Platform MX6
Software option S109
VPN Client + IXON Agent

1 Identification

Identification	
Option ID	S109
Order number	S-05000311-0000
Short name	VPN Client + IXON Agent
Brief description	With this software option it is possible to integrate the controller into a virtual private network (VPN). The applied VPN Technology is OpenVPN. The extension for IXON has additional features like Cloud Logging or Cloud Notify over OPC-UA or ModbusTCP.
Revision ID document	V4.0

2 System requirements and restrictions

System requirements and restrictions	
Supported Platforms and devices	Berghof PLC devices of the MX6 platform (e.g.: MCs, CCs, DCs). Additional information regarding availability and compatibility can be found in options section of the product catalog.
Firmware	MX6-PLC Version 1.18.4 or higher for OpenVPN Client MX6-PLC Version 1.23.0 or higher for IXON Agent
Additional requirements	— OpenVPN Server or compatible OpenVPN portal — IP network connection to the OpenVPN Server — IXON account - https://connect.ixon.cloud/login — S-05000801-0000 - IX-Agent Cloud registration is required to activate device in the cloud
Restrictions	— Only Host-to-Host connectivity is supported

BERGHOF

3 Product description

With this expansion it is possible to connect the controller to a VPN Server and thus to a distributed network structure by using the VPN technology via an encrypted IP connection. Due to the encryption, the linking of network members over unsecure networks (e.g. Internet) is still possible. A typical use case is, the linking of distant locations for remote services or data exchange between headquarters and field locations, based on the IP protocol.

This expansion provides an OpenVPN Client on the PLC that connects to an already configured VPN Server.
By using the plc integrated web-configuration, the configuration files (key, certificate and OpenVPN config file) are loaded onto the PLC.
During boot-up the VPN connection to the server is established by the PLC. Starting there the PLC is registered in the VPN and can be reached over the VPN. Depending on the server configuration it is also possible for the PLC to reach other VPN members. The VPN connection is assigned its own IP network range, which is defined in the configuration data of the VPN server.

The PLC establishes a host to host connection. Therefor it is possible to reach the PLC via its special VPN IP address. An access over this IP address to other network members of the local network of the PLC is not possible. But it is still possible to login into other CODESYS PLCs in the same local network as the VPN PLC with help of the CODESYS Gateway functionality.

The PLC with the VPN Client can operate behind a Firewall (Router), as no outside connections are necessary for the connection to the VPN server. For a flawless operation, many routers will need some additional configuration in order to provide a working internet connection, so that the PLC can establish a connection to the VPN Server over the internet.

After the installation of the software expansion it will be possible to use the VPN functions. Only after the installation of the software expansion it will be possible to access the VPN configuration in the web interface of the PLC.

The integrated support of the IXON Cloud Service offers besides the already described remote access via a VPN connection extended features like the display of web pages and VNC Server. Optionally, the Cloud Logging functionality can be activated with order no. S-05000802-0x0x, which allows to transfer data points via OPCuA or ModbusTCP into the Cloud, to store them and to display them visually via different widgets. You can order between 1000 and 20000 points/H and a runtime of 1 - 5 years the suitable Cloud Logging package. With the order no. S-05000803-0000 Cloud Notify, the IXON Cloud system is supplemented by an alarm function, whereby data is transferred from the controller to the Cloud and monitored according to values set by the user, in the event of a limit value being exceeded, a warning email is sent automatically to the user set in the Cloud Notify.
A complete overview of all functions of the IXON Cloud can be found in the online help: https://support.ixon.cloud/hc/en-us

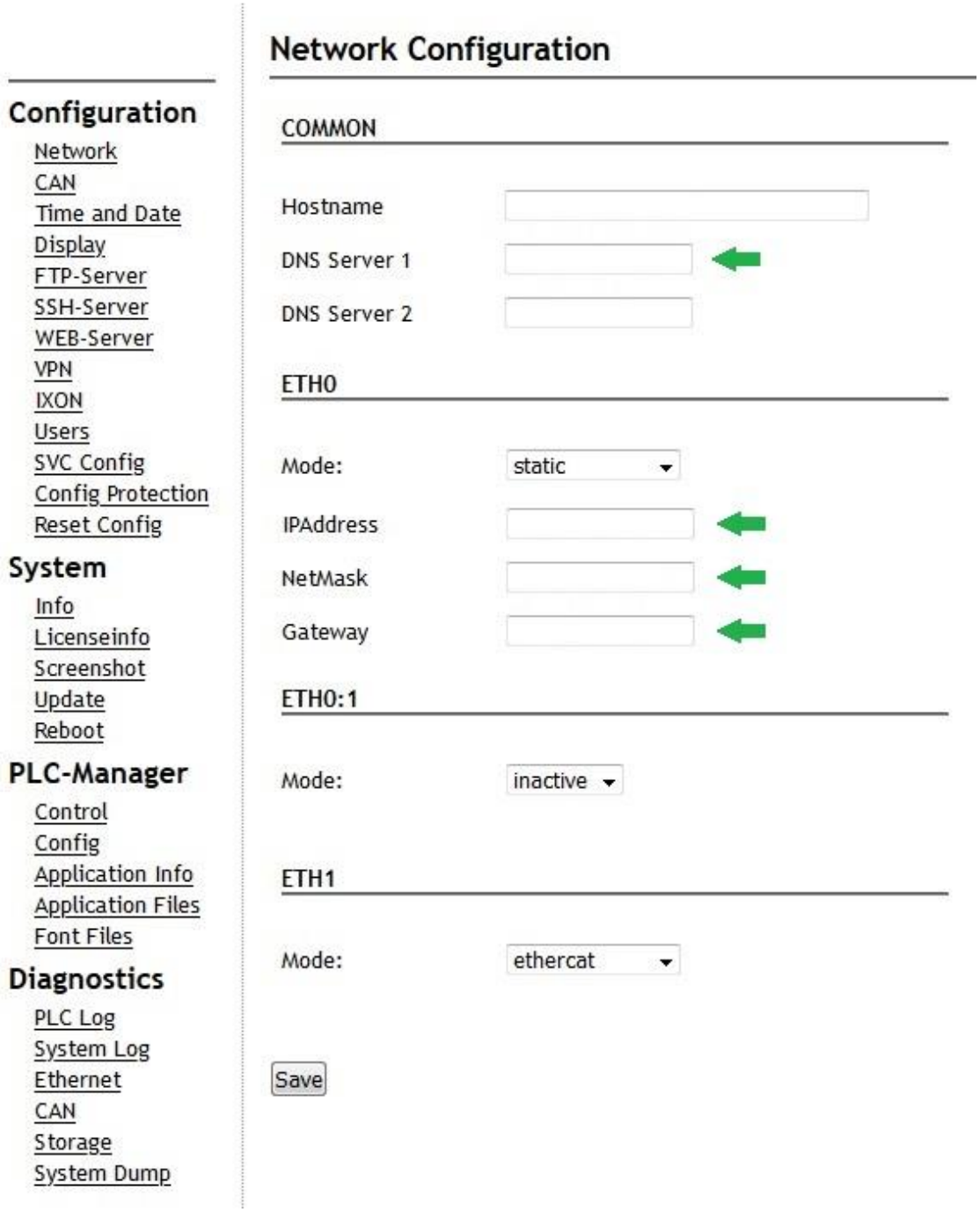
4 Technical data

Technical Data	
Integrated Version	OpenVPN Version 2.4.8 (or newer)
Compression algorithm	LZO
OpenSSL Library	OpenSSL Version 1.0.2p (or newer)

5 Quick Start Guide

5.1 Network configuration of the PLC

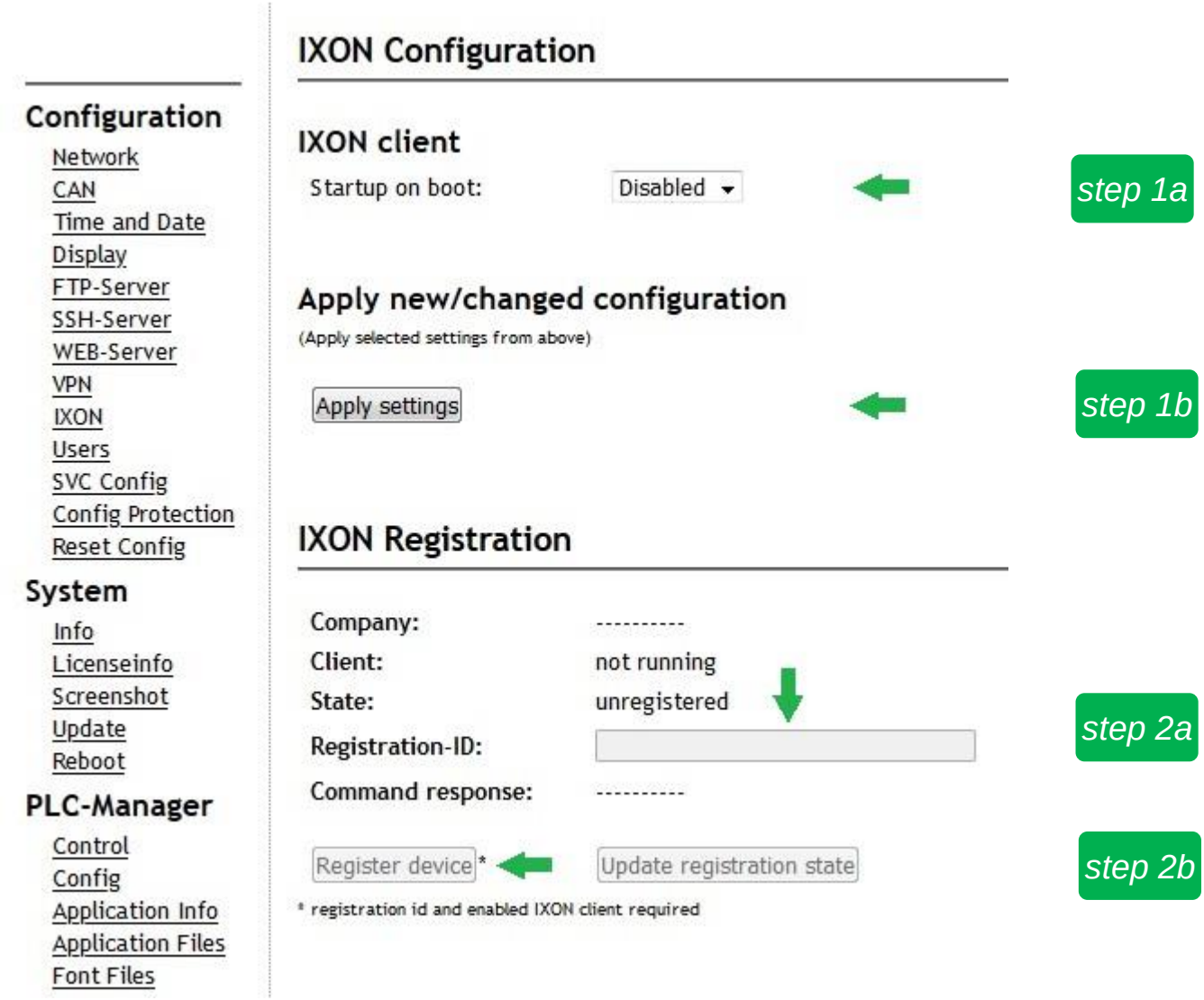
To connect to a VPN-server specific data has to be registered in the network settings. The IP address of at least one name server (DNS), the IP address of the gateway which provides access to the internet and the net mask, are needed (see green arrows). This information has to refer to the network in which the PLC is running.



The PLC should have an own static IP address, which provides access to the internet.

5.2 IXON configuration

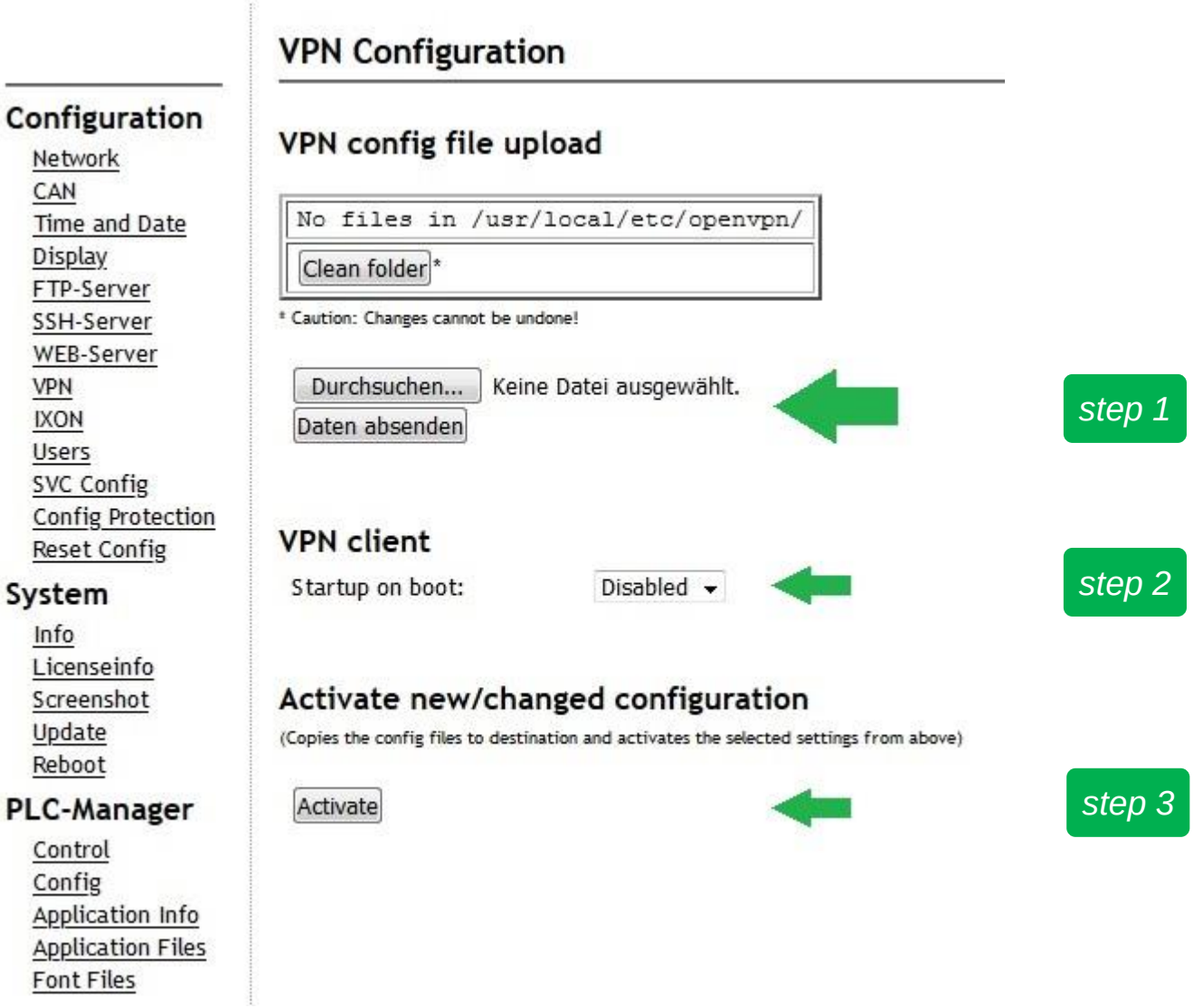
You can either use the IXON connection which uses it's own VPN configuration or use a dedicated VPN connection to an Open-VPN server. But you can't enable the IXON client and the VPN client at the same time. To successfully activate the PLC within IXON you will need an activation code from IXON (can be purchased directly from Berghof, order no. S-05000801-0000 - IX-Agent Cloud registration). If you only want to use OpenVPN you can head over to the next chapter.
The IXON client gets his configuration directly from the IXON servers, so you have to enable the client (step 1a) and apply the settings (step 1b). To start the IXON client and continue with the registration a reboot is required.



The registration of this PLC within IXON requires an registration of you (as person) or your company on the IXON website (https://connect.ixon.cloud/login). Once you were registered (following the steps from the IXON website) you will get a company id. This id is required to register your PLC within your IXON account. Select your company id and paste it into the Registration-ID field (step 2a). Make sure the company id matches the registration id. Then click on Register device to add this control to your IXON account (step 2b). After a few seconds the Command response should show a message about a successful registration and State should show registered. The registered control can now be activated with a valid activation code available from Berghof (order no. S-05000801-0000 - IX-Agent Cloud registration) .
To use the IXON VPN connection you have to download and install the VPN client software available on the IXON website. You will need administration rights to install it on your local PC. Once you have installed the client software no additional configuration is needed..

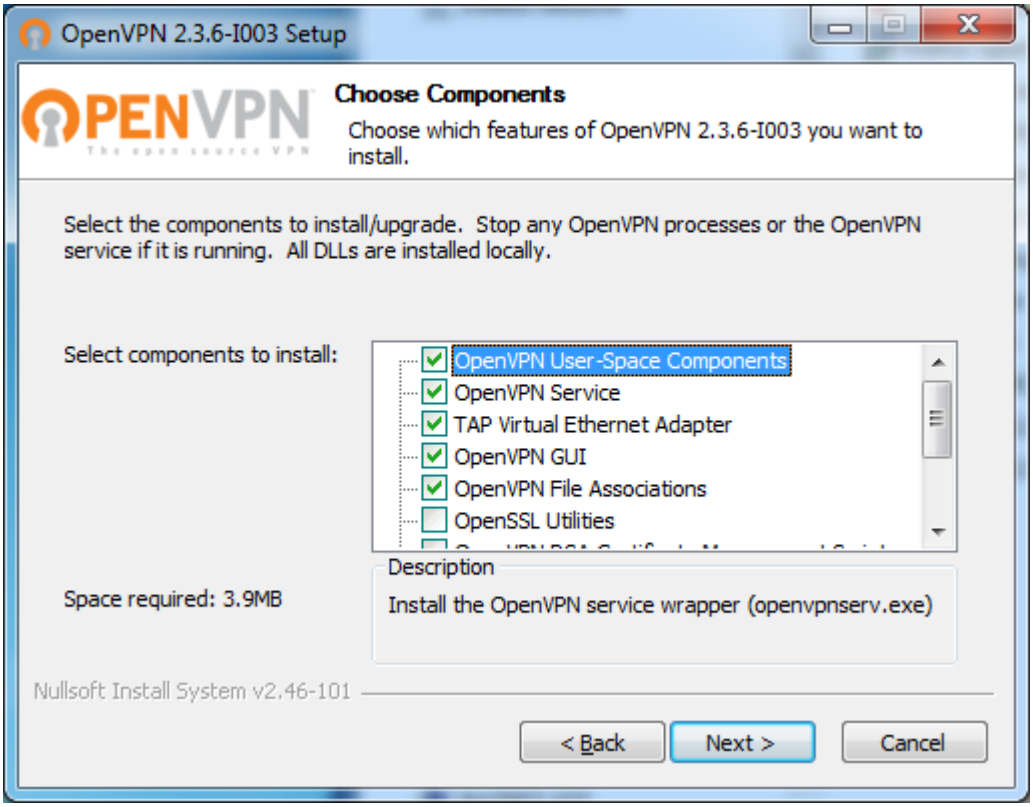
5.3 VPN configuration

You can either use a dedicated VPN connection to a VPN server or the IXON connection, which uses it's own VPN configuration and is independent from this VPN configuration. But you can't enable the VPN client and the IXON client at the same time. To configure this VPN connection, you have to upload the necessary configuration, key and certificate files to the control (step 1). This can be done within the web interface. You can either upload each file separate or all together as a ZIP file. Once all files are uploaded successfully, the VPN client can be enabled to startup on boot (step 2). Last step (step 3) is the activation of the configured VPN client. After a reboot the VPN connection is automatically set up with the configured VPN server (if all conditions are met). The connection remains as long as the internet connection is ensured and the PLC isn´t shut down. While doing a reboot the connection is aborted, after the booting procedure the connection is re-established.

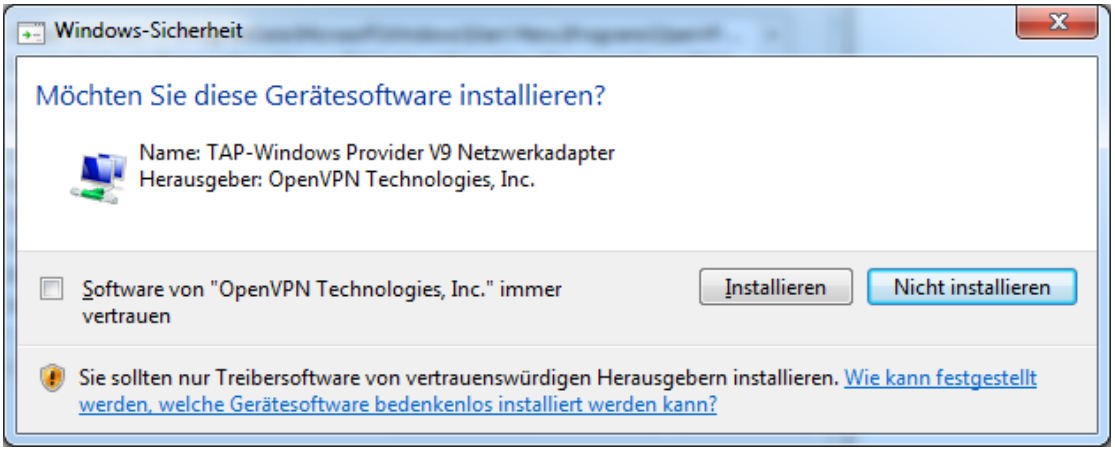


5.4 PC software installation

An OpenVPN client is necessary to provide a VPN connection from a PC. Further a configuration file and various certificate and key files are necessary for the encrypted connection set-up. These files are usually provided by the host of the VPN server.
Admin rights are needed to install the OpenVPN-client software, because specific entries in the routing table of the PC can only be done with the appropriate rights.
During the installation of the software the preselected components can be directly adopted. Further optional components are not necessary for the operation.



During the installation an additional network interface is installed. The appearing notification offers the options „install“ and „not install”, you need to select „install“ or the OpenVPN client won´t work.



5.5 PC software configuration

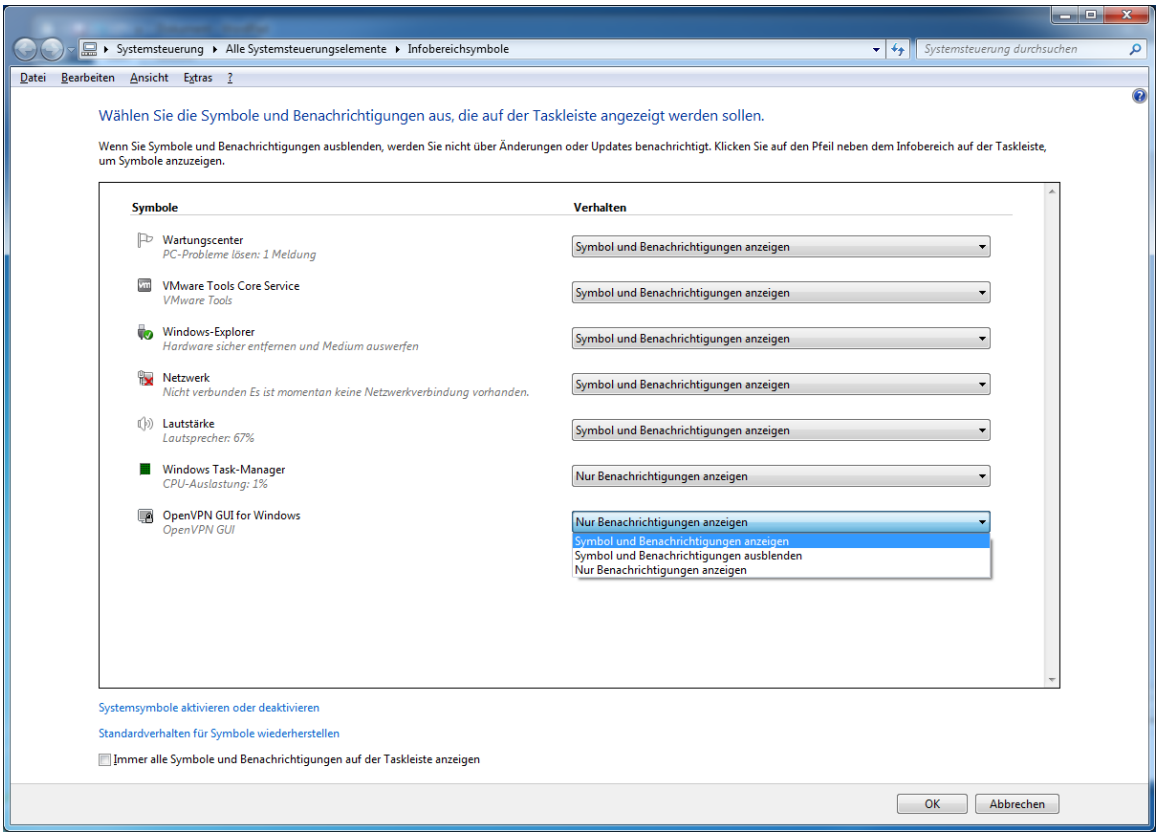
The client needs relevant information for the connection with the VPN server. Here for the VPN server provider offer specific configuration packages, which (usually) just need to be copied and unzipped into a relevant subfolder of the VPN client. Now the configuration of the OpenVPN client is complete in most cases.

5.6 First start of the OpenVPN client

The first start of the OpenVPN clients can last a bit longer, because the software creates a lot of registry entries and configures the tunnel interface. All upcoming starts should run significant faster. It is very important to start the program with admin rights!

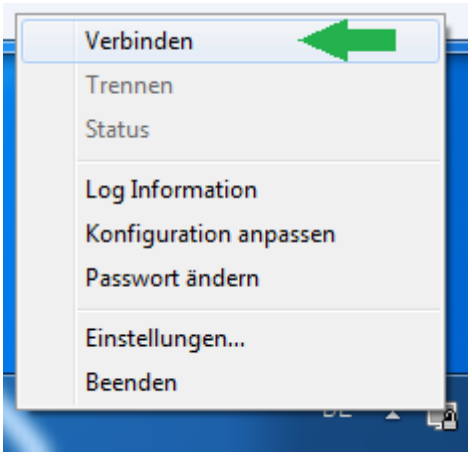
It´s possible that the icon of the OpenVPN client does not appear in the task bar. In this case just click on the arrow and select “adjust”.

The display of the symbol in the task bar can now be changed in the dialogue shown below. With the setting “show symbol and notification“ the symbol is permanently shown in the task bar as long as the software runs.



5.7 Connection set-up

To secure a connection with the OpenVPN-server, the menu item „connect“ has to be selected with a right-hand click on the client symbol (see green arrow).



The OpenVPN-client now connects with the OpenVPN-server. During the connection process a dialogue window appears which shows particular log messages. The log messages can give a first hint for the debugging in cases of connection and diagnosis problems.
After the connection is set up correctly, the dialogue window disappears and the color of the client symbol turns from grey to green.

5.8 Disconnection

To end a consisting connection with an OpenVPN-server, the menu item „disconnect“ has to be selected with a right-hand click on the client symbol. The connection with the OpenVPN-server is thereupon ended.

Important: the connection and disconnection of the PCs have no influence on the connection between the control and the OpenVPN-server. Responsible therefore is the particular client.

5.9 Communication

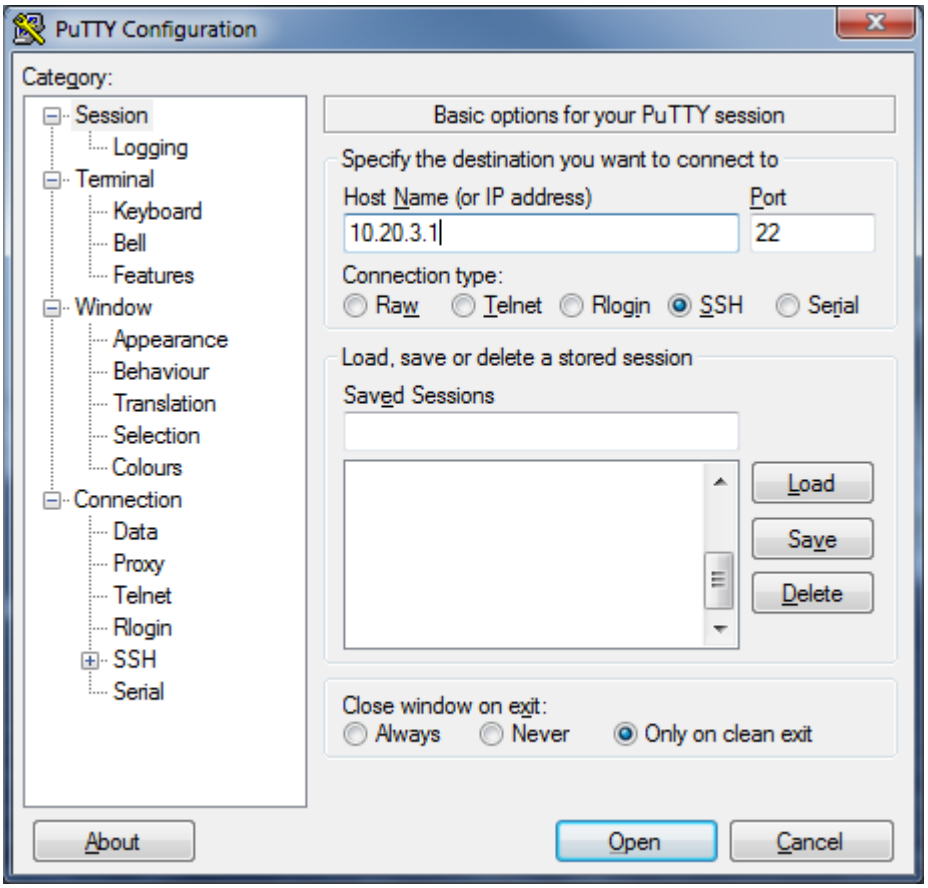
For the communication through VPN both clients (PC and control) have to be connected with the OpenVPN-server. The control can be reached from the PC through the VPN IP address. Further the web interface, the SSH-connection (console) and Codesys are available.

5.10 Connecting with the web interface

Just type the VPN IP address into the local web browser (e.g. 10.20.3.1). After a short waiting period the web interface of the control should answer with the login screen.

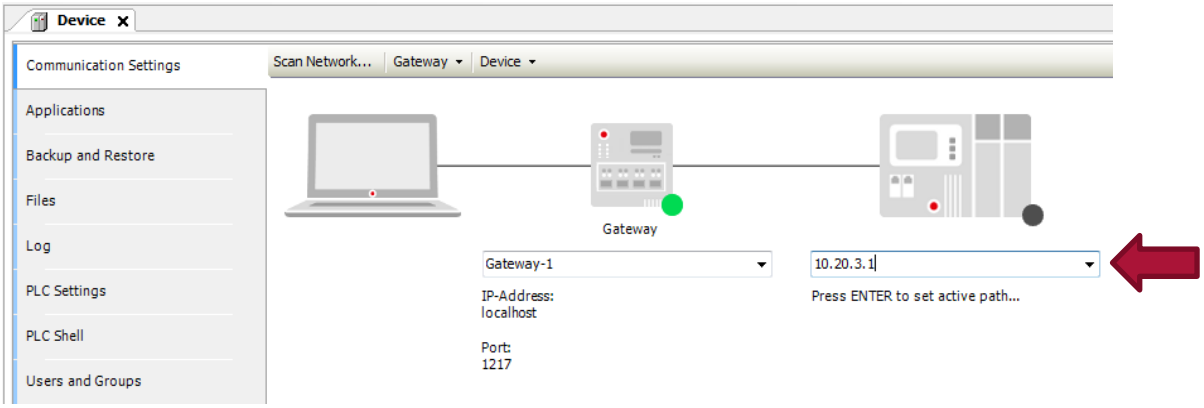
5.11 Conncting via SSH

Type the VPN IP address as host name into the local terminal program (e.g. PuTTY), select SSH as connection type. After the connection is secured, the console is available for the control.



5.12 Connecting via CODESYS

Important: CODESYS can´t find controls via network scan, that are accessible via VPN.
To connect with the control via VPN, the VPN address has to be typed directly into the CODESYS surface. On the left side of the CODESYS surface mark the entry „Device (Berghof MX6 Control)“ located in the „Devices“ area and perform a right-click on “Device (Berghof MX6 Control)” to open the context menu and select “Edit Object”.
Now the gateway (the local PC) of the control should appear in the tab „Communication Settings”. Right next to the gateway symbol is the control symbol, in the text field underneath the control symbol (marked with red arrow) the VPN-IP address of the control can now be entered. CODESYS should now be able to connect to the control via VPN.



Attention: screenshots shown in this document can be different on windows 10.

Your contact partner can be reached under:
Sales team | T +49.7121.894-131 | controls@berghof.com