



INGENIEURBÜRO FÜR
TECHNOLOGIE TRANSFER
DIPL.-ING. B. P. SCHULZ-HEISE

IBH Link UA

Manual Part 1

Setup

Version 5.20

IBHsoftec GmbH
Turmstr. 77
64760 Oberzent / Beerfelden
Tel.: +49 6068 3001
Fax: +49 6068 3074
info@ibhsoftec.com
www.ibhsoftec.com

TTI Ingenieurbüro für
Technologie Transfer
Dipl. Ing. B. Peter Schulz-Heise
Tel.: +49 6061 3382
Fax: +49 6061 71162
TTI@schulz-heise.com
www.schulz-heise.com

Windows® is a registered trademark of Microsoft® Corporation.
TeamViewer® is a registered trademark of TeamViewer AG, Göppingen.
Simatic® S5, Step® 5, Simatic® S7, Step® 7, S7-200®, S7-300®, S7-400®, S7-1200®; S7-1500® and
GRAPH® 5 are registered trademarks of Siemens Aktiengesellschaft, Berlin and Munich.
Image source: © Siemens AG 2001, All rights reserved.
Product names are trademarks of their respective owners.

Contents

Contents.....	I
1 IBH Link UA – Setup.....	1-1
1.1 Installation and connection.....	1-1
1.2 Configuration of the IP addresses (default setting).....	1-2
Standard IP-Address configuration:	1-3
1.3 Login browser window	1-3
Language selection	1-4
OPC server running display	1-4
IBH Link UA type display	1-4
Remember me.....	1-4
Login.....	1-4
Change Password.....	1-5
1.4 Network browser window.....	1-5
1.4.1 Management Level Settings.....	1-5
1.4.2 Control Level Settings	1-6
1.4.3 Management Level / Control Level adjustments.....	1-7
Endpoint URL	1-8
1.4.4 Einstellungen 802.1x.....	1-8
1.5 OpenVPN settings.....	1-9
1.6 TeamViewer IoT activation – IBH Link UA	1-10
1.6.1 PC preparations – connected to the Ethernet port of the Management Level	1-11
Download and install the TeamViewer software	1-11
Download and install the IBHNet-IoT software	1-12
1.6.2 Open the TeamViewer IoT Management Console.....	1-12
Assignment token dialog box	1-13
1.6.3 Insert assignment token.....	1-14
Assignment token taken from TeamViewer IoT	1-15
Copy the TeamViewer ID	1-15
1.6.4 TeamViewer IoT – Logfile	1-17
1.6.5 Teamviewer IoT – MQTT settings	1-18
1.7 TeamViewer IoT License IBH Link UA.....	1-18
1.8 Security browser window.....	1-19
Server Security	1-20
Reverse Connection.....	1-21
Integrated client security	1-21
Download	1-22
Firewall	1-22
Web Configuration	1-23
1.9 Certificates browser window	1-23
1.10 Time settings browser window	1-24

1.11	System browser window.....	1-25
1.11.1	Device Information	1-26
1.11.2	Backup and Restor the settings	1-27
	Saving the IBH Link UA configuration	1-27
	Restore the IBH Link UA configuration.....	1-27
	Firmware Update.....	1-28
1.11.3	Restart the IBH Link UA.....	1-31
1.11.4	Variable format	1-31
1.11.5	OPC UA options.....	1-33
1.12	Users browser window	1-34
1.13	Browser window Siemens slots.....	1-34
	Load the OPC Editor project	1-35
	Save the OPC Editor project	1-35
	Insert SoftPLC	1-36
	Insert SINUMERIK.....	1-36
	Read SINUMERIK Model	1-37
	Import NC-VAR file	1-38
	Change SINUMERIK.....	1-38
1.14	History browser window	1-39
	History tree	1-39
	History vars (variables).....	1-39
	Retentive history.....	1-40
	History variable list as XML file	1-40
1.15	OPC Client browser window.....	1-41
	Define read variables	1-42
	Connect with variable	1-43
1.16	Diagnostics browser window	1-44
	Controller diagnosis.....	1-44
	Client diagnostics	1-45
	Network diagnostics	1-45
	System Log.....	1-47
1.17	MQTT browser window	1-47
1.18	SoftPLC browser window	1-48
	Browser window SoftPLC / SoftPLC status.....	1-48
1.19	Modbus browser window.....	1-49
1.20	Mitsubishi browser window.....	1-50
1.21	Rockwell browser window.....	1-51
1.22	MicroSD browser window.....	1-51
1.23	IBH Link UA default factory configuration	1-53
1.24	Open the Wiki	1-53
1.25	Use STEP7 or TIA projects	1-54
1.25.1	Example IBH Link UA Editor	1-55
1.25.2	Configuration with the STEP® 7 SIMATIC Manager	1-55
	OPC server configuration.....	1-56
	Ethernet CP configuration	1-56

1.25.3	Configuration with the TIA Portal (V13 / V14 / V15 / V16).....	1-57
	Ethernet CP configuration	1-57
	OPC server configuration.....	1-57
2	Unified Automation UaExpert –OPC UA Client and OPC UA Server	2-1
2.1.1	Starting UaExpert.....	2-2
2.2	Establishing a connection to the IBH Link UA	2-3
	IBH Link UA browser window <i>System</i>	2-7
2.3	Encrypted connection to the IBH Link UA	2-8
	Desired encrypted connection.....	2-9
	Trusting the IBH Link UA Certificate	2-10
2.4	Download the OPC UA Demo Server (Windows)	2-11
	Install the OPC UA Demo Server.....	2-12
2.4.1	OPC UA Server <i>Endpoint URL</i>	2-12
	Add UaCPPServer in the UaExpert Client	2-13

1 IBH Link UA – Setup

1.1 Installation and connection

The IBH Link UA is designed for DIN rail mounting:



The IBH Link UA has two (2) interfaces, which are separated by a firewall and having separate MAC addresses, which are designed for data exchange within the management level or in the process level.

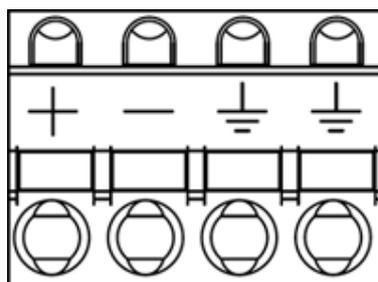
The interface of the process level consists of a 3-port switch.

The power is supplied via the included plug.

ATTENTION!



A supply voltage of **12VDC** to **36VDC** is to be used for the operation of the IBH Link UA. A higher supply voltage may destroy the device.



Power supply: **24VDC / 0.2A**

1.2 Configuration of the IP addresses (default setting)

If the IBH Link UA is in its default factory setting the configuration can be done with an up-to-date web browser via the Ethernet ports 2 to 4 using the IP address 192.168.1.14.

The Ethernet port 1 can only be used to configure the **IBH Link UA** if a **DHCP server** assigns the IP address, and a DNS server resolves the name by specifying the hostname

`http://ibhlinkua_<serial number>`

(Example: `http://ibhlinkua_010331`)

No additional applications or drivers are required.

The following information is printed on the IBH Link UA housing.



Default logon data

Username: admin

Password: admin

Standard IP-Address configuration:

Level	Port	Address
Management level	Port 1	Hostname: ibhlinkua_<serial number>
Control level	Port 2 - 4	192.168.1.14



Note:

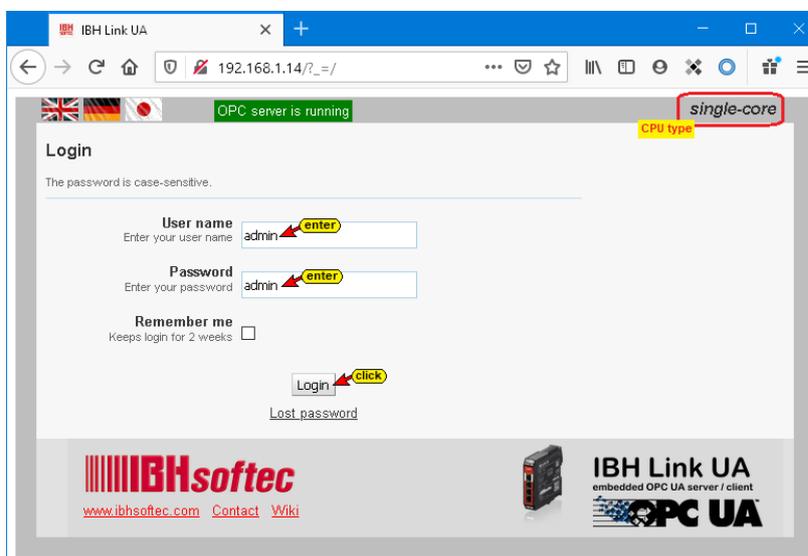
In the IBH Link, UA default factory setting the configuration may be accessed using an Internet browser (FireFox, Microsoft Edge, Internet Explorer, etc.) as followed:

Via the management level (port 1) with the host name if the port is connected to a network with a DHCP server and DNS server.

Via the ports of the machine level, it is only possible if the connected network has the sub-address 192.168.1.nn.

Otherwise, a fixed IP address from the subnet 192.168.1.nn (e.g., 192.168.1.10) must be provided to the connected PC.

1.3 Login browser window



Language selection

The languages English, German and Japanese are available in the browser window.



OPC server running display

There is a display that provides information about the activities of the OPC server.

OPC server is running

IBH Link UA type display

The IBH link UA is available in two performance levels:

- **Single core** - the processor used in the IBH Link UA is a single core processor (serial numbers 10000 -). Older IBH Link UA's with single core processors do not have a performance level display (Serial numbers 1000 - 4999).

single-core
- **Quad Core** - the processor used in the IBH Link UA is a quad core processor. These IBH Link UA's have a significantly higher processor performance (serial numbers 5000 - 9999)

quad-core

Remember me

If this login is marked, no username and password will be requested when the same browser window is called up again. This setting remains in effect for up to two weeks.

Login

When you click Login, the following security messages are displayed one after the other.

Important information about HTTP access

i With unencrypted connections, it is possible that personal information can be revealed.
Therefore we recommend to disable HTTP in the 'Security' page.

confirm → **Ok**

Important information about the Password

i Currently a default password is used.
It is highly recommended to change the password.

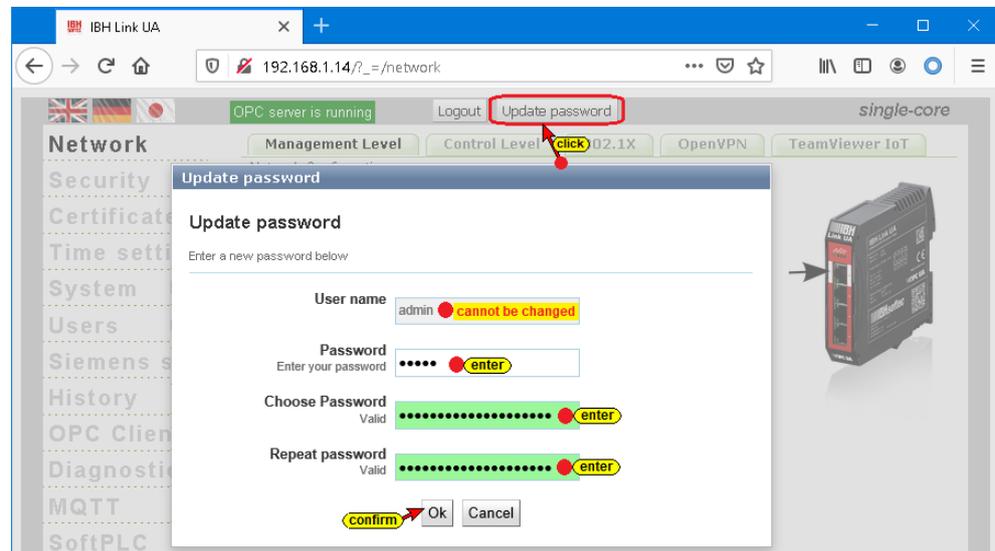
confirm → **Ok**

After the security messages have been confirmed, we recommend changing the password.

Change Password

For security reasons, the password should be changed. The username may also be changed.

In the open browser window **Management level / control level** click the button **Update password**.



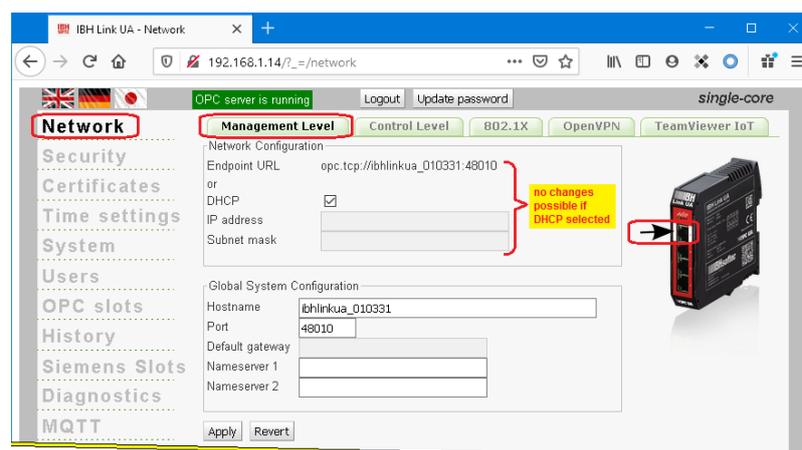
If the password is not long enough or if you have not entered enough different characters (A - Z; 0 - 9; special characters), the background is "red". For security reasons, the password must be 12 or 16 characters long.

The browser access username cannot be changed.

1.4 Network browser window

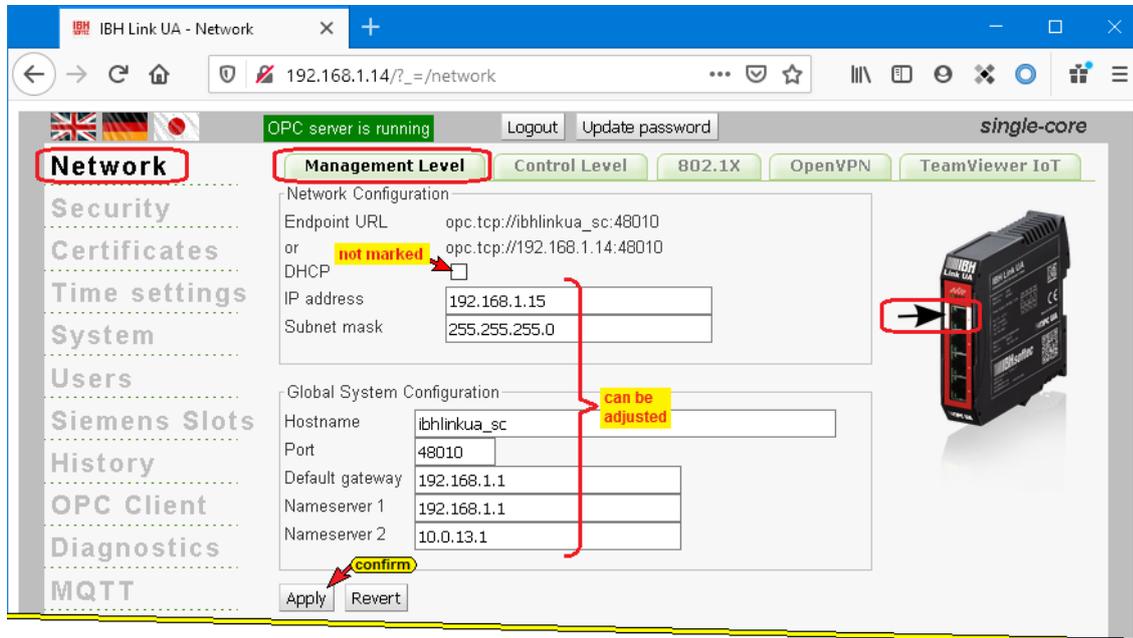
1.4.1 Management Level Settings

Port 1 **Network Configuration** and **Global System Configuration**.



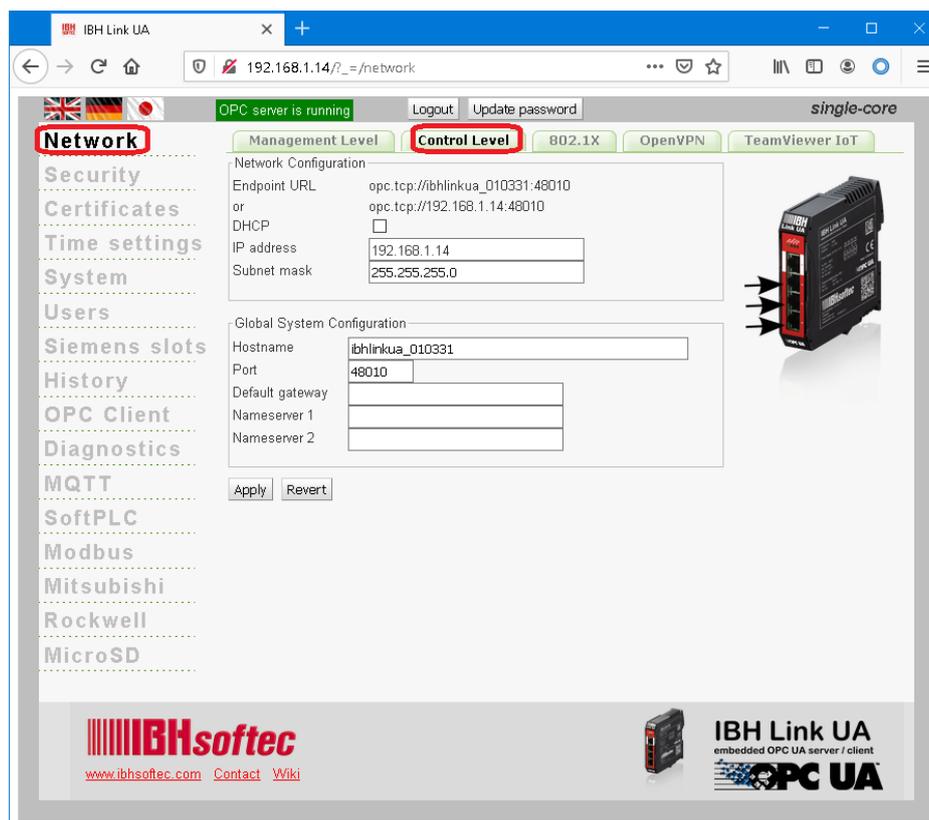
Management Level Settings

With DHCP disabled, the **Network Configuration** and **Global System Configuration** may be modified. The hostname can always be adjusted.



1.4.2 Control Level Settings

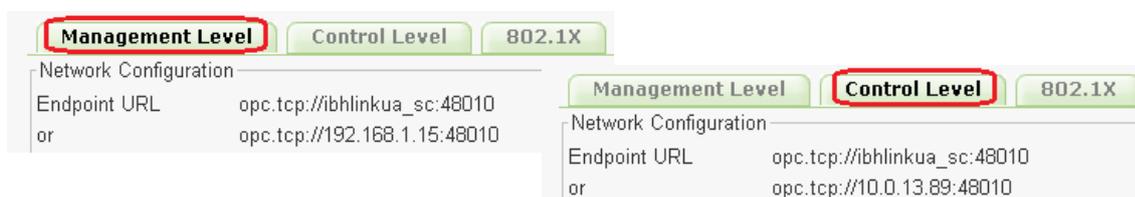
Ports 2 to Port 4 Control Level **Network Configuration** and **Global System Configuration**.



Note:
 The management level (port 1) must have a different subnet address than the control level (port 2 to port 4) to clearly identify the belongings of the ports to the Ethernet interfaces.

Endpoint URL

The **Endpoint URL** is displayed in the **Management Level** and in the **Control Level**. The endpoint URL is generated by the **IBH Link UA** based on the settings. The endpoint URL consists of the protocol: **opc tcp // hostname: port**.

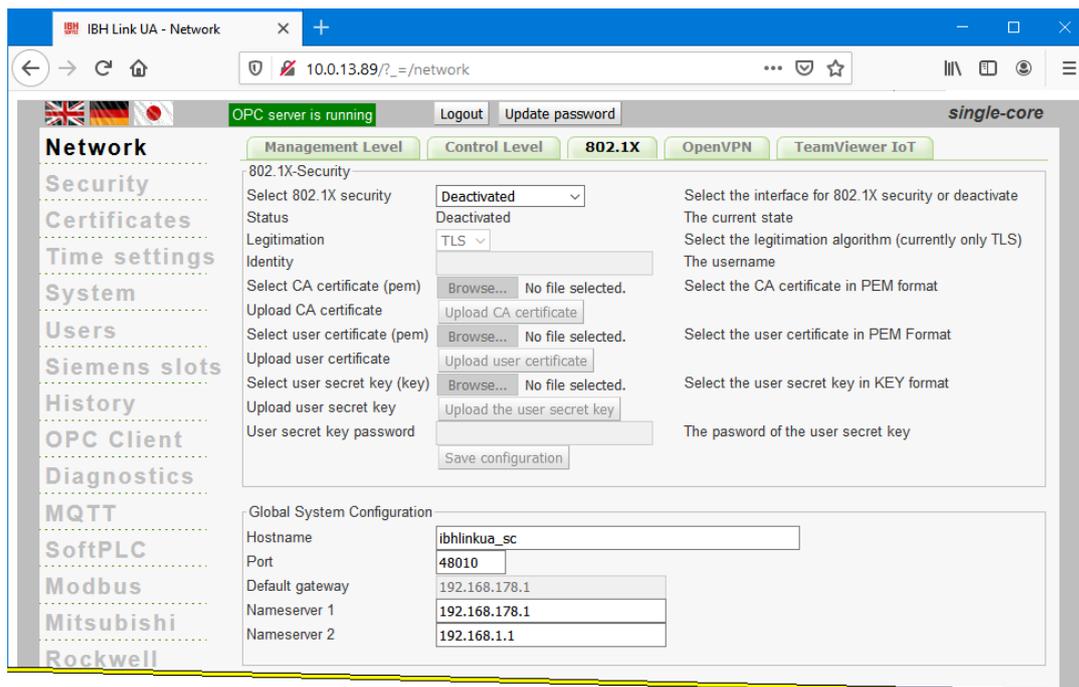


This **Endpoint URL** is required to set an OPC UA client.

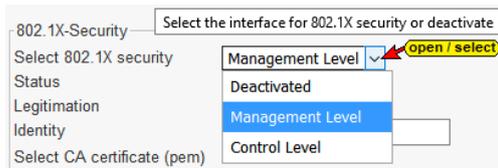
Clients can use this endpoint URL to find out the configuration of the server - for example, regarding the security options used.

1.4.4 Settings 802.1x

The IBH Link IoT provides IEEE 802.1X for authentication and authorization in IEEE 802 networks.



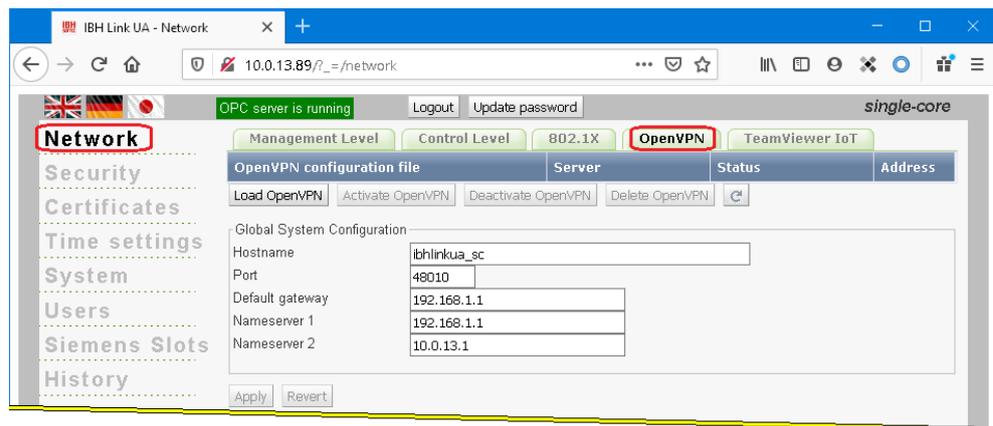
The activated settings in the 802.1X window can be assigned to the network connections at the control level or the management level.



The configuration of the IEEE 802.1X security settings can be saved.

1.5 OpenVPN settings

OpenVPN is a VPN client. With OpenVPN an encrypted SSL connection to a virtual network (VPN) can be established.



OpenVPN requires a configuration file and key / certificate files.

Clicking on **Load OpenVPN** opens the **Load OpenVPN Configuration** dialog box.

Load OpenVPN

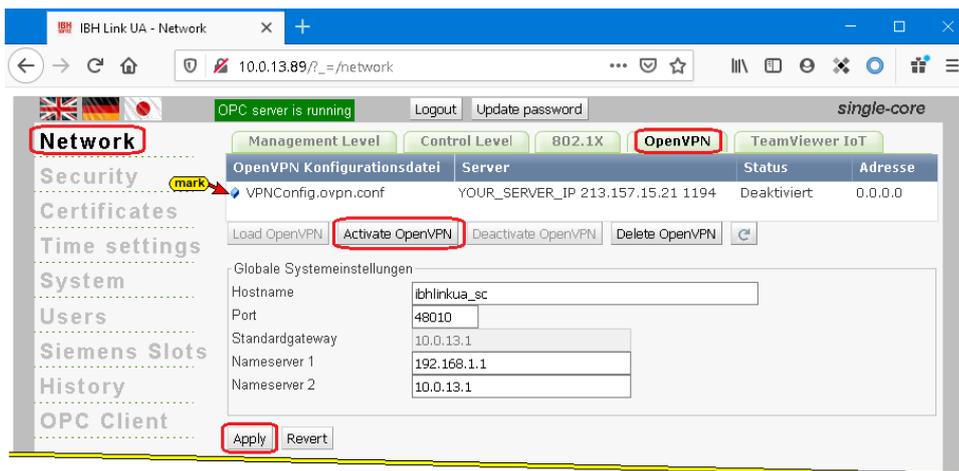


The configuration file with the client settings and the certificates is selected using the **Search** button. It is loaded using the **Load OpenVPN configuration** button.

Clicking **Apply OpenVPN configuration** closes the **Load OpenVPN** dialog box.



Configuration file information are displayed.

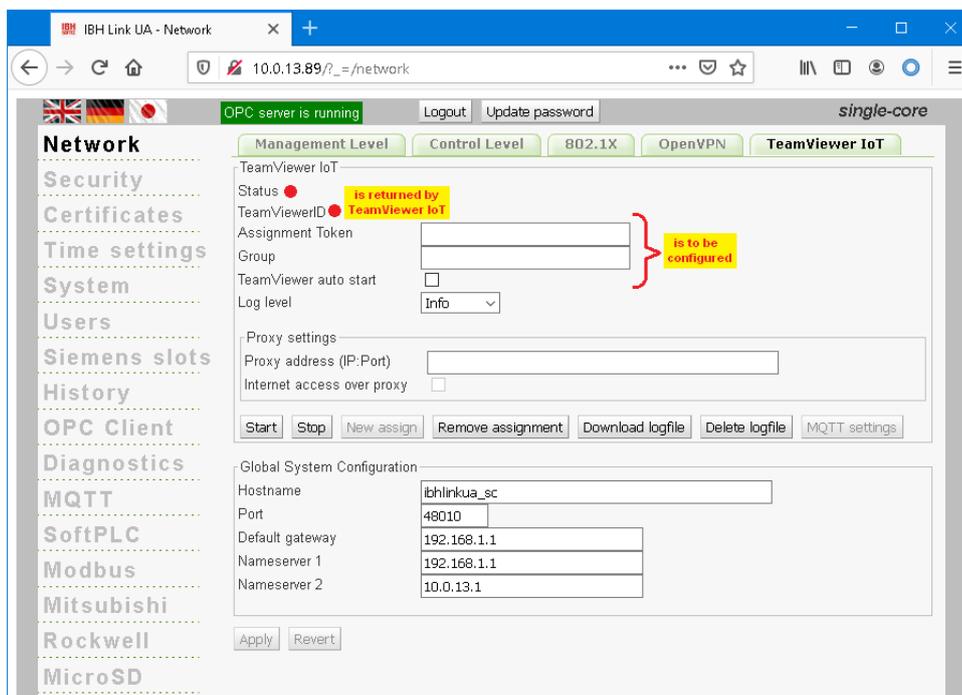


With a click on Activate OpenVPN the virtual network connection (VPN) is activated and with Apply the settings are loaded into the IBH Link UA.

1.6 TeamViewer IoT activation – IBH Link UA

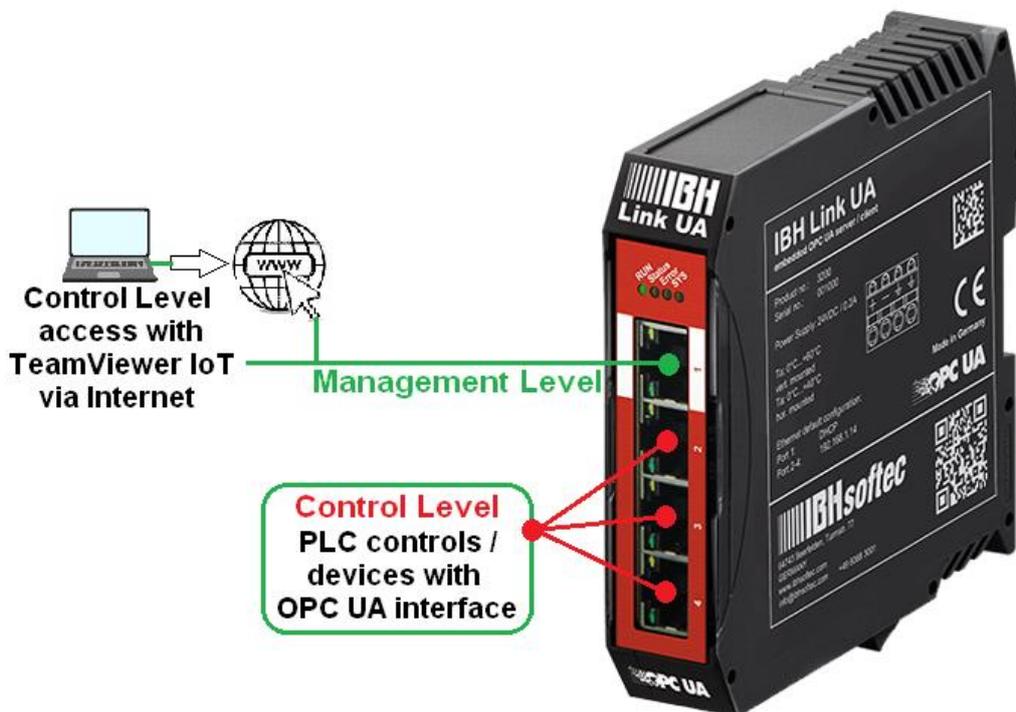
TeamViewer IoT software option is pre-installed in the IBH Link UA starting firmware V 7.5. This option offers the possibility of being able to access almost all PLC systems anytime and anywhere.

Complex modem solutions or the use of a PC on site are a thing of the past.



If the Internet must be accessed via a proxy, the address can be entered in the form **Proxy: Port** or **User: Password @ Proxy: Port**. The proxy access to the Internet must be activated.

To establish a connection via **TeamViewer-IoT**, the Ethernet subnet of the control level must have access to the Internet.



The IBH Link UA manages two subnet addresses separated by a firewall, each with its own MAC address.

Ethernet areas:

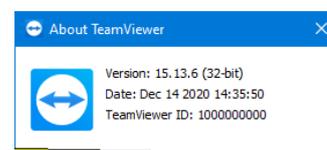
Level	Port	must be in different subnets
Management Level	Port 1	
Control Level	Port 2 - 4	

1.6.1 PC preparations – connected to the Ethernet port of the Management Level

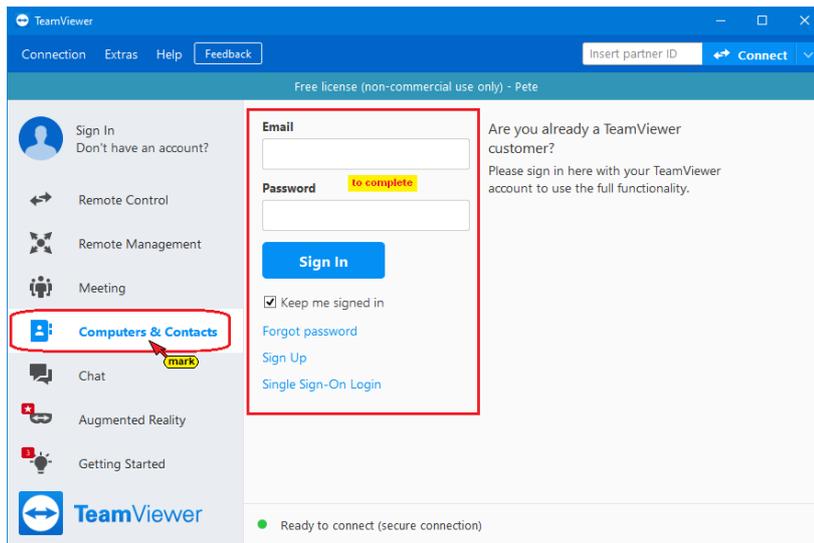
To use the access options of the pre-installed TeamViewer IoT software, follow the steps below:

Download and install the TeamViewer software

TeamViewer software version 15.13.6 or newer must be installed on the PC that is to be used to access the external IBH Link UA.



The software can be downloaded for free from the TeamViewer web page <https://www.teamviewer.com>. The **Sign In** is required for the further steps.



Download and install the IBHNet-IoT Agent software

Install the **IBHNet-IoT-Setup.exe** software on the PC.

This software is available for download at

<https://download.ibhsoftec.com/neutral/IBHNet-IoT-Setup.exe>

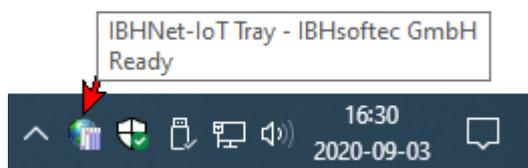


Double-click the **IBHNet-IoT** icon created during installation. The **ibhsoftec-agent-service** is started.

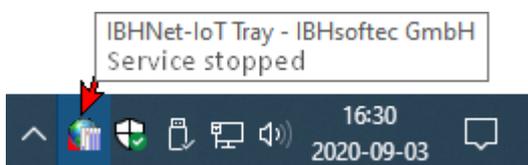
The **IBHNet-IoT Agent** software version 1.11 or newer must be installed.



The service is displayed in the **IBHNet-IoT Tray** in the task bar. It may be necessary to change the properties of the taskbar to display the icon.



Pointing to the icon, displays the readiness of the service.



If the symbol indicates a stopped service, it must be started.

Once the connection has been established, the IBHNet-IoT tray symbol has a green corner at the bottom left and transmission data is displayed

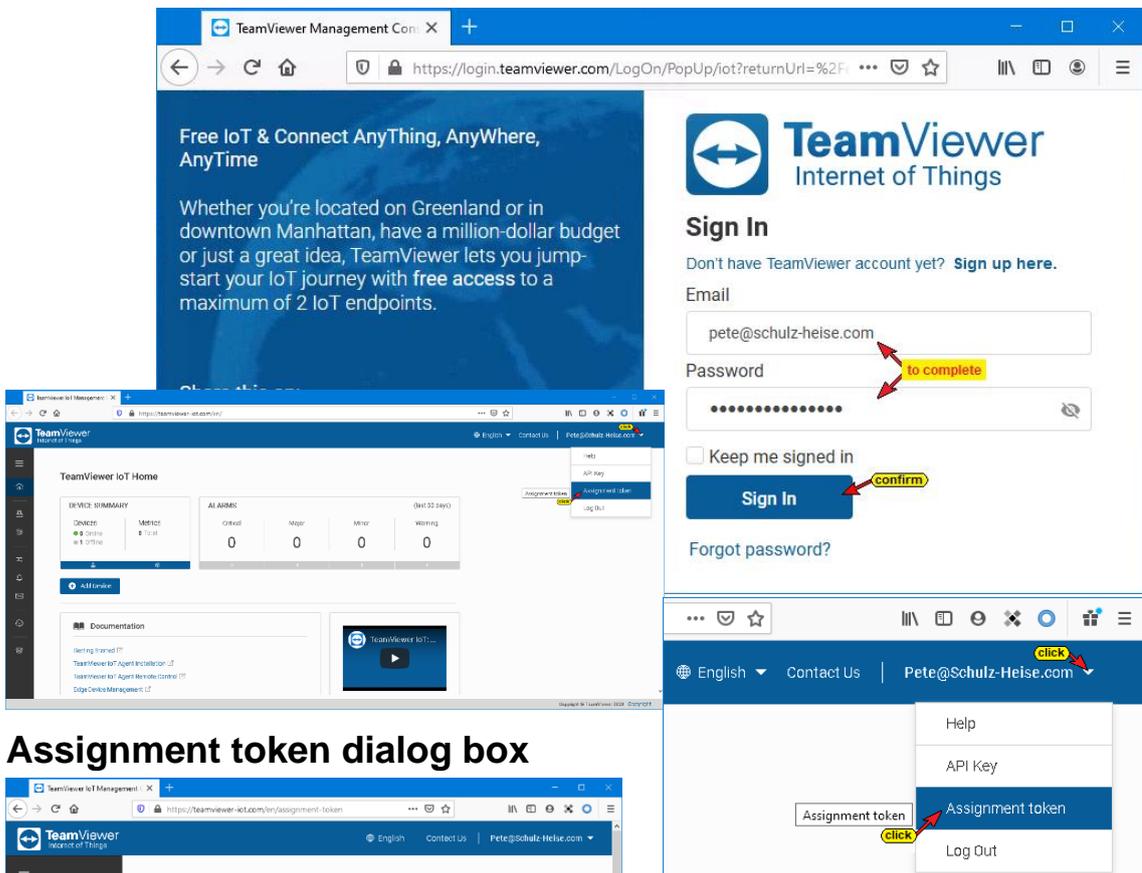


1.6.2 Open the TeamViewer IoT Management Console

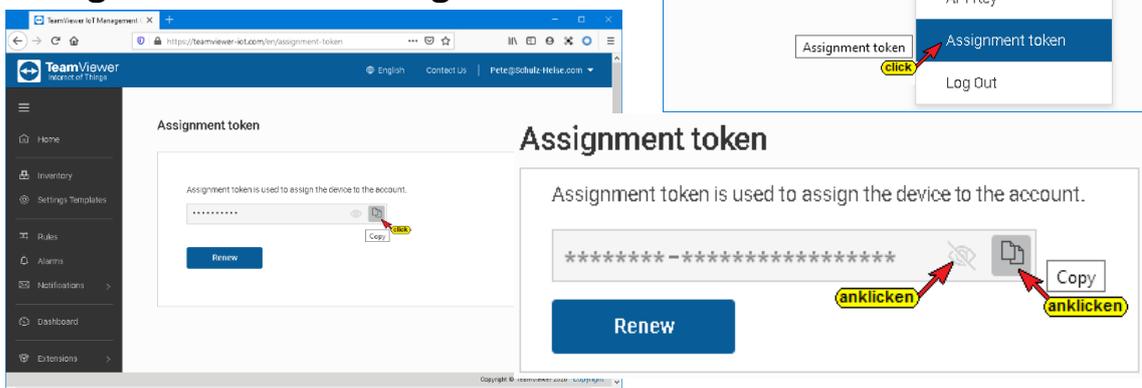
Use the link <https://teamviewer-iot.com/en/> to open the **TeamViewer Internet of Things** login page. Use the email and password of the **TeamViewer account** established in the previous step to **Sign In**.

TeamViewer IoT Management Console

After logging into the **TeamViewer IoT Management Console**, open the **Assignment token** dialog box.



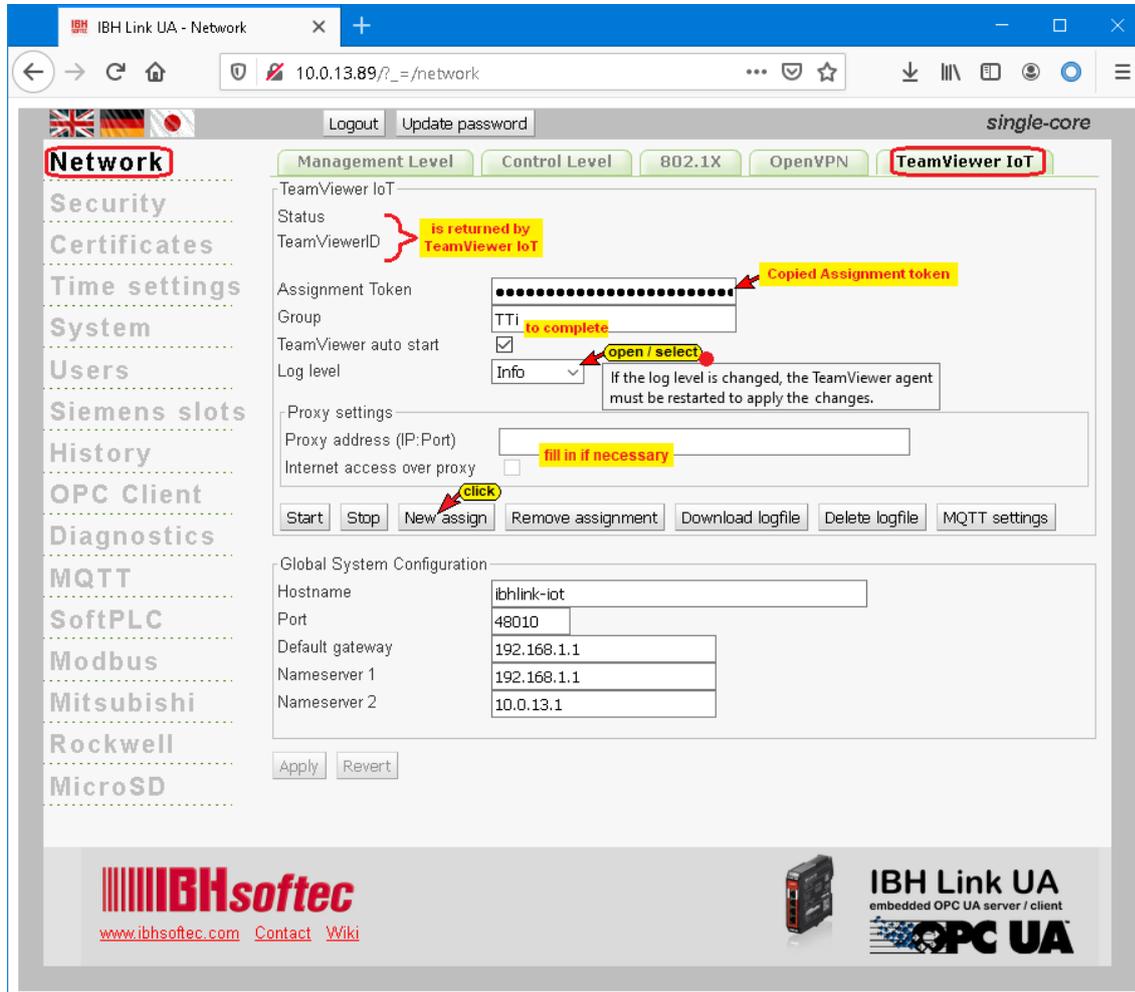
Assignment token dialog box



By clicking the Copy icon, the **Assignment token**, shown with several dots, is copied to the Windows clipboard.

1.6.3 Insert assignment token

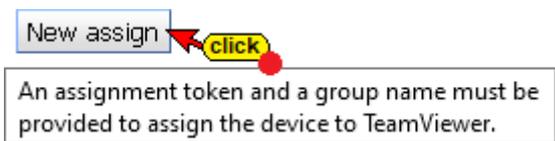
The **Assignment token** must be copied into the field with the same name in the **IBH Link UA** browser window Network/TeamViewer IoT.



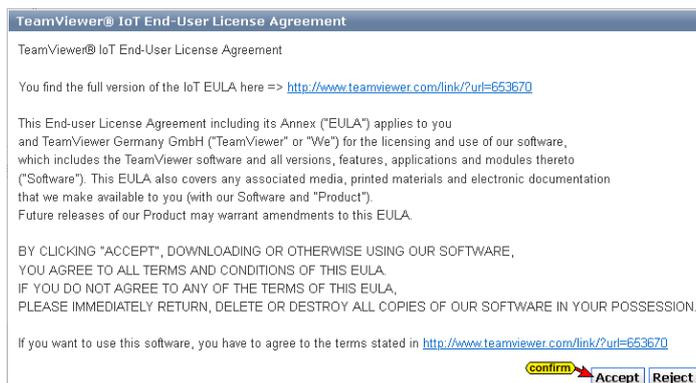
Enter the group name and mark that the TeamViewer is switched on automatically.

Clicking the **New assign** button opens the

TeamViewer IoT End-User License Agreement.



TeamViewer IoT End-User License Agreement



To apply the settings, the TeamViewer IoT end user license agreement must be accepted by clicking the button **Accept**.

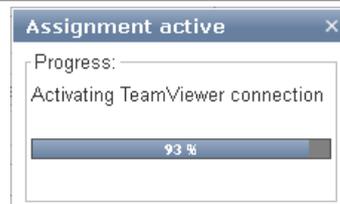


Note!



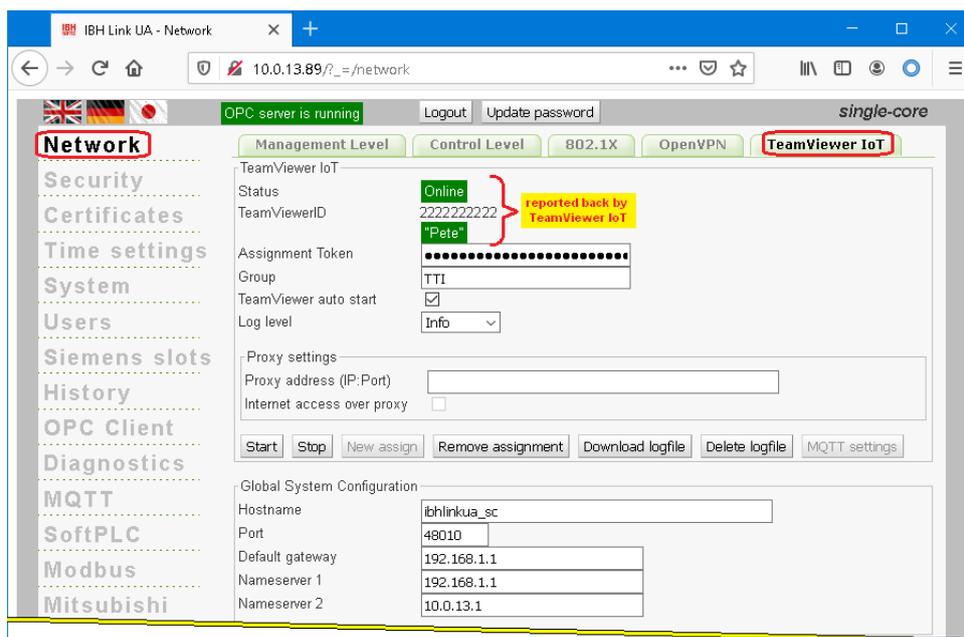
The transmission of the **Assignment token** to **TeamViewer** can take some time.

The online connection to the **TeamViewer IoT server** is established.



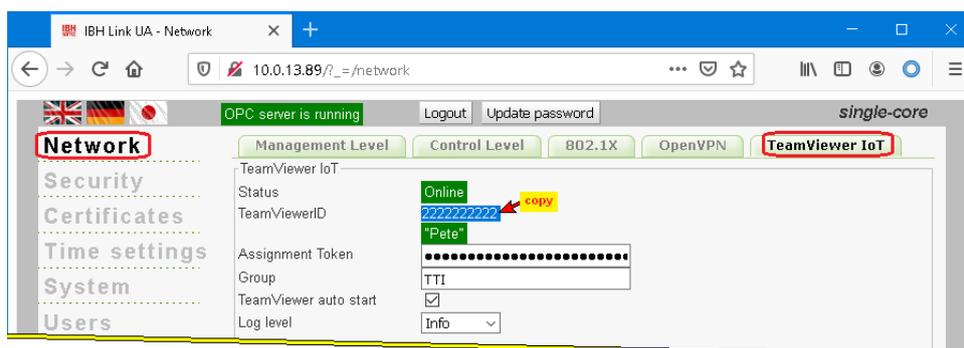
Assignment token taken from TeamViewer IoT

If the assignment token has been accepted, the status and the **TimeViewerID** with the name are displayed in the web browser window **Network/TeamViewer IoT**.

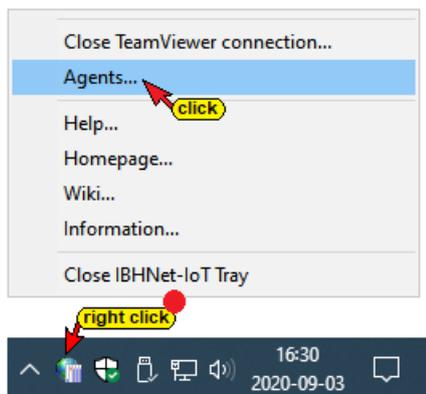


Copy the TeamViewer ID

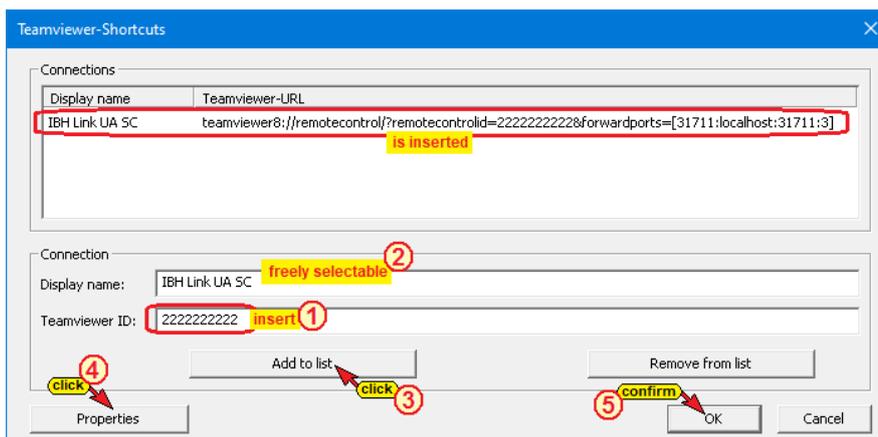
Copy the TeamViewer ID number to the Windows clipboard.



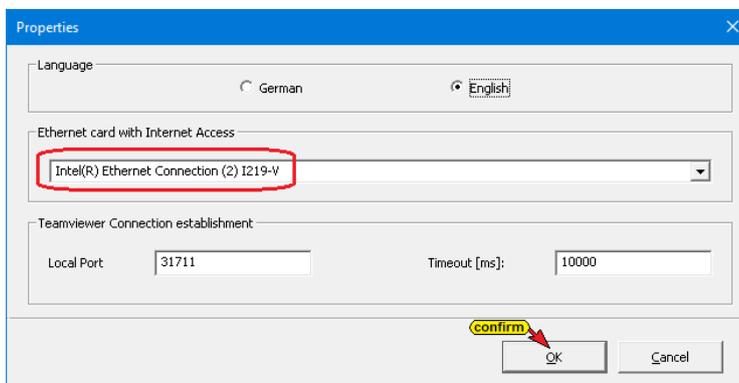
Right-click on the **IBHNet-IoT Tray** icon to open the context menu. The **Agents...** command opens the **TeamViewer Shortcuts** dialog box.



Insert the TeamViewer ID number in the field of the same name. The display name is transferred to the **TeamViewer account**. This name can be used to establish a connection to the IBH Link UA via the Internet.



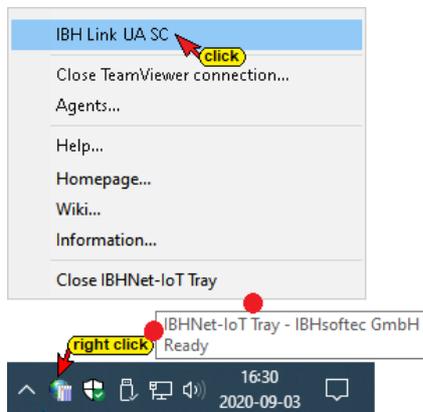
Clicking the Properties button, a dialog box appears with the details of the network card via which the **IBH Link UA** is connected.



By clicking the Add to list button, the display name and the TeamViewer ID are adopted. The dialog box is closed with **OK**.

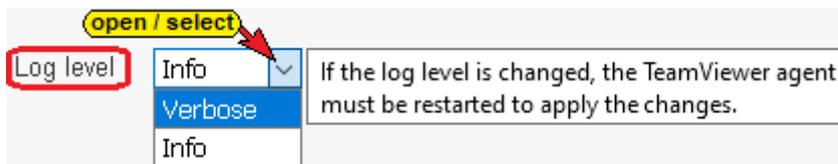
The installation of **TeamViewer IoT** in the IBH Link UA is now complete.

The **IBHNet-IoT Tray** provides a context menu. The devices registered with the **TeamViewer account** are listed in the upper area of the context menu.

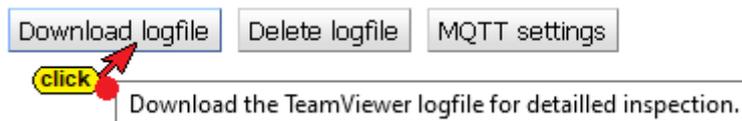


A connection is established with a click on the desired device (IBH Link UA SC).

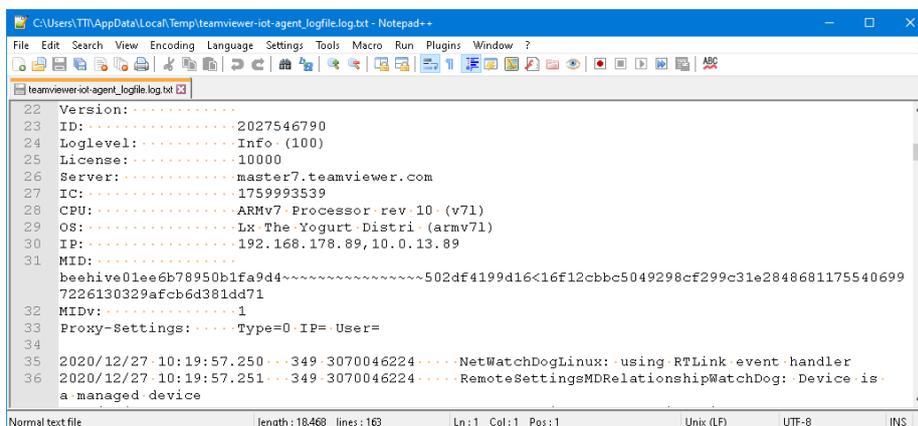
1.6.4 TeamViewer IoT – Logfile



The **log output** selected is stored in the IBH Link UA.



By clicking the **Download logfile** button, the saved states of the TeamViewer IoT connections (error-free / faulty) can be displayed in an editor or saved as a text file.



Since the evaluation of the log-file requires some specialist knowledge, this diagnosis should be carried out in the event of a malfunction using the IBHsoftec hotline.

To have a defined beginning of the log file, the stored file can be deleted.

1.6.5 Teamviewer IoT – MQTT settings

The **MQTT** option is useful in conjunction with the **IBH Link UA MQTT** option.

click Open a dialog with MQTT settings for the TeamViewer cloud
MQTT settings Clicking the MQTT button opens the **Establish connection to the Teamviewer IoT cloud** dialog box.



Details on the use of **MQTT** with the **IBH Link UA** is described on the **IBHsoftec WIKI** website.



1.7 TeamViewer IoT License IBH Link UA

With the latest, freely available firmware the functionality of the **IBH Link UA** is extended, to allow remote maintenance via **TeamViewer IoT**.

This new feature allows to access nearly all PLC systems always and everywhere.

Complex modem solutions or the use of a PC on site are obsolete.

To use this functionality with **IBH Link UA**, you need a **TeamViewer IoT** license.

Use the following link to purchase a **TeamViewer IoT** license:

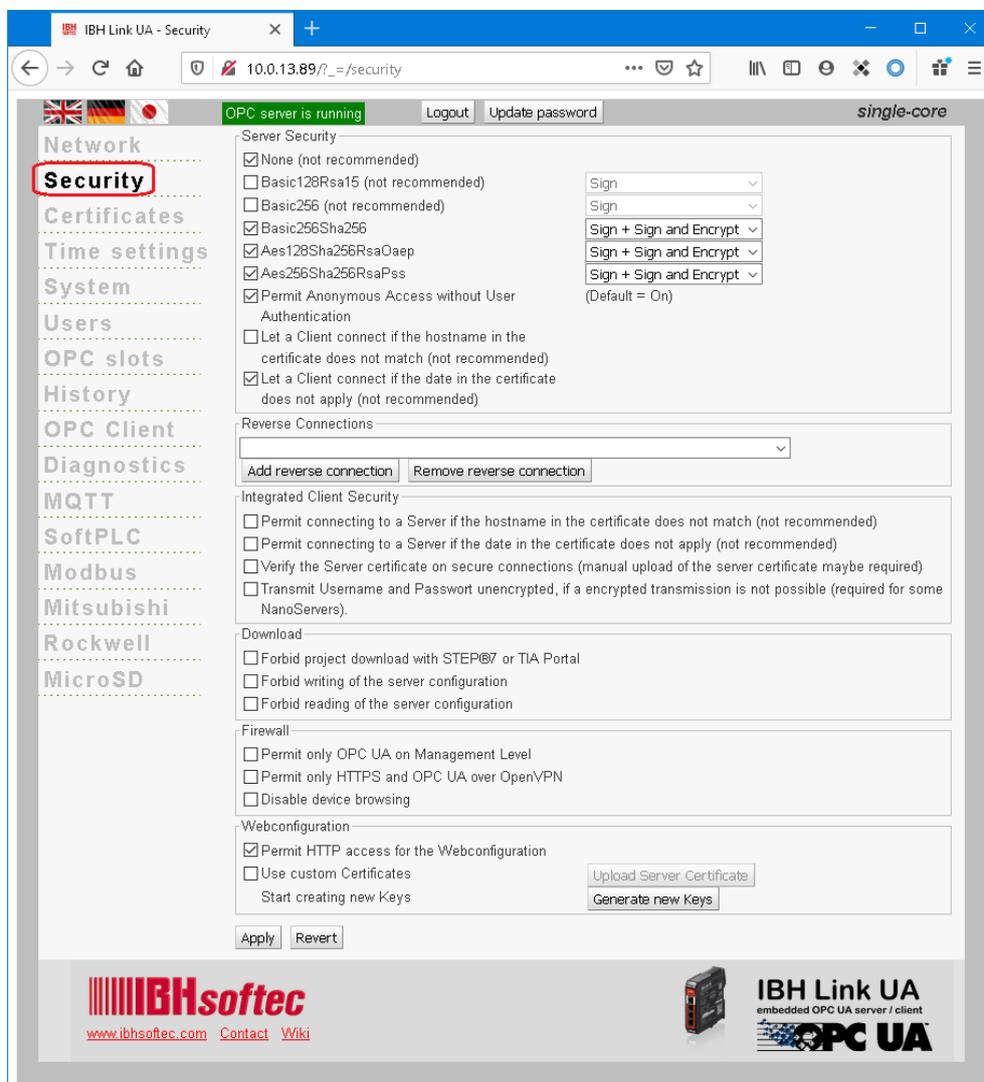
https://wiki.ibhsoftec.com/en/IBH_Link_IoT:TeamViewer_IoT_License_IBH_Link_UA

1.8 Security browser window

The connection security between an OPC UA client and OPC UA server (also OPC UA server / OPC UA server) is available for selection in this window and can be specified.

To establish a connection between an **OPC UA client** and an **OPC UA server**, security settings must be performed.

The IBH Link UA has a certificate management to enable a secure communication defined by OPC UA (**SecureChannel**). The web browser is used to configure the security levels and manages the certificates.



The mechanisms defined by the **OPC Foundation** are used as a base. **OPC UA Security** includes authentication and authorization, encryption, and data integrity by signing. This allows the control system to be protected against uncontrolled access via a higher-level system.

In the IBH Link UA Browser window **Security**, the security levels offered by OPC UA are listed for selection.

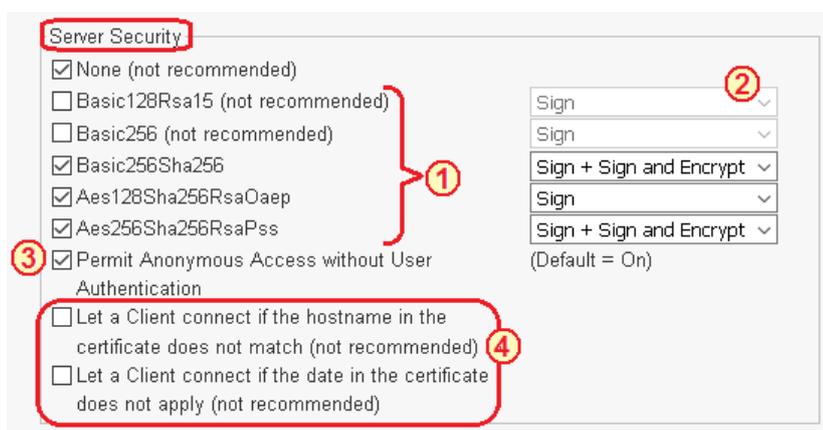
The client queries the server's security configuration via SecureChannel to then set up a communication channel in which the security (confidentiality) and the completeness (integrity) of the messages exchanged are guaranteed.

Note:
 Encrypted messages prevent or at least make it exceedingly difficult for untrustworthy third parties to read the content of the messages that are exchanged between the OPC client and the OPC server.

Server Security

There are different levels of encryption. These are all specified by the OPC UA Foundation.

Note:
 If a change is made in the security browser window, the buttons Apply and Revert are activated. If the change is to be adopted, the click the Apply button.



- ① Is the security level for the OPC UA client / server connection selected, in addition the levels **Sign**, **Sign and Encrypt** as well as **Sign + Sign and Encrypt** can be selected?

- ② The security level is set by opening and selecting.



Sign The messages contain security signs. It is signed with the associated **Private Key** of the **Application Instance Certificate** of the OPC UA client. Signed messages can detect whether a received message has been manipulated by an untrustworthy third party.

Signed messages can detect whether a received message has been manipulated by an untrustworthy third party.

Sign und Encrypt The messages contain security tokens and are encrypted. They are also encrypted with the **Public Key** of the **Application Instance Certificate** of the OPC server.

Sign + Sign and Encrypt The messages contain the security labels of **Sign** and additionally those of the **Sign and Encrypt** definition.

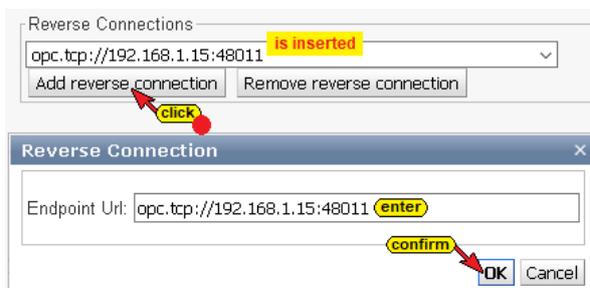
- ③ Anonymous access without user authentication is allowed as a standard and can be deactivated.
- ④ Settings can be made to allow OPC UA client / server connections not recommend for security reasons by the OPC UA specifications.

However, it has been shown that in some applications these settings are unavoidable to establish an OPC UA client / server connection.

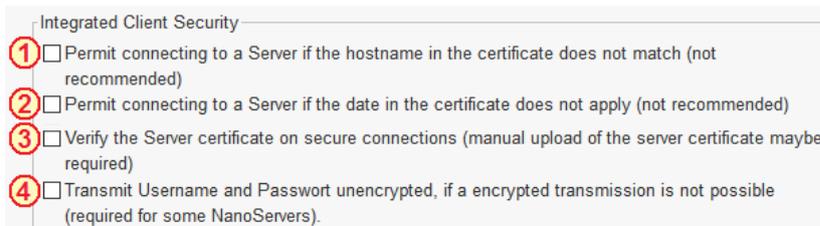
Reverse Connection

In contrast to conventional client-server connections, in which the client establishes the connection with the server, in the **reverse connection** the server actively connects to the client.

An inverse server connection can be set up if the server is in a more protected area behind a firewall than the client. To do this, the endpoint URL of the OPC UA client must be entered. This makes it easier to configure the firewall. Of course, the client must support incoming server connections.



Integrated client security



- ① The host name should preferably be used to connect to a server. If there is no DNS server, no host name is available.

If the option is selected, the absolute IP address can be used for the connection to the server, even if only its host name is entered in the server's certificate. The better way is to include both the host name

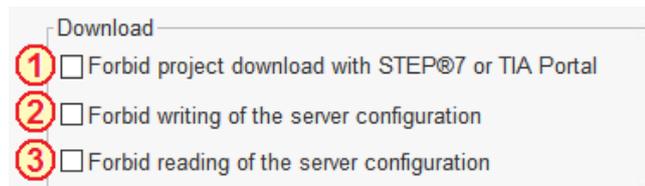
and its IP address(es) in the server's certificate.

This setting is not recommended by OPC UA.

For security reasons, OPC UA works with time stamps. The date and

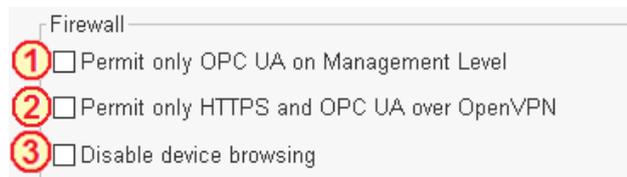
- ② time must therefore be set correctly. If a correct time setting is impossible, this setting must be marked. This setting is not recommended by OPC UA.
- ③ The server certificate is checked for an encrypted connection. For this, it is necessary that the required server certificate is installed on the IBH Link UA and is available as trusted. A manual upload of the server certificate may be required.
- ④ With some OPC UA servers, especially with **NanoServers**, a connection can only be established if the username and password are transmitted unencrypted.

Download



- ① The downloading of STEP® 7 or TIA Portal projects in the IBH Link UA can be prevented.
- ② It is prevented that new server configurations can be written / transferred to the IBH Link UA. The existing server configurations can, therefore, not be changed.
- ③ Server configurations in the IBH Link UA cannot be read out. This prevents a server configuration from being multiplied for reading into other OPC UA servers.

Firewall



- ① The firewall can be instructed only allowing OPC UA connections on the management level. With a web browser, it is no longer possible to address / configure the IBH Link UA via the management level (Ethernet port 1).
- ② The encrypted SSL connection to a virtual network (VPN) can be restricted to the use of the HTTPS, and OPC UA protocols.

- ③ The broadcast functions of the IBH Link UA is prevented. If **ProfiNet IO** devices are present in the same network, the device search should be deactivated, since the Profinet IO data, exchange also works without a connection.

A ping also works when the device search is deactivated.

Web Configuration

The screenshot shows a 'Webconfiguration' window with the following elements:

- ① Permit HTTP access for the Webconfiguration
- ② Use custom Certificates
- ③

Other visible elements include 'Start creating new Keys' and 'Upload Server Certificate' buttons.

- ① For security reasons, access to the configuration of the IBH Link UA should only take place via secure transport encryption (**HyperText Transfer Protocol Secure - HTTPS**).

Therefore, the option **Allow HTTP access to the web configuration** should be deactivated.

- ② Every IBH Link UA has the same parameter set for negotiating the keys for encryption. This is usually not a problem.

However, it is possible to create a new parameter set for the encryption.

If **Use custom certificate** is selected, a dialog box is opened via the **Upload Server Certificate** button. There are buttons here for searching, reading in, and installing the **server certificate** and **private key**.

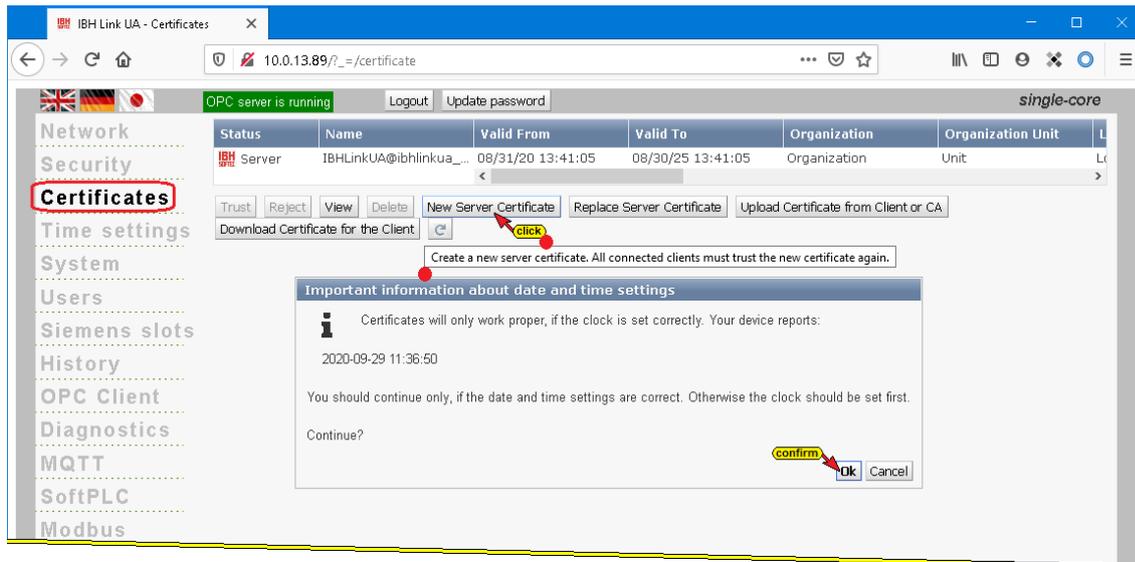
- ③ The button **Generate new Keys** opens a message that must be confirmed to generate a new key. The note must be observed, as the generation of a parameter set for negotiating the keys for the encryption can take several hours.

1.9 Certificates browser window

The existing certificates with data and status are displayed in the window. Buttons are provided to trust, block or delete listed certificates.

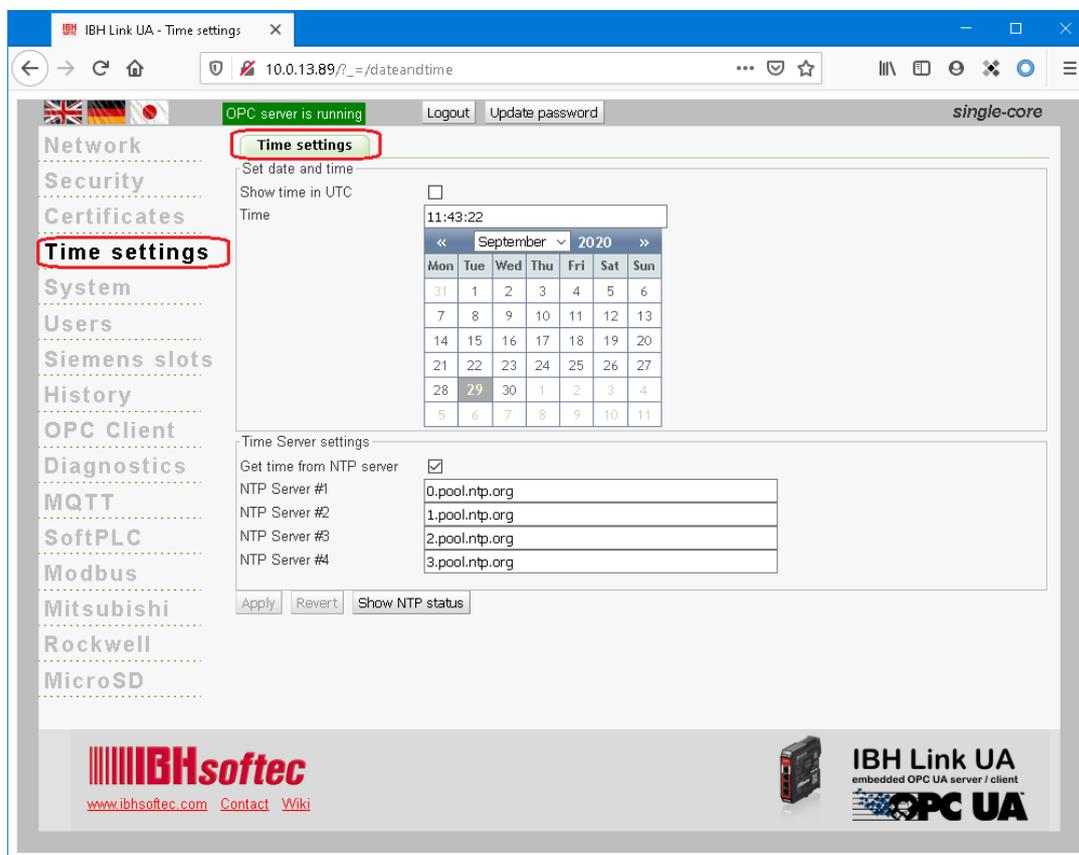
Certificates can be created, downloaded, or read into the designated certificate store.

Certificates browser window



1.10 Time settings browser window

For the correct allocation of certificates, the date and time of the IBH Link UA must correspond exactly to the actual values.



By clicking on **Show NTP status**, the status of the transmitting time server is displayed with their IP address.



NTP status

```

ntpq -pn
ntpq -pn output:
remote refid st t when poll reach delay offset jitter
=====
-193.30.35.11 94.198.159.10 2 u 19 64 377 34.703 -0.921 0.165
+51.75.67.47 207.197.87.124 4 u 40 64 377 31.919 -0.897 0.231
+2a01:4f8:c17:64 147.231.2.6 2 u 29 64 377 34.980 1.056 0.178
*129.70.132.37 129.70.130.70 2 u 38 64 377 39.162 2.094 0.176
    
```

The date and time can be entered manually or automatically via the time server. Four (4) time servers are already preset.

Note:



The date and time must be set correctly because **OPC UA** works with time stamps. Certificates lose their validity if the time comparison is incorrect. A correct time for communication between server and client is, therefore, important.

1.11 System browser window

Information about the IBH Link UA is listed and system settings are offered in the System browser window.

The screenshot shows the 'System' browser window for an IBH Link UA device. The left sidebar has a 'System' tab selected. The main content area displays the following information:

- System:** Device information (IBH Link UA V5.18 Dec 22 2020 15:09:00), Serial number (10331), HW revision (2.0.1 im6 single-core), MAC address 1 (50:2D:F4:19:9D:16), MAC address 2-4 (50:2D:F4:15:A8:07), Variable count (0), CPU load (11.4%), Memory usage (25.6%), Temperature (48.6°C), VBAT_5V (5.00V), VIN_24 (23.80V).
- Backup and Restore settings:** Configuration file (Browse... No file selected), Restore (Upload Configuration, Download), Firmware Update (Browse... No file selected, Upload Firmware).
- Restart IBH Link UA:** Reboot (Reboot).
- Variable Names:** Classic (selected), Compact, S7-1500 compatible, Compatible.
- OPC UA options:** Build structure variables, Update Source Timestamp only on change, Show Byte Arrays as ByteString, Route S7 connections always to slot 2, Client Timeout [ms] (10000), Forbid datatype conversion.

1.11.1 Device Information

System	
Device information	
Firmware Version	IBH Link UA V5.18 Dec 22 2020 15:09:00
Serial number	10331
HW revision	2.0.1 imx6 single-core
MAC address 1	50:2D:F4:19:9D:16
MAC address 2-4	50:2D:F4:15:A8:07
Variable count	0
CPU load (%)	15.0
Memory usage (%)	25.7
Temperature (°C)	49.2
VBAT_5V	5.00V
VIN_24	23.80V



Firmware version Firmware Version IBH Link UA V5.18 Dec 22 2020 15:09:00

The version number is important to carry out a firmware update. Only a firmware updated with a higher version number should be done.

Serial number Serial number 10331

The serial number gives the IBHsoftec hotline information about the series and the age of the device.

HW revision HW revision 2.0.1 imx6 single-core

The HW revision indicates with which firmware version (HW1, HW2 SC or HW2 QC) a firmware updated can be carried out (see page 1 - 40).

MAC addresses MAC address 1 50:2D:F4:19:9D:16
MAC address 2-4 50:2D:F4:15:A8:07

The IBH Link UA (SC, QC) has two separate MAC addresses. One MAC address is for the management level, and the other MAC address is for the three ports of the control level.

Variable count Variable count 0

The number of variables registered as OPC UA variables is displayed.

Hardware information CPU load (%) 15.0
Memory usage (%) 25.7
Temperature (°C) 49.2
VBAT_5V 5.00V
VIN_24 23.80V

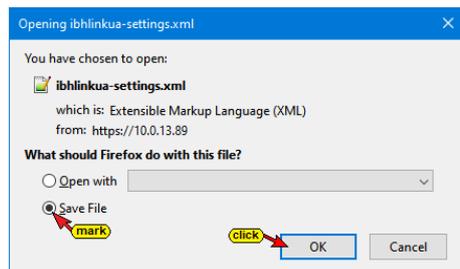
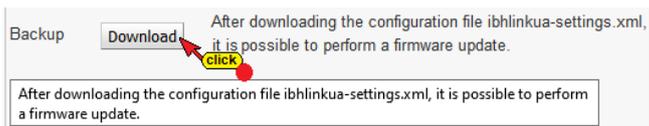
The current CPU load, memory usage and temperature as well as an internal voltage (VBAT_5V) and the supply voltage (VIN_24) of the device are displayed.

1.11.2 Backup and Restor the settings

In this field, there are buttons to save or restore the IBH Link UA configuration or to carry out a firmware update.

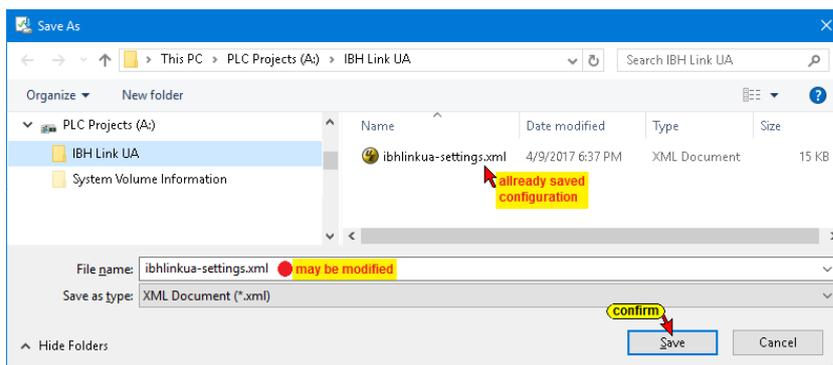
Saving the IBH Link UA configuration

Click on the button **Download** and select **Save File** from the open dialog box.



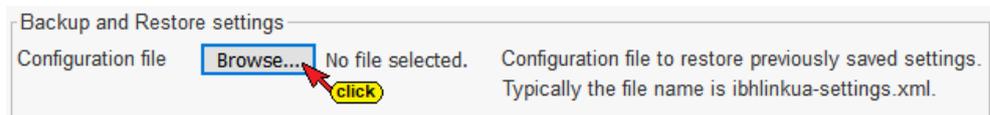
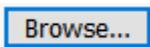
Specify the path and filename in the **Save As** dialog box and confirm by clicking **Save**.

This procedure saves the existing settings.

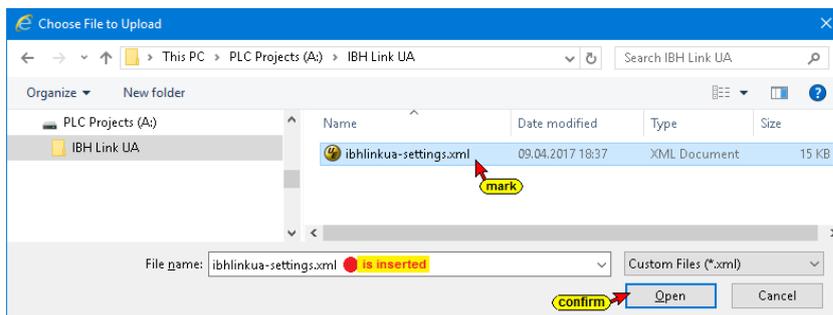


Restore the IBH Link UA configuration

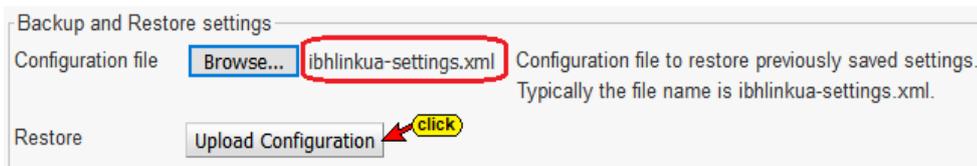
An already saved configuration can be restored at any time. Click the Browse button.



The **Choose file to upload** window opens.



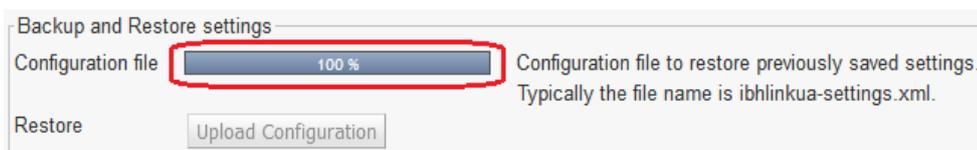
Select the storage location (Path) and the file (ibhlinkua-settings.xml) and confirm with **Open**.



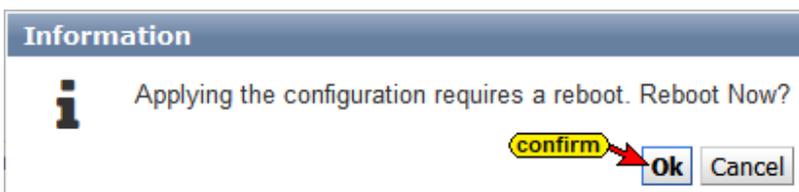
The selected file name is displayed next to the Browse button.

Click the activated **Upload Configuration** button.

The progress of the upload is displayed.



A restart must be performed to complete the configuration transfer.



Firmware Update

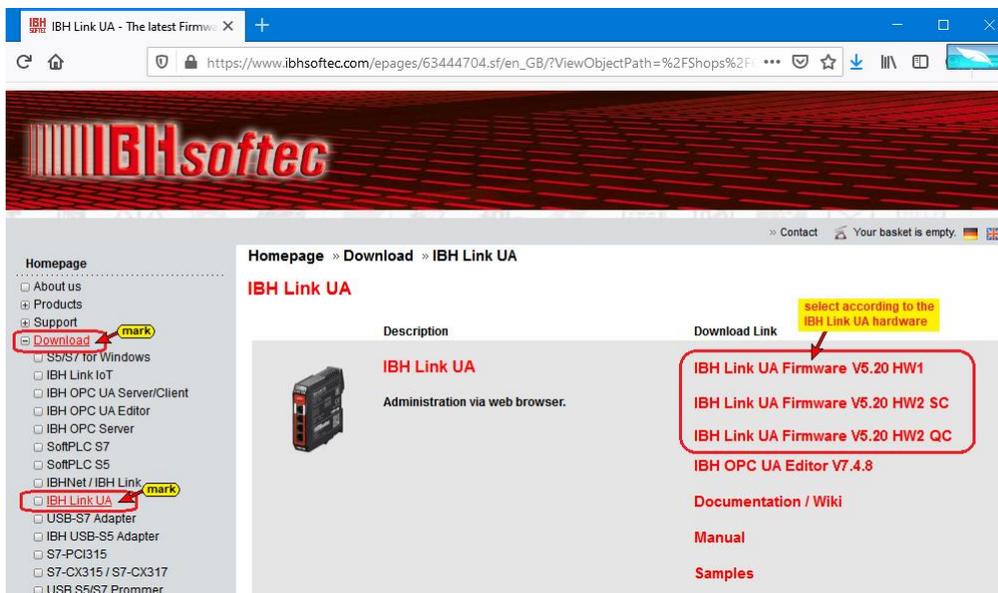
The following procedure is necessary to carry out a firmware update:

1. Save the configuration.

The existing configuration must be saved as described above (click Download).



2. Download the firmware for the IBH Link UA from the IBHsoftec homepage.



There are three firmware versions available for download.

HW1

IBH Link UA Firmware V5.20 HW1

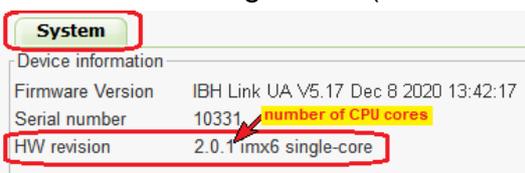
This firmware version is only intended for IBH Link UAs in whose browser window the system, under HW revision, shows a number separated by dots without any additions.



HW2 SC

IBH Link UA Firmware V5.20 HW2 SC

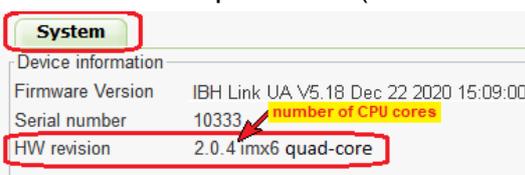
This firmware version is only intended for IBH Link UAs, in their browser window system, under HW revision, a number separated by dots (2.0.1 - the last digit indicates the number of CPU cores) and the Addition imx6 single-core (1 CPU core) indicates.



HW2 QC

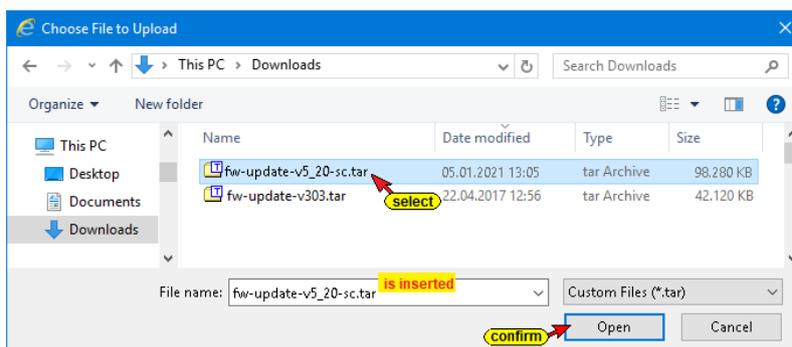
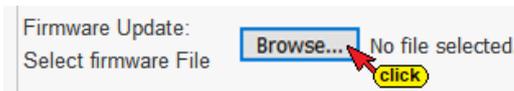
IBH Link UA Firmware V5.20 HW2 QC

This firmware version is only intended for IBH Link UAs, in their browser window system, under HW revision, a number separated by dots (2.0.4 - the last digit indicates the number of CPU cores), and in the Additional quad-core (4 CPU cores) is included.

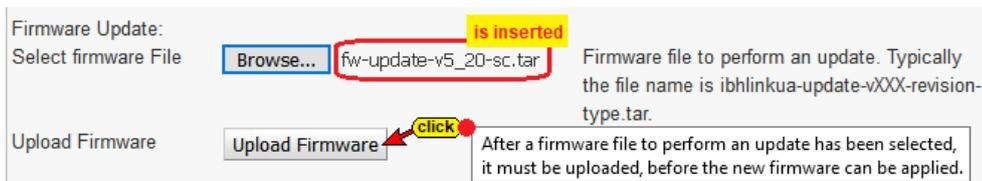


3. Select the saved firmware file

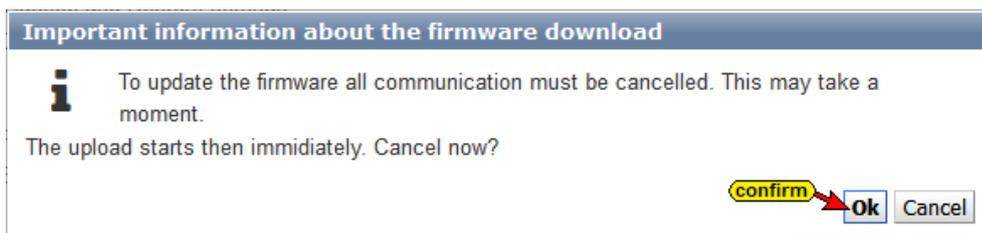
By clicking the **Browse** button, select the firmware file ***.tar** for uploading.



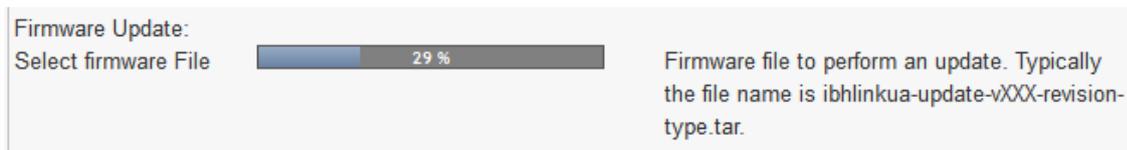
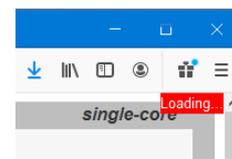
The firmware file *.tar is displayed in the IBH Link UA's System browser window.



- 4. Click the **Upload Firmware** button to load the new firmware into the IBH Link IoT. The new firmware is not yet accepted (updated). Confirm the message.

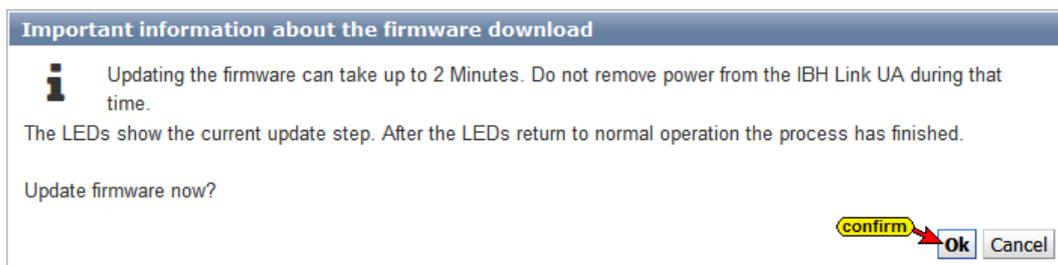


The firmware update process is indicated. In the upper-right corner of the browser window Loading appears.

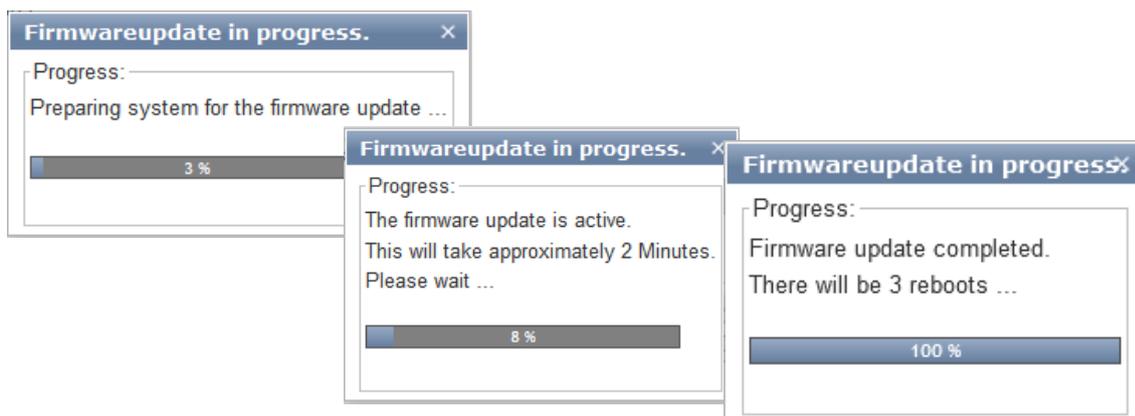


The loading of the firmware is indicated.

If the loading is completed, the following message is displayed.

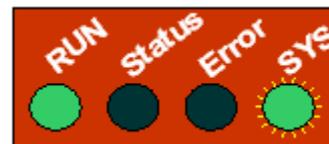


- 5. Confirm the message.

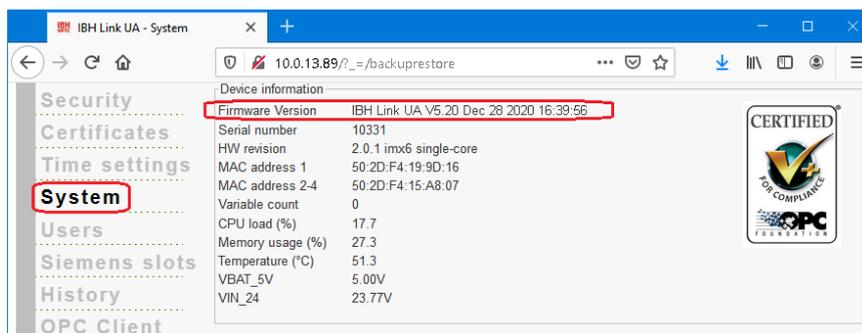


If the LEDs show normal operation, the browser window of the **IBH Link UA** must be reopened and the firmware updates is completed.

In normal operation, the **RUN** LED is lit, the **SYS** LED flashes, and the LED's **Status** and **Error** are off.

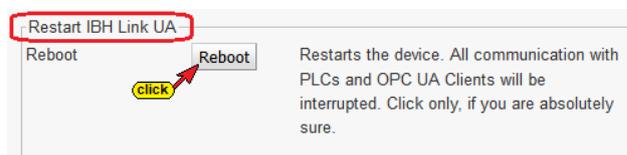


Update completed



1.11.3 Restart the IBH Link UA

By clicking the **Reboot** button, the **IBH Link UA** software is restarted.



1.11.4 Variable format

The representation of the variables can be adapted.

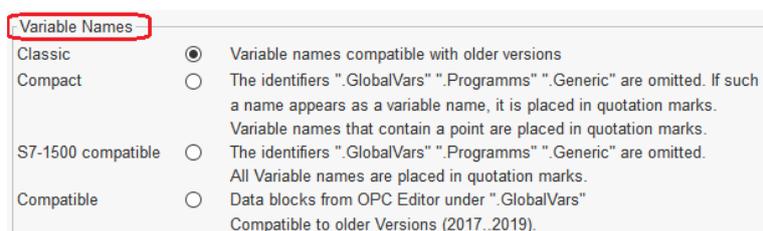
Note:

The programming systems S7 SIMATIC Manager and the TIA Portal allow dots in variable names (e.g. **Switch 7.1**).

The OPC UA specification does not allow periods in variable names.

The S7 SIMATIC Manager programming system does not transfer any variables for a period in the name to an OPC UA server !

The IBH Link UA software offers four options for variable acceptance.



Classic:

The IBH Link UA software only accepts variable names who correspond to the OPC UA specification.

Points in variable names must be removed in the symbol tables (S7 SIMATIC Manager) or TIA Portal) before transfer to the IBH Link UA. The identifiers **".GlobalVars"**, **".Programms"**, **".Generic"** are added to the name of a variable.

The **IBH UA Editor** accepts variable names with a period. These names who contain a point are placed in quotation marks by the IBH Link UA software during transmission.

Identifier	CPU 416.CPU 416-3 PN/DP.Programs.DatenBlock.Var_INT
Identifier	CPU 416.CPU 416-3 PN/DP.GlobalVars.Bit_Var
Identifier	IBH Link UA.CPU414.Generic.Off_2

Compact:

Points in variable names must be removed from the symbol table (S7 SIMATIC Manager) before transfer to the IBH Link UA.

Tag names with periods are accepted in the TIA Portal.

The IBH UA Editor accepts variable names with a period.

Variable names who contain a point are placed in quotation marks by the IBH Link UA software during transmission.

The identifiers **".GlobalVars"**, **".Programms"**, **".Generic"** are omitted in the variable names. If such a name occurs as a variable name, it is placed in quotation marks.

If **Compact** is marked, the identifier of a variable is shorter than in the case of the **Classic** mark.

Identifier	CPU 416.CPU 416-3 PN/DP."GlobalVars"
Identifier	CPU 416.CPU 416-3 PN/DP.DatenBlock.Var_Bool
Identifier	CPU 416.CPU 416-3 PN/DP.Lamp
Identifier	IBH Link UA.CPU414."Off_47.B"
Identifier	IBH Link UA.CPU414.Off_2
Identifier	IBH Link UA.CPU414.Bit_Var

S7-1500 compatible:

Points in variable names must be removed from the symbol table (S7 SIMATIC Manager) before transfer to the IBH Link UA.

In the TIA Portal programming system, dots are allowed in tag names. The variable names who do not correspond to the S7-1500 format are placed in quotation marks by the IBH Link UA software during the transfer and thus brought to the name format of the S7-1500.

The identifiers **".GlobalVars"**, **".Programms"**, **".Generic"** are omitted in the variable names.

Identifier	CPU 416.CPU 416-3 PN/DP."Generic"
Identifier	CPU 416.CPU 416-3 PN/DP."Bit_Var"
Identifier	CPU 416.CPU 416-3 PN/DP."DatenBlock"."Var_INT"
Identifier	CPU 416.CPU 416-3 PN/DP."DatenBlock"."Programms"
Identifier	S7-400-Station_1.CPU 416."On_5.3"
Identifier	IBH Link UA.CPU414."Off.2"

Compatible

Mark if data block variables (OPC tags) are defined as "GlobalVars" in the IBH OPC UA editor / variable transfer in the target name. Only to be used in older IBH OPC UA Editor versions (2017...2019)

1.11.5 OPC UA options

OPC UA options		
Build structure variables	<input type="checkbox"/>	Build structure variables. It will require more memory ! Setting is applied when you restart
Update Source Timestamp only on change	<input type="checkbox"/>	The source timestamp will not be refreshed on every successful read. Instead, only a value change on the controller will refresh the timestamp.
Show Byte Arrays as ByteString	<input type="checkbox"/>	If the PLC variable is a ByteArray, the OPC variable is normally also a ByteArray. This can be changed to a ByteString.
Route S7 connections always to slot 2	<input type="checkbox"/>	With some S7-PLCs the S7 communication points to the CP instead of the CPU. This can be forced to CPU slot 2.
Client Timeout [ms]	<input type="text" value="10000"/>	For some slow responding Servers it can be necessary to increase the timeout for the client. The default is 10000 ms.
Forbid datatype conversion	<input type="checkbox"/>	If the PLC variable has a different datatype than the OPC variable, forbid the conversion to another type, even if the value would fit.

Build structure variables

The use of structure variables is described in the Manual part 2 and part 3. Structure tags are not activated by default.

Update Source Timestamp only on change.

The source timestamp is usually updated every time it is read. When the selection is activated, the source timestamp is only updated when the value changes.

Show byte arrays as ByteString

The IBH Link UA software can allow variables that are defined as **ByteArray** in the PLC to be used as OPC variables in the **ByteString** format.

Route S7 connections always to slot 2.

With some S7 controllers, the S7 connection, if configured with the S7 SIMATIC Manager, points to the CP instead of the CPU. This can be redirected to CPU slot 2.

Client Timeout [ms]

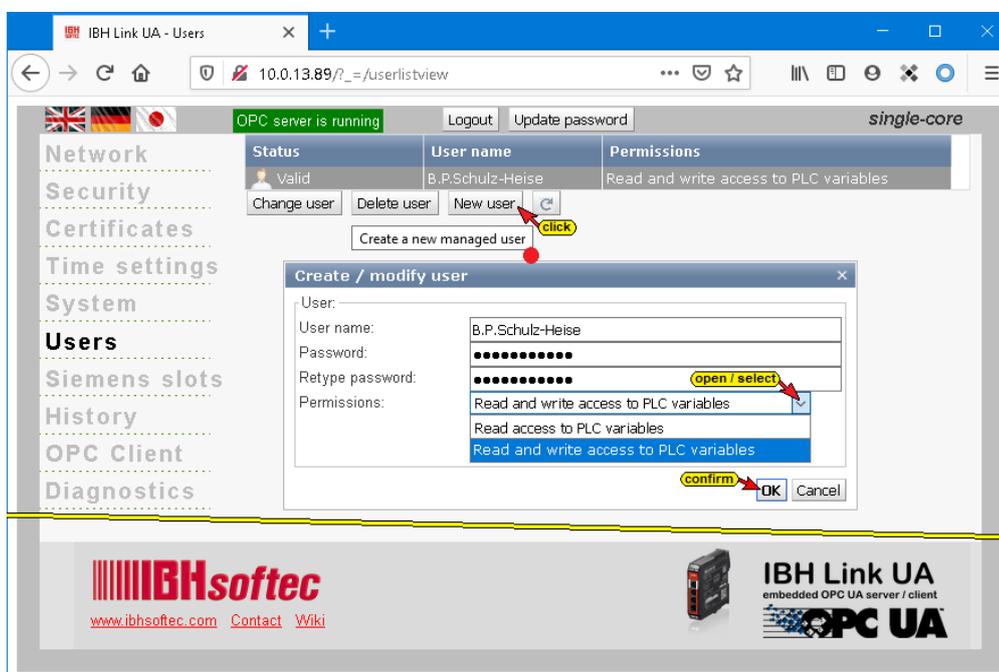
With some slow servers, it may be necessary to increase the timeout for the client. The default client timeout is 10000 ms.

Forbid data type conversion

If the PLC variable has a different data type than the OPC variable, do not convert, even if the value matched.

1.12 Users browser window

Several users with different access rights can be password-protected for the use of the IBH Link UA (**OPC UA user**).



If inadmissible characters (e.g. spaces) are entered in the user name or password, the background of the input line changes to be red. The input must be corrected accordingly.

Spaces are not allowed in the username.

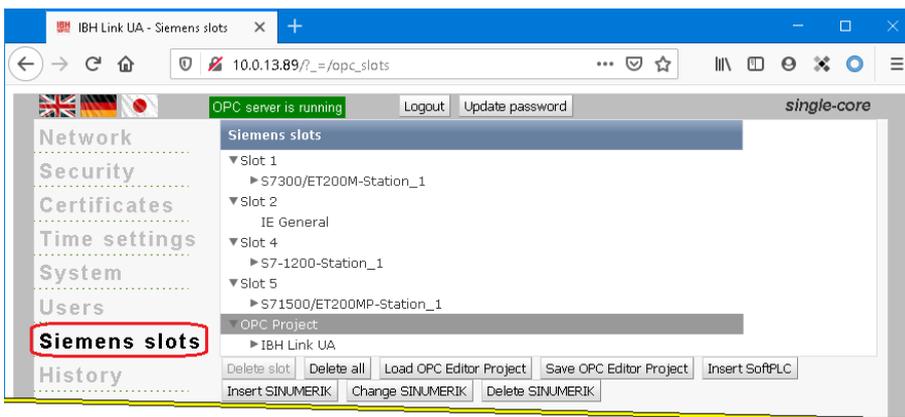
User name:

Password:

The user name for browser access is always **admin**.

1.13 Browser window Siemens slots

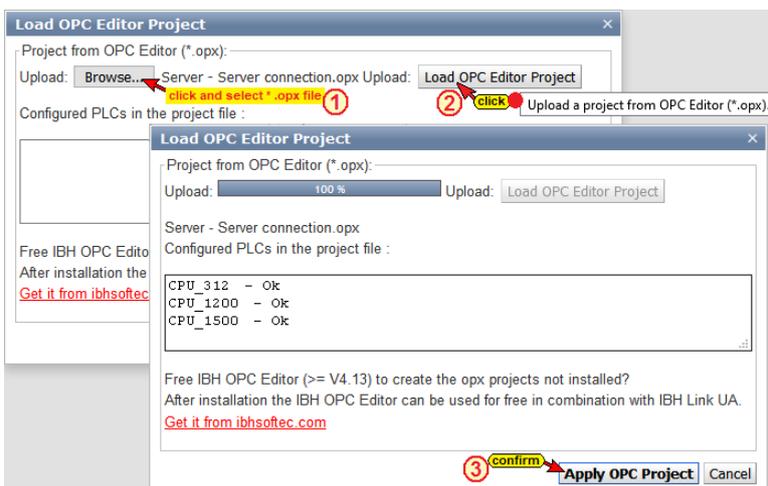
The projects that have been loaded into the IBH Link UA is listed here. Up to 31 STEP 7 and / or TIA projects can be processed in parallel. One slot is used per project.



Load the OPC Editor project

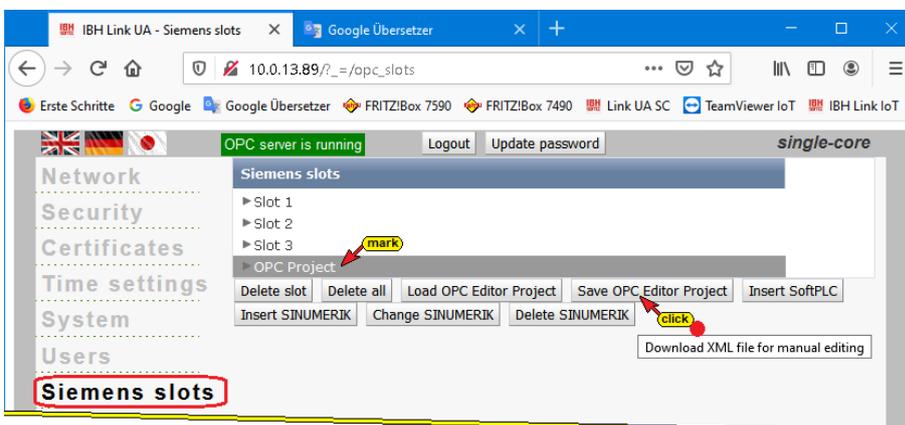
Load OPC Editor Project

An **.XML file** with the filename extension **opx**, which was created for a project with the **IBH OPC Editor** or **IBH OPC UA Editor**, can be accepted as an **OPC project** by clicking on **Load OPC Editor Project**.



Save the OPC Editor project

An OPC project available under Siemens Slots can be saved as an XML file with the file name extension **opx**.

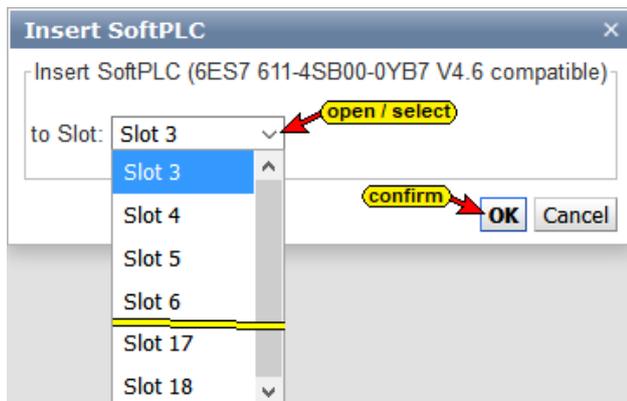


Such a file can be opened for further processing with the **IBH OPC UA Editor**.

Insert SoftPLC

Insert SoftPLC

The IBH Link UA internal **SoftPLC** is activated by clicking on Insert SoftPLC. The slot to be occupied is freely selectable.



Note:

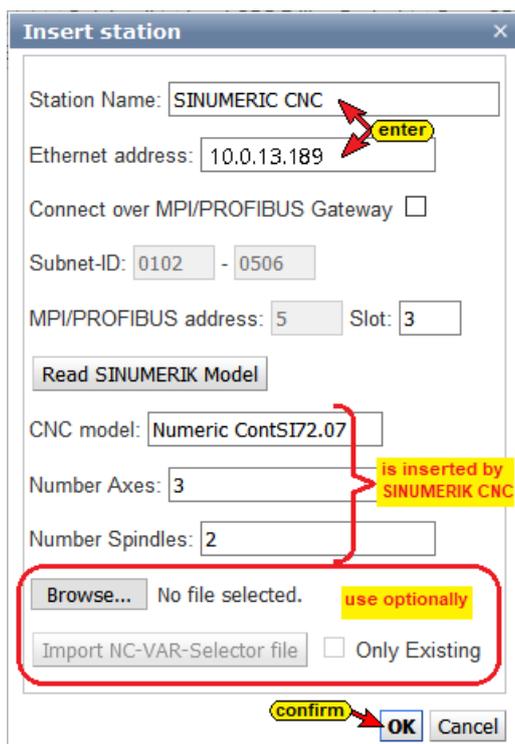


The SoftPLC must never be activated in slot 2.
Slot 2 is reserved exclusively for communication - **IE General**.

Insert SINUMERIK

Variables can be taken as OPC tags from **SINUMERIK CNC** controls of the **PowerLine** and **SolutionLine** series.

The **SolutionLine** series has Ethernet ports (X120 / X130) here the IBH Link UA can be connected directly. If the IBH Link UA is connected to port X130, port 102 of the firewall must be activated in the SINUMERIK.



The CNC controls of the **PowerLine** series do not have an Ethernet interface.

Here the connection is to be established via an **IBH Link S7++**, which is switched to the configured mode. These CNC controls have two (2) connection channels to the SPS (PLC) and five (5) connection channels to the NCK. A connection channel to the PLC (PLC) is always occupied by the connected HMI.

Connect via MPI / Profibus gateway

If this option is activated, the subnet ID, address and slot can be adjusted.

Read SINUMERIK Model

Read SINUMERIK Model

When you click **Read SINUMERIK Model**, a connection to the CNC is established and information that is available in the SINUMERIK is read.

If model, axis, and spindle information can be read, the model name, axis and spindle number are displayed in the dialog box. The complete information, prepared as an **XML** file, is accepted by clicking **OK** under OPC project.

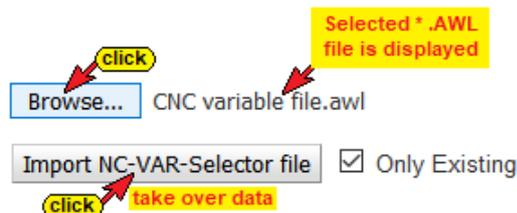
Import NC-VAR file

The SINUMERIK auxiliary program **NC VAR Selector** lists variables according to the SINUMERIK CNC software version. Variables that are to be used as OPC tags can be selected from this list.

The program can generate a file (***.awl**) from a file (***.var**) saved with the **NC VAR Selector** program.

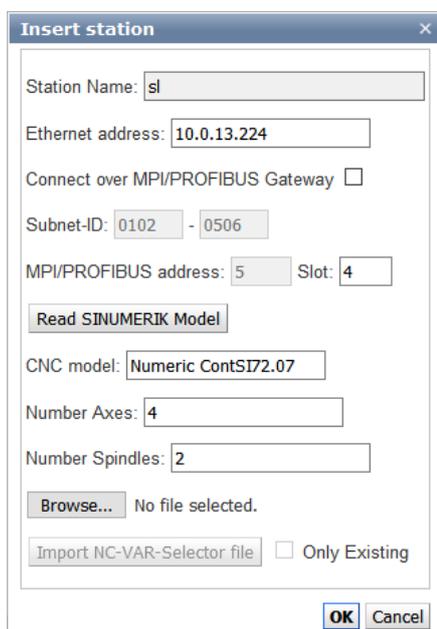
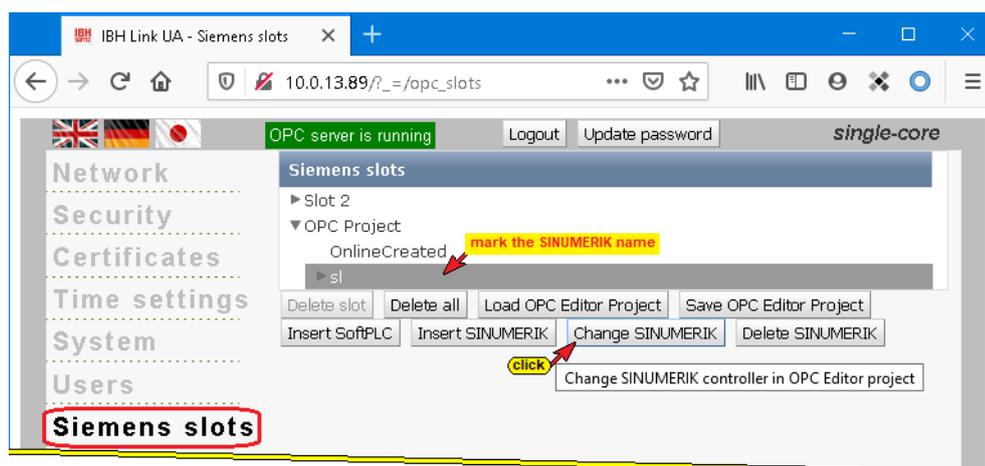
The variable information from such an STL file can be transferred in addition to the data read from the SINUMERIK CNC.

This information, prepared as an **XML file**, is accepted under OPC project by clicking **OK**.



Change SINUMERIK

A project that has been taken over from a SINUMERIK CNC can be changed.



If the name of a SINUMERIK CNC is highlighted, the Insert Station dialog box opens when you click **Change SINUMERIK**. Changes can be made here.

1.14 History browser window

OPC Historical Data Access, also known as OPC HDA, supports access to data stored in a buffer.

From simple data logging systems to complex SCADA systems, historical data can be queried in a standardized way.

The historical data is activated via the IBH Link UA history browser window. The historical data are organized in the IBH Link UA as a ring buffer in the RAM.

History tree

The screenshot shows the IBH Link UA History browser window. The left sidebar contains a 'History' menu item. The main area displays a table of history parameters for various PLCs. A 'History parameter' dialog box is open, allowing configuration of sampling rate, buffer size, and minimum change. The dialog has 'can be changed' labels and a 'confirm' button. A 'Remanent history on' button is also visible at the bottom.

Address space	History active	Sampling Rate	History Buffer Size	Minimum Change
example 7 - multi CPUs S7				
▶ CPU 416 Master				
▶ S7 PLC 1 CPU 312				
▼ S7 PLC 2 CPU 312				
DeviceManual				
DeviceRevision				
HardwareRevision				
Manufacturer				
Model				
RevisionCounter				
SerialNumber				
SoftwareRevision				
▼ Programs				
SupportedTypes				
▼ Counter Values				
MinValue_2	History active	0.5	1000	0
MaxValue_2	History active	0.5	1000	0
Control_ON_2				
Controlling_is_ON_2				
Value_2	History active	0.5	1000	0
▶ Tasks				
DeviceHealth				
▶ S5 PLC 3 CPU 103				
▶ S5 PLC 4 CPU 941				

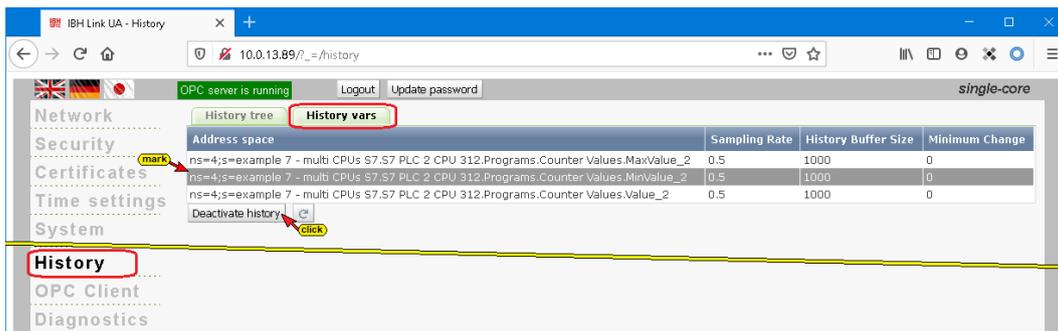
In the opened history parameter input field, the required values must be entered and confirmed.

History vars (variables)

The OPC UA variables declared as history variables are listed. Marked history variables can be removed from the list of declared history variables by clicking on Deactivate history.

For more information see IBH Link UA manual, Part 2 and Part 3 - Connection of a CPU 416 to the IBH Link UA - **Historical data**.

History vars



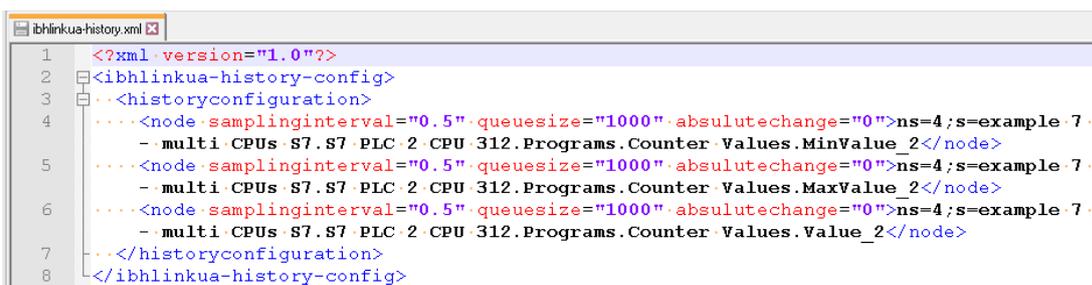
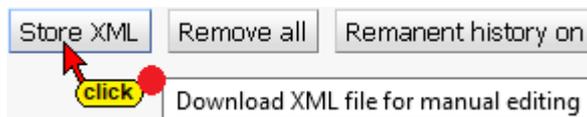
Retentive history

If a micro SD-card is installed and formatted, the *retentive history* function can be activated.



History variable list as XML file

By clicking the **Save XML** button, the currently available history variable list is downloaded as an XML file for manual editing.



By clicking the Load XML button, a manually edited list of history variables is uploaded to the IBH Link UA in XML file format.



1.15 OPC Client browser window

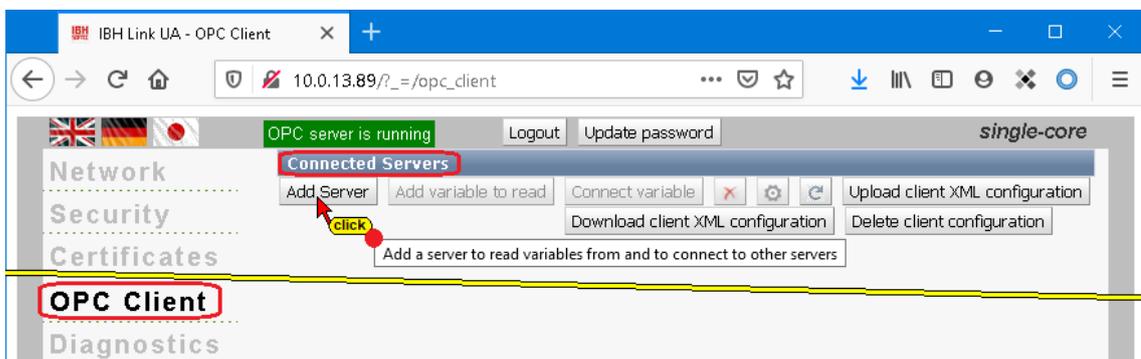
The OPC client function is used to read data from an OPC server and to write this data to the other OPC server. This function can be used by both OPC servers.

The **IBH Link UA** from IBHsoftec is a **server / client module**.

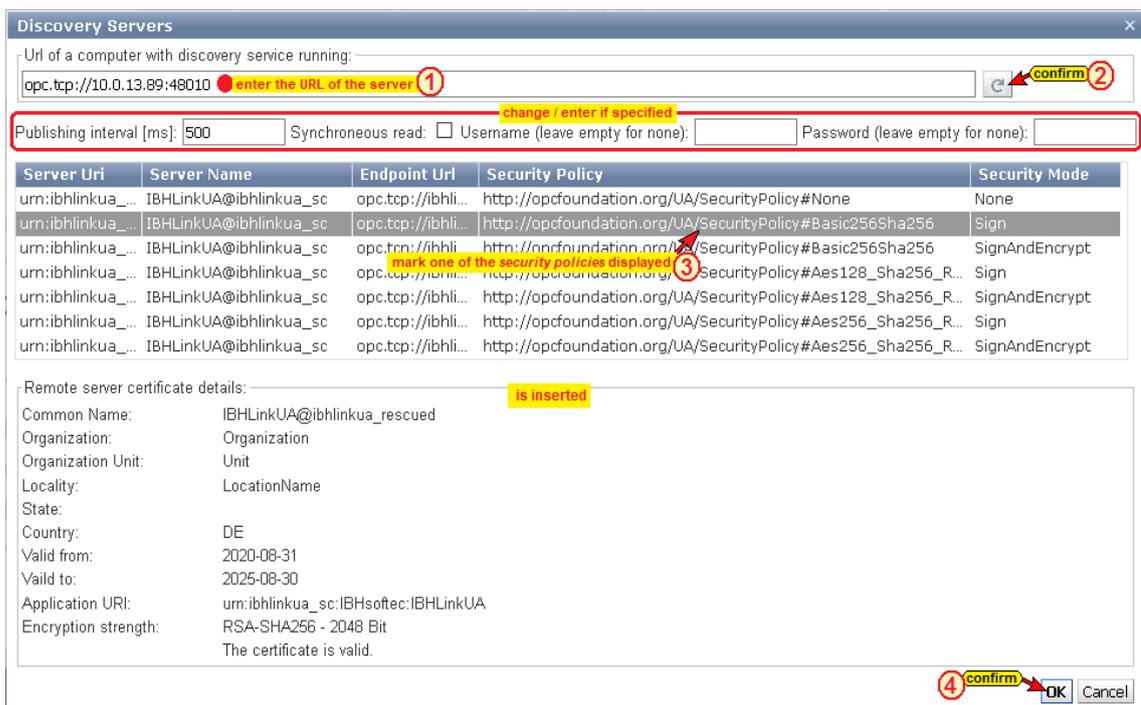
The OPC client function enables data to be exchanged between OPC servers. This makes it possible to exchange variables between two CPUs.

In the IBH Link, UA web browser window **OPC Client**, the server and the variables for the data exchange are specified.

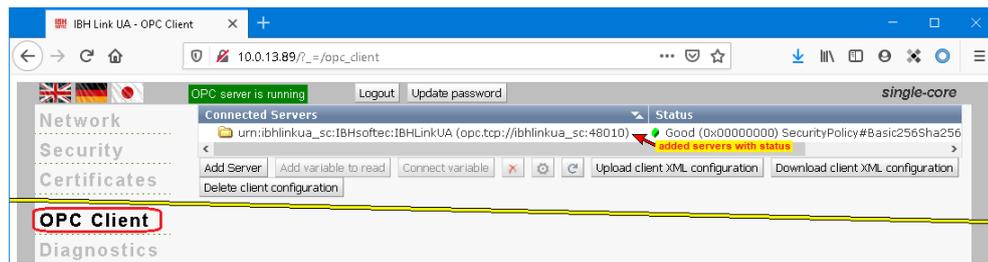
Discover servers



The endpoint URL should preferably be entered with a symbolic IP address. An absolute IP address can be entered in the Security browser window (not recommended).

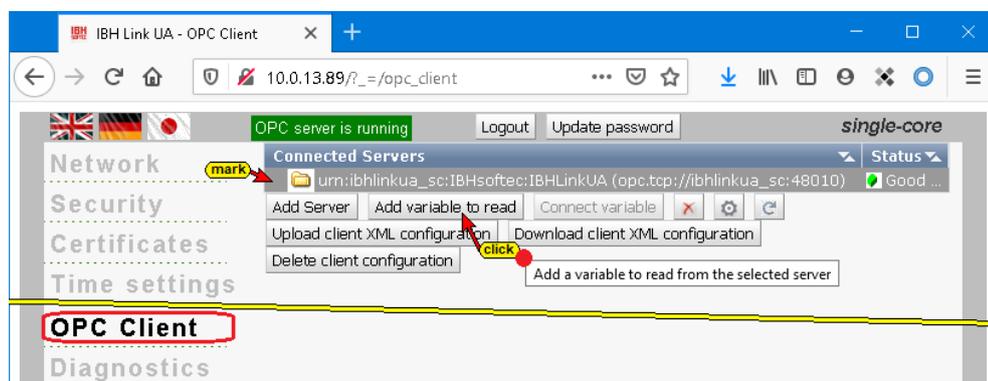


Connected servers with status are listed.

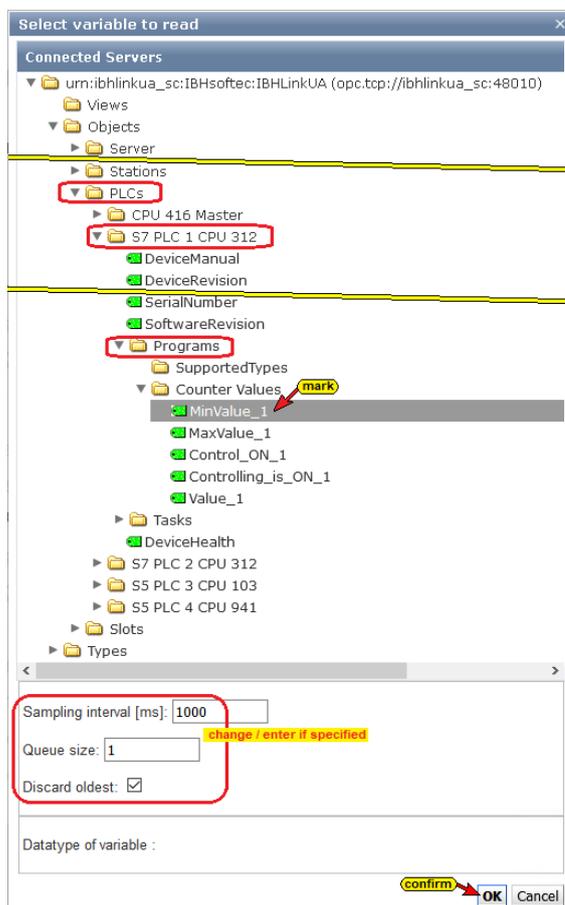


Define read variables

If a listed server is marked, the variables that are to be read by the IBH Link UA client can be selected.

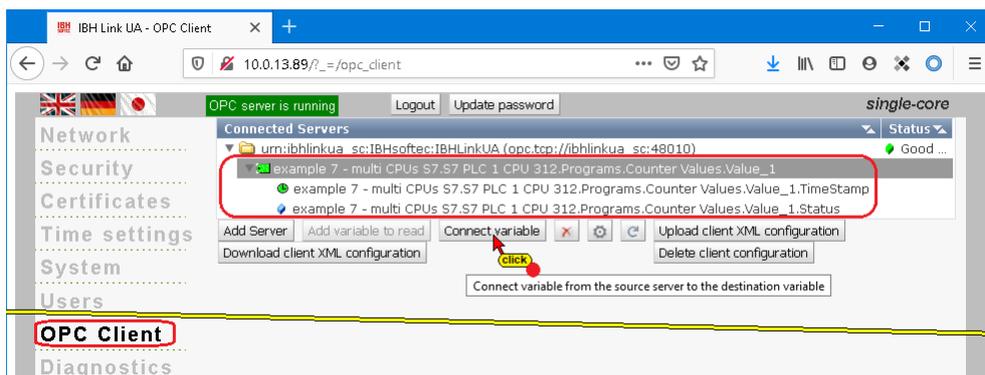


Clicking on Add read variable opens the Select read variable window. The OPC variable that is to be read must be selected here.

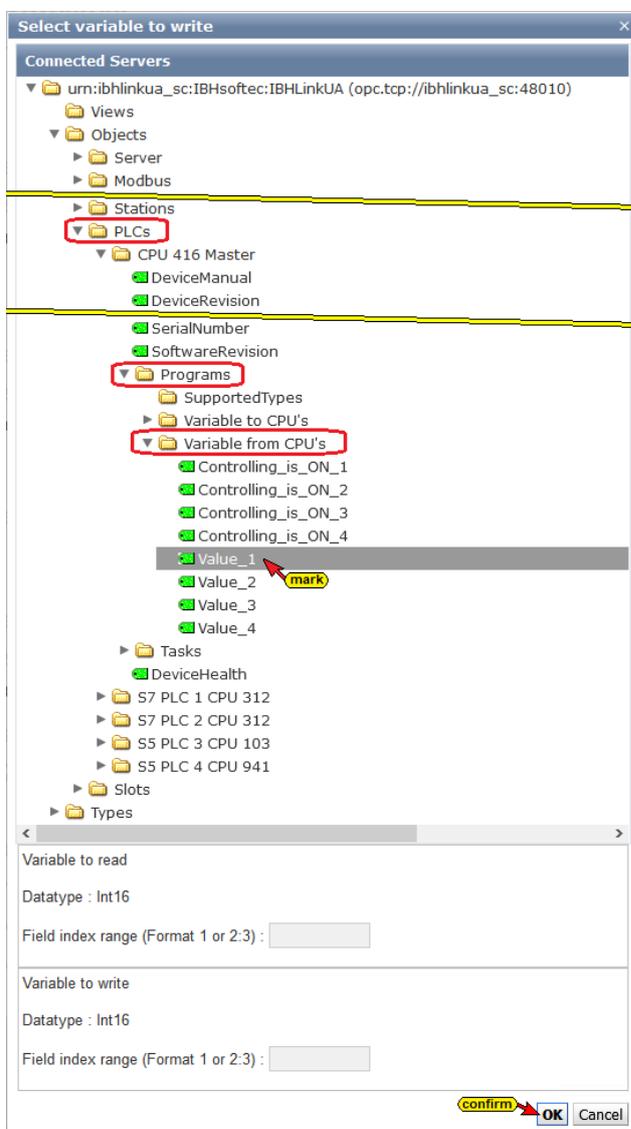


The selected variable (**Counter Values**) as OPC variable with value, time stamp and status) is listed and can be linked to another variable that is available on the same or a different server.

Connect with variable

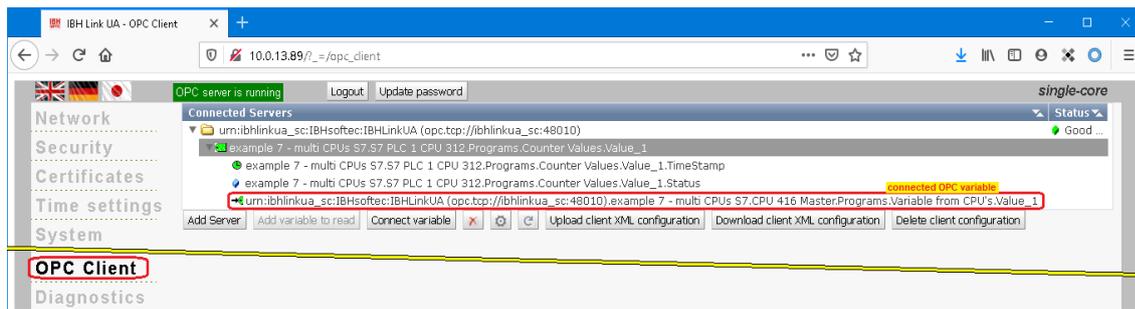


Clicking on **Connect variable** opens the **Select variable to write** window. The OPC variable to be written to must be selected here (as TimeStamp, Status and Value).



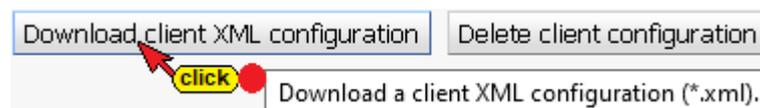
The OPC variable value is available in the data block Variables from CPU's. This variable is connected to the read variable provided. If further variables are to be linked, the procedure described must be repeated for each variable.

The connected OPC variable is listed.

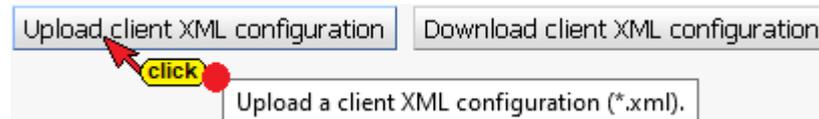


Buttons are available to configure the connection of OPC variables directly via XML files.

By clicking the **Download client XML configuration** button, the currently available configuration of the OPC variable connections is downloaded as an XML file for manual editing.



By clicking the **Upload client XML configuration** button, a manually edited configuration of the OPC variable connections is uploaded to the IBH Link UA in XML file format.

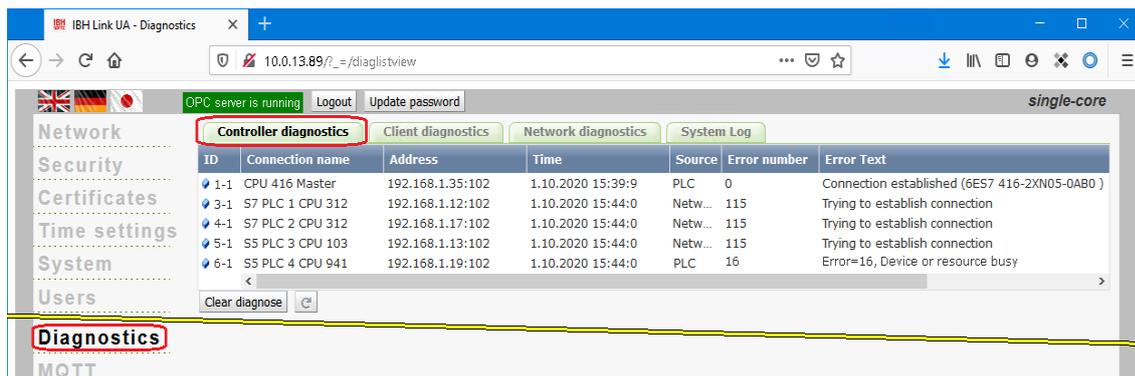


1.16 Diagnostics browser window

The browser window **Diagnostics** has several tabs to display details about established or faulty connections.

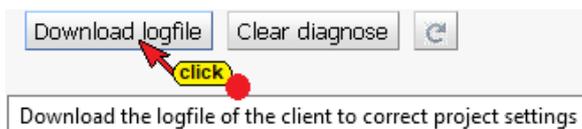
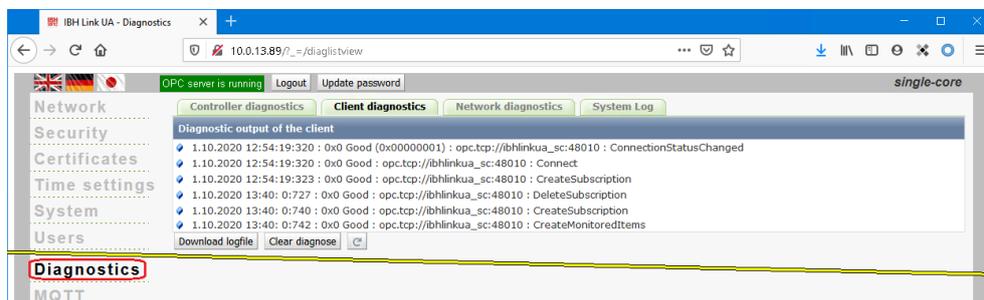
Controller diagnosis

The configured connections and their status (error-free / faulty) are displayed.

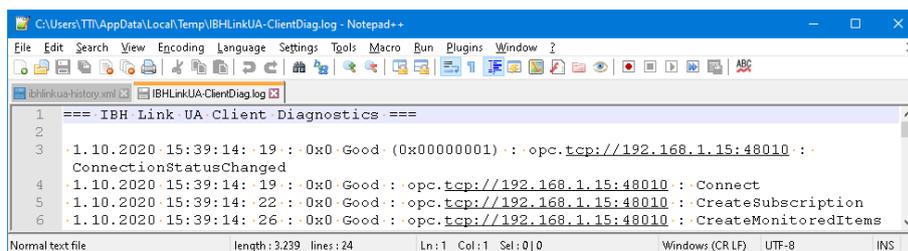


Client diagnostics

The current states of the configured OPC client connections (error-free / faulty) are displayed.

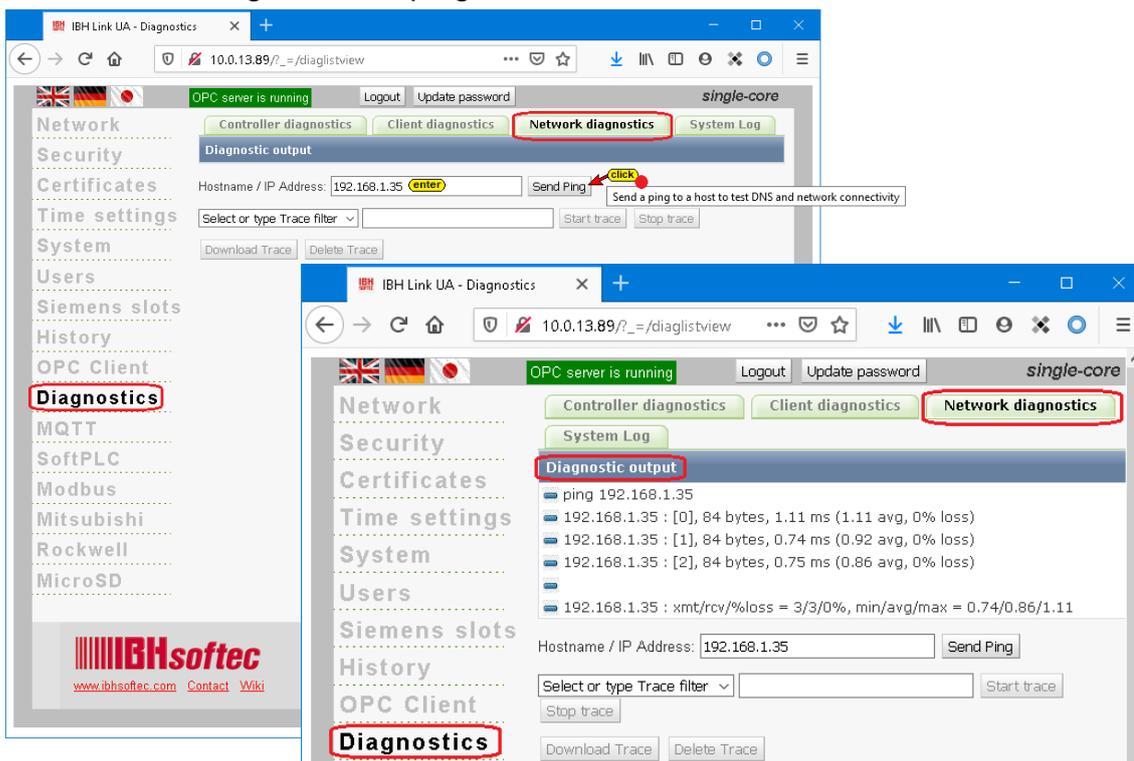


By clicking the **Download logfile** button, the saved states of the configured OPC client connections (error-free / faulty) can be displayed in an editor or saved as a text file.

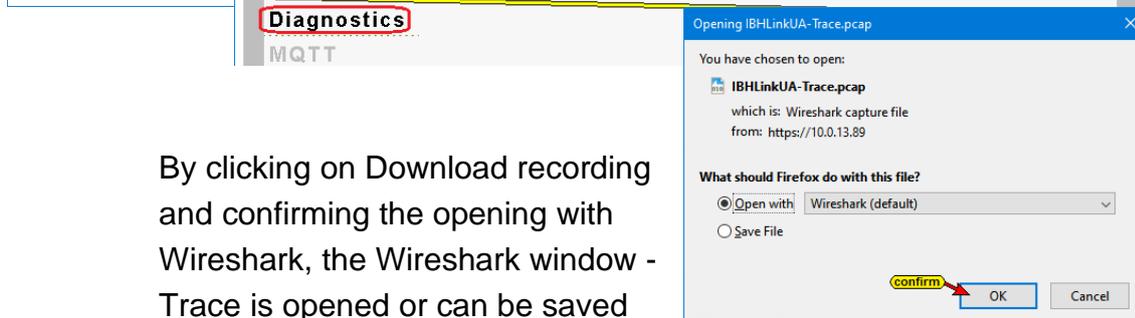
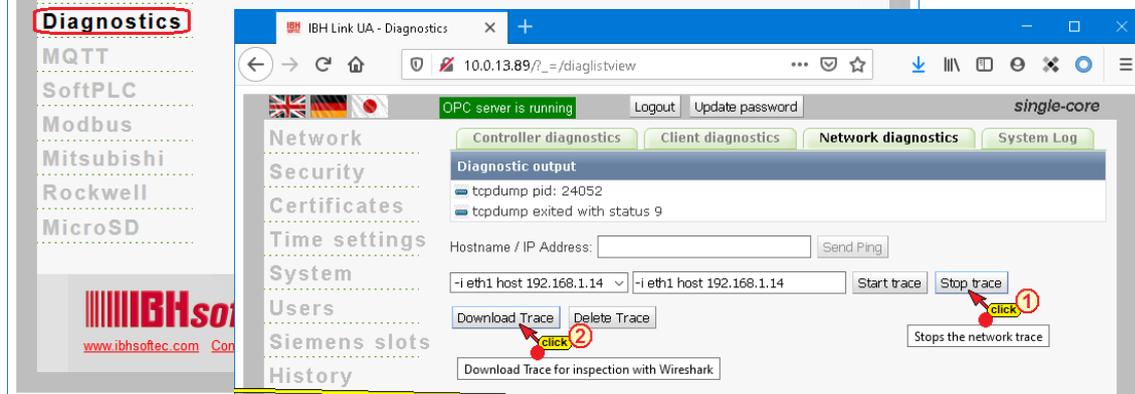
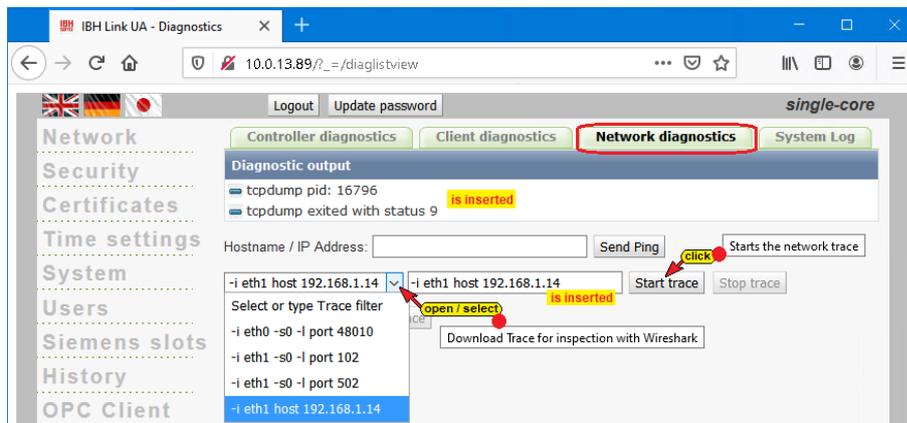


Network diagnostics

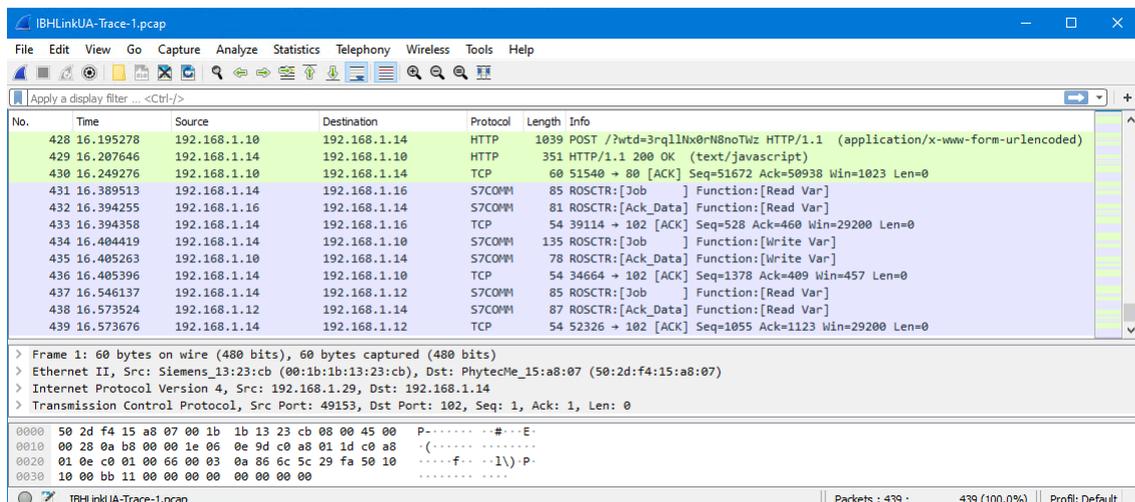
An ICMP ping is sent to the specified IP address (host name) by clicking the Send ping button.



If the Wireshark diagnostic software is installed on the PC, a very extensive network analysis can be carried out.

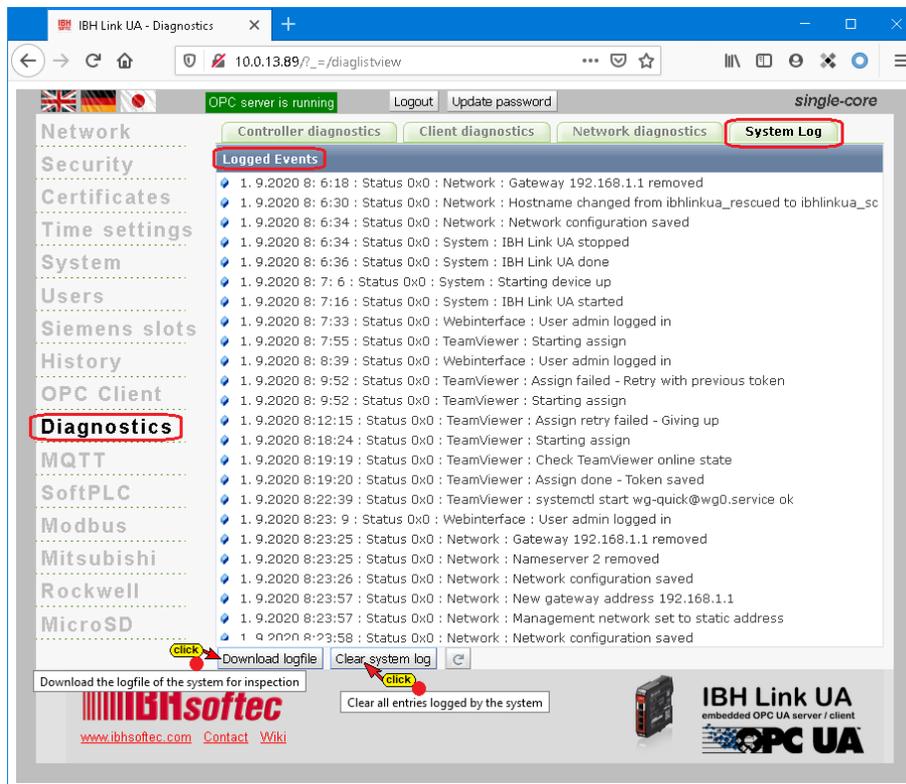


By clicking on Download recording and confirming the opening with Wireshark, the Wireshark window - Trace is opened or can be saved in a file. Since the evaluation of Wireshark-Trace requires some specialist knowledge, this diagnosis should be carried out in the event of a malfunction using the IBHsoftec hotline.



System Log

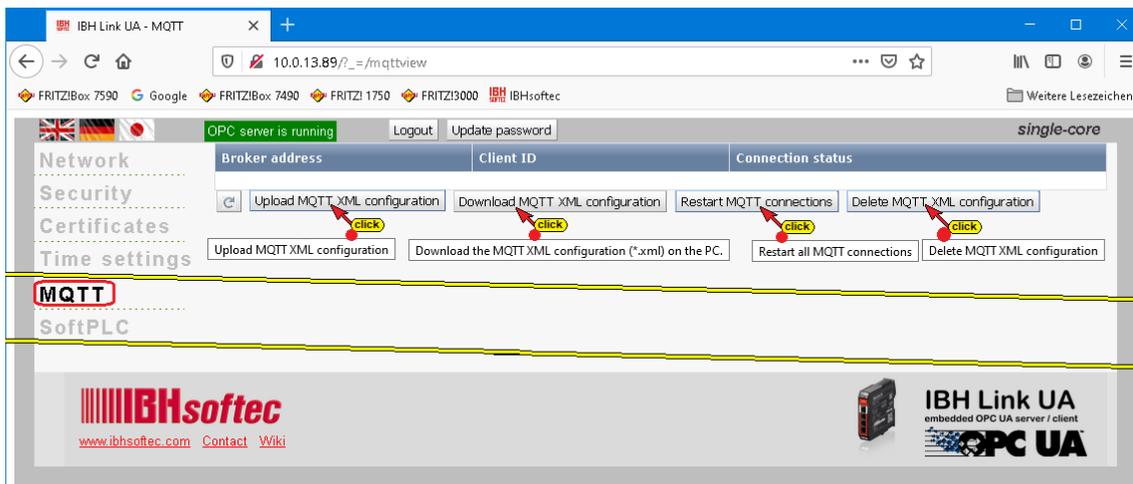
The IBH Link UA diagnosis creates a log file in which IBH Link UA activities are recorded with a time stamp.



Buttons are provided to display the log file in an editor or to save it as a text file or to delete it. In the event of a malfunction, an analysis can be carried out using the IBHsoftec hotline.

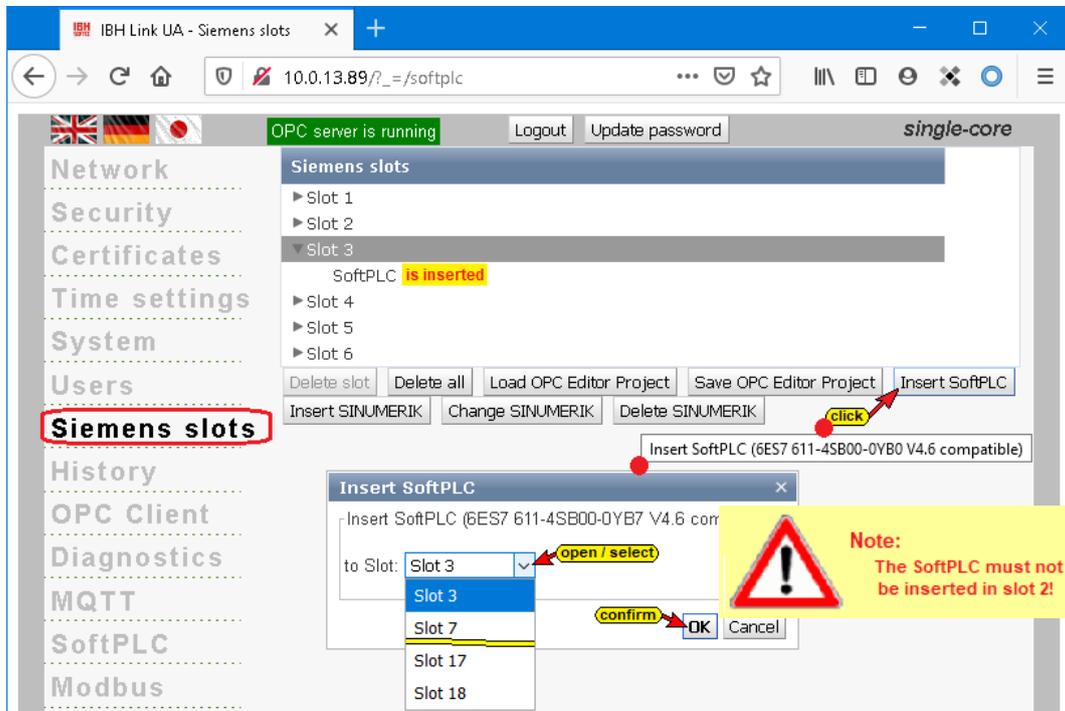
1.17 MQTT browser window

It is possible to load or delete an MQTT configuration. An existing MQTT connection can be restarted. Information about connections to existing MQTT brokers is displayed in the connection status.



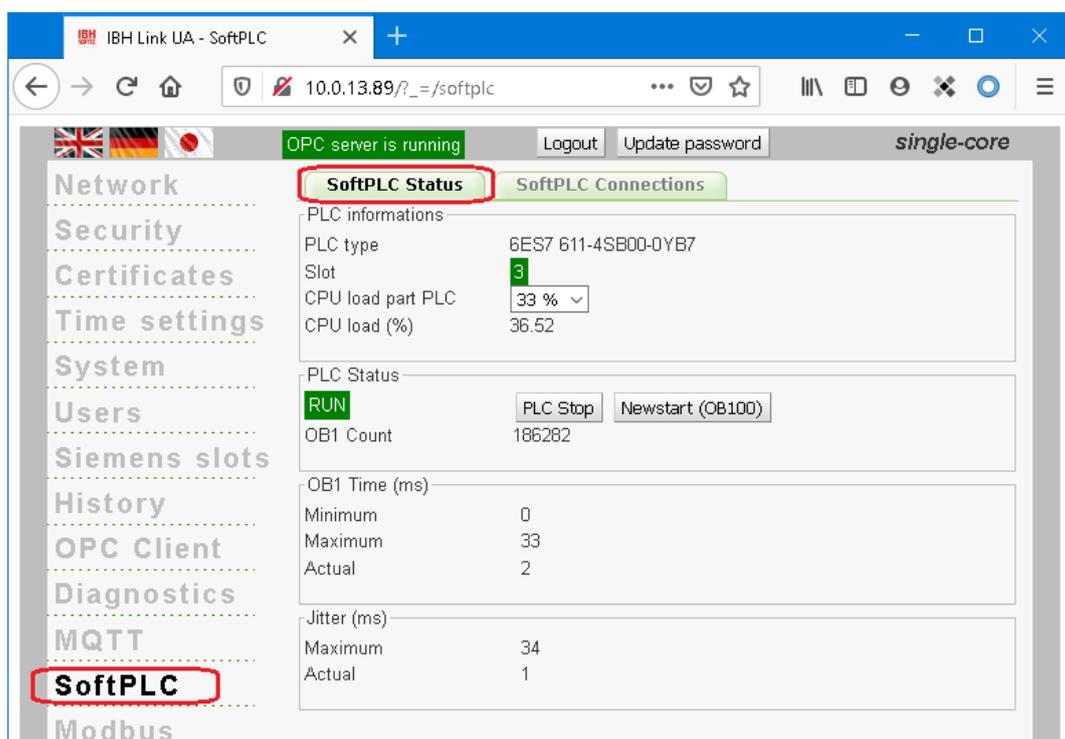
1.18 SoftPLC browser window

The IBH Link UA internal SoftPLC is activated in the **Siemens Slots** browser window.

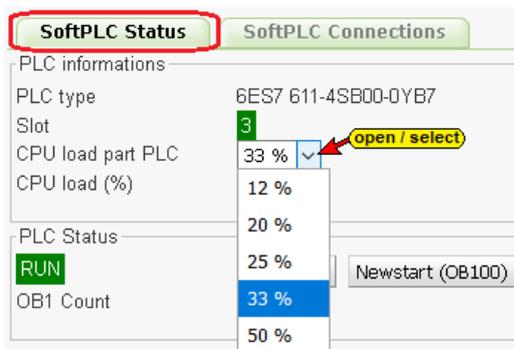


Browser window SoftPLC / SoftPLC status

The SoftPLC status and the settings are listed here. The connections created by the SoftPLC during startup are displayed under the SoftPLC connections tab.



The proportion of CPU power that is transferred to the PLC can be set.



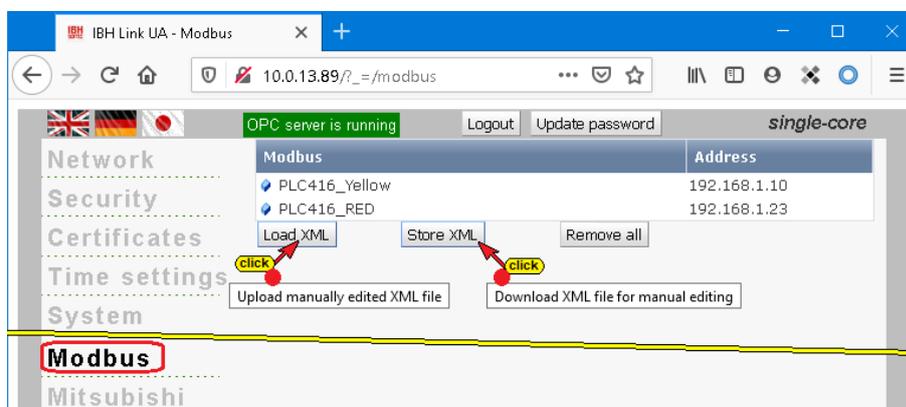
There are buttons to start and stop the SoftPLC.



The handling of the SoftPLC is described in the **IBH Link UA Manual part 2** PLC projects with TIA Portal chapter 3 and **IBH Link UA Manual part 3** PLC projects with S7 SIMATIC Manager chapter 4.

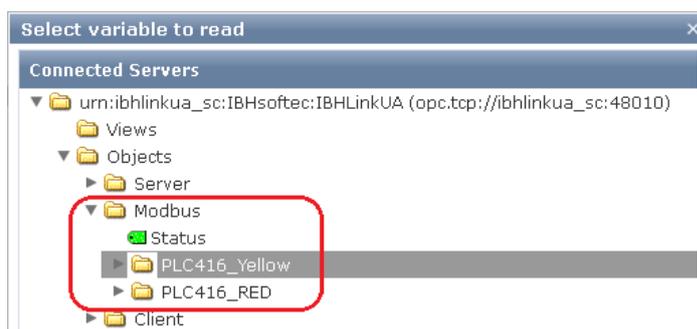
1.19 Modbus browser window

A created Modbus configuration can be transferred directly to the IBH Link UA from the IBH OPC UA Editor.



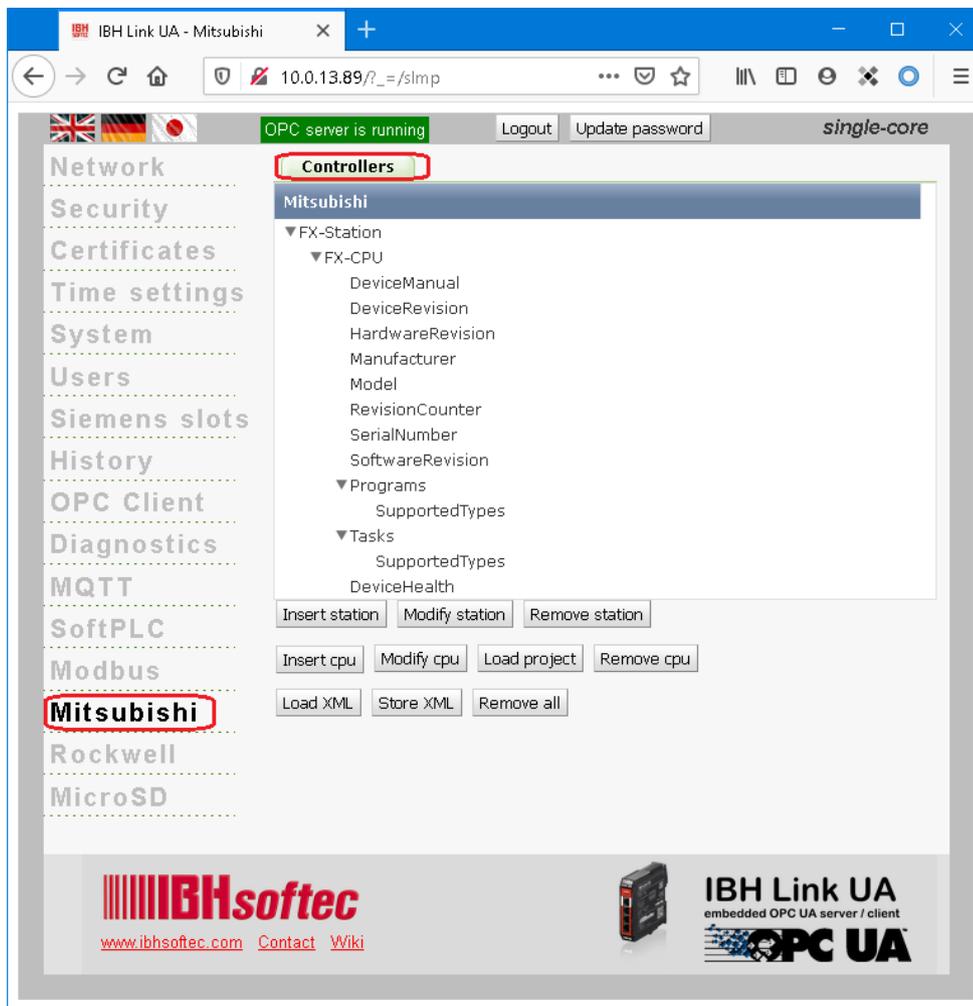
Buttons are provided to configure OPC variables directly via XML files.

The created Modbus variables cannot be seen in the web interface. The existing Modbus variables can be displayed via the OPC Client browser window.



1.20 Mitsubishi browser window

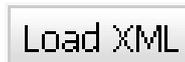
With the IBH OPC UA Editor, a created OPC UA variable configuration for a Mitsubishi controller or a Mitsubishi robot can be transferred directly to the IBH Link UA.



In the **OPC Client** browser window, the existing Mitsubishi controller or Mitsubishi robot variables can be declared as read variables or as variables to be connected.

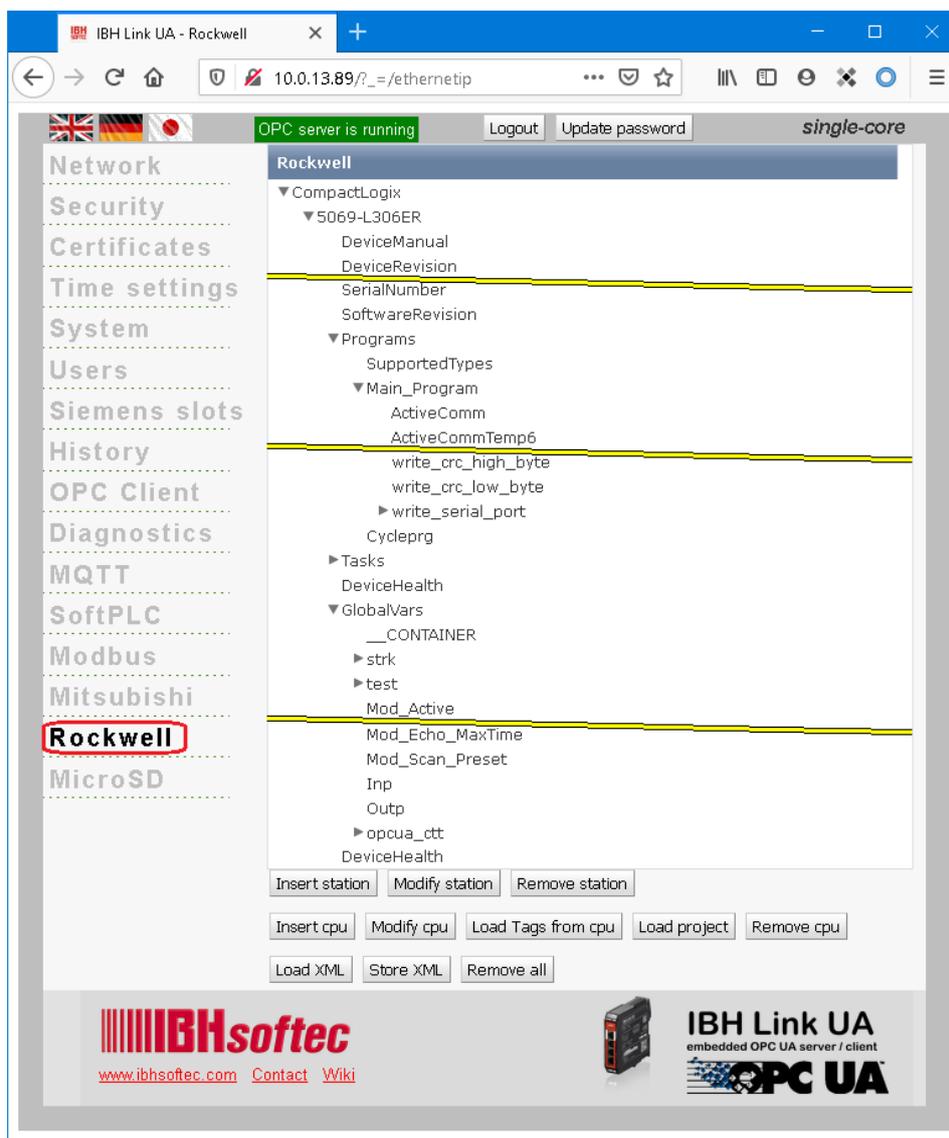
There is also the possibility of inserting or changing a station / CPU and of configuring OPC variables directly via XML files.

The Load XML button enables an XML file exported with the **Mitsubishi Melsoft** software to be loaded directly into the IBH Link UA.



1.21 Rockwell browser window

It is possible to insert or change a station / CPU and to configure OPC variables via XML files. Variables (tags) can be read from Rockwell PLC controllers (**ControlLogix** and **CompactLogix series**) via the Ethernet connection.



If an XML file of a Rockwell PLC controller is loaded into the IBH Link UA, the variables (tags) of the controller are listed.

1.22 MicroSD browser window

The IBH Link UA has a slot for a MicroSD card on the back.

If a Micro SD-card is installed and formatted, the **Remanent History** function can be activated in the **History browser window**.

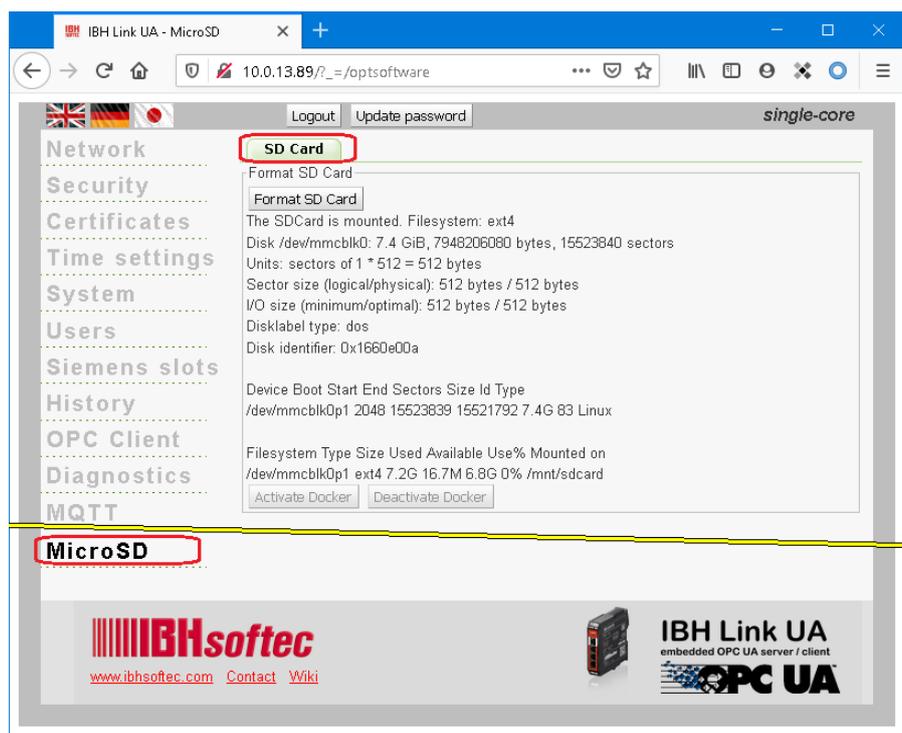
If the function is activated, the **history variables** are also saved on the micro SD-card and can be called up after a failure of the supply voltage of the IBH Link UA.

If there is a formatted SD-card in the IBH Link UA, the currently available configuration is saved on the SD-card.

If the software is reset to factory settings with the reset button, the configuration saved on the SD-card is transferred to the IBH Link UA at the end of the procedure.



Information on formatting is displayed and must be confirmed.



The formatted SD-card will be mounted automatically.

1.23 IBH Link UA default factory configuration

The reset button for resetting the software to the factory settings is in the hardware revisions **HW2 SC** and **HW2 SQ** on the printed side of the IBH Link UA, behind the second ventilation slot above the printing. With hardware revisions **HW1**, the reset button is located behind the middle ventilation slot below the QR code.

The reset procedure resets the IBH Link UA to the factory settings of the firmware currently in the device.



Procedure:

- Power down the IBH Link UA
- Press and hold the reset button
- Power up the IBH Link UA
- Wait until all four LEDs turn red and go off again
- Release the reset button

Note:

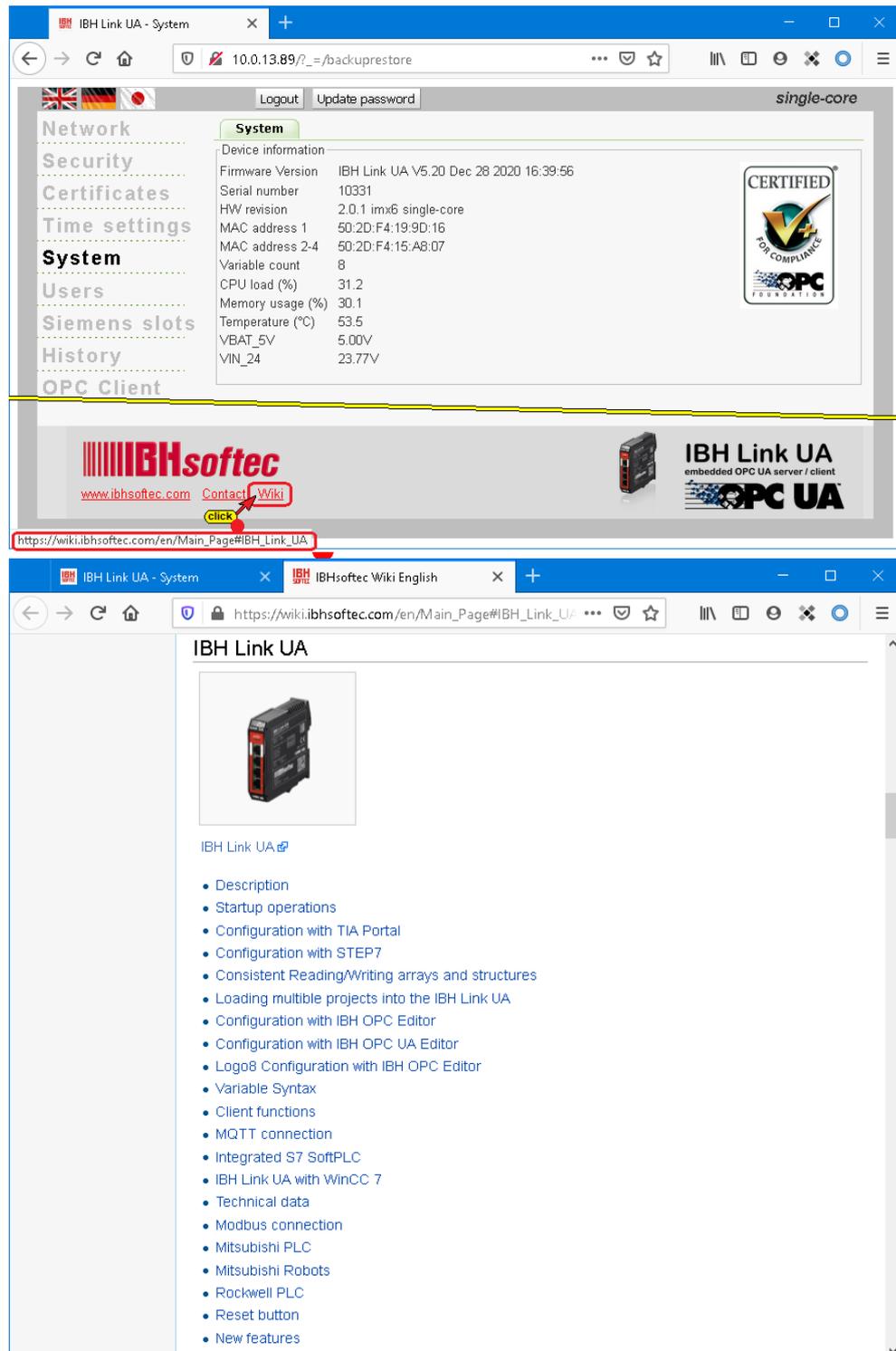
If there is a formatted SD-card in the IBH Link UA, the currently available IBH Link, UA configuration is saved on the SD-card.

If the software is reset to factory settings with the reset button, the configuration stored on the SD-card is transferred to the IBH Link UA at the end of the procedure.

1.24 Open the Wiki

IBHsoftec GmbH maintains a **WIKI site** on the Internet. An extra section for the **IBH Link UA** is provided. Here the use of the **IBH Link UA** is described in detail.

If your PC is connected to the Internet, the WIKI page can be directly called from the **IBH Link UA**.



1.25 Use STEP7 or TIA projects

Projects can be created with the TIA Portal or S7-Simatic Manager programming systems. Up to 32 slots can be used for a project. The communications processor (**Ethernet CP [IE General V8.2]**) in slot 2

is available for transmission to the individual CPUs and the OPC server. One (1) slot is occupied by the OPC server. The remaining 30 slots are intended for CPUs. One slot can be used by the CPU integrated in the IBH Link UA.

If it is not possible for all controls to be combined in a common project, the settings of the communications processor (***Ethernet CP [IE General V8.2]***) must apply to all projects. This is difficult in practice.

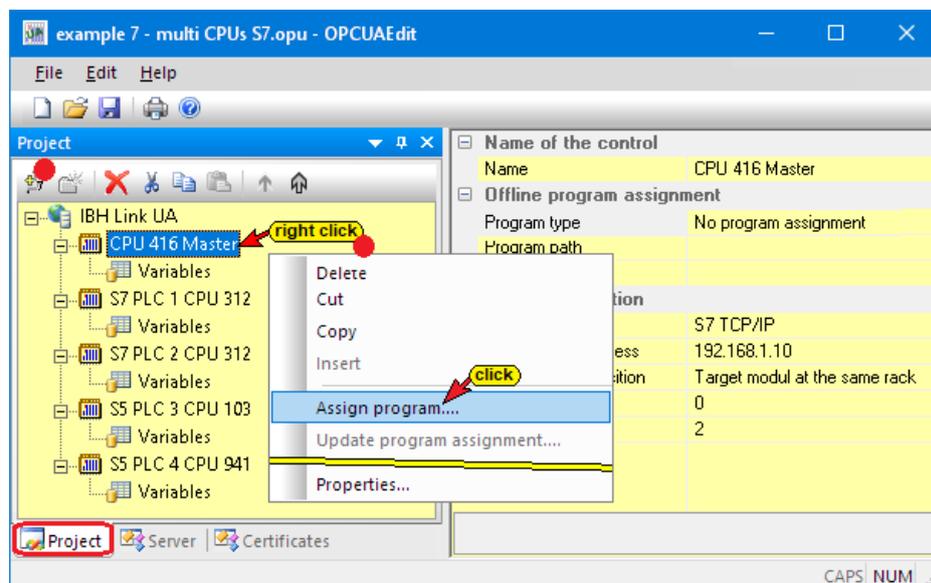
Note:

The slot position of the Ethernet CP [IE General V8.2] MUST be identical in ALL projects (position 2) !

It is therefore recommended to configure the IBH Link UA for several individual CPUs with the ***IBH OPC UA Editor***. The ***IBH OPC UA Editor manual*** contains examples with projects from the TIA Portal and the S7 Simatic Manager.

1.25.1 Example IBH Link UA Editor

Data exchange between several S7 / S5 CPUs. The inserted PLC controls are displayed in the project window. The program can be assigned directly.



1.25.2 Configuration with the STEP® 7 SIMATIC Manager

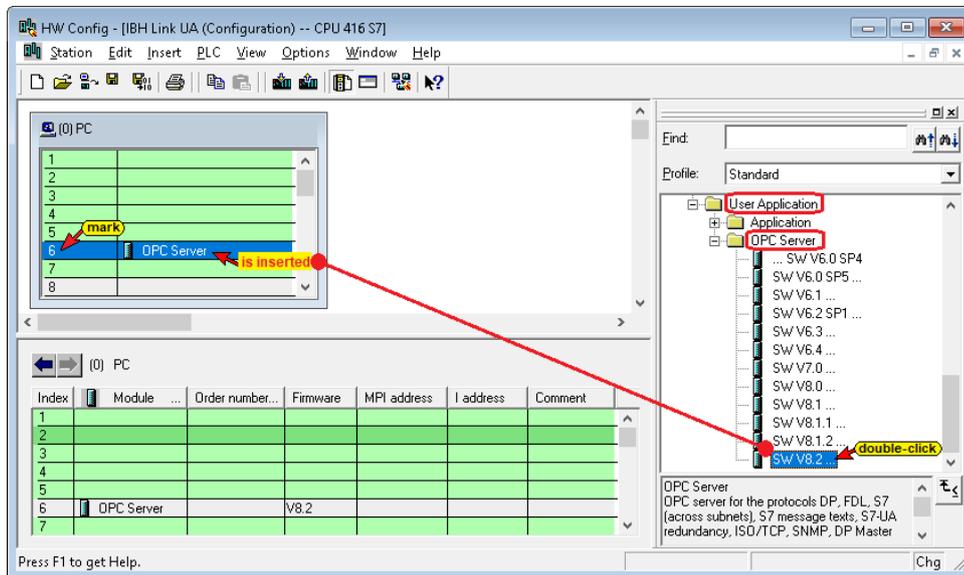
A project that is loaded into the IBH Link UA consists of one or more CPUs, the peripheral modules and a SIMATIC PC station. The SIMATIC PC station is set up



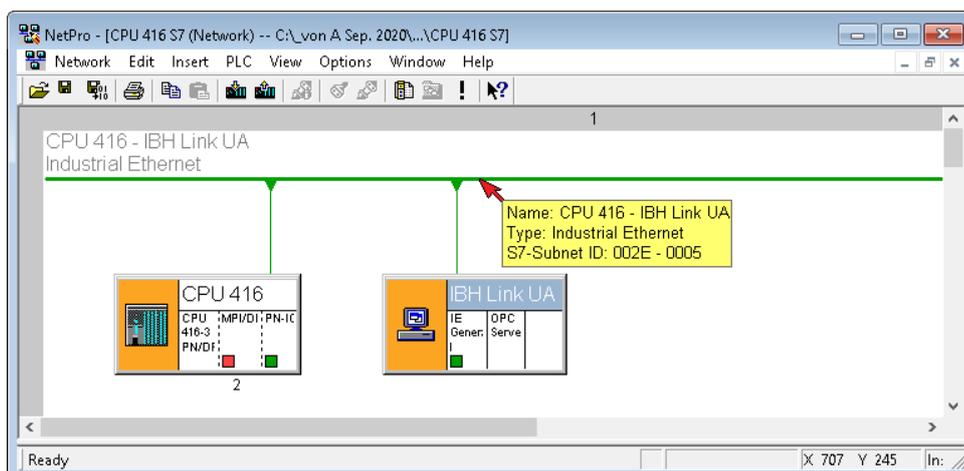
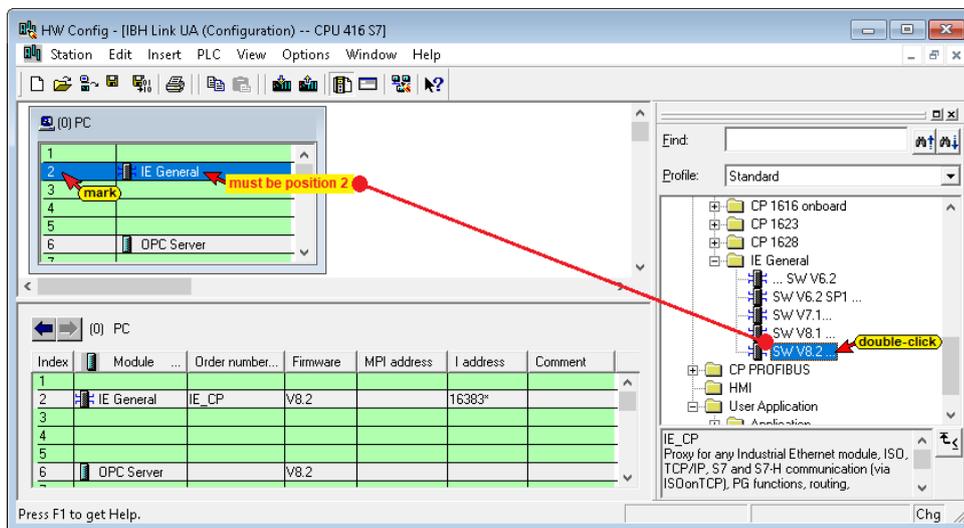
with the Ethernet CP [IE General V8.2]) and the OPC server [Software V8.2].

OPC server configuration

OPC servers can use slots 1 and 3 - 32.



Ethernet CP configuration



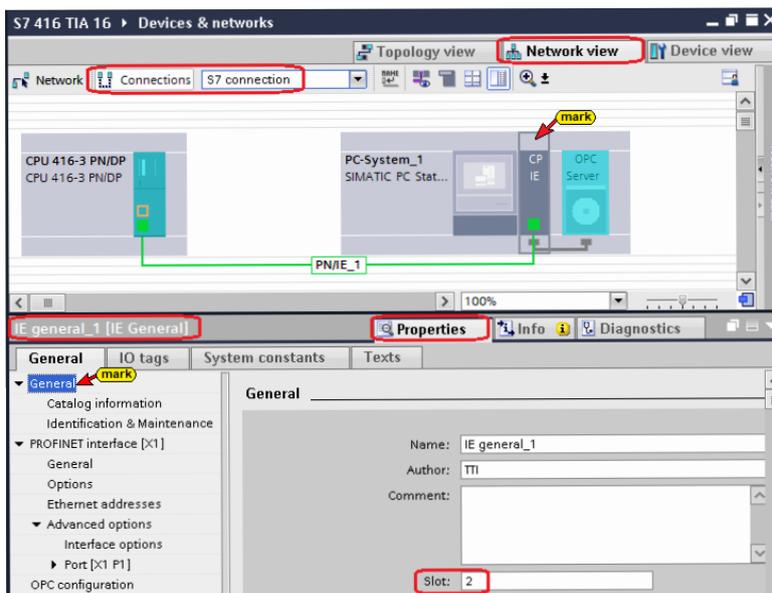
1.25.3 Configuration with the TIA Portal (V13 and newer)

A project that is loaded into the IBH Link UA consists of one or more CPUs, the peripheral modules and an SIMATIC PC station. The SIMATIC PC station is set up with the Ethernet CP [IE General V8.2] and the OPC server [Software V8.2].



Ethernet CP configuration

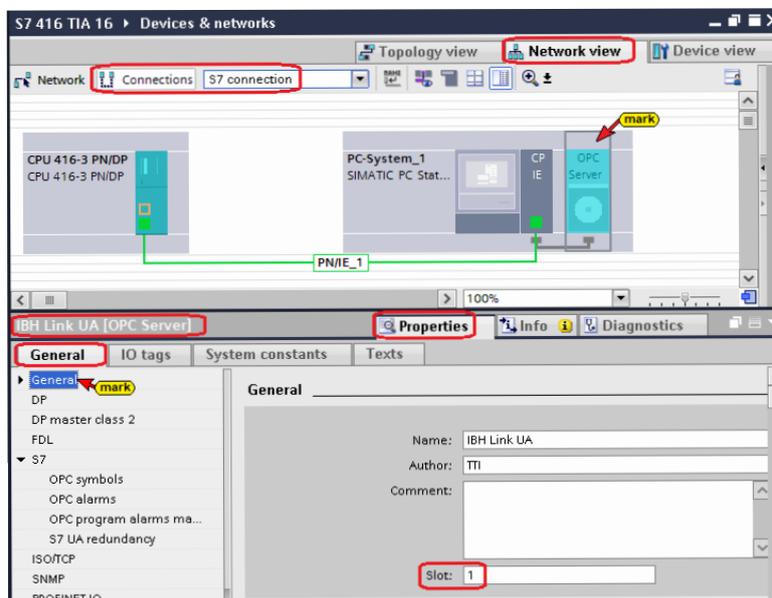
The Ethernet CP must be positioned in slot 2.



OPC server configuration

For the OPC server (IBH Link UA), slots 1 and 3-32 can be used (in TIA Portal V13 the slot is designated with an index).

OPC server on slot (index) 1.



2 Unified Automation UaExpert –OPC UA Client and OPC UA Server

To demonstrate the work of the IBH Link UA, it is helpful to have an OPC client and an OPC Server program running on the PC. It is recommended to use the OPC UA client program **UaExpert** and the OPC Server program **UaCCPServer** from Unified Automation. They can be downloaded via: <http://www.unified-automation.com> Free download requires Unified Automation registration.

The image consists of three screenshots of the Unified Automation website, illustrating the steps to reach the download page for OPC UA Clients.

Top Screenshot: Shows the main website with the 'Downloads' menu item highlighted. A red arrow points to the 'Downloads' link in the navigation bar.

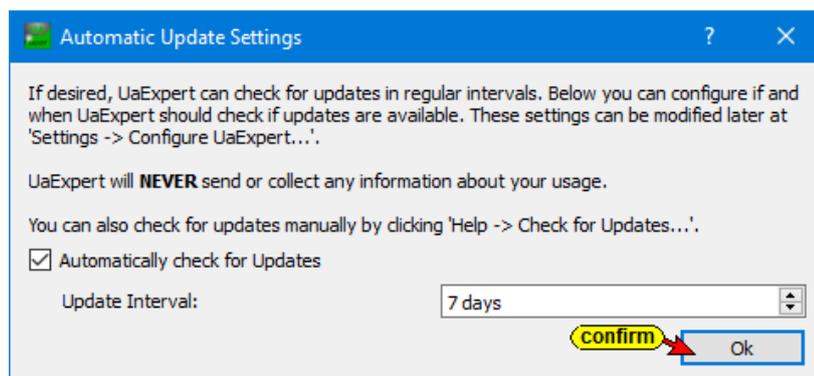
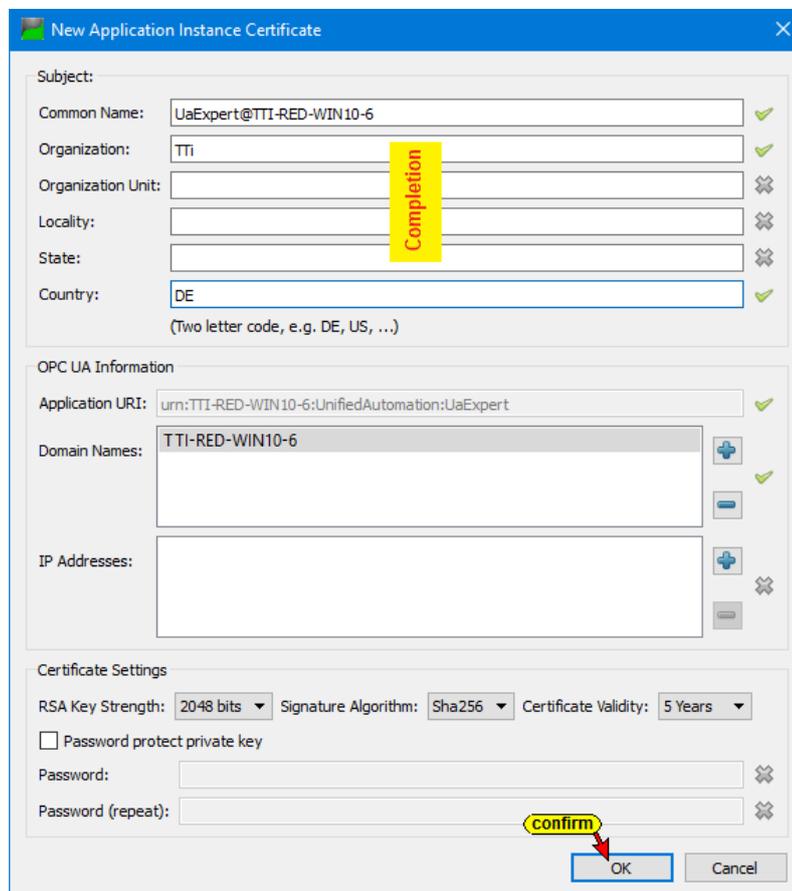
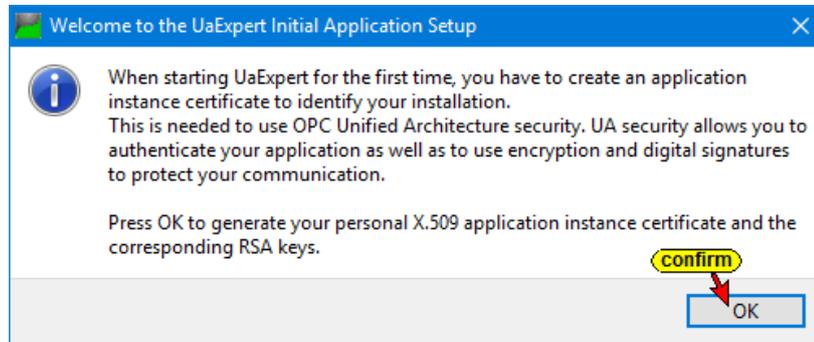
Middle Screenshot: Shows the 'Unified Automation Downloads' page. The 'Downloads' menu is expanded, and the 'OPC UA Clients' link is highlighted with a red arrow. A red circle highlights the 'OPC UA Clients' link in the 'Download Categories' section.

Bottom Screenshot: Shows the 'OPC UA Clients - Downloads' page. The 'Register' link in the left sidebar is circled in red and labeled with a '1'. The 'UaExpert v1.4.4' download card is circled in red and labeled with a '2', with a 'Download' button highlighted in yellow.

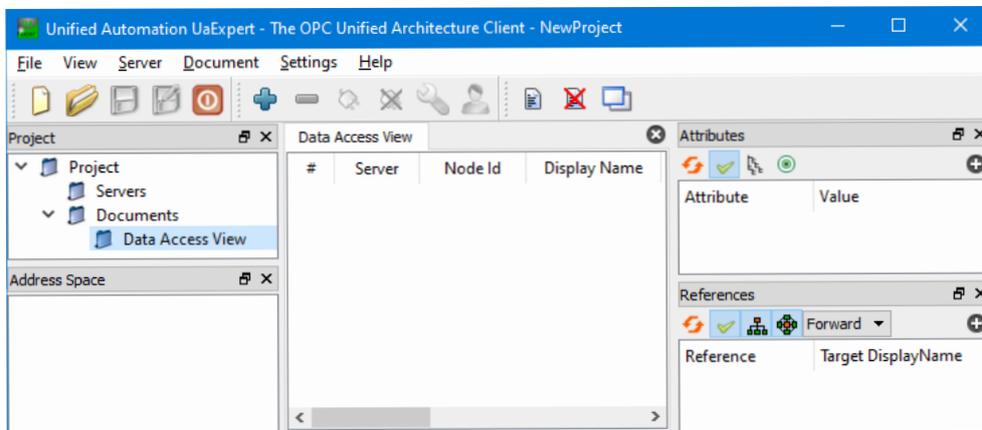
2.1.1 Starting UaExpert

After download and installation of the software, a UaExpert icon double-click starts the program.

Several presets are to be made and confirmed.

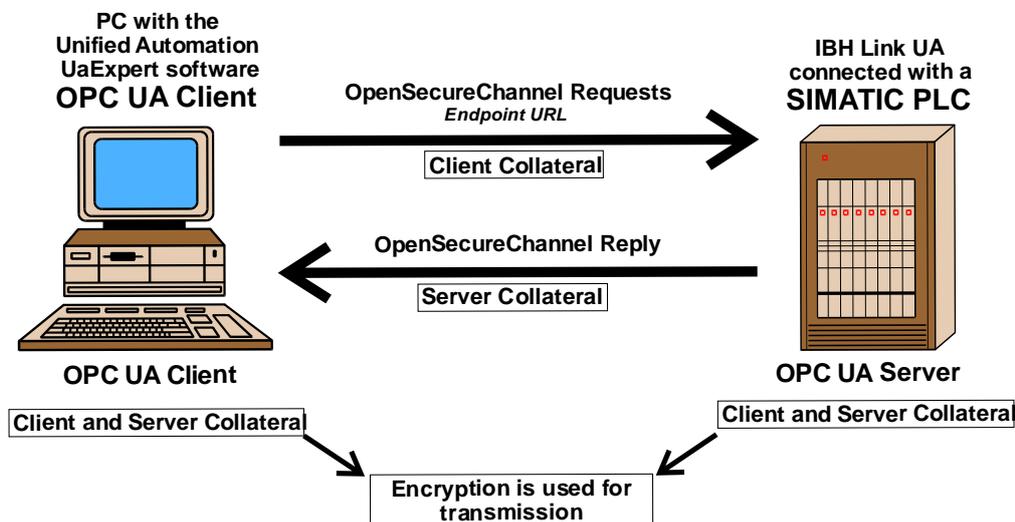


After confirming the Features, the UaExpert program window opens. All necessary tools to establish a connection to an OPC UA server (IBH Link UA) to display the security options and the transferred data are available.



2.2 Establishing a connection to the IBH Link UA

Several steps are necessary to establish the connection between an OPC UA client and an OPC UA server. The connection is only possible if the server and the client have identical certificates.

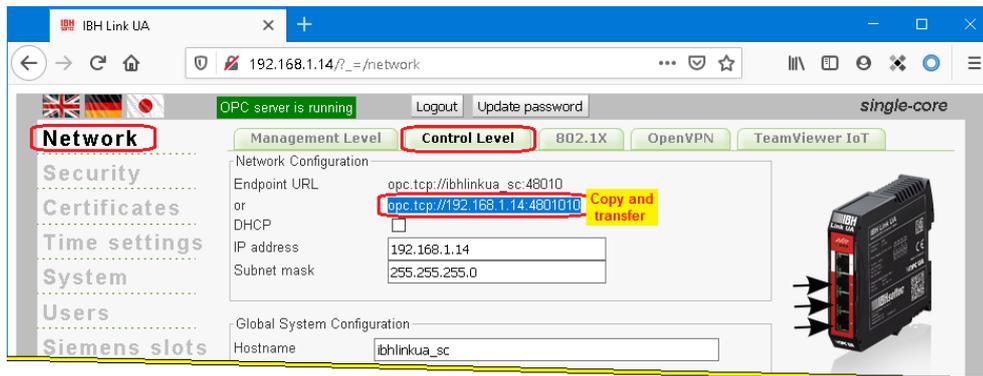


To establish a connection to the IBH Link UA, the **Endpoint URL**, from the IBH Link UA browser window **Network / Control Level** must be entered.

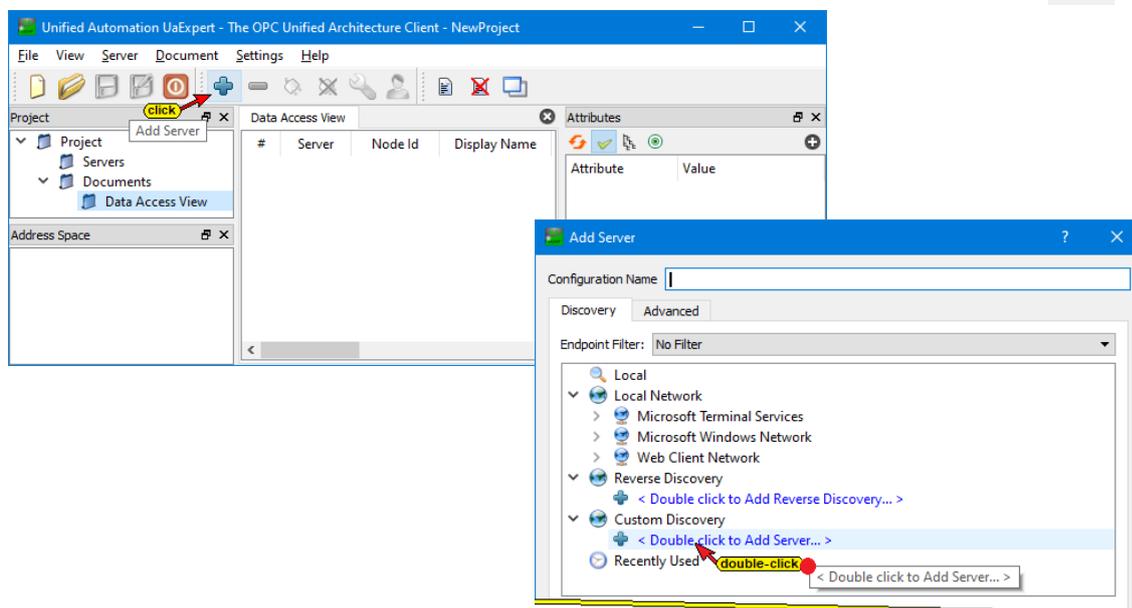
Preferably, the **Endpoint URL** with the hostname should be used to enable the client to validate the names of the endpoints and the names in the certificate.

Since no DNS server is available in the workshop, the absolute IP address is used as an exception.

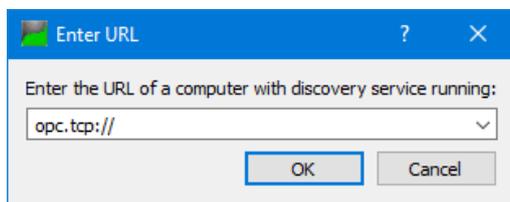
In this case, the absolute **Endpoint URL** is copied from the browser window to the clipboard.



Clicking the Plus icon opens the **AddServer** dialog box.



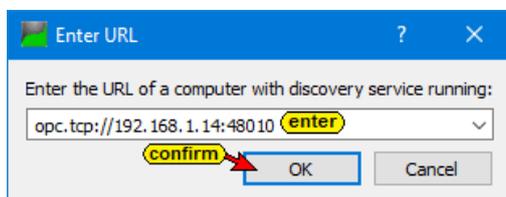
A double-click on  **< Double click to Add Server... >** opens the **Enter URL** dialog box.



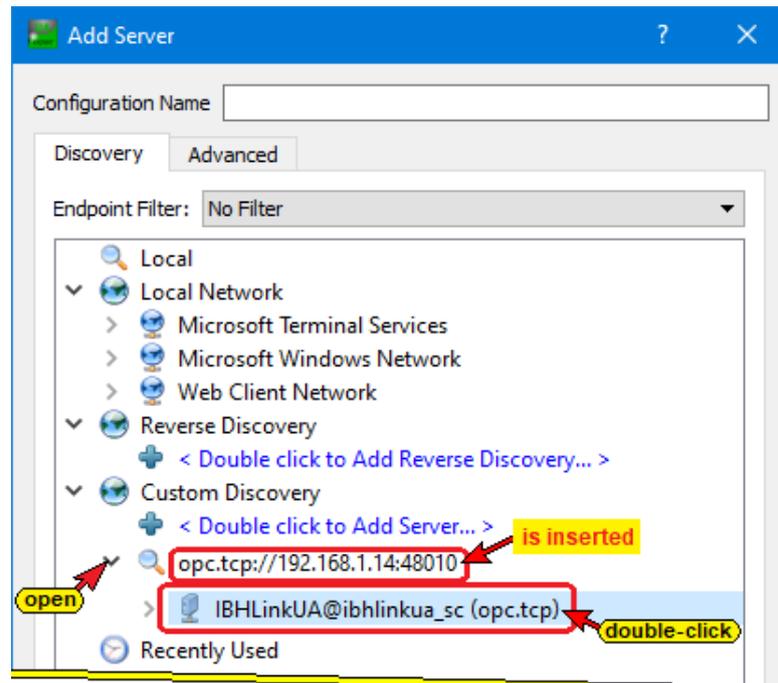
Here the **Endpoint URL** from the IBH Link UA browser window **Network / Control Level** must be entered.

Preferably, the **Endpoint URL** with the hostname should be used to enable the client to validate the names of the endpoints and the names in the certificate.

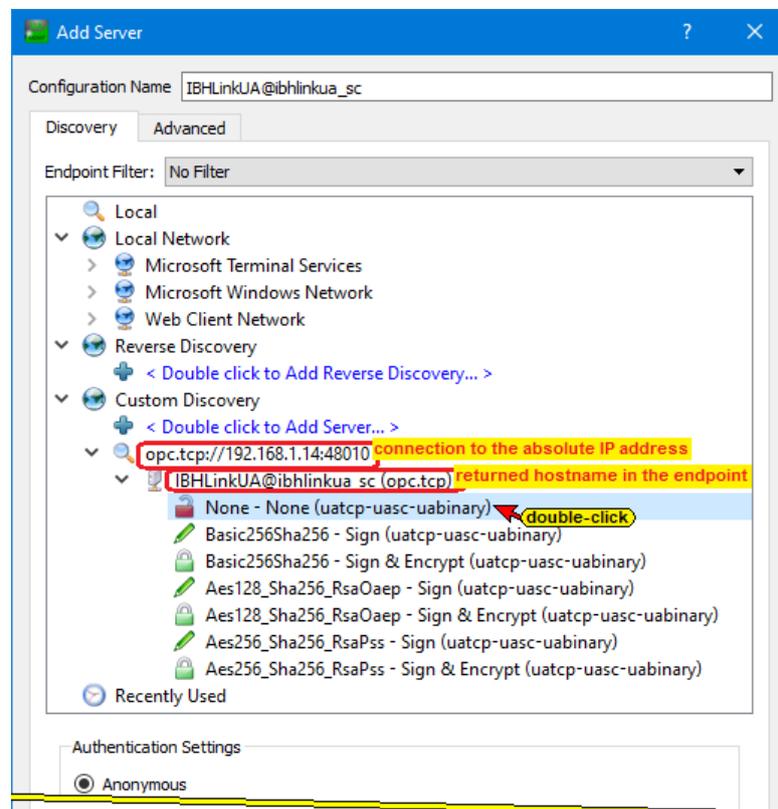
Endpoint URL copied and transferred to the *Enter URL* dialog box.



The **Endpoint URL** has been accepted and is displayed in the **AddServer** dialog box.

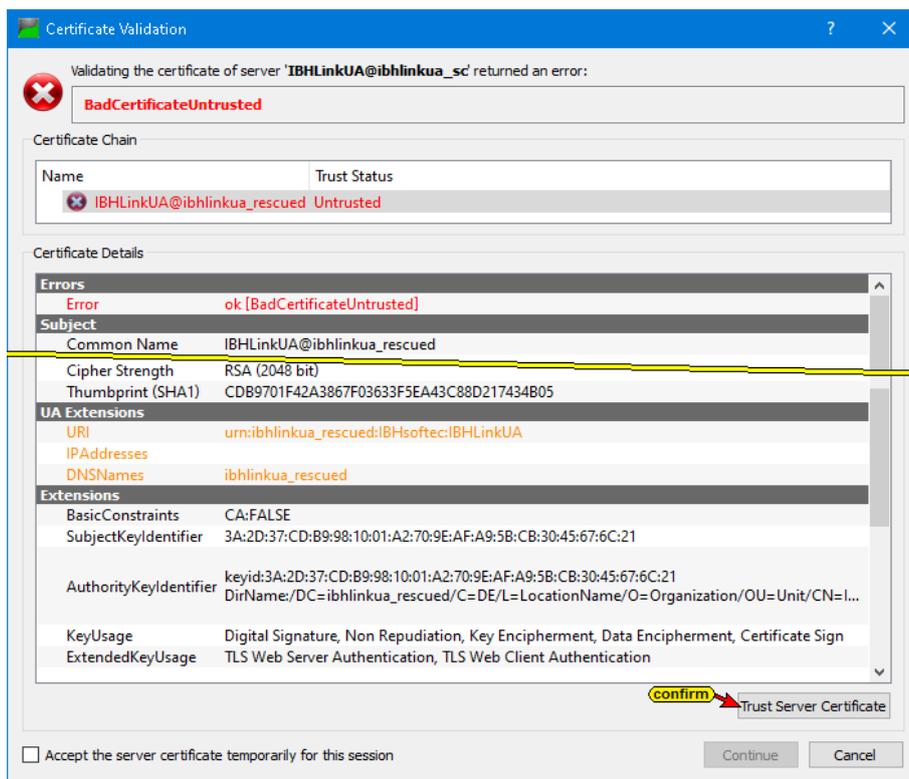


A double click on **IBHLinkUA@ibhlinkua_sc (opc.tcp)** inserts the security levels marked in the **IBHLinkUA@ibhlinkua_sc (opc.tcp)** IBH Link UA browser window **Security / Server Security**.



Double-clicking the security level **None - None (uatcp-uasc-uabinary)** **None (uatcp-uasc-uabinary)** in the AddServer dialog box sets the security level and the **AddServer** dialog box is closed.

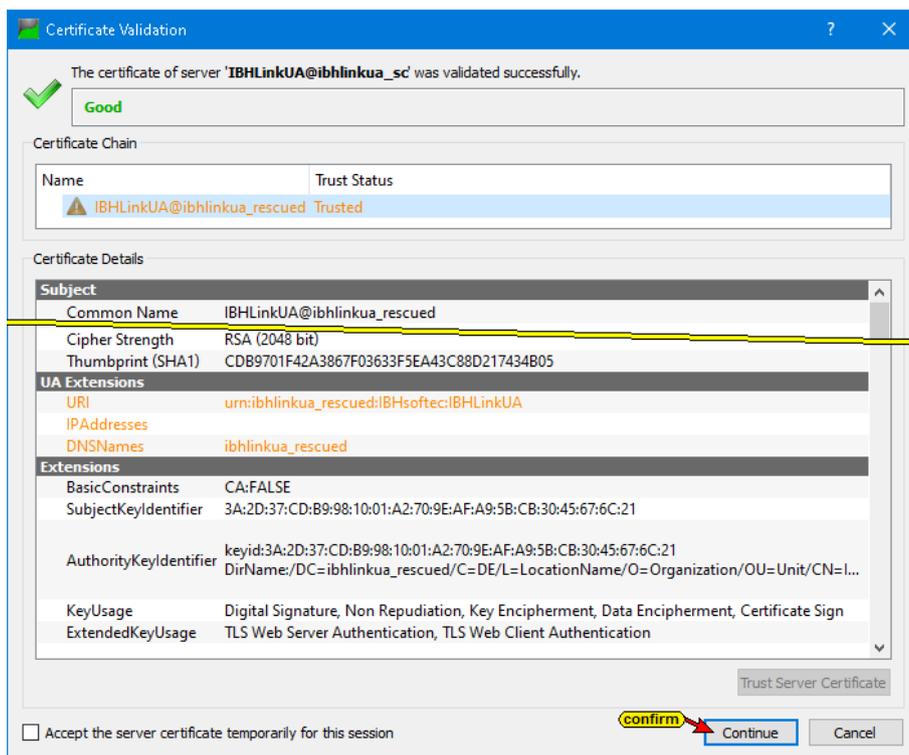
The Certificate Validation dialog box for accepting the OPC UA server certificate of the **IBHLinkUA@ibhlinkua_sc** is displayed.



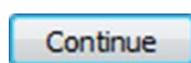
Click the **Trust Server Certificate** button to confirm the selected certificate.



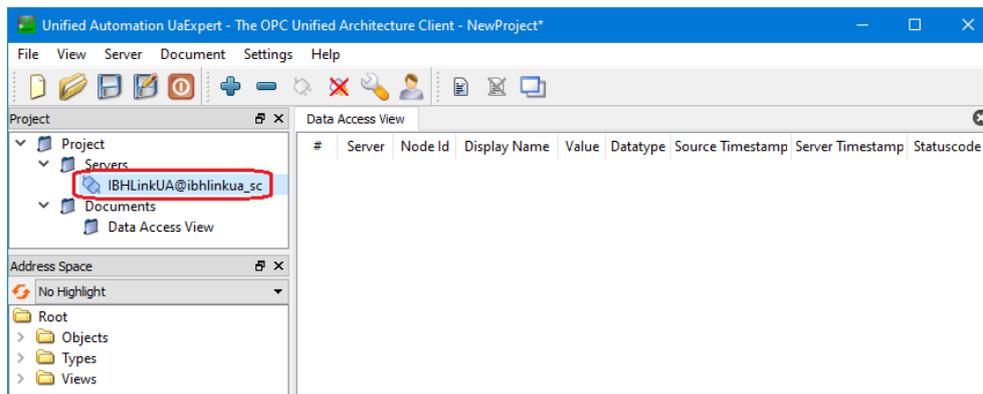
The confirmed server certificate **IBHLinkUA@ibhlinkua_sc** is displayed.



Clicking the **Continue** button closes the dialog box.

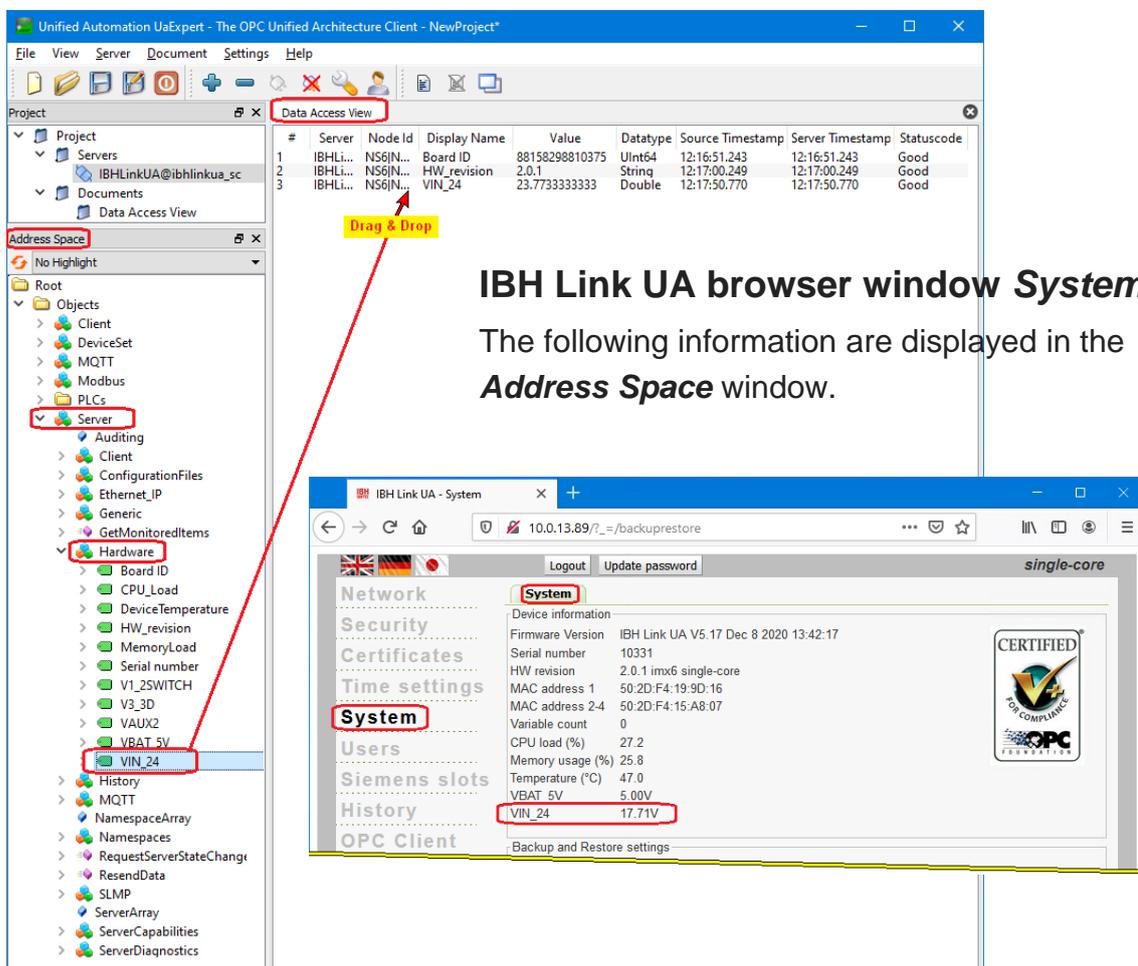


The connected server with the defined security level is displayed in the opened **UaExpert program window**.



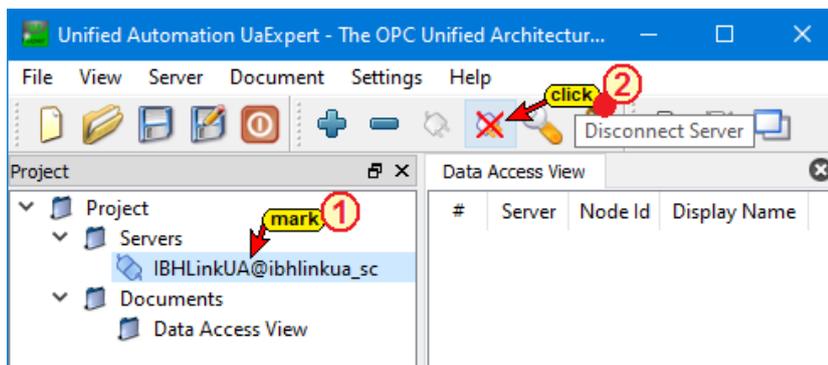
AddressSpace in the **UaExpert** program window, displays information about the connected server. Pull down **Server / Hardware** to list the OPC information from the IBH Link UA browser window **System**.

Drag & drop an information (for example, VIN_24) into the **Data Access Viewer** window. Details of VIN_24 (voltage supply of the IBH Link UA) is displayed. With **drag & drop** any number of information can be pulled from the **AddressSpace** window into the **DataAccess Viewer** window to show details.

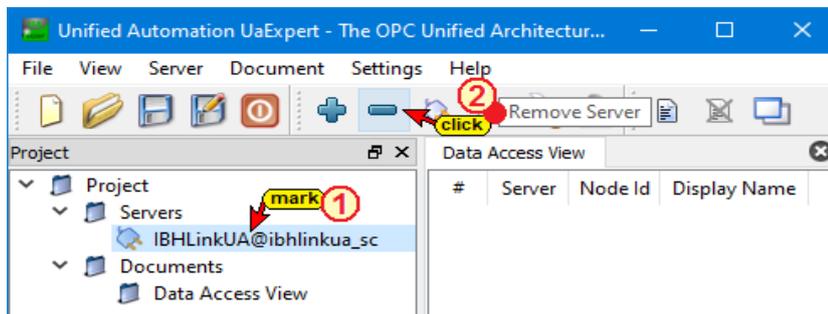


2.3 Encrypted connection to the IBH Link UA

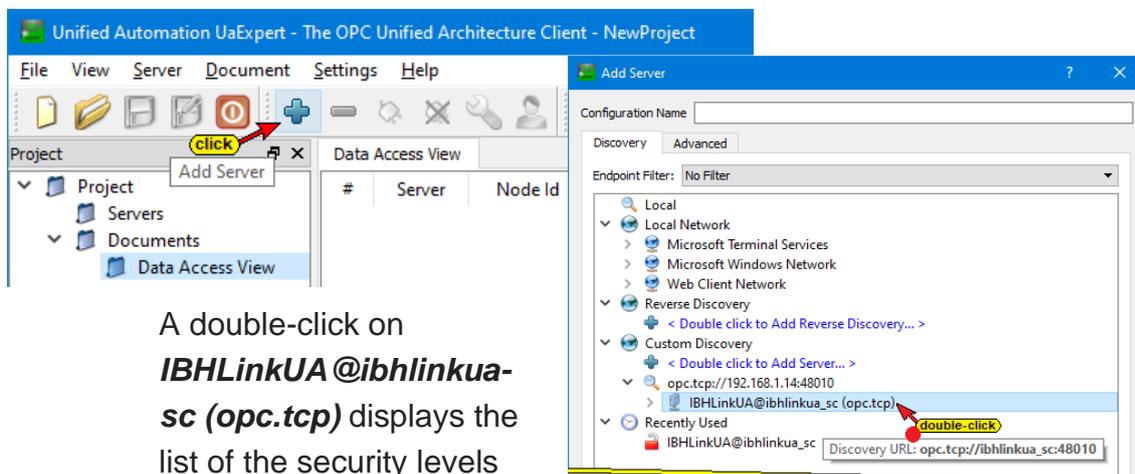
To establish another (e.g. encrypted) connection to the IBH Link UA, the existing must be disconnected, as only one connection can exist. Mark the connected server name **IBHLinkUA@ibhlinkua_sc** and then click the **Disconnect Server** icon.



To remove the Server out of the **Project**, mark the connected server name **IBHLinkUA@ibhlinkua_sc** and then click the **Remove Server** icon.



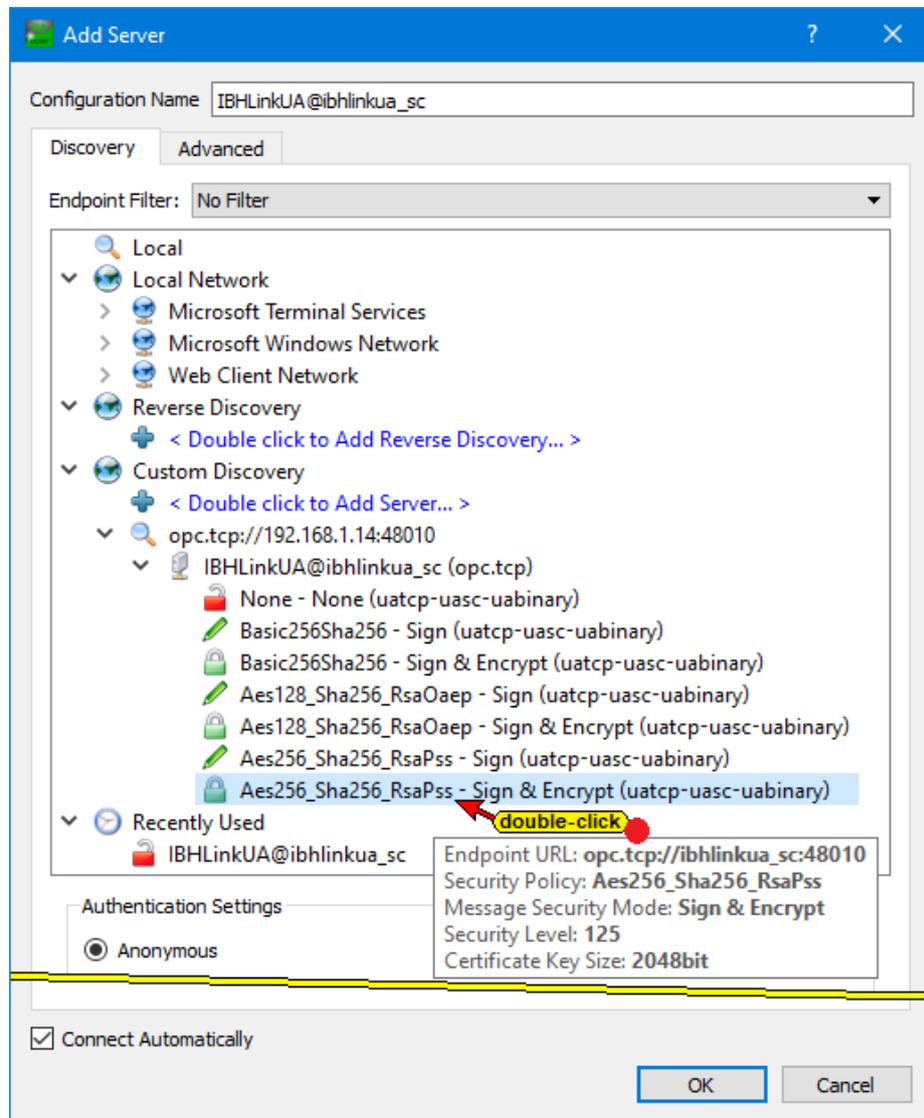
To establish an encrypted connection to the IBH Link UA click the **Plus** icon in the Unified Automation **UaExpert** window to open the **AddServer** dialog box.



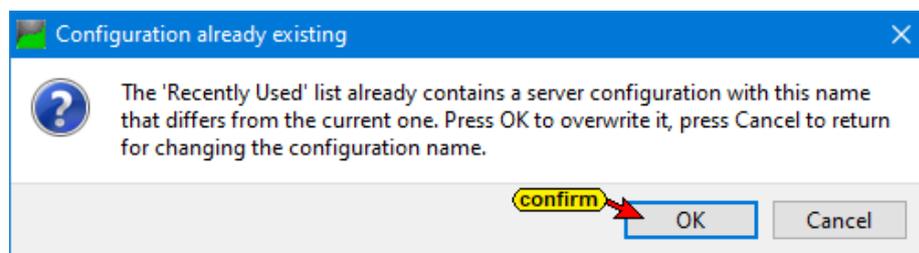
A double-click on **IBHLinkUA@ibhlinkua-sc (opc.tcp)** displays the list of the security levels marked in the IBH Link UA browser window **Security / Server Security**.

Desired encrypted connection

In the **AddServer** dialog box double-click the desired encrypted connection. This closes the **Add Server** dialog box.

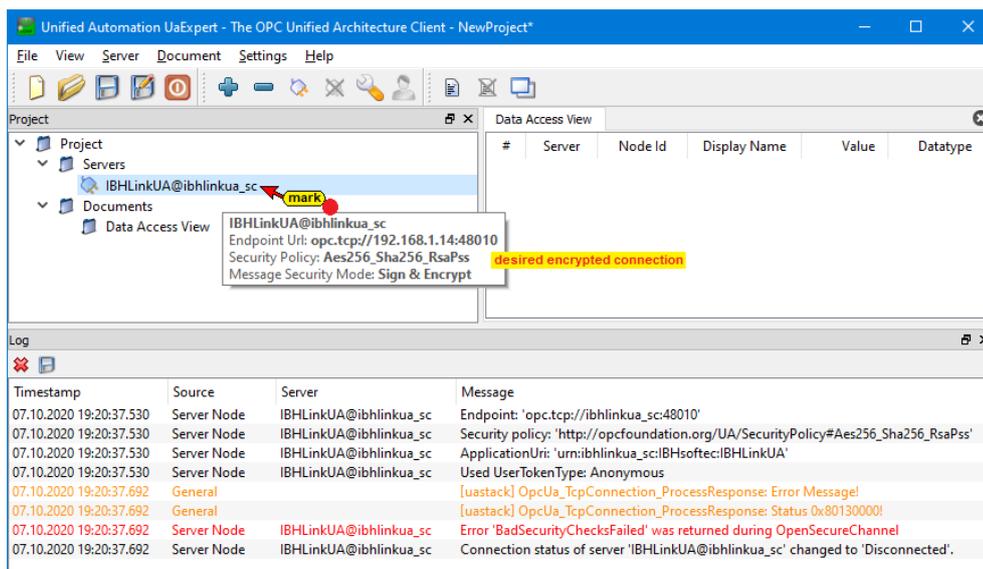


A double-click on the required encryption displays a message. A server configuration with the same name already exists, but it differs from the current one. Clicking OK will apply the selected encryption.



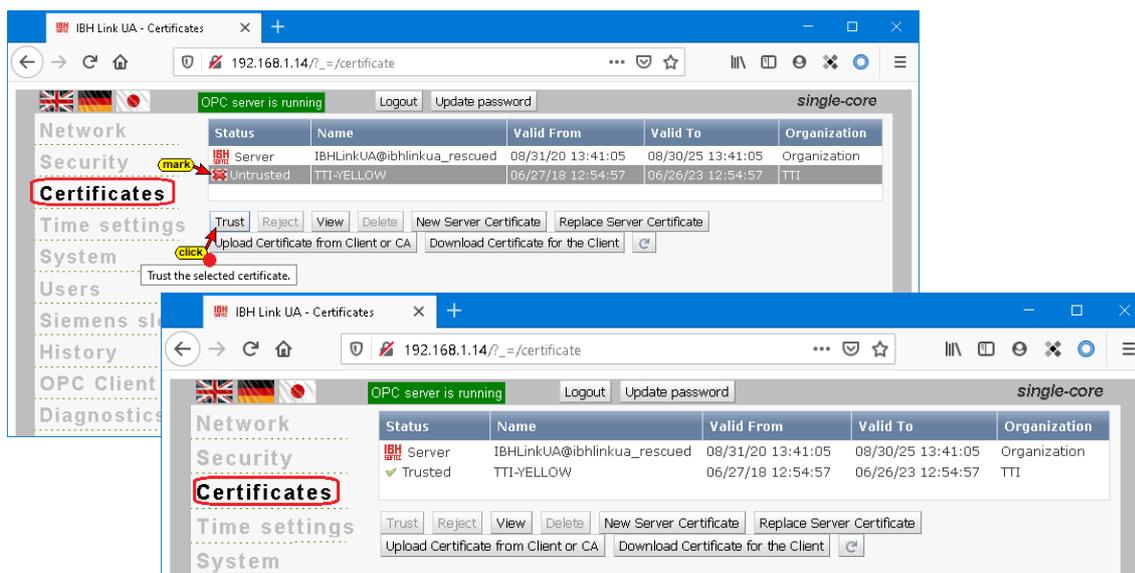
Confirming this message, and the selected encrypted connection is displayed under **Project / Servers** in the **Unified Automation UaExpert** window. The connection to the name **IBHLinkUA@ibhlinkua_sc** OPC server cannot be established.

The Log is listing the errors.



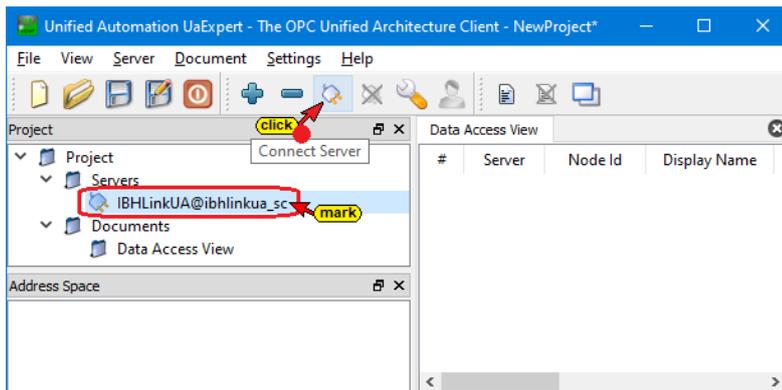
Trusting the IBH Link UA Certificate

In the IBH Link UA the certificate for the encrypted connection must be trusted.

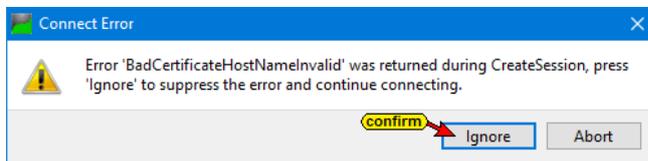


After trusting the certificate, in the UaExpert client, the validation of the certificate can take place.

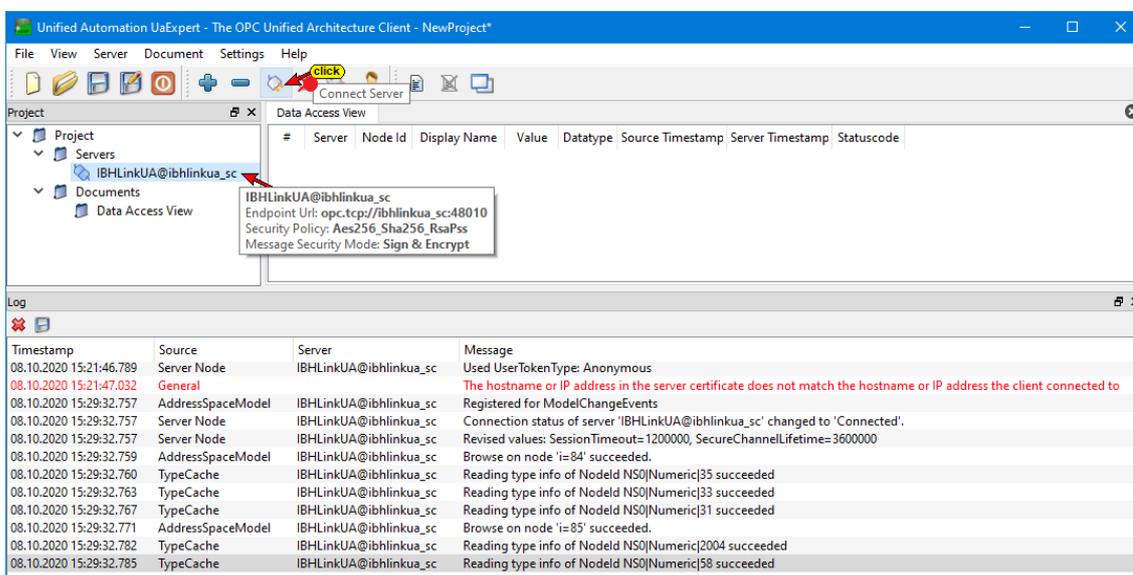
Clicking **Connect Server** cannot establish the connection to the OPC UA server



An error message is displayed. The hostname in the server certificate does not match the hostname or IP address the client connected to. This is because the Endpoint URL has an absolute address, and a symbolic address was returned. The warning can be ignored.

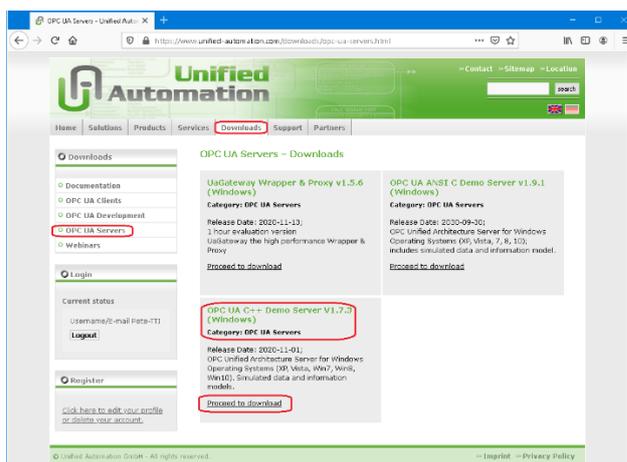


With a new click on **Connect Server** the connection to the OPC UA server is established.

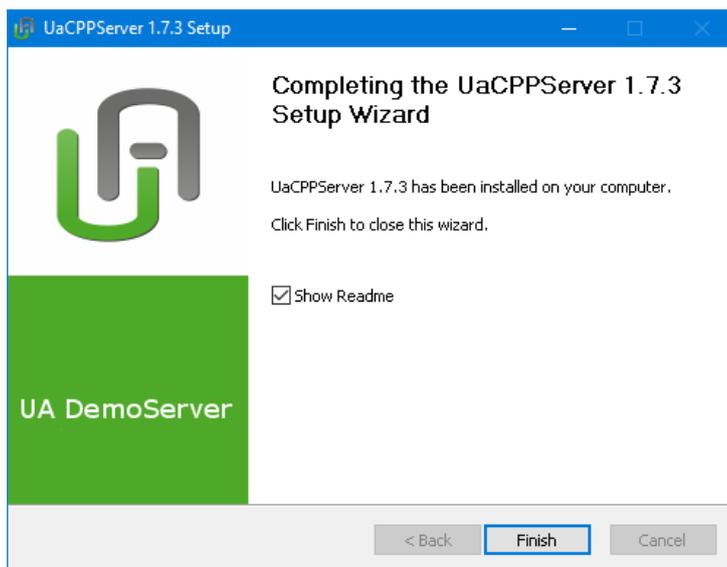


2.4 Download the OPC UA Demo Server (Windows)

The OPC Server program **UaCCPServer** from Unified Automation can be downloaded via: <http://www.unified-automation.com>
Free download requires Unified Automation registration.



Install the OPC UA Demo Server



ATTENTION!

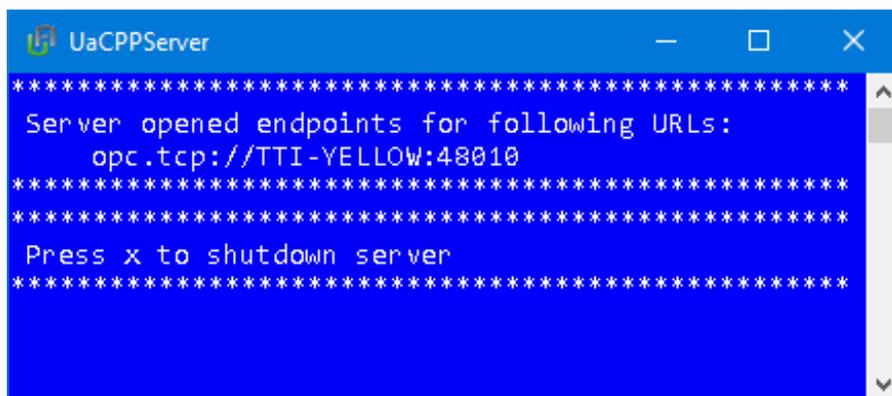


The Firewall must be opened for the App
OPC United Architecture C++ Demo Server

During the installation of the **OPC UA Server** (UaCPPServer) an icon has been inserted. Double click the icon **UaCPPServer** to start the OPC UA Server.



The Server opens with the following window.



The window can be reduced. The OPC UA Server software will run in the background.



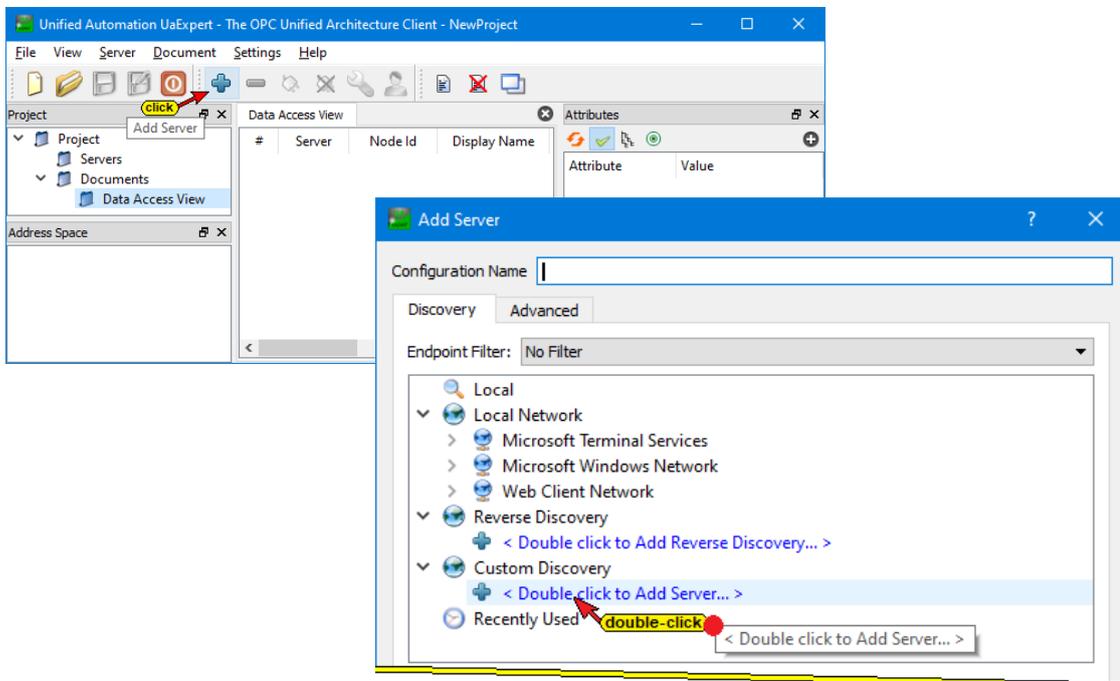
2.4.1 OPC UA Server *Endpoint URL*

The **Endpoint URL** is displayed in the **UaCPPServer** window. The URL is made of the hostname (**TTI-YELLOW**), and the port (**48010**) used. The hostname is the name of the PC executing the UaCPPServer software.

If the PC is running in network having no DNS server, the absolute IP address of the PC must be used.

Add UaCPPServer in the UaExpert Client

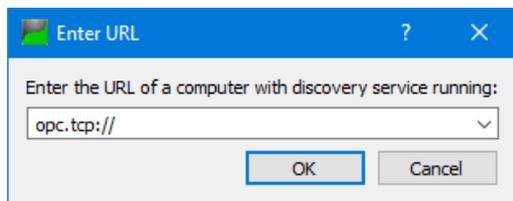
Clicking the Plus icon opens the **AddServer** dialog box.



A double-click on



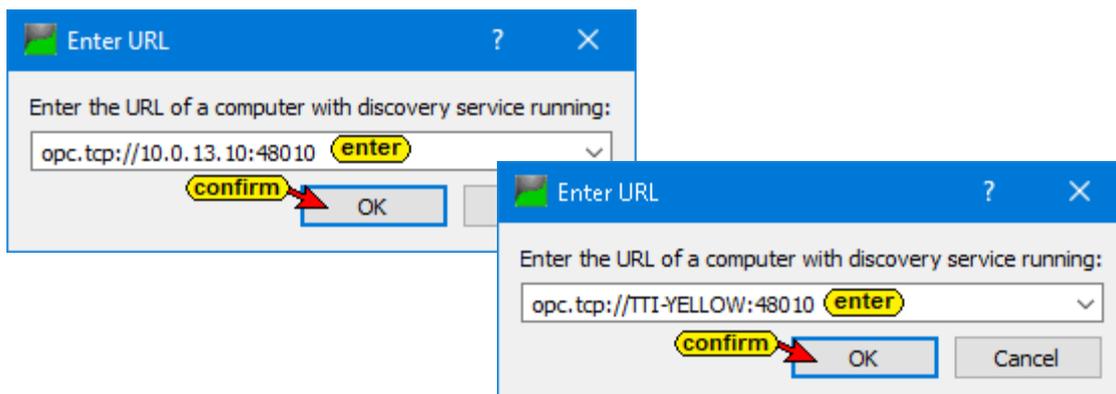
<Double click to Add Server ...> opens the **Enter URL** dialog box.



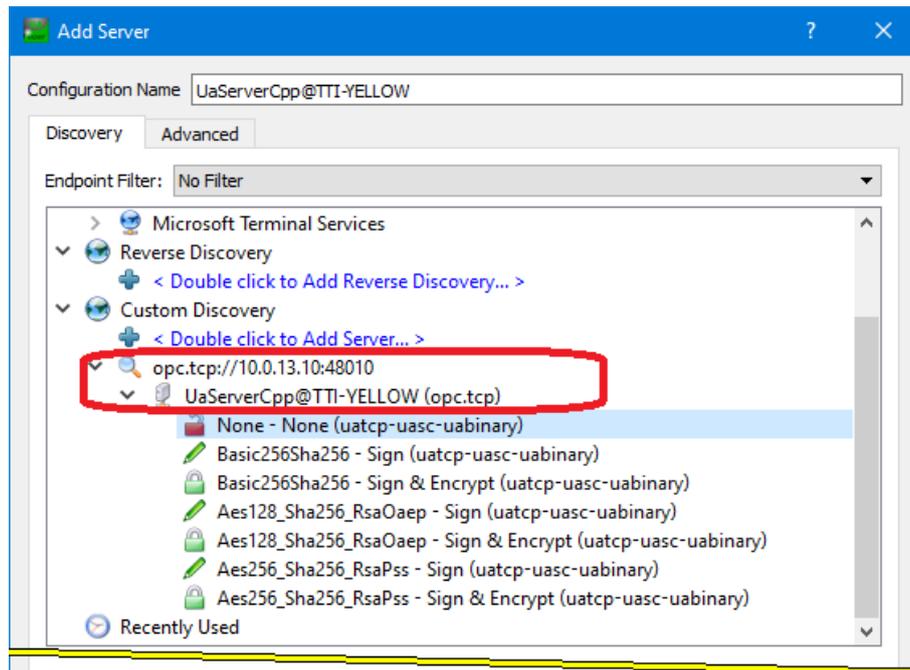
Here the **Endpoint URL** from the **UaCPPServer** window must be entered.

The **Endpoint URL** with the hostname should be used to enable the client to validate the names of the endpoints and the names in the certificate. It is also possible to use the absolute address of the PC and the port number.

Endpoint URL entered in the **Enter URL** dialog box.



The **Endpoint URL** has been accepted and is displayed in the **AddServer** dialog box with the security levels provided.



AddressSpace in the **UaExpert** program window, displays information about the connected server.

