Industrial Data Communication

VPN with INSYS routers

Configuring OpenVPN server with certificate-based authentication under Windows

Configuration Guide

Trademarks

The use of a trademark not shown below is not an indication that it is freely available for use.

MNP is a registered trademark of Microcom Inc.

IBM PC, AT, XT are registered trademarks of International Business Machine Corporation.

Windows™ is a registered trademark of Microsoft Corporation.

Linux is a registered trademark of Linus Torvalds.

INSYS ® is a registered trademark of INSYS icom GmbH.

The principles of this publication may be transferred to similar combinations. INSYS icom GmbH does not assume liability or provide support in this case. Moreover, it cannot be excluded that other effects or results than described here are produced, if other, similar components are combined and used.

INSYS icom GmbH is not liable for possible damages.

Publisher

INSYS icom GmbH
Hermann-Köhl-Str. 22
D-93049 Regensburg
Germany

Phone	+49 941 58692 0
Fax	+49 941 58692 45
E-mail	info@insys-icom.com
URL	http://www.insys-icom.com

Print	17. Jan. 2024
Item No.	-
Version	1.6
Language	EN

1 Introduction

General

The present publication refers to a combination of selected hardware and software components of INSYS icom GmbH as well as other manufacturers. All components have been combined with the target to realize certain results and effects for certain applications in the field of professional data transfer.

All components have been prepared, configured and used as described in this publication. Thus, the desired results and effects have been achieved.

The exact descriptions of all used components, to which this publication refers, are described in the tables *Hardware, Accessories* and *Software* at the end of this publication.

The symbols and formattings used in this publication are explained in the correspondent section at the end of this publication.

Some configurations or preparations, which are precondition in this publication, are described in other publications. Therefore, always refer to the related device manuals. INSYS devices with web interface provide you with helpful information about the configuration possibilities, if you click on "display help text" in the header.

Target of this Publication

A Windows PC can also act as an OpenVPN server in an OpenVPN network. Refer to http://www.openvpn.eu for further information about OpenVPN.

Use this publication to find out how to set up a Windows PC as OpenVPN server with certificate-based authentication for an OpenVPN network with INSYS routers as clients.

The present publication describes the proceeding under Windows 7. Proceed accordingly for an installation under Windows Vista or Windows XP.

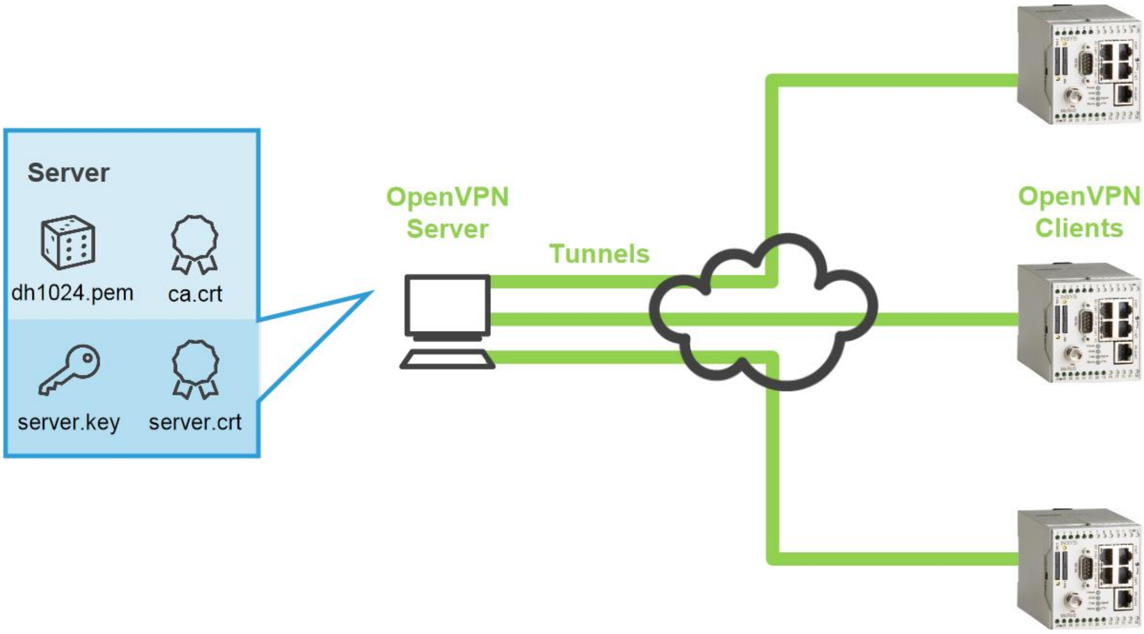


Figure 1: Windows PC as OpenVPN server with certificate-based authentication

2 Configuration

Provisions

Please prepare the following items before starting the configuration:

- **Downloading the OpenVPN Package**
- **Installing the OpenVPN Package on a Windows PC**
- **Creating a Certificate Structure**
- **Configuring INSYS Router as OpenVPN Client and Display Configuration File**

- **Downloading the OpenVPN Package**

  How to download the OpenVPN package from our website.

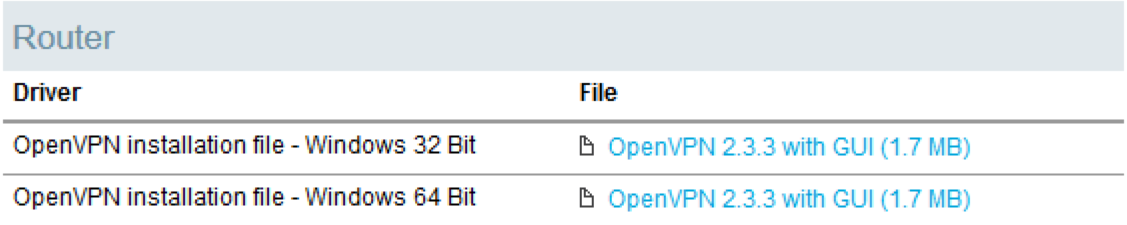
→ PC with approx. 1.5 MB free disk space

→ Web browser

→ Internet connection

1. Open http://www.insys-icom.com/driver/ to download the drivers.
2. Click on the link for your Windows version in the "Router" section:

   ⓘ *Refer to Control Panel, System, System section and System type for your Windows version (32 or 64 bit).*



Router

Driver	File
OpenVPN installation file - Windows 32 Bit	OpenVPN 2.3.3 with GUI (1.7 MB)
OpenVPN installation file - Windows 64 Bit	OpenVPN 2.3.3 with GUI (1.7 MB)

   ⓘ *If a more recent version is available, download this.*

3. Save the file on your PC.

   ✓ You have downloaded the OpenVPN package software with this.

■ Installing the OpenVPN Package on a Windows PC

How to install the OpenVPN GUI and the programs for creating the certificates and keys on your PC successfully.

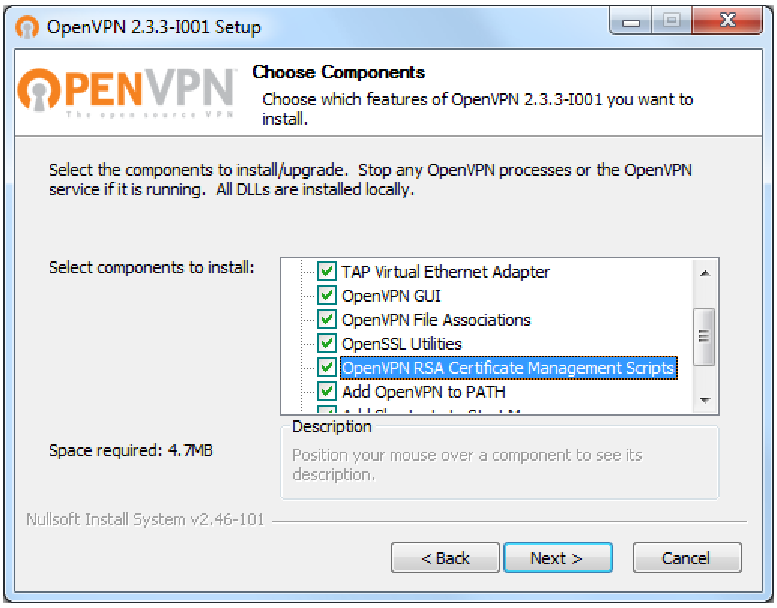
→ You have downloaded the OpenVPN packet (version 2.3.3 or higher) from the INSYS website (www.insys-icom.com/driver).

1. Execute the previously downloaded installation file

   ▶ *If Windows displays a security request, confirm it.*

2. Start the setup wizard and accept the license agreement.

   ✓ The component selection window appears.



OpenVPN 2.3.3-I001 Setup

Choose Components

Choose which features of OpenVPN 2.3.3-I001 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

Select components to install:

☑ TAP Virtual Ethernet Adapter
☑ OpenVPN GUI
☑ OpenVPN File Associations
☑ OpenSSL Utilities
☑ OpenVPN RSA Certificate Management Scripts
☑ Add OpenVPN to PATH

Space required: 4.7MB

Description

Position your mouse over a component to see its description.

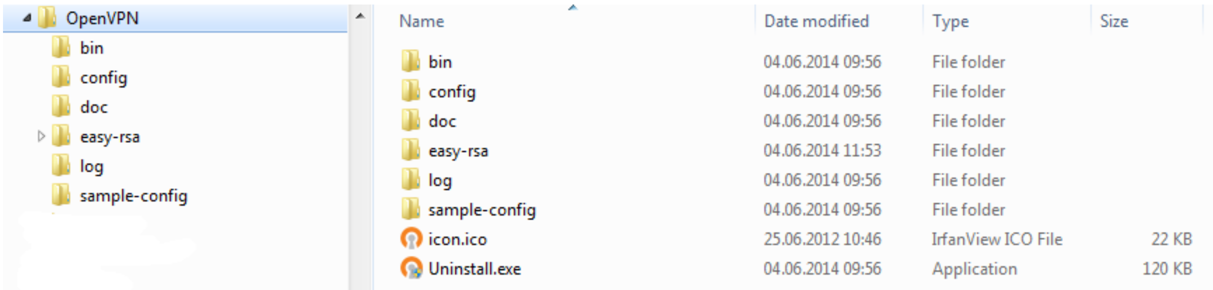
Nullsoft Install System v2.46-101

3. Check the "OpenVPN RSA Certificate Management Scripts", select Next > and continue the setup wizard.

   ▶ *If a Windows log test warning is displayed, confirm it.*

4. Click on Finish upon completion of the installation.

   ✓ The OpenVPN GUI, the SSL software and the programs for creating the certificates and keys are now in the specified directories (default: C:\Program Files\OpenVPN\).



Name	Date modified	Type	Size
bin	04.06.2014 09:56	File folder	
config	04.06.2014 09:56	File folder	
doc	04.06.2014 09:56	File folder	
easy-rsa	04.06.2014 11:53	File folder	
log	04.06.2014 09:56	File folder	
sample-config	04.06.2014 09:56	File folder	
icon.ico	25.06.2012 10:46	IrfanView ICO File	22 KB
Uninstall.exe	04.06.2014 09:56	Application	120 KB

✓ You have successfully installed the OpenVPN package on your PC and completed the provisions with this.

Creating a Certificate Structure

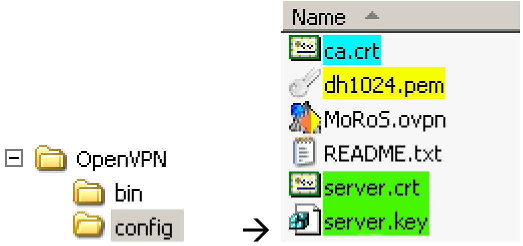
How to create a certificate structure for your application.

1. Create a certificate structure for your application.

   ⓘ *A detailed description of this process can be found in our Configuration Guides "Creating X509.V3 Certificates for VPNs with easy-rsa" or "Creating X509.V3 Certificates for VPNs with XCA".*

   ✓ You have created a certificate structure consisting of certificates and keys for CA, server and clients, as well as a Diffie-Hellman parameter set.

2. Copy server key and certificate, CA certificate and Diffie-Hellman parameter set into the working directory of the OpenVPN package (default: C:\Program Files\OpenVPN\config).



   ▶ *If you have received a PKCS#12 file that contains certificates and key (e.g. "Server.p12"), this already contains all files. Copy only this file and the Diffie-Hellman parameter set to above directory in this case.*

   ✓ The OpenVPN server has the required keys and certificates available with this.

Configuring INSYS Router as OpenVPN Client and Display Configuration File

How to create a configuration file for the OpenVPN server using an INSYS router, which is configured as OpenVPN client. This is the most convenient way to generate a configuration file. Of course, this can also be created manually.

→ You have created a certificate structure for your application.

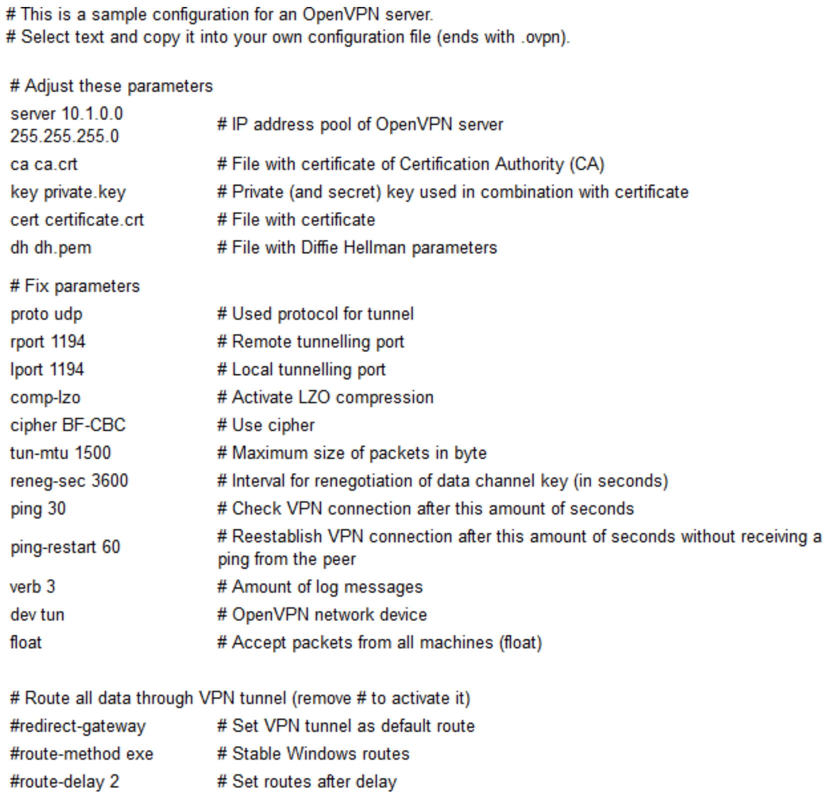
1. Configure an INSYS router, which shall act as OpenVPN client, according to your application.

   ⓘ *A detailed description about this can be found in the configuration guide "Configuring an OpenVPN Client with Certificate-Based Authentication".*

   ✓ The INSYS router can generate a suitable configuration file for the OpenVPN server after this processes have been completed.

2. Click on the link "Create sample configuration file for remote terminal" to display this configuration file.

Configuration



```
# This is a sample configuration for an OpenVPN server.
# Select text and copy it into your own configuration file (ends with .ovpn).

# Adjust these parameters
server 10.1.0.0
255.255.255.0          # IP address pool of OpenVPN server
ca ca.crt              # File with certificate of Certification Authority (CA)
key private.key        # Private (and secret) key used in combination with certificate
cert certificate.crt   # File with certificate
dh dh.pem              # File with Diffie Hellman parameters

# Fix parameters
proto udp              # Used protocol for tunnel
rport 1194             # Remote tunnelling port
lport 1194             # Local tunnelling port
comp-lzo               # Activate LZO compression
cipher BF-CBC          # Use cipher
tun-mtu 1500           # Maximum size of packets in byte
reneg-sec 3600         # Interval for renegotiation of data channel key (in seconds)
ping 30                # Check VPN connection after this amount of seconds
ping-restart 60        # Reestablish VPN connection after this amount of seconds without receiving a
                       ping from the peer
verb 3                 # Amount of log messages
dev tun                # OpenVPN network device
float                  # Accept packets from all machines (float)

# Route all data through VPN tunnel (remove # to activate it)
#redirect-gateway      # Set VPN tunnel as default route
#route-method exe      # Stable Windows routes
#route-delay 2         # Set routes after delay
```

3. Copy the complete text of this configuration file to the clipboard to able to paste it into a text editor in the next step.

   ✓ You have created a configuration file for the OpenVPN server with this, which must be adjusted to your application now.

Configuration

Adjust the example configuration to your application now. The following steps are necessary for this:

- **Creating the Configuration File from the Example Configuration**
- **Adjusting the Configuration File for Routing**

■ Creating the Configuration File from the Example Configuration

How to create a configuration file for the OpenVPN server from the example configuration of the INSYS router.

→ The OpenVPN package is installed on the computer, which shall act as server.

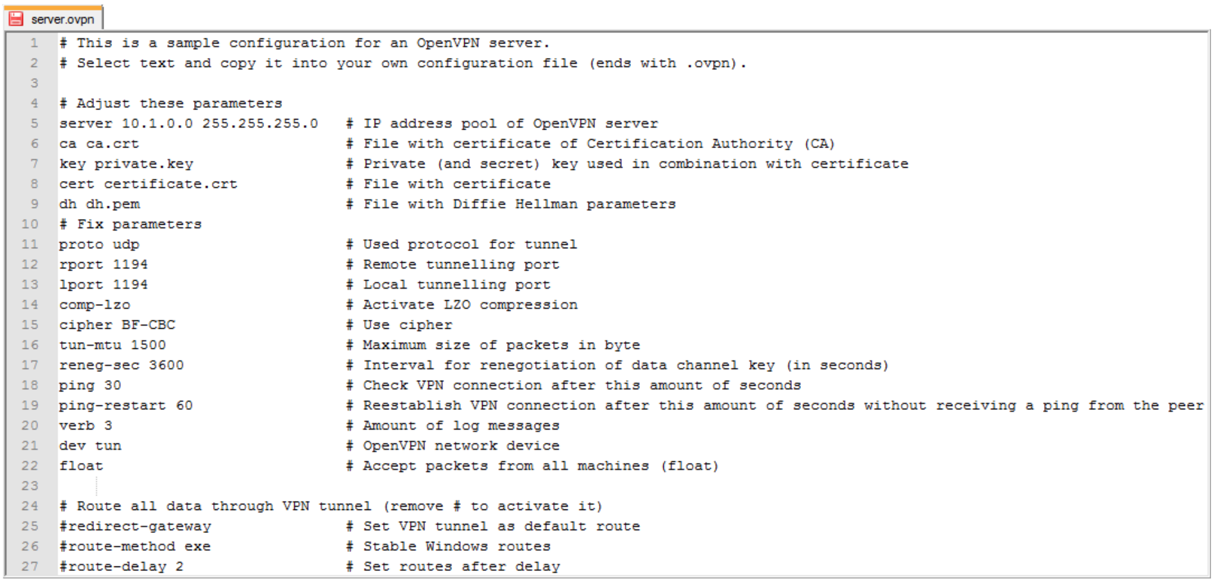
→ You have created the example configuration for the remote terminal using an INSYS router, which is configured as OpenVPN client, and copied it to the clipboard.

1. Change to the working directory of the OpenVPN package (default: C:\Program Files\OpenVPN\config).
2. Create a new text file there and assign it a file name with the suffix ".ovpn" (e.g. "server.ovpn").

ⓘ *Make sure that your text editor has not appended the suffix ".txt" to the file. Depending on the Windows configuration, it might also be possible that the display of this suffix is suppressed even if it exists.*

ⓘ *It is also possible that several configuration files are present in the working directory.*

3. Open the file with a text editor.
4. Copy the previously created example configuration into this file.



```
 1  # This is a sample configuration for an OpenVPN server.
 2  # Select text and copy it into your own configuration file (ends with .ovpn).
 3
 4  # Adjust these parameters
 5  server 10.1.0.0 255.255.255.0   # IP address pool of OpenVPN server
 6  ca ca.crt                       # File with certificate of Certification Authority (CA)
 7  key private.key                 # Private (and secret) key used in combination with certificate
 8  cert certificate.crt            # File with certificate
 9  dh dh.pem                       # File with Diffie Hellman parameters
10  # Fix parameters
11  proto udp                       # Used protocol for tunnel
12  rport 1194                      # Remote tunnelling port
13  lport 1194                      # Local tunnelling port
14  comp-lzo                        # Activate LZO compression
15  cipher BF-CBC                   # Use cipher
16  tun-mtu 1500                    # Maximum size of packets in byte
17  reneg-sec 3600                  # Interval for renegotiation of data channel key (in seconds)
18  ping 30                         # Check VPN connection after this amount of seconds
19  ping-restart 60                 # Reestablish VPN connection after this amount of seconds without receiving a ping from the peer
20  verb 3                          # Amount of log messages
21  dev tun                         # OpenVPN network device
22  float                           # Accept packets from all machines (float)
23
24  # Route all data through VPN tunnel (remove # to activate it)
25  #redirect-gateway               # Set VPN tunnel as default route
26  #route-method exe               # Stable Windows routes
27  #route-delay 2                  # Set routes after delay
```

5. Adjust the file names for CA certificate, server certificate and key and Diffie-Hellman parameters according to the previously created files (here lines 6 to 9).

   ▶ *If you have received a PKCS#12 file that contains certificates <u>and</u> key (e.g. "Server.p12"), this already contains all files. Delete in this case the lines 6 to 8 and insert a line for this file instead (e.g. "pkcs12 server.p12").*

6. If required, adjust the address pool for the internal VPN routing, if already used networks are in this range (here line 5).
7. Remove the "#" symbol to enable the "route-method exe" command (here line 27).
8. Remove the "#" symbol to enable the "route-delay 2" command (here line 28).

   ✓ You have created a configuration file from the example configuration with this. An OpenVPN client can register to the server with this. However, the correct routing must still be adjusted.

■ Adjusting the Configuration File for Routing

How to adjust the configuration file for the OpenVPN server to your application.

→ The OpenVPN package is installed on the computer, which shall act as server.

→ You have created a configuration file for the OpenVPN server and opened it in a text editor.

1. Add new lines with the **push** command at the end of the configuration file for "pushing" the routes from the server to the client for the routing into the Server network. The server IP address range must be communicated to every client with this.

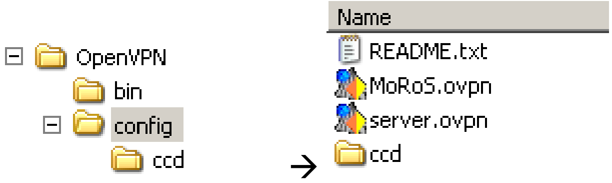
```
# Route für die Clients anlegen
# Server-Netzwerk
push "route 192.168.200.0 255.255.255.0"
```

2. Specify the directory, in which the files for the routing into the client network are located, which define the IP address ranges behind the respective clients (e.g. "ccd" directory).

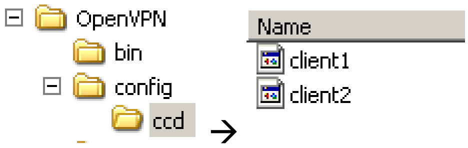
```
# Routen für die Clients festlegen
client-config-dir ccd
```

ⓘ *The connection of IP address range and "common name" is made here that the server can route to the correct client.*

3. Create a directory with exactly the same name as specified above under the working directory of the OpenVPN package (e.g. C:\Program Files\OpenVPN\config\ccd).

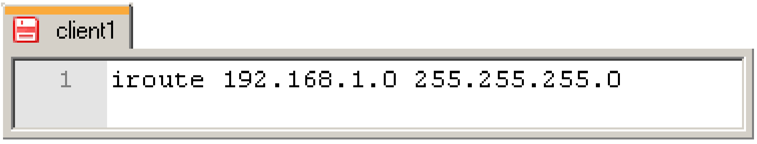


4. Create a text file in this directory for each client, which defines the IP address range behind the client. The file name of this text file must be identical with the "common name" of the client and must not have a file extension.



ⓘ *Observe the capitalization with this!*

5. Enter the **iroute** command with specification of the respective IP address range into each file.



```
iroute 192.168.1.0 255.255.255.0
```

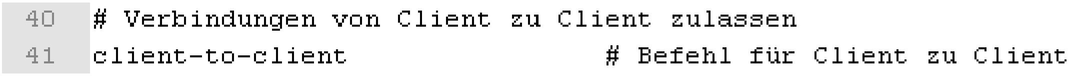
ⓘ *Only on line gets into this text file!*

6. Add new lines with the **route** command at the end of the configuration file to inform the operating system about the IP address ranges, which are to be routed through the tunnel(s) (2 clients are assumed in the following examples).

```
# Windows-Routen hinzufügen
route 192.168.1.0 255.255.255.0
route 192.168.2.0 255.255.255.0
```

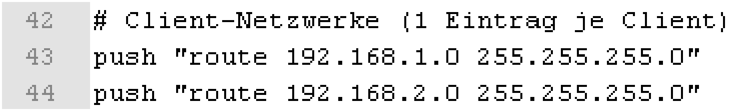
▶ *If client to client connections are to be allowed as well, the following steps must also be performed.*

7. Add a new line with the **client-to-client** command to allow connections between the individual clients.



```
# Verbindungen von Client zu Client zulassen
client-to-client                  # Befehl für Client zu Client
```

8. If you want to treat all clients the same, i.e. each client is allowed to communicate with each client, add new lines with the **push** command at the end of the configuration file. This informs each client about all client address ranges (except the own) that a direct communication is possible again.



```
# Client-Netzwerke (1 Eintrag je Client)
push "route 192.168.1.0 255.255.255.0"
push "route 192.168.2.0 255.255.255.0"
```

▶ *If only certain clients are allowed to communicate with certain clients due to reasons of safety, above* ***push*** *commands must not be entered into the server configuration file. In this case, the* ***push*** *command must be entered following the* ***iroute*** *command into the text file (in the "ccd" sub-directory) of the client that is allowed to communicate. One line must be entered for each client that can be reached from this client.*

9. Save the modified configuration file.

   ✓ You have adjusted the configuration file to your application with this.

Initial Operation

Start the OpenVPN server now to set up an OpenVPN network together with the clients. The following steps are necessary for this:

- **Starting the OpenVPN-Server**

  How to start the OpenVPN server with the computer already in operation. This option via the GUI is suitable for testing the configuration. The option to start the OpenVPN server automatically with the start of the computer is described below.

→ The OpenVPN package is installed on the computer, which shall act as server.

→ You have already saved server certificate and key, CA certificate and Diffie-Hellman parameter set in the OpenVPN working directory.

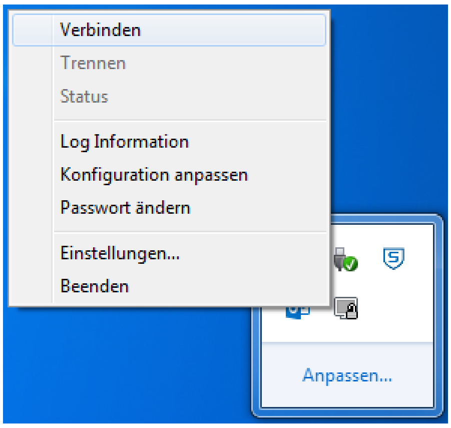
→ You have adjusted the configuration file to your application.

1. Start the OpenVPN GUI via Start → Program Files → OpenVPN → Open-VPN GUI or the desktop icon.

   ⓘ *The OpenVPN GUI must be „run as administrator“ (via the context menu) explicitly under Windows 7 and Windows Vista . It is not sufficient to be registered as administrator when the OpenVPN GUI is started.*

2. If necessary, click on the symbol for showing the hidden icons in the task bar .

3. Right-click onto the symbol of the OpenVPN GUI in the task bar and select Connect (or server → Connect (server indicates your configuration file here; in our example server.ovpn)).



✓ You have started the OpenVPN server with this. The symbol of the OpenVPN GUI is displayed green. The OpenVPN server is ready now to accept client connections. A connection log can be displayed using the menu item "View Log".

▶ *The respective service can also be enabled for an automatic start of the OpenVPN server with the start of the computer.*

ⓘ *In this case, instances for all configuration files, which are present in the working directory of the OpenVPN package, will be started. Therefore, delete all configuration files, which are not required, from the directory.*

1. Open the Control Center via Start → Settings → Control Center.
2. Double-click in the section "Control Center" the entry "Management".
3. Double-click in the section "Management" the entry "Services".
4. Double-click in the section "Services" the entry "OpenVPNService".
5. Change the "Start type" to "Automatic" and click on "OK".

✓ You have configured the OpenVPN server for an automatic start when starting up the computer.

3 Used Components

Software

Description	Manufacturer	Type	Version
OpenVPN package	Open Source	OpenVPN with GUI	2.3.3
Operating system	Microsoft	Windows	7

Table 1: Used software

4 Further Information

4.1 Literature

OpenVPN
Das Praxisbuch
ISBN: 978-3-8362-1197-0
Publisher: Galileo Computing

OpenVPN
Grundlagen, Konfiguration, Praxis
ISBN: 978-3-89864-396-2
Publisher: dpunkt.verlag

4.2 Web Links

OpenVPN Technologies, Inc.:
http://www.openvpn.net

OpenVPN e.V.:
http://www.openvpn.eu

Germany

INSYS icom GmbH
Hermann-Köhl-Str. 22
93049 Regensburg
Germany

Phone	+49 941 58692 0
Fax	+49 941 58692 45
E-mail	info@insys-icom.com
URL	www.insys-icom.com

Czech Repulic

INSYS icom CZ, s.r.o.
Slovanská alej 1993 / 28a
326 00 Plzen-Východní Předměstí
Czech Republic

Phone	+420 377 429 952
Fax	+420 377 429 952
Mobile	+420 777 651 188
E-mail	info@insys-icom.cz
URL	www.insys-icom.cz