

Plattform MX6

Softwareoption S109

VPN Client + IXON Agent

1 Identifikation

Identifikation	
Optionskennung	S109
Bestellnummer	S-05000311-0000
Kurzbezeichnung	VPN Client + IXON Agent
Kurzbeschreibung	Mit dieser Softwareoption ist es möglich, die Steuerung in ein virtuelles privates Netzwerk (VPN) zu integrieren. Die angewandte VPN-Technologie ist OpenVPN. Die Erweiterung für IXON verfügt über zusätzliche Features wie Cloud-Logging über OPC-UA oder Modbus Interface.
Revisionskennung Dokument	V3.0

2 Systemvoraussetzungen und Einschränkungen

Systemvoraussetzungen und Einschränkungen	
Unterstützte Plattformen oder Geräte	Berghof SPS der MX6 Plattform (z.B.: MCs, CCs, DCs). Weitere Informationen bezüglich Verfügbarkeit und Kompatibilität finden Sie im Produktkatalog im Abschnitt Optionen.
Firmware	MX6-SPS ab Version 1.18.4 oder höher für OpenVPN Client MX6-SPS ab Version 1.23.0 oder höher für IXON Agent
Weitere Anforderungen	<ul style="list-style-type: none">– OpenVPN-Server oder kompatibles OpenVPN-Portal– Netzwerkverbindung zum OpenVPN-Server– IXON Konto bzw. Zugang
Einschränkungen	<ul style="list-style-type: none">– Nur Host-zu-Host-Konnektivität wird unterstützt

3 Produktbeschreibung

Mit dieser Erweiterung ist es möglich, die SPS über eine verschlüsselte IP-Verbindung an einen VPN-Server und damit an eine verteilte Netzwerkstruktur anzubinden, indem die VPN-Technologie genutzt wird. Durch die Verschlüsselung ist die Anbindung von Netzwerkteilnehmern über unsichere Netze (z.B. Internet) möglich. Ein typischer Anwendungsfall ist die Anbindung von entfernten Standorten für Fernwartungsdienste oder den Datenaustausch zwischen Zentrale und Außendienststellen auf Basis des IP-Protokolls.

Diese Erweiterung stellt einen OpenVPN-Client auf der SPS zur Verfügung, der eine Verbindung zu einem bereits konfigurierten VPN-Server herstellt. Mit Hilfe des in der SPS integrierten Web-Interface werden die Konfigurationsdateien (Schlüssel, Zertifikat und OpenVPN-Konfigurationsdatei) auf die SPS geladen. Beim Hochfahren wird die VPN-Verbindung zum Server durch die SPS aufgebaut. Dort wird die SPS im VPN registriert und ist über das VPN erreichbar. Je nach Serverkonfiguration ist es der SPS auch möglich, andere VPN-Teilnehmer zu erreichen. Der VPN-Verbindung wird ein eigener IP Adressbereich zugewiesen, der in den Konfigurationsdaten des VPN-Servers definiert ist.

Die SPS stellt eine Host-zu-Host Verbindung her. Dadurch ist die SPS über ihre spezielle VPN IP-Adresse erreichbar. Ein Zugriff über diese IP-Adresse auf andere Netzwerkteilnehmer des lokalen Netzwerks, in der sich die SPS befindet, ist nicht möglich. Es besteht aber die Möglichkeit, sich mit Hilfe der CODESYS Gateway-Funktionalität auf anderen CODESYS SPSen im gleichen lokalen Netzwerk wie die VPN-SPS einzuloggen.

Die SPS mit dem VPN-Client kann hinter einer Firewall (Router) betrieben werden, da für die Verbindung zum VPN-Server keine direkten Verbindungen nach außen erforderlich sind. Für einen einwandfreien Betrieb benötigen viele Router eine zusätzliche Konfiguration, um eine funktionierende Internetverbindung bereitzustellen, so dass die SPS über das Internet eine Verbindung zum VPN-Server herstellen kann.

Nach der Lizenzierung dieser Software-Erweiterung stehen die VPN-Funktionen zur Verfügung. Die Einstellungen zur Konfiguration der VPN-Funktionalität über das Web-Interface stehen erst nach erfolgreicher Lizenzierung zur Verfügung.

4 Technische Daten

Technische Daten	
Integrierte Version	OpenVPN Version 2.4.8 (oder neuer)
Komprimierungs-Algorithmus	LZO
OpenSSL Bibliothek	OpenSSL Version 1.0.2p (oder neuer)

5 Quick Start Guide

5.1 Netzwerk Konfiguration der SPS

Um sich mit einem VPN-Server zu verbinden, sind einige Netzwerkeinstellungen bzw. Angaben notwendig. Benötigt werden die IP-Adresse von mindestens einem Server für die Namensauflösung (Nameserver bzw. DNS), die IP-Adresse des Gateways, das den Zugang zum Internet ermöglicht, und die Netzwerkmaske (siehe grüne Pfeile). Diese Informationen müssen sich auf das Netzwerk beziehen, in dem die SPS läuft.

Configuration

- [Network](#)
- [CAN](#)
- [Time and Date](#)
- [Display](#)
- [FTP-Server](#)
- [SSH-Server](#)
- [WEB-Server](#)
- [VPN](#)
- [IXON](#)
- [Users](#)
- [SVC Config](#)
- [Config Protection](#)
- [Reset Config](#)

System

- [Info](#)
- [Licenseinfo](#)
- [Screenshot](#)
- [Update](#)
- [Reboot](#)

PLC-Manager

- [Control](#)
- [Config](#)
- [Application Info](#)
- [Application Files](#)
- [Font Files](#)

Diagnostics

- [PLC Log](#)
- [System Log](#)
- [Ethernet](#)
- [CAN](#)
- [Storage](#)
- [System Dump](#)

Network Configuration

COMMON

Hostname


DNS Server 1 


DNS Server 2

ETH0

Mode:

IPAddress 

NetMask 

Gateway 

ETH0:1

Mode:

ETH1

Mode:

Die SPS sollte idealerweise über eine eigene statische IP-Adresse verfügen, die den Zugang zum Internet ermöglicht.

5.2 IXON Konfiguration

Sie können entweder die IXON-Verbindung verwenden, die ihre eigene VPN-Konfiguration mitbringt, oder eine dedizierte VPN-Verbindung zu einem OpenVPN-Server. Es können aber nicht gleichzeitig der IXON-Client und der VPN-Client aktiv sein. Zur erfolgreichen Aktivierung der SPS und um die Dienste von IXON nutzen zu können, benötigen Sie einen Aktivierungscode (kann direkt bei IXON erworben werden). Wenn Sie nur OpenVPN verwenden möchten, können Sie zum nächsten Kapitel übergehen.

Der IXON-Client erhält seine Konfiguration direkt von den IXON-Servern. Daher müssen Sie nur den Client aktivieren (Schritt 1a) und die Einstellungen übernehmen (Schritt 1b). Um den IXON-Client zu starten und mit der Registrierung fortzufahren, ist ein Neustart der SPS erforderlich.

Configuration

- [Network](#)
- [CAN](#)
- [Time and Date](#)
- [Display](#)
- [FTP-Server](#)
- [SSH-Server](#)
- [WEB-Server](#)
- [VPN](#)
- [IXON](#)
- [Users](#)
- [SVC Config](#)
- [Config Protection](#)
- [Reset Config](#)

System

- [Info](#)
- [Licenseinfo](#)
- [Screenshot](#)
- [Update](#)
- [Reboot](#)

PLC-Manager

- [Control](#)
- [Config](#)
- [Application Info](#)
- [Application Files](#)
- [Font Files](#)

IXON Configuration

IXON client

Startup on boot:

Apply new/changed configuration

(Apply selected settings from above)

IXON Registration

Company: -----

Client: not running

State: unregistered

Registration-ID:

Command response: -----

*

* registration id and enabled IXON client required

Schritt 1a

Schritt 1b

Schritt 2a

Schritt 2b

Um die Dienste von IXON nutzen zu können ist eine Registrierung von Ihnen (als Person) oder Ihrer Firma auf der IXON Webseite (<https://connect.ixon.cloud/login>) erforderlich. Sobald die Registrierung erfolgreich durchgeführt wurde (folgen Sie den Schritten auf der IXON Webseite), erhalten Sie eine Firmen-ID. Diese ID wird benötigt, um die SPS mit dem IXON Konto zu verknüpfen. Wählen Sie Ihre Firmen-ID aus und fügen Sie diese in das Registration-ID Feld ein (Schritt 2a, siehe grüner Pfeil). Stellen Sie sicher, dass die Firmen-ID mit der Registrierungs-ID übereinstimmt. Klicken Sie dann auf „Register device“, um die SPS dem IXON-Konto hinzuzufügen (Schritt 2b). Nach einigen Sekunden sollte neben „Command Response“ eine Meldung über die erfolgreiche Registrierung angezeigt werden und der Status sich auf „registered“ ändern. Die so registrierte SPS kann nun mit einem gültigen Aktivierungscode, der bei IXON erhältlich ist, aktiviert werden.

Um die IXON VPN-Verbindung nutzen zu können, müssen Sie die auf der IXON-Webseite verfügbare VPN-Client-Software herunterladen und installieren. Für die Installation auf Ihrem lokalen PC benötigen Sie Administrationsrechte. Sobald Sie die Client-Software installiert haben, ist keine weitere Konfiguration erforderlich.

5.3 VPN Konfiguration

Sie können entweder eine dedizierte VPN-Verbindung zu einem OpenVPN-Server verwenden oder die IXON Verbindung, die ihre eigene VPN-Konfiguration mitbringt. Es können aber nicht gleichzeitig der VPN-Client und der IXON-Client aktiv sein. Um die VPN-Verbindung zu konfigurieren, müssen Sie die dafür erforderlichen Konfigurations-, Schlüssel- und Zertifikatsdatei mit Hilfe des Web-Interface auf die SPS hochladen (Schritt 1). Die benötigten Dateien können einzeln oder alle zusammen als ZIP-Datei hochladen werden. Wurden alle Dateien erfolgreich auf die SPS hochgeladen, kann der VPN-Client aktiviert werden, sodass er beim Hochfahren gestartet wird (Schritt 2). Der letzte Schritt (Schritt 3) der Einstellungen ist die Aktivierung des konfigurierten VPN-Clients. Nach einem Neustart wird die VPN-Verbindung mit dem konfigurierten VPN-Server automatisch aufgebaut (wenn alle Bedingungen erfüllt sind). Die Verbindung wird so lange gehalten, wie die Internetverbindung besteht und die SPS nicht heruntergefahren wird. Während eines Neustarts der SPS wird die Verbindung unterbrochen, nach dem Bootvorgang aber sofort wieder aufgebaut.

Configuration

- [Network](#)
- [CAN](#)
- [Time and Date](#)
- [Display](#)
- [FTP-Server](#)
- [SSH-Server](#)
- [WEB-Server](#)
- [VPN](#)
- [IXON](#)
- [Users](#)
- [SVC Config](#)
- [Config Protection](#)
- [Reset Config](#)

System

- [Info](#)
- [Licenseinfo](#)
- [Screenshot](#)
- [Update](#)
- [Reboot](#)

PLC-Manager

- [Control](#)
- [Config](#)
- [Application Info](#)
- [Application Files](#)
- [Font Files](#)

VPN Configuration

VPN config file upload

No files in /usr/local/etc/openvpn/

* Caution: Changes cannot be undone!

Keine Datei ausgewählt.
←
Schritt 1

←
Schritt 2

VPN client

Startup on boot: Disabled ▼
←
Schritt 3

Activate new/changed configuration

(Copies the config files to destination and activates the selected settings from above)

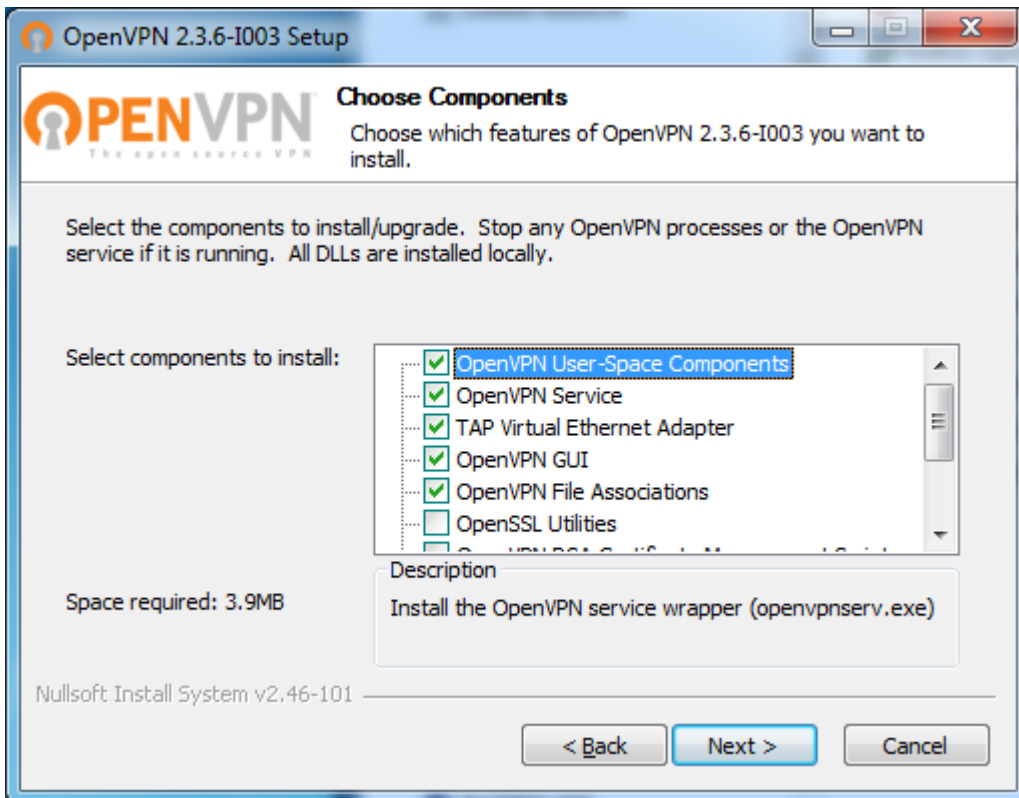
←
Schritt 3

5.4 Software Installation auf dem PC

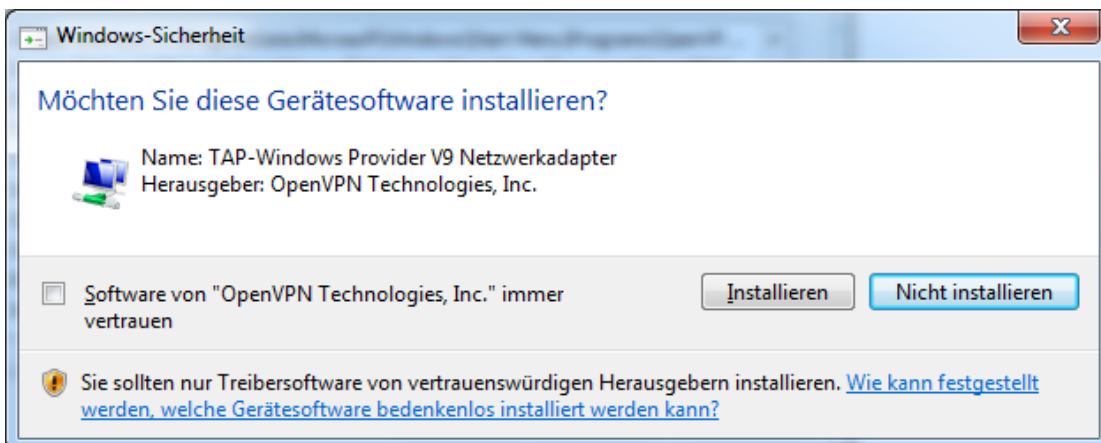
Eine OpenVPN-Client Software wird benötigt, um eine VPN-Verbindung von einem PC aus herzustellen. Weiterhin sind eine Konfigurationsdatei und verschiedene Zertifikats- und Schlüsseldateien für den verschlüsselten Verbindungsaufbau erforderlich. Diese Dateien werden in der Regel vom Betreiber des VPN-Servers bereitgestellt.

Zur Installation der OpenVPN-Client Software sind Administrationsrechte erforderlich, da bestimmte Einträge in der Routing-Tabelle des PCs nur mit den entsprechenden Rechten vorgenommen werden dürfen.

Bei der Installation der Client Software können die vorgewählten Komponenten direkt übernommen werden. Weitere optionale Komponenten sind für den Betrieb nicht erforderlich.



Während der Installation wird eine zusätzliche Netzwerkschnittstelle installiert. Die erscheinende Meldung bietet die Optionen "Installieren" und "Nicht installieren". Wählen Sie "Installieren", sonst funktioniert die OpenVPN-Client Software nicht.



5.5 PC Software Konfiguration

Der OpenVPN-Client benötigt einige Informationen für die Verbindung mit dem VPN-Server. Dafür stellt der Betreiber des VPN-Servers Konfigurationspakete bereit, die (in der Regel) nur in einen entsprechenden Unterordner des OpenVPN-Clients kopiert und entpackt werden müssen. Damit ist die Konfiguration des OpenVPN-Clients in den meisten Fällen abgeschlossen.

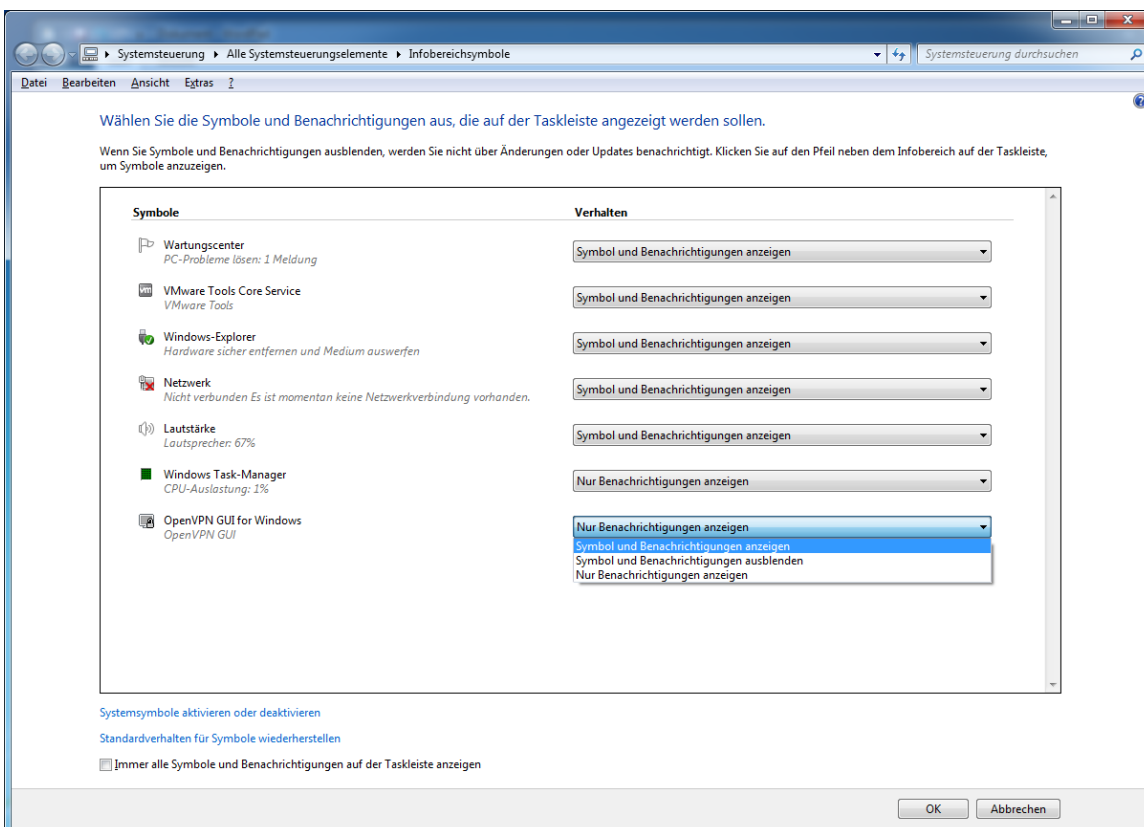
5.6 Erster Start des OpenVPN-Client

Der erste Start der OpenVPN-Clients kann etwas länger dauern, da die Software Registrierungseinträge erstellt und die Tunnel-schnittstelle konfiguriert. Alle folgenden Starts sollten deutlich schneller ablaufen. Es ist sehr wichtig, das Programm mit administrativen Rechten zu starten !

Möglicherweise erscheint das Symbol des OpenVPN-Clients nicht in der Taskleiste. In diesem Fall klicken Sie einfach auf den kleinen, nach oben zeigenden Pfeil (siehe grüner Pfeil) und wählen Sie "Anpassen".

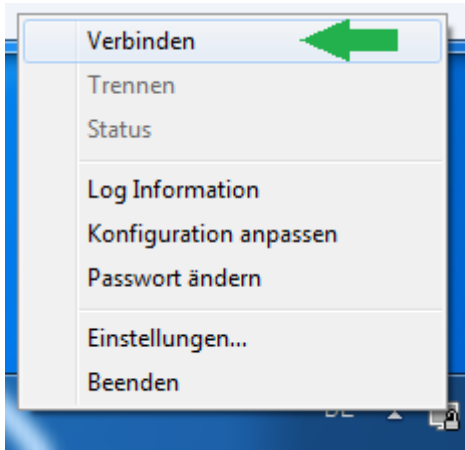


Die Anzeige des Symbols in der Taskleiste kann jetzt im unten abgebildeten Dialog geändert werden. Mit der Einstellung "Symbol und Benachrichtigung anzeigen" wird das Symbol permanent in der Taskleiste angezeigt, solange die Software läuft.



5.7 Verbindungsaufbau

Um eine Verbindung mit dem VPN-Server herzustellen, muss zuerst mit einem Rechtsklick auf das OpenVPN-Client Symbol in der Taskleiste das Menü des Clients geöffnet, danach der Menüeintrag "Verbinden" (siehe grüner Pfeil) ausgewählt werden.



Der OpenVPN-Client verbindet sich nun mit dem VPN-Server. Während des Verbindungsaufbaus erscheint ein Dialogfenster, das bestimmte Protokollmeldungen anzeigt. Die Logmeldungen können bei Verbindungsproblemen einen ersten Anhaltspunkt für die Ursache des Fehlers geben.

Wurde die Verbindung korrekt hergestellt, verschwindet das Dialogfenster und die Farbe des Client Symbols in der Taskleiste wechselt von grau nach grün.

5.8 Trennung der Verbindung

Um eine bestehende Verbindung mit einem VPN-Server zu beenden, muss der Menüpunkt "Verbindung trennen" ausgewählt werden (Menü öffnen durch Rechtsklick auf das Client Symbol in der Taskleiste). Die Verbindung mit dem VPN-Server wird daraufhin beendet.

Wichtig: der Auf- oder Abbau der PC Verbindung zum VPN-Server hat keinen Einfluss auf die Verbindung zwischen der SPS und dem VPN-Server. Dafür ist der jeweilige Client zuständig.

5.9 Kommunikation

Für die Kommunikation über VPN müssen beide Clients (PC und SPS) mit dem VPN-Server verbunden sein. Die SPS ist vom PC aus über die VPN IP-Adresse erreichbar. Weiterhin stehen das Web-Interface, die SSH-Verbindung (Konsole) und Codesys zur Verfügung.

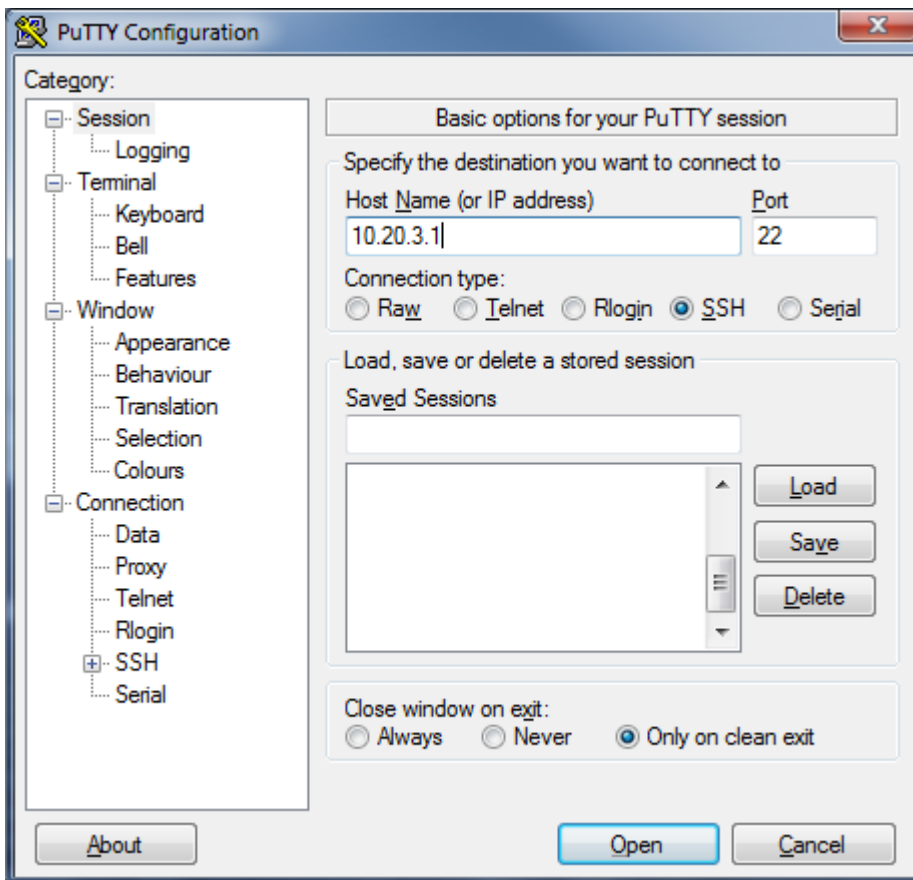
5.10 Verbindung mit dem Web-Interface herstellen

Geben Sie die VPN IP-Adresse in den Webbrowser ein (z.B. 10.20.3.1). Nach einer kurzen Wartezeit sollte das Web-Interface der Steuerung mit dem Anmeldebildschirm erscheinen.



5.11 Herstellen einer Verbindung über SSH

Geben Sie die VPN IP-Adresse als Hostname in das Terminalprogramm ein (z. B. PuTTY), wählen Sie SSH als Verbindungstyp. Nachdem die Verbindung gesichert ist, steht die Konsole für die Steuerung zur Verfügung.

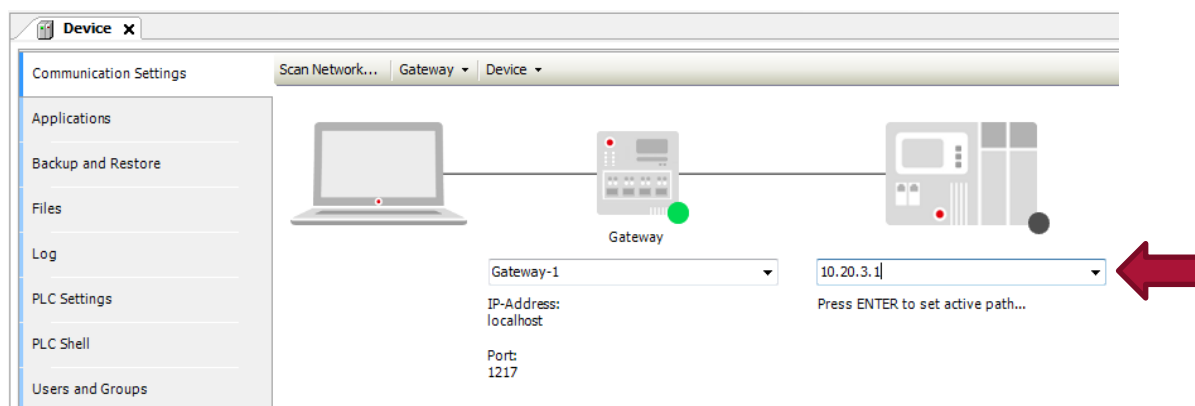


5.12 Verbindung über CODESYS herstellen

Wichtig: CODESYS kann per Netzwerk-Scan keine Steuerungen finden, die über VPN zugänglich sind.

Um sich über VPN mit der SPS zu verbinden, muss die VPN-Adresse direkt in die CODESYS-Oberfläche eingegeben werden. Markieren Sie auf der linken Seite der CODESYS-Oberfläche im Bereich "Geräte" den Eintrag "Gerät (Berghof MX6 Control)" und klicken Sie mit der rechten Maustaste darauf, um das Kontextmenü zu öffnen. Danach wählen Sie "Objekt bearbeiten" aus.

Nun sollte das Gateway (der lokale PC) der SPS im Register "Kommunikationseinstellungen" erscheinen. Direkt neben dem Gateway-Symbol befindet sich das Steuerungssymbol, im Textfeld unter dem Steuerungssymbol (mit rotem Pfeil markiert) kann nun die VPN IP-Adresse der SPS eingegeben werden. CODESYS sollte nun in der Lage sein, sich über VPN mit der SPS zu verbinden.



Achtung: Die Bildschirmaufnahmen wurden unter Windows 7 erstellt. Sie können auf anderen Windows-Versionen unterschiedlich sein.

Ihre Ansprechpartner erreichen Sie unter:

Vertriebsteam | T +49.7121.894-131 | controls@berghof.com

Berghof Automation GmbH | Arbachtalstraße 26 | 72800 Eningen | www.berghof-automation.com
SoftwareOption S109 OpenVPN Client + IXON Agent V3 DE.docx