netFIELD Remote Service Introduction

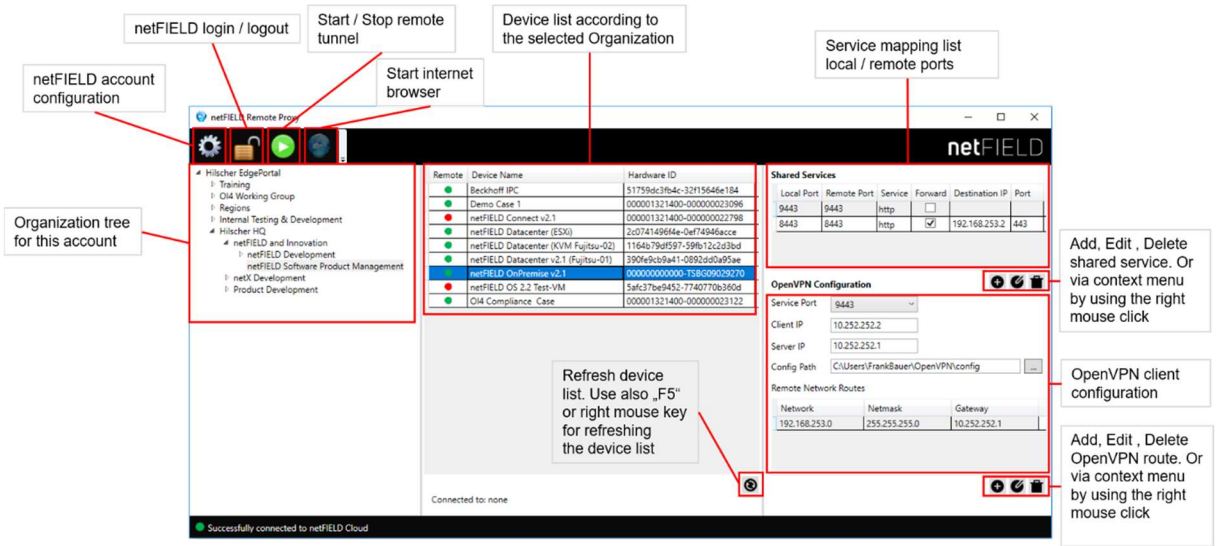
The introduction of netFIELD Cloud and netFIELD OS v2.2 will enhance the capabilities of remote access. Currently only the remote access to the local Device Manager is supported. This will change with version 2.2 of netFIELD Cloud and netFIELD OS.

The new remote access features will provide four additional scenarios to access on site services from a remote Windows PC.

- Access to IP services provided by Docker containers running on the IoT or Standard Docker of the Edge device
- Access to IP services provided by other devices connected to a reachable network
- Access to any remote device which is connected to a routed network
- Applications requires a logical network adapter (e.g. TIA Portal) for the access to the remote device.

In order to use the enhanced remote access capabilities the installation of the netFIELD Remote Proxy on a local Windows PC is required. The application is compatible with Windows 7, 8.1 and 10 (32 / 64 Bit).

netFIELD Remote Proxy UI (version ≥ 0.9.8.0)

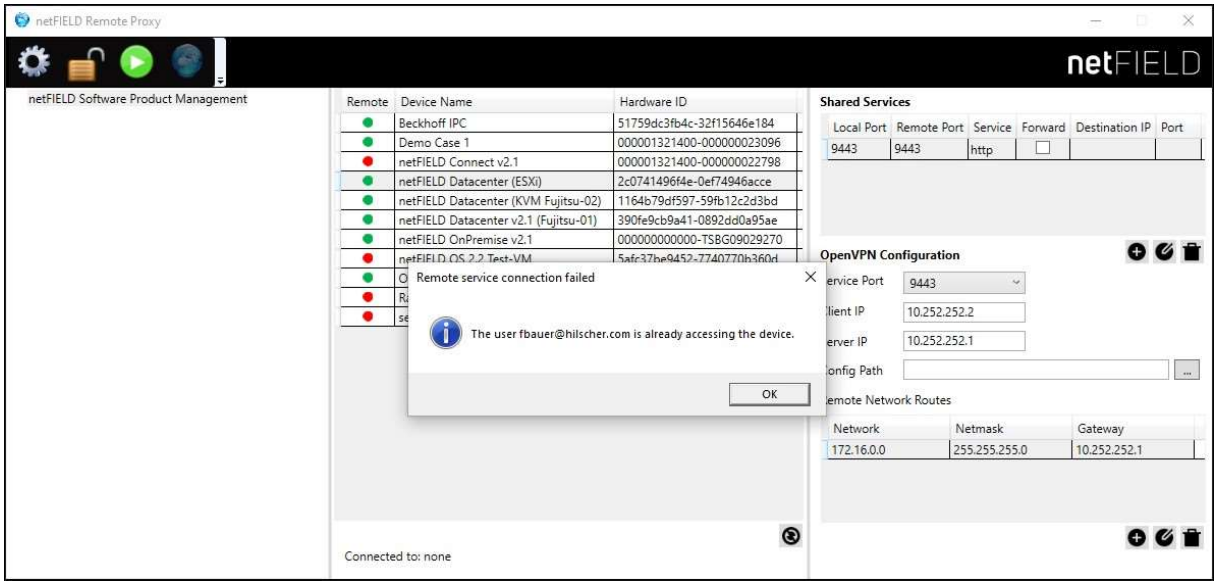


netFIELD account configuration	API endpoint, username, password used for the netFIELD Cloud login
netFIELD login / logout	Toggle between netFIELD Cloud login and logout state
Organization tree	A tree with all sub-organizations for which the user has permissions.
Start / Stop remote tunnel	Start / Stop of a remote tunnel for each mapped port in the service list
Start internet browser	Bring up an internet browser and open a tab for each “http” service
Device list	List of all devices with remote access status belonging to the selected organization.

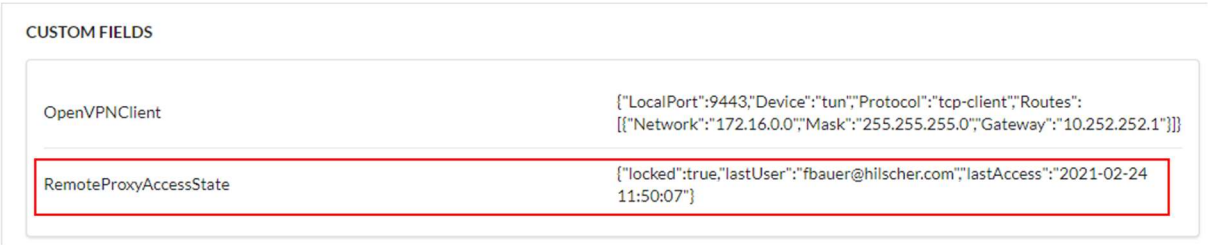
Service mapping list	Add/Edit and Delete services shared from the netFIELD Edge device. The configuration is stored in netFIELD Cloud via the netFIELD Platform API. After changes, the netFIELD Edge device will go “offline” because of the restart of the “netfield-remote-control” container. The refresh of the device state can be triggered by using the “Refresh” context menu (right mouse click) in the device list.
OpenVPN client configuration	The service port is used via localhost to connect the OpenVPN client to the OpenVPN service running on the netFIELD Edge device. The route list is needed for the OpenVPN client to add the network routes into the route table of the remote PC. The OpenVPN configuration is stored in a custom field in the netFIELD Platform. On the remote PC site, the configuration files for the OpenVPN client are also created automatically by the netFIELD Remote Proxy. The configuration of the OpenVPN service running on the netFIELD Edge device is generated automatically during the first start of netFIELD OS 2.2. The OpenVPN service itself is still disabled by default and has to be activated by using the terminal CLI. In earlier netFIELD OS versions the configuration files can be created also manually.

Device locking information (version ≥ 0.9.8.4)

If a user already accesses a netFIELD Edge device via the netFIELD Remote Proxy, this device cannot be reached by a second user. In this case, the user is informed by displaying an information window.



The information about the last access and the current state is stored in the netFIELD Platform



netFIELD Cloud shared Remote Services

REMOTE CONTROL SETTINGS

Host	Http Port
127.0.0.1	25000

Services

Edge Device Port	Service	Forward Service	Destination IP	Destination Port
9443	http(s)	false		
22	ssh	false		

Service	Description
http(s)	This option is used for other TCP/IP services not listed below. It works with many other client protocols like MQTT, OpenVPNn OPC UA etc. The “Start Internet Browser” button creates Tabs for services marked as http(s) only.
ssh	Access via ssh or scp protocol for remote shell access or file operations
rdp	The Remote Desktop Protocol (RDP) is used by Mircosoft to access the Windows desktop
vnc	Virtual Network Computing is a graphical desktop-sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer.

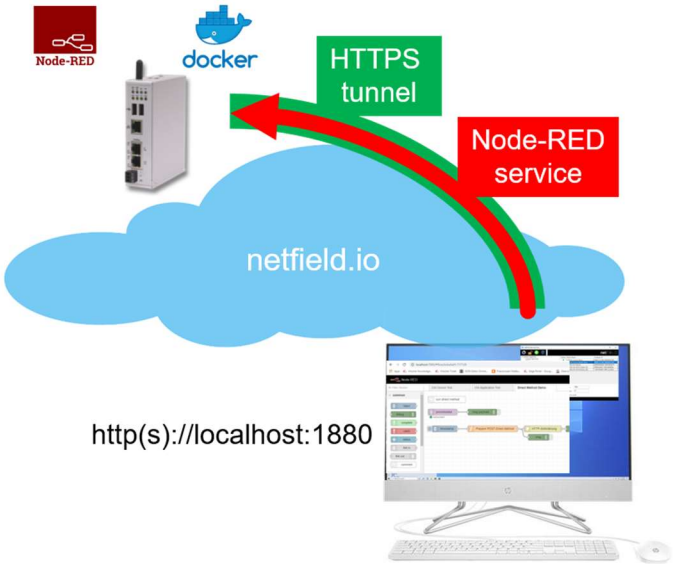
netFIELD Cloud OpenVPN client settings

CUSTOM FIELDS

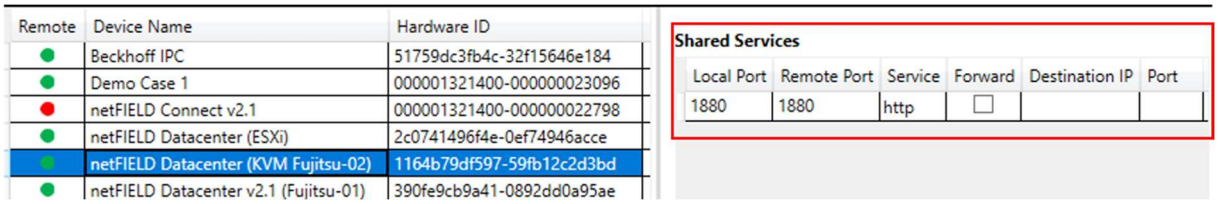
OpenVPNClient	{"localPort":9443,"device":"tun","protocol":"tcp-client","routes":[{"network":"192.168.0.0","mask":"255.255.255.0","gateway":"10.252.252.1"},{"network":"192.168.1.0","mask":"255.255.255.0","gateway":"10.252.252.1"}]}

Scenario: Share services with a remote PC

A good example is a running Node-RED container either on the IoT Docker deployed via netFIELD Cloud or a locally deployed container on the Standard Docker instance. In this cases the container is exposing a port (usually port 1800) to the netFIELD Edge device. By using the netFIELD Remote Proxy application this port can be shared with the “localhost” of the remote PC.



In this case a mapping from the local port e.g. 1800 to the exposed remote port 1800 of Node-RED has to be created. A shared service can be added, edited or deleted by using the mouse right click context menu.

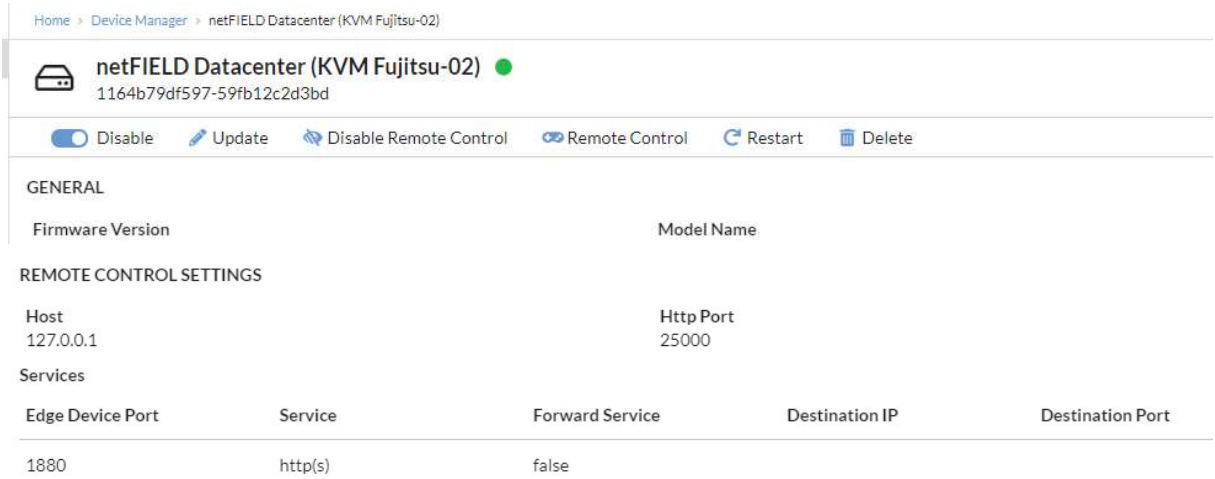


Remote	Device Name	Hardware ID
●	Beckhoff IPC	51759dc3fb4c-32f15646e184
●	Demo Case 1	000001321400-000000023096
●	netFIELD Connect v2.1	000001321400-000000022798
●	netFIELD Datacenter (ESXi)	2c0741496f4e-0ef74946acce
●	netFIELD Datacenter (KVM Fujitsu-02)	1164b79df597-59fb12c2d3bd
●	netFIELD Datacenter v2.1 (Fujitsu-01)	390fe9cb9a41-0892dd0a95ae

Shared Services

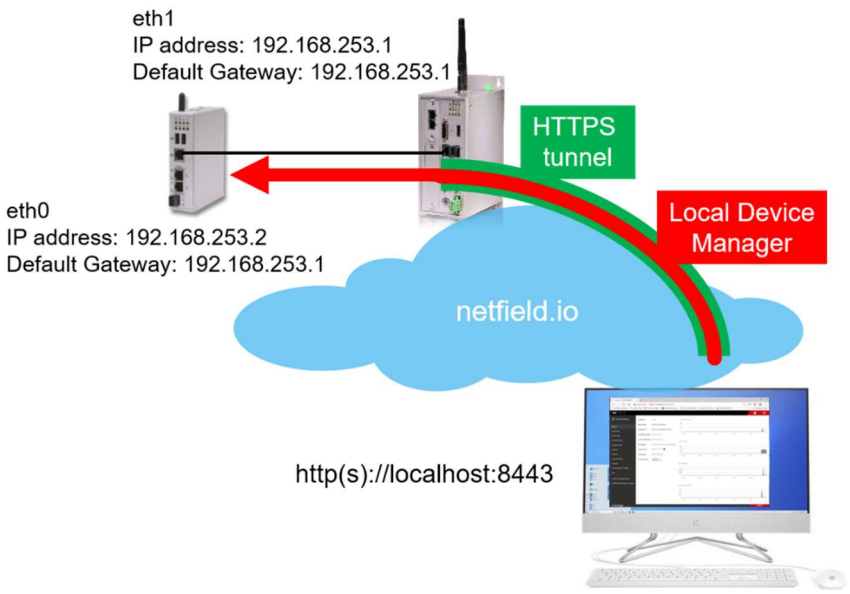
Local Port	Remote Port	Service	Forward	Destination IP	Port
1880	1880	http	☐		

By adding this service in the netFIELD Remote Proxy, the service is also added to the device configuration in the netFIELD Cloud.



Scenario: Share a service of a network device with a remote PC

This option can be useful if another network device (e.g. an IPC on the machine network) provides a service that the user wants to share with a remote PC for service purposes. In this case the shared service port can be forwarded to another IP address.



In this case, the local port e.g. 8443 is mapped to the device with the IP address 192.168.253.2 and the service listening on port 443. In the example shown above, this is the local Device Manager of the netFIELD Connect Gateway.

netFIELD Remote Proxy configuration

Remote	Device Name	Hardware ID
●	Beckhoff IPC	51759dc3fb4c-32f15646e184
●	Demo Case 1	000001321400-000000023096
●	netFIELD Connect v2.1	000001321400-000000022798
●	netFIELD Datacenter (ESXi)	2c0741496f4e-0ef74946acce
●	netFIELD Datacenter (KVM Fujitsu-02)	1164b79df597-59fb12c2d3bd
●	netFIELD Datacenter v2.1 (Fujitsu-01)	390fe9cb9a41-0892dd0a95ae
●	netFIELD OnPremise v2.1	000000000000-TSBG09029270
●	netFIELD OS 2.2 Test-VM	5afc37be9452-7740770b360d

Shared Services

Local Port	Remote Port	Service	Forward	Destination IP	Port
8443	8443	http	☑	192.168.253.2	443
9443	9443	http	☐		

By adding this service in the netFIELD Remote Proxy, the service is also added to the device configuration in the netFIELD Cloud.

Services

Edge Device Port	Service	Forward Service	Destination IP	Destination Port
8443	http(s)	true	192.168.253.2	443

Scenario: Share networks via OpenVPN

On the one hand, this option may not be in line with the client's IT security policy in most cases, but on the other hand, it can be a valuable way to provide cost-effective support. The security vulnerability occurs when the client network is shared with an external network, e.g. that of the service technician. However, netFIELD Cloud and netFIELD Remote Proxy also support this possibility.

In this case, two use cases are supported. On the one hand, transparent access to all IP endpoints and services in the target network is possible and on the other hand, the OpenVPN client provides a logical network adapter, which is required, for example, by the TIA Portal to connect to a PLC.

Preparing netFIELD OS

From the netFIELD OS version 2.2 onwards, all server-side configurations are automatically created at the first system boot. The OpenVPN service only needs to be started by the user.

Start / Stop the OpenVPN Service

```
$ sudo systemctl start|stop openvpn@server.service
```

Enable / Disable autostart of the OpenVPN Service

```
$ sudo systemctl enable|disable openvpn@server.service
```

Before netFIELD OS version 2.2, the OpenVPN server must be configured manually.

```
$ sudo mkdir /etc/openvpn
$ sudo vi  /etc/openvpn/server.conf
```

Save the following configuration in the server.conf file

```
port 9443
proto tcp-server
dev tun
cipher AES-256-CBC
secret /etc/openvpn/static.key
ifconfig 10.252.252.1 10.252.252.2
keepalive 10 120
```

Create the static.key file

```
$ sudo openvpn --genkey --secret /etc/openvpn/static.key
$ sudo chmod 644 /etc/openvpn/static.key
```

After these steps, the OpenVPN Server can be used with older netFIELD OS versions also.

Start / Stop the OpenVPN Service

```
$ sudo systemctl start|stop openvpn@server.service
```

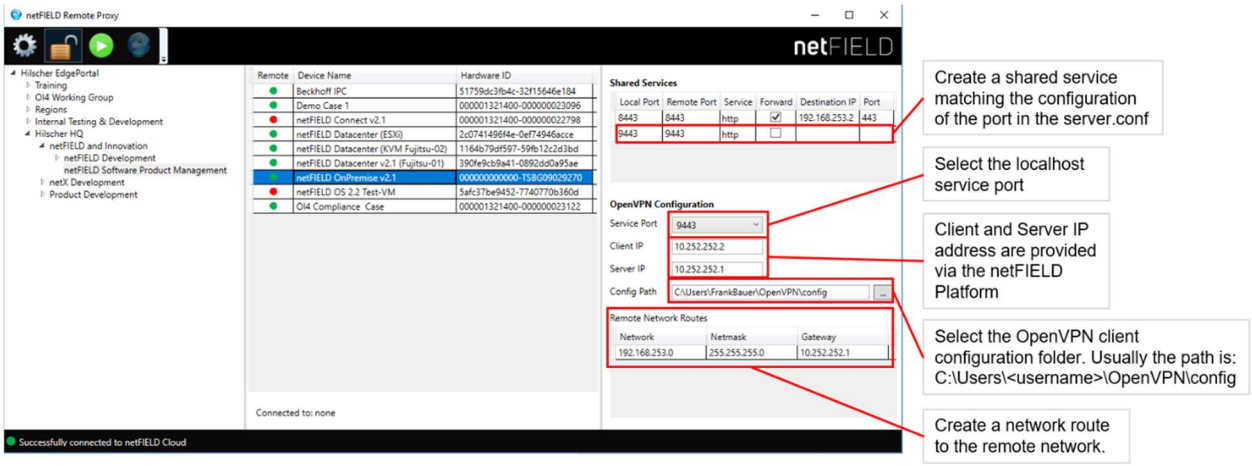
Enable / Disable autostart of the OpenVPN Service

```
$ sudo systemctl enable|disable openvpn@server.service
```

The IP address of the server (10.252.25.1) and the client IP address (10.252.252.2) as well as the cipher mode and the key are provided to the netFIELD Remote Proxy automatically via the netFIELD Platform. Only the shared service and the route configuration has to be done at the netFIELD Remote Proxy. Please keep in mind that the netFIELD Remote Proxy is not aware, if the OpenVPN server is running or not.

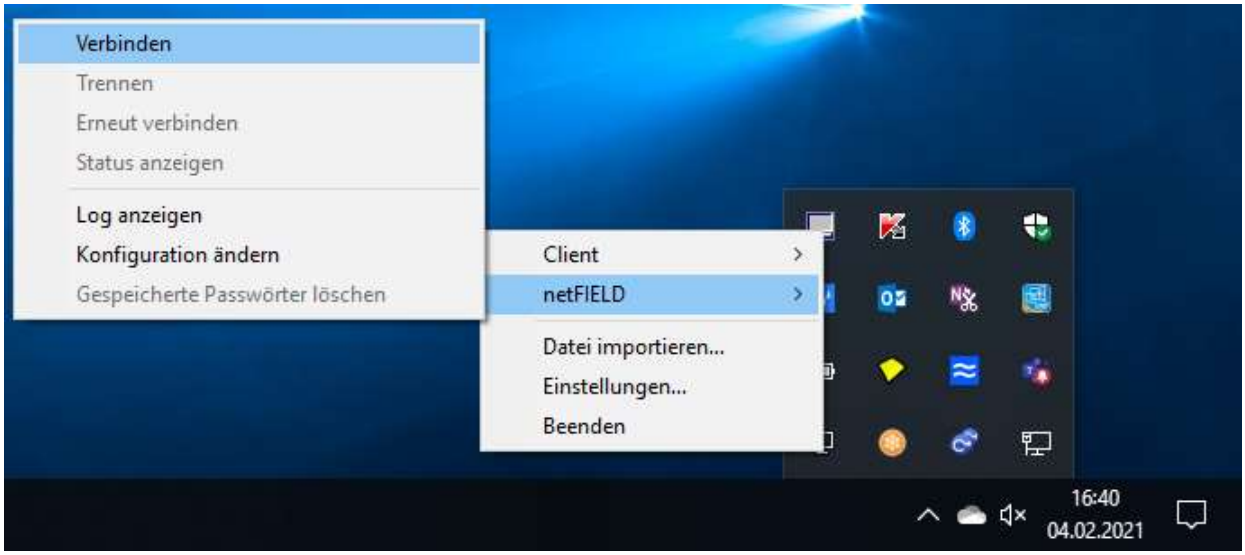
Prepare the remote PC

Before you start with the netFIELD Remote Proxy please install the OpenVPN Community client from this website https://openvpn.net/community-downloads/ on your Windows PC

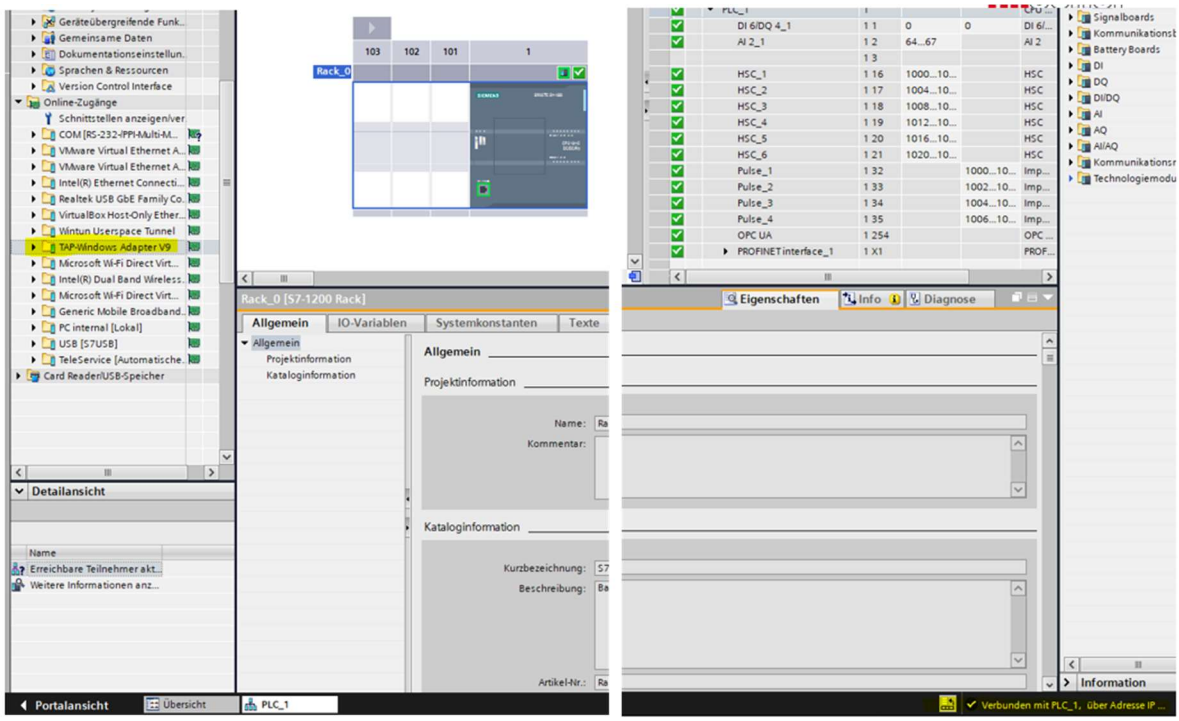
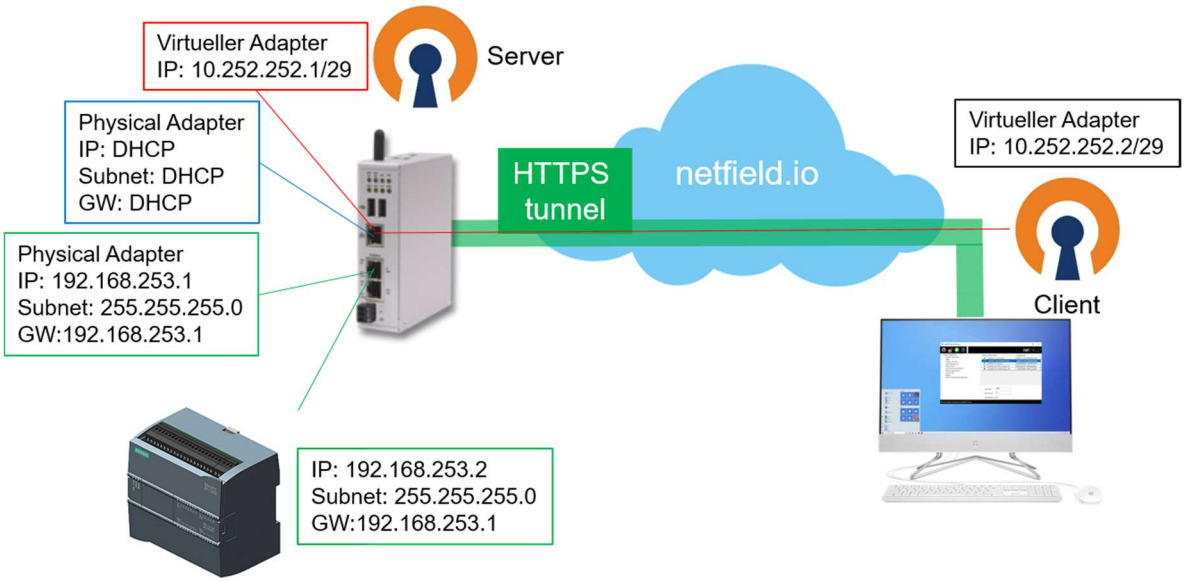


In this case the network 192.168.253.0 with the netmask 255.255.255.0 is tunneled between the remote PC and the netFIELD Edge device. Due to the netmask the route configuration is including the IP address range between 192.168.253.1 and 192.168.253.254. Please keep in mind, this is a routed network, that won't support broadcast traffic. After the configuration, the required files are written to the configuration folder of the OpenVPN Client. The connection is now ready to use after the netFIELD Remote Proxy tunnel is enabled by the “play” button.

With a right mouse click on the OpenVPN client, which is located in the system tray, the connection can be established.



By installing the OpenVPN client, the additional logical network adapter “TAP-Windows Adapter V9” is now available on the remote PC. Since the adapter is recognized by the TIA Portal, it can be used for a remote connection to the PLC.



It is important to understand that multiple networks need to be routed. Within the Internet connection we have the transfer (VPN) network 10.252.252.0 with network mask 255.255.255.252 and physically we have the network 192.168.252.0 with network mask 255.255.255.0 connected to an Ethernet port on the netFIELD Edge device. In this network setup, the netFIELD Edge device acts as a router between the networks. To get this to work, the IP address (here the cifx interface) of the netFIELD Edge device must be configured as the default gateway for each network device (e.g. the PLC). Since no layer 2 information is exchanged between the subnets in a routed network, the PROFINET DCP protocol does not work. For this reason, the "Name of Station", for example, cannot be set remotely.