

IBH Link UA

Setup

Quad-Core 64, Quad-Core 32, Single-Core 32
Manual

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
Interface IBH Link UA Quad-/Single-Core 32 Bit (QC-32 / SC-32)	1-1
Interface IBH Link UA Quad Core 64 Bit (QC-64)	1-1
Power supply IBH Link UA Quad Core 64 Bit	1-1
Power supply IBH Link UA Quad-/Single-Core 32 Bit	1-1
1.2 Configuration of the IP addresses (default setting)	1-1
Standard IP address configuration (QC-32 / SC-32)	1-2
Standard IP address configuration (Quad Core 64 Bit)	1-2
1.3 Login browser window	1-2
Language selection	1-2
OPC server running display	1-2
1.3.1 IBH Link UA type display	1-3
Remember me	1-3
1.3.2 Login	1-3
Change Password	1-3
1.4 Network browser window	1-4
Management Level Settings (QC-32 / SC-32)	1-4
Management level settings (QC-64)	1-4
Control Level Settings (QC-32 / SC-32)	1-5
Control Level Settings (QC-64)	1-5
Management Level / Control Level adjustments (QC-64 / QC-32 / SC-32)	1-5
Endpoint URL	1-5
1.5 Settings Routes	1-6
1.6 Settings 802.1x	1-6
1.7 OpenVPN settings	1-6
1.8 TeamViewer IoT activation – IBH Link UA	1-7
Ethernet areas:	1-8
Insert assignment token	1-8
Assignment Token taken from TeamViewer IoT	1-8
Copy the TeamViewer ID	1-8
Teamviewer IoT – MQTT settings	1-9
1.9 1.8 Activate Any Viz	1-9
OPC UA Tag CounterValue1500 as a diagram	1-10
1.10 Security browser window	1-10
Server Security	1-11
Reverse Connection	1-11
Redundant servers (only HOT mode supported) – quad core only	1-12
Hot failover mode	1-12
Integrated client security	1-12
Download	1-13

Firewall	1-13
Web Configuration	1-13
1.11 Certificates browser window	1-13
1.12 Browser window GDS.....	1-14
1.13 Time settings browser window.....	1-14
NTP status.....	1-14
1.14 System browser window	1-14
1.14.1 Device Information	1-15
1.14.2 Backup and Restore the settings	1-15
Saving the IBH Link UA configuration	1-15
Restore the IBH Link UA configuration	1-15
1.14.3 Firmware Update	1-16
HW1	1-16
HW2 SC	1-16
HW2 QC	1-16
HW3 QC-64.....	1-16
Select saved firmware file	1-16
Restart the IBH Link UA	1-17
1.14.4 Variable format	1-17
Classic:	1-18
Compact:	1-18
S7-1500 compatible:	1-18
Compatible	1-18
1.14.5 OPC UA options	1-18
Update Source Timestamp only on change.	1-18
Show byte arrays as ByteString	1-19
Route S7 connections always to slot 2.	1-19
Only allow one S7 frame to the PLC	1-19
Client Timeout [ms]	1-19
No client initial update	1-19
Forbid data type conversion	1-19
1.15 Users browser window	1-19
1.16 Browser window Siemens slots	1-19
Load the OPC Editor project	1-20
Save the OPC Editor project.....	1-20
Insert SoftPLC	1-20
Insert SINUMERIK	1-20
Connect via MPI / Profibus gateway	1-21
Read SINUMERIK Model.....	1-21
Import NC-VAR file.....	1-21
Change SINUMERIK.....	1-21
Save OPC Editor Project.....	1-21
1.17 History browser window	1-21
History tree	1-22
History vars (variables)	1-22
Retentive history	1-22
History variable list as XML file	1-22
1.18 OPC Client browser window	1-23
Define read variables	1-23

	Connect with variable	1-24
1.19	Diagnostics browser window	1-24
	Controller diagnosis	1-24
	Client diagnostics	1-24
	Network diagnostics	1-25
	System Log	1-26
1.20	MQTT browser window	1-26
1.21	Browser window variables	1-26
1.22	Browser window node set	1-27
1.23	SoftPLC browser window	1-27
	Browser window SoftPLC / SoftPLC status	1-27
1.24	Modbus browser window	1-28
1.25	Mitsubishi browser window	1-28
	Mitsubishi robot	1-29
1.26	Rockwell browser window	1-29
1.27	MicroSD browser window	1-29
1.27.1	Docker Container	1-30
	Activate Docker	1-31
	Open Node-RED	1-31
1.28	IBH Link UA default factory configuration	1-32
	Reset button hardware revisions HW3 Quad-Core 64	1-32
	Reset button hardware revisions HW2 SC and HW2 SQ	1-32
	Reset button hardware revisions HW1	1-32
1.29	Open the Wiki	1-32
2	Unified Automation UaExpert –OPC UA Client and OPC UA Server	2-1
2.1	Unified Automation UaExpert – The OPC UA Client and OPC UA Server	2-1
2.1.1	Starting UaExpert	2-1
2.2	Establishing a connection to the IBH Link UA	2-2
	UaExpert window	2-3
	UaExpert Certificate Violation window	2-4
2.3	Encrypted connection to the IBH Link UA	2-5
	Desired encrypted connection	2-6
	UaExpert window – encrypted connection	2-6
	Trusting the IBH Link UA Certificate	2-7
2.4	UaExpert window Data Access View	2-7
2.4.1	Historical data	2-8
	The historical data of values	2-8
	Show under UA Nodes	2-11

1 IBH Link UA – Setup

1.1 Installation and connection

The **IBH Link UA Quad Core 64 Bit**, the **IBH Link UA Quad Core 32 Bit** and the **IBH Link UA Single Core 32 Bit** are designed for DIN rail mounting:



All IBH Link UA have two (2) interfaces separated by a firewall, which are designed for data exchange at the management level or at the control level.

Interface IBH Link UA Quad-/Single-Core 32 Bit (QC-32 / SC-32)

The management level has an Ethernet port (10 / 100 MBit/s). The interface of the control level consists of a 3-port switch (10 / 100 MBit/s).

Interface IBH Link UA Quad Core 64 Bit (QC-64)

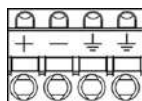
The control level and management level each have an Ethernet port (10 / 100 / 1000 MBit/s). There is also a USB port and a slot for a micro-SD card.

Power supply IBH Link UA Quad Core 64 Bit



The power is supplied via the included plug.
Power supply: 24VDC / 0.2A

Power supply IBH Link UA Quad-/Single-Core 32 Bit



The power is supplied via the included plug.
Power supply: 24VDC / 0.2A

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.

1.2 Configuration of the IP addresses (default setting)



This information is printed on the side of the IBH Link UA. The administration interface can be accessed in the delivery state with a current web browser via the Ethernet port 2 (QC-32 / SC-32 via port 2 to 4) via 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>** (**http://ibhlinkua_010331**)
No additional applications or drivers are required.

Default logon data

Username: admin

Password: admin

Standard IP address configuration (QC-32 / SC-32)



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

Standard IP address configuration (Quad Core 64 Bit)



Level	Port	Address
Management level	Port 1	Hostname: ibhlinkua_<Seriennummer>
Control level	Port 2	192.168.1.14

Note:

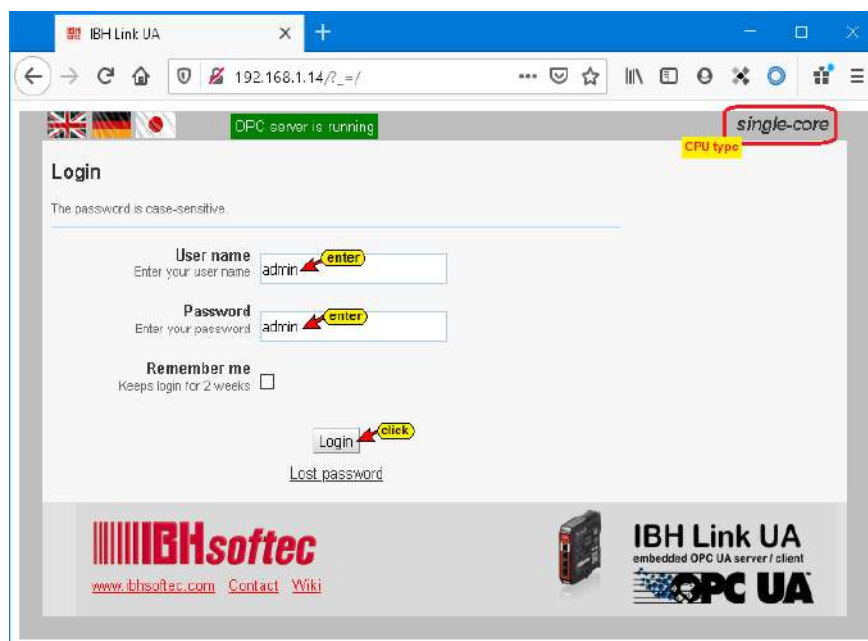
In the IBH-Link-UA default factory setting the configuration may be accessed using an Internet browser (FireFox, Microsoft Edge, Internet Explorer, etc.) as follows:

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 192.168.1.0-[24] (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

OPC server is running

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

1.3.1 IBH Link UA type display

The IBH link UA is available at three performance levels:

Single core 3 2Bit – the processor (imx6) used in the IBH Link UA is a single core processor with 32 bits. Possible Ethernet transmission rates (10 / 100 Mbit/s) (Serial numbers 010000 – 011999). Older IBH Link UA with single core processors do not have a performance level display (Serial numbers 1000 - 4999).

single-core

Quad Core 32 Bit – the processor (imx6) used in the IBH Link UA is a single core processor with 32 bits. Possible Ethernet transmission rates (10 / 100 Mbit/s) (serial numbers 5000 - 9999)

quad-core

Quad Core 64 Bit – The processor (imx8) used in the IBH Link UA is a quad core processor with 64 bits (serial numbers 030000 – 039999). These IBH Link UA have a significantly higher processor performance and possible Ethernet transmission rates of (10 / 100 / 1000 MBit/s).

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.

1.3.2 Login

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**

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

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.

Important information about date and time settings

i Certificates will only work proper, if the clock is set correctly. Your device reports:
2024-09-28 15:33:45

You should continue only, if the date and time settings are correct. Otherwise the clock should be set first.

Continue?

confirm **Ok** **Cancel**

It is important that the time is set correctly, otherwise any OPC UA data transfer and therefore firmware updates cannot be carried out.

Change Password

IBH Link UA

192.168.1.14/_=/network

OPC servers running Logout Update password

single-core

Network Management Level Control Level click 02.LX OpenVPN TeamViewer IoT

Update password

Update password

Enter a new password below

User name admin cannot be changed

Password Enter your password enter

Choose Password Valid enter

Repeat password Valid enter

confirm **Ok** **Cancel**

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**.

Note



The username for browser access cannot be changed.

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.

Choose Password

Too short



1.4 Network browser window

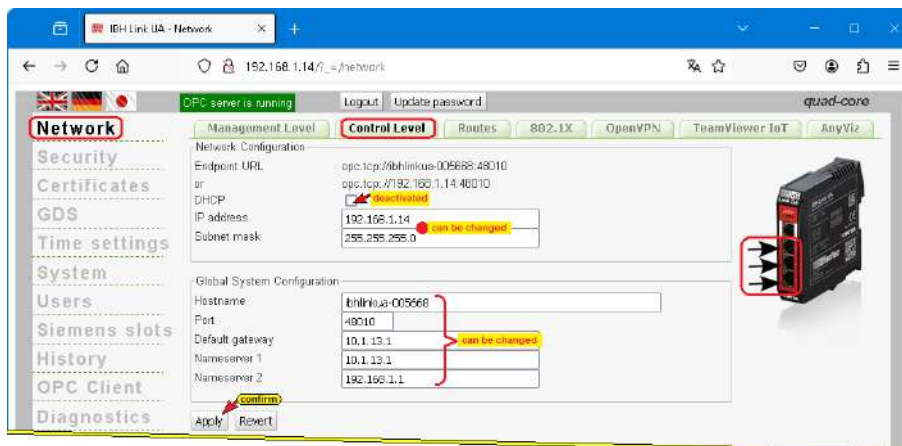
Management System Settings (QC-32 / SC-32)

Port 1 **Network Configuration** and **Global System Configuration**. With DHCP disabled, the **Network Configuration** and **Global System Configuration** may be modified. The hostname can always be adjusted.

Management level settings (QC-64)

Here, adjustments to the network configuration for port 1 and global system settings can be made. If DHCP is deactivated, the network configuration and global system settings can be changed. The hostname can always be changed.

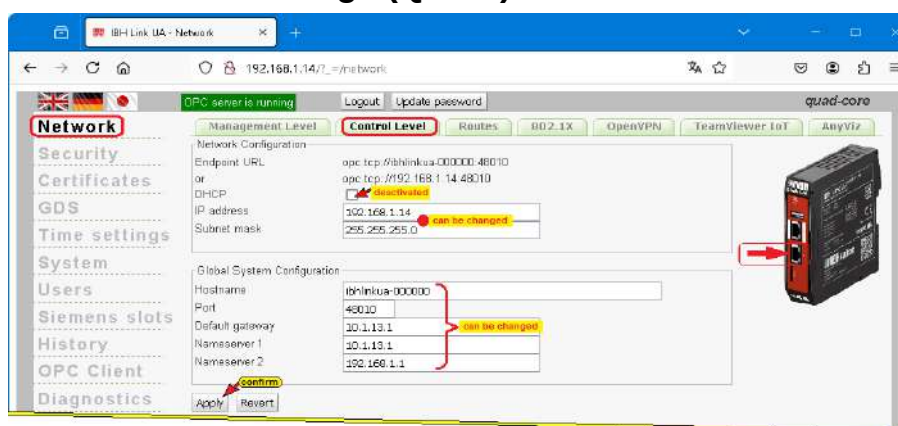
Control Level Settings (QC-32 / SC-32)



Here, adjustments to the network configuration for ports 2 to 4 (control level) and global system settings can be made.

If DHCP is deactivated, the network configuration and global system settings can be changed. The hostname can always be changed.

Control Level Settings (QC-64)

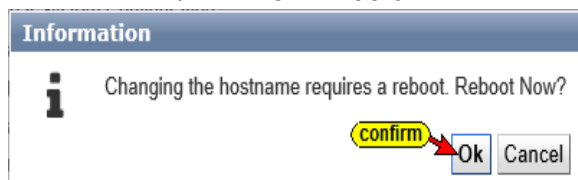


Here, adjustments to the network configuration for port 2 (control level) and global system settings can be made.

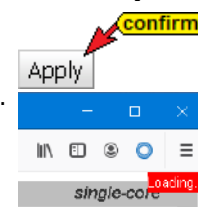
If DHCP is deactivated, the network configuration and global system settings can be changed. The hostname can always be changed.

Management Level / Control Level adjustments (QC-64 / QC-32 / SC-32)

By clicking the **Apply** button, the changed settings of the control level are applied to the **IBH Link UA**. The execution of the change is displayed.



The transfer of the adjusted settings is displayed in the upper right corner of the browser window.



Since the web browser of the Link was opened using the IP address of the control level, access to the web browser of the IBH Link UA can only take place via the changed IP address of the control level or the IP address of the management level.

The changes require a restart of the IBH Link UA, corresponding information is displayed.

Note:

The **management level** (port 1) must have a different subnet address than the **control level** (QC-64 port 2, QC-32 / SC-32 port 2 to port 4) to clearly identify the belongings of the ports to the Ethernet interfaces.

Endpoint URL

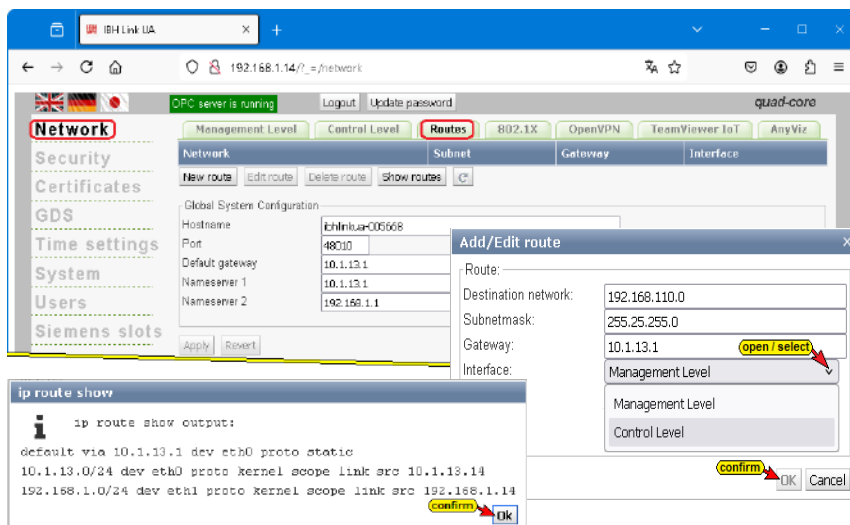


The **Endpoint URL** is displayed at the **Management Level** and in the **Control Level**. The endpoint URL is generated by the **IBH Link UA** based on the settings. The endpoint URL consists of the protocol: **opc tcp // hostname: port**.

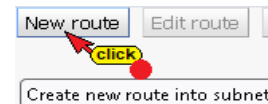
This **Endpoint URL** is required to set up an OPC UA client.

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

1.5 Settings Routes



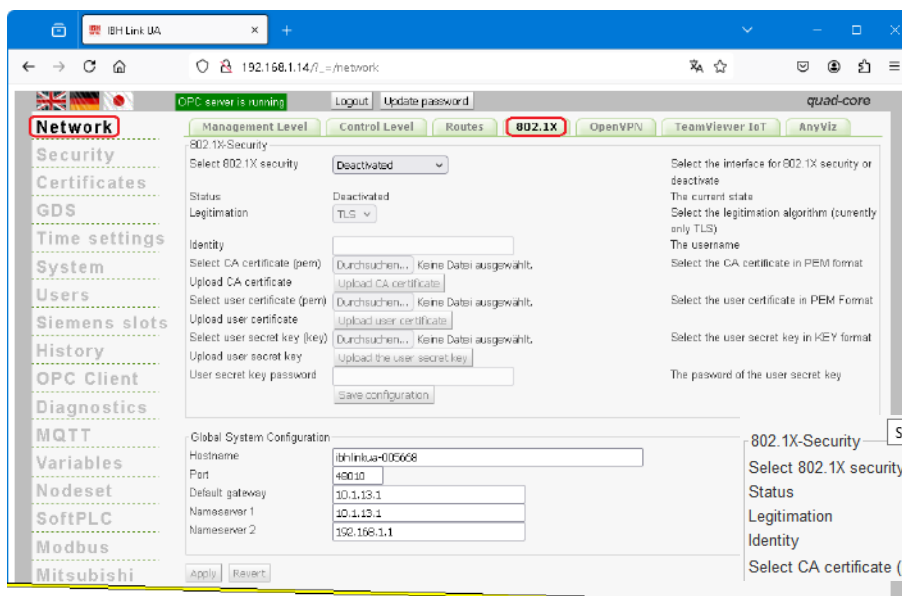
The IBH Link UA allows you to create a route to a device in another subnet, change the route, delete, and display it.



Clicking the **New Route** button opens the dialog box for adding or changing the route.

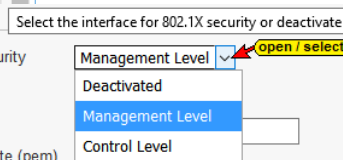
Clicking the **Show Routes** button displays the added route.

1.6 Settings 802.1x



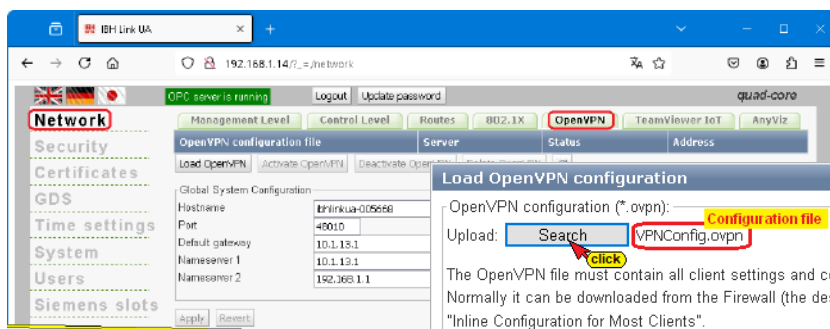
The IBH Link UA provides IEEE 802.1X for authentication and authorization in IEEE 802 networks.

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



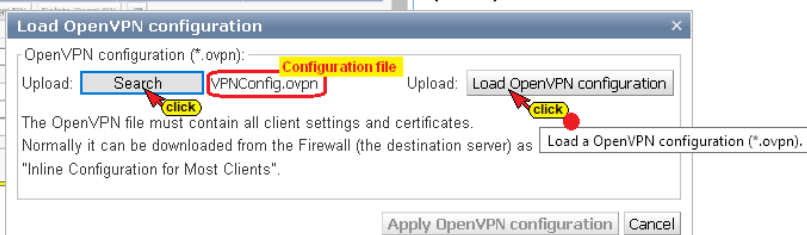
The configuration of the IEEE 802.1X security settings can be saved.

1.7 OpenVPN settings

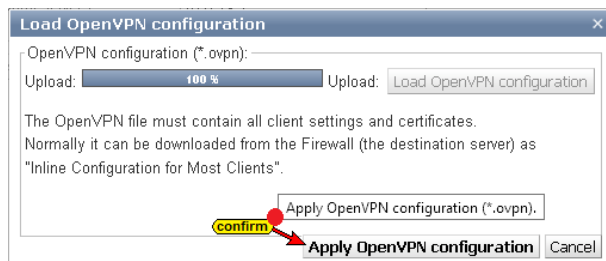


OpenVPN is a VPN client. With OpenVPN an encrypted SSL connection to a virtual network (VPN) can be established.

OpenVPN requires a configuration file and



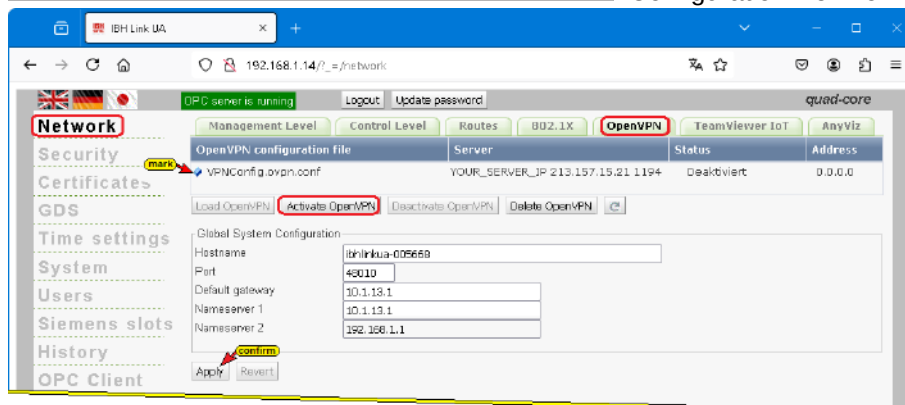
key / certificate files. Clicking on **Load OpenVPN** opens the **Load OpenVPN Configuration** dialog box.



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 is displayed.

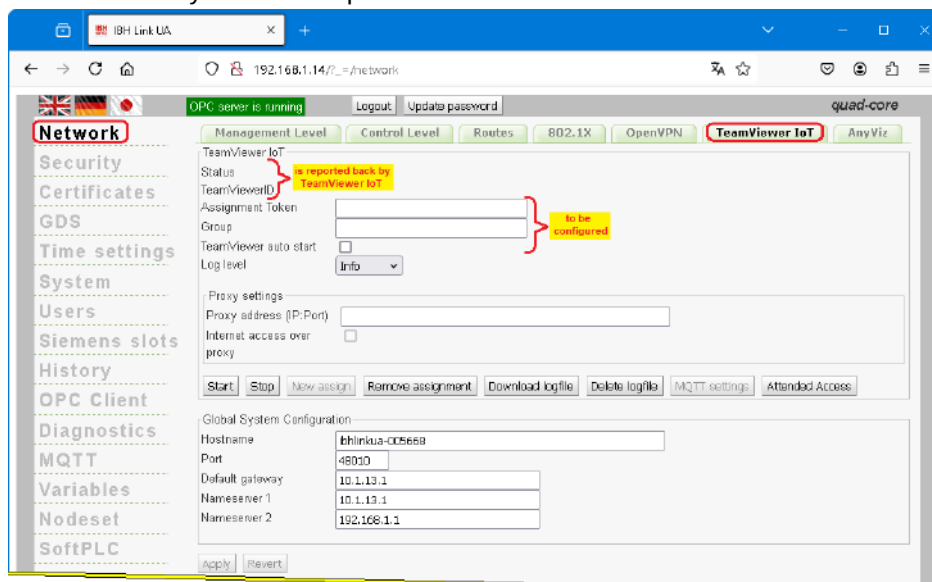


With a click on Activate OpenVPN the virtual network connection (VPN) is activated and with Apply the settings are loaded into the IBH Link UA.

1.8 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 all PLC systems anytime and anywhere. Complex modem solutions or the use of a PC on site are outdated.



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.

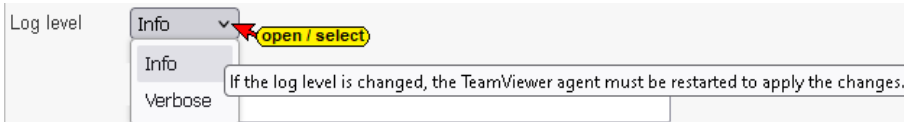
The IBH Link UA manages two subnet addresses separated by a firewall, each with its own MAC address.

Ethernet areas:

Level	Port	
Management level	Port 1	must be in different IP networks
Control level	QC-64 – Port 2 QC-32 / SC-32 – Port 2 – 4	

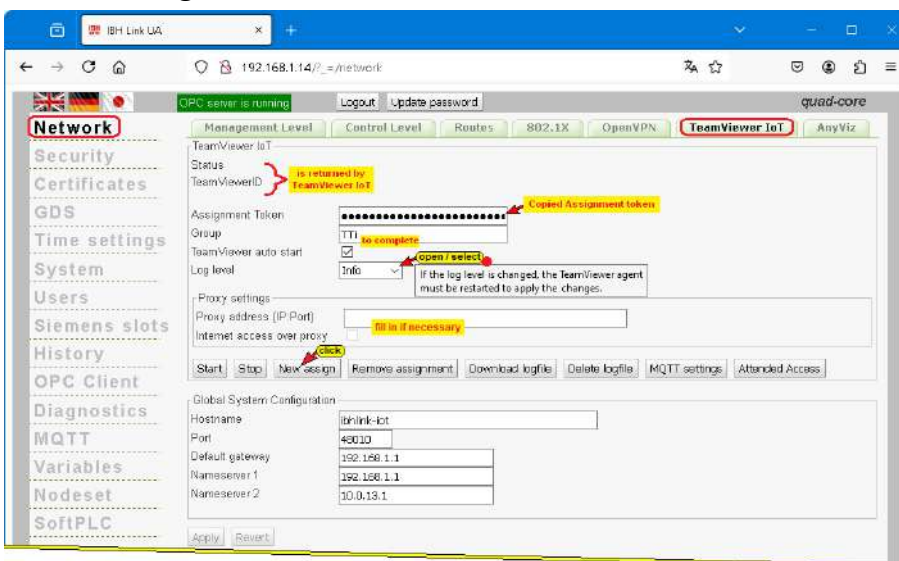
If you need to access the Internet via a proxy, you can enter the address in the form **Proxy:Port** or **User: Password@Proxy:Port**.

Proxy access to the Internet must be activated.



The log output can be customized.

Insert assignment token



The **Assignment token** must be copied into the field of the same name in the **IBH Link UA** browser window Network/TeamViewer IoT. Enter the group name and mark that Team Viewer is switched on automatically.

Clicking the **New assign** button opens the **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!

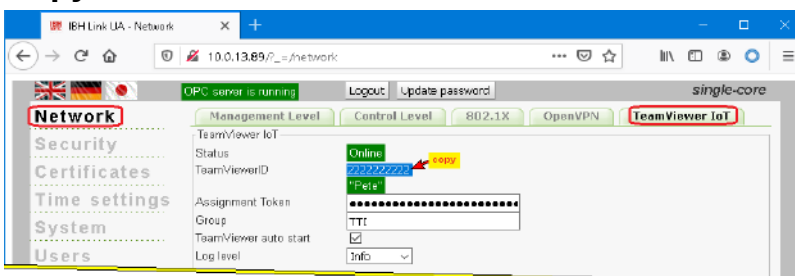


The transmission of the **Assignment token** to **TeamViewer** can take same time.

Assignment Token taken from TeamViewer IoT

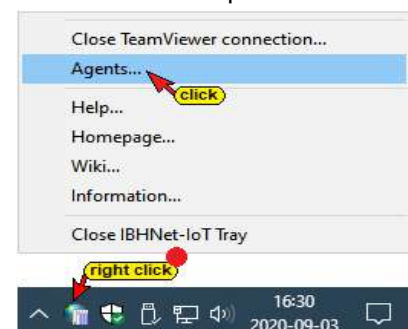
If the assignment token has been accepted, the status and the **TimeViewerID** with the name are displayed in the web browser window **Network/TeamViewer IoT**.

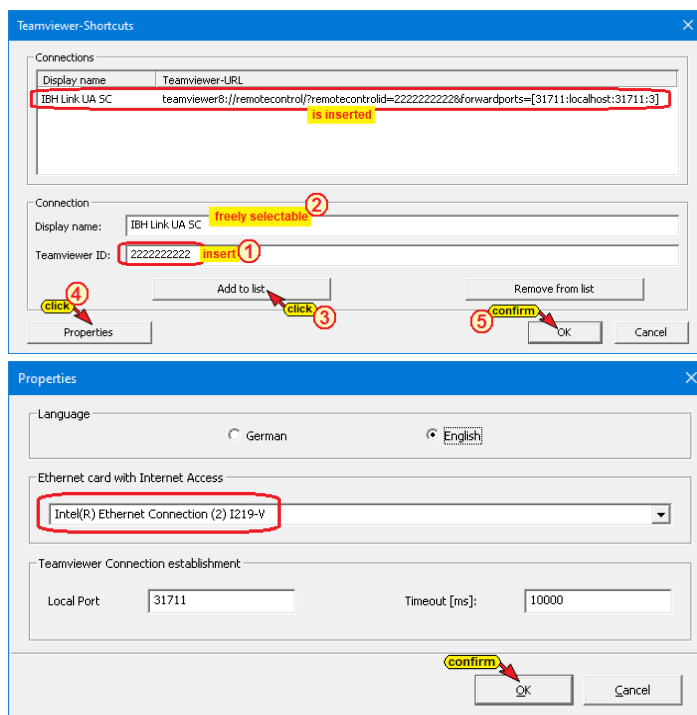
Copy the TeamViewer ID



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

Copy the TeamViewer ID number to the Windows clipboard.





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.

Teamviewer IoT – MQTT settings

click Open a dialog with MQTT settings for the TeamViewer cloud

MQTT settings

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



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** are described on the **IBHsoftec WIKI** website.

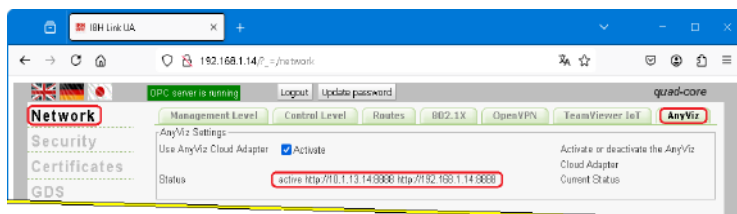


1.9 1.8 Activate Any Viz

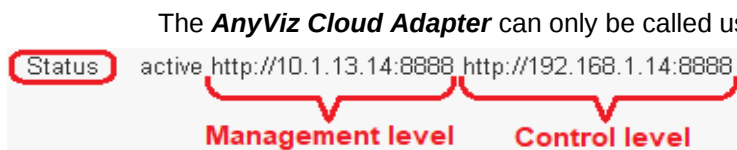
The **Any Viz** option has been integrated since firmware V5.26. Data can be recorded and evaluated using the **AnyViz Cloud**.

The **AnyViz Cloud Adapter** can be activated, and the status displayed in the **Any Viz** tab.





If Activate **AnyViz Cloud Adapter** is selected, access URLs are displayed under Status. These are the URLs (via IBH Link UA management level / control level) with which the AnyViz Cloud Adapter browser window is called.

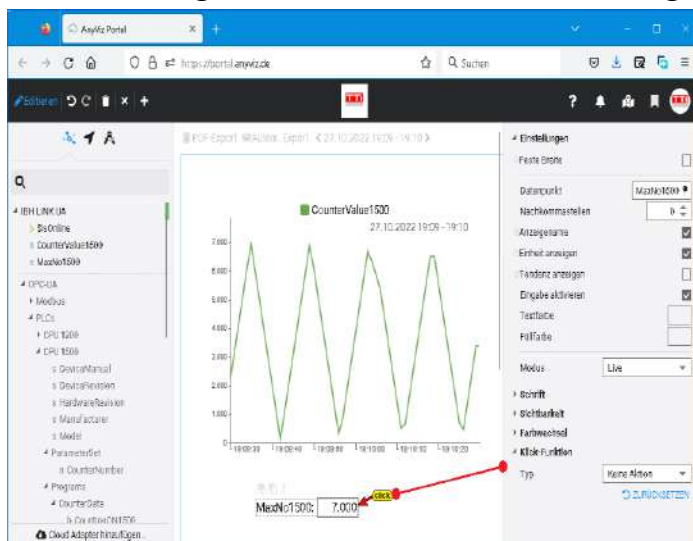


The **AnyViz Cloud Adapter** can only be called using the subnet URL in which the PC to be called and the **IBH Link UA are located (with port 8888)**. The PC must have Internet access.

Note:

There is no need to install the **AnyViz Cloud Adapter for Windows**. If this software is installed, uninstall it.

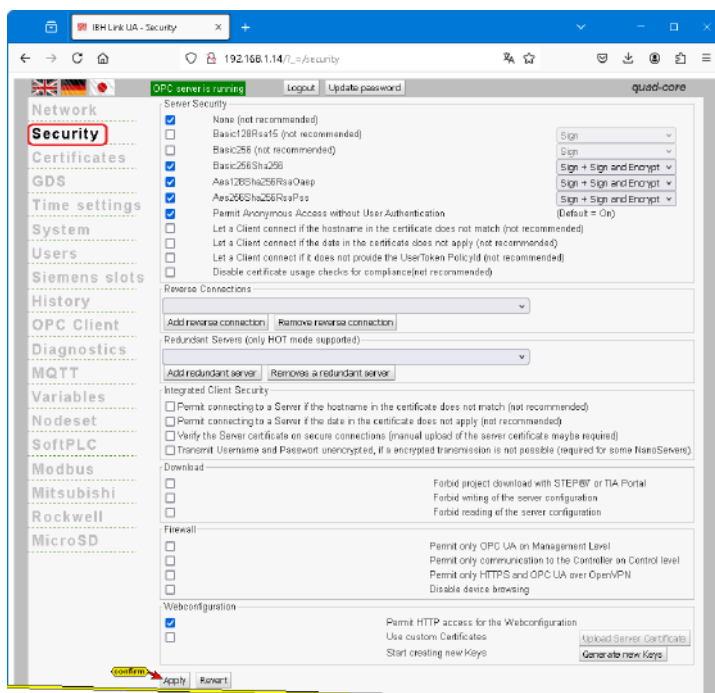
OPC UA Tag CounterValue1500 as a diagram



AnyViz Cloud HMI offers many display types. All OPC UA variables from controllers, sensor and measuring systems provided by the IBH Link UA can be displayed.

The manual and example for using AnyViz are available for download on the IBHsoftec WIKI website.

1.10 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 certificate management to enable secure communication defined by OPC UA (**SecureChannel**). The web browser is used to configure the security levels and manage 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:

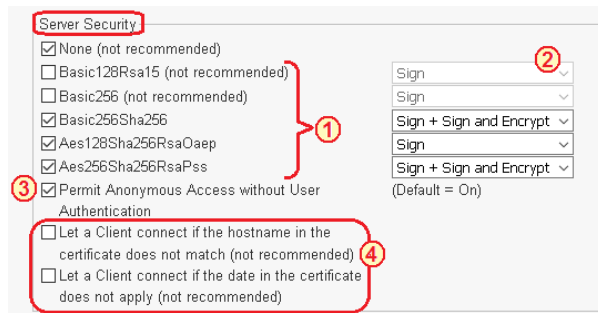
Encrypted messages prevent or at least make it exceedingly difficult for untrustworthy third parties to read the content of the messages that are exchanged between the OPC client and the OPC server.

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, click the Apply button.

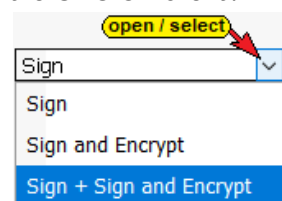


Server Security



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

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.

Sign and 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

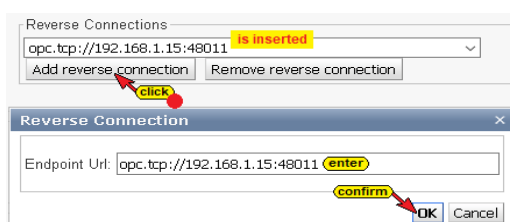
The messages contain the security labels of **Sign** and additionally those of the **Sign and Encrypt** definition.

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.

Redundant servers (only HOT mode supported) – quad core only

The software in the IBH Link UA – quad-core offers the possibility to set up redundant OPC UA servers. Of the **server redundancies** defined by OPC UA, the IBH Link UA supports the following modes:

- **Non-transparent redundancy, with the sub mode Hot.**

All servers in the redundant set have their own **server URL** and **endpoint URL**. Each server in the redundant set provides a list of the other redundant servers in the set (server URI) with the failover mode Hot. With this feature, a client only needs to know one of the servers and can find the other available servers using the information in the server object (**Objects** → **Servers** → **ServerRedundancy**). The advantage of non-transparent redundancy is that it can be easily supported on the server side. The disadvantage is that the client must do something to benefit from the redundancy. However, implementing generic support in a client can be done without much effort using the information provided by the server.

Note:



If the **IBH UA Editor** was used to configure the first redundant IBH Link UA (OPC server), this configuration can be transferred to other IBH Link UA (OPC server) after changing the server settings.

The configuration of the individual redundant IBH Link UAs must be adjusted as described in the IBH UA Editor manual (enter IP addresses of all IBH Link UAs (OPC server) belonging to the redundancy).

Hot failover mode

All servers are powered on and operational. In scenarios where servers are collecting data from a downstream device such as a PLC, one or more servers are actively connected to the downstream device(s) in parallel. These servers have minimal knowledge of the other servers in their group and function independently. If a server fails or encounters a serious problem, its **service level** drops. Upon recovery, the server returns to the redundant set of servers with an appropriate **service level** to indicate that it is available.

Integrated client security

Integrated Client Security

- ① ☐ Permit connecting to a Server if the hostname in the certificate does not match (not recommended)
- ② ☐ Permit connecting to a Server if the date in the certificate does not apply (not recommended)
- ③ ☐ Verify the Server certificate on secure connections (manual upload of the server certificate maybe required)
- ④ ☐ Transmit Username and Password unencrypted, if a encrypted transmission is not possible (required for some NanoServers).

① The hostname 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.

- ② This setting is not recommended by OPC UA.
For security reasons, OPC UA works with time stamps. The date and 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

Download

- ① ☐ Forbid project download with STEP® 7 or TIA Portal
- ② ☐ Forbid writing of the server configuration
- ③ ☐ Forbid reading of the server configuration

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 cannot 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

Firewall

- ① ☐ Permit only OPC UA on Management Level
- ② ☐ Permit only HTTPS and OPC UA over OpenVPN
- ③ ☐ Disable device browsing

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 are 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

Webconfiguration

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

Start creating new Keys

Upload Server Certificate

Generate new Keys

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**.

The button **Generate new Keys** opens a message that must be confirmed to generate a new key.

③ The note must be observed, as the generation of a parameter set for negotiating the keys for the encryption can take several hours.

Upload Server Certificate

Generate new Keys

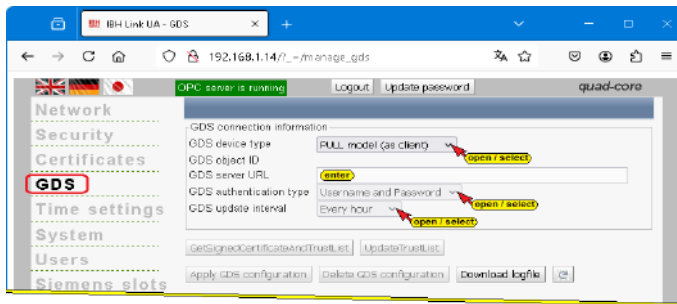
1.11 Certificates browser window



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

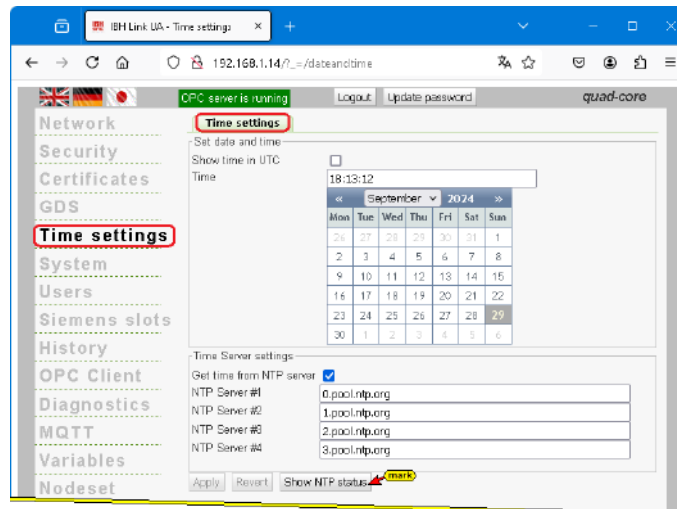
Certificates can be created, downloaded, or read into the designated certificate store.

1.12 Browser window GDS



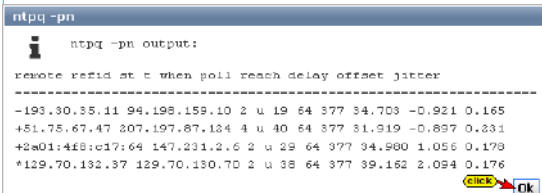
GDS stands for **Global Discovery Server**. The OPC UA GDS concept allows the configuration of cross-subnet discovery services on the one hand and on the other hand it provides interfaces to operate central certificate management.

1.13 Time settings browser window



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

NTP status



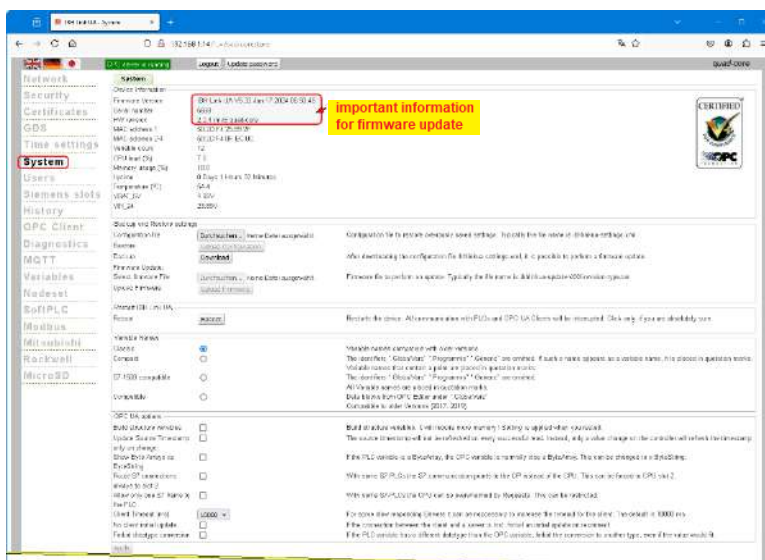
The date and time can be entered manually or automatically via the time server. Four (4) time servers are already preset.

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.

1.14 System browser window



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

1.14.1 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

ersion IBH Link UA V5.18 Dec 22 2020 15:09:00

The version number is important to carry out a firmware update. Only the 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, HW2 QC or HW3 QC-64) a firmware updated can be carried out (see page 1 - 40).

MAC addresses

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.

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

Variable count

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

Variable count 0

Hardware information

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.

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

1.14.2 Backup and Restore 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

Backup **Download** After downloading the configuration file ibhlinkua-settings.xml, it is possible to perform a firmware update.

After downloading the configuration file ibhlinkua-settings.xml, it is possible to perform a firmware update.

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 **Select file to upload** window opens.

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

Browse...

Backup and Restore settings

Configuration file **Browse...** **ibhlinkua-settings.xml** Configuration file to restore previously saved settings. Typically the file name is ibhlinkua-settings.xml.

Restore **Upload Configuration**

Backup and Restore settings

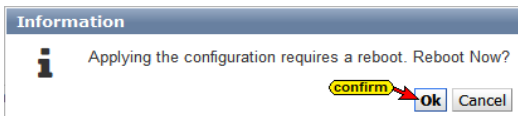
Configuration file **100 %** Configuration file to restore previously saved settings. Typically the file name is ibhlinkua-settings.xml.

Restore **Upload Configuration**

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.

1.14.3 Firmware Update



IBHsoftec Support will send you a link to the firmware update via email.

The firmware can be downloaded as a ZIP file.

To unpack the **ZIP file**, you will need a **password** that is attached to the link in the email.

Note:



The date and time must be set correctly in the browser window, as an OPC UA certificate with time stamps is required for the update.

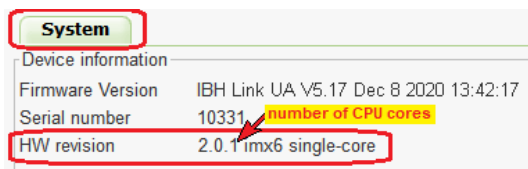
Certificates lose their validity if the time comparison is not correct. It is then no longer possible to update the firmware. (Error message).

HW1



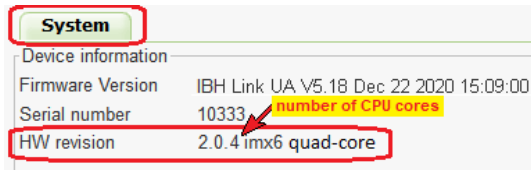
This firmware version is only intended for IBH Link UAs in whose browser window the system, under HW revision, shows a number separated by dots without any additions.

HW2 SC



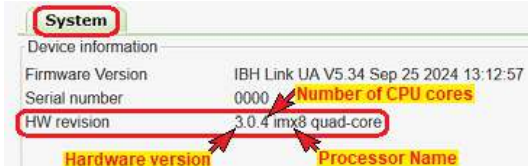
This firmware version is only intended for IBH Link UAs, in their browser window system, under HW revision, a number separated by dots (2.0.1 - the last digit indicates the number of CPU cores) and the Addition imx6 single-core (1 CPU core) indicates.

HW2 QC



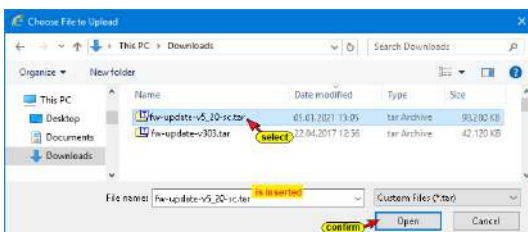
This firmware version is only intended for IBH Link UAs, in their browser window system, under HW revision, a number separated by dots (2.0.4 - the last digit indicates the number of CPU cores), and in the Additional quad-core (4 CPU cores) is included.

HW3 QC-64

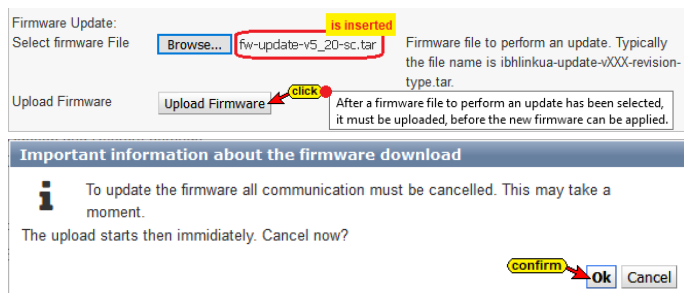


This firmware version is only intended for IBH Link UAs, in their browser window system, under HW revision, a number separated by dots (2.0.4 - the last digit indicates the number of CPU cores), and in the Additional quad-core (4 CPU cores) is included.

Select saved firmware file

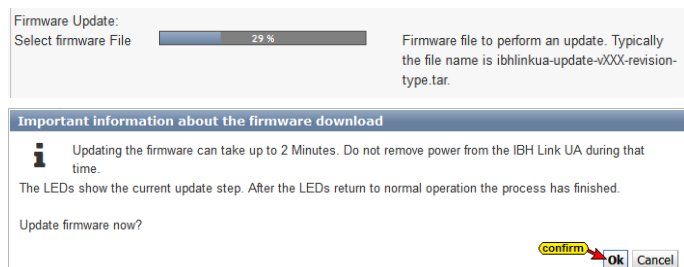
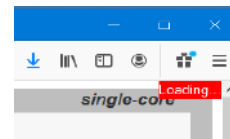


The **firmware file *.tar** is displayed in the IBH Link UA's System browser window.



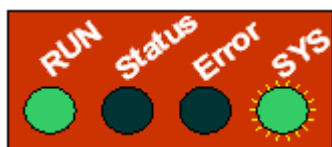
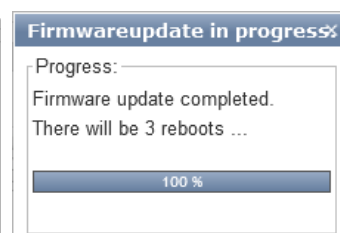
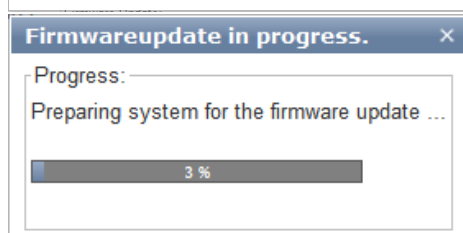
Click the **Upload Firmware** button to load the new firmware into the IBH Link IoT. The new firmware is not yet accepted (updated). Confirm the message.

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



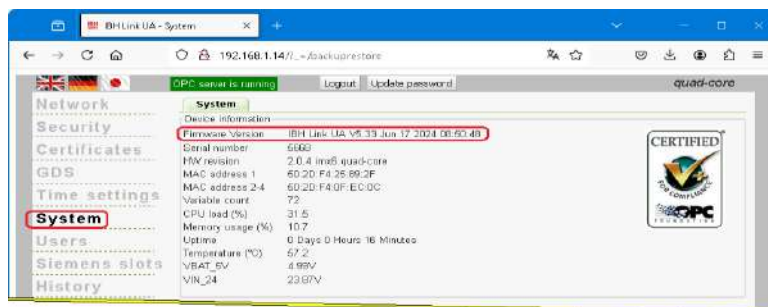
The loading of the firmware is indicated. If the loading is completed, the following message is displayed.

Confirm the message.



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

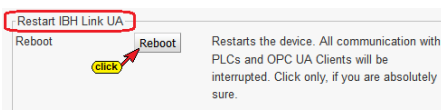
In normal operation, the **RUN** LED is lit, the **SYS** LED flashes, and the LED's **Status** and **Error** are off.



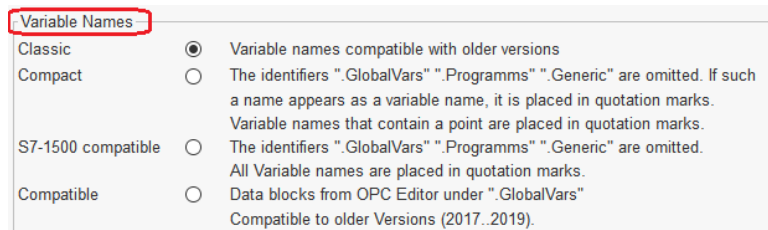
Update completed

Restart the IBH Link UA

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



1.14.4 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:

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

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 transferring to the IBH Link UA. The identifiers **".GlobalVars"**, **".Programs"**, **".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.

Compact:

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

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"**, **".Programs"**, **".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.

S7-1500 compatible:

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."Off2"

Points in variable names must be removed from the symbol table (S7 SIMATIC Manager) before transferring 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"**, **".Programs"**, **".Generic"** are omitted in the variable names.

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)

1.14.5 OPC UA options

Variable Names	
Classic	☒
Compact	☐
S7-1500 compatible	☐
Compatible	☐
Variable names compatible with older versions The identifiers ".GlobalVars", ".Programms", ".Generic" are omitted. If such a name appears as a variable name, it is placed in quotation marks. Variable names that contain a point are placed in quotation marks. The identifiers ".GlobalVars", ".Programms", ".Generic" are omitted. All Variable names are placed in quotation marks. Data blocks from OPC Editor under ".GlobalVars" Compatible to older Versions (2017...2019)	
OPC UA options	
Build structure variables	☐
Update Source Timestamp only on change	☐
Show Byte Arrays as ByteString	☐
Route S7 connections always to slot 2	☐
Allow only one S7 frame to the PLC	☐
Client Timeout [ms]	10000
No client initial update	☐
Forbid datatype conversion	☐
Build structure variables. It will require more memory! Setting is applied when you restart The source timestamp will not be refreshed on every successful read. Instead, only a value change on the controller will refresh the timestamp. If the PLC variable is a ByteArray, the OPC variable is normally also a ByteArray. This can be changed to a ByteString. With some S7-PLCs the S7 communication points to the CP instead of the CPU. This can be forced to CPU slot 2. With some S7-PLCs the CPU can be overwhelmed by Requests. This can be restricted. For some slow responding Servers it can be necessary to increase the timeout for the client. The default is 10000 ms. If the connection between the client and a server is lost, forbid an initial update on reconnect. 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 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.

Only allow one S7 frame to the PLC

Some S7 controllers can be overwhelmed by the number of requests. The number of requests is limited by activating this option.

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.

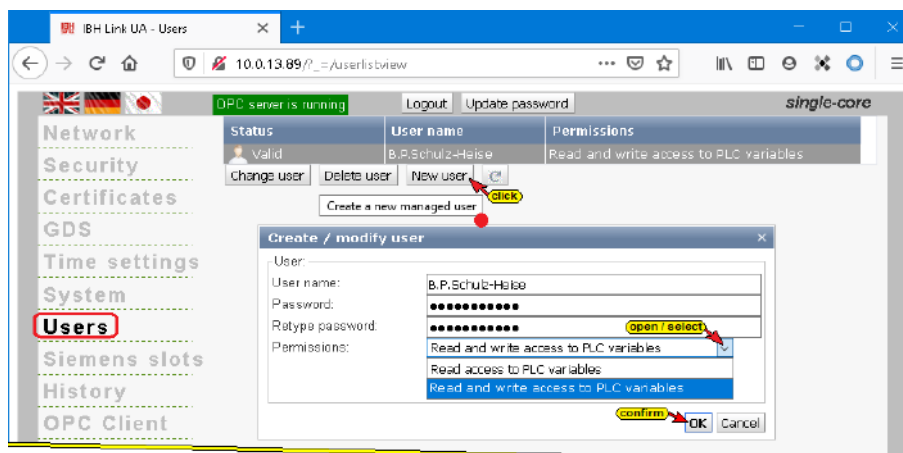
No client initial update

If the connection between the client and the server was interrupted, do not perform an initial update when reconnecting.

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.

1.15 Users browser window



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

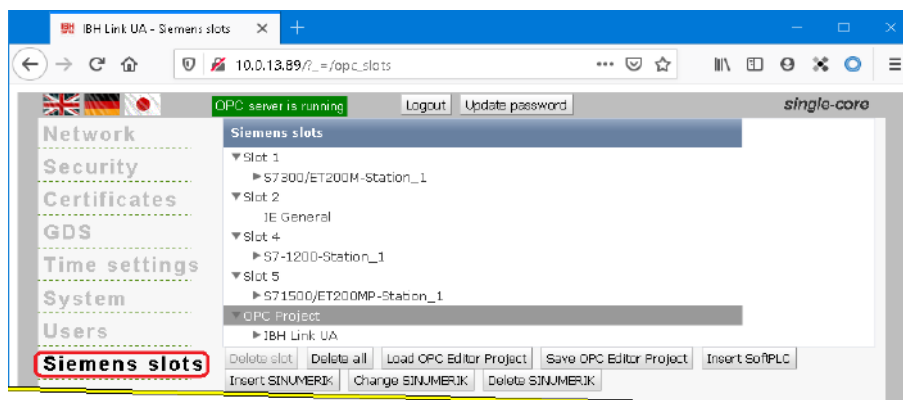
If inadmissible characters (e.g. spaces) are entered in the username or password, the background of the input line changes to be red. The input must be corrected accordingly.

Spaces are not allowed in the username.

The username for browser access is always **admin**.

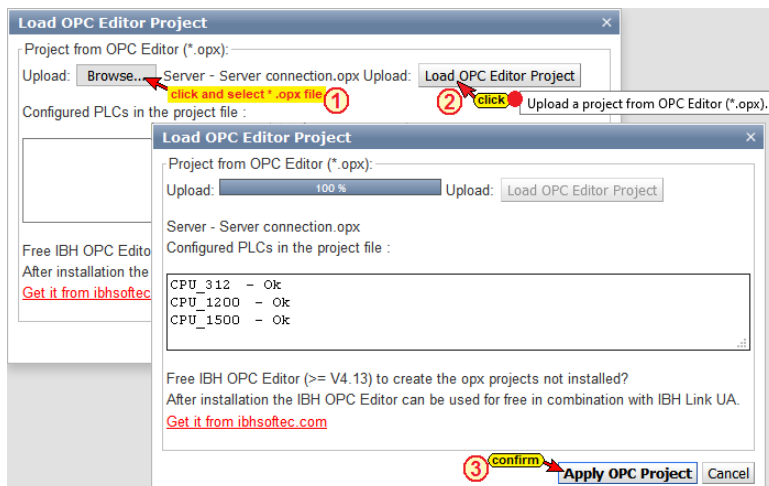
User name: B. P. Schulz-Heise
Password:

1.16 Browser window Siemens slots



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

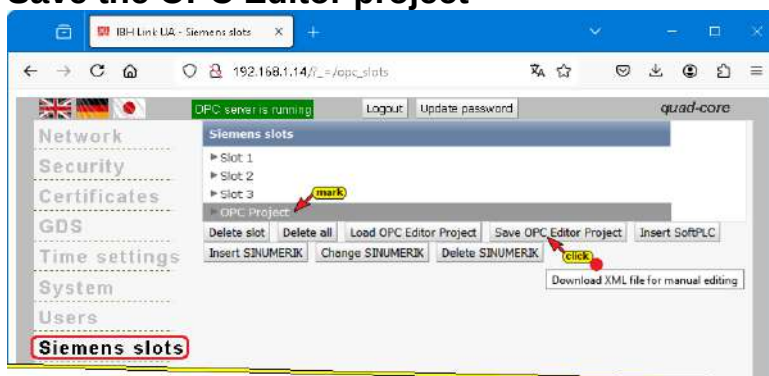
Load the OPC Editor project



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**.

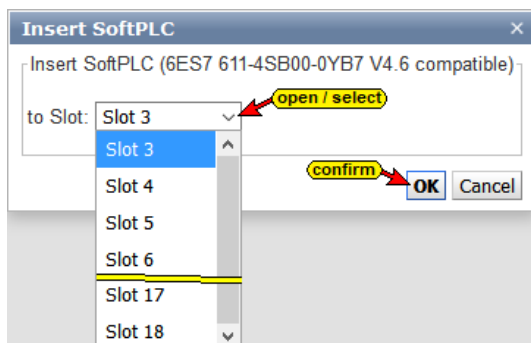
Save the OPC Editor project



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



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

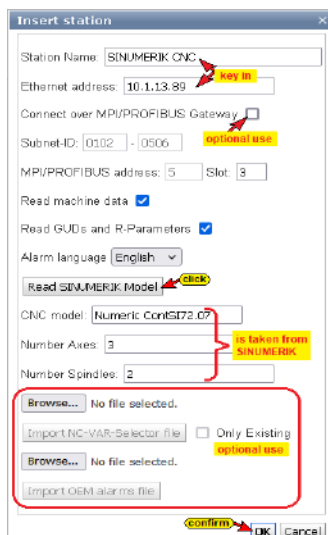
Insert SoftPLC

Note:



The **SoftPLC** must not be activated in Slot 2 under any circumstances. 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**, **SolutionLine** and **SINUMERIK One**.

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

Connect over MPI/PROFIBUS Gateway ☒ **activated**

Subnet-ID: 0102 - 0506 **can be changed**

MPI/PROFIBUS address: 3 Slot: 4

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

Read SINUMERIK Model

Read SINUMERIK Model

CNC model: Numeric ContSI72.07

Number Axes: 3

Number Spindles: 2

**is inserted by
SINUMERIK CNC**

By clicking on **Read SINUMERIK** model, a connection to the CNC is established and information available in the SINUMERIK is read.

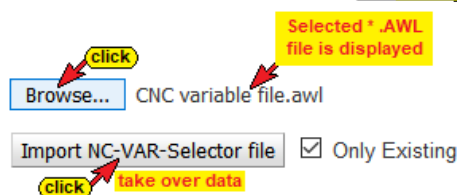
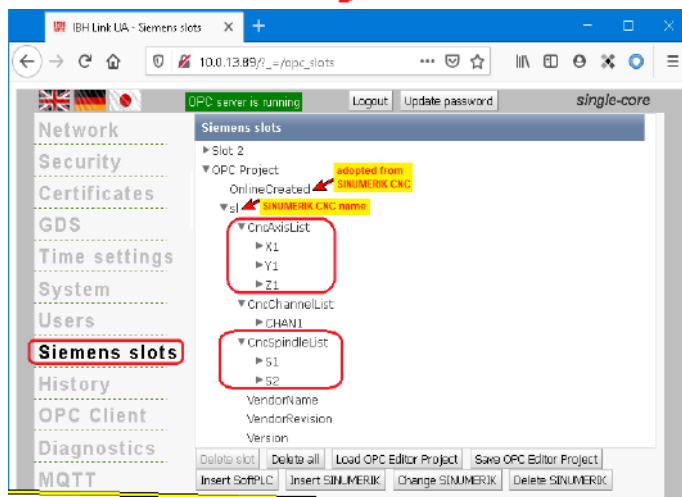
If model, axis and spindle information can be read, the **SINUMERIK** model name, number of axes and spindles

are displayed in the dialog box. The complete information, prepared as an XML file, is adopted under OPC Project by clicking **OK**.

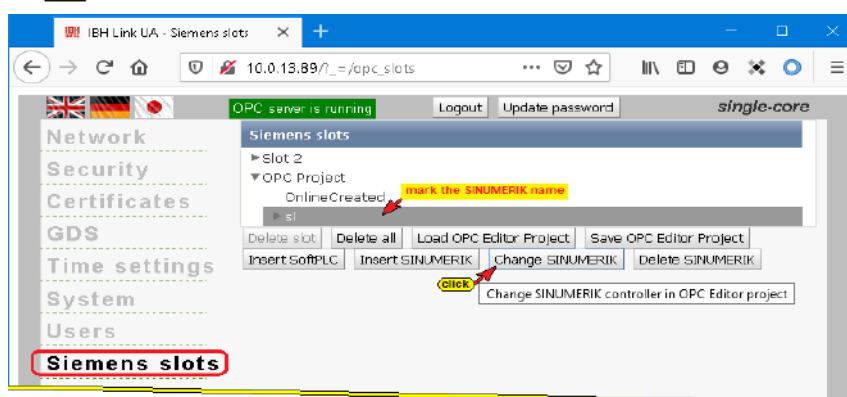
Import NC-VAR file

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



Change SINUMERIK

A project that has been adopted by SINUMERIK CNC can be changed.

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

Save OPC Editor Project

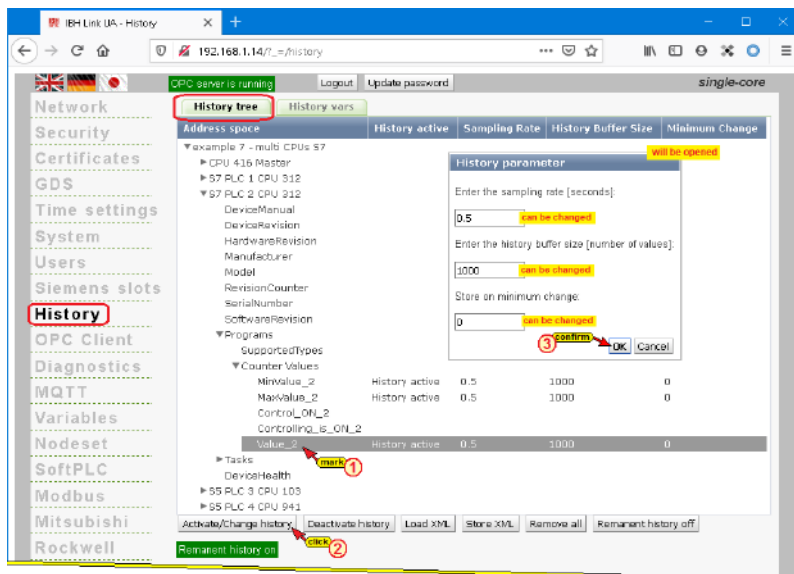
A SINUMERIK CNC project that is available in the Siemens Slots browser window (OPC project) can be saved to be further edited with the IBH Link UA Editor.

1.17 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.

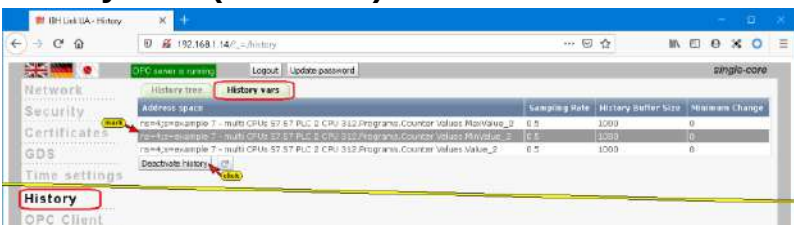
History tree



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 RAM.

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**.

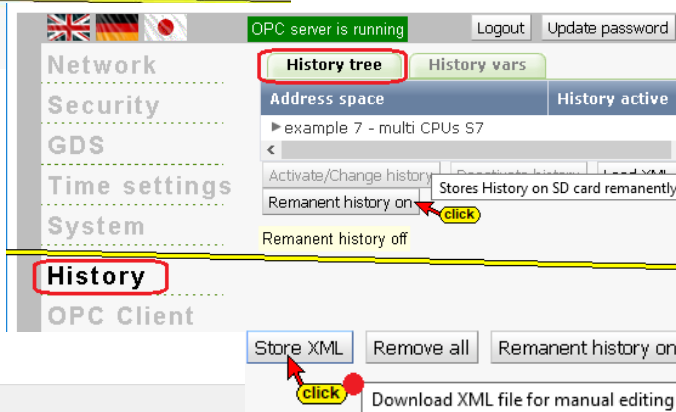
Retentive history



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.



```

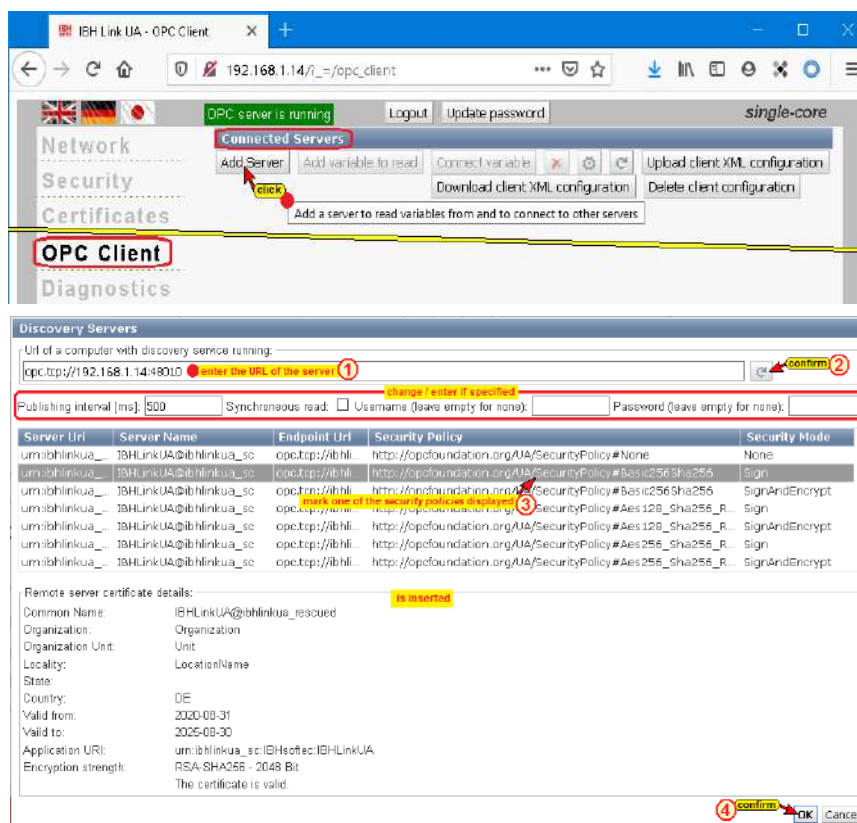
1 <?xml version="1.0"?>
2 <ibhlinkua-history-config>
3 <historyconfiguration>
4 <node samplinginterval="0.5" queueSize="1000" absolutechange="0" ns=4; s=example 7 -
5 - multi CPUs S7, S7 PLC 2 CPU 312, Programs.Counter Values.MinValue_2 </node>
6 <node samplinginterval="0.5" queueSize="1000" absolutechange="0" ns=4; s=example 7 -
7 - multi CPUs S7, S7 PLC 2 CPU 312, Programs.Counter Values.MaxValue_2 </node>
8 <node samplinginterval="0.5" queueSize="1000" absolutechange="0" ns=4; s=example 7 -
9 - multi CPUs S7, S7 PLC 2 CPU 312, Programs.Counter Values.Value_2 </node>
10 </historyconfiguration>
11 </ibhlinkua-history-config>

```

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



1.18 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.

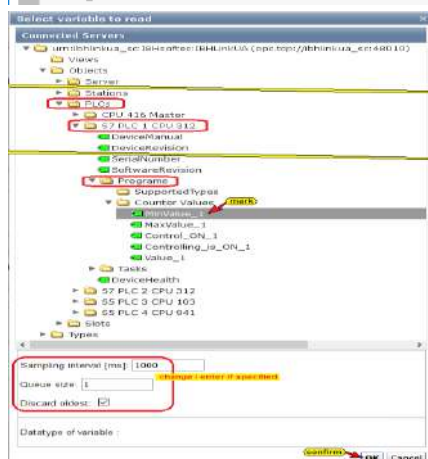
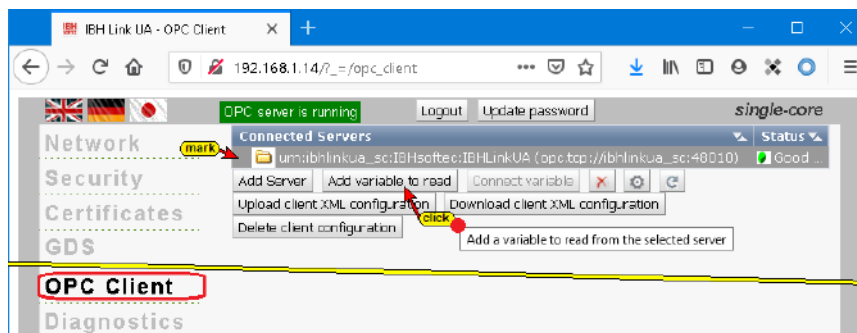
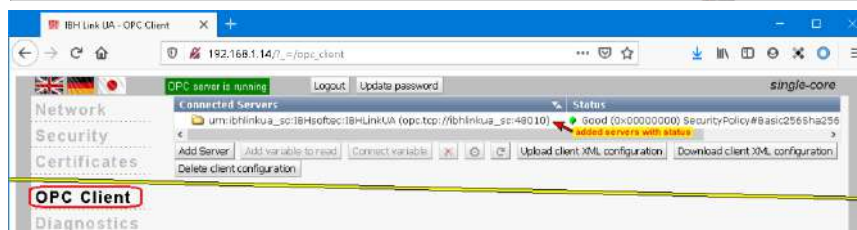
In the IBH Link, UA web browser window **OPC Client**, the server and the variables for the data exchange are specified. The endpoint URL should preferably be entered with a symbolic IP address. An absolute IP address can be entered in the Security browser window (not recommended).

Connected servers with status are listed.

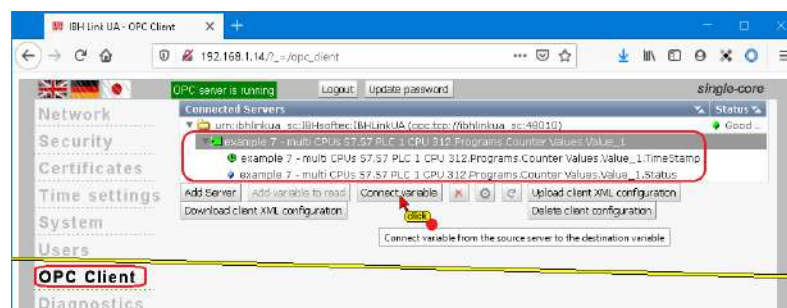
Define read variables

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

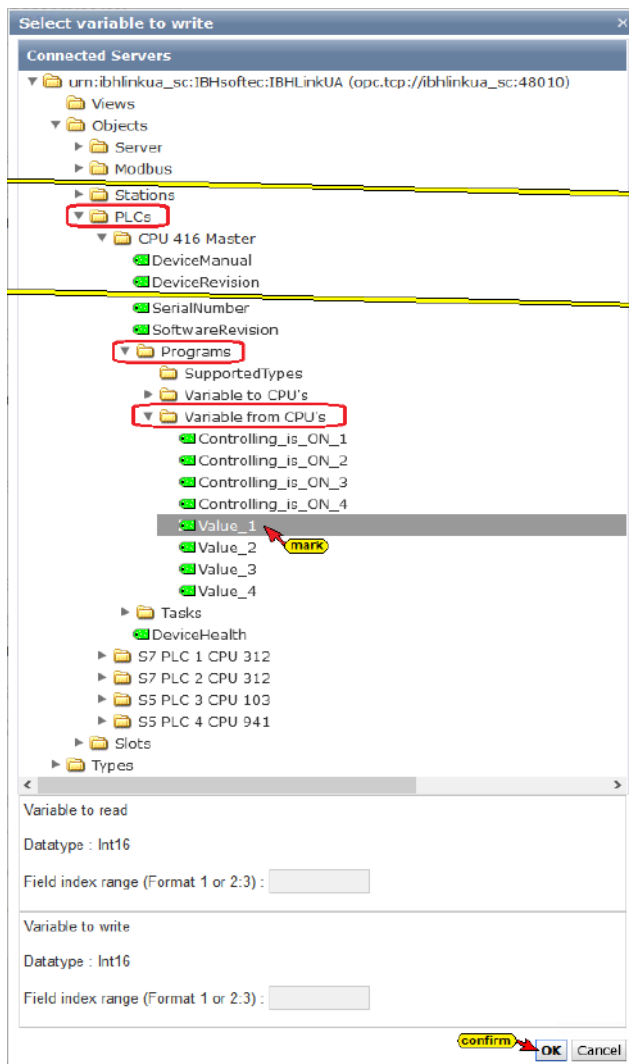
Clicking on Add read variable opens the Select read variable window. The OPC variable that is to be read must be selected here.



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



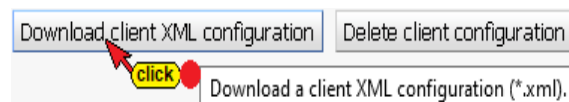
Clicking on **Connect variable** opens the **Select variable to write** window. The OPC variable to be written must be selected here (as TimeStamp, Status and Value).

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.



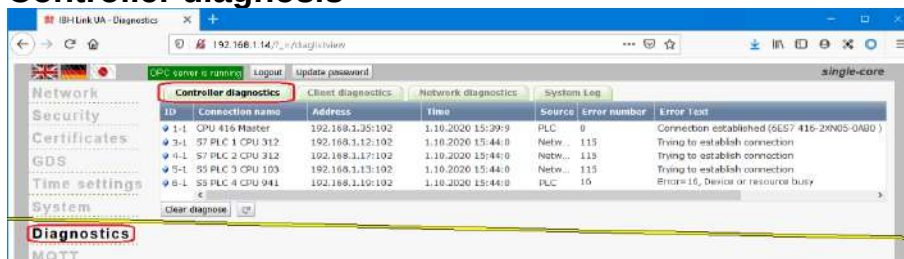
By clicking the **Upload client XML configuration** button, a manually edited configuration of the OPC variable connections is uploaded to the IBH Link UA in XML file format.



1.19 Diagnostics browser window

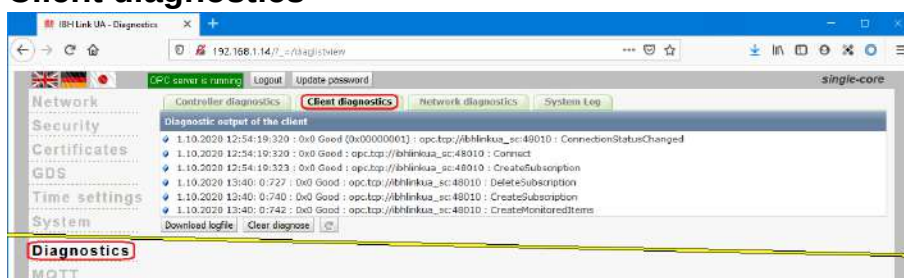
The browser window **Diagnostics** has several tabs to display details about established or faulty connections.

Controller diagnosis

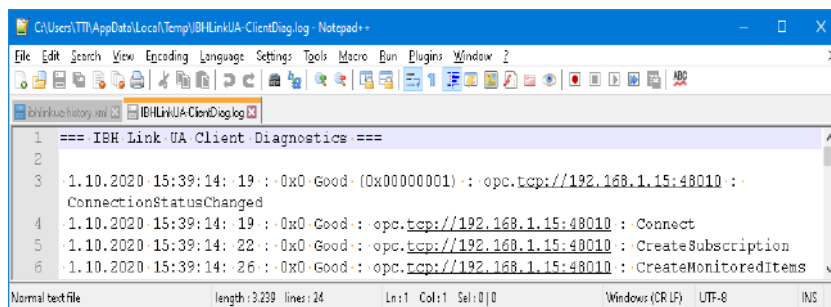


The configured connections and their status (error-free / faulty) are displayed.

Client diagnostics



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

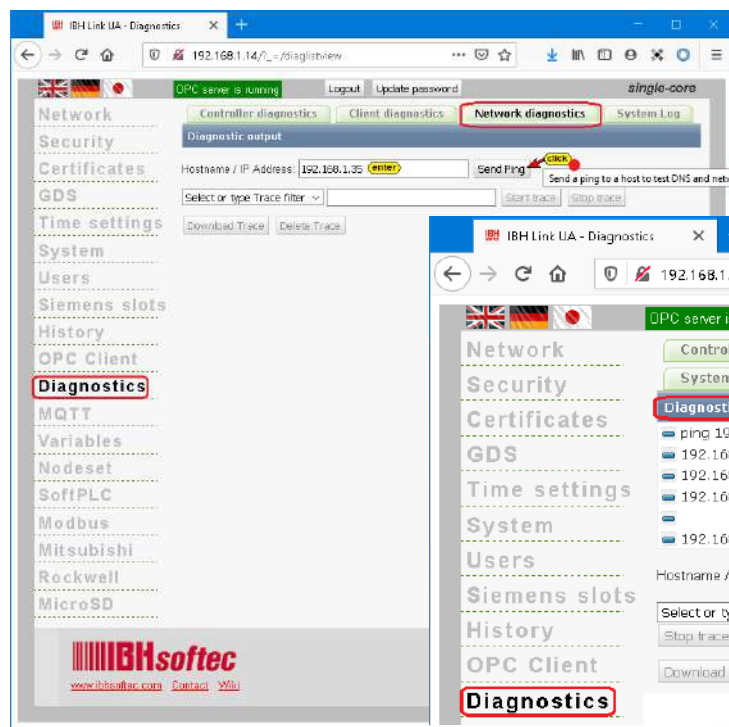


By clicking the **Download logfile** button, the saved states

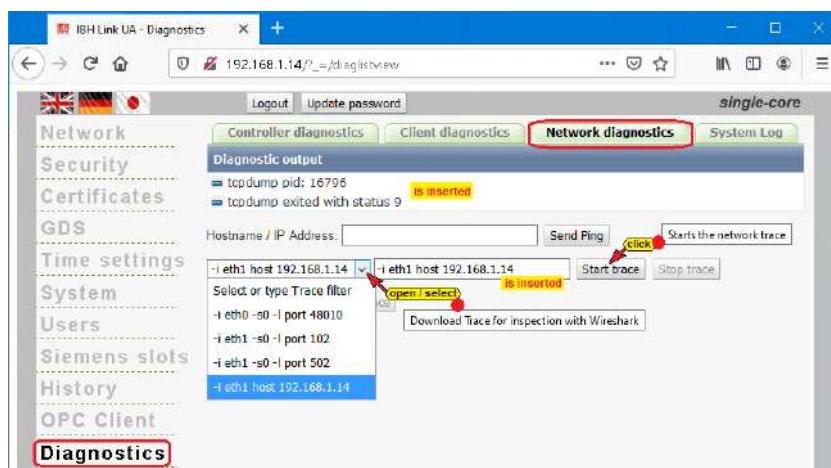
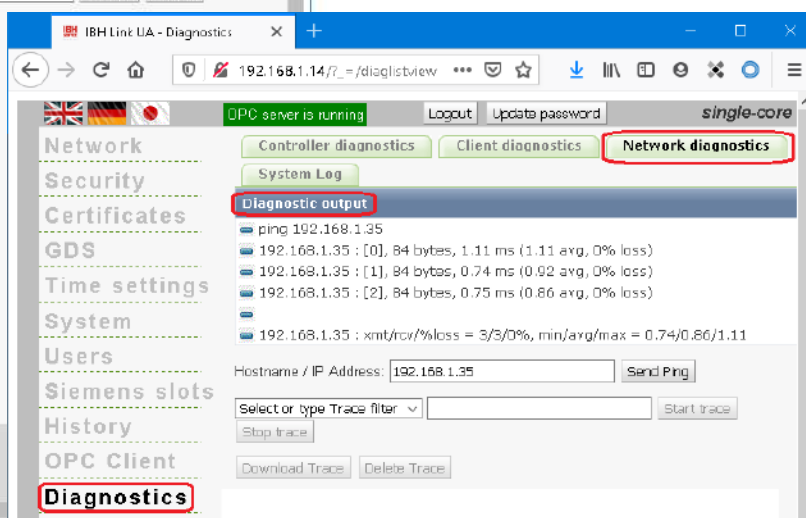
Download logfile Clear diagnose

Download the logfile of the client to correct project settings of the configured OPC client connections (error-free / faulty) can be displayed in an editor or saved as a text file.

Network diagnostics



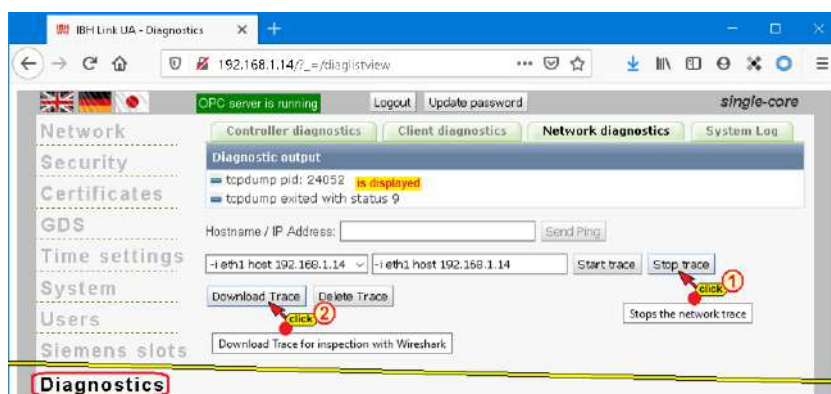
An ICMP ping is sent to the specified IP address (host name) by clicking the Send ping button.

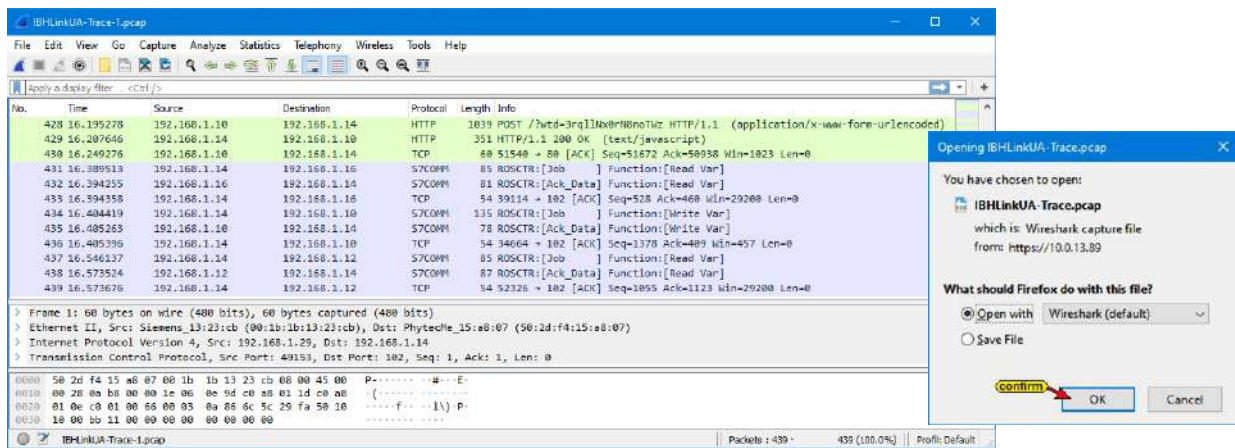


If the Wireshark diagnostic software is installed on the PC, a very extensive network analysis can be carried out.

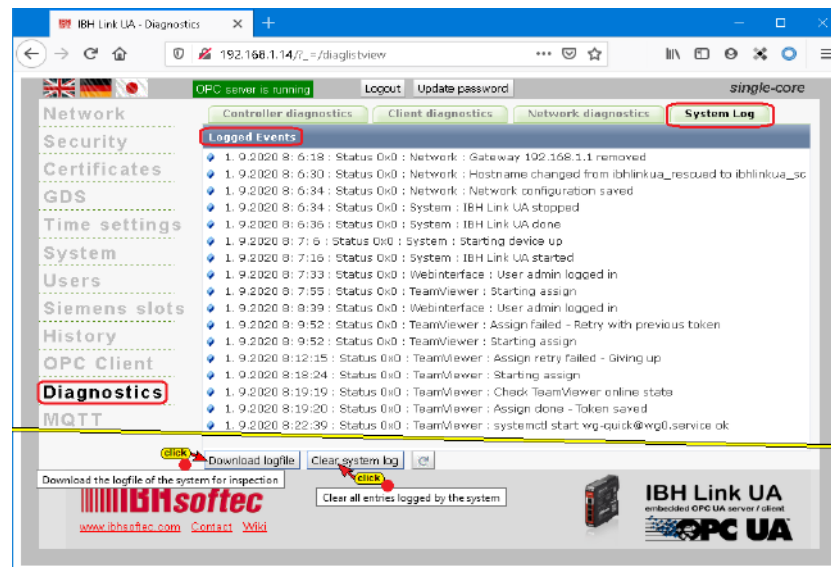


By clicking on Download recording and confirming the opening with Wireshark, the Wireshark window - Trace is opened or can be saved in a file. Since the evaluation of Wireshark-Trace requires some specialist knowledge, this diagnosis should be carried out in the event of a malfunction using the IBHsoftec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





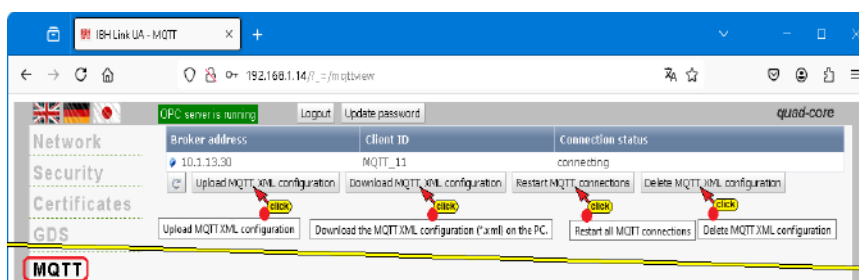
System Log



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

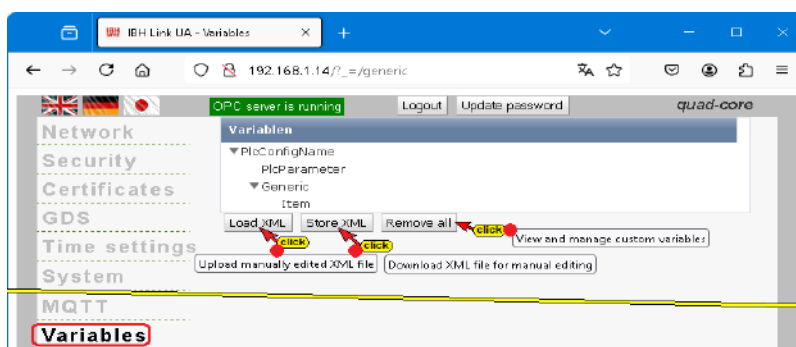
Buttons are provided to display the log file in an editor or to save it as a text file or to delete it. In the event of a malfunction, an analysis can be carried out using the IBHsofttec hotline.

1.20 MQTT browser window



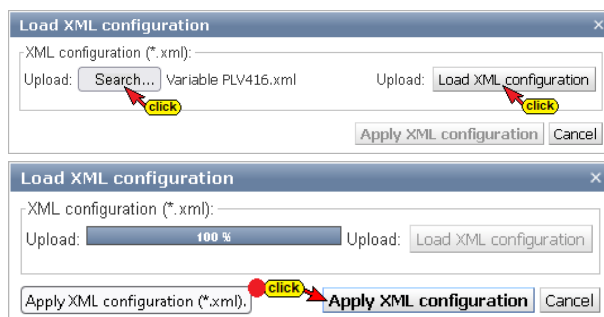
It is possible to load or delete an MQTT configuration. An existing MQTT connection can be restarted. Information about connections to existing MQTT brokers is displayed in the connection status.

1.21 Browser window variables



If variables that were created in the IBH OPC UA Editor and transferred from there are not required as OPC variables, they can be removed by clicking on the **Remove all** button.

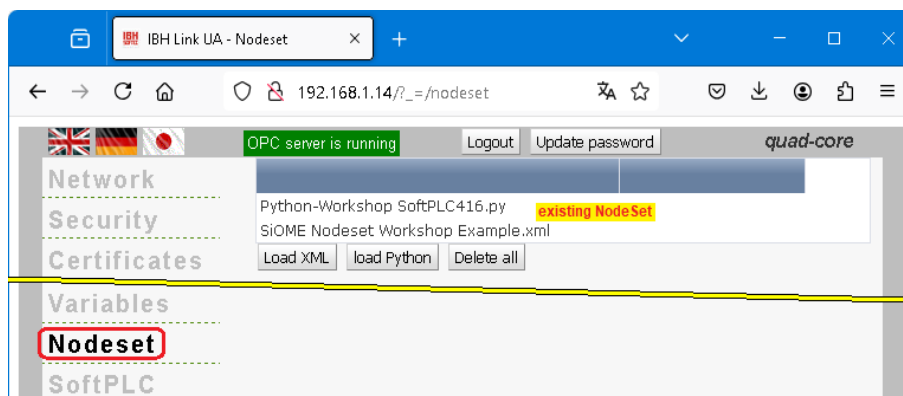
Clicking on the **Store XML** button automatically saves the XML file.



By clicking the **Load XML** button, the desired file can be selected in the Upload File dialog box. Clicking the Load XML Configuration button starts the loading process. The file is accepted by clicking **Accept XML Configuration**.

OPC variables created in the IBH OPC UA Editor can be exported as an **.xml file**.

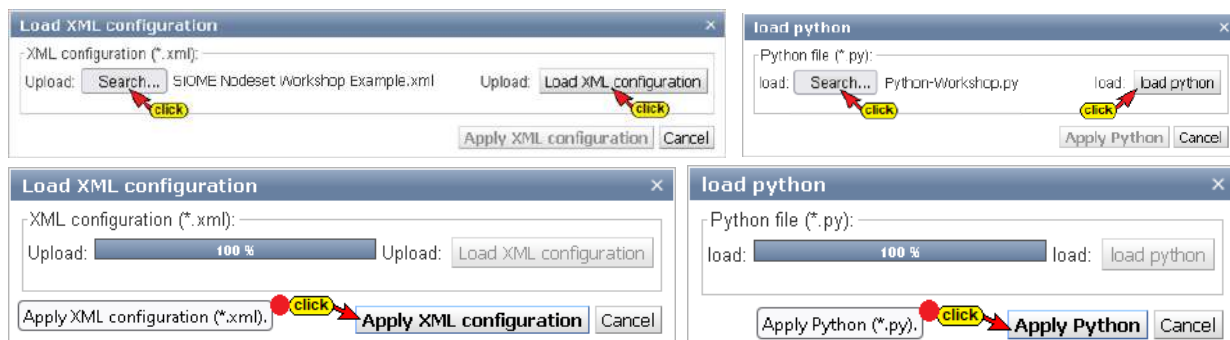
1.22 Browser window node set



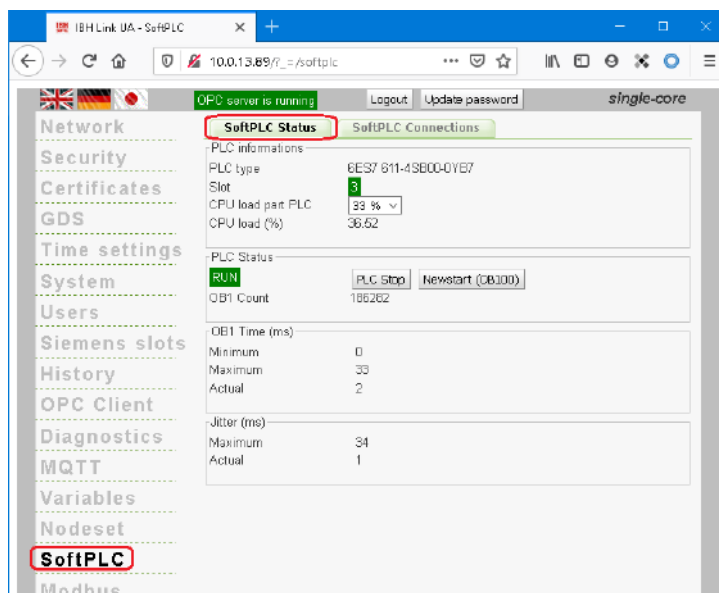
This option is only activated in the IBH-Link-UA-QC-64 / QC-32, as this requires more memory.

Data models or companion specs can be read in on the IBH Link UA using Python modules. To do this, the desired companion spec or data model is integrated into a project

on the IBH Link UA. To do this, the corresponding XML file is uploaded to the IBH Link UA.



1.23 SoftPLC browser window



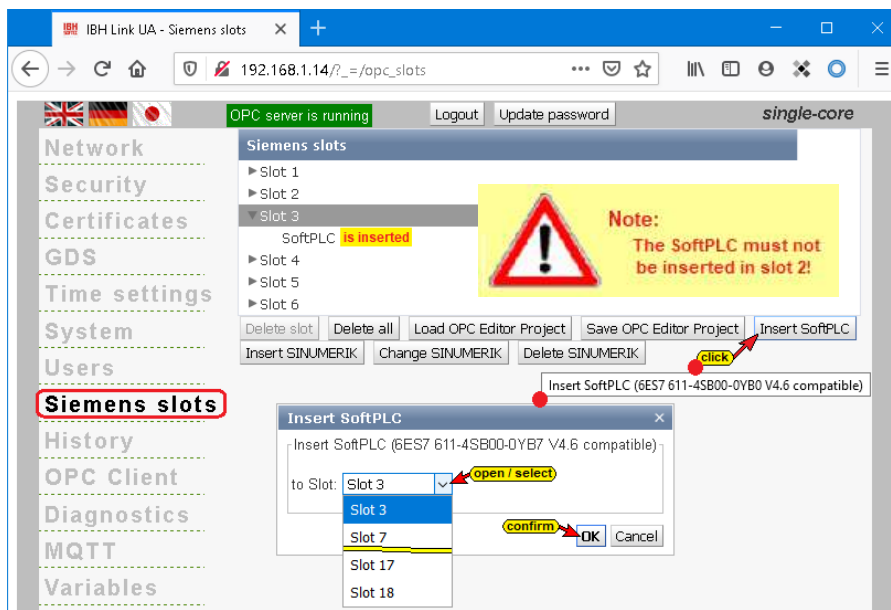
Browser window SoftPLC / SoftPLC status

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

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

Buttons for starting and stopping SoftPLC are available.

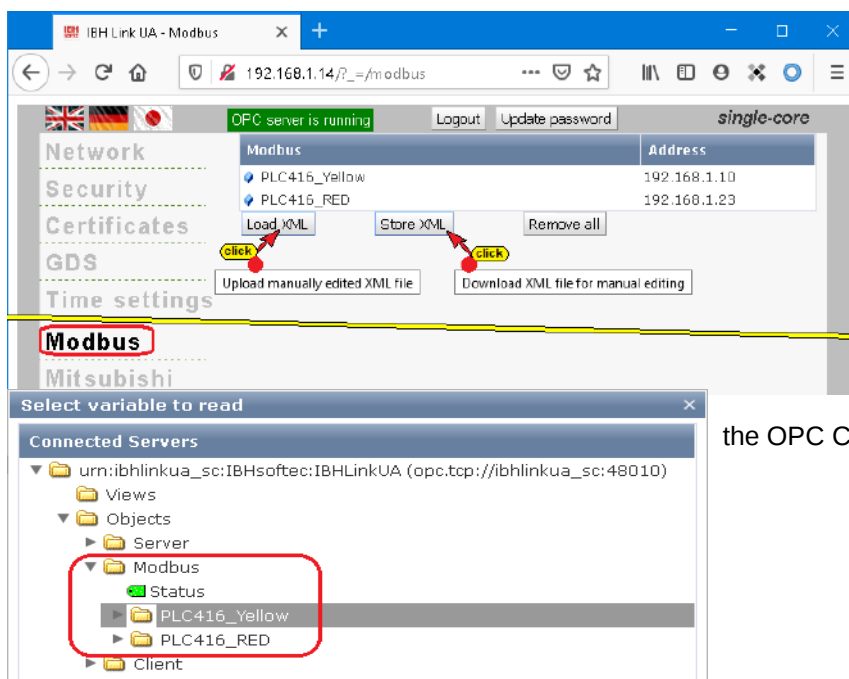




Manuals for handling the **SoftPLC**, IBH Link UA Manual **PLC projects with TIA Portal** and IBH Link UA **Manual PLC projects with S7 SIMATIC Manager**, are available for download on the IBHsoftec WIKI website.

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

1.24 Modbus browser window

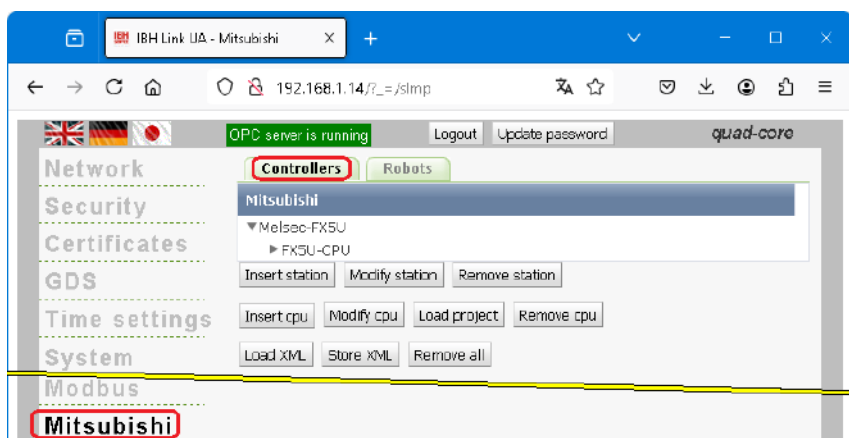


A created Modbus configuration can be transferred directly to the IBH Link UA from the IBH OPC UA Editor.

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

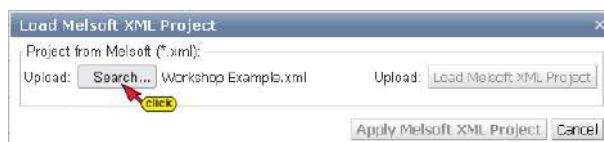
The created Modbus variables cannot be seen in the web interface. The existing Modbus variables can be displayed via the OPC Client browser window.

1.25 Mitsubishi browser window

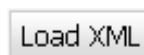


In the **Mitsubishi** browser window **Controllers**, variables of an online connected Mitsubishi PLC can be read in, declared as read / write or as variables to be connected.

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

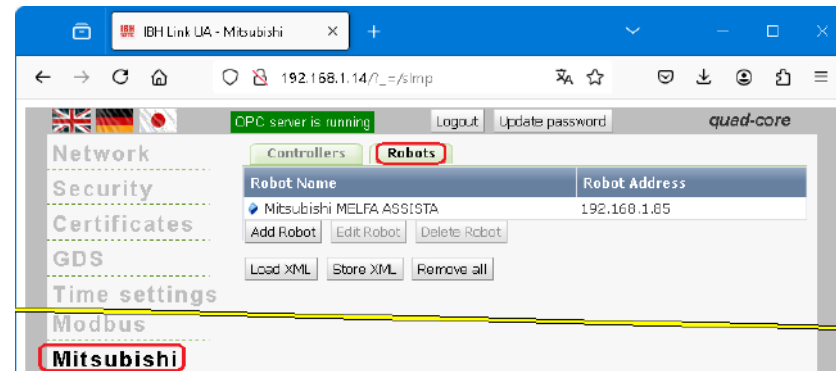


The Load XML button enables an XML file exported with the **Mitsubishi Melssoft** software to be loaded directly into the IBH Link UA.



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.

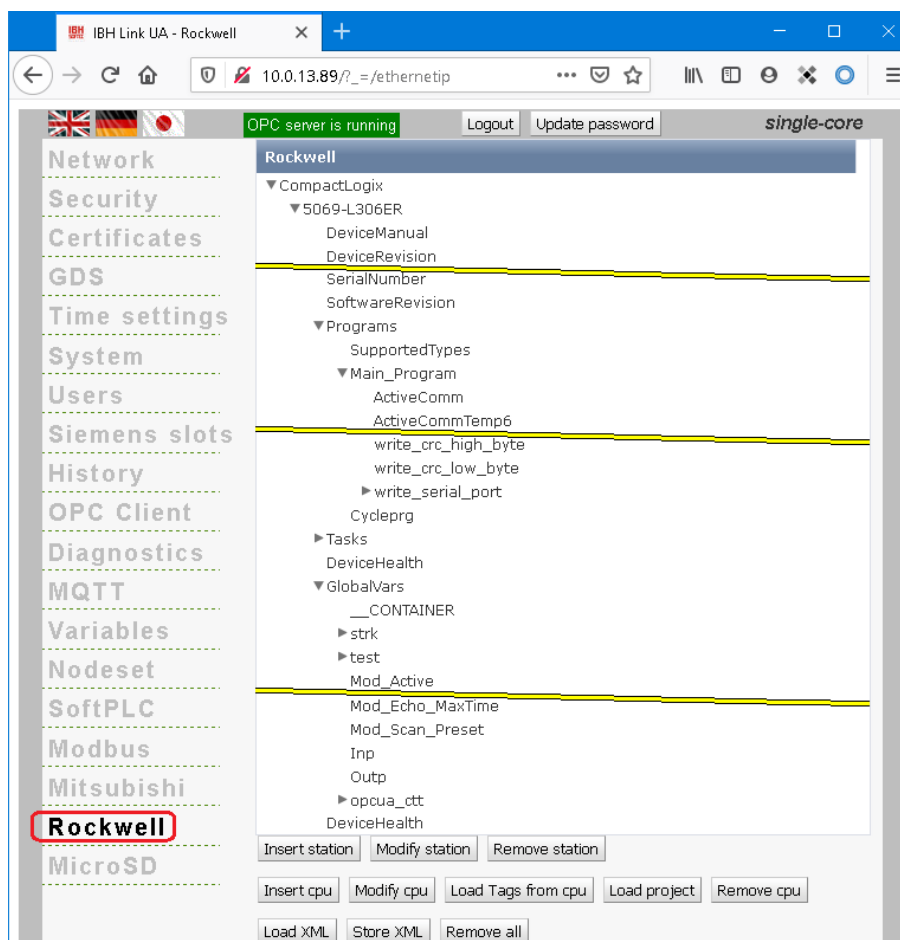
Mitsubishi robot



In the **Mitsubishi** browser window **Robots**, variables of an online connected Mitsubishi Robot can be read in, declared as read / write 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.

1.26 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.

1.27 MicroSD browser window

The **IBH Link UA Quad Core 64** has a slot for a MicroSD card on the front and the **IBH Link UA Quad Core 32** and the **IBH Link UA Single Core** have 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 **historical variables** are also saved on the Micro SD card and can be accessed after a power failure of the IBH Link UA.

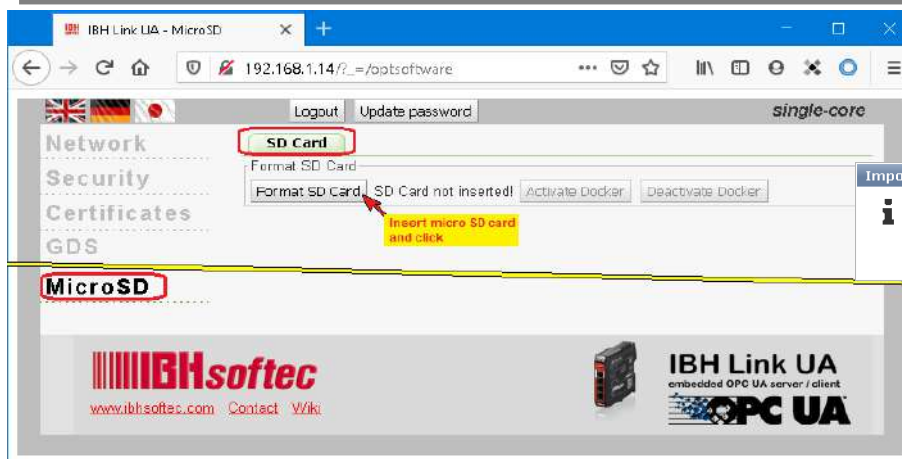
Information on formatting is displayed and must be confirmed.



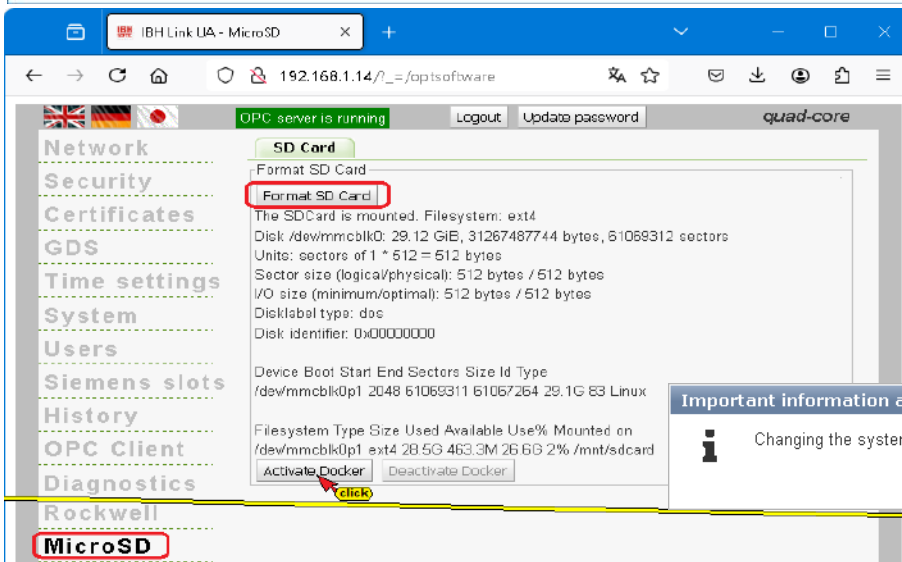
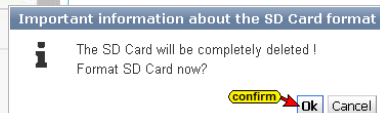
Note:

If there is a formatted Micro SD card in the IBH Link UA, the current IBH Link UA configuration is saved on the Micro SD card.

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

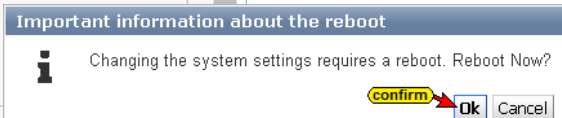


Information on formatting is displayed and must be confirmed.



The formatted SD-card will be mounted automatically.

Activate Docker



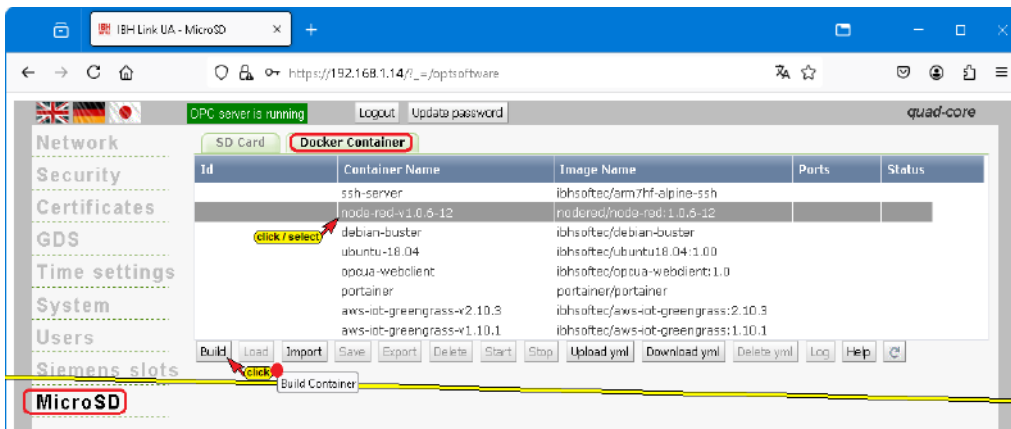
1.27.1 Docker Container

The Docker option can be activated in IBH Link UA devices with the **Quad Core performance level (QC-64, QC-32)**. The **Docker container** software provides an interface for creating and managing containers. The following containers are already present in the base package:

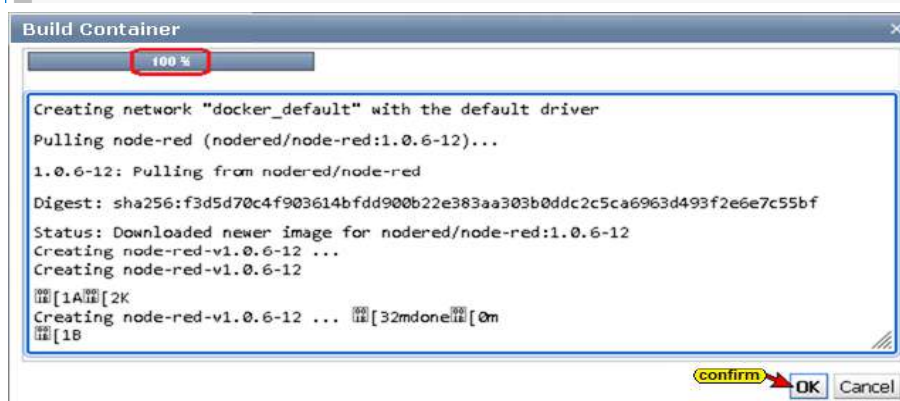
quad-core 64
quad-core

- ssh-server (ibhsoftec/arm7hf-alpine-ssh)
- node-red-v1.0.6-12 (nodered/node-red:1.0.6-12)
- debian-buster (ibhsoftec/debian-buster)
- ubuntu-18.04 (ibhsoftec/ubuntu 18.04:1.00)
- opcua-webclient (ibhsoftec/opocua-webclient: 1.0)
- portainer (portainer/portainer)
- aws-iot-greengrass-v2.10.3 (ibhsoftec/aws-iot-greengrass: 2.10.3)
- aws-iot-greengrass-v1.10.1 (ibhsoftec/aws-iot-greengrass: 1.10.1)

Activate Docker



An SD card is required for the additional storage space required for a Docker container. Docker can then be activated. This requires a restart of the IBH Link UA.

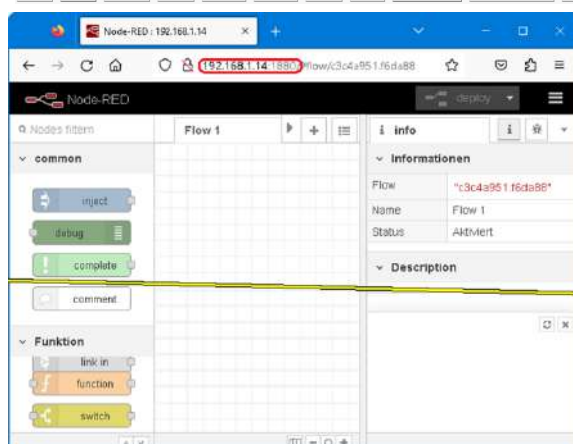


Clicking the Create button starts container creation. The creation process is displayed. Once the container has been created, it is listed in the MicroSD/Docker Container browser window. The container can then be used, e.g. Node-RED.

Open Node-RED



Once Node-RED has started, Node-RED can be called up. To do this, enter the IBH Link UA address (management or control level) in the



web browser with the port specified under Ports (1880).

The Node-RED input field is displayed in the web browser and is ready for input.

Other programs in the Docker container are called in much the same way.

1.28 IBH Link UA default factory configuration

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.

Reset button hardware revisions HW3 Quad-Core 64



The reset button for resetting the software to factory settings is located on the front of the hardware revisions HW3 QC, below the display LEDs.

Reset button hardware revisions HW2 SC and HW2 SQ

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.



Reset button hardware revisions HW1

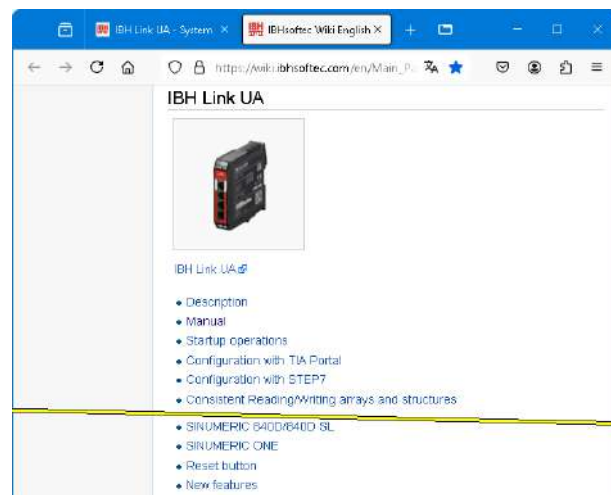
With hardware revisions **HW1**, the reset button is located behind the middle ventilation slot below the QR code.

1.29 Open the Wiki

IBHsofttec 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.



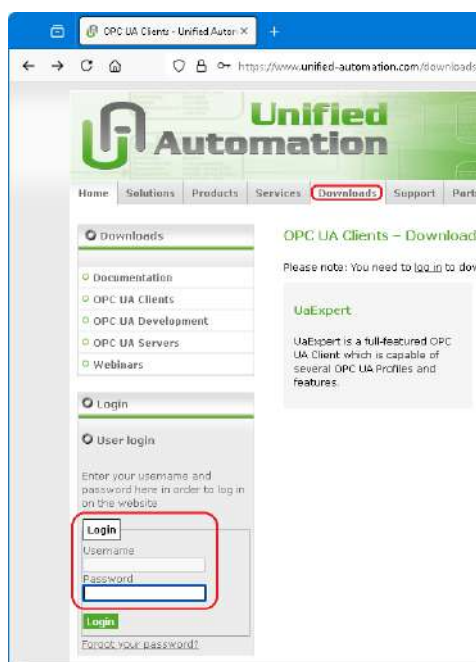
If your PC is connected to the Internet, the WIKI page can be directly called from the **IBH Link UA**.



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

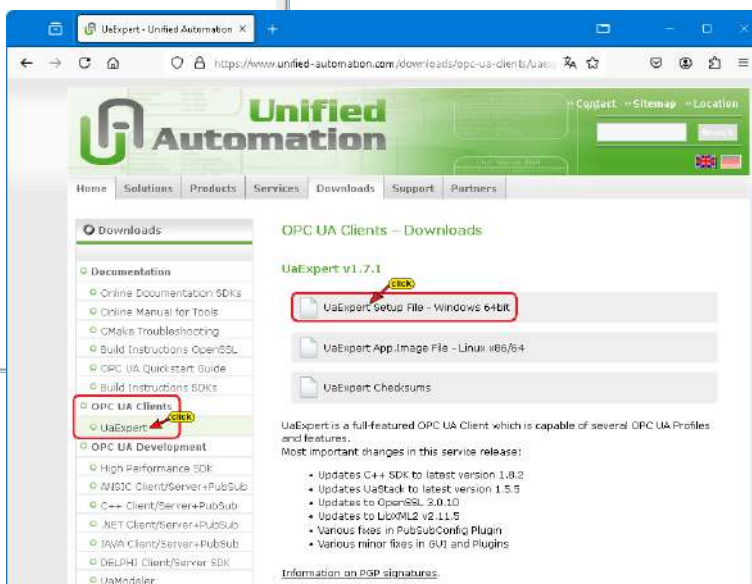
The tool kit manufacturer Unified Automation offers an OPC UA client as free software on its homepage, which is particularly suitable for testing and displaying OPC variables (OPC tags) provided by an OPC server.

2.1 Unified Automation UaExpert – The OPC UA Client and OPC UA Server

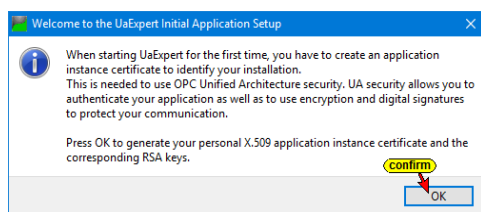


They can be downloaded via: <http://www.unified-automation.com>
Free download requires Unified Automation registration.

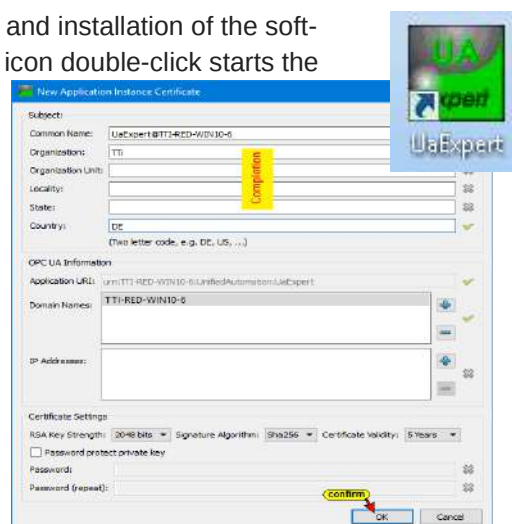
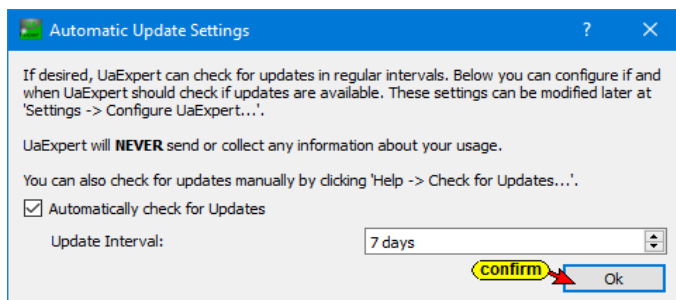
To demonstrate the work of the IBH Link UA, it is helpful to have an OPC client and an OPC Server program running on the PC. It is recommended to use the OPC UA client program **UaExpert** and the OPC Server program **UaCCPServer** from Unified Automation.

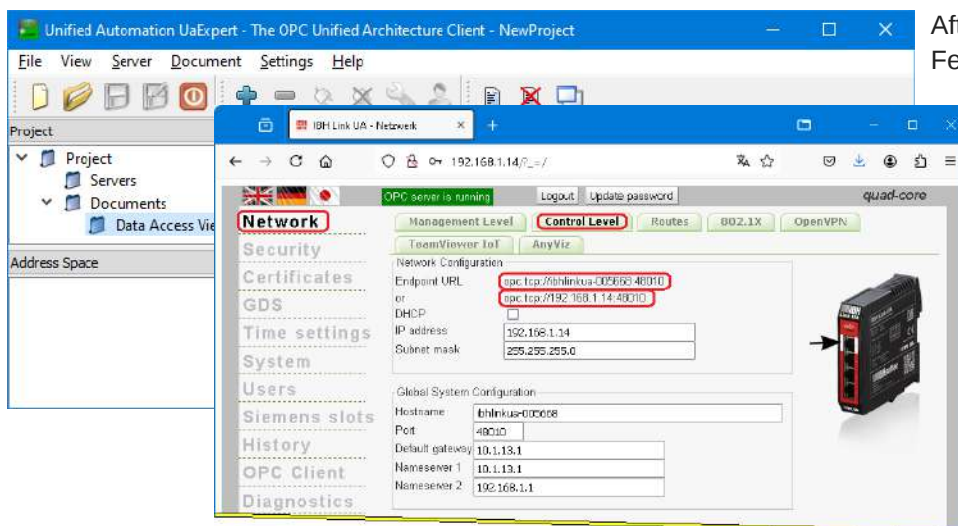


2.1.1 Starting UaExpert



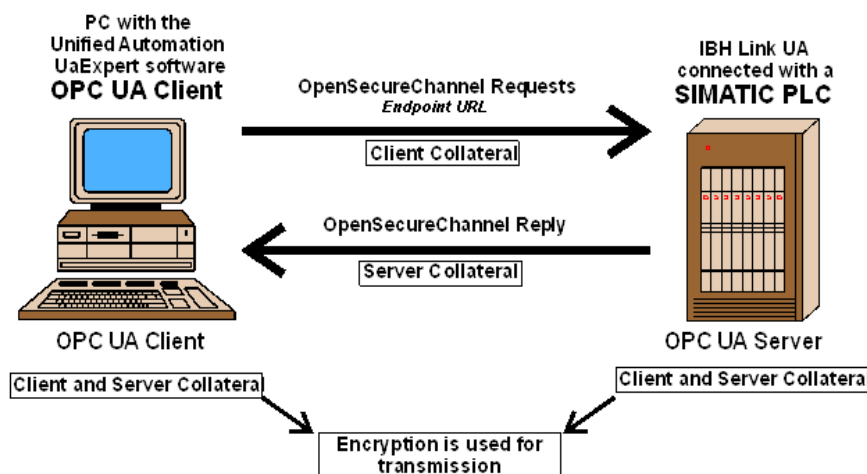
After downloading and installation of the software, a **UaExpert** icon double-click starts the program. Several presets are to be made and confirmed.





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.

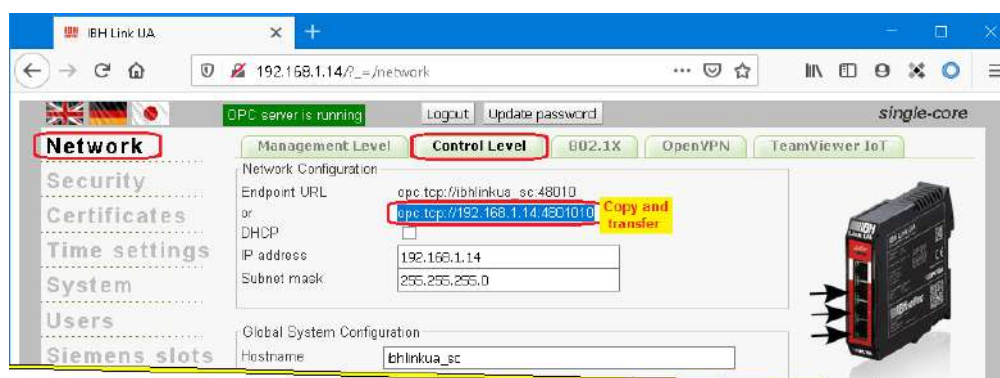
Note:

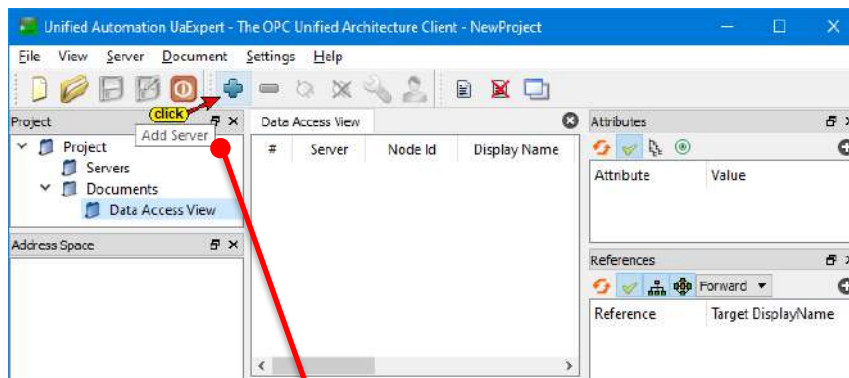


If an **absolute IP address** is used as the host name when entering the **endpoint URL**, an error message is displayed when establishing the connection from the OPC UA client (**UaExpert**) to the OPC UA server (**IBH Link UA**) stating that the host name or **configuration name** do not match. **These messages can be ignored !**

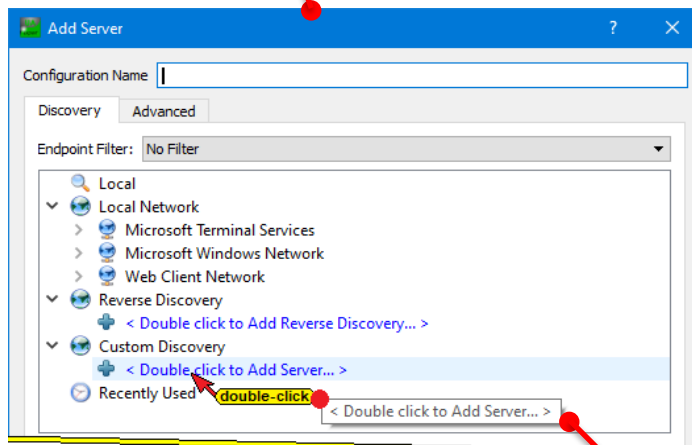
In this manual, the absolute IP address is used as the host name in the examples when entering the **endpoint URL**.

To do this, the **endpoint URL** is copied from the browser window to the clipboard.





Clicking on the **plus** symbol opens the **AddServer** dialog box.

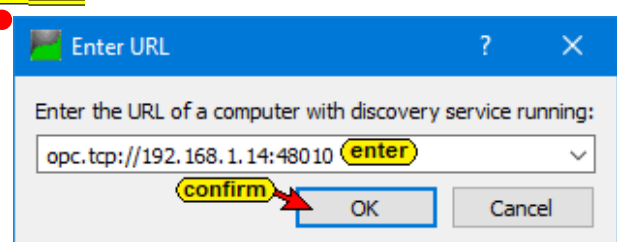
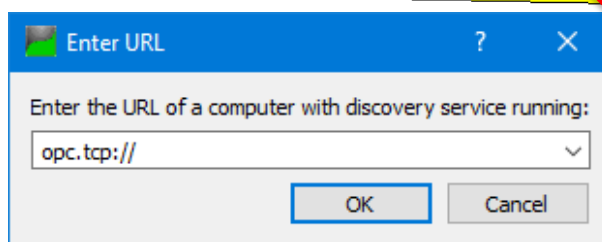


Double-clicking on **< Double click to Add Server... >** opens the

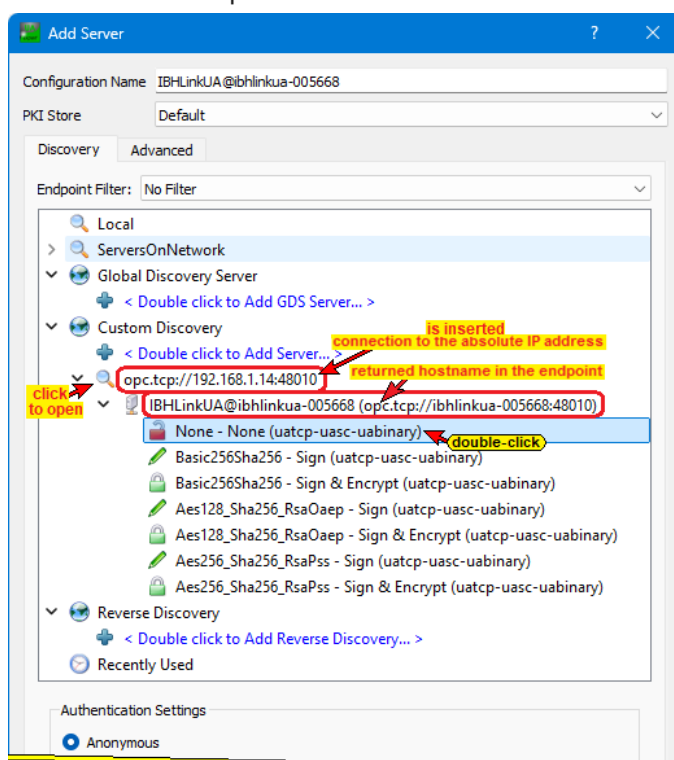


Enter URL dialog box. The **endpoint URL** from the IBH OPC UA Server/Client Browser window **Network / Control Level** must be entered here.

Preferably, the **endpoint URL** should be used with the hostname so that the client can verify the names of the endpoints and the names in the certificate.



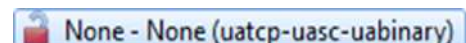
If no **DNS** server is available to supply a hostname, the absolute IP address is used as an exception. In this case, the absolute **Endpoint URL** is copied from the browser window to the clipboard.



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

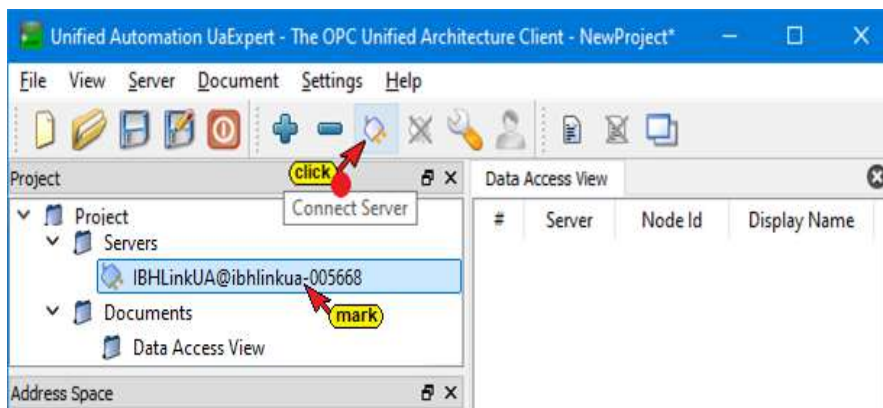
With a click on the inserted **IBHLinkUA@ibhlinkua-005668** opens the security levels marked in the IBH Link UA browser window **Security / Server Security**.

Double-clicking the security level **None (uatcp-uasc-uabinary)** in the **AddServer**

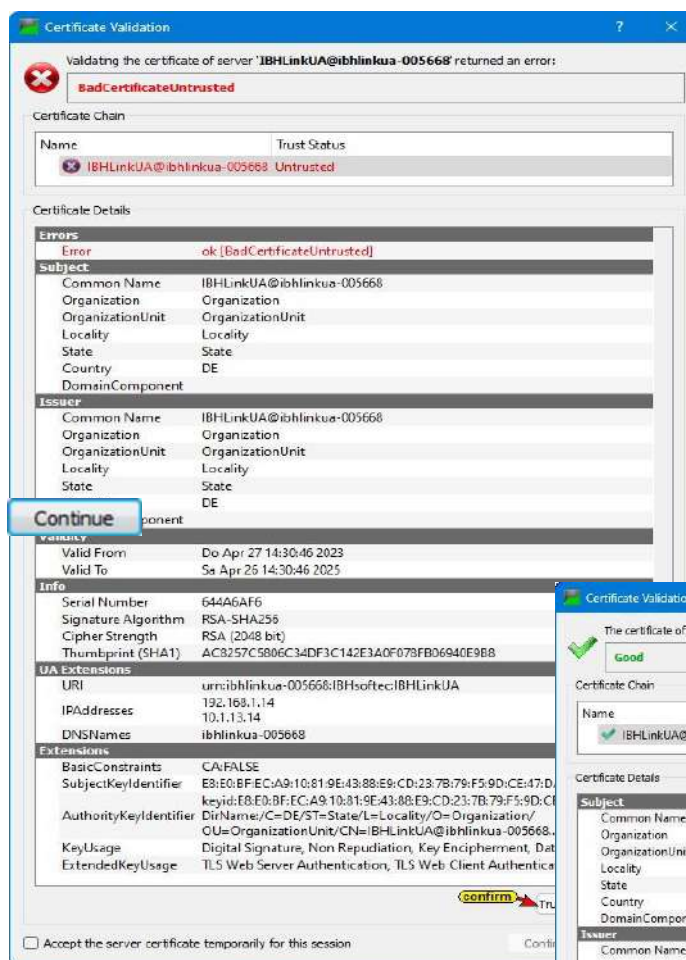
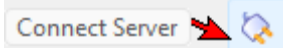


dialog box sets the security level, the **AddServer** dialog box is closed and the **UaExpert** window opens.

UaExpert window



To display the contents of OPC Variables (OPC-Tags and the corresponding OPC UA connecting information, the selected server **IBH Link UA@ibhlinkua-005668** must be connect. Mark the Server and click the **Connect Server** icon.



The Certificate Validation dialog box for accepting the OPC UA server certificate of the **IBHLinkUA@ibhlinkua-005668** is displayed.

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

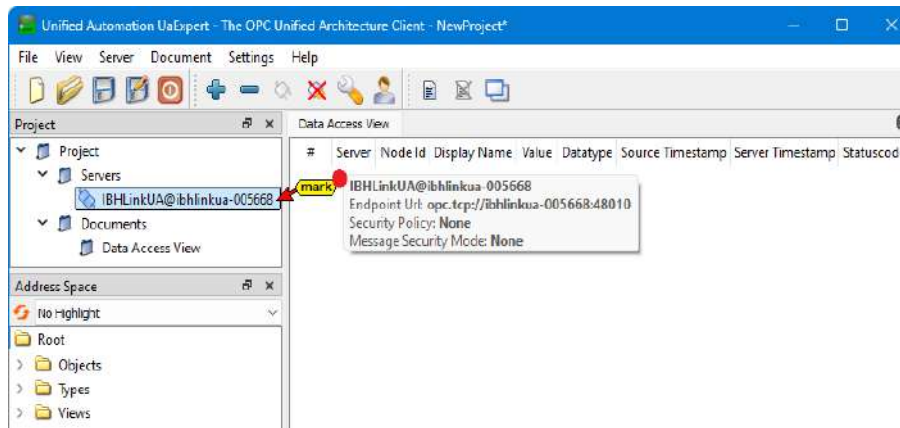


The confirmed server certificate **IBHLinkUA@ibhlinkua-005668** is displayed.

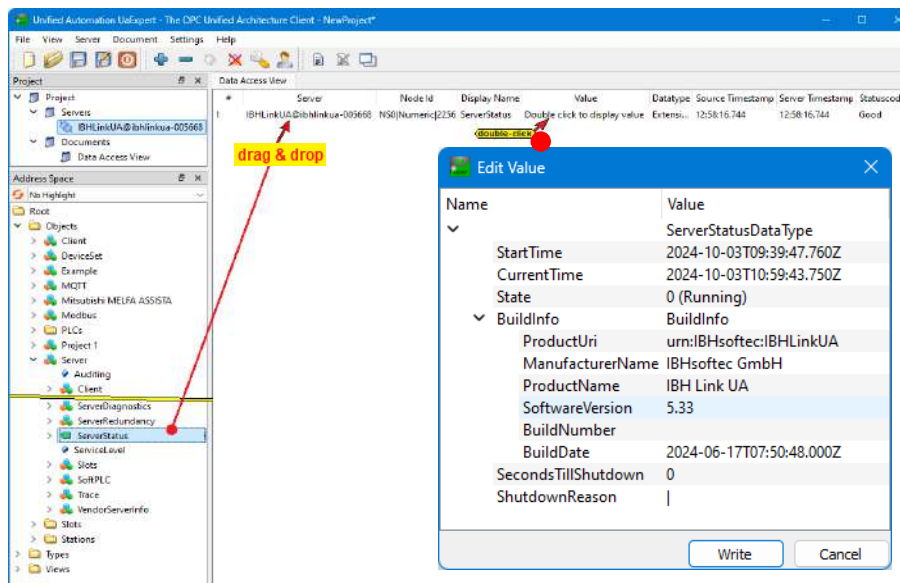
Clicking the **Continue** button closes the dialog box.



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



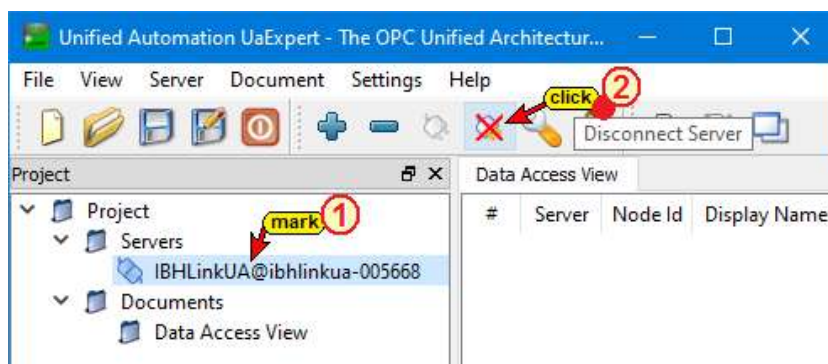
In the **UaExpert** program window, information about the connected server is displayed under **Address Space**. After opening Server/Server Status, information from the IBH OPC UA Server/Client software is listed.



Using **Drag & drop** information (server) can be pulled into the Data Access Viewer window. Details of the IBH OPC UA Server/Client are displayed here.

With **drag & drop** any number of information can be pulled from the **AddressSpace** window into the **DataAccess Viewer** window to show details.

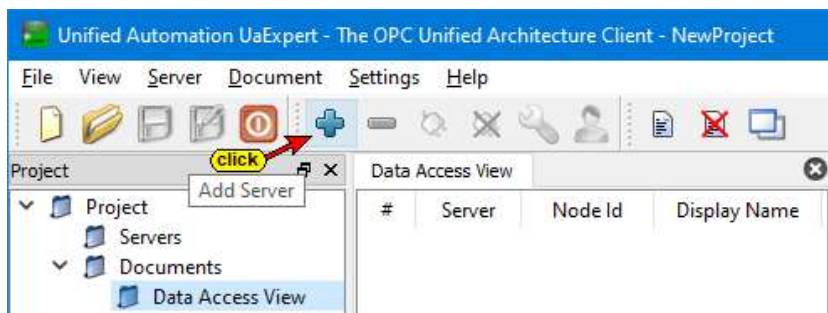
2.3 Encrypted connection to the IBH Link UA



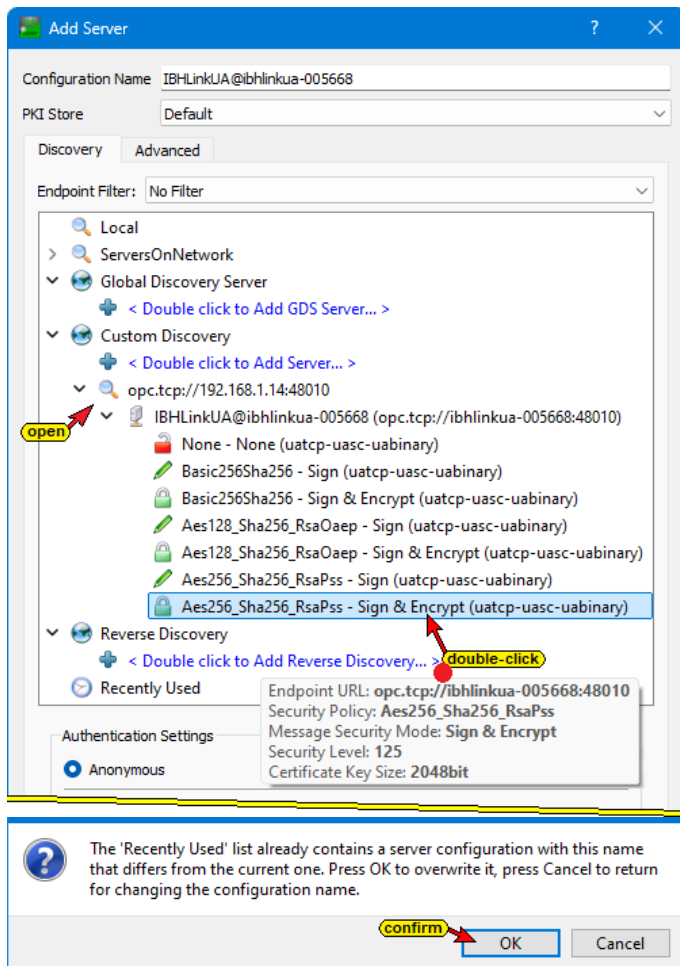
To establish another (e.g. encrypted) connection to the IBH Link UA, the existing must be disconnected, as only one connection can exist. Mark the connected server name **IBHLinkUA@ibhlinkua-005668** and then click the **Disconnect Server** icon.



To remove the Server out of the **Project**, mark the connected server name **IBHLinkUA@ibhlinkua-005668** and then click the **Remove Server** icon (minus symbol)



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.



Open the recently activated connected server **IBHLinkUA@ibhlinkua-005668** to display the list of the security levels marked in the IBH Link UA browser window **Security / Server Security**.

The encrypted connection to the OPC UA server of the IBH OPC UA Server/Client software is configured here.

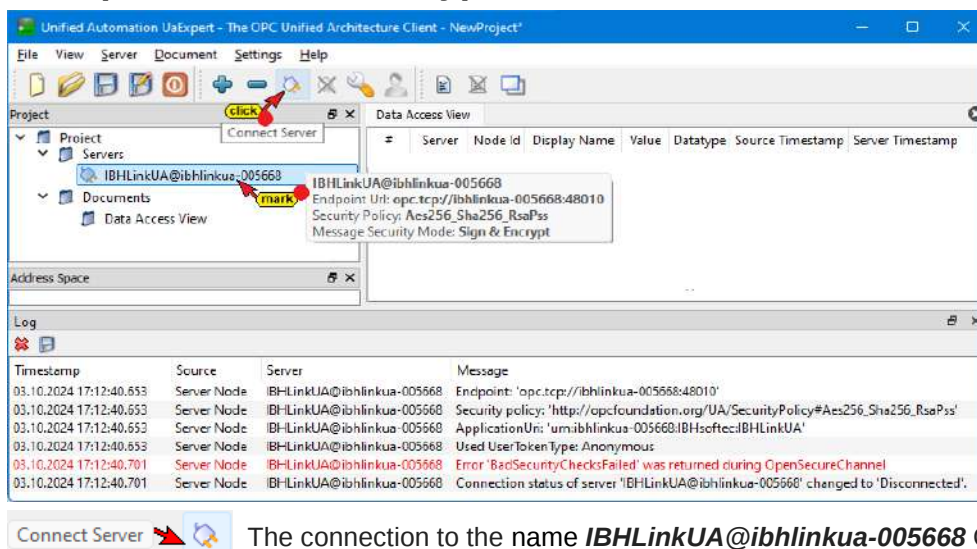
Desired encrypted connection

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, the selected encrypted connection is displayed under **Project / Servers** in the **Unified Automation UaExpert** window.

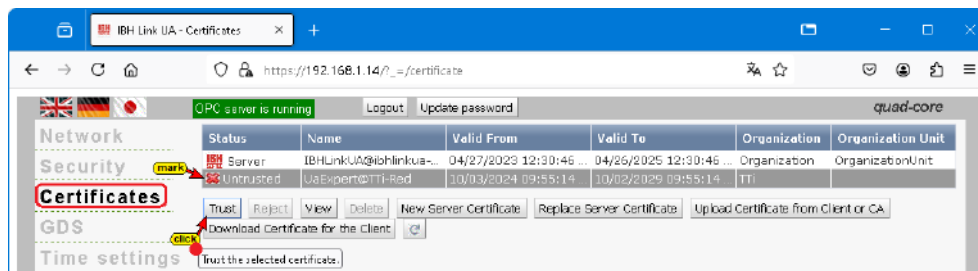
UaExpert window – encrypted connection



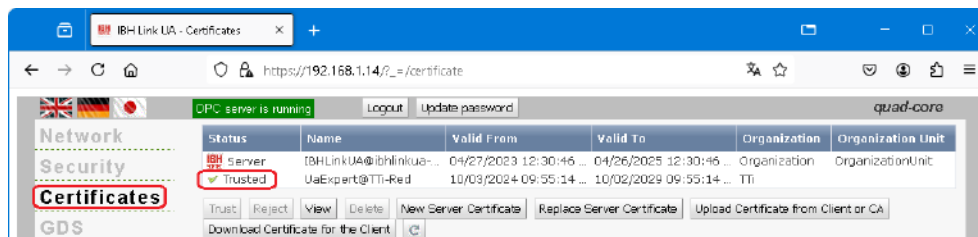
To display the contents of OPC Variables (OPC-Tags) and the corresponding OPC UA connecting information, the selected server **IBH Link UA@ibhlinkua-005668** must be connect. Mark the Server and click the **Connect Server** icon.

The connection to the name **IBHLinkUA@ibhlinkua-005668** OPC server cannot be established. An error message is displayed in the **UaExpert log**.

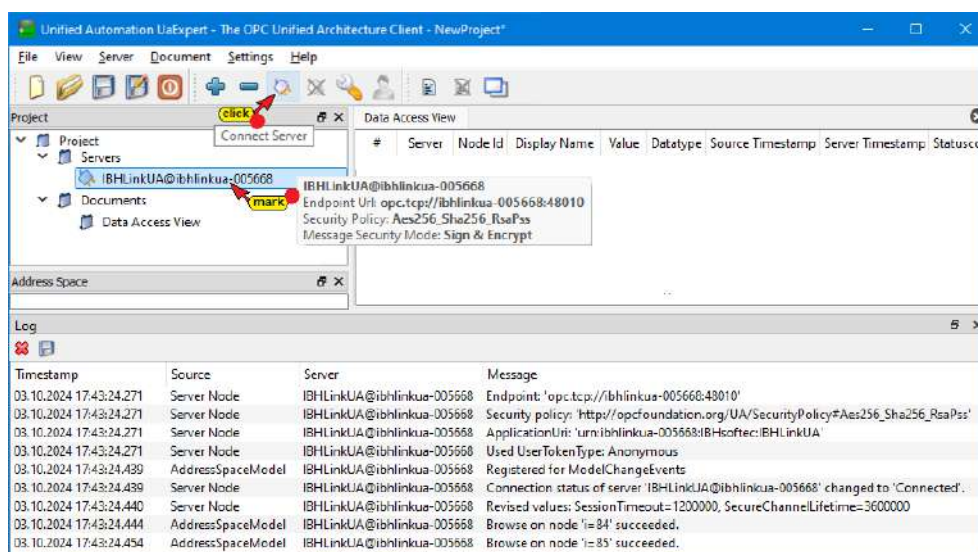
Trusting the IBH Link UA Certificate



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

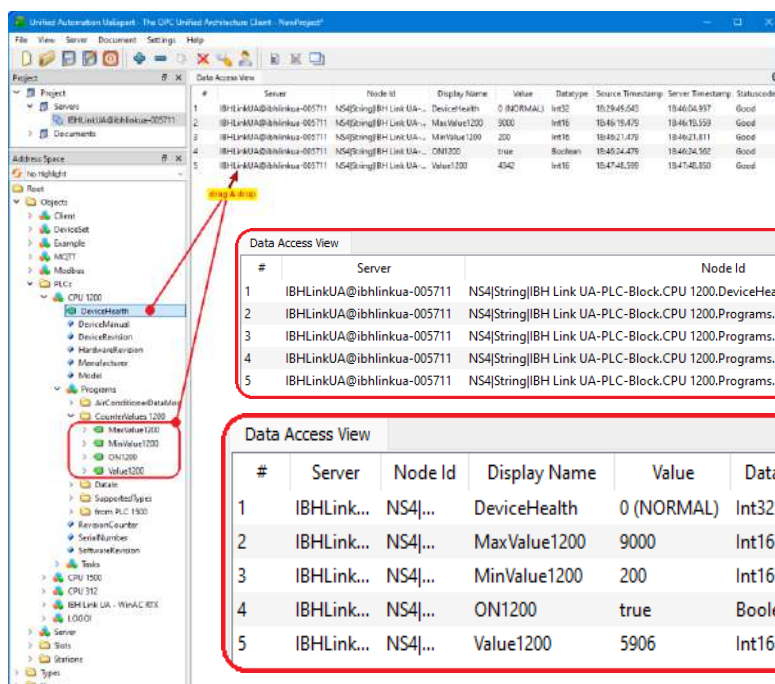


After trusting the certificate, with the UaExpert client, the validation of the certificate can take place.



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

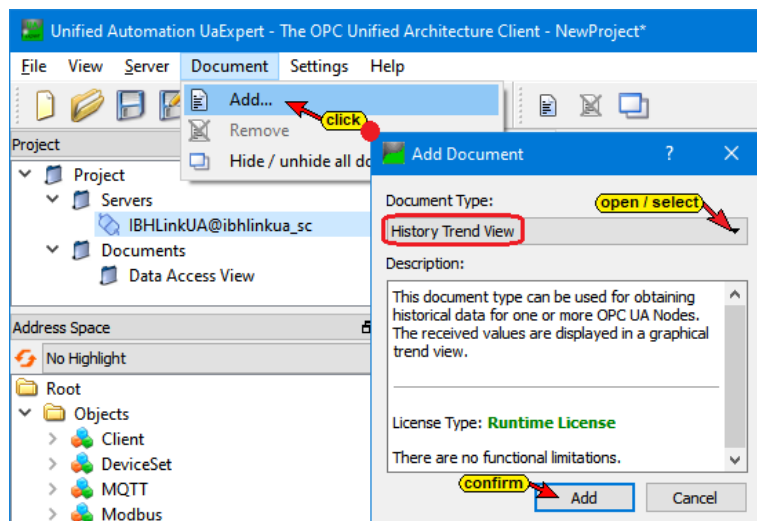
2.4 UaExpert window Data Access View



#	Server	Node Id	Display Name	Value	Datatype	Source Timestamp	Server Timestamp	Statuscode
1	IBHLinkUA@ibhlinkua-005711	NS4 String IBH Link UA-PLC-Block.CPU 1200.DeviceHealth	DeviceHealth	0 (NORMAL)	Int32	18:29:49.643	18:46:04.937	Good
2	IBHLinkUA@ibhlinkua-005711	NS4 String IBH Link UA-PLC-Block.CPU 1200.Programs.CounterValues 1200.MaxValue1200	MaxValue1200	9000	Int16	18:46:19.479	18:46:19.559	Good
3	IBHLinkUA@ibhlinkua-005711	NS4 String IBH Link UA-PLC-Block.CPU 1200.Programs.CounterValues 1200.MinValue1200	MinValue1200	200	Int16	18:46:21.479	18:46:21.811	Good
4	IBHLinkUA@ibhlinkua-005711	NS4 String IBH Link UA-PLC-Block.CPU 1200.Programs.CounterValues 1200.ON1200	ON1200	true	Boolean	18:46:24.479	18:46:24.562	Good
5	IBHLinkUA@ibhlinkua-005711	NS4 String IBH Link UA-PLC-Block.CPU 1200.Programs.CounterValues 1200.Value1200	Value1200	5240	Int16	18:47:48.399	18:47:48.800	Good

#	Server	Node Id	Display Name	Value	Datatype	Source Timestamp	Server Timestamp	Statuscode
1	IBHLink...	NS4 ...	DeviceHealth	0 (NORMAL)	Int32	18:29:49.643	18:46:04.937	Good
2	IBHLink...	NS4 ...	MaxValue1200	9000	Int16	18:46:19.479	18:46:19.559	Good
3	IBHLink...	NS4 ...	MinValue1200	200	Int16	18:46:21.479	18:46:21.811	Good
4	IBHLink...	NS4 ...	ON1200	true	Boolean	18:46:24.479	18:46:24.562	Good
5	IBHLink...	NS4 ...	Value1200	5906	Int16	19:01:42.958	19:01:43.208	Good

2.4.1 Historical data



Click in UaExpert Document / Add. In the opened dialog box, select History Trend View and confirm.

The historical data of values

