INSYS icom
Industrial Data Communication

VPN with INSYS routers

Configuring OpenVPN server with authentication via static key

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	1.4
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

In the following, you will find a description of how to set up the INSYS router as OpenVPN server with authentication via static keys.

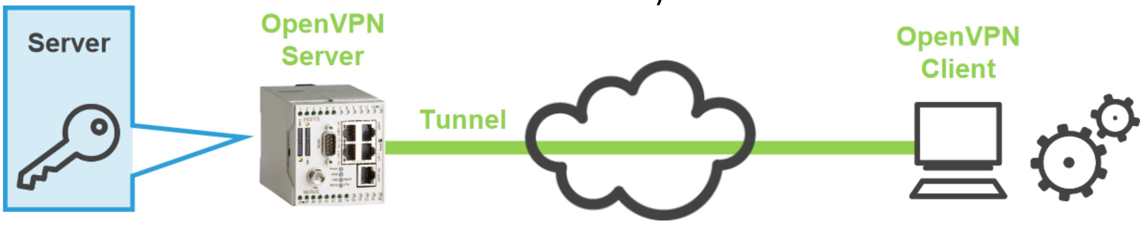


Figure 1: Configuring an OpenVPN server with authentication via static keys

2 Summary

OpenVPN Server Configuration

How to configure an INSYS router as OpenVPN server. You will find detailed step by step instructions in the following section.

1. Open in the menu → Dial-In / Dial-Out / LAN (ext) / WWAN the page → OpenVPN server
2. Check "Activate OpenVPN server"
3. Save settings
4. "Generate a new static key"
5. Check "No authentication or authentication with preshared key"
6. Download static key
7. Enter "IP address or domain name of remote site"
8. Enter local and remote IP address of the VPN tunnel
9. Enter "Netaddress of network behind the VPN tunnel" and "Netmask of network behind the VPN tunnel" if required
10. Save settings

3 Configuration

Provisions

Please prepare the following items before starting the configuration:

- **Connection to the INSYS router**

→ INSYS router is connected to power supply and ready for operation.
→ You have access to the INSYS router via your web browser.
→ Date and time are correctly set in the INSYS router.

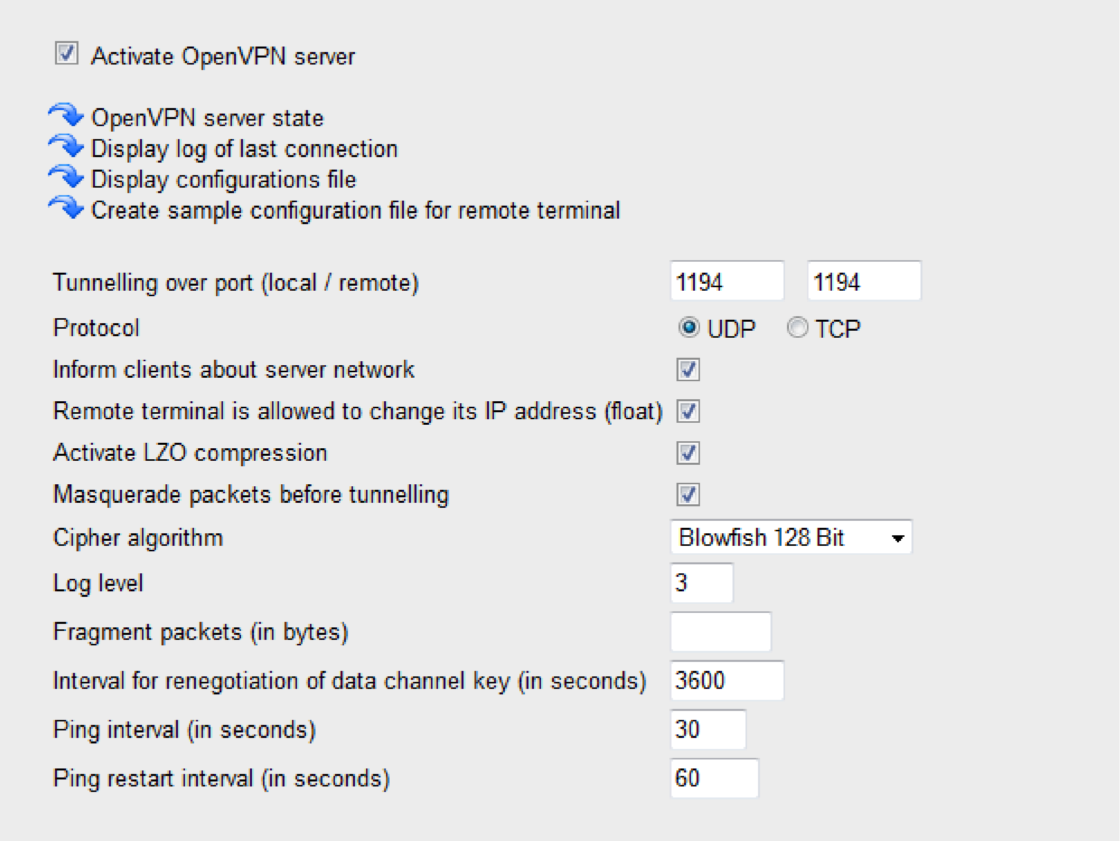
- **Configuring the OpenVPN Server**

How to configure the connection data to the remote terminal for the connection set-up of the OpenVPN server.

1. Select in the menu the page → OpenVPN server.

ⓘ *This page is under the menu item Dial-In, Dial-Out, LAN (ext), or WWAN depending on the used INSYS router.*

2. Check the check box "Activate OpenVPN server".



☑ Activate OpenVPN server

- OpenVPN server state
- Display log of last connection
- Display configurations file
- Create sample configuration file for remote terminal

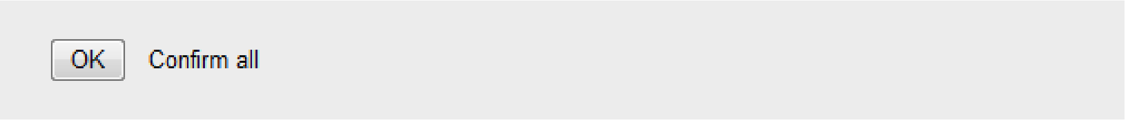
Tunnelling over port (local / remote)	1194 / 1194
Protocol	● UDP ○ TCP
Inform clients about server network	☑
Remote terminal is allowed to change its IP address (float)	☑
Activate LZO compression	☑
Masquerade packets before tunnelling	☑
Cipher algorithm	Blowfish 128 Bit
Log level	3
Fragment packets (in bytes)	
Interval for renegotiation of data channel key (in seconds)	3600
Ping interval (in seconds)	30
Ping restart interval (in seconds)	60

3. Configure the further OpenVPN parameters according to your application.

ⓘ *The default settings can be maintained for most applications. It is important that client and server have a consistent configuration.*

ⓘ *You can check the settings in OpenVPN syntax using the "Display configuration file" link. You can display settings, which might be suitable for the remote terminal, using the "Create sample configuration file for remote terminal" link.*

4. Click OK at "Confirm all" to save the settings.



OK Confirm all

✓ The connection data to the remote terminal for the connection set-up of the OpenVPN server is configured with this.

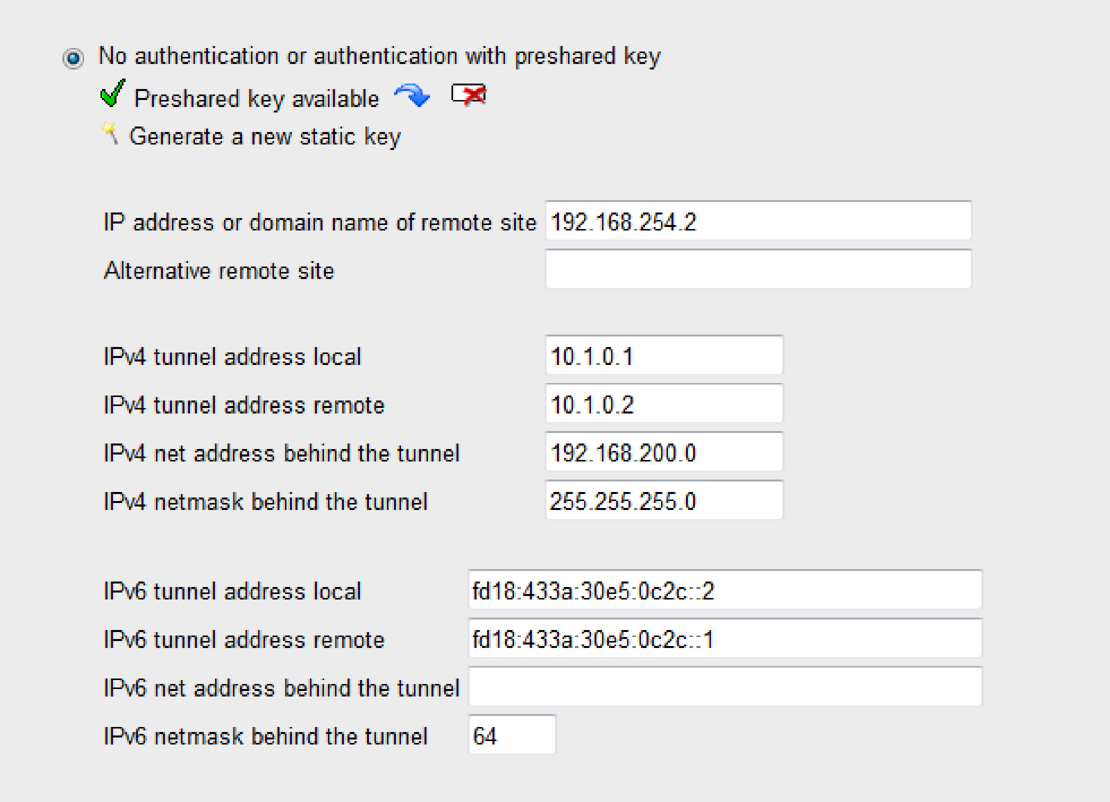
■ Configuring Authentication with Static Key

How to configure the authentication with static key for an OpenVPN server and generate the key for the OpenVPN client.

1. Select in the menu the page → OpenVPN server.

ⓘ *This page is under the menu item Dial-In, Dial-Out, LAN (ext), or WWAN depending on the used INSYS router.*

2. Scroll down to → No authentication or authentication with preshared key.



● No authentication or authentication with preshared key

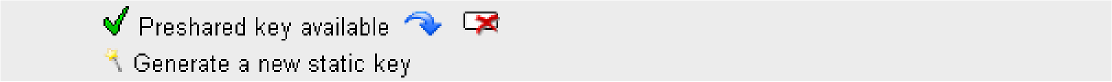
✓ Preshared key available

Generate a new static key

IP address or domain name of remote site	192.168.254.2
Alternative remote site	
IPv4 tunnel address local	10.1.0.1
IPv4 tunnel address remote	10.1.0.2
IPv4 net address behind the tunnel	192.168.200.0
IPv4 netmask behind the tunnel	255.255.255.0
IPv6 tunnel address local	fd18:433a:30e5:0c2c::2
IPv6 tunnel address remote	fd18:433a:30e5:0c2c::1
IPv6 net address behind the tunnel	
IPv6 netmask behind the tunnel	64

3. Click on the link "Generate a new static key".

✓ A new static key is generated and a green check mark appears instead of the red "X" at "... preshared key available ...".



✓ Preshared key available

Generate a new static key

ⓘ *No authentication will be used if no static key is present. This is not recommended and only useful for test purposes because the data sent through the tunnel will not be encrypted without authentication.*

ⓘ *OpenVPN client and OpenVPN server require the same static key!*

4. Click on the blue arrow behind "Preshared key available" to download the generated static key and save it.

   ⓘ *This static key must also be uploaded to the client to allow a connection.*

   ▶ *You can also use an already existing static key by uploading this in the "Upload key or certificates" section. The same key must also be present on the client.*

5. Select the option "No authentication or authentication with preshared key".
6. If necessary, adjust the OpenVPN client data at "IP address or domain name of remote site".

   ⓘ *This may be necessary, if this IP address is in a used address range. This IP address should always be in an unused, private address range. This information may not be omitted.*

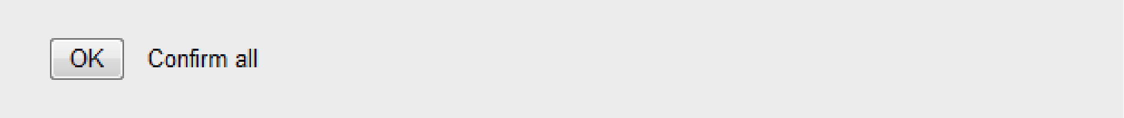
7. Enter the IP address of the local tunnel end into the "IP address of VPN tunnel local" field and the IP address of the remote tunnel end into the "IP address of VPN tunnels remote" field.

   ⓘ *These IP addresses must be swapped at the VPN remote terminal of the client, i.e. the address, which is the local tunnel end at the server, is the remote tunnel end at the client, and vice versa. The default settings can be used here in most cases.*

8. If required, enter the network address of the network, to which the VPN tunnel is to be established, into the "Netaddress of the network behind the VPN tunnel" field and the netmask of this network into the "Netmask of network behind the VPN tunnel" field.

   ⓘ *This is only necessary, if the IP addresses are in a network, which is already used either local or at the remote terminal. In this case, the IP address of a network is an address ending with "0", e.g. 192.168.200.0. The network mask in this case is 255.255.255.0.*

9. Click OK at "Confirm all" to save the settings.



✓ The authentication via static key is configured with this.

4 Used Components

Please observe: The power supply units required to operate devices are not listed here in detail. Take care for a provision at the site, if they are not part of the scope of delivery.

Hardware

Description	Manufacturer	Type	Version
Router	INSYS	INSYS router	Firmware 2.12.1

Table 1: Used hardware

Software

Description	Manufacturer	Type	Version
Operating system	Microsoft	Windows 7	SP1
Browser	Mozilla	Firefox	30

Table 2: Used software

Notes

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