IBHsoftec

TTi
INGENIEURBÜRO FÜR
TECHNOLOGIETRANSFER
DIPL.-ING. B. P. SCHULZ-HEISE

IBH Link IoT

Manual

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

Contents

PLC Examples-Projects (PLC-Programs)

PLC control	IP address *Control level*	Programming system
CPU 416 S7e	10.0.13.11	**STEP 7 Simatic Manager**
CPU 312 S7e	**S7++1** / 10.0.13.25	
PLC 1500 TIA16e	10.0.13.90	**TIA Portal V16**
PLC 1200 TIA16e	10.0.13.91	
CPU 312 TIA16e	**S7++2** / 10.0.13.26	
CPU 416 TIA16e	10.0.13.9	
S5 CPU 103U Counter S5W.S5P	**S5++1** / 10.0.13.27	***S5 for Windows***

1 IBH Link IoT setup

1.1 Installation and connection

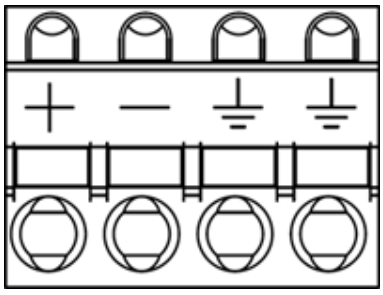
The IBH Link IoT is designed for DIN rail mounting:

The IBH Link IoT 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 IoT. A higher supply voltage may destroy the device.



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

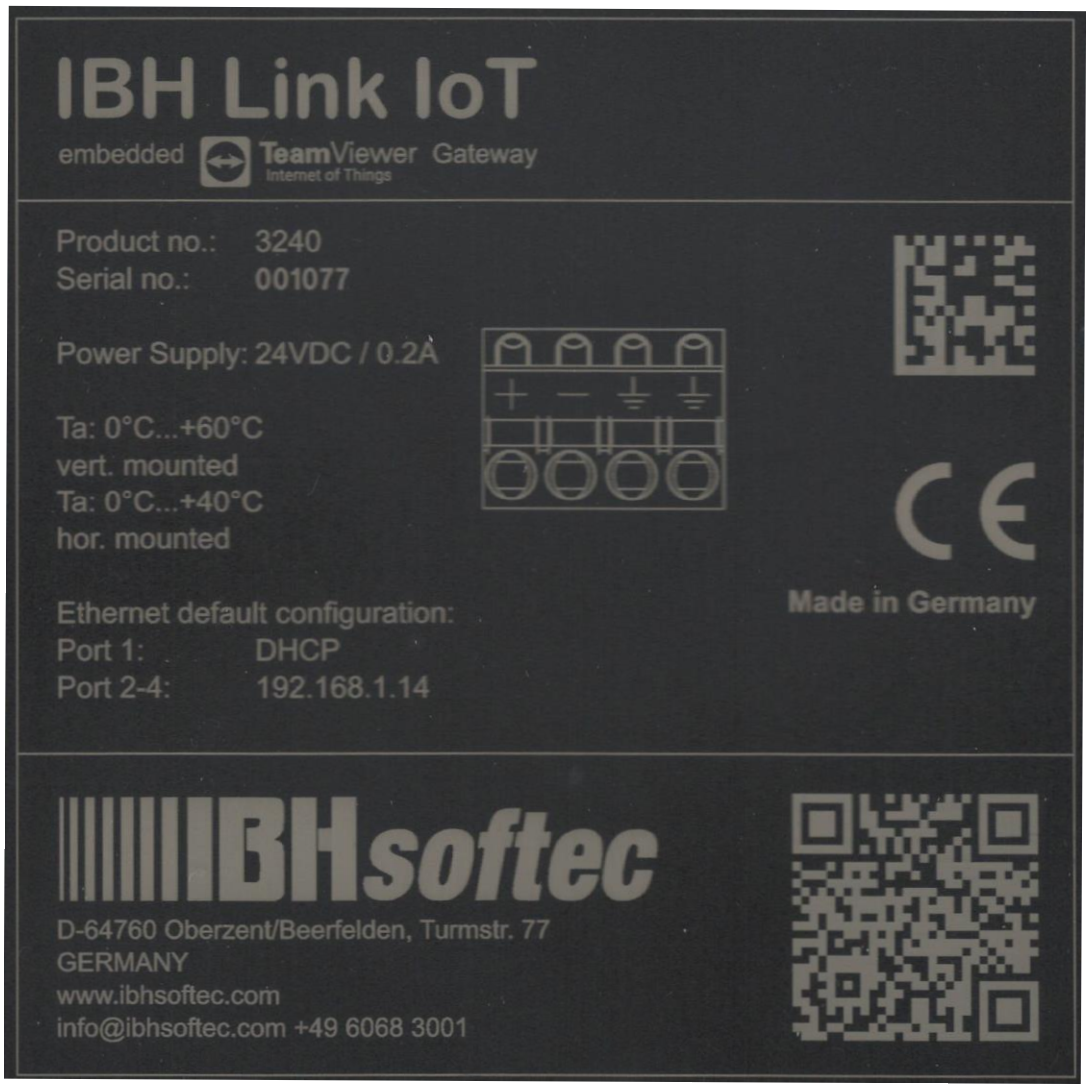
1.2 Configuration of the IP addresses (default setting)

With the IBH Link IoT default factory setting the configuration can be done with an up-to-date web browser. The Ethernet ports 2 to 4 have the IP address 192.168.1.14.

The Ethernet port 1 can only be used to configure the ***IBH Link IoT*** if a ***DHCP server*** assigns the IP address, and a DNS server resolves the name by specifying the hostname
http://**ibhlink-iot_<serial number>**
(Example: http://**ibhlink-iot_001077**)

No additional applications or drivers are required.

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

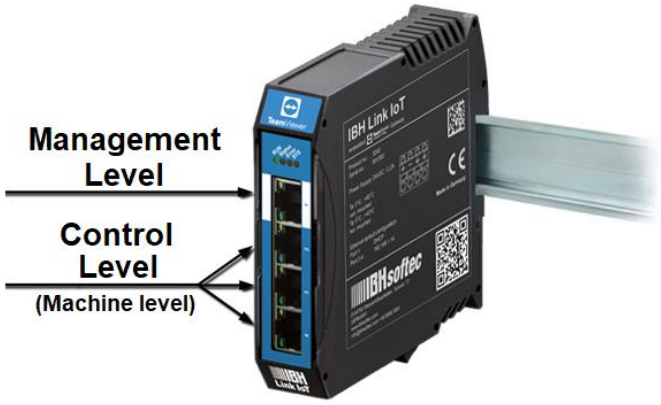


Default logon data

Username: admin
Password: admin

Standard IP-Address configuration:

Level	Port	Address
Management Level	Port 1	Hostname: **ibhlink-iot_<serial number>**
Control Level	Port 2 - 4	**192.168.1.14**

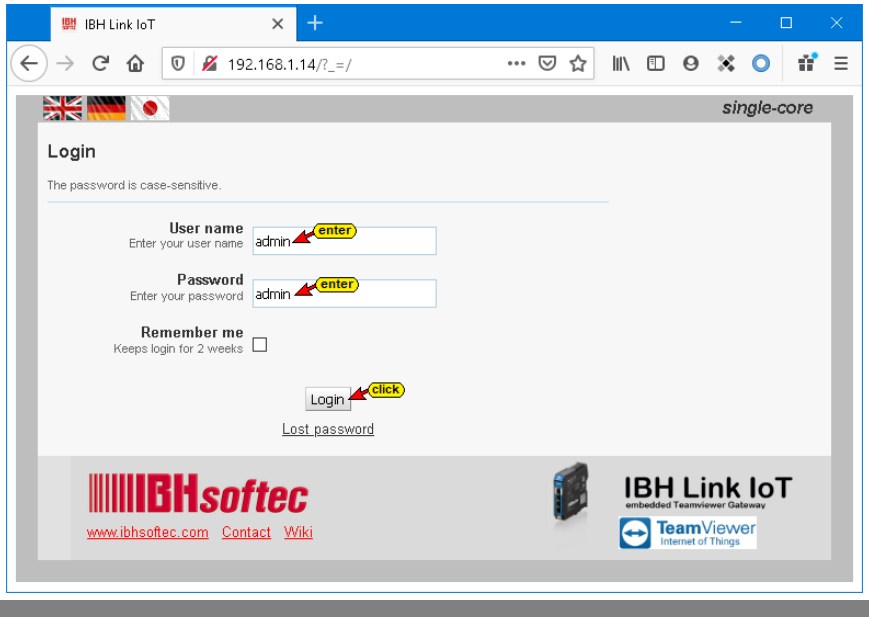


Note:

With the IBH Link IoT default factory setting the configuration can be made using an Internet browser (Microsoft Edge, FireFox, Internet Explorer, etc.):

- 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 control level. The connected network must have the sub-address 192.168.1.nn.
  Or the connected PC a has a fixed IP address from the subnet 192.168.1.nn

1.3 Login browser window



Language selection

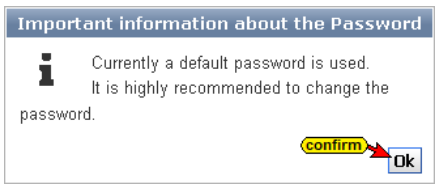
The languages English, German and Japanese are available in the browser window.

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.

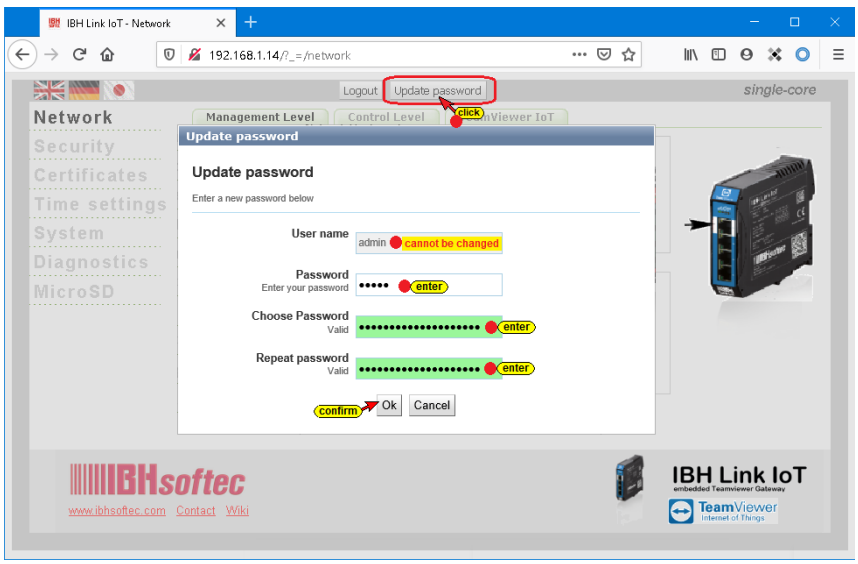


After the security messages have been confirmed, we recommend changing the password.

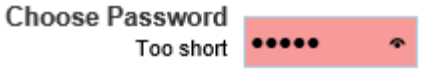
Change Password

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

In the open browser window ***Management level / control level*** klick 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.

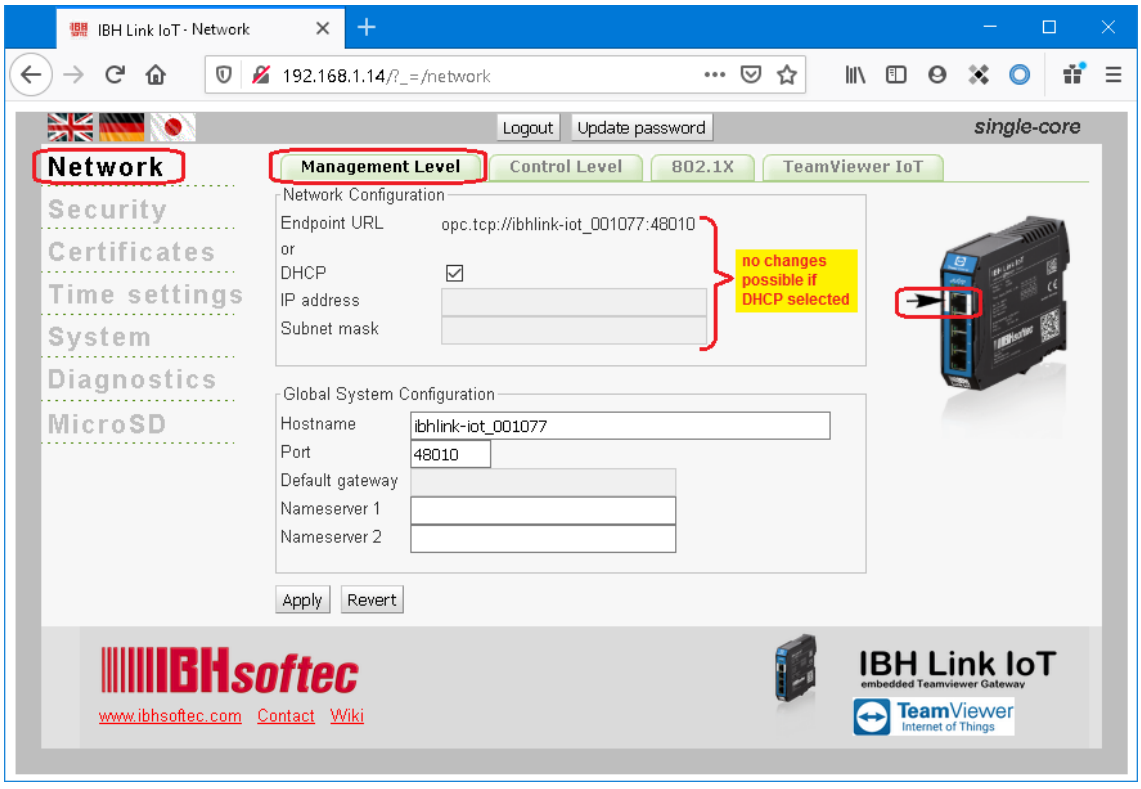
1.4 Network browser window

Note:

The management level (port 1) must have a different subnet address than the subnet address of the control level (port 2 to port 4) so that it is unequivocally which connection must be established via which Ethernet interface.

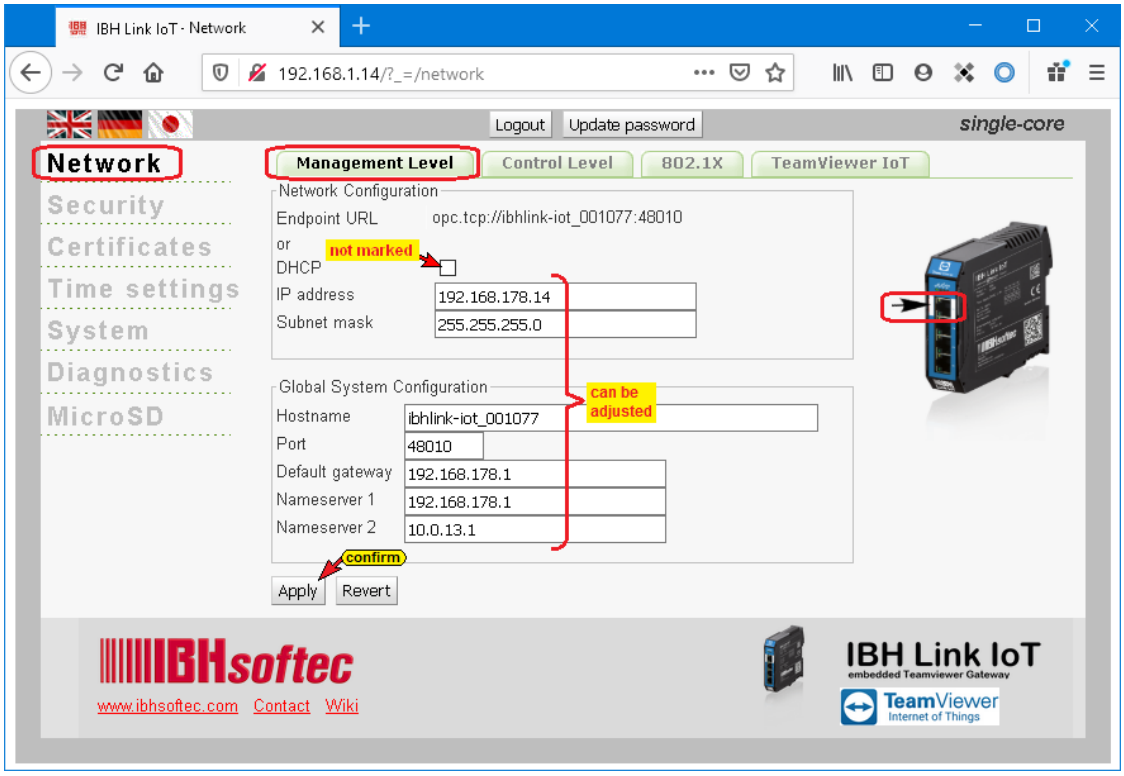
1.4.1 Management Level Settings

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.

1.4.2 Setting the IP address - management level



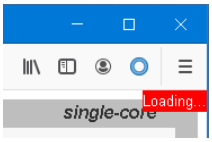
By clicking the ***Apply*** button, the changed settings of the management level are applied to the ***IBH Link IoT***. Since the IBH Link IoT web browser was accessed via the IP address of the control level, the changes are displayed immediately after they have been accepted. It is not necessary to reopen the ***IBH Link IoT*** web browser.

The screen shot shows the settings of the management level for access from an external PC.

1.4.3 Control Level Settings

The network configuration for ports 2 to 4 (control level) and global system settings can be adjusted. If DHCP is deactivated, the network configuration and global system settings can be changed. The host name can always be changed.

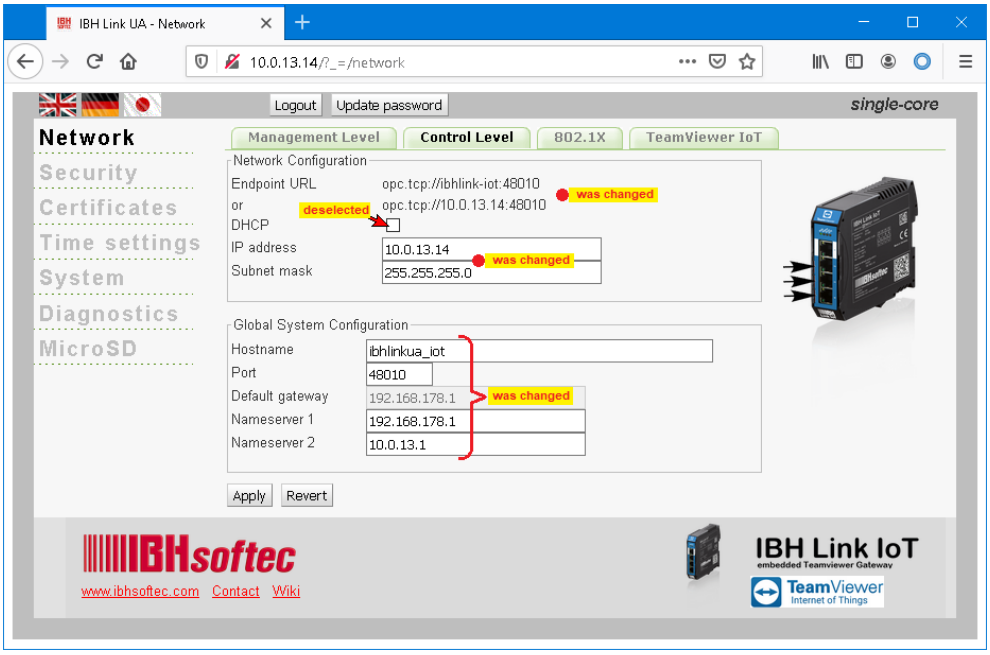
By clicking the ***Apply*** button, the changed settings of the control level are applied to the IBH Link IoT. The execution of the change is displayed.



Since the web browser of the ***IBH Link IoT*** was accessed via 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.

Control level with adapted IP addresses

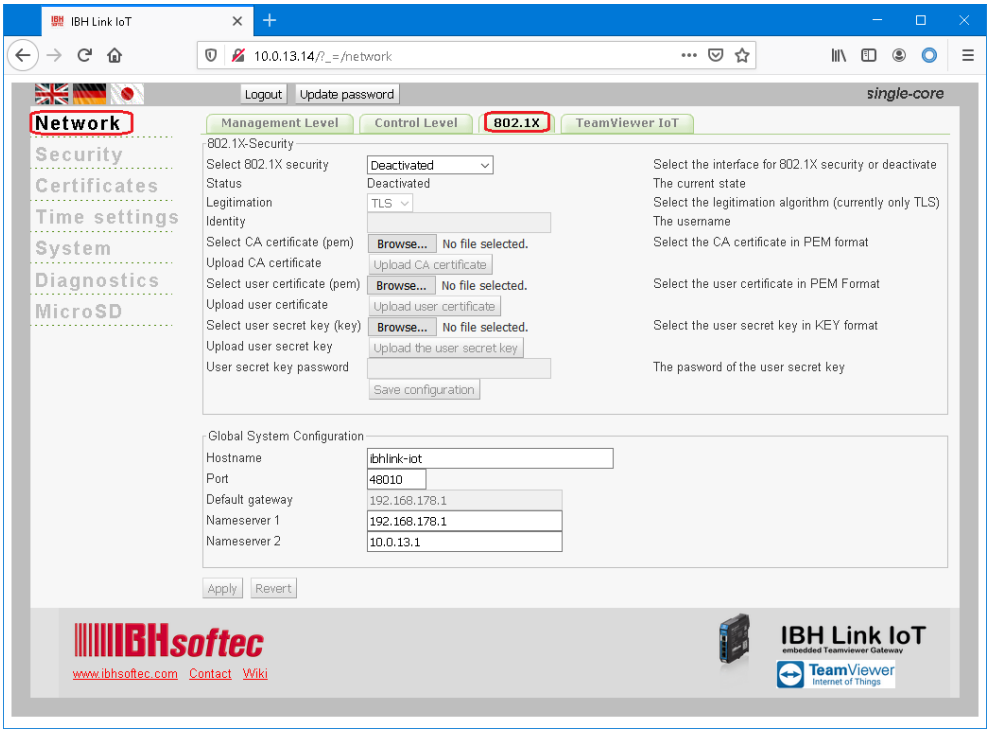
The ***IBH Link IoT*** browser window was accessed via the IP address specified at the control level. After logging in, the control level browser window is displayed with the changed addresses.



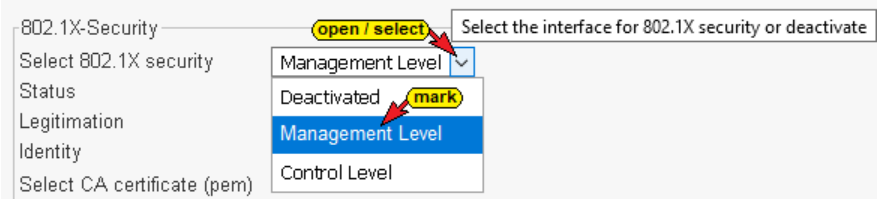
The screen shot shows the settings of the control level for access from an external PC.

1.4.4 802.1x settings

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.

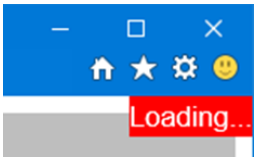


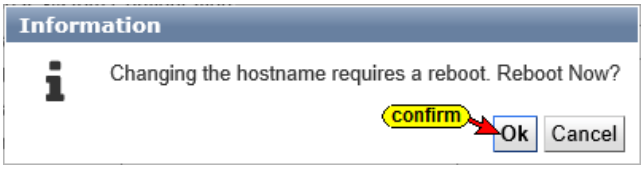
The configuration of the IEEE 802.1X security settings can be saved.

1.4.5 Apply network adjustments

Click the ***Apply*** button to save the adjustments done in the ***Management level*** tab, ***Control level*** tab, ***802.1X*** tab, or ***TeamViewer IoT*** tab. The ***Apply*** button should be clicked for each tab separately. Confirm the displayed note to adopt the changes.

The transfer of the adjusted settings is displayed in the upper right corner of the browser window. Since the changes require a restart of the IBH Link IoT, a corresponding information is displayed.



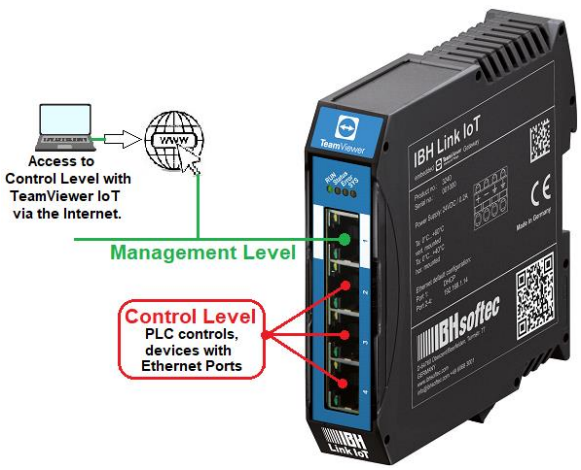


1.5 TeamViewer IoT activation

The ***TeamViewer software*** is pre-installed in the ***IBH Link IoT***. This offers the possibility of being able to access almost all devices (PLCs) connected at the ***Control level*** of the ***IBH Link IoT*** anytime and anywhere.

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

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

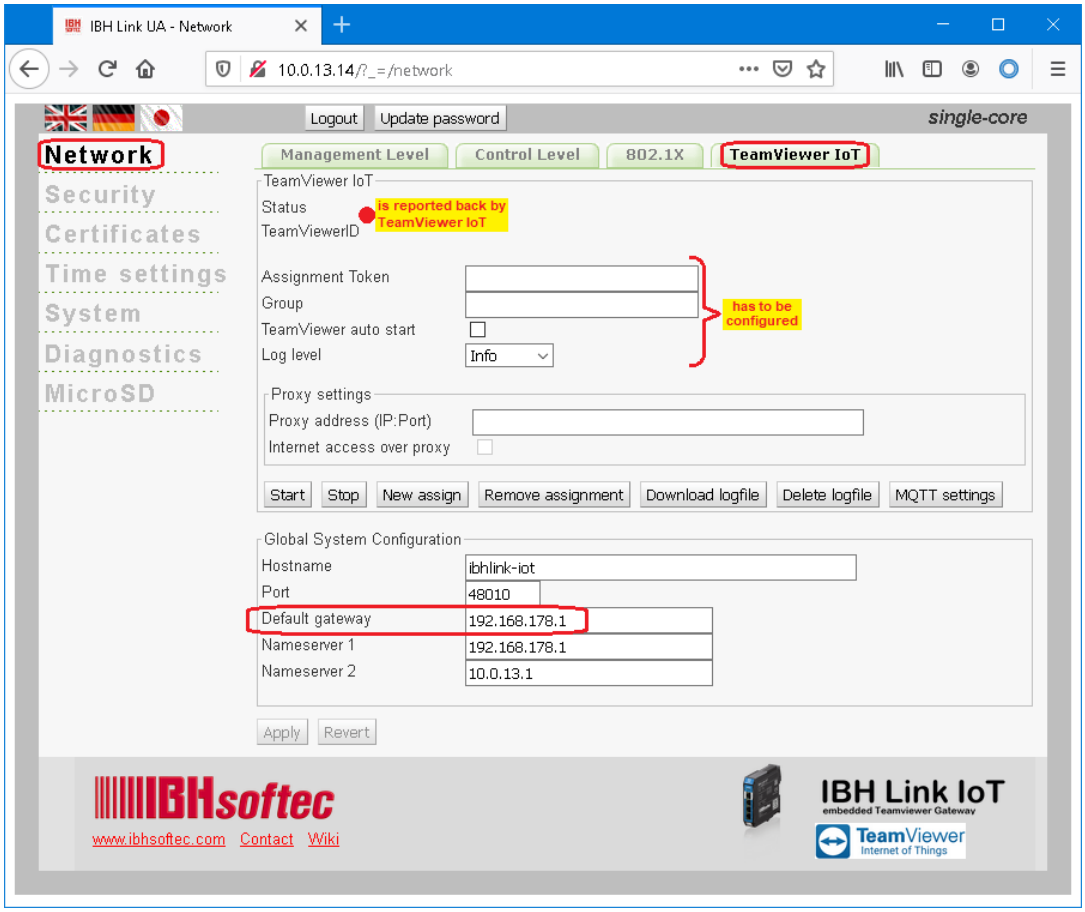


The ***IBH Link IoT*** manages two subnet addresses separated by a firewall, each with its own ***MAC address***.

Ethernet areas:

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

Team Viewer IoT tab

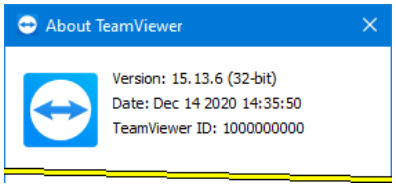


If the Internet must be accessed via a proxy, the address can be entered in the form ***Proxy: Port*** or ***User: Password @ Proxy: Port***. The proxy access to the Internet must be activated.

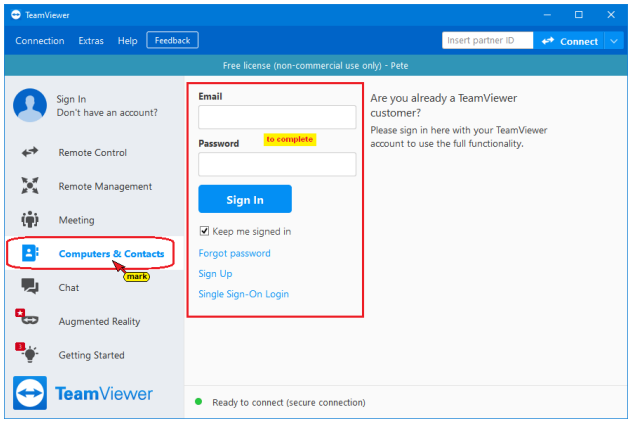
PC preparations – connected to the Ethernet port of the Management Level

To use the access options of the pre-installed TeamViewer IoT software, the following conditions must be met:

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 IoT.



A ***TeamViewer account*** with a corresponding ***license*** must be ready for activation.



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

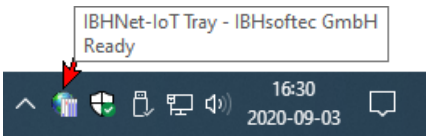
It is important that the latest software version of the ***IBHNet-IoT Agent*** is always installed.

Install IBHNet-IoT software

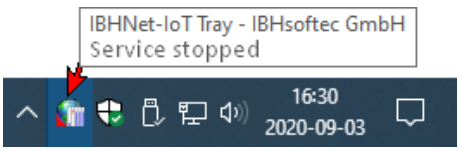
Double-click the ***IBHNet-IoT*** icon created during installation. The ***ibhsoftec-agent-service*** is started.

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.

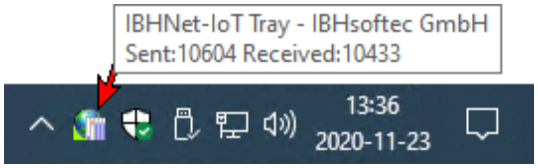
Pointing to the icon, displays the readiness of the service.



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

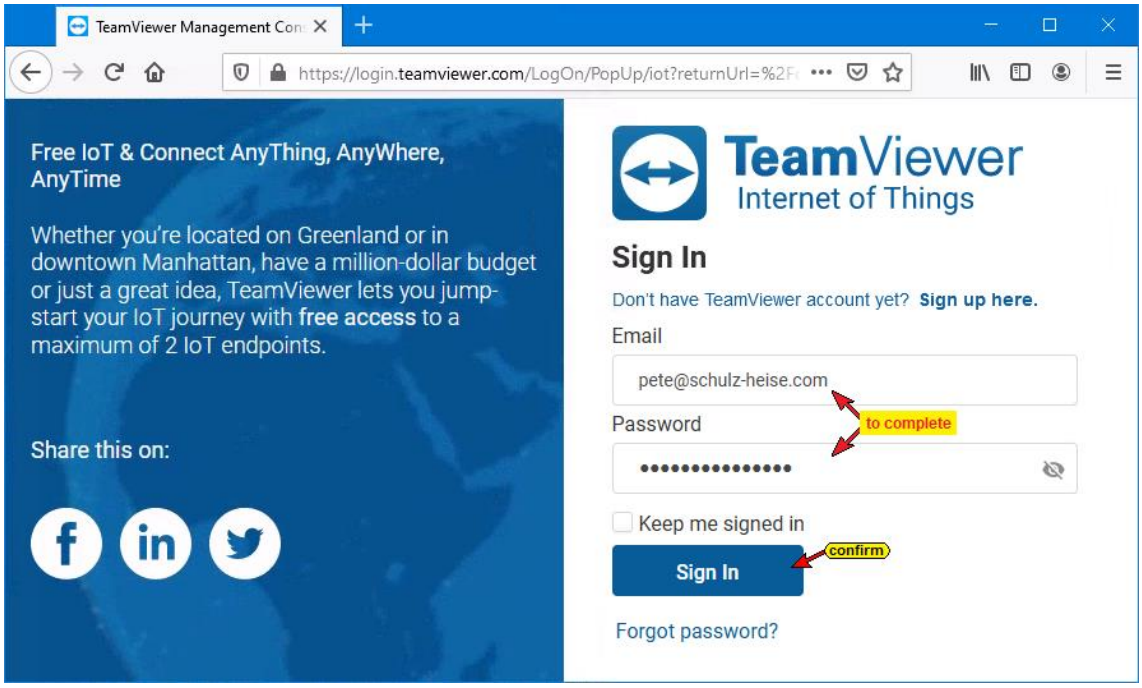


Once the connection has been established, the IBHNet-IoT tray symbol has a green corner at the bottom left and transmission data is displayed

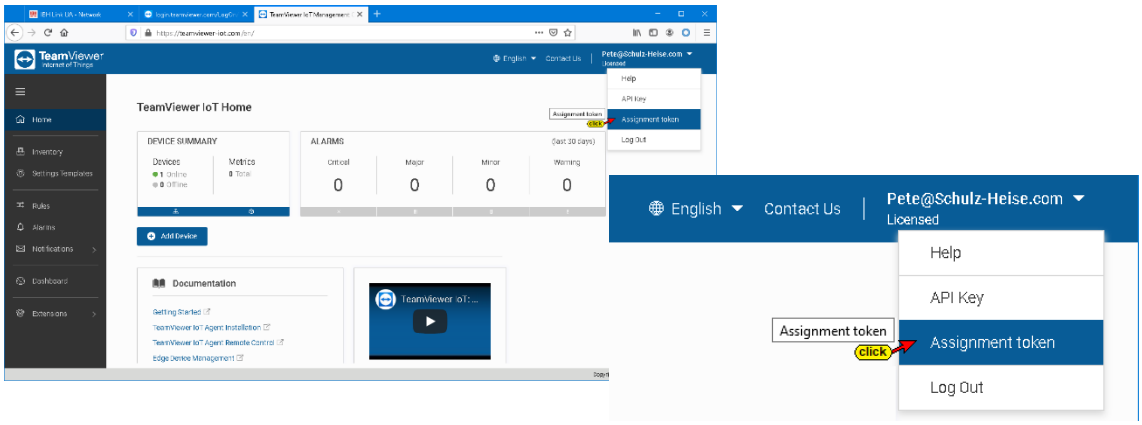


1.5.1 Opening the TeamViewer IoT Management Console

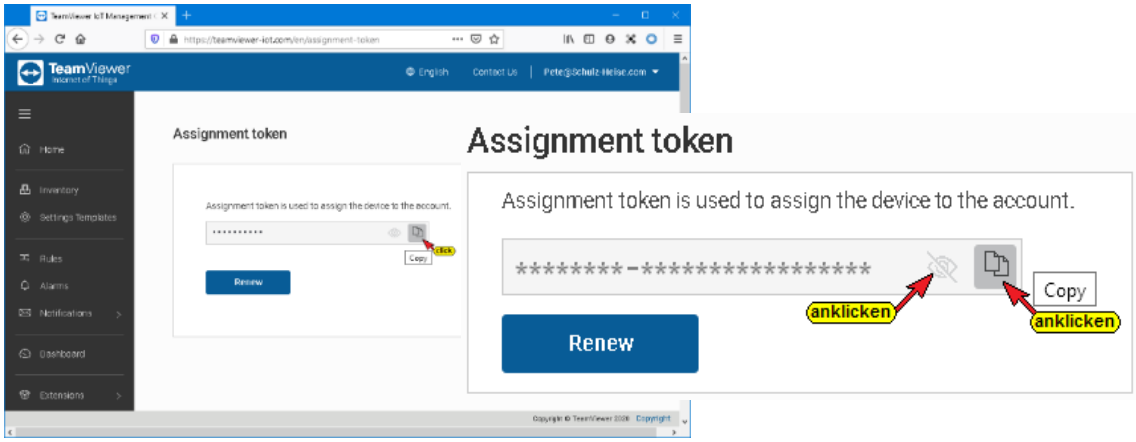
Use the link https://teamviewer-iot.com/en/ to open the TeamViewer Internet of Things login page and log in.



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



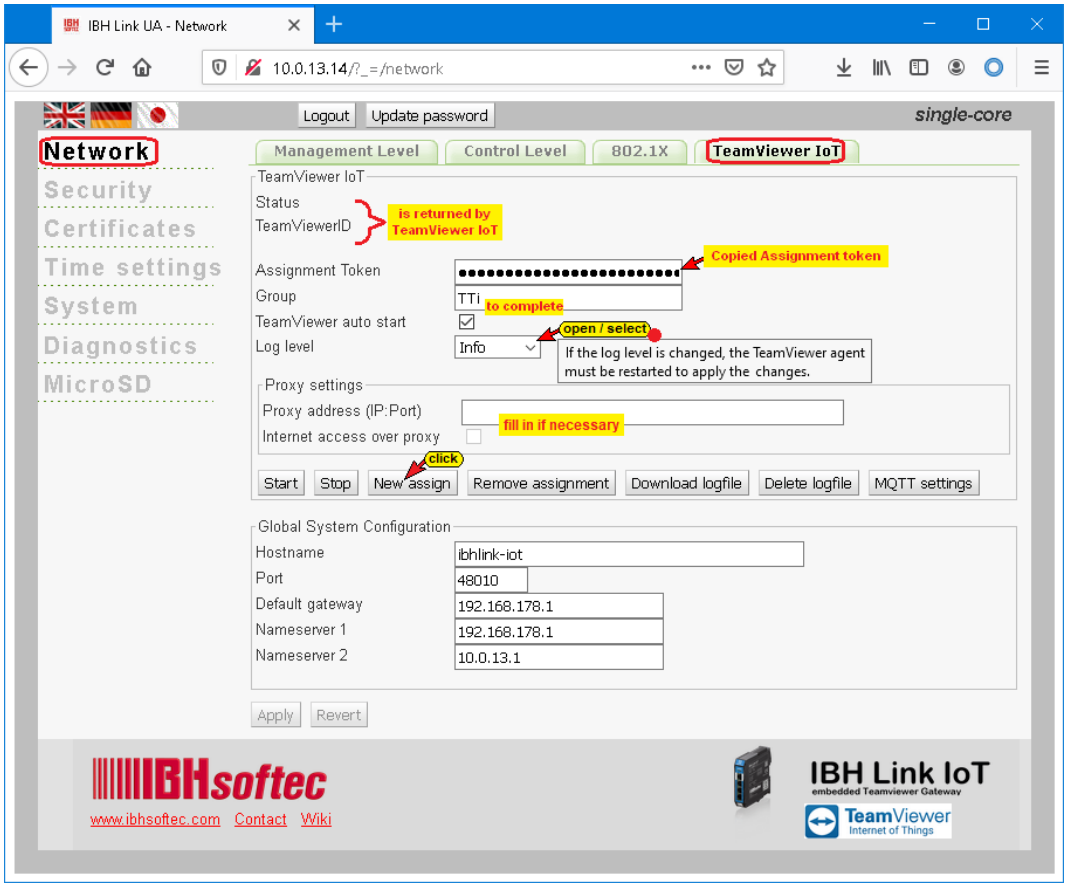
Assignment token dialog box



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

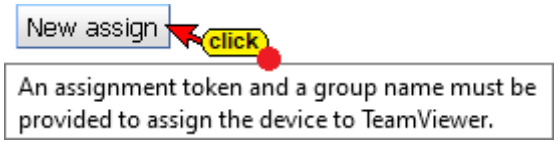
Insert assignment token

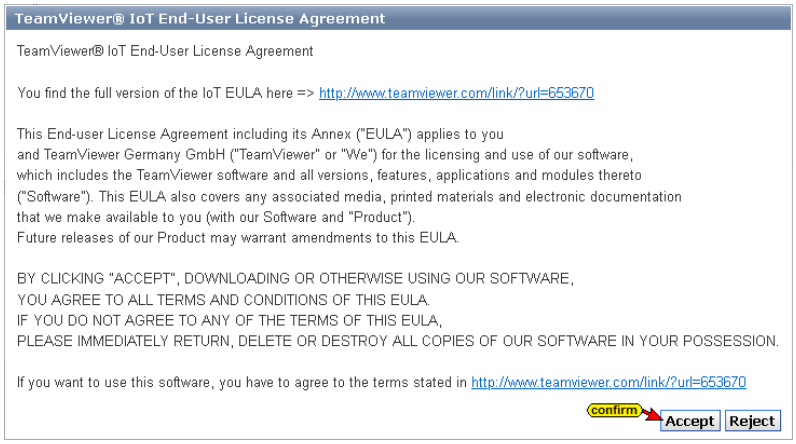
The ***Assignment token*** must be copied into the field with the same name in the ***IBH Link IoT*** browser window Network/TeamViewer IoT.



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***.

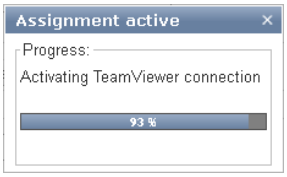
Note!

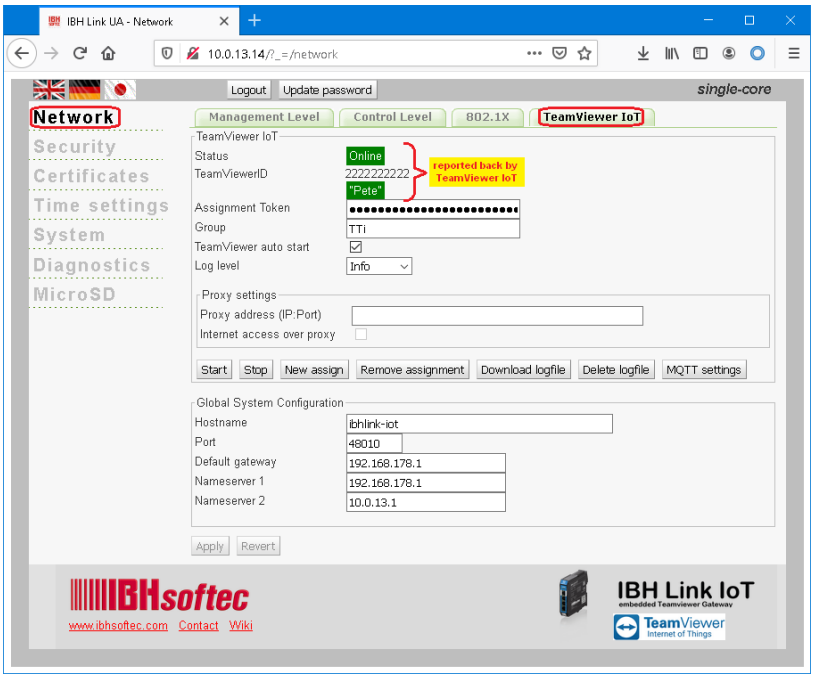
The transmission of the ***Assignment token*** to ***TeamViewer*** can take some time.

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

Assignment token taken from TeamViewer IoT

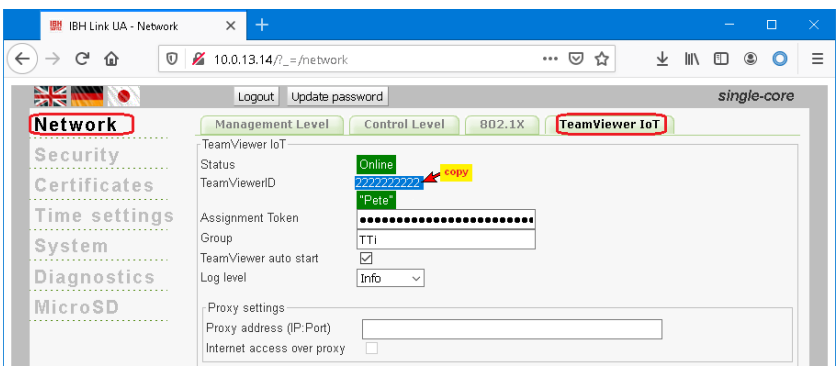
If the assignment token has been accepted, the status and the ***TimeViewerID*** with the name are displayed in the web browser window ***Network/TeamViewer IoT***.



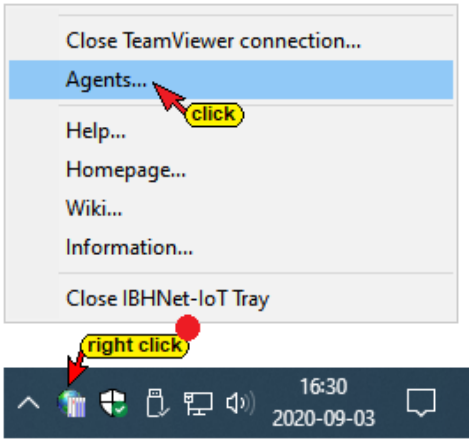


Copy the TeamViewer ID

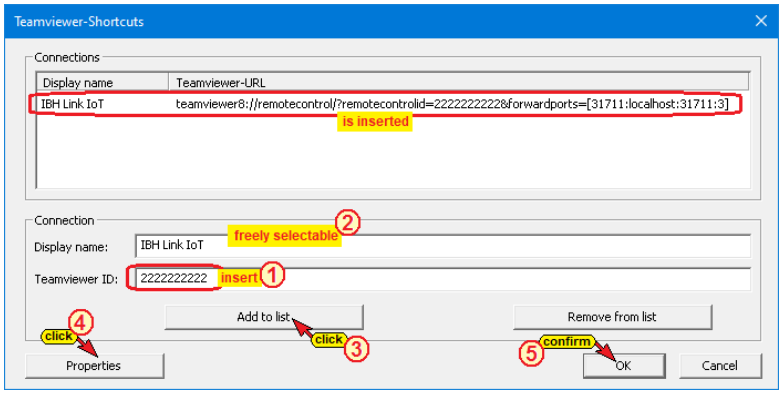
Copy the ***TeamViewer ID number*** to the Windows clipboard.



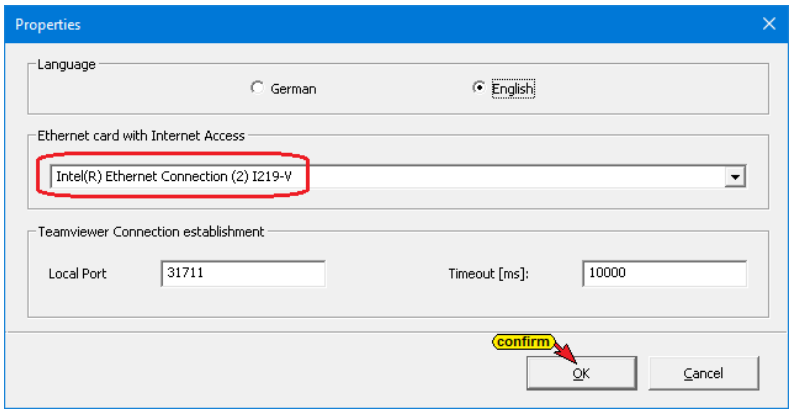
Right-click on the ***IBHNet-IoT Tray*** icon to open the context menu. The ***Agents…*** command opens the ***TeamViewer Shortcuts*** dialog box.



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 IoT*** via the Internet.



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

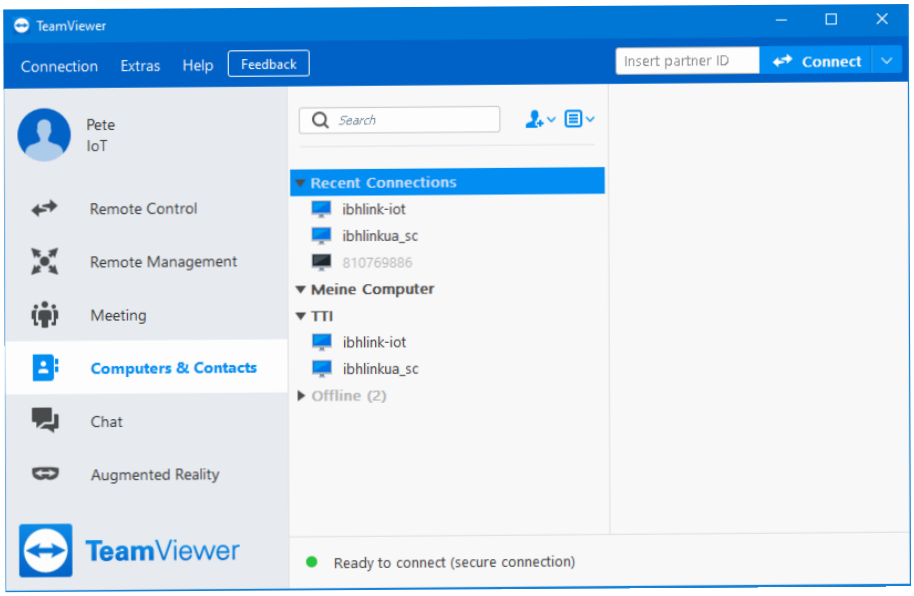
1.5.2 Establishing a connection

A connection to the ***IBH Link IoT*** and thus to the PLC controls and other devices that are connected to the ports of the control level can be established via the Internet from any PC.

The ***IBHNet-IoT software*** must be installed on this PC.

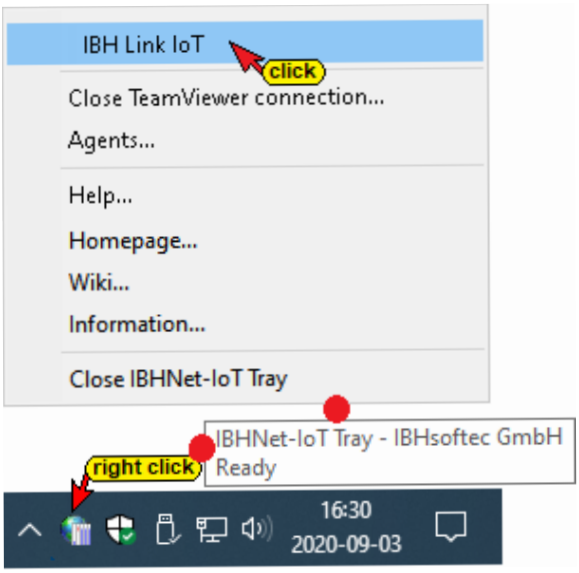
TeamViewer must be started, and you have logged into the ***TeamViewer account***.

Registered TeamViewer IoT account.

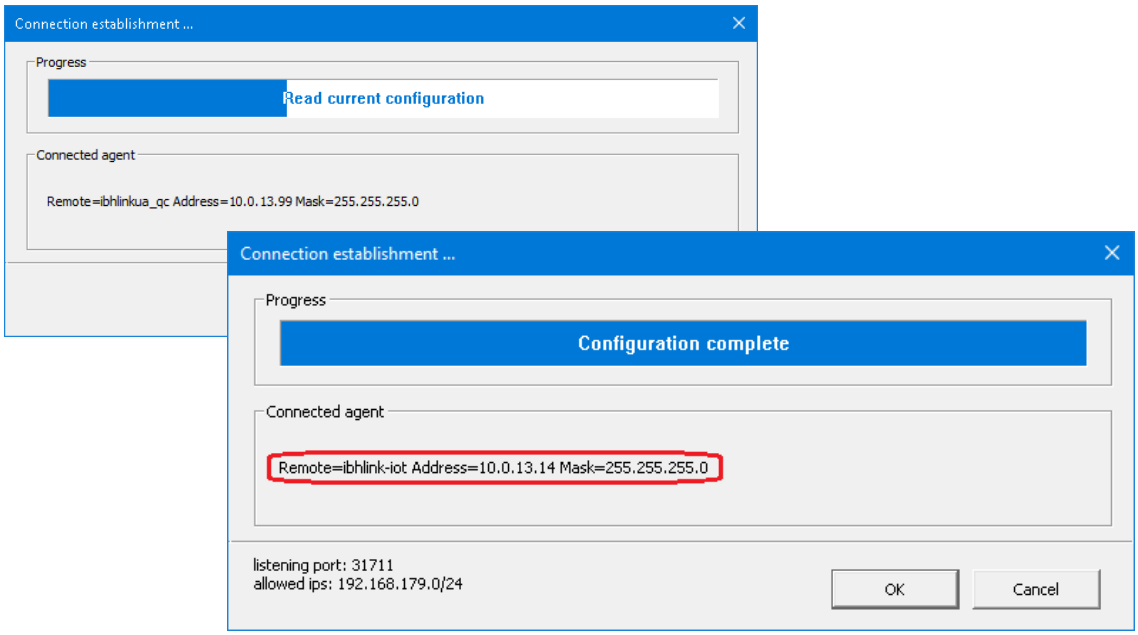


Right-click on the ***IBHNet-IoT Tray*** icon to open the context menu. The devices registered with the ***TeamViewer account*** are listed in the upper area of the context menu.

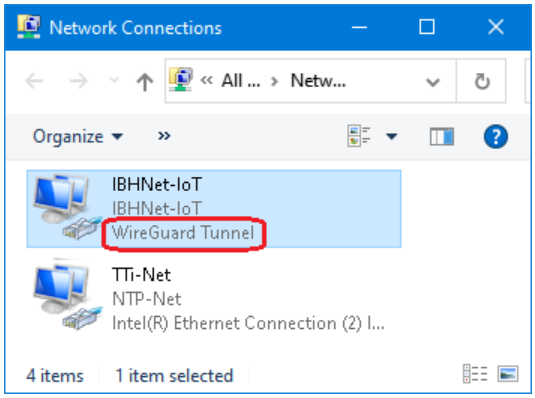
The connection is established with a click on the desired device (IBH Link IoT).



The establishment of the connection is displayed.



After the connection has been successfully established, the ***IBH Link IoT*** appears as a ***WireGuard Tunnel*** under the network adapters of the PC.



Note!

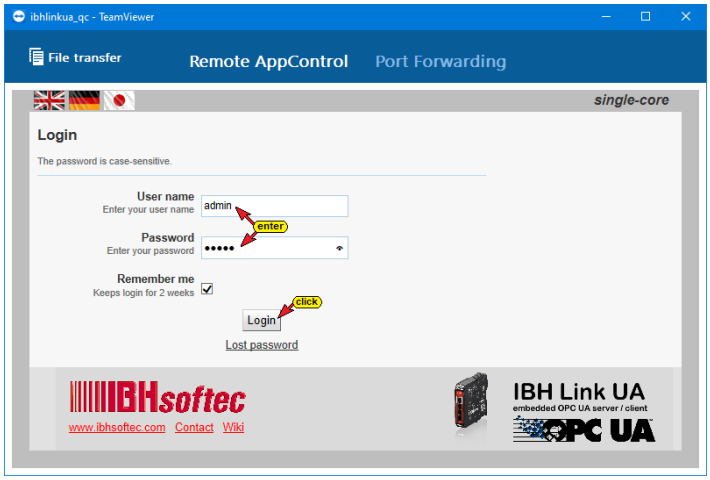
Windows use two names for network adapters, the ***Name*** given by the ***Hardware*** or the ***FriendlyName***.

- **WireGuard Tunnel**
- **Wintun Userspace Tunnel**

The different names are therefore displayed in the screenshots.

From now on, all controls and devices that are connected via the ***Control Level*** of the ***IBH Link IoT*** can be reached.

Error messages starting process

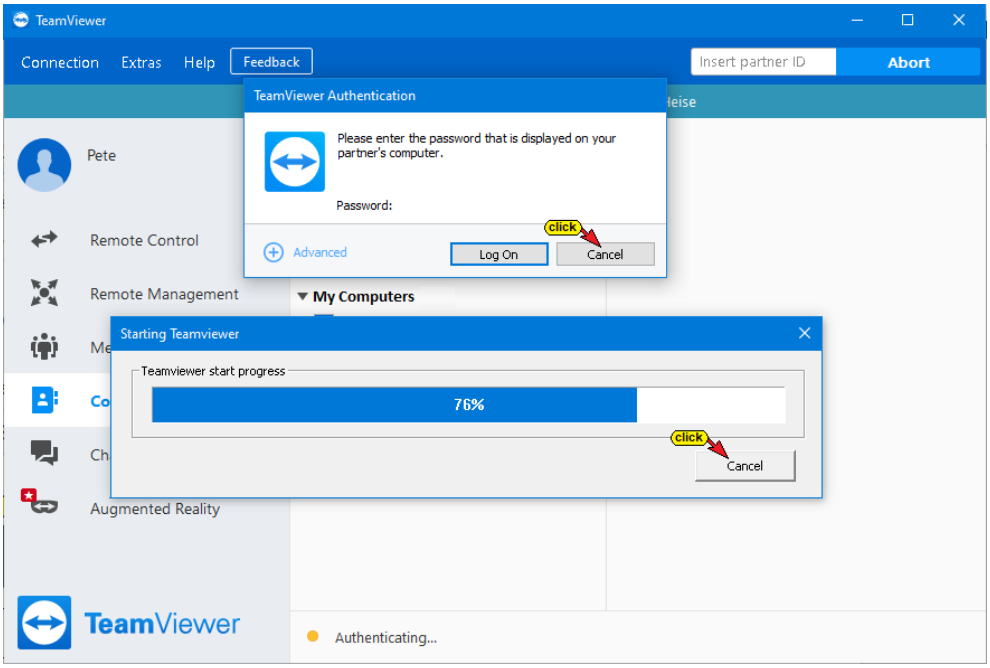


Error messages starting the process

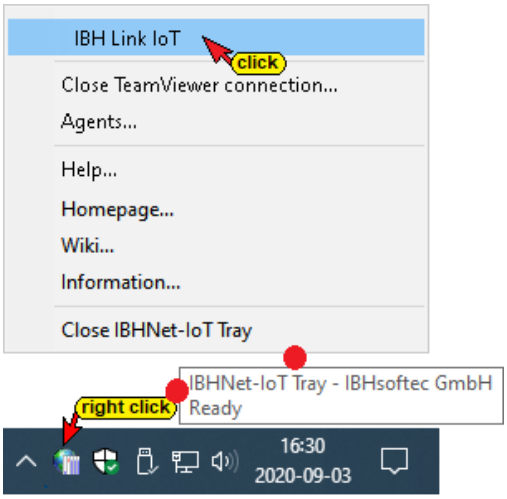
Note!

During the ***TeamViewer*** start process it may happen that no connection is established, and the error messages are displayed. These error messages are to close with ***Cancel***.

The starting process must be started again.

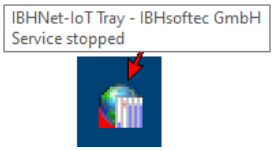


Activate the start process again



After the connection has been successfully established, the ***IBHNet-IoT Tray*** icon in the taskbar changes. It gets an additional green mark.

From the PC, whose ***IBHNet-IoT Tray*** Icon shows the existing online connection, controls (CPUs / devices) connected to the ***Control level***

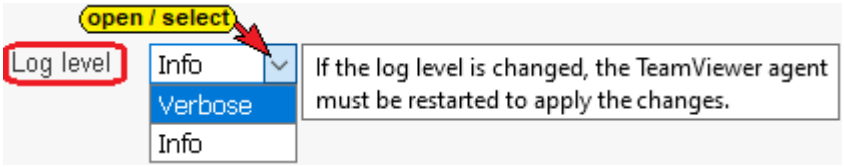


ports can be accessed with the appropriate software (programming system).

If the online connection to the IBH Link IoT cannot be established because a required service has been stopped, this will be displayed.

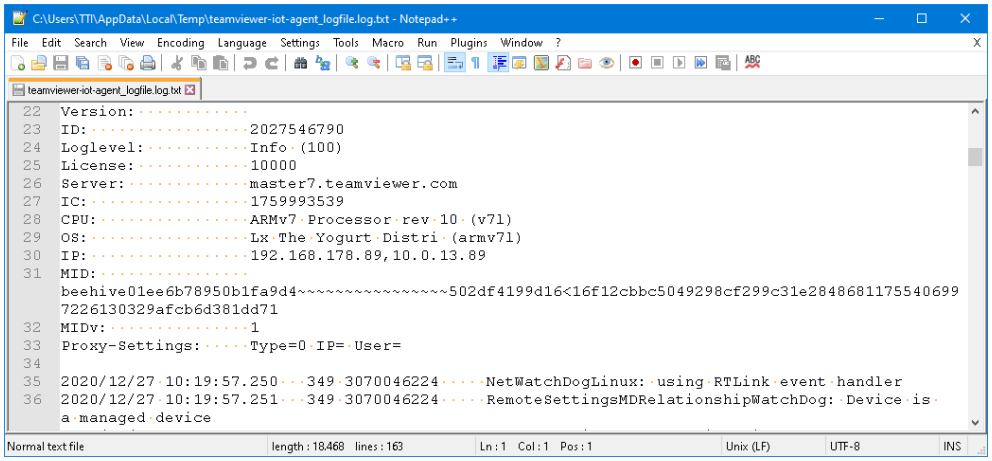
1.5.3 TeamViewer IoT – Logfile

The ***log output*** can be adjusted.



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.

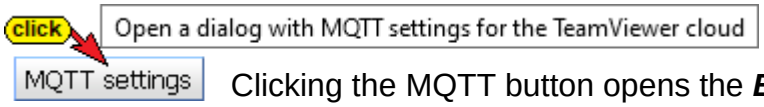


Since the evaluation of the log-file requires some specialist knowledge, this diagnosis should be carried out in the event of a malfunction using the IBHsoftec hotline.

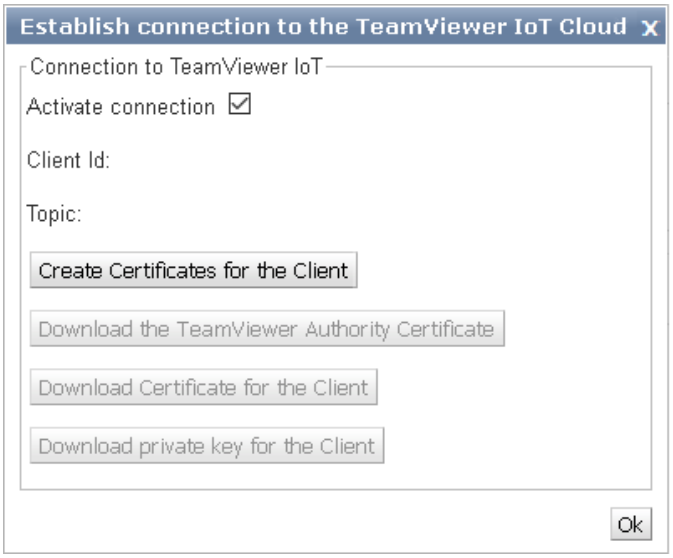
To have a defined beginning of the log file, the stored file can be deleted.

1.5.4 Teamviewer IoT – MQTT settings

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



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.

1.6 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.

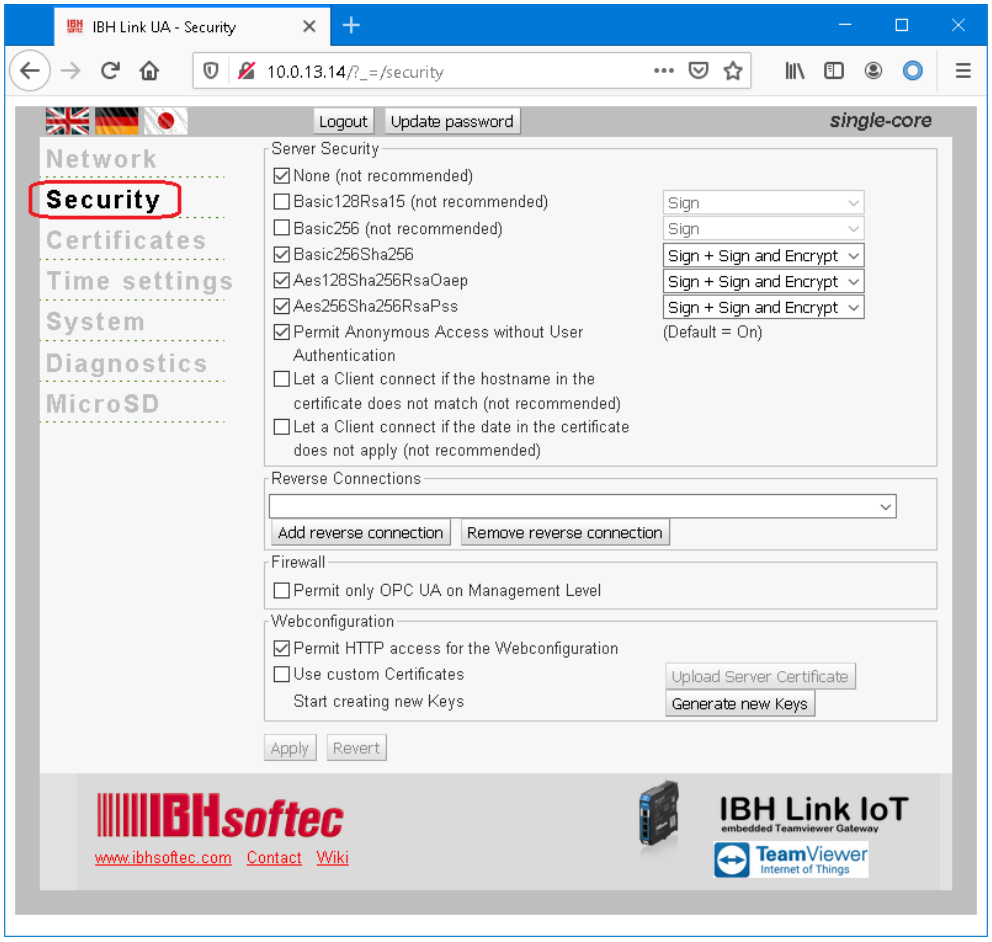
To use this functionality with **IBH Link UA**, you need a **TeamViewer IoT** license.

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

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

1.7 Security browser window

The connection security between a client and a server is available for selection in this window and can be specified.



Note:

After changes made in the security browser window, the buttons Apply and Revert are activated.

If the change is to be adopted, click the ***Apply*** button.

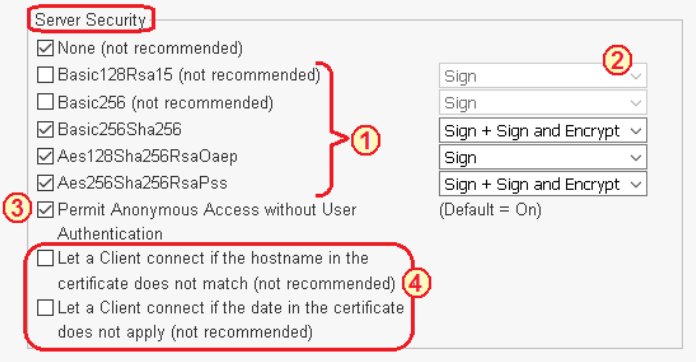
The client queries the server's security configuration via SecureChannel to then set up a communication channel in which the security (confidentiality) and the completeness (integrity) of the messages exchanged are guaranteed.

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.

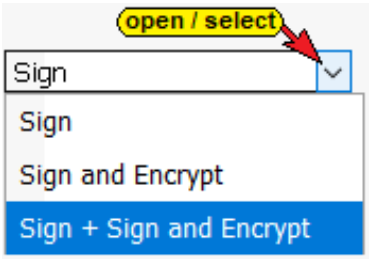
Server Security

There are different levels of encryption.



1 Is the security level for the 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 client. 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 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.

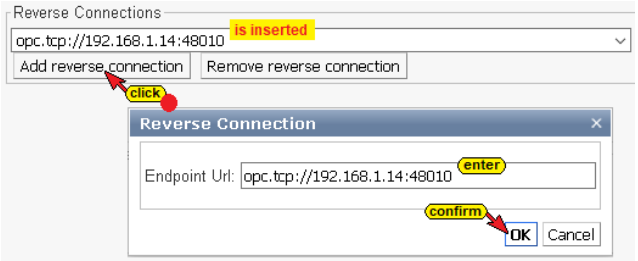
4 Settings can be made to allow client / server connections for security reasons not recommend.

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

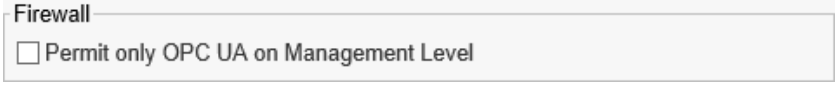
Reverse Connection

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, enter the

endpoint URL of the client. This makes it easier to configure the firewall. Of course, the client must support incoming server connections.



Firewall



The firewall can be instructed to allow OPC UA connections on the management level only. With a web browser it is no longer possible to address / configure the ***IBH Link IoT*** via the management level (Ethernet port 1).

Web Configuration

1 For security reasons, the configuration should only be accessed using the secure transport encryption ***(HyperText Transfer Protocol Secure - HTTPS)***.

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

2 All IBH Link IoT have 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 certificates*** is selected, a dialog box is opened via the ***Upload Server Certificate*** button. Buttons are available 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.

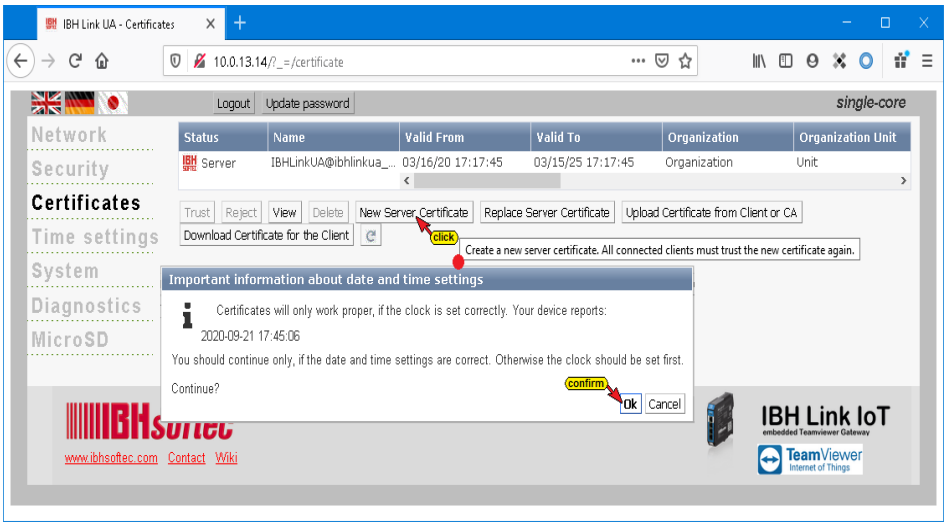
Note:

The generation of a parameter set for negotiating keys for encryption may take several hours.

1.8 Certificates browser window

Note:

All settings that can be made in the ***Certificates browser window*** are intended for future firmware upgrades and are currently of no significance.



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

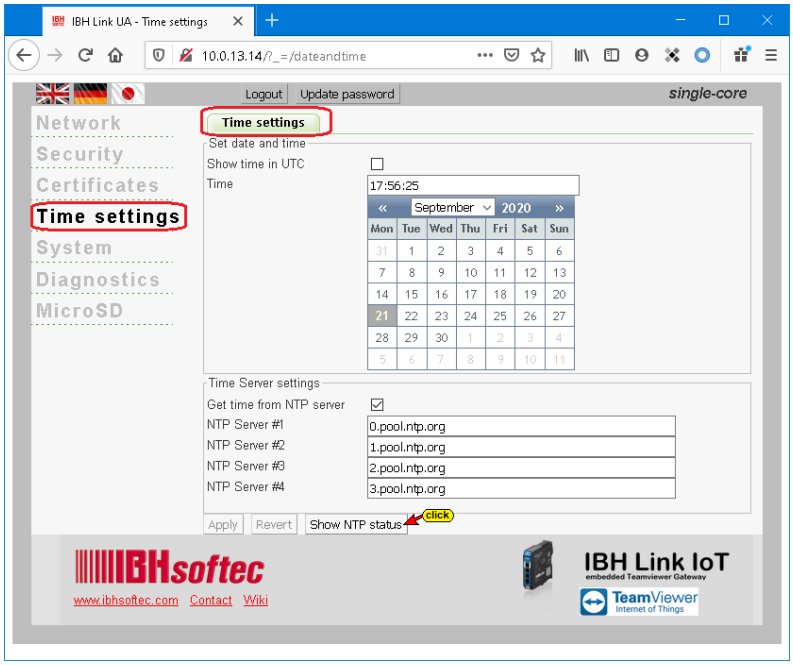
The existing certificates with data and status are displayed in the window. Buttons are provided to trust, block or delete listed certificates.

1.9 Time settings browser window

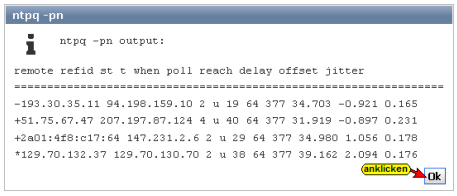
The date and time can be entered manually or automatically via the time server.

Note:

If a change has be made in the Time settings browser window the Apply and Revert buttons are activated.
If the change is to be adopted, click the Apply button.

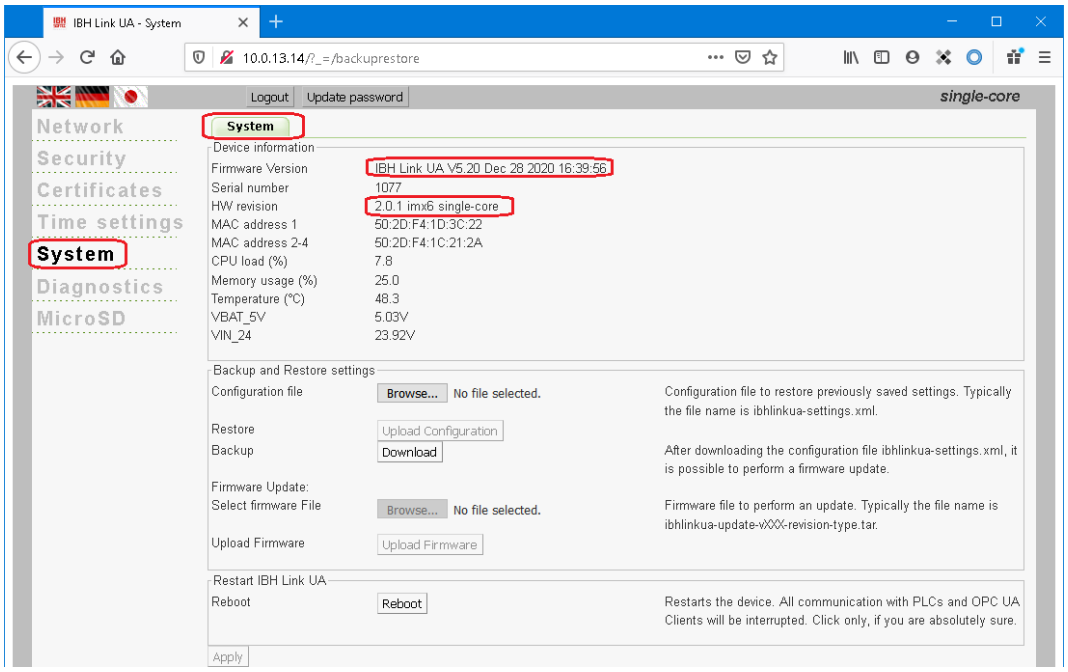


Clicking on ***NTP status*** displays the status of the transmitting time servers with their IP address. Four (4) ***Time Servers*** are already specified.

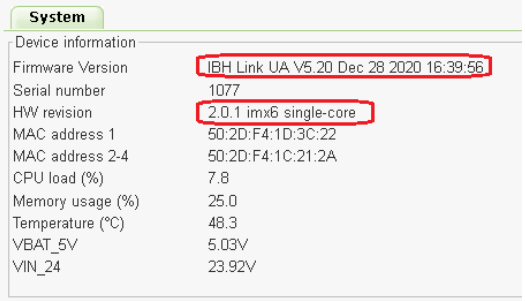


1.10 System browser window

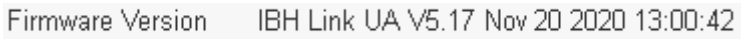
The system browser window lists information about the ***IBH Link IoT***.



1.10.1 Device information

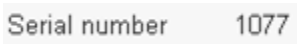


Firmware version



The version number is important for the firmware update. Only a firmware update with a higher version number should be carried out.

Serial number



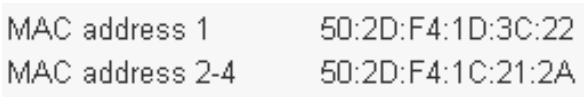
The serial number gives the IBHsoftec hotline information about the series and the age of the device.

HW revision

The HW revision specifies with which firmware version (HW2 SC or HW2 QC) an update can be carried out (see page 1 - 22).

MAC addresses

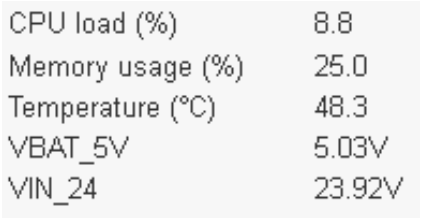
The IBH Link IoT has two separate MAC addresses.



One MAC address for the management level and another MAC address for the three ports of the control level.

Hardware information

The current CPU load (%), Memory usage (%) and Temperature (°C) as well as an internal voltage (VBAT_5V) and the supply voltage (VIN_24) of the device are displayed.

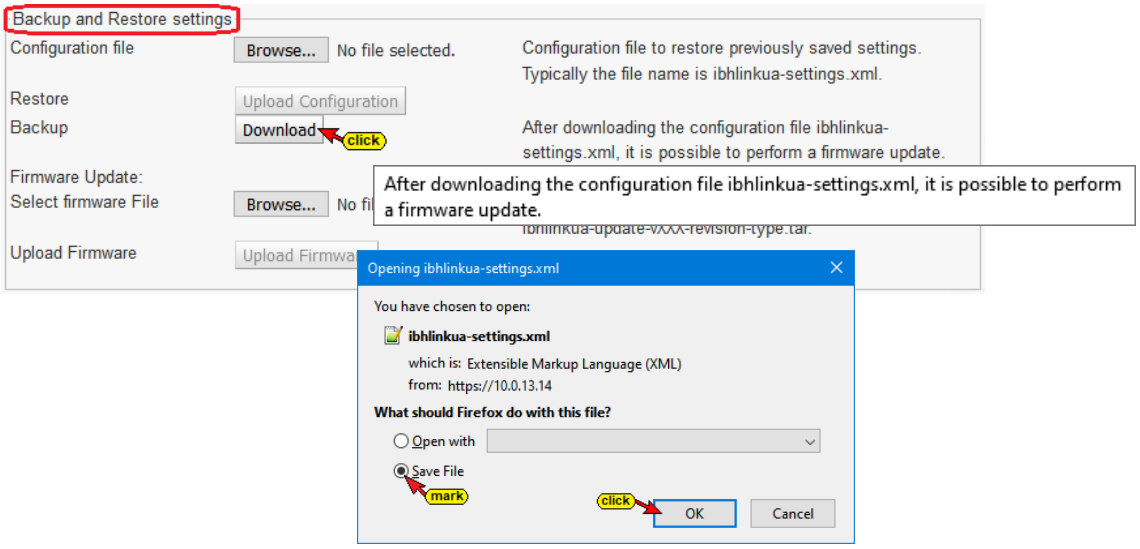


1.10.2 Backup and restoring the configuration

In this field there are buttons to save or restore the ***IBH Link IoT*** configuration. The backup function must be carried out prior the firmware update.

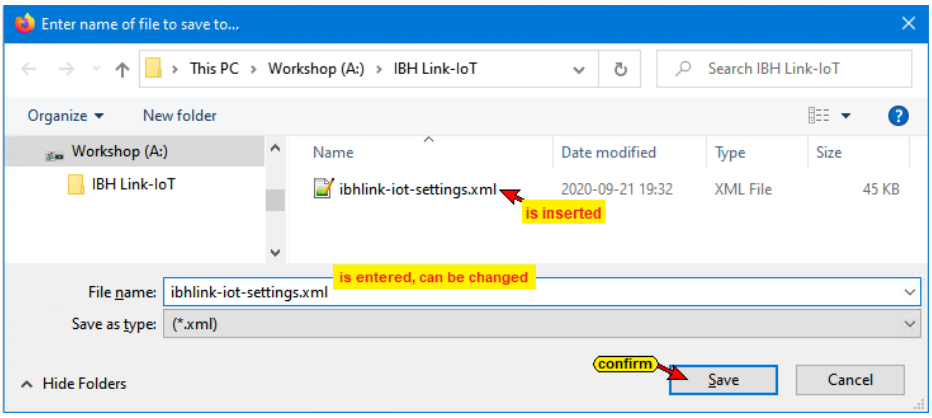
Backup configuration

To save the configuration, click the ***Download*** button and select ***Save As*** in the opened dialog box.



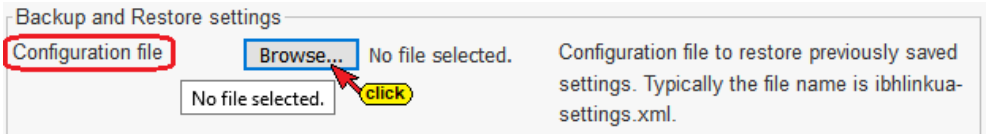
Specify the path and filename in the Save to dialog box and confirm by clicking ***Save***.

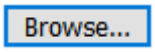
This procedure saves the existing settings.

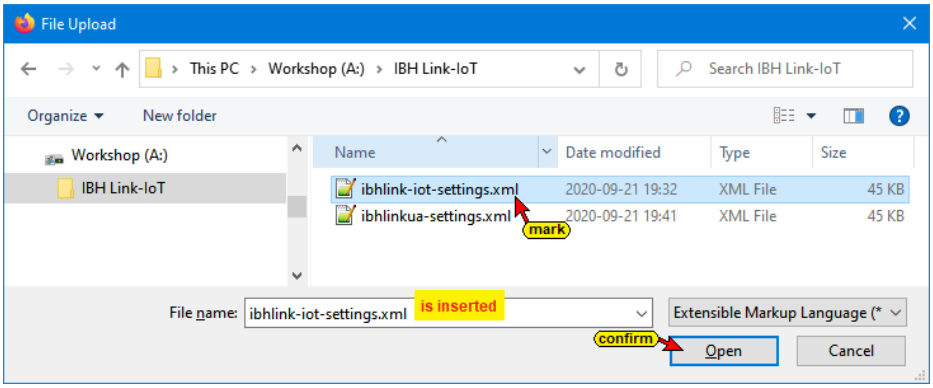


Restore the IBH Link IoT configuration

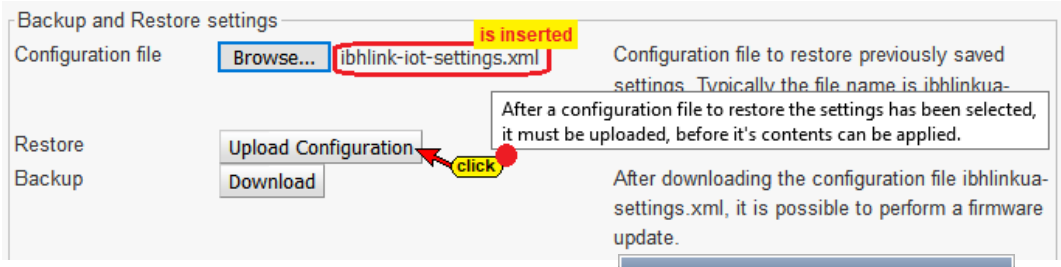
An already saved configuration can be restored.



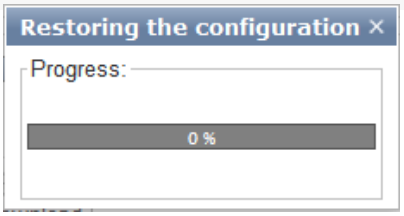
Click the ***Browse*** button.  The ***File Upload*** dialog box opens.



Click ***Open*** to close the ***File Upload*** dialog box and click the ***Upload Configuration*** button.



The progress of the upload is displayed.



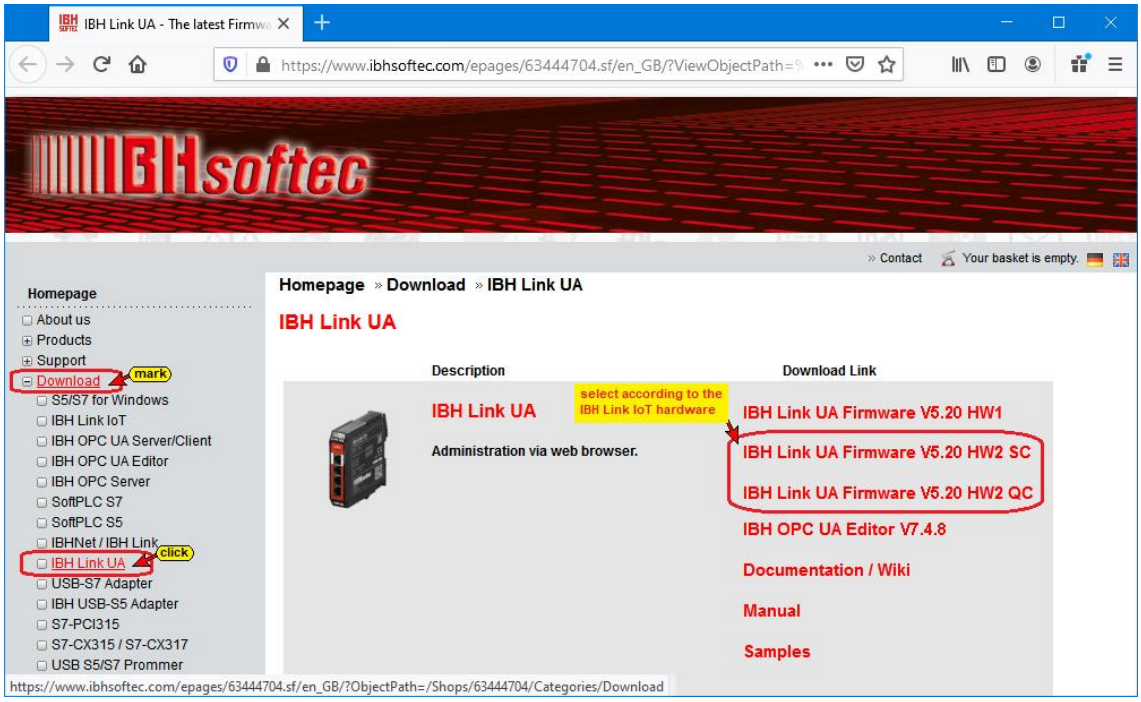
A restart is required to complete the configuration transfer.

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.



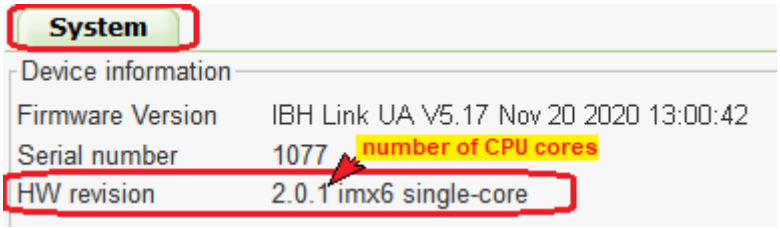
There are three firmware versions available for download.

HW1 IBH Link UA Firmware V5.20 HW1

This firmware version is only intended for IBH Link UA's, not for IBH Link IoT's.

HW2 SC IBH Link UA Firmware V5.20 HW2 SC

This is the firmware version for the IBH Link IoT having the following HW revision shown in the System browser window:



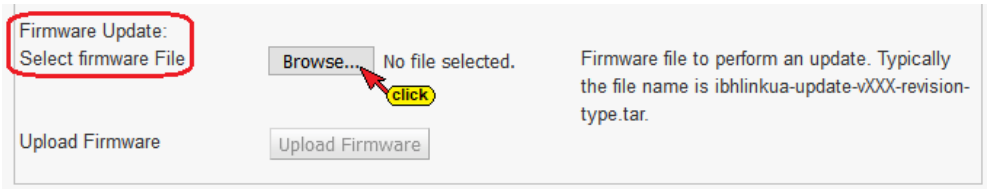
A number separated by dots (2.0.1 - the last digit indicates the number of CPU cores) and the addition imx6.

HW2 QC IBH Link UA Firmware V5.20 HW2 QC

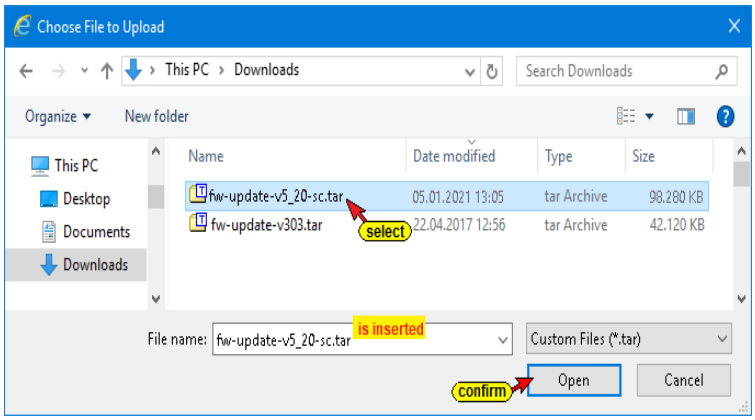
This firmware version is only intended for IBH Link UA's, currently not for IBH Link IoT's.

3. **Backup configuration**.
   Backup the IBH Link IoT configuration as described above.

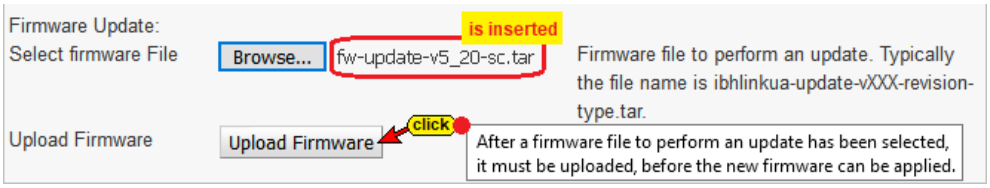
4. **Select the saved firmware file**.
   Click the ***Browse*** button. Browse... The ***File Upload*** dialog box opens. Select the firmware file * .tar for uploading.



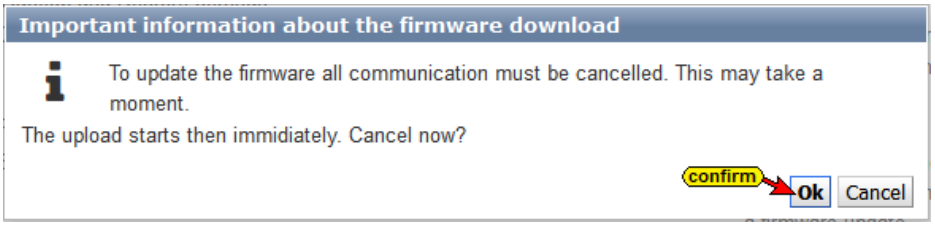
File Upload dialog box



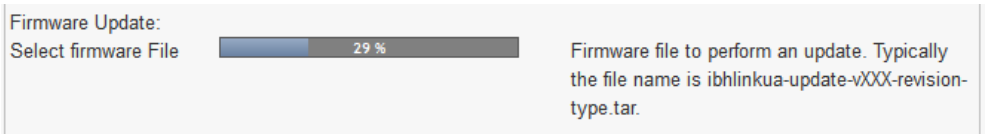
The firmware file ***.tar** is displayed.



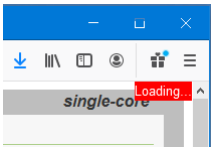
5. Click the ***Upload Firmware*** button to load the new firmware into the IBH Link IoT. The new firmware is not yet accepted (updated). Confirm the message.

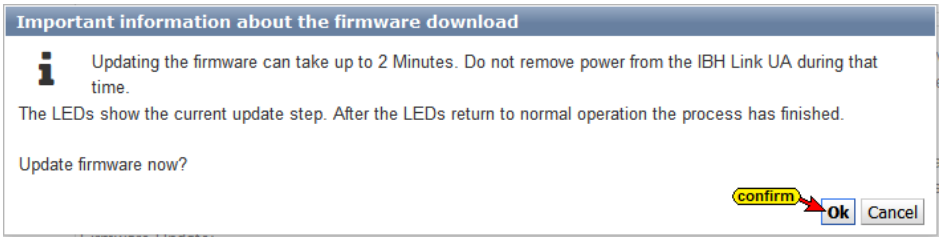


The progress of loading the firmware update is displayed.

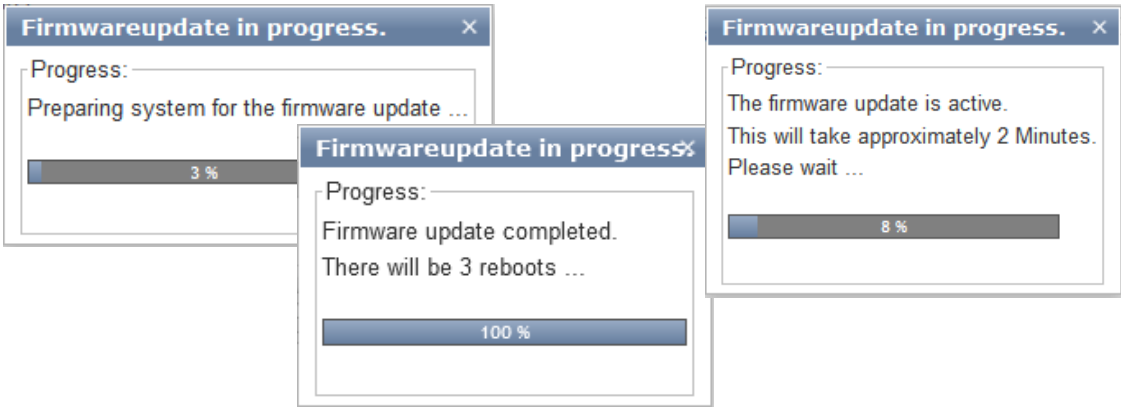


The loading of the firmware is indicated. If the loading is completed, the following message is displayed.



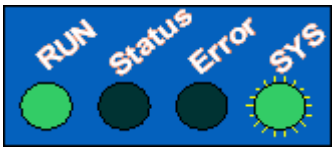


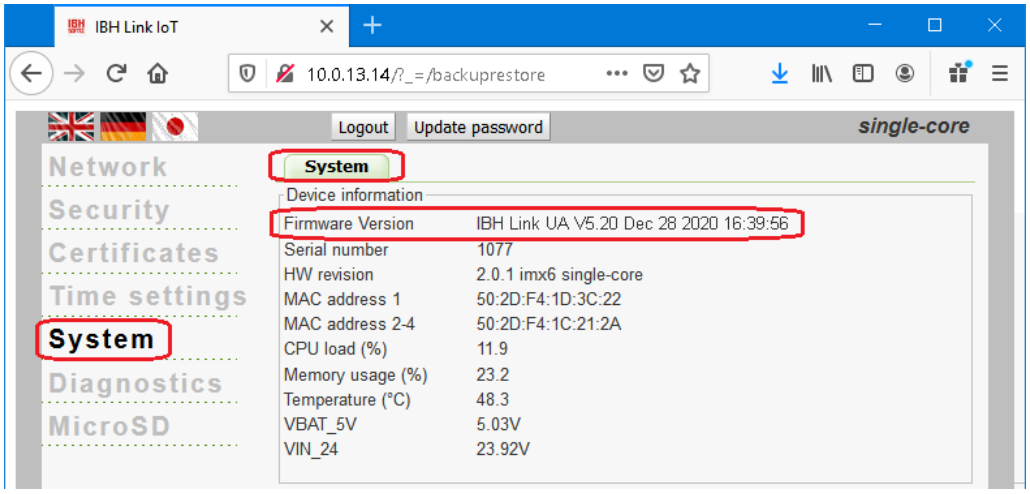
6. **Confirm the message**.
   The firmware update process is indicated. In the upper-right corner of the browser window Loading appears.



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

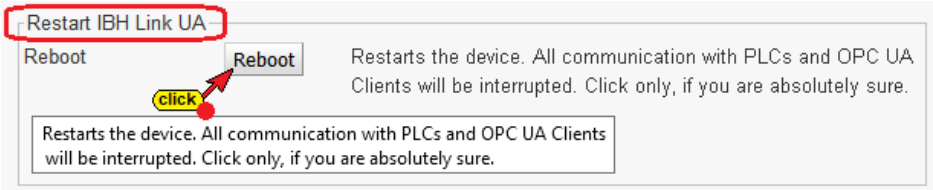
In normal operation, the ***RUN*** LED is lit, the ***SYS*** LED flashes, and the LED's ***Status*** and ***Error*** are off.





1.10.3 Restart the IBH Link IoT

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

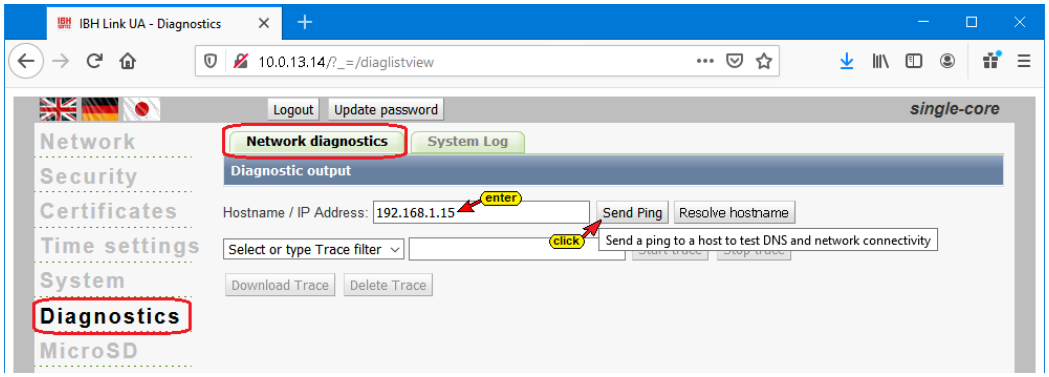


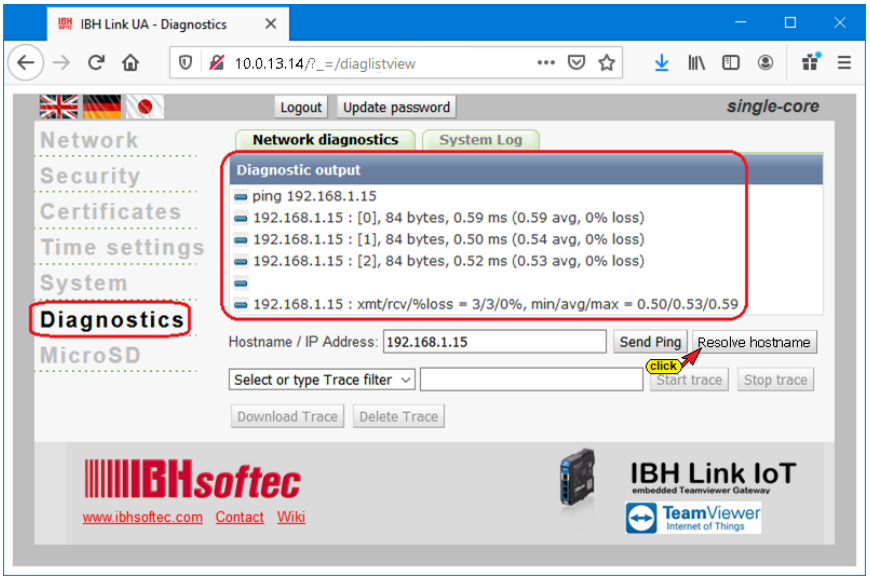
1.11 Diagnosis Browser window

The browser window Diagnosis has two tabs to display details about established or faulty connections.

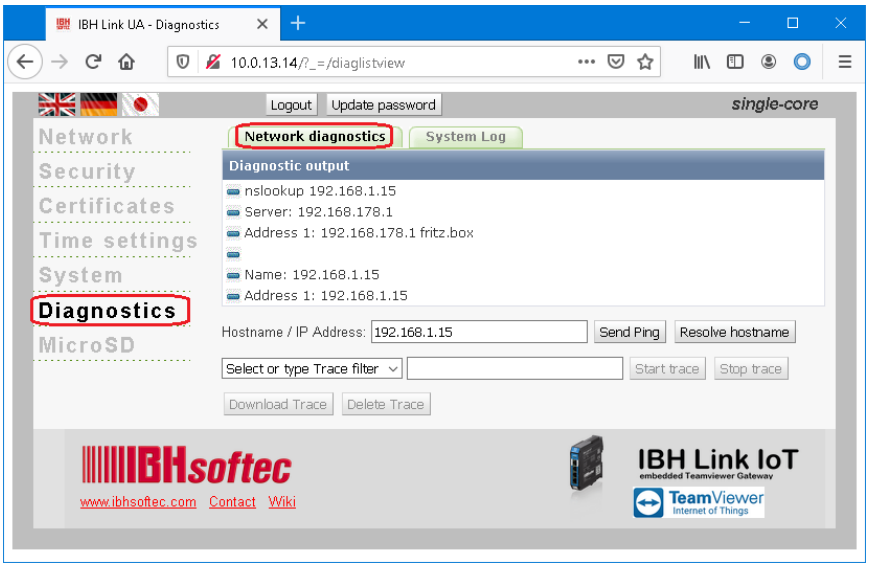
Network diagnostics

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

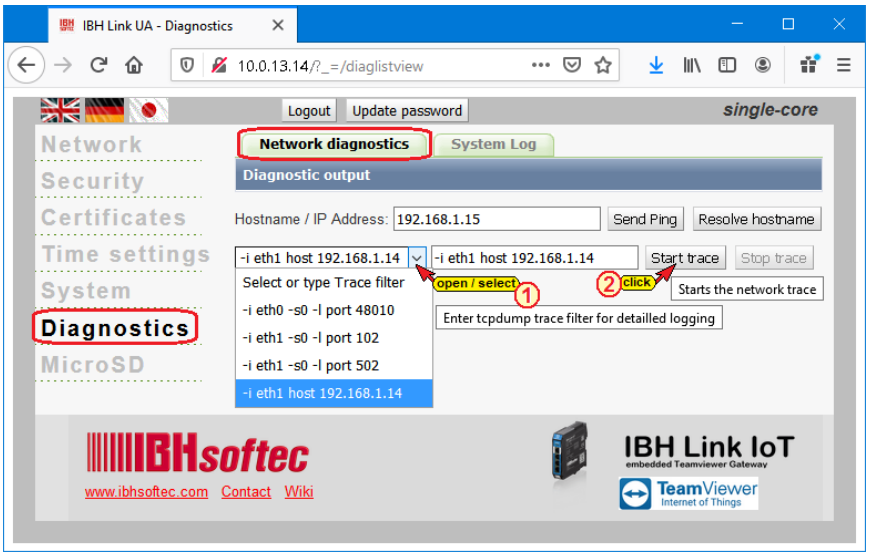




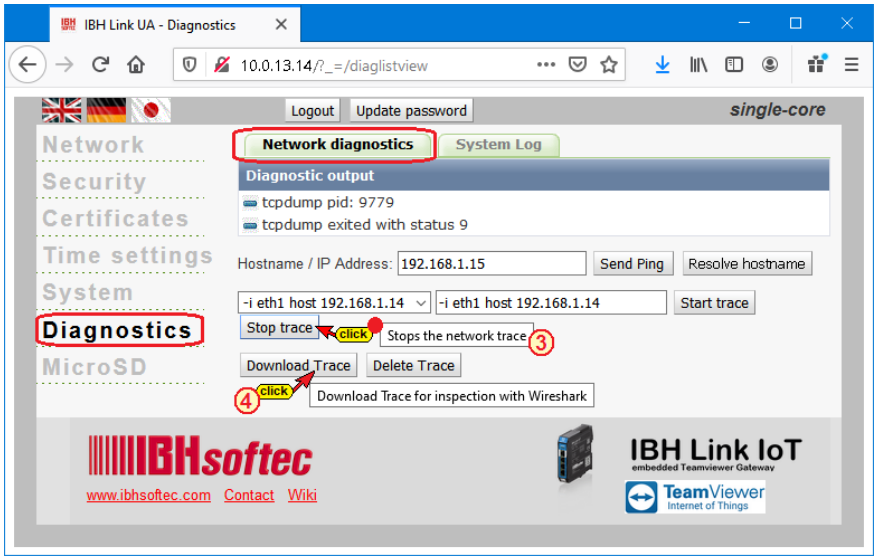
Resolve Hostname



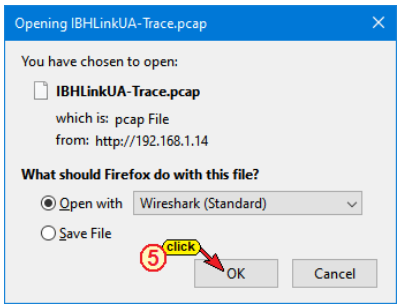
Is the Wireshark diagnostic software installed on the PC, a very extensive network analysis can be carried out?

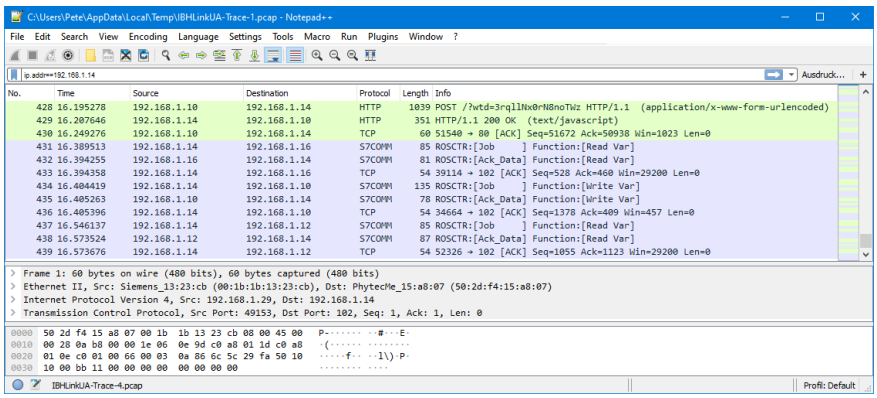


Download recording for evaluation with Wireshark



By clicking on Download Trace 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***.

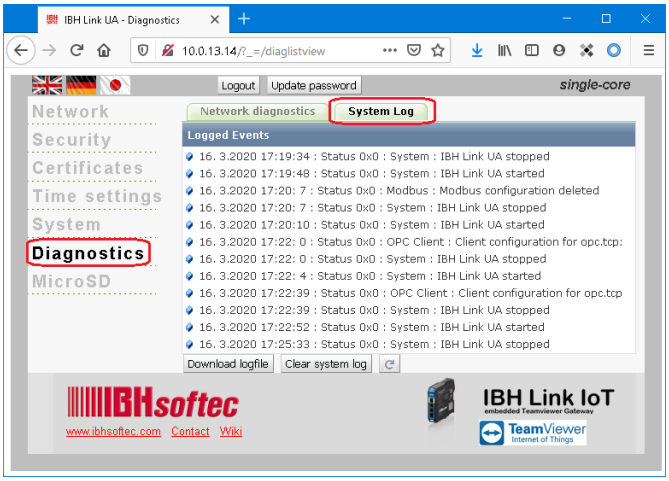




System logs

The ***IBH Link IoT*** diagnosis creates a log file in which IBH Link IoT 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.



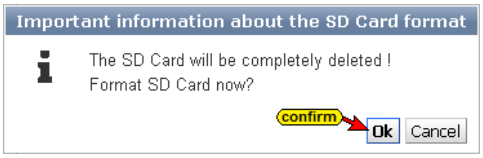
1.12 MicroSD browser window

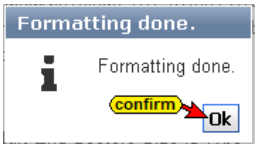
The IBH Link IoT has a slot for a ***MicroSD*** card on the back.

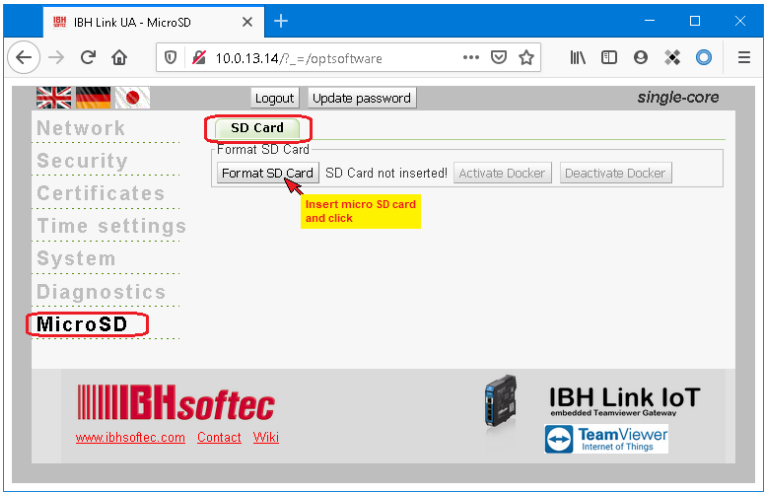
Note:

The use of the ***MicroSD*** card is intended for future firmware upgrades and currently has no function.

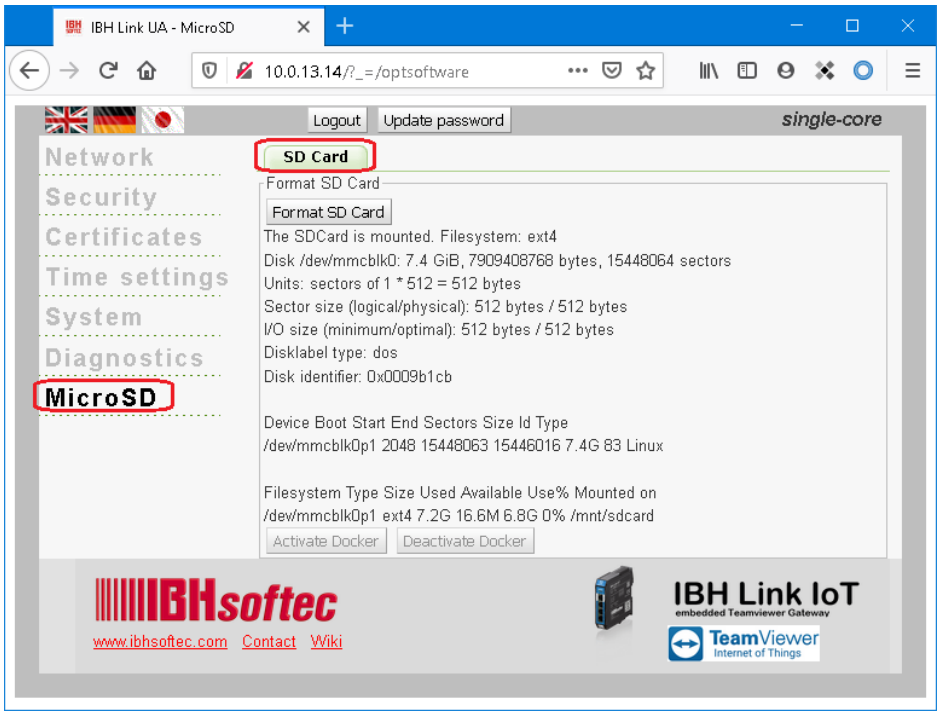
Information on formatting is displayed and must be confirmed.







The formatted SD card will be mounted automatically.



1.13 IBH Link IoT default factory configuration

The button to reset the software to the default factory configuration is located on the printed side of the IBH Link IoT, behind the middle ventilation slot above the printing.
The reset procedure reset the ***IBH Link IoT*** is to the default factory configuration with the current firmware loaded into the device.

Procedure:

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

Note:

With a formatted SD card is in the IBH Link IoT, the currently available IBH Link IoT configuration is saved on the SD card.

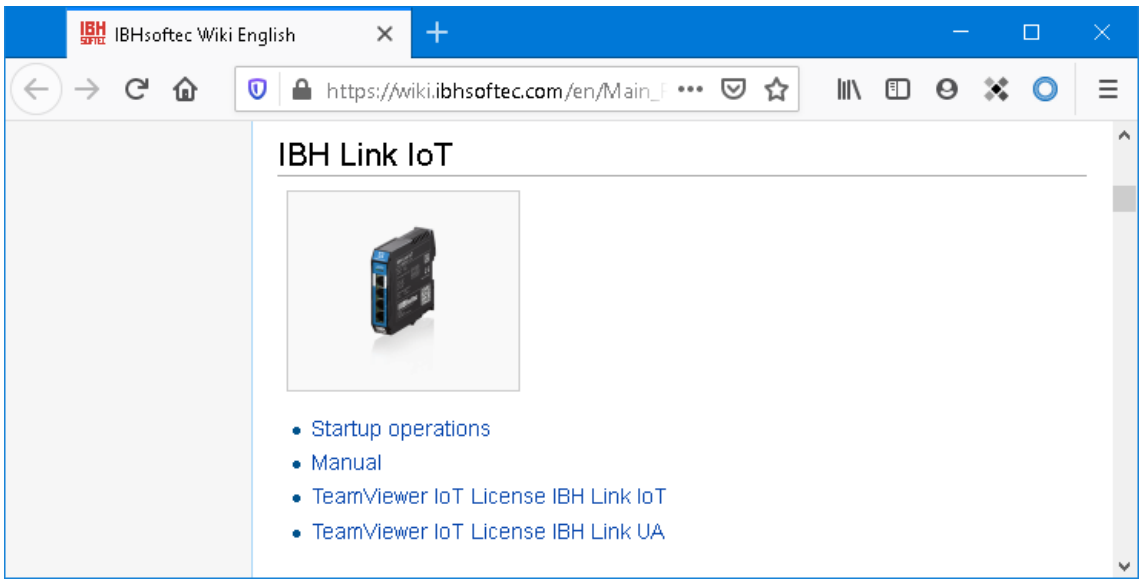
If the software is reset to the factory settings with the reset button, the configuration saved on the SD card is transferred to the IBH Link IoT at the end of the procedure.

1.14 Open the Wiki

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

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

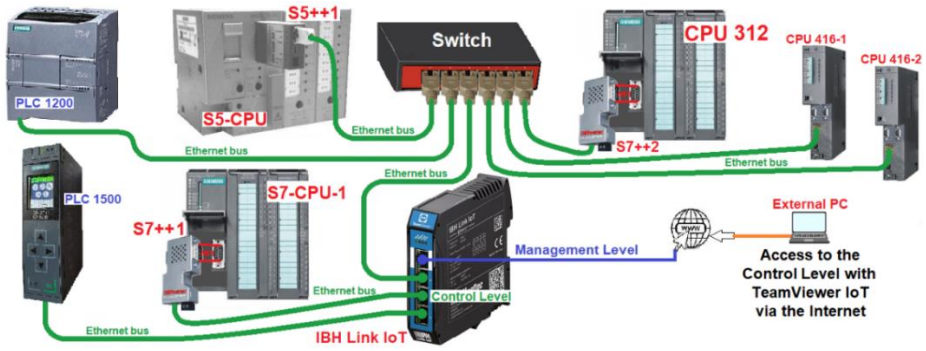
Open WIKI website



2 Access to controls (devices) connected to the ports of the control level

The example demonstrates the possible to display the online status of CPUs connected to the Control level of an IBH Link UA.

2.1 Remote IBH Link UA with connected CPUs



Several PLC programming systems for online access to the individual controls are installed on the external PC.

PLC control	IP address *Control level*	Programming system
CPU 416 S7e	10.0.13.11	**STEP 7 Simatic Manager**
CPU 312 S7e	**IoT S7++1** / 10.0.13.25	
PLC 1500 TIA16e	10.0.13.90	**TIA Portal V16**
PLC 1200 TIA16e	10.0.13.91	
CPU 312 TIA16e	**IoT S7++2** / 10.0.13.26	
CPU 416 TIA16e	10.0.13.9	
S5 CPU 103Ue	**IoT S5++1** / 10.0.13.27	***S5 for Windows***

IBH Link IoT	**Control Level**	**10.0.13.14**
	Management Level	**DHCP**

The ***Management Level*** port has direct access to the Internet.

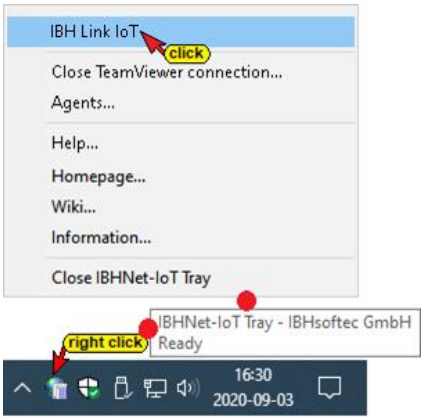
The ***IBH Link UA TeamViewer IoT*** function has been activated on the remote ***IBH Link UA*** as described in chapter 1.5.

2.1.1 Local PC

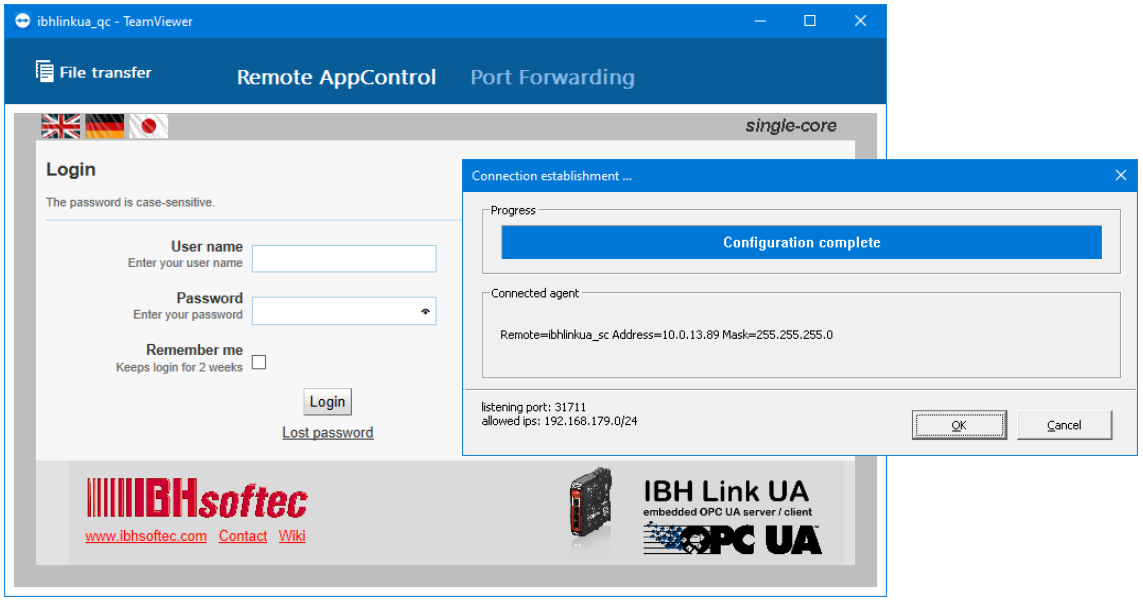
Several PLC programming software are installed on the local PC to display the online status of the CPUs.

TeamViewer is installed on the local PC. There is access to a TeamViewer account with the corresponding IoT license. The IBHsoftec software ***IBHNet-IoT-Setup.exe*** is installed. The TeamViewer ID of the Remote IBH Link UA and its name has been inserted into the TeamViewer Shortcuts dialog box via the Agents… command from the IBHNet-IoT Tray context menu.

- Start the ***TeamViewer*** software.
- Right click on the ***IBHNet-IoT Tray*** icon to open the context menu.
- With a click on IBH Link UA SC, the connection to the ibhlink-iot address is established via the Internet.



The establishment of the connection is displayed and the ***Port Forwarding*** of the Remote ***AppControl*** are displayed.



Note:

To access the individual CPUs (devices) (e.g. status) no registration to the ***IBH Link IoT*** is necessary.

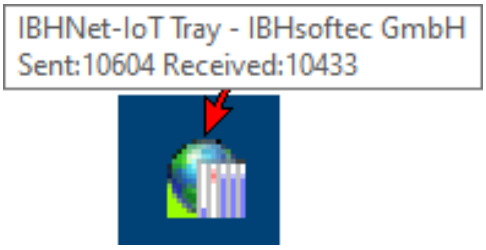
- **Start the programming software (STEP 7, TIA, *S5 for Windows* etc.).**

  The examples show connections from the CPU to the control level of an ***IBH Link IoT*** via an ***IBH Link S7++*** or ***IBH Link S5++***. It is possible to check the connections and the settings of the IBH links.

2.1.2 Check IBH Link S7++ settings

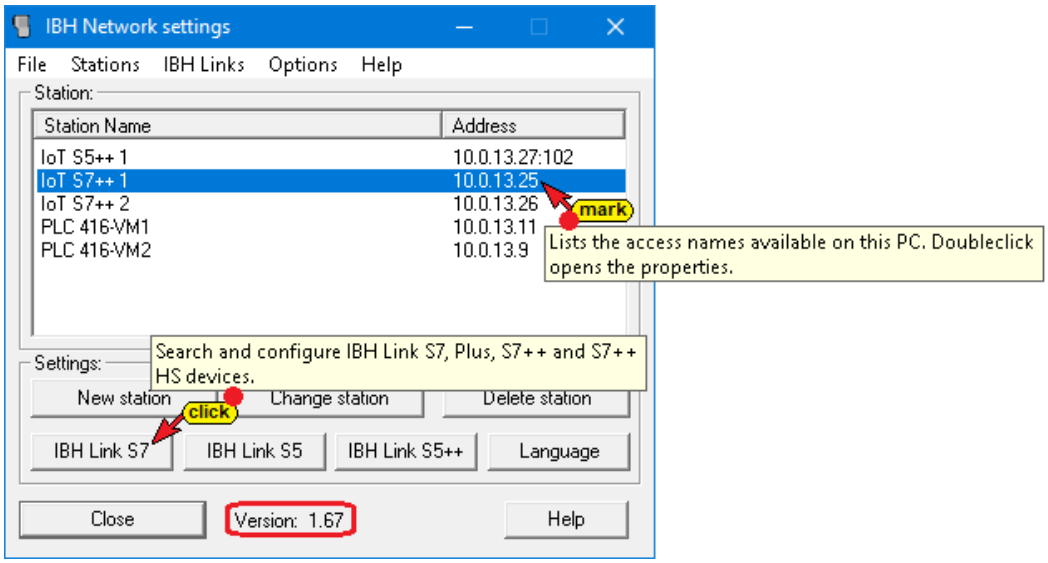
CPUs of the S7-300 and S7-400 series not having a free Ethernet interface can be connected to the IBH Link IoT via ***MPI bus*** via an ***IBH Link S7++*** via Ethernet (RFC 1006 protocol).
The ***IBH Link S7++*** is an Ethernet converter. The protocol used is standard ***TCP / IP***. The user can benefit from all the advantages of Ethernet without any problems.

If the connection to the ***IBH Link IoT*** is established via the Internet, the IBHNet-IoT tray symbol has a green corner at the bottom left, and transmission data is displayed.

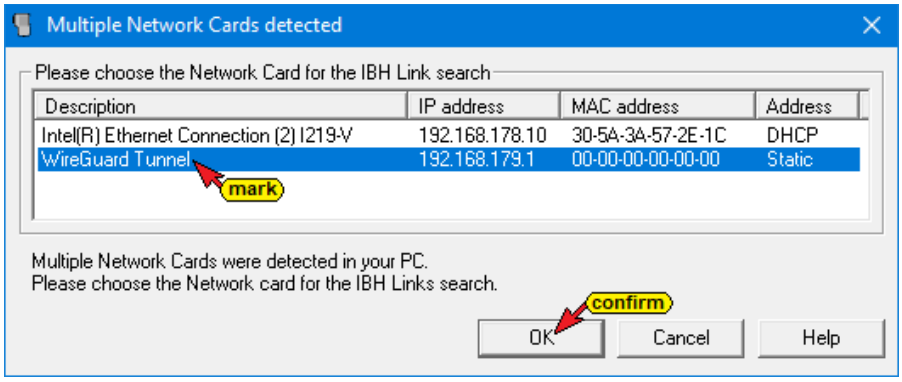


After starting ***Manage IBHNet Stations***, the ***IBH Network Settings*** dialog box opens. Click the IBH Link S7 button to open the Detect multiple network cards dialog box.

Dialog box IBH Network Settings



Mark ***WireGuard Tunnel*** and confirm with ***OK***.

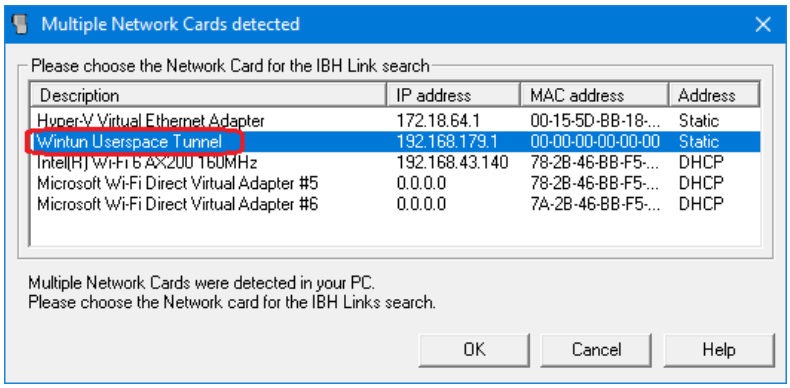


Note!

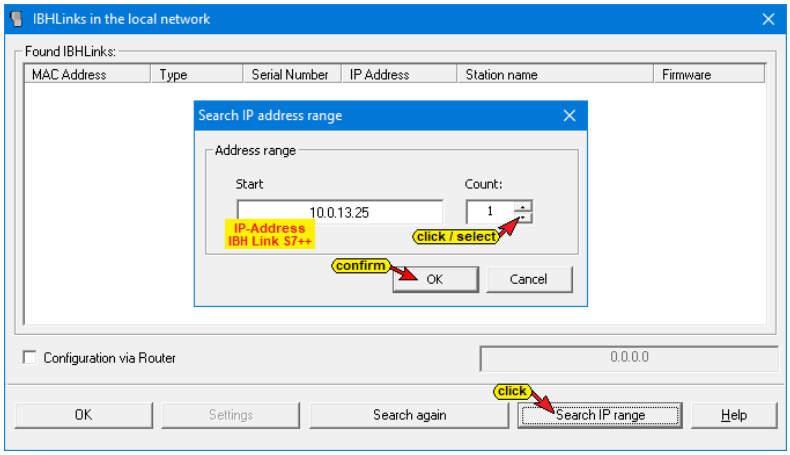
Windows use two names for network adapters, the ***Name*** given by the ***Hardware*** or the ***FriendlyName***.

- **WireGuard Tunnel**
- **Wintun Userspace Tunnel**

Depending on the software using network adapter and the Windows status the ***Hardware Name*** or the ***FriendlyName*** is displayed.

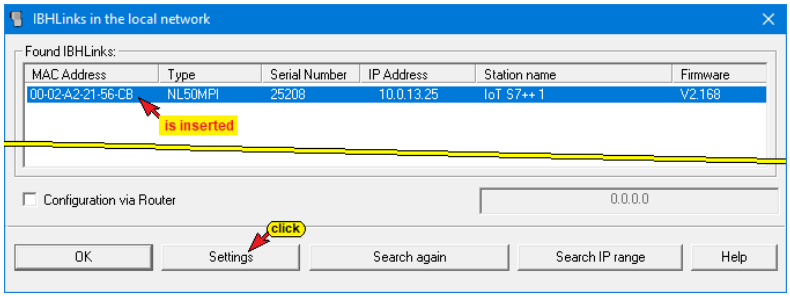


In the ***IBH Links in the local network*** dialog box, click the ***Search IP range*** button.

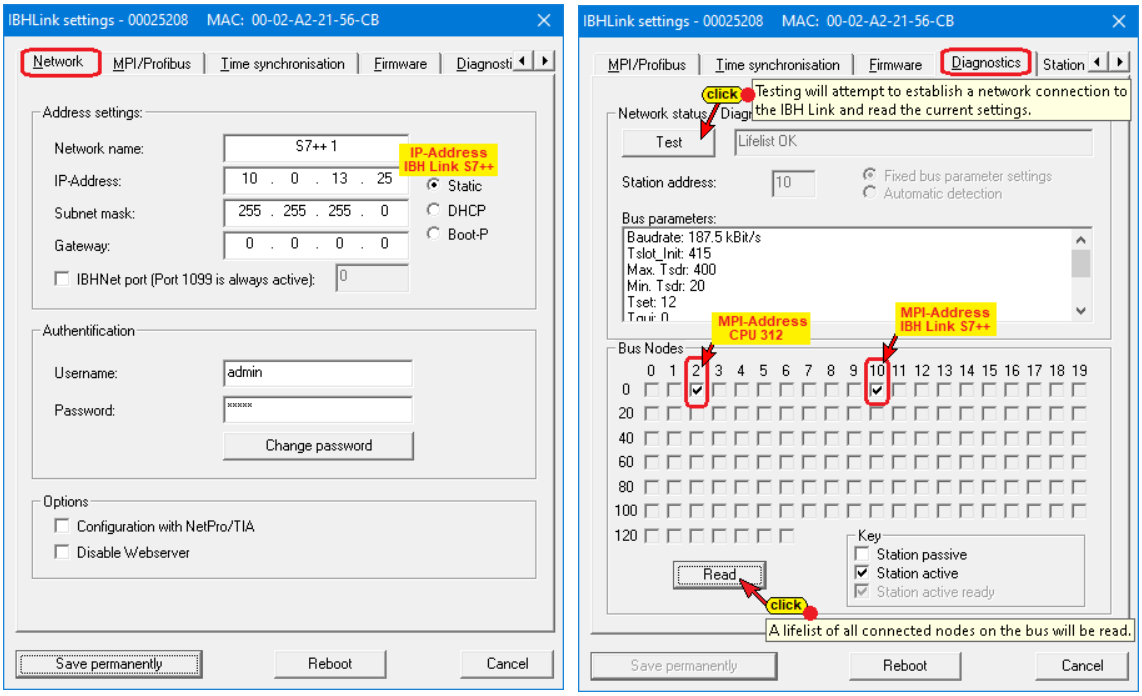


Searching for several IBH links is impossible over the Internet. In the ***Search IP Range*** dialog box, enter the IP address of the ***IBH Link S7++*** to be searched and the number 1. When you click ***OK***, the connection to the IBH Link S7++ is established.

Information of the connected ***IBH Link S7++*** are displayed.

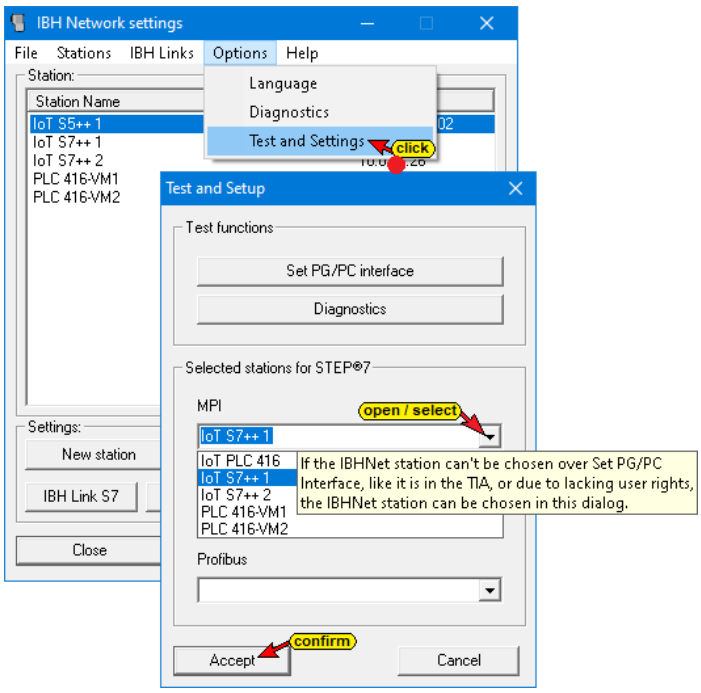


Click on the button ***Settings*** to display several tabs with information on the connected ***IBH Link S7++***.



2.1.3 Two or more IBH Link S7++ in one Subnet

The TIA Portal programming environment does not have a dialog to select different IBH Link S7++. The selection must be performed using the ***IBH Network Settings*** dialog box.

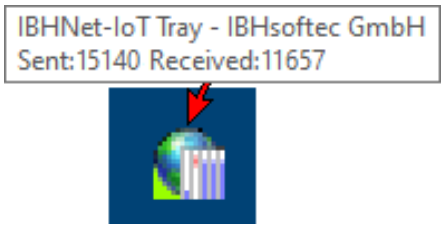


By clicking the ***Accept*** button, the IBHNet driver is given the IP address. The TIA Portal, therefore, only has access to the assigned CPU via the ***IBH Link S7++***.

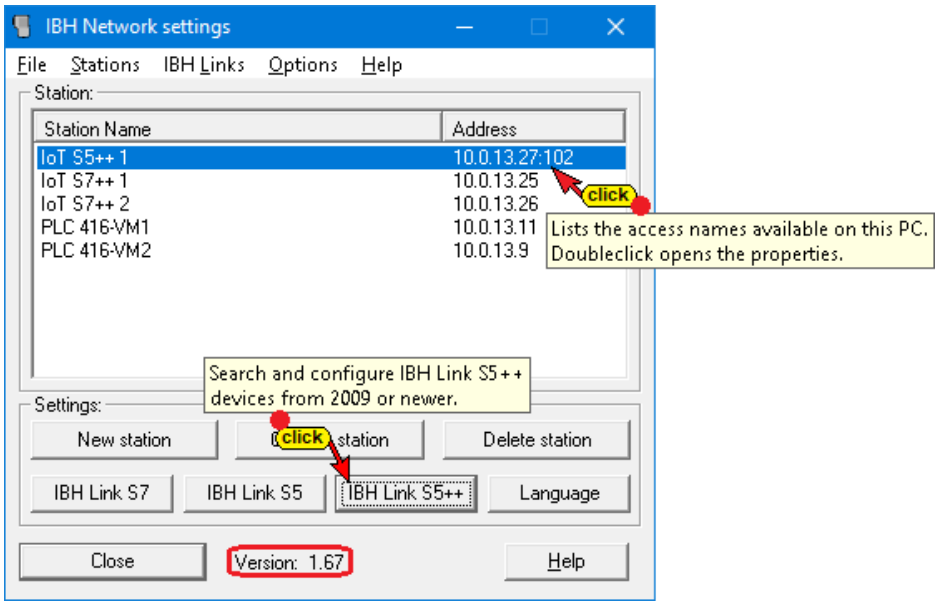
2.1.4 Check IBH Link S5 ++ settings

CPUs of the ***S5*** series not having a free Ethernet port can be connected to the IBH Link IoT via the ***PG interface*** via an ***IBH Link S5++*** via Ethernet (RFC 1006 protocol).
The IBH Link S5++ is an Ethernet converter. The protocol used is standard TCP / IP. The user can benefit from all the advantages of Ethernet.

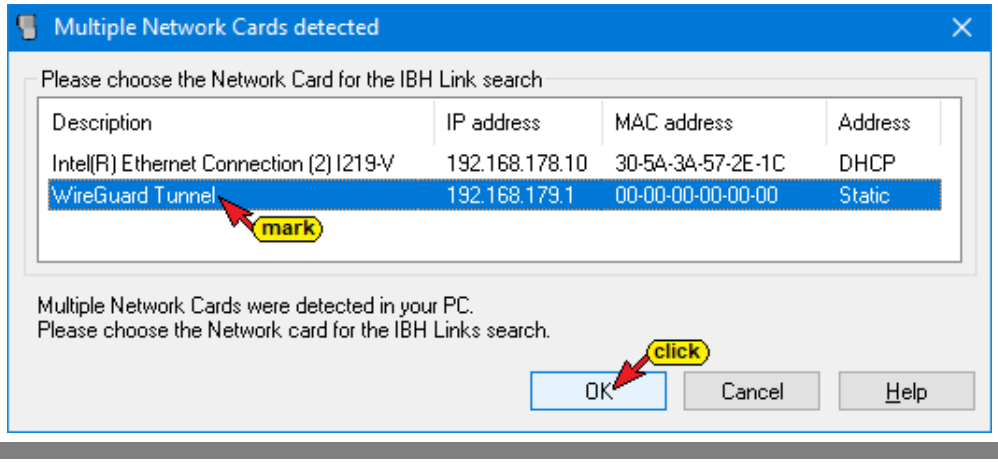
If the connection to the ***IBH Link IoT*** is established via the Internet, the IBHNet-IoT tray symbol has a green corner at the bottom left, and transmission data is displayed.



After starting IBHNet Manage Stations, the ***IBH Network Settings*** dialog box opens. Click the ***IBH Link S5++*** button to open the ***Detect multiple network cards*** dialog box.



Mark ***WireGuard Tunnel*** and confirm with ***OK***.



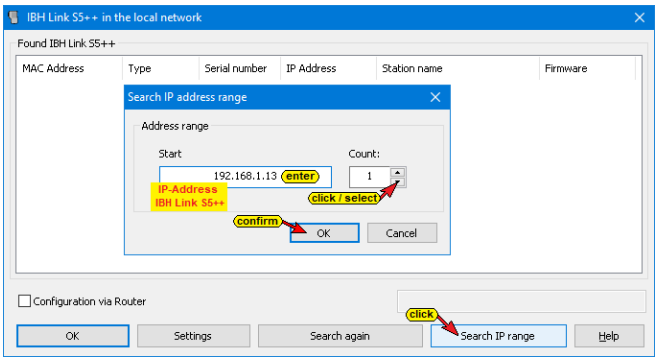
Note!

Windows use two names for network adapters, the ***Name*** given by the ***Hardware*** or the ***FriendlyName***.

- **WireGuard Tunnel**
- **Wintun Userspace Tunnel**

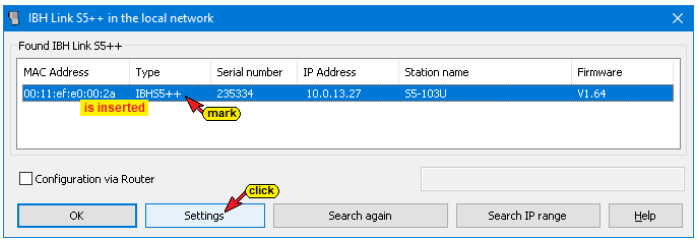
Depending on the software using network adapter and the Windows status the ***Hardware Name*** or the ***FriendlyName*** is displayed.

In the ***IBH Link S5++ in the local network*** dialog box, click the ***Search IP range*** button.

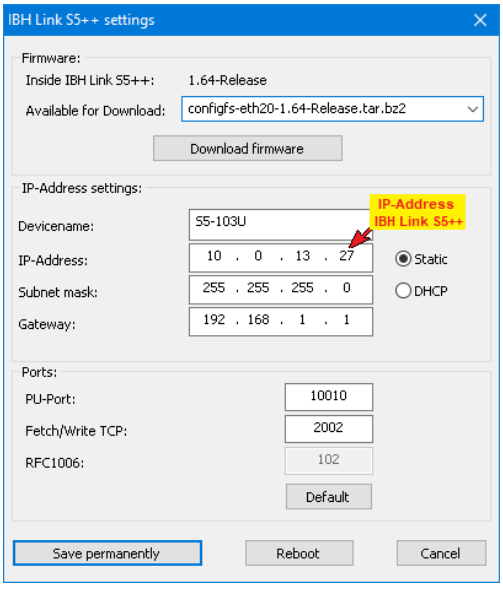


Searching for several IBH links is impossible over the Internet. In the ***Search IP address range*** dialog box, enter the IP address of the ***IBH Link S5++*** to be searched and the number 1.

When you click ***OK***, the connection to the ***IBH Link S5++*** is established.
Information of the connected ***IBH Link S5++*** are displayed.



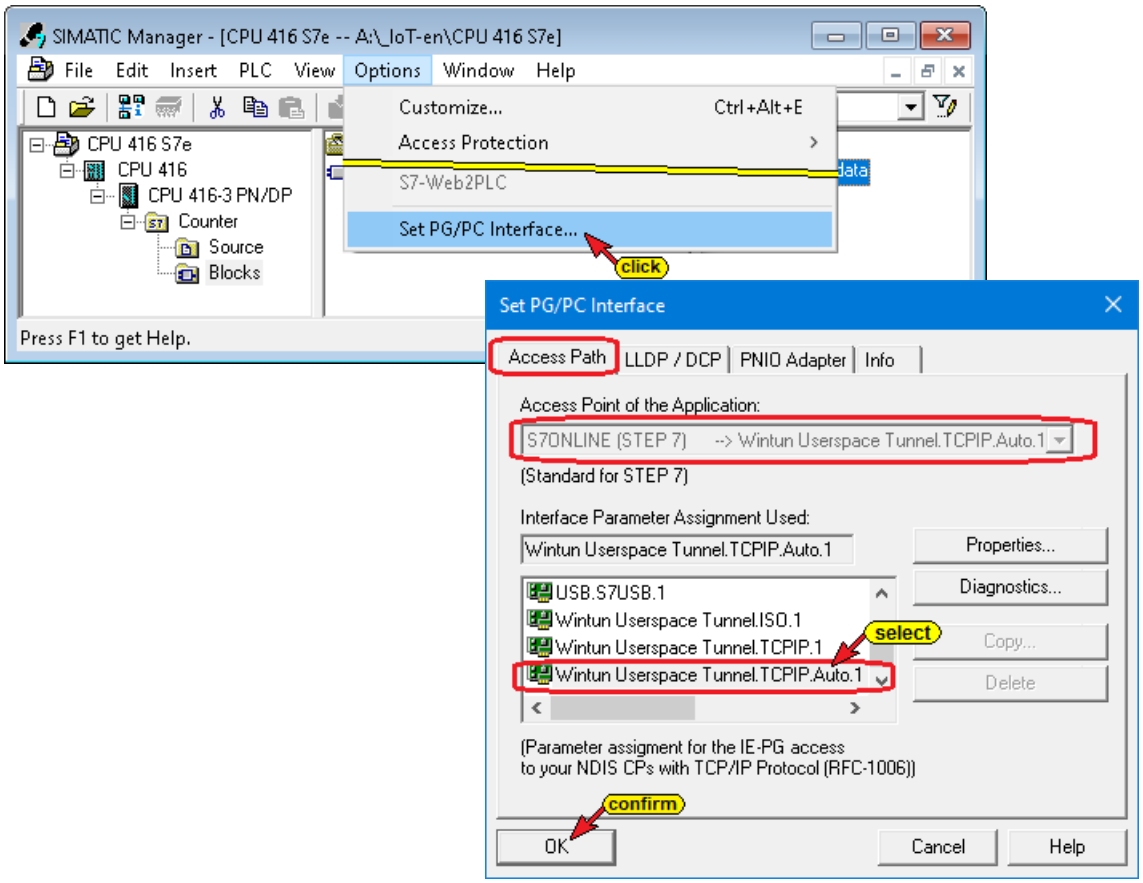
Click on the button ***Settings*** to display information on the connected ***IBH Link S5++***.



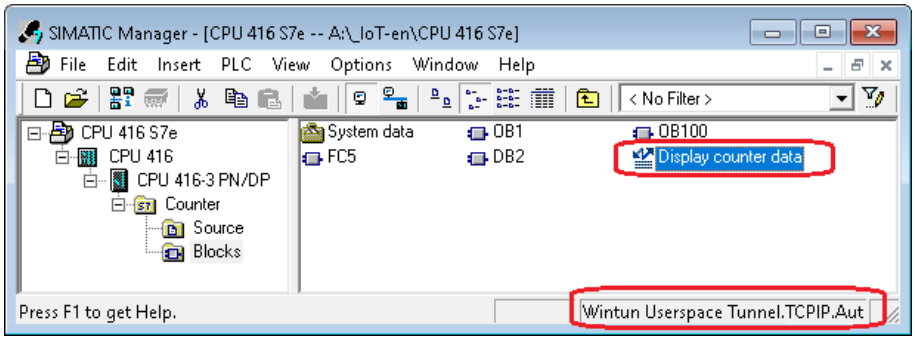
2.1.5 STEP 7 Simatic Manager – CPU 416 S7e

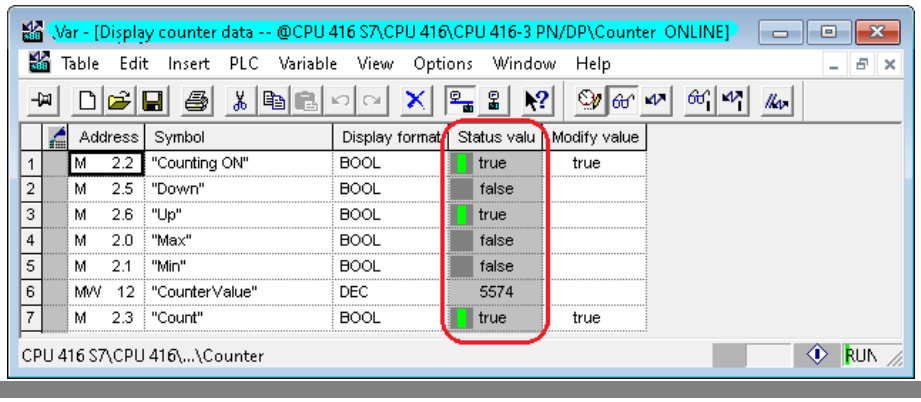
The CPU 416 has an Ethernet port (***IP address 10.0.13.11***) and is directly connected to the Control Level of the IBH Link IoT.

Set interface



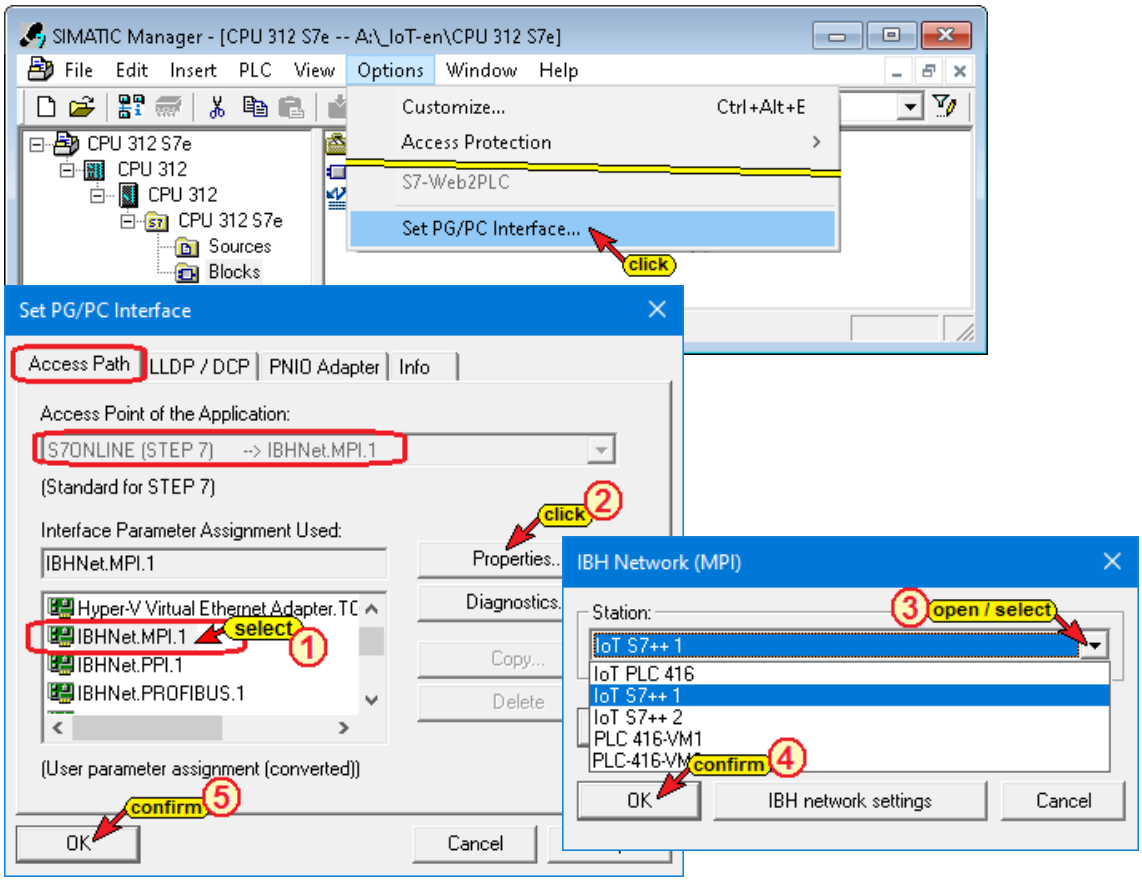
Status S7 CPU 416



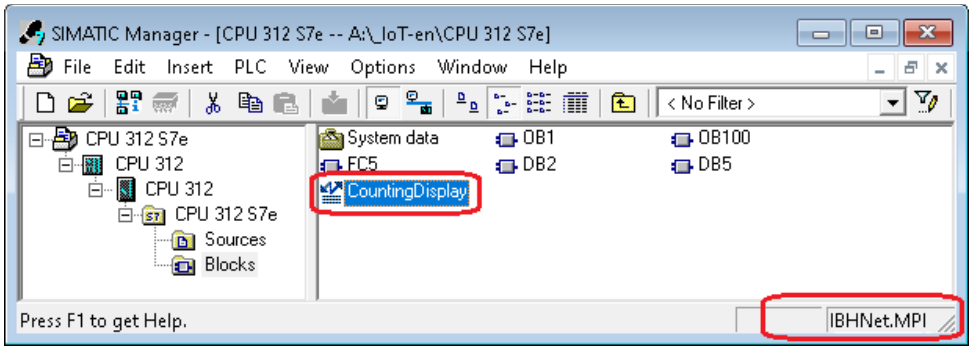


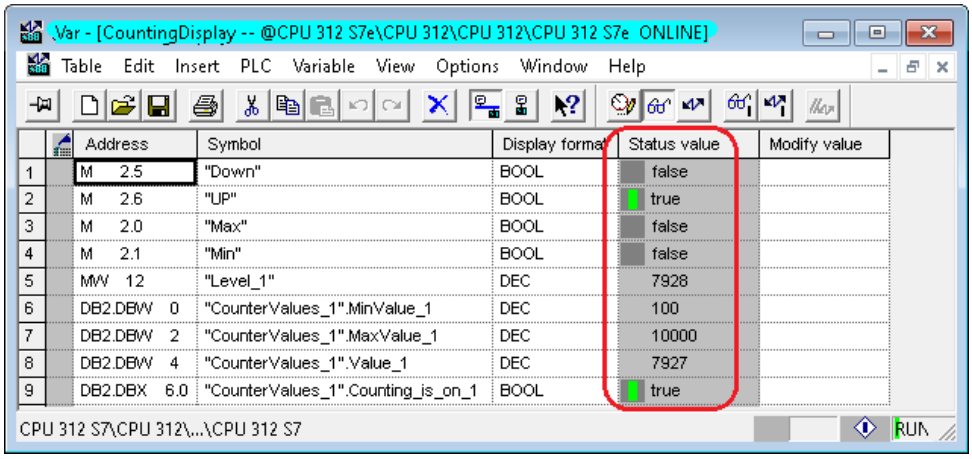
2.1.6 STEP 7 Simatic Manager –CPU 312 S7e –

The CPU 312 is connected to the control level of the IBH Link IoT via an LBH Link S7++ (IoT S7++ IP address 10.0.13.25).



Status S7 CPU 312



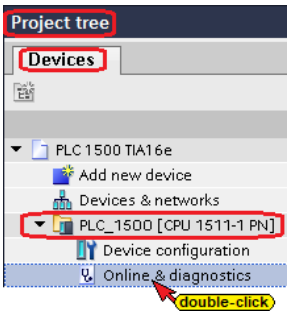


2.1.7 TIA Portal V16 – PLC 1500 TIA16e

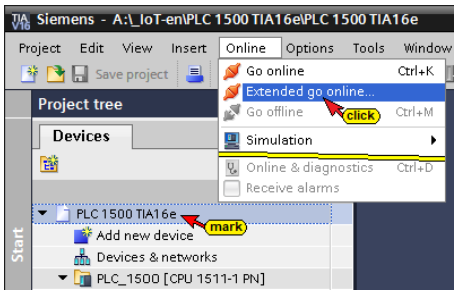
There are several ways to establish an online connection in the TIA Portal. The CPU of the opened project must have the same IP address as the CPU that is connected to the IBH Link IoT / control level.

The CPU 1500 is connected to the control level of the IBH Link IoT (IP address 10.0.13.90).

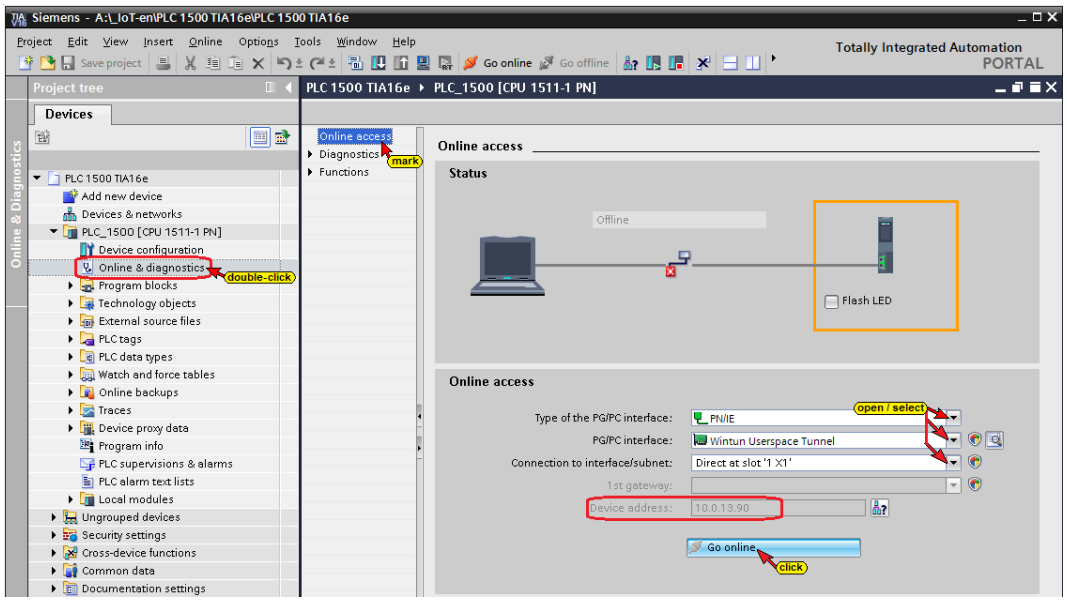
1. ***Project tree / devices*** (PLC 1500) ***/ online & diagnostics***.
   The same command is available in the Online menu. A double-click opens the Online access window. Settings must be made here.



2. ***Online / Extended go online...***
   The command opens the ***Go online*** dialog box. There are other ways to open the Go online dialog box. The required settings are identical.

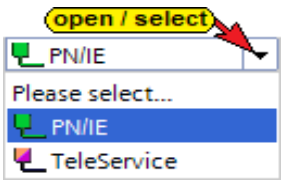


Online & diagnostics – Online access window

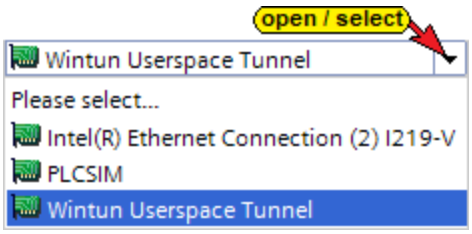


In the Online Access dialog box, select the settings as follows:

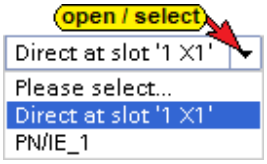
The ***Type of PG/PC interface*** must be selected according to the hardware configuration of the CPU.



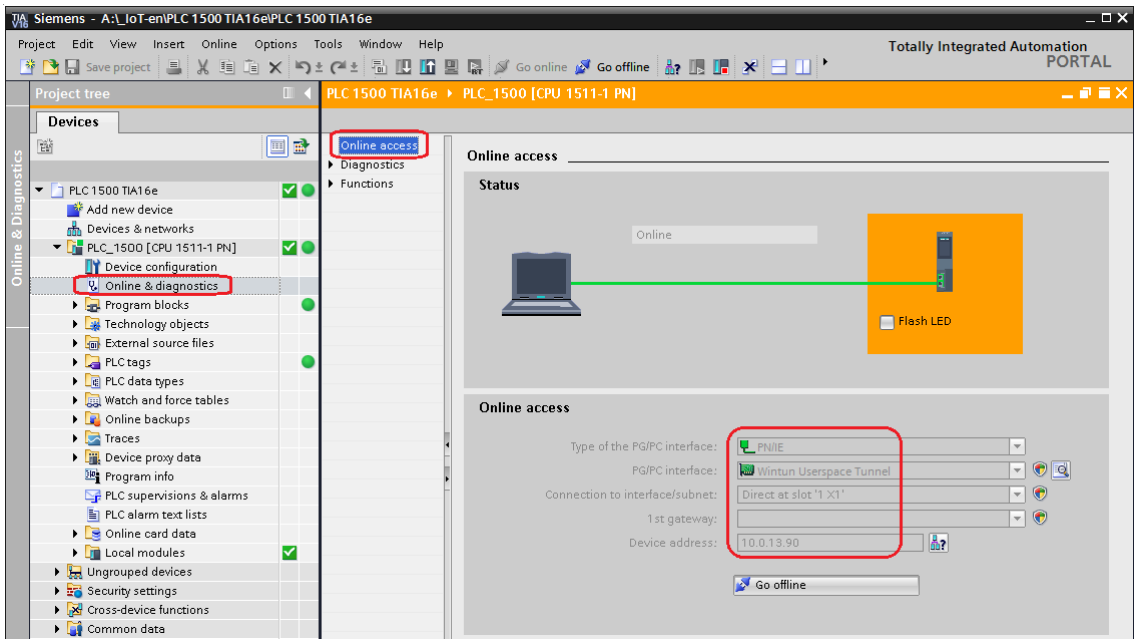
Wintum Userspace Tunnel must be specified as the PG / PC interface if there is a direct connection between the CPU and IBH Link IoT / control level.



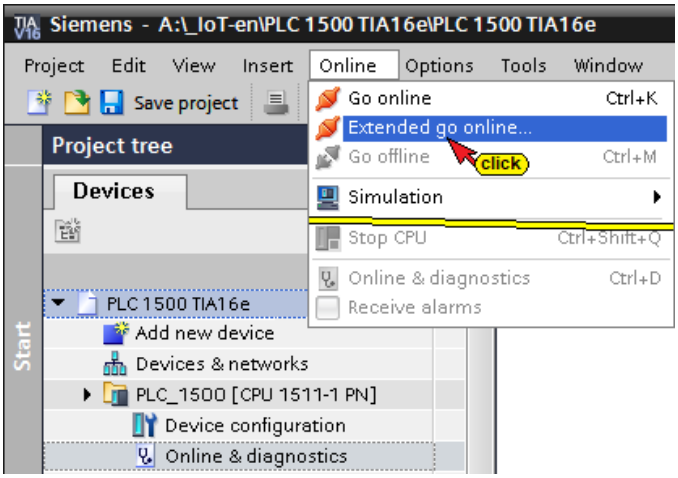
The physical location or the name of the Ethernet connection must be specified at ***Connection to interface/subnet***.

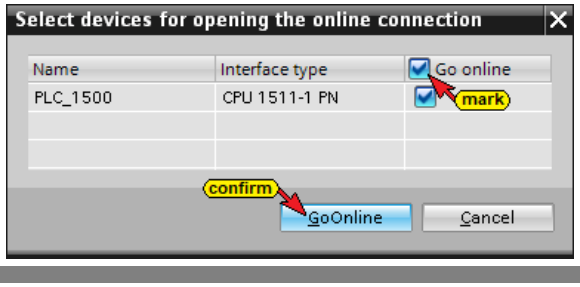


The online connection to the CPU1500 is established.

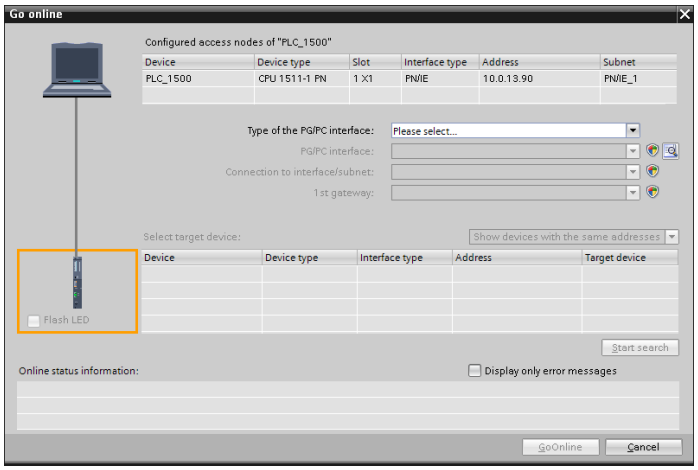


Extended go online access – Online access dialog box



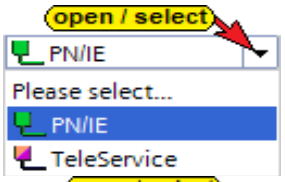


The Go online dialog box opens.

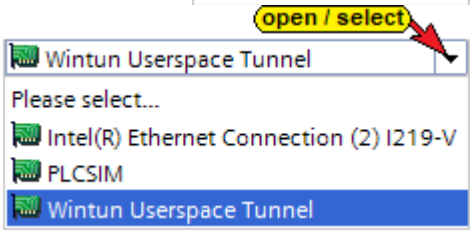


In the *Go online* dialog box select the following settings:

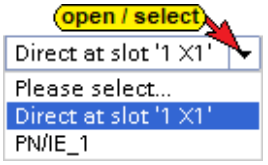
The ***Type of PG/PC interface*** must be selected according to the hardware configuration of the CPU.



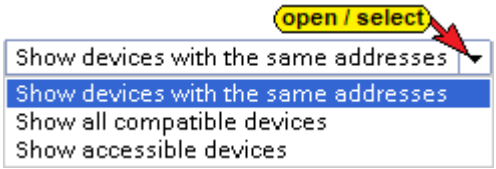
Wintum Userspace Tunnel must be specified as the PG / PC interface if there is a direct connection between the CPU and IBH Link IoT / control level.



The physical location or the name of the Ethernet connection must be specified at ***Connection to interface/subnet***.

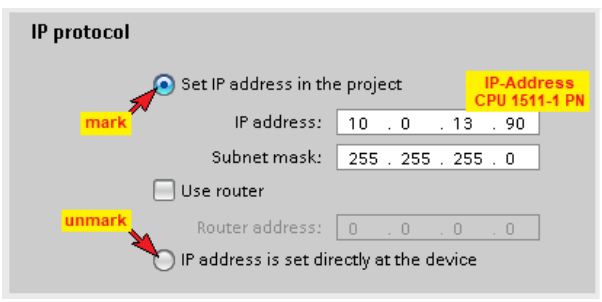


Show device with the same address must be selected as the target device.



Note:

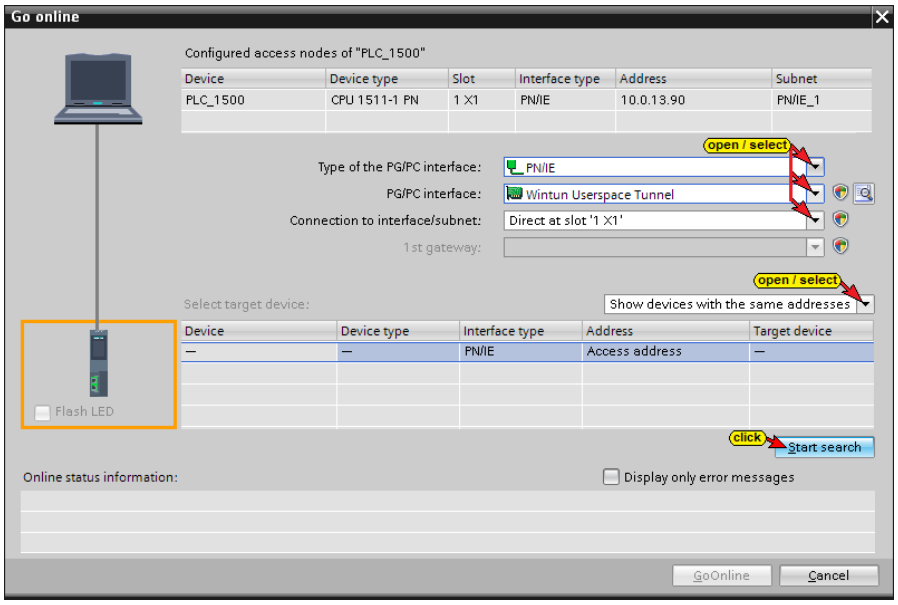
If the command ***Show device with the same address*** is not available, no connection to the CPU can be established.
In the hardware configuration of the CPU, the option ***IP address is set directly at the device*** must be deactivated.



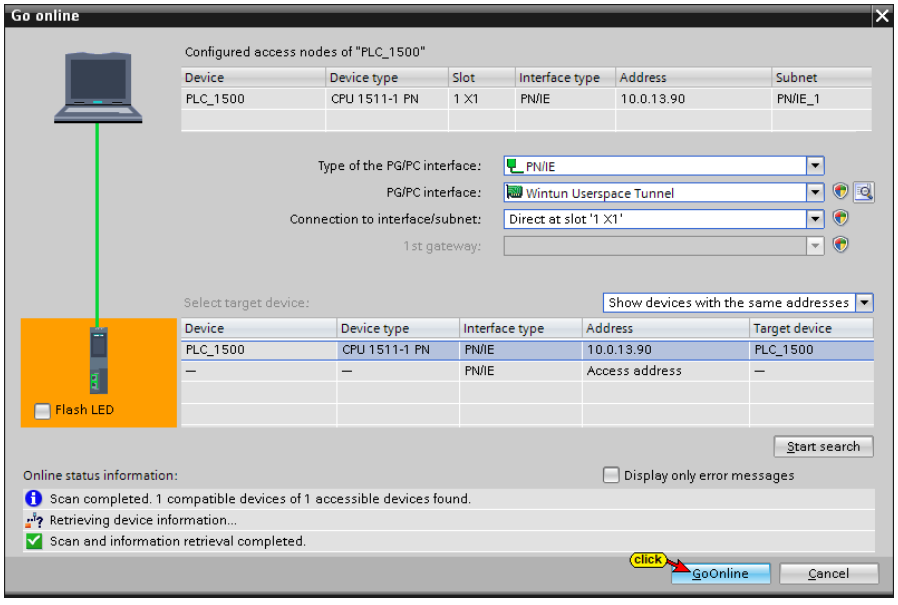
Deactivate ***IP address is set directly on the device.***

Search – Go online

Clicking the ***Start search*** button attempts to establish an online connection to the CPU.

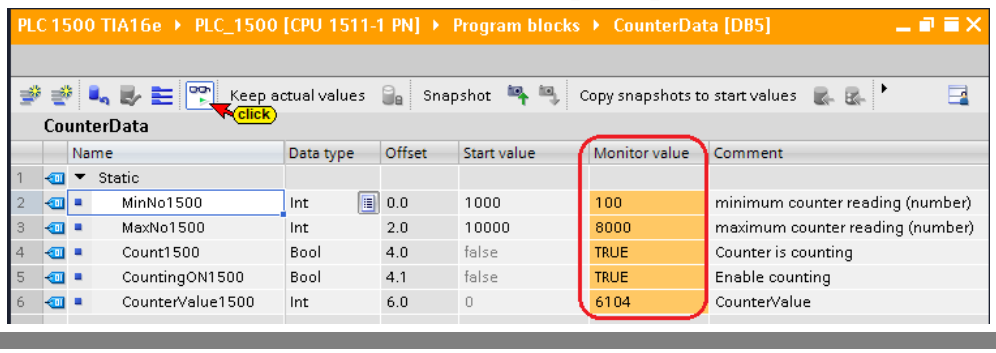


If the CPU to be connected is found, further data exchange is enabled with a click on the ***Go Online*** button.



The online connection to the CPU1500 is established.

Status CPU 1500 – data block CounterData [DB5]

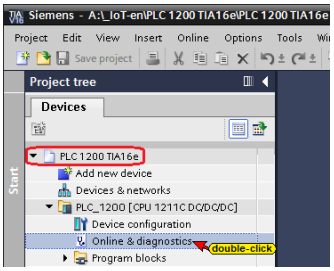


2.1.8 PLC 1200 TIA16d – IP-Address 10.0.13.91

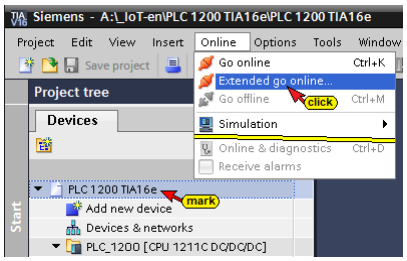
There are several ways to establish an online connection in the TIA Portal. The CPU of the opened project must have the same IP address as the CPU that is connected to the IBH Link IoT / control level.

The CPU 1200 is connected to the control level of the IBH Link IoT (IP address 10.0.13.91).

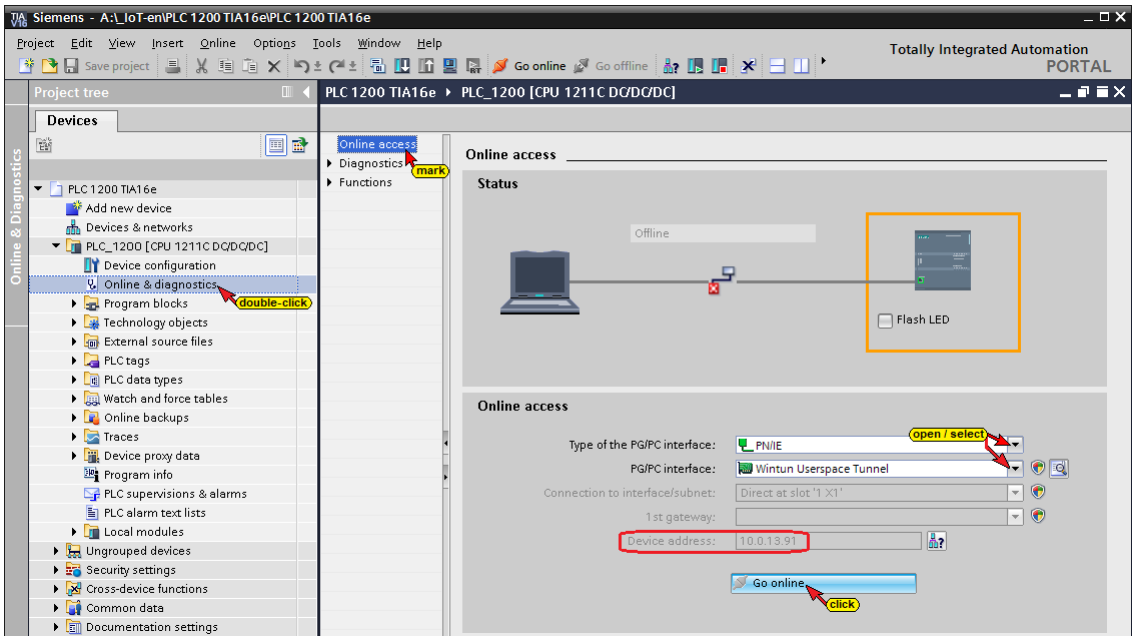
1. ***Project tree / devices*** (PLC 1200) ***/ online & diagnostics***.
   The same command is available in the Online menu. A double-click opens the Online access window. Settings must be made here.



2. ***Online / Extended go online...***
   The command opens the ***Go online*** dialog box. There are other ways to open the Go online dialog box. The required settings are identical.

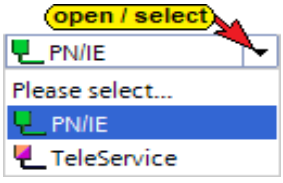


Online & diagnostics – Online access window

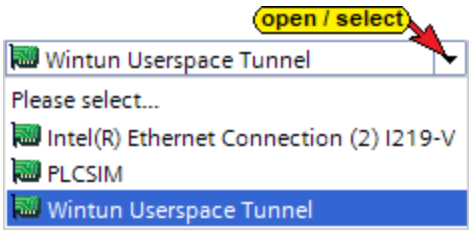


In the Online Access dialog box, select the settings as follows:

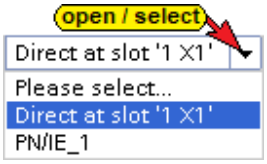
The ***Type of PG/PC interface*** must be selected according to the hardware configuration of the CPU.



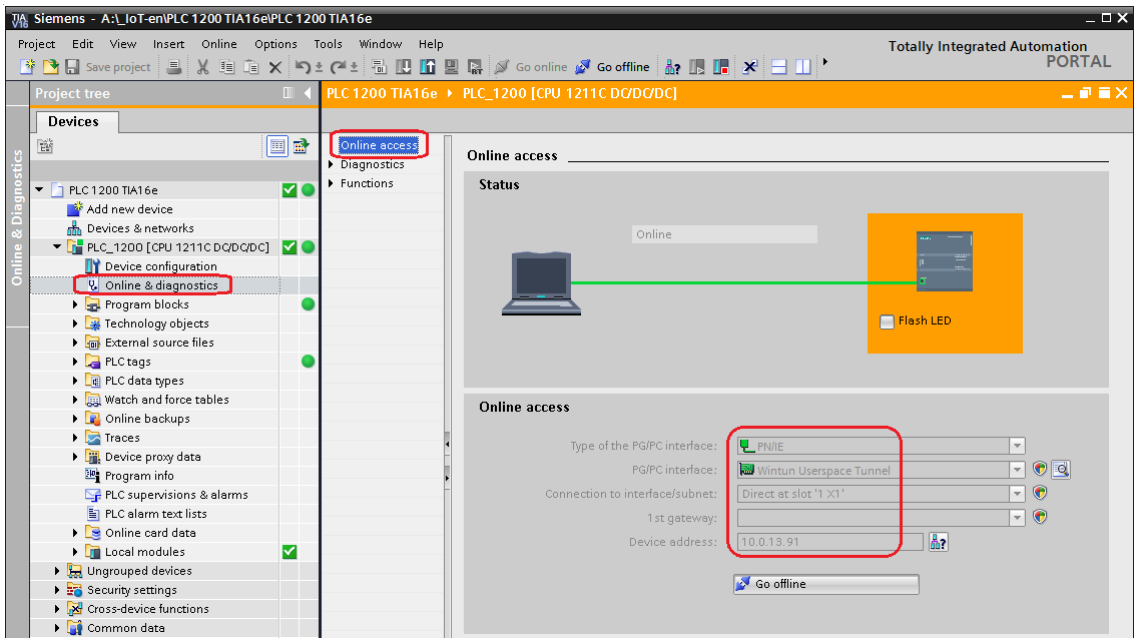
Wintum Userspace Tunnel must be specified as the PG / PC interface if there is a direct connection between the CPU and IBH Link IoT / control level.



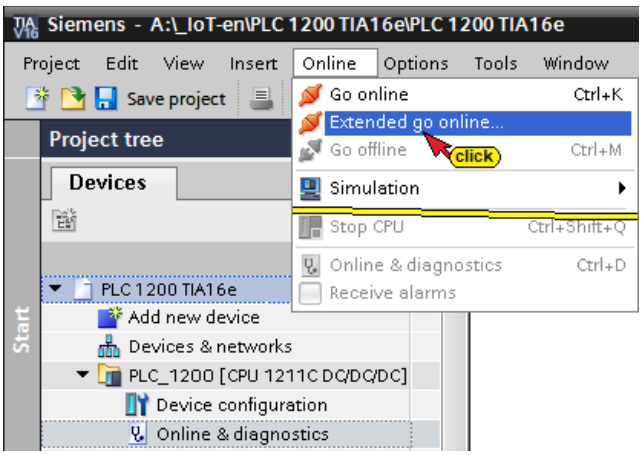
The physical location or the name of the Ethernet connection must be specified at ***Connection to interface/subnet***. This selection is only available if a network is configurated.

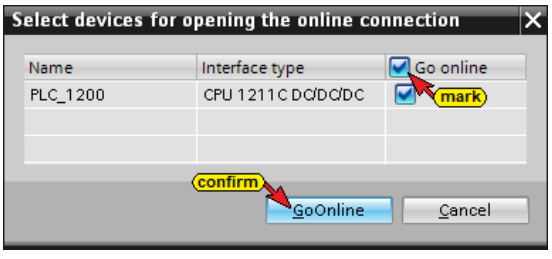


The online connection to the CPU1200 is established.

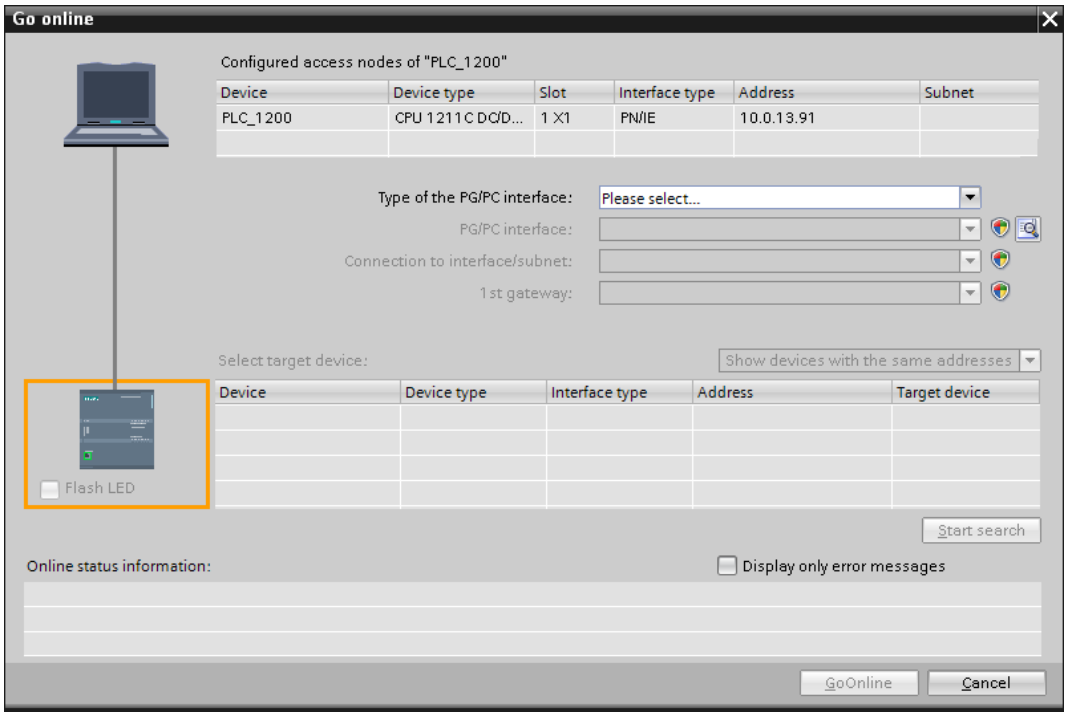


Extended go online access – Online access dialog box



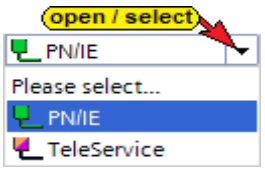


The Go online dialog box opens.

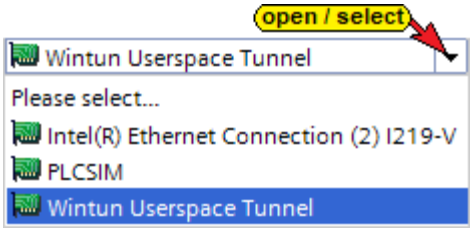


In the *Go online* dialog box select the following settings:

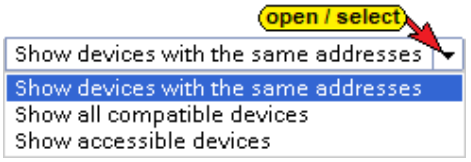
The ***Type of PG/PC interface*** must be selected according to the hardware configuration of the CPU.



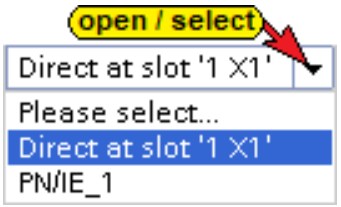
Wintum Userspace Tunnel must be specified as the PG / PC interface if there is a direct connection between the CPU and IBH Link IoT / control level.



Show device with the same address must be selected as the target device.



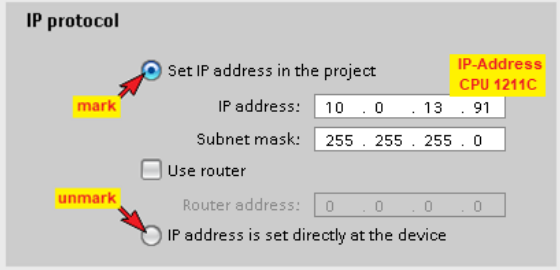
The physical location or the name of the Ethernet connection must be specified at ***Connection to interface/subnet***. This selection is only available if a network is configurated.



Note:

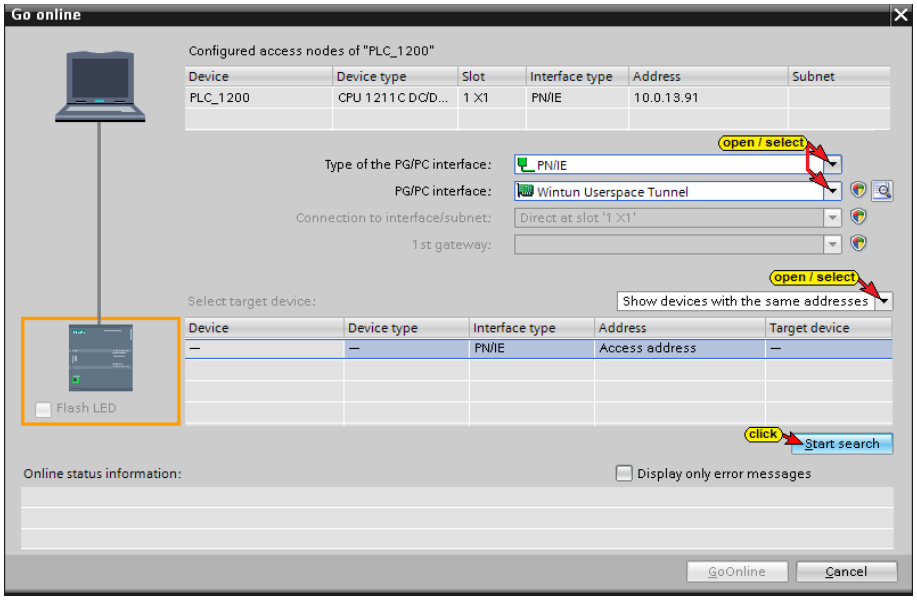
If the command ***Show device with the same address*** is not available, no connection to the CPU can be established.
In the hardware configuration of the CPU, the option ***IP address is set directly at the device*** must be deactivated.

Deactivate ***IP address is set directly on the device.***

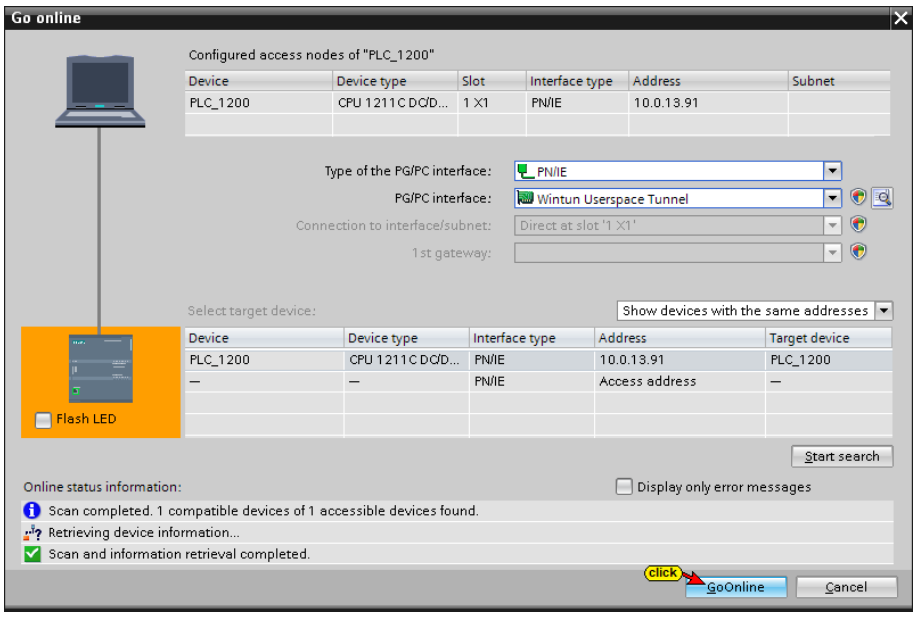


Search – Go online

Clicking the ***Start search*** button attempts to establish an online connection to the CPU.

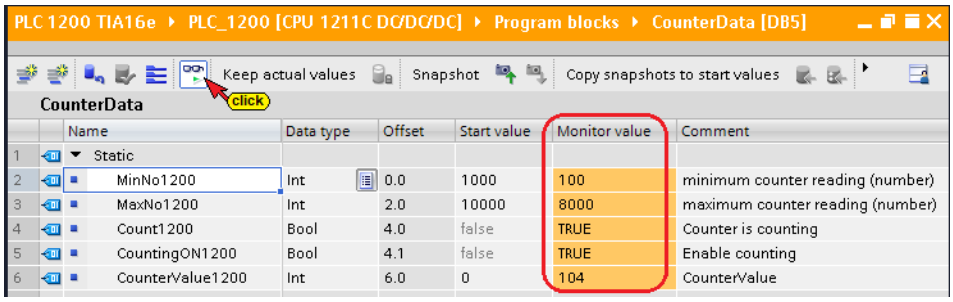


If the CPU to be connected is found, further data exchange is enabled with a click on the ***Go Online*** button.

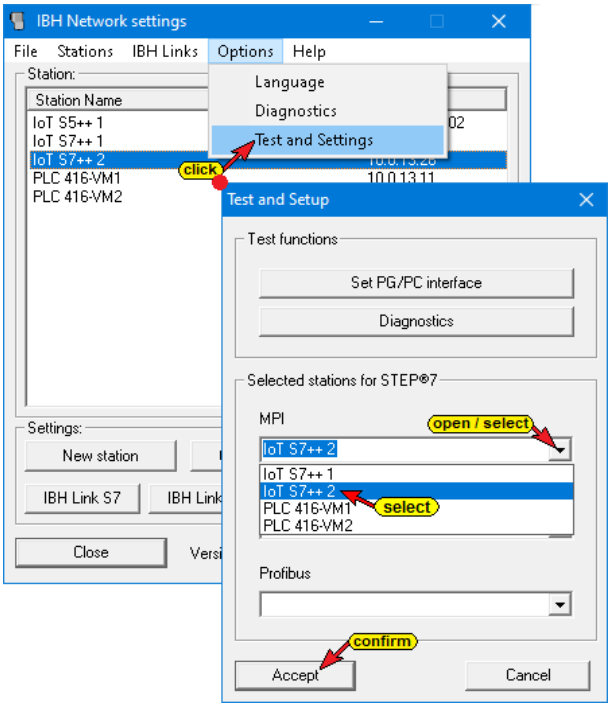


The online connection to the CPU1200 is established.

Status CPU 1200 – data block CounterData [DB5]



CPU 312 TIA16e– IoT S7++2 – IP address 10.0.13.26

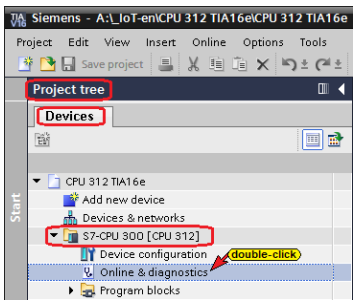


The CPU 312 is connected to the control level of the IBH Link IoT via an ***IBH Link S7++*** (IP address 10.0.13.26).

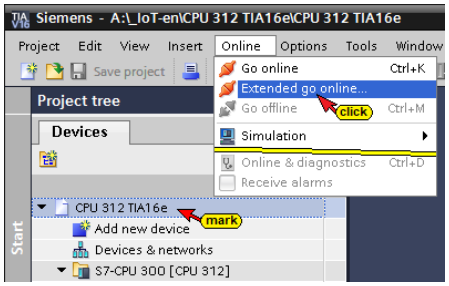
The ***IBH Link S7++ (IoT S7++2 – IP address 10.0.13.26)*** must be selected. The project CPU is addressed via its MPI address. The IBHNet driver of the IBH Link S7++ automatically assigns the IP address to the MPI address. The IBH Link S7++ is connected to the IBH Link IoT / control level.

There are several ways to establish an online connection in the TIA Portal.

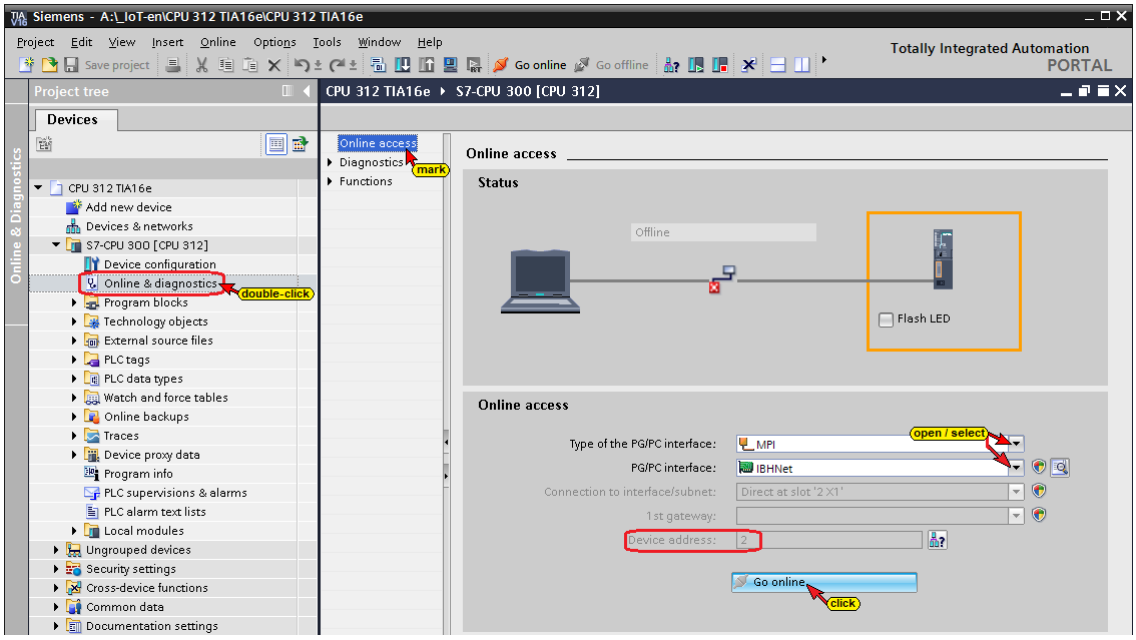
1. ***Project tree / devices*** (S7-CPU 300) ***/ online & diagnostics***.
   The same command is available in the Online menu. A double-click opens the Online access window. Settings must be made here.



2. ***Online / Extended go online...***
   The command opens the ***Go online*** dialog box. There are other ways to open the Go online dialog box. The required settings are identical.

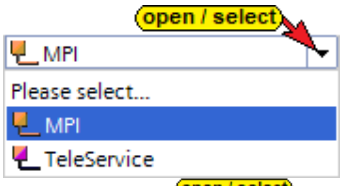


Online & diagnostics – Online access window

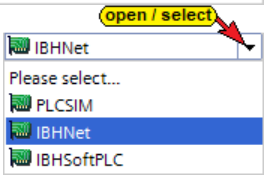


In the Online Access dialog box, select the settings as follows:

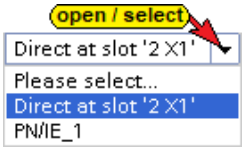
The ***Type of PG/PC interface*** must be selected according to the hardware configuration of the CPU (MPI interface).



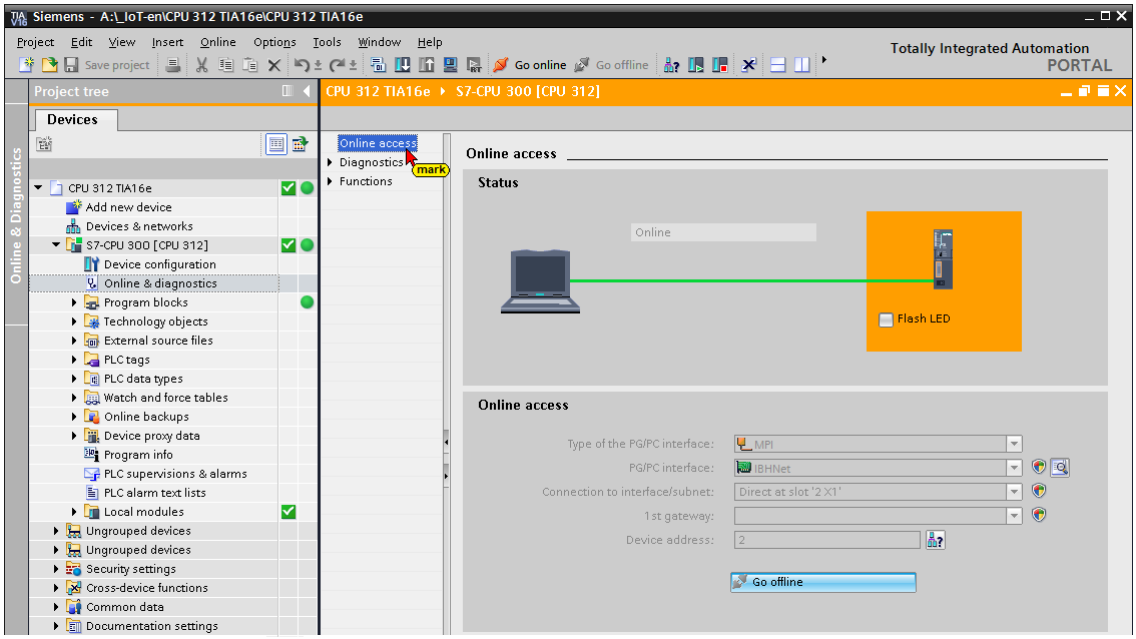
IBHNet must be defined as the PG / PC interface if an IBH Link S7 ++ is used as the connection between CPU and IBH Link IoT / control level.



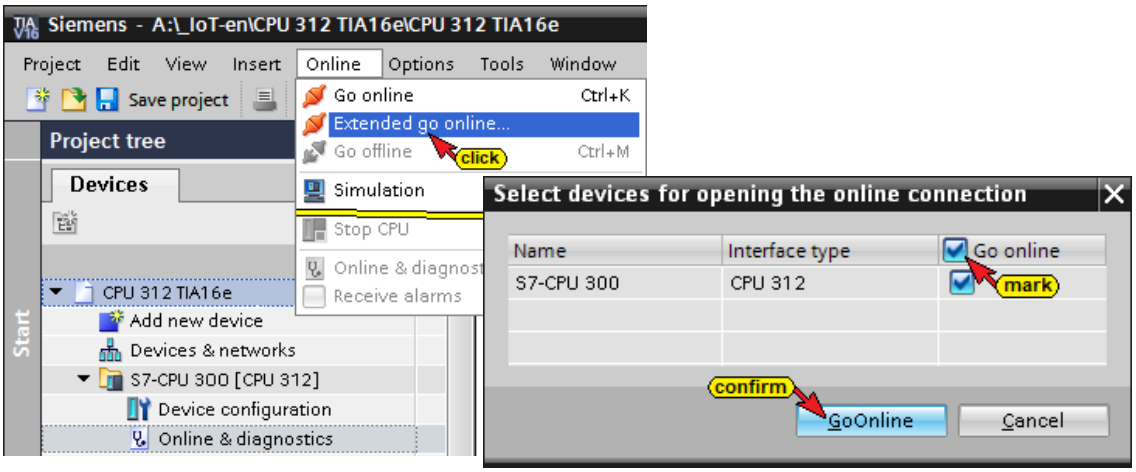
The physical location or the name of the Ethernet connection is only available if a network is configurated.



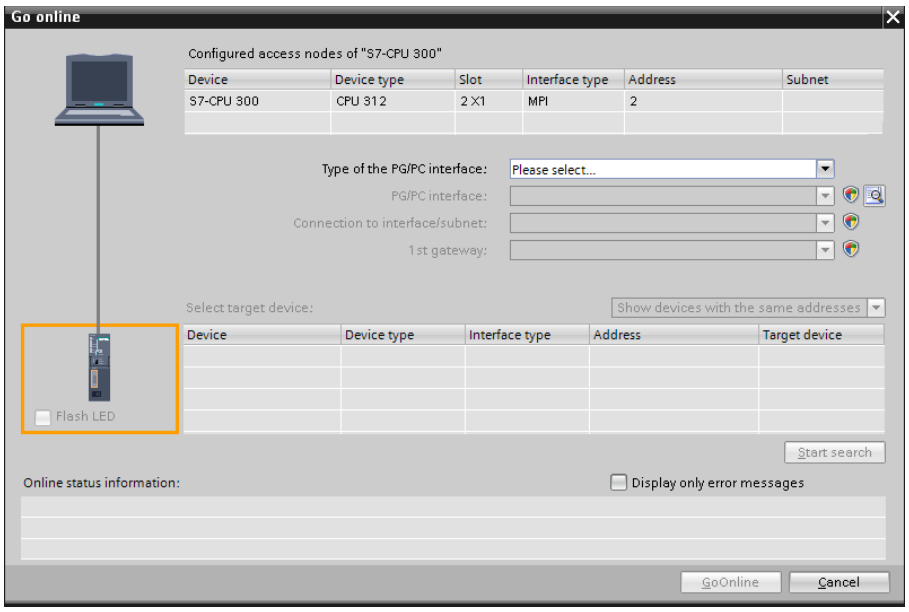
The online connection to the CPU312 is established.



Extended go online access – Online access dialog box

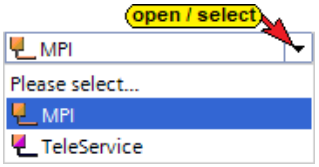


The Go online dialog box opens.



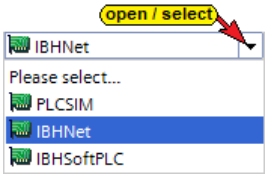
In the Online Access dialog box, select the settings as follows:

The ***Type of PG/PC interface*** must be selected according to the hardware configuration of the CPU (MPI interface).

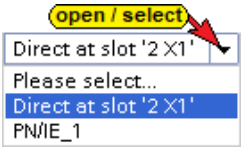


IBHNet must be defined as the PG / PC interface if an IBH Link S7++ is used as the connection between CPU and IBH Link IoT / control level.

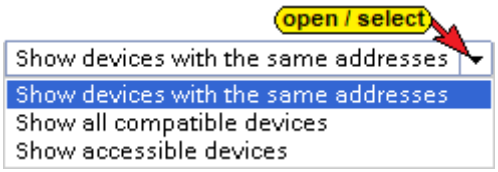
The physical location or the name of the Ethernet connection is only available if a network is configurated.



The physical location or the name of the Ethernet connection is only available if a network is configurated.

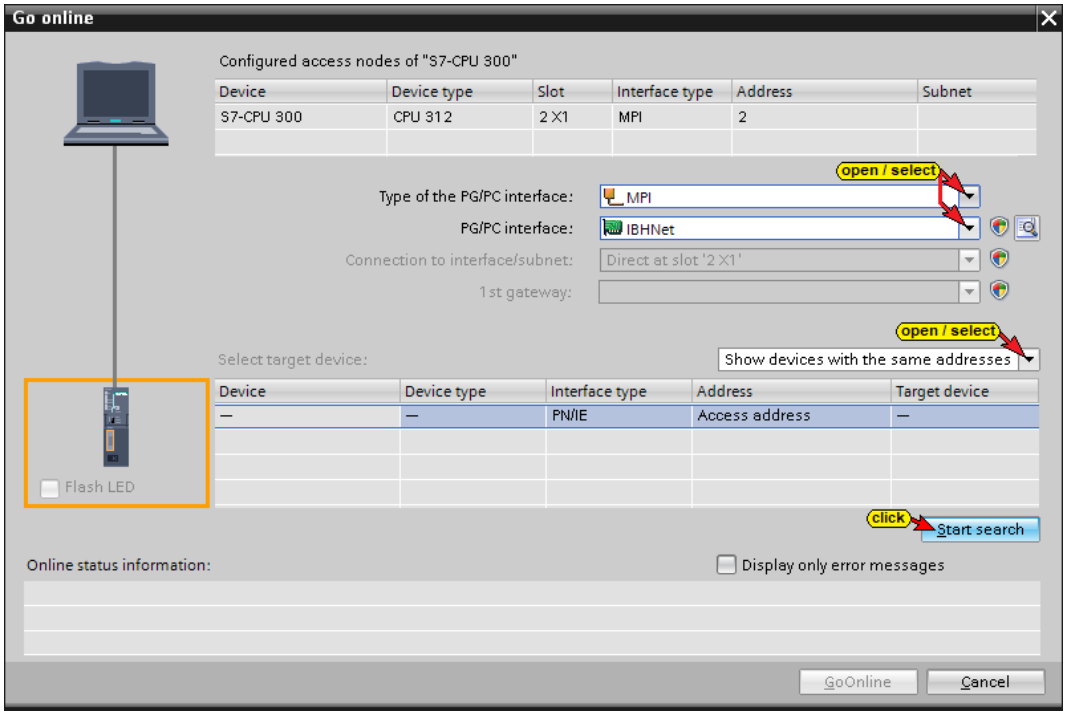


Show device with the same address must be selected as the target device.

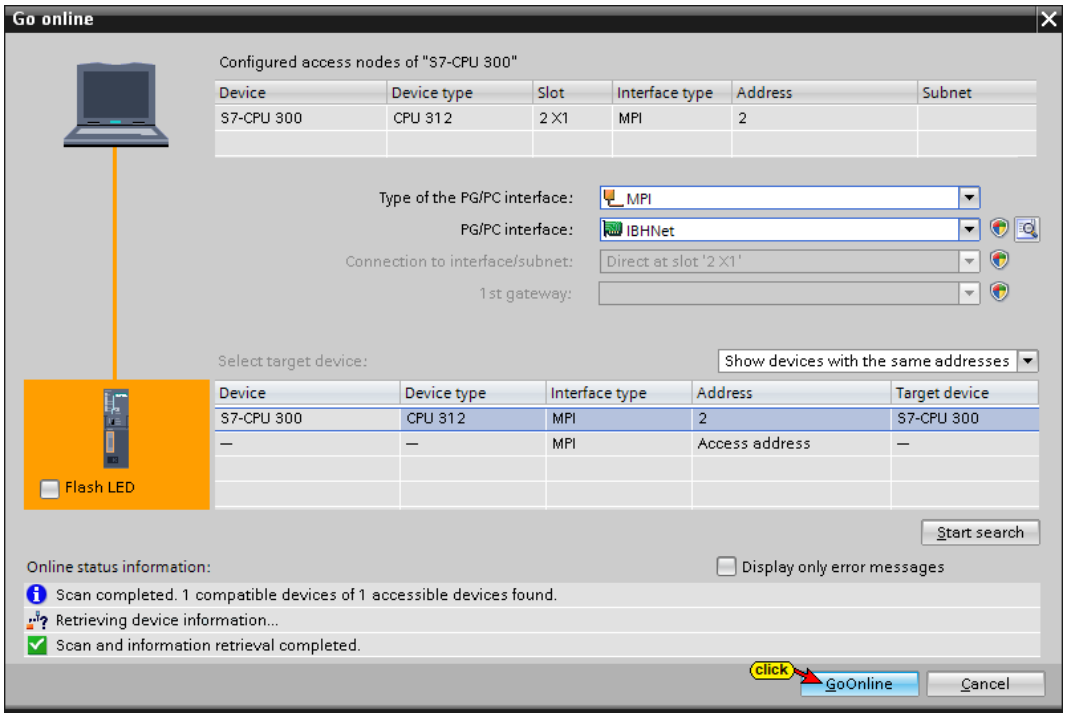


Search – Go online

Clicking the ***Start search*** button attempts to establish an online connection to the CPU.

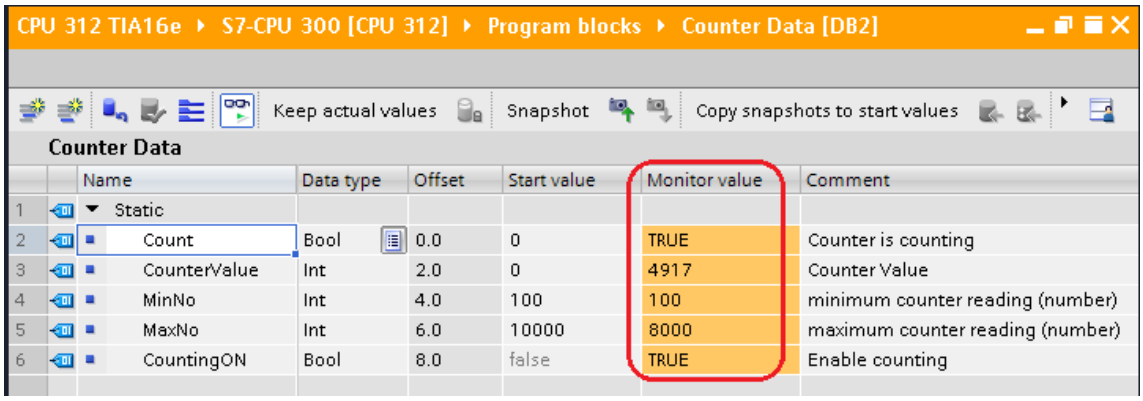


If the CPU to be connected is found, further data exchange is enabled with a click on the ***Go Online*** button.



The online connection to the CPU300 is established.

Status CPU 300 – data block Counter Data [DB2]

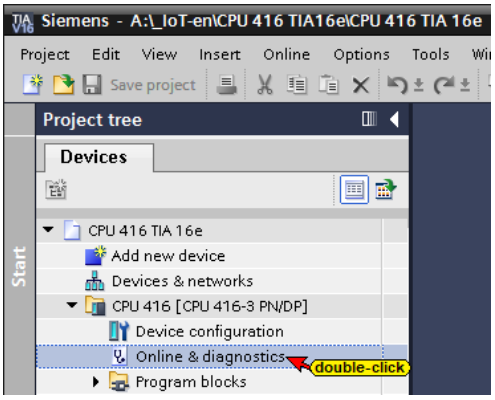


2.1.9 CPU 416 TIA 16e – (IP-Adresse 10.0.13.9)

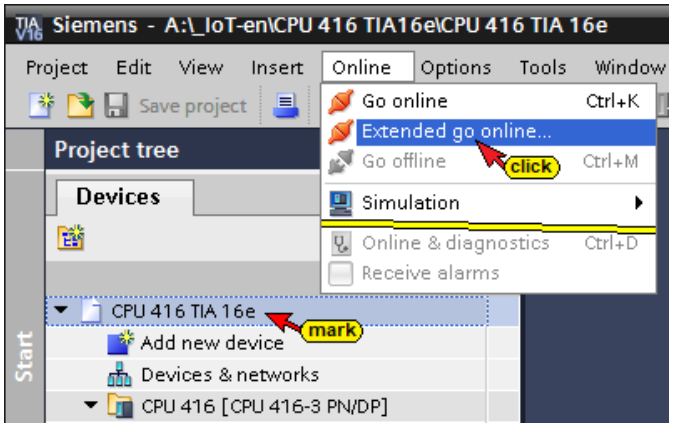
There are several ways to establish an online connection in the TIA Portal. The CPU of the opened project must have the same IP address as the CPU that is connected to the IBH Link IoT / control level.

The CPU 416 is connected to the control level of the IBH Link IoT (IP address 10.0.13.9).

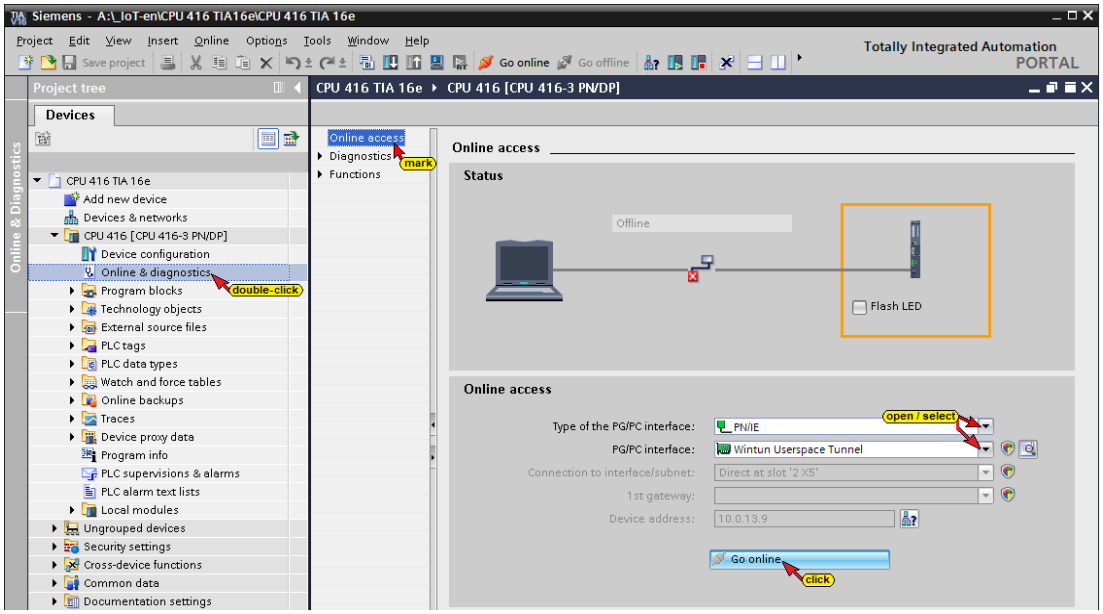
1. ***Project tree / devices*** (CPU 416) ***/ online & diagnostics***.
   The same command is available in the Online menu. A double-click opens the Online access window. Settings must be made here.



2. ***Online / Extended go online...***
   The command opens the ***Go online*** dialog box. There are other ways to open the Go online dialog box. The required settings are identical.

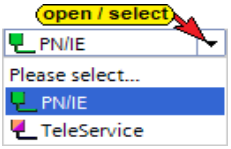


Online & diagnostics – Online access window

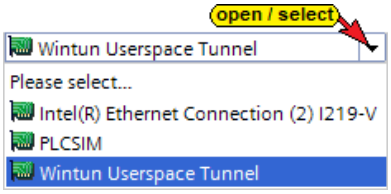


In the Online Access dialog box, select the settings as follows:

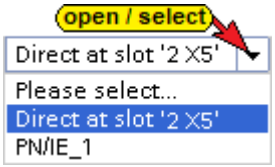
The ***Type of PG/PC interface*** must be selected according to the hardware configuration of the CPU.



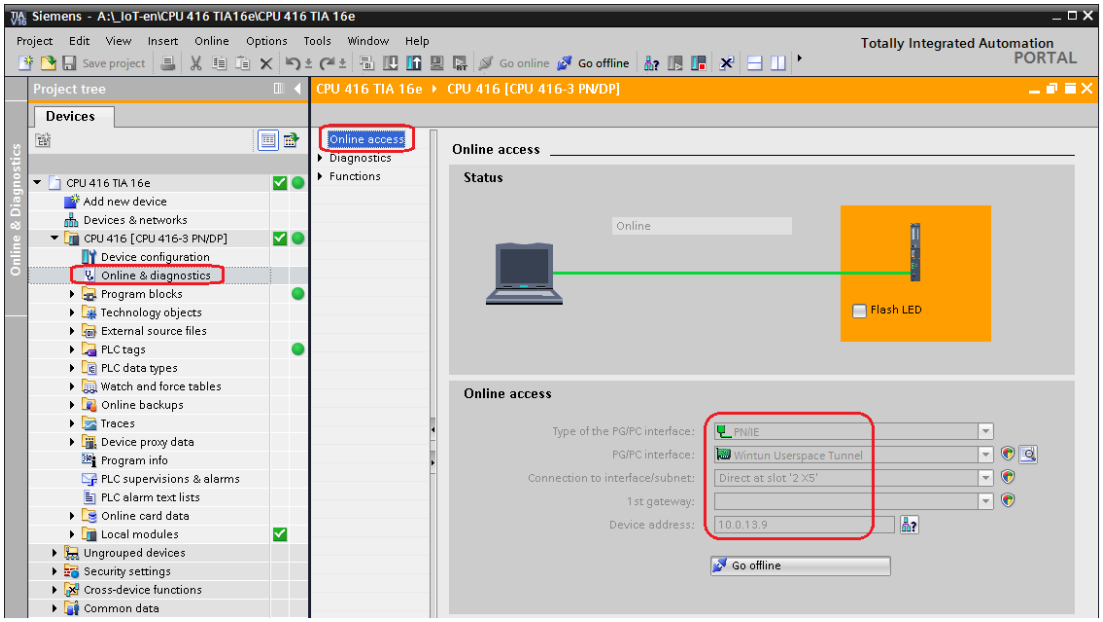
Wintum Userspace Tunnel must be specified as the PG / PC interface if there is a direct connection between the CPU and IBH Link IoT / control level.



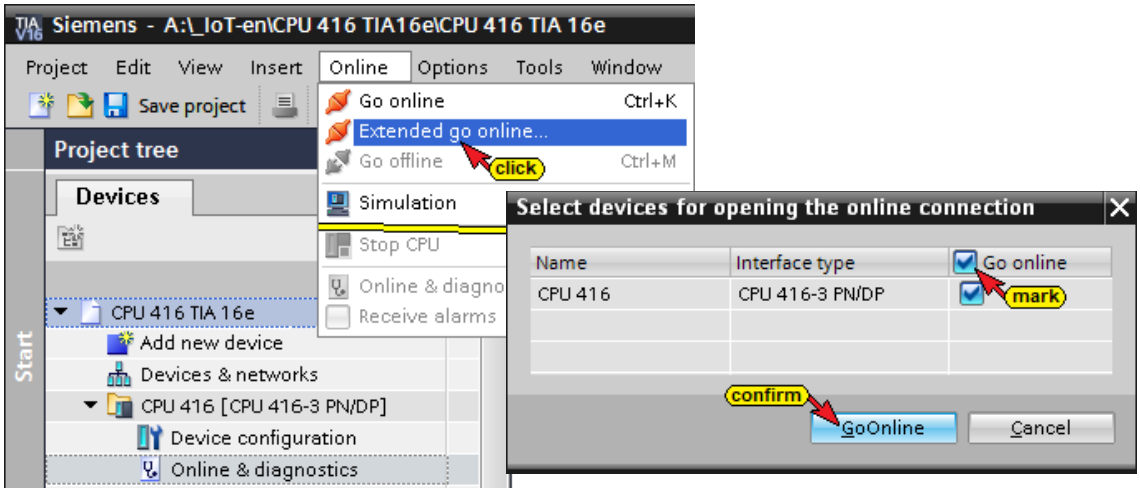
The physical location or the name of the Ethernet connection must be specified at ***Connection to interface/subnet***. This selection is only available if a network is configurated.



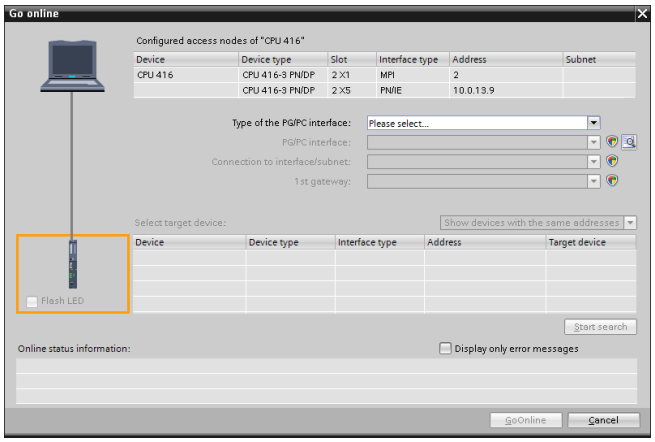
The online connection to the CPU 416 is established.



Extended go online access – Online access dialog box

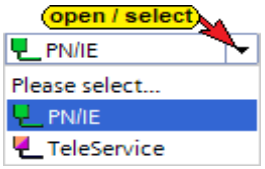


The Go online dialog box opens.

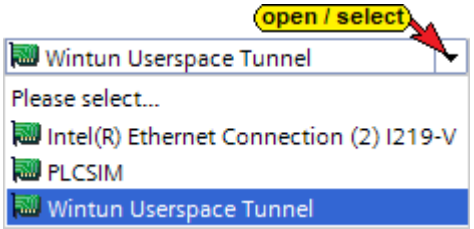


In the *Go online* dialog box select the following settings:

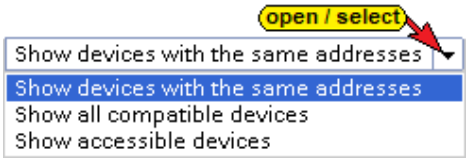
The ***Type of PG/PC interface*** must be selected according to the hardware configuration of the CPU.



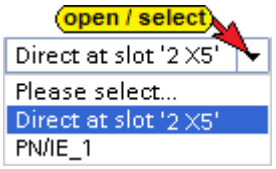
Wintum Userspace Tunnel must be specified as the PG / PC interface if there is a direct connection between the CPU and IBH Link IoT / control level.



Show device with the same address must be selected as the target device.

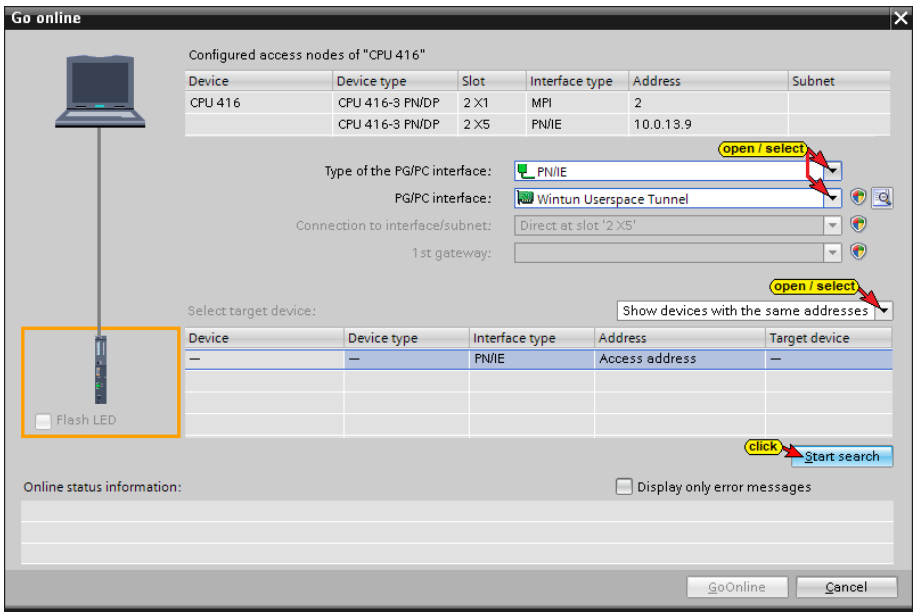


The physical location or the name of the Ethernet connection must be specified at ***Connection to interface/subnet***. This selection is only available if a network is configurated.

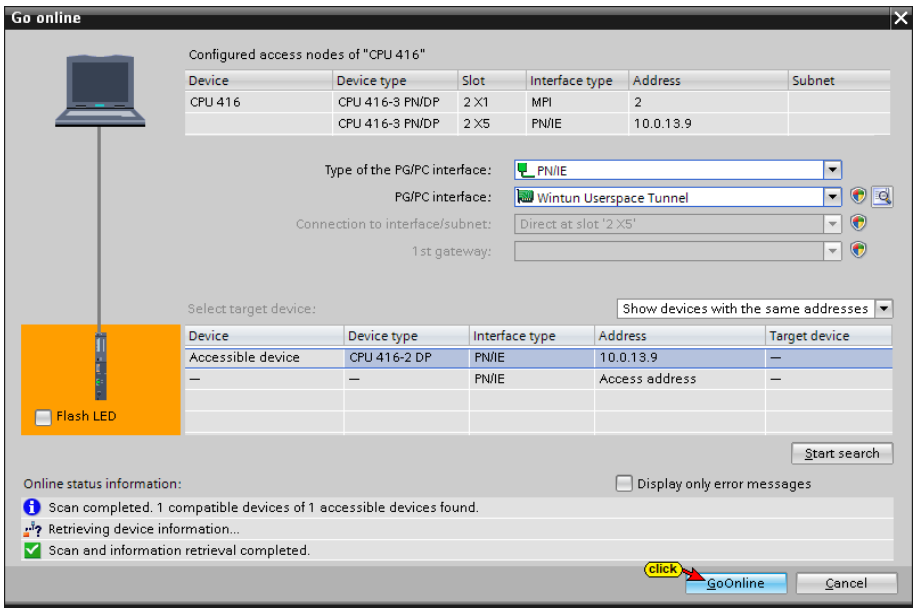


Search – Go online

Clicking the ***Start search*** button attempts to establish an online connection to the CPU.

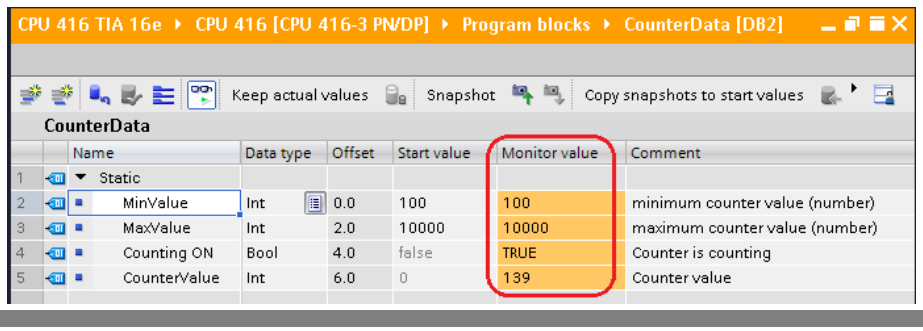


If the CPU to be connected is found, further data exchange is enabled with a click on the ***Go Online*** button.

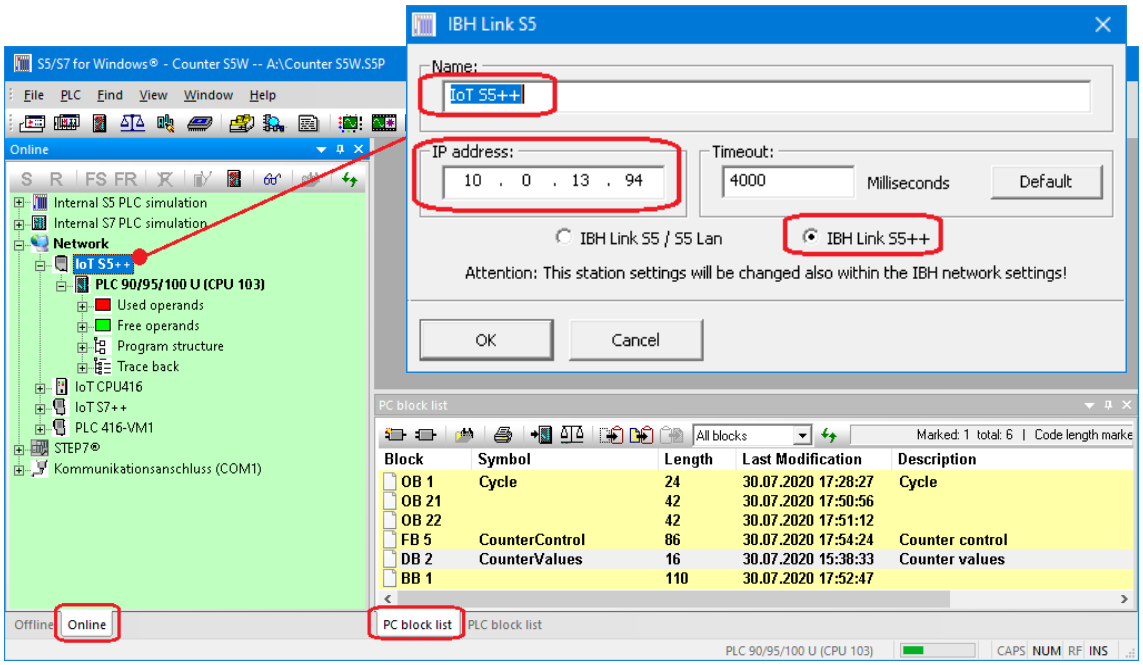


The online connection to the CPU416 is established.

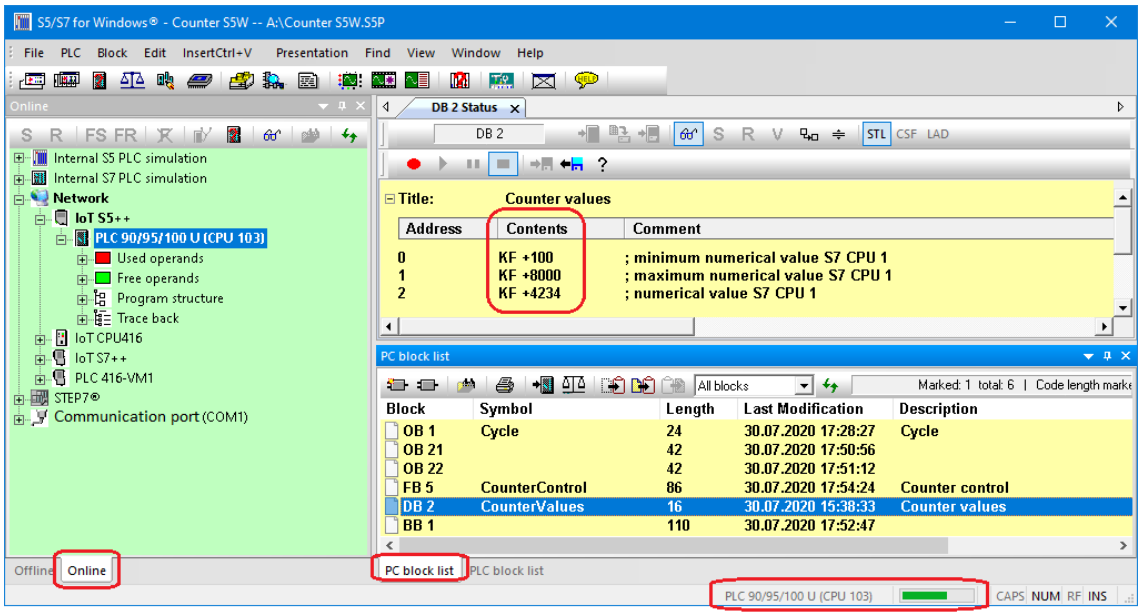
Status CPU 416 – data block CounterData [DB2]



S5 for Windows – CPU103-S5++ IoT – IP address 10.0.13.94



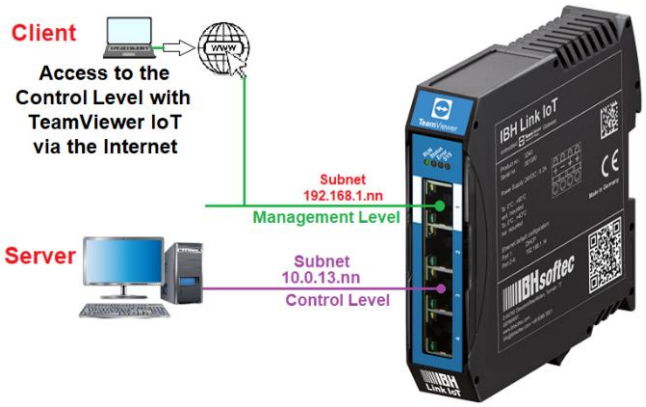
Status S5 CPU 103



2.2 Access to a PC - Remote Desktop.

It should be possible to access a PC via an IBH Link IoT, which is connected to the same subnet as the control level.

To ensure that the connection and the data traffic are secure, TeamViewer uses end-to-end encryption using RSA public / private key exchange and 256-bit AES session encryption. In addition, the IBH Link IoT has a firewall between the management and control level.



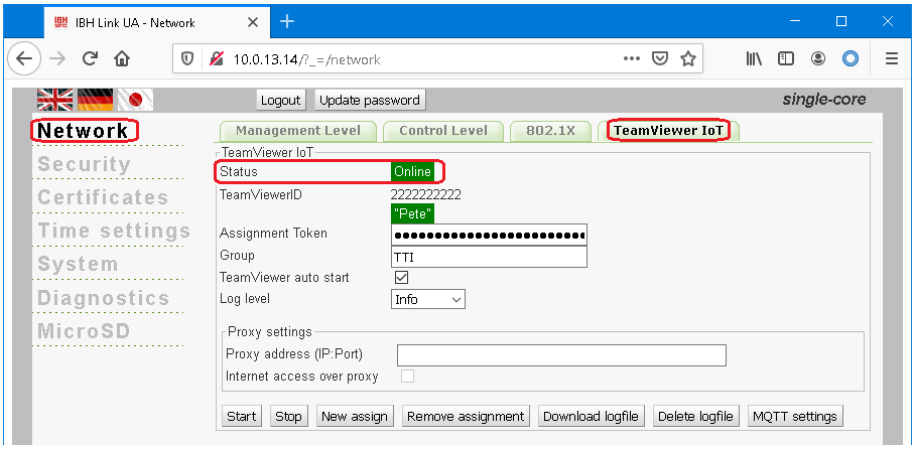
Remote desktop refers to the remote access to the desktop of a computer. Application programs are executed on one computer (server) and displayed and operated on another computer (client). In contrast to screen sharing, no user must log on locally to the server.

A remote desktop session runs independently of any other session that may be running.

2.2.1 Preparation of IBH Link IoT and Server (PC)

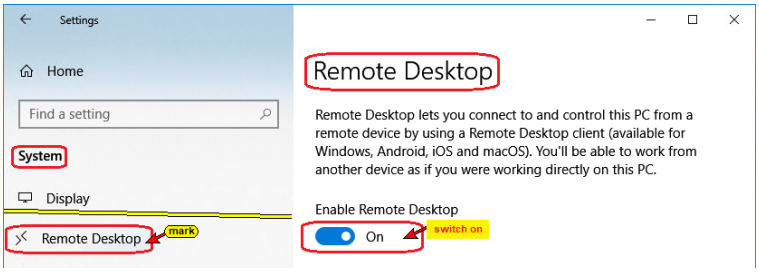
The management level port of the IBH Link UA has direct access to the Internet. The ***TeamViewer IoT Status*** must be ***Online***.

TeamViewer IoT Status



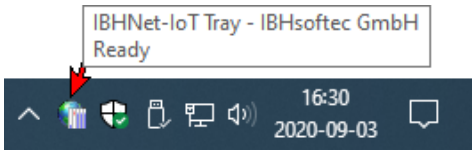
2.2.2 Local PC (client)

Remote Desktop is activated on the client PC. As an example, Windows 10 - Settings.



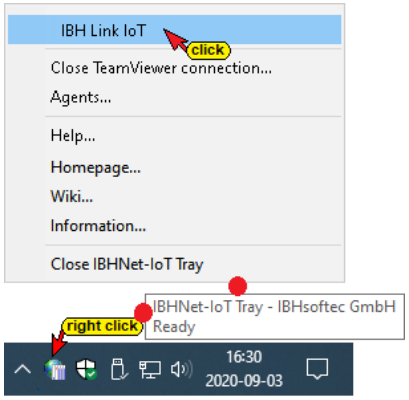
The icon to start the remote desktop connection is available in the start menu under Windows accessories.

- The ***TeamViewer software*** is installed on this PC.
- The ***IBHNet-IoT software*** is installed. The service is displayed in the ***IBHNet-IoT Tray*** in the task bar.

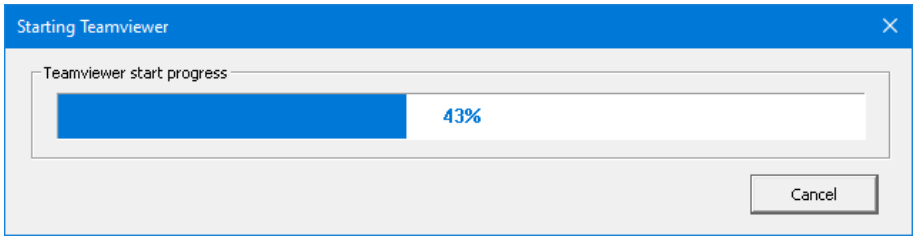


- The name (e.g. ***IBH Link UA SC***) given in the ***TeamViewer-Shortcut*** dialog box is transferred to the ***TeamViewer account***.
- Start the ***TeamViewer software*** with a double-click.

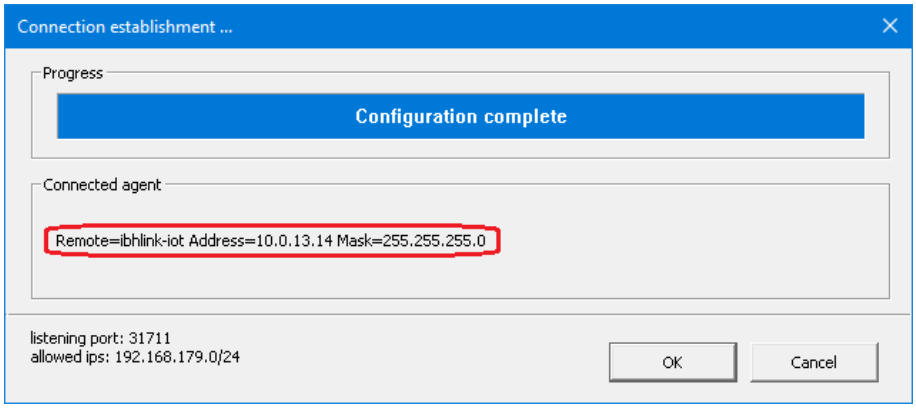
- Right-click on the ***IBHNet-IoT Tray*** icon to open the context menu. The devices registered with the ***TeamViewer account*** are listed in the upper area of the context menu.



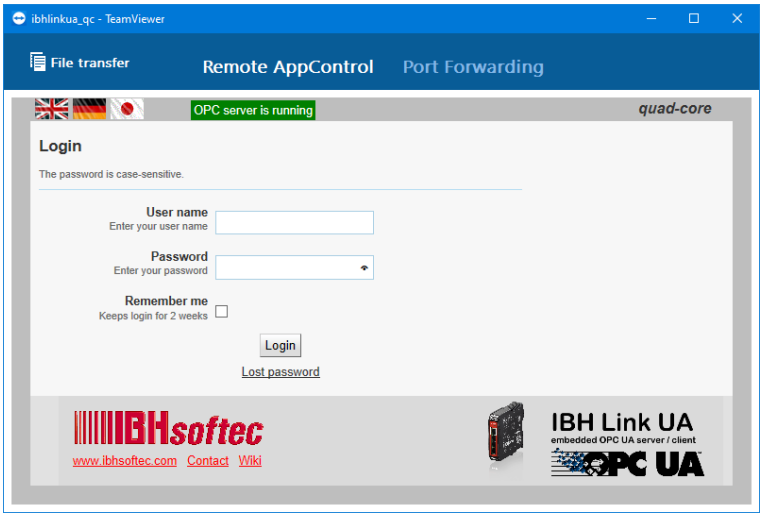
- With a click on ***IBH Link UA SC***, the connection to the ***ibhlinkua_sc*** address is established via the Internet.



The establishment of the connection is displayed.



The establishment of the connection is displayed and the ***Port Forwarding*** of the Remote ***AppControl*** are displayed.

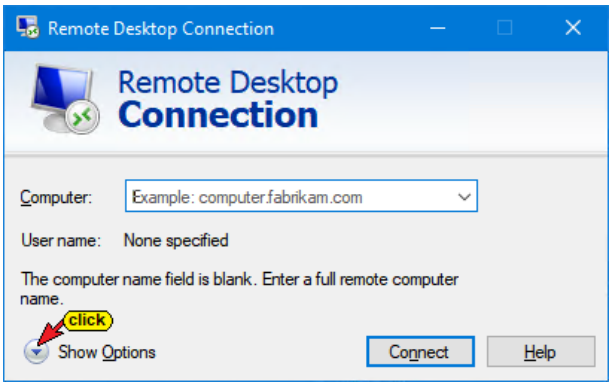


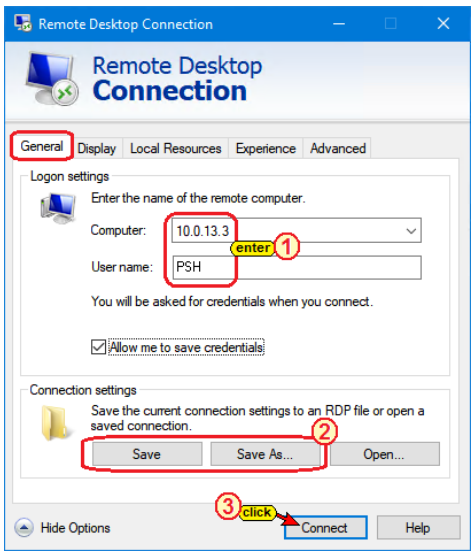
To access the individual PCs (devices) no registration to the ***IBH Link UA*** is necessary.

Establish remote desktop connection

Double-click the Remote Desktop Connection icon.

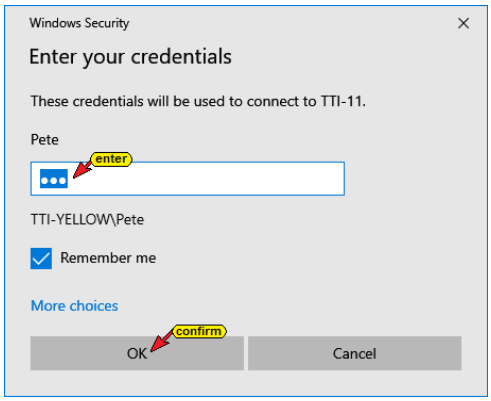
In the Remote Desktop Connection dialog box, click the ***Show Options*** button.





Enter the computer ***(IP address)*** and username in the opened dialog box. These settings can be saved. Clicking the Connect button opens the dialog box for entering the password.

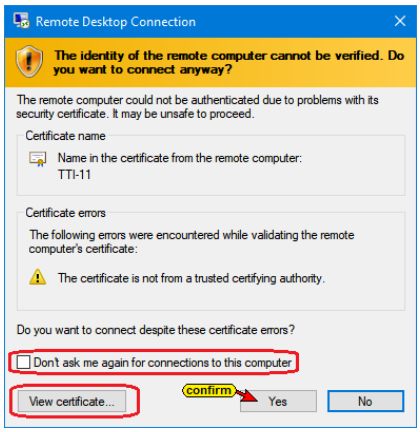
Enter User and Password dialog box



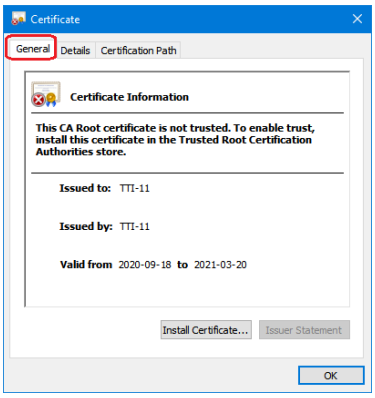
The establishment of the connection is displayed.

Remote computer Certificate verification

If the certificate of the remote computer is not known, a corresponding message is displayed.

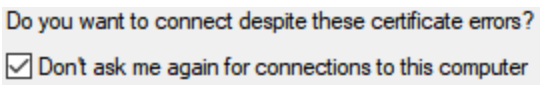


The existing certificate on the remote computer can be viewed.



If the remote computer / certificate is trustworthy, the connection can be established (click ***Yes***).

The corresponding option must be activated so that there is no further inquiry when the connection to the PC is established again.



The remote computer's desktop appears. All programs on the PC can be executed.