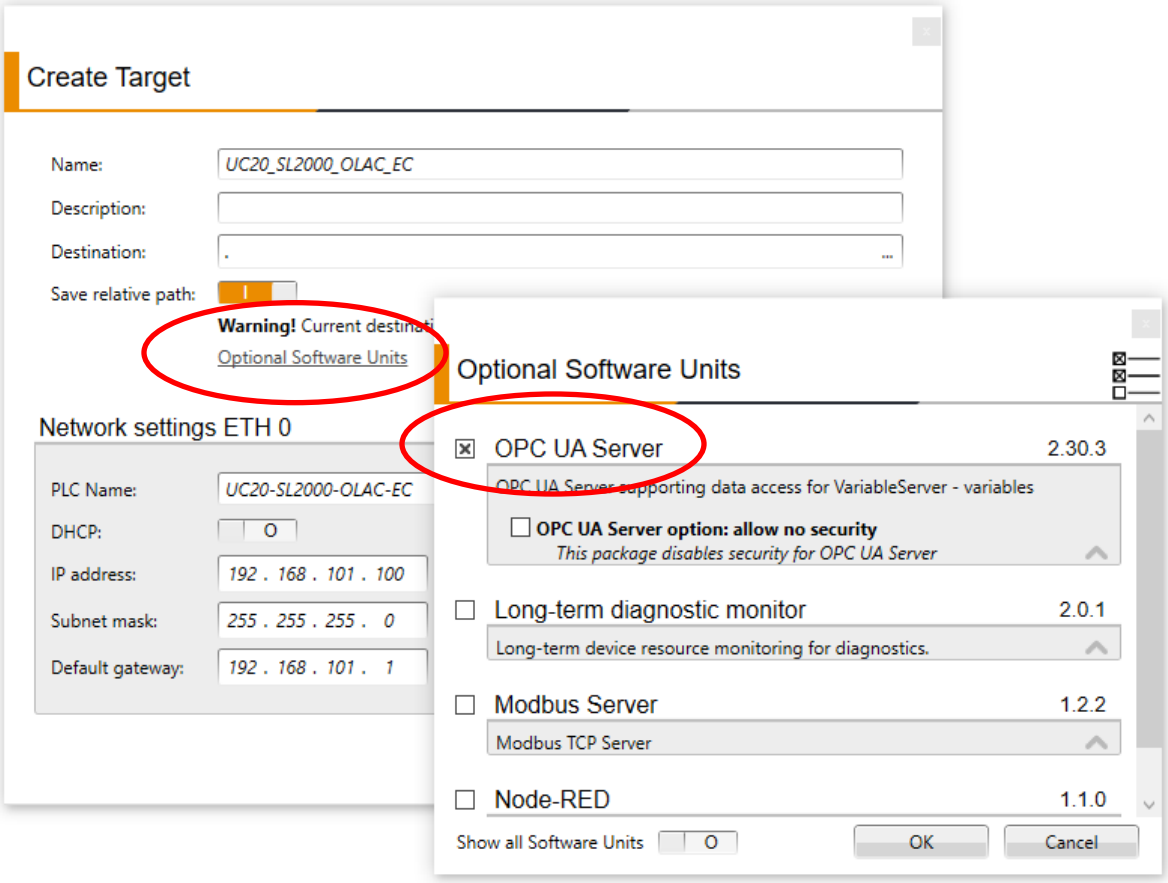


The picture above shows how the OPC-UA server is configured to add the complete variable server to it. The configuration is done in the expert entries of the controller.

Warning: This option makes ALL variables of the variable server available via OPC-UA. If there are security issues in having the complete variable server available, please refer section 0 to create your own information model!

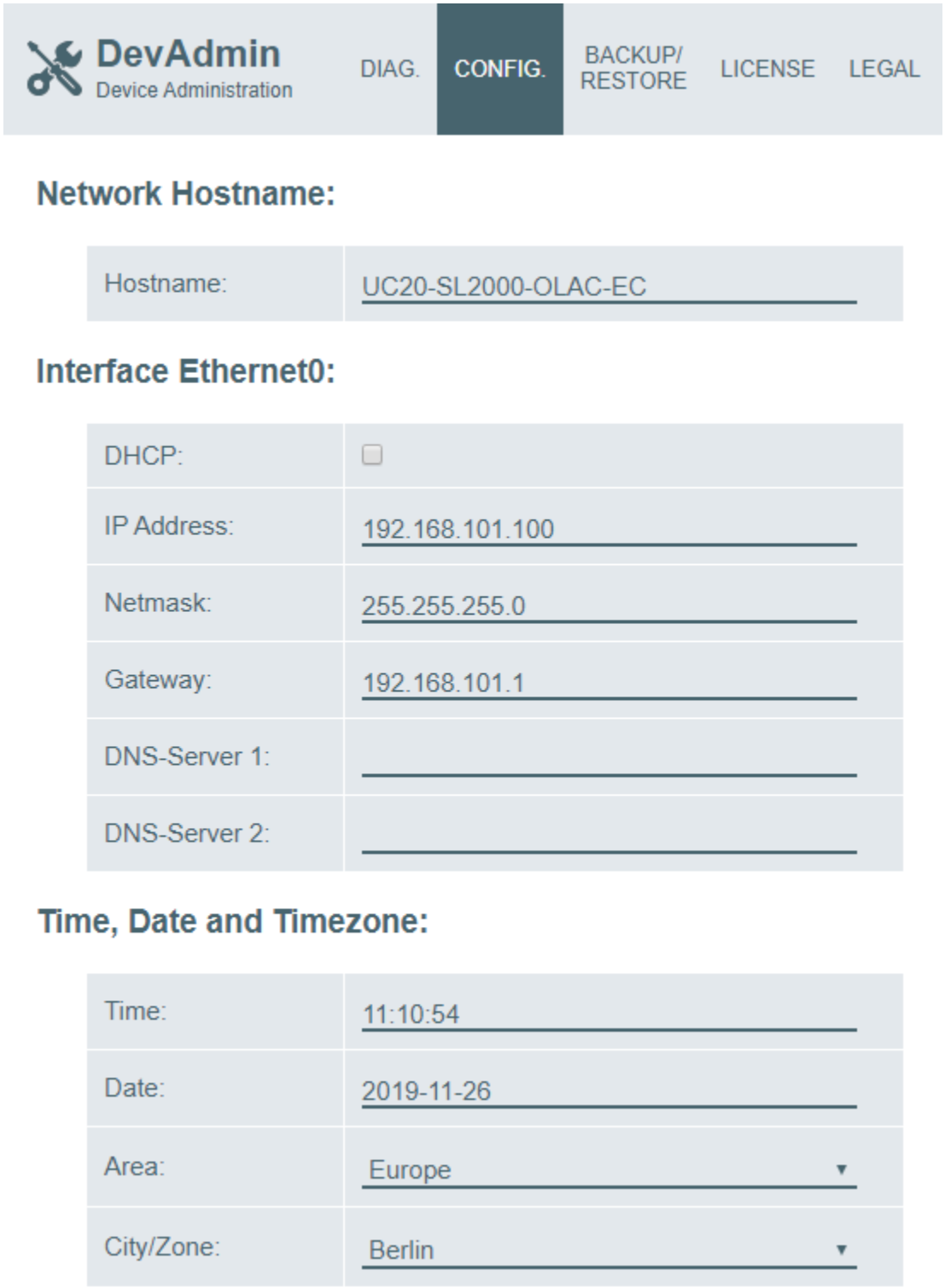
4.3. Configuring the target and licensing

After the u-create studio project has been configured, a target that includes the OPC-UA server, needs to be created. “Project -> Create Target” opens the dialogue shown in the picture below.

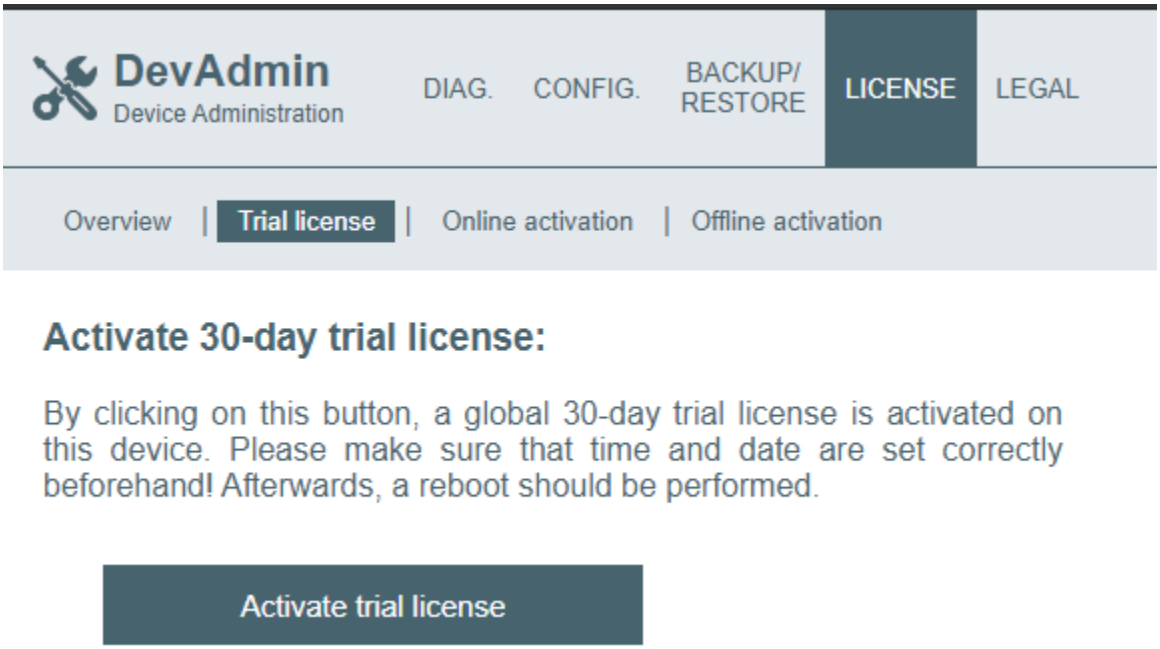


The optional package “OPC UA Server” adds the OPC-UA server to the target. The option “allow no security” allows unsecure connections. It should just be used in case of testing approaches during development phase.

Once the target has been installed, the OPC-UA server needs a license to work properly. Before a license can be activated, the clock needs to be set to current time. This can be done via “DevAdmin” side, see picture below.



To enter the “DevAdmin” web side, enter the controllers IP-addressee into the web browser. Once the clock das been set to current time and proper time zone, a license can be activated.

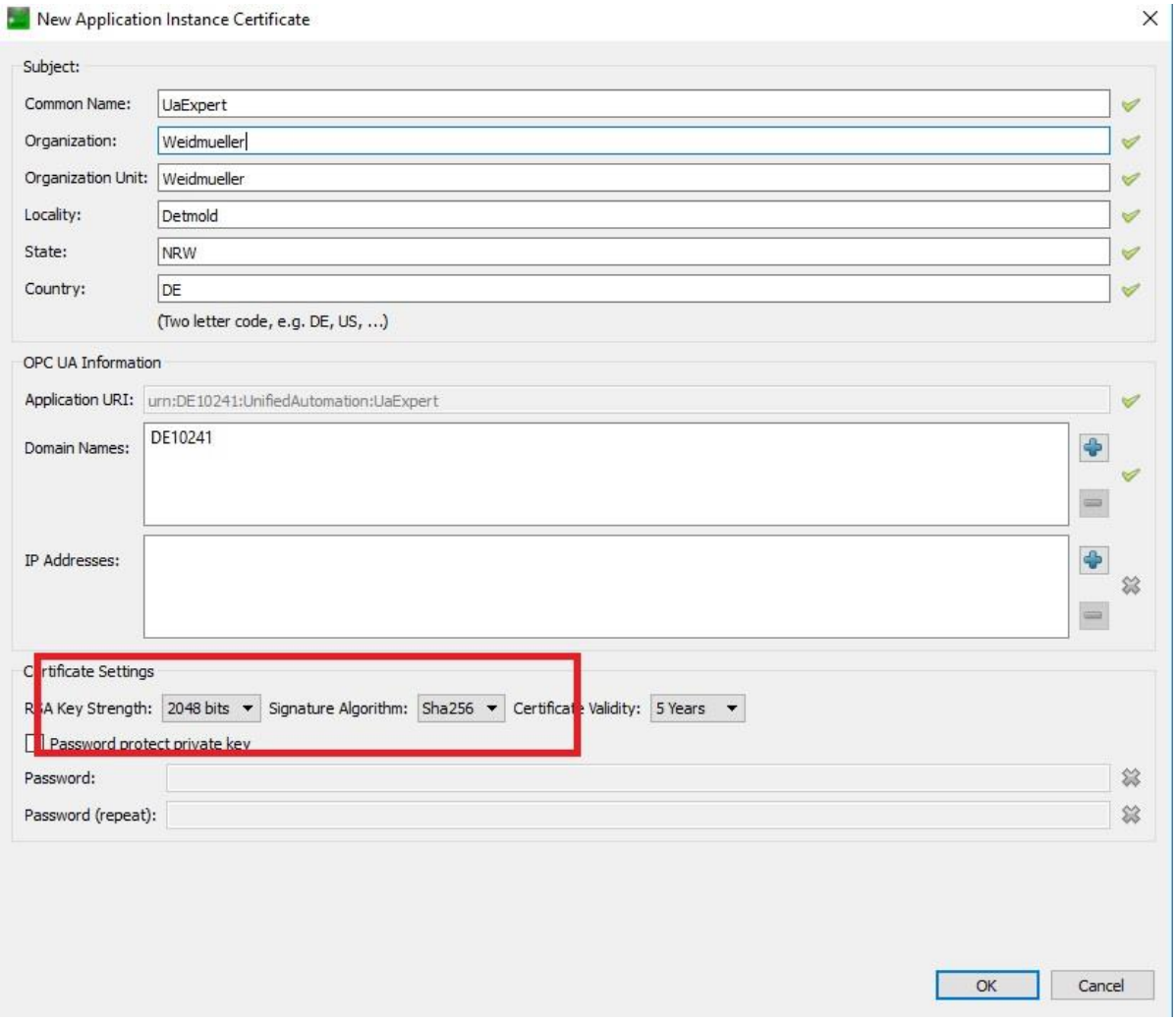


For a quick test, the 30 days trail license is enough, but a regular license should be used for any kind of productive system. After the license has been activated, a restart of the controller is required.

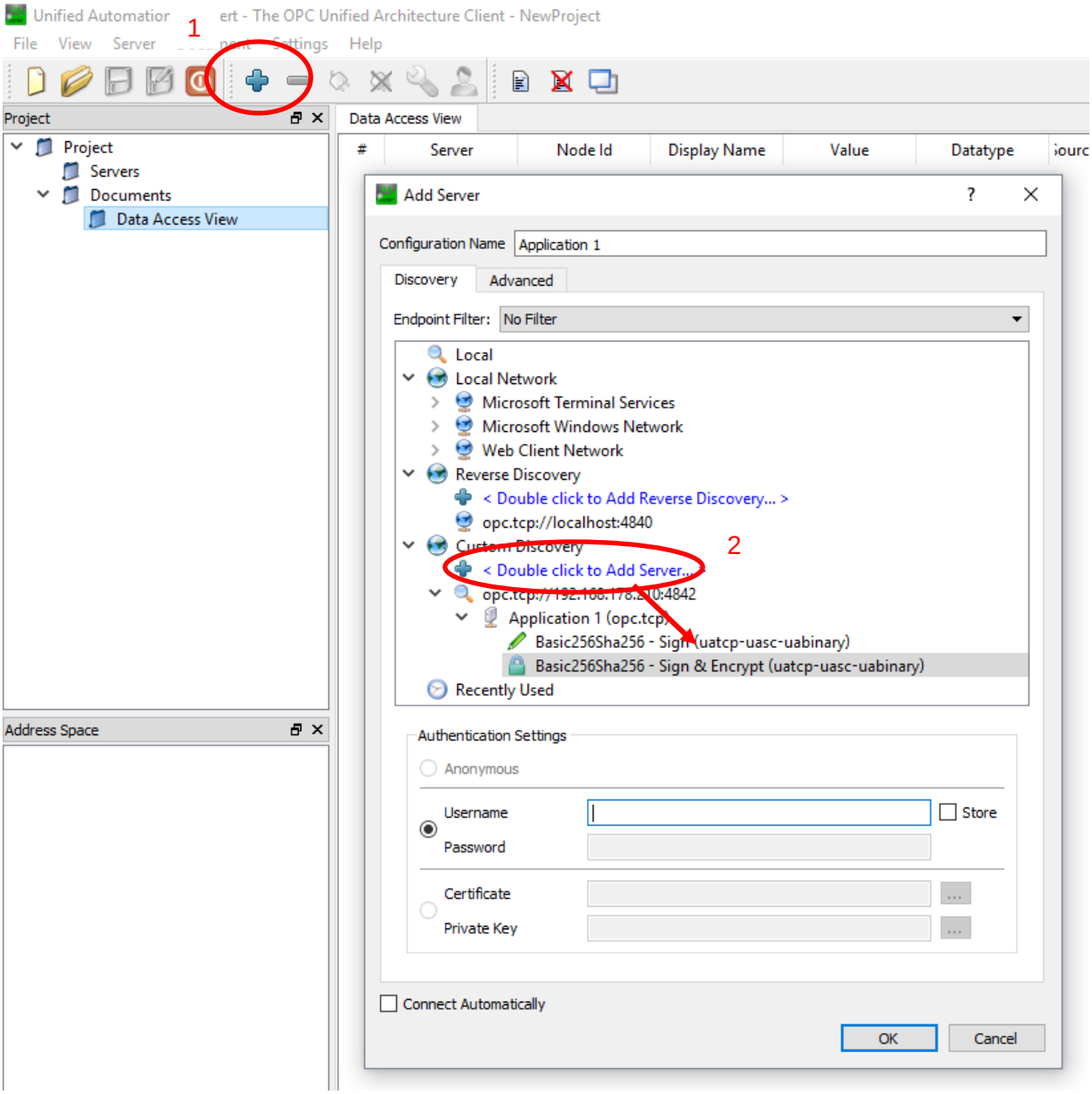
The OPC-UA server needs to be licensed separately from the regular u-create studio runtime! It requires a second license-code!

5. Connecting the client

Before a connection can be established, the certificate of the client needs to be configured as shown in the picture below. The dialogue is opened by **settings/Manage Certificates/** and a click on **“Create new Application Certificate...”.**

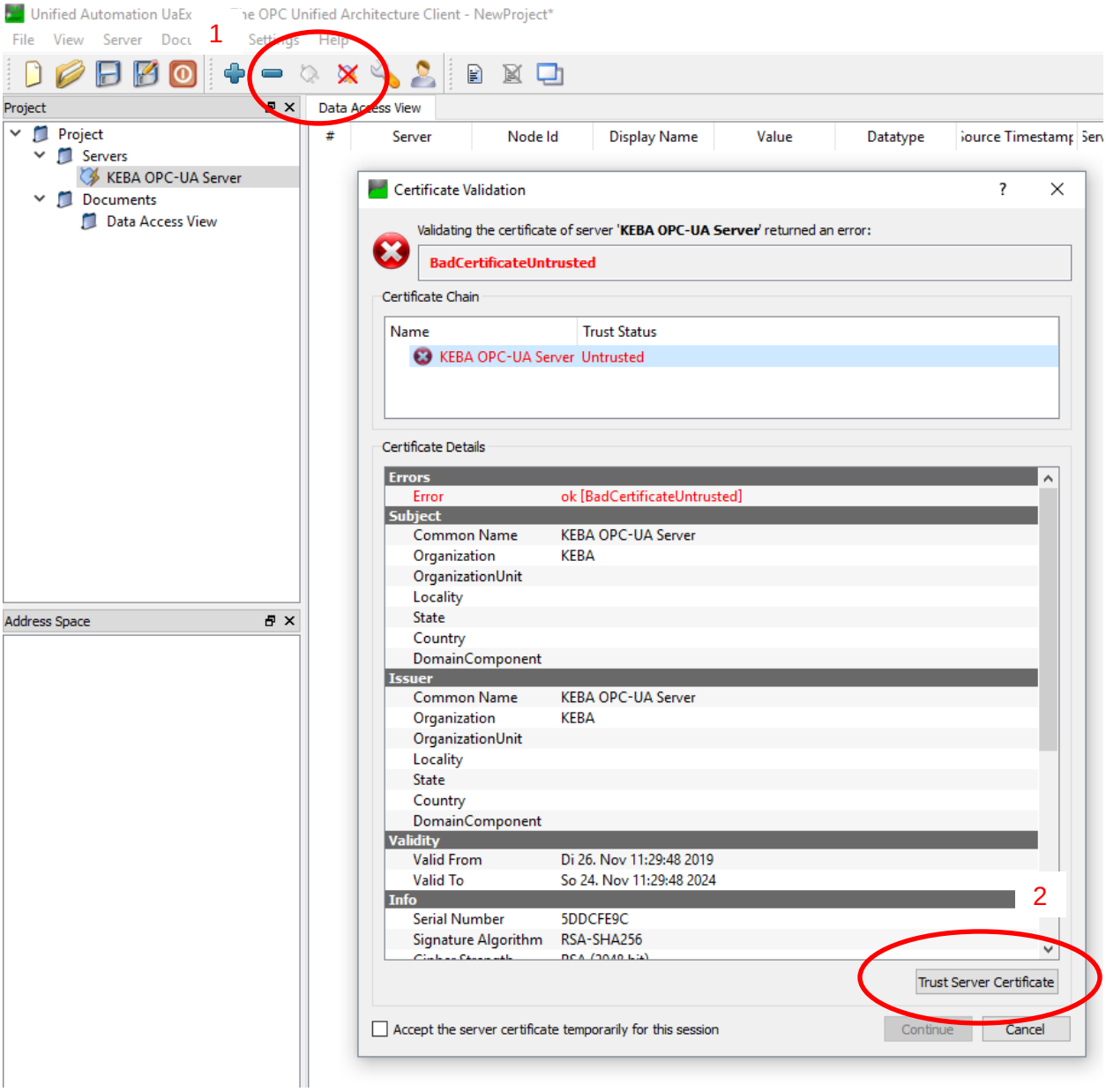


To establish a new connection via UaExpert, a new server must be added. The required steps are roughly described in the picture below. The “Add Server” dialogue is called by clicking on the “plus”-symbol on the main window. In this dialogue, a new server is added by “Custom Discovery” under “Double click to Add Server”. Enter opc.tcp://ip-address-of-the-plc:4842 and select the connection type.

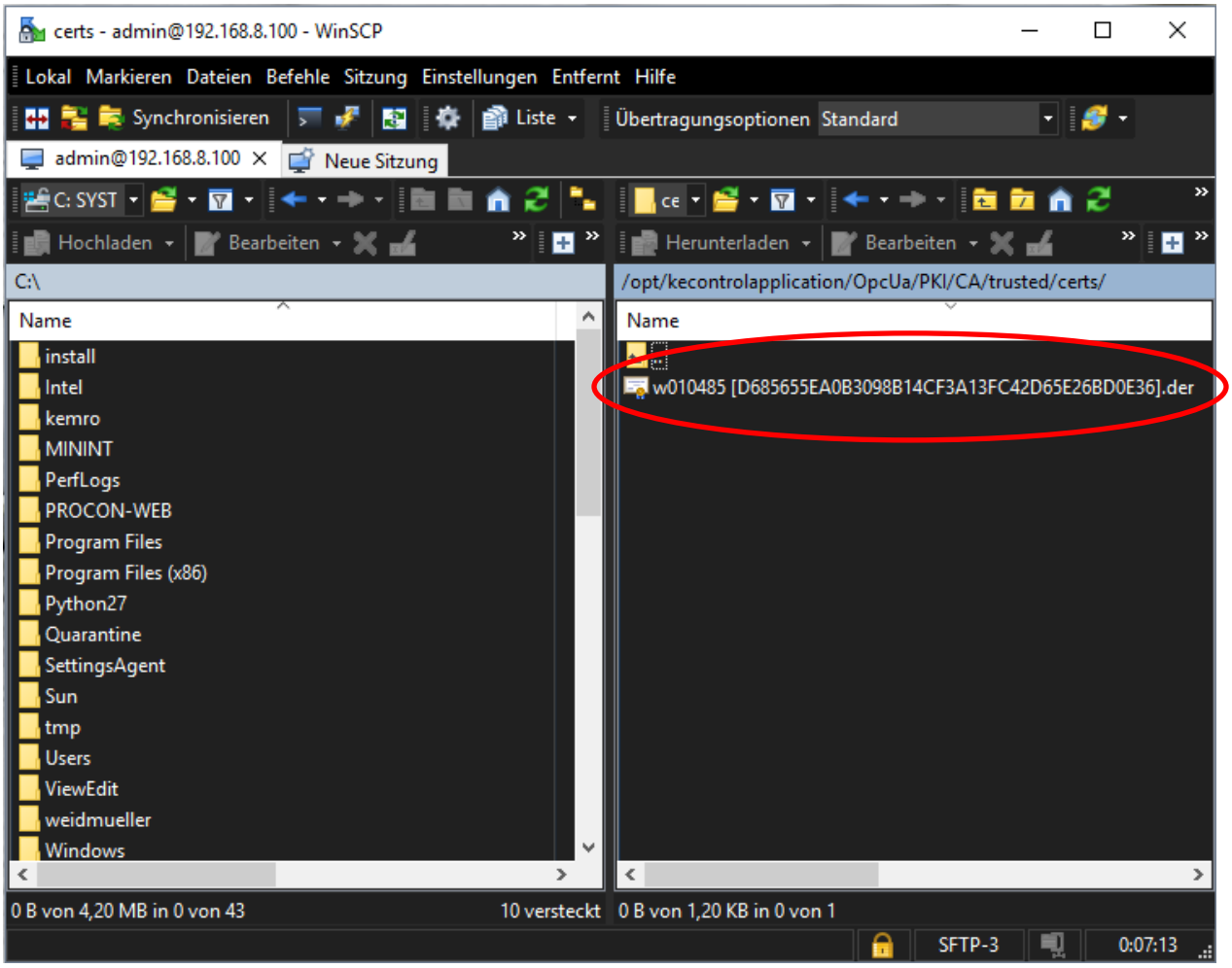


The default username is “Administrator” and the default password is “tobechanged”. The default password should be changed in case of a productive system. This can be done via user management of the controller.

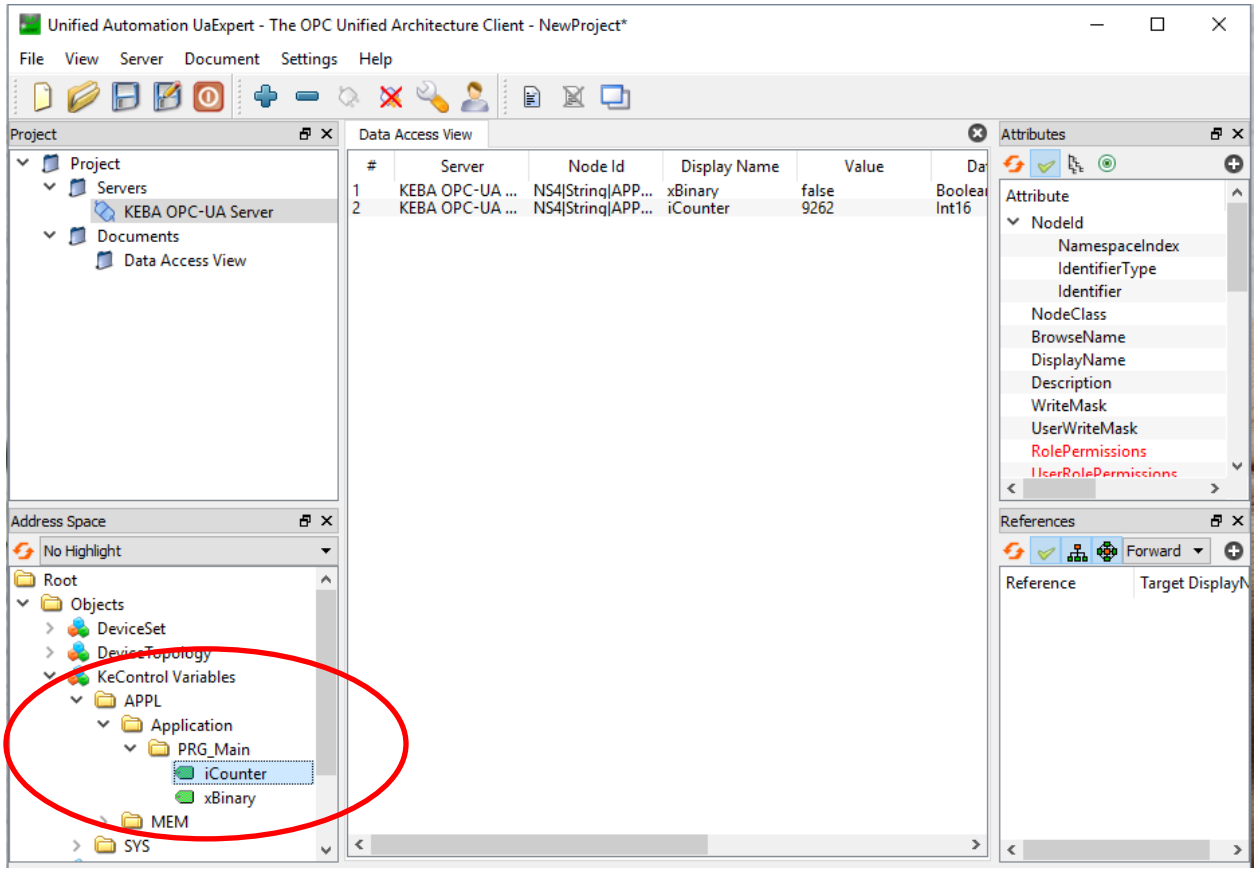
The picture below shows the steps to verify the server certificate on the client’s side. After the new server has been created, a connection is established by clicking on the connect button. During the first connection, the certificate needs to be validated by clicking on “Trust Server Certificate”.



The first time a connection is attempted, the connection is terminated. This is not an error, but part of the connection process. The reason for this is that the client's certificate is not yet accepted by the server. To accept the certificate, it needs to be moved from the folder "../rejected" to the folder "../trusted/certs/. Both folders can be found under the path "/opt/kecontrolapplication/OpcUa/PKI/CA/".



Moving the certificates can be achieved on a windows system using the program WinSCP, see picture above. The screen shot shows a trusted certificate in the right folder.



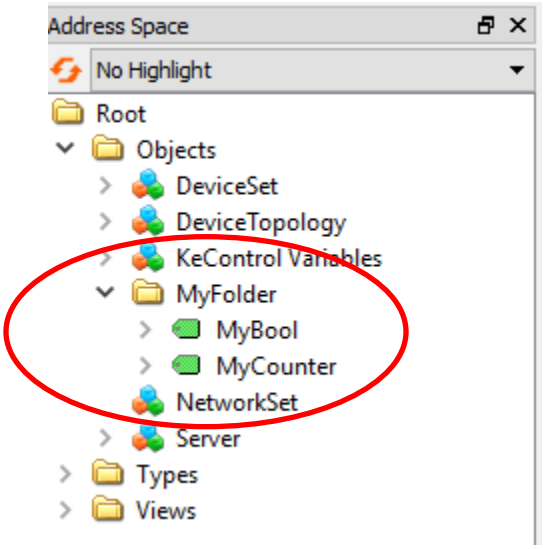
A new connection is now accepted by the server. If the “VariablesTree” has been activated (refer section 4.2), the available variable can be found under “KeControl Variables”.

6. Building an information model

To expose a defined set of variables, an object model can be created. The description of this information model is done in form of an .xml file that must be created under the path “/opt/kecontrolapplication/application/OpcUa/”. Just one .xml file is allowed in this folder.

```
<OpcUAInformationModel>
<!-- Declaration of namespace URIs -->
<NamespaceUris>
    <Uri ns="1" isDefaultNs="1">www.company.com</Uri>
</NamespaceUris>

<DefaultRolePermissions>
    <RolePermission RoleName="Administrator" Permissions="0x61"/>
    <!-- Bit 0 - Browse, Bit 5 - Read, Bit 6 - Write -->
</DefaultRolePermissions>

<!-- Declaration of instances -->
<!-- add child instances to parent Root/Objects node -->
<Instances Parent="0:Objects">

    <Object
    DataType="0:Types.0:ObjectTypes.0:BaseObjectType.0:FolderType"
    NodeId="i=1000" BrowseName="MyFolder" DisplayName="MyFolder">

        <Variable DataType="0:Types.0:DataTypes.0:BaseDataType.0:Number.0:Integer.0:Int16"
        NodeId="i=1001" BrowseName="MyCounter" DisplayName="MyCounter"
        ValuePath="APPL.Application.PRG_Main.iCounter" AccessLevel="0x03"/>

        <Variable DataType="0:Types.0:DataTypes.0:BaseDataType.0:Boolean"
        NodeId="i=1002" BrowseName="MyBool" DisplayName="MyBool"
        ValuePath="APPL.Application.PRG_Main.xBinary" AccessLevel="0x03"/>

    </Object>
</Instances>
```

The picture above shows a very simple example of a .xml file that adds the two variables mentioned in section 4.1 to a folder and exposes them.



The picture above shows the result in UaExpert. For further details on datatypes and other topics regarding structure or datatypes in the information model file, please refer the u-create studio manual.