INSYS icom

Industrial Data Communication

# VPN with INSYS routers

## Configuring OpenVPN client with certificate-based authentication

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 client with certificate-based authentication.

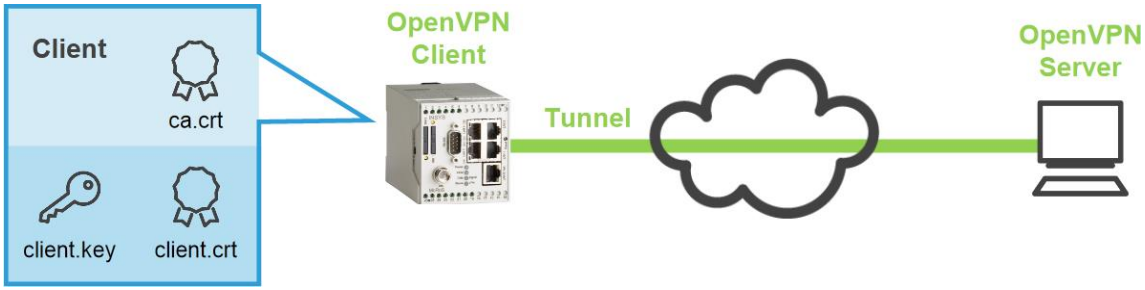



Figure 1: Configure the OpenVPN Client with certificate-based authentication

# 2 Summary

## OpenVPN Client Configuration

How to configure an INSYS router as OpenVPN client. 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 → Open-VPN client
2. Upload CA certificate
3. Upload client certificate
4. Upload client key
5. Check "Activate OpenVPN client"
6. Enter "IP address or domain name of remote site"
7. Check "Authentication based on certificate"
8. Check "Check remote certificate type" if required
9. 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.

### ■ Uploading Client Certificates and Keys

How to upload the certificates and keys for an OpenVPN client.

ⓘ *You can upload new files with existing configuration as well. All other configuration settings are maintained except overwriting possibly present files.*

→ The following files are required for uploading, which have been created before (refer to separate Configuration Guide) or provided for you:
public CA certificate, e.g. "ca.crt"
public client certificate, e.g. "client.crt"
secret client key, e.g. "client.key"

▶ *If you have received a PKCS#12 file that contains certificates and key (e.g. "Client_1.p12"), this already contains all files.*

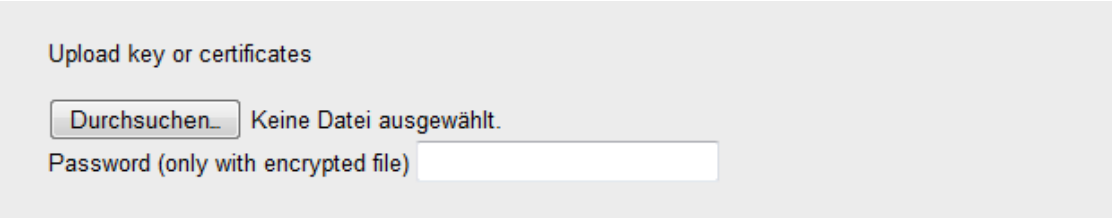
1. Select in the menu the page → OpenVPN client.

   ⓘ *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 → Authentication based on certificate.

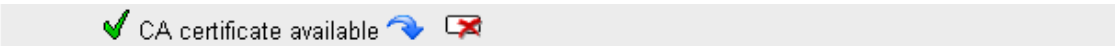
   ⓘ *The INSYS router detects the file type automatically and assigns the file correctly during the following upload.*

3. Click in the section "Upload key or certificates" on Browse...




4. Select the file with the CA certificate (e.g. "ca.crt").
5. Click OK to upload the file.

   ✓ A green check mark appears instead of the red "X" at "... CA certificate ...".



6. Proceed accordingly for the public certificate of the OpenVPN client (e.g. "client.crt") and the secret key of the OpenVPN client (e.g. "client.key") in order to upload both files to the INSYS router.

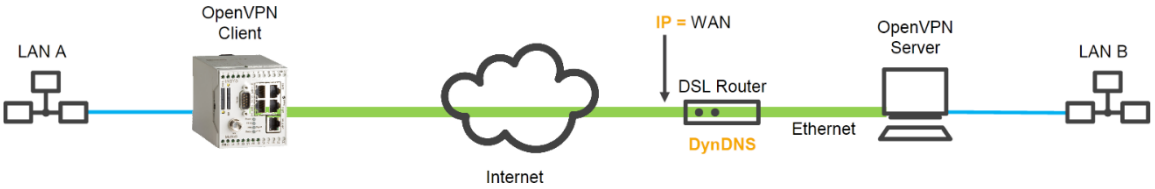
   ✓ A green check mark appears instead of the red cross for each uploaded file. Uploading the certificates and keys is completed with this.

## ■ Configuring Connection Data to the Remote Terminal and Certificate-Based Authentication

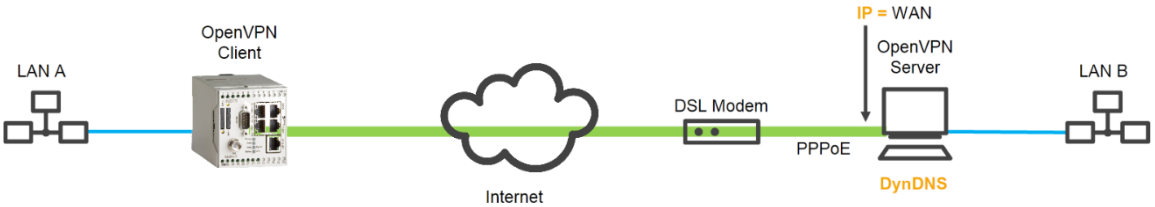
How to configure the connection data to the remote terminal for the connection set-up of the VPN client and the authentication with certificates.

→ You must know the IP address accessible via the internet or the domain name of the remote terminal.

ⓘ *This IP address depends on the architecture of the server network. If the server is behind a DSL router like in the following figure for example, its WAN IP address must be used. A corresponding port forwarding rule of the tunnel to the server must be present in the DSL router.*




ⓘ *If the server is directly connected to a DSL modem without intermediate router like in the following figure, the IP address of the server must be used.*

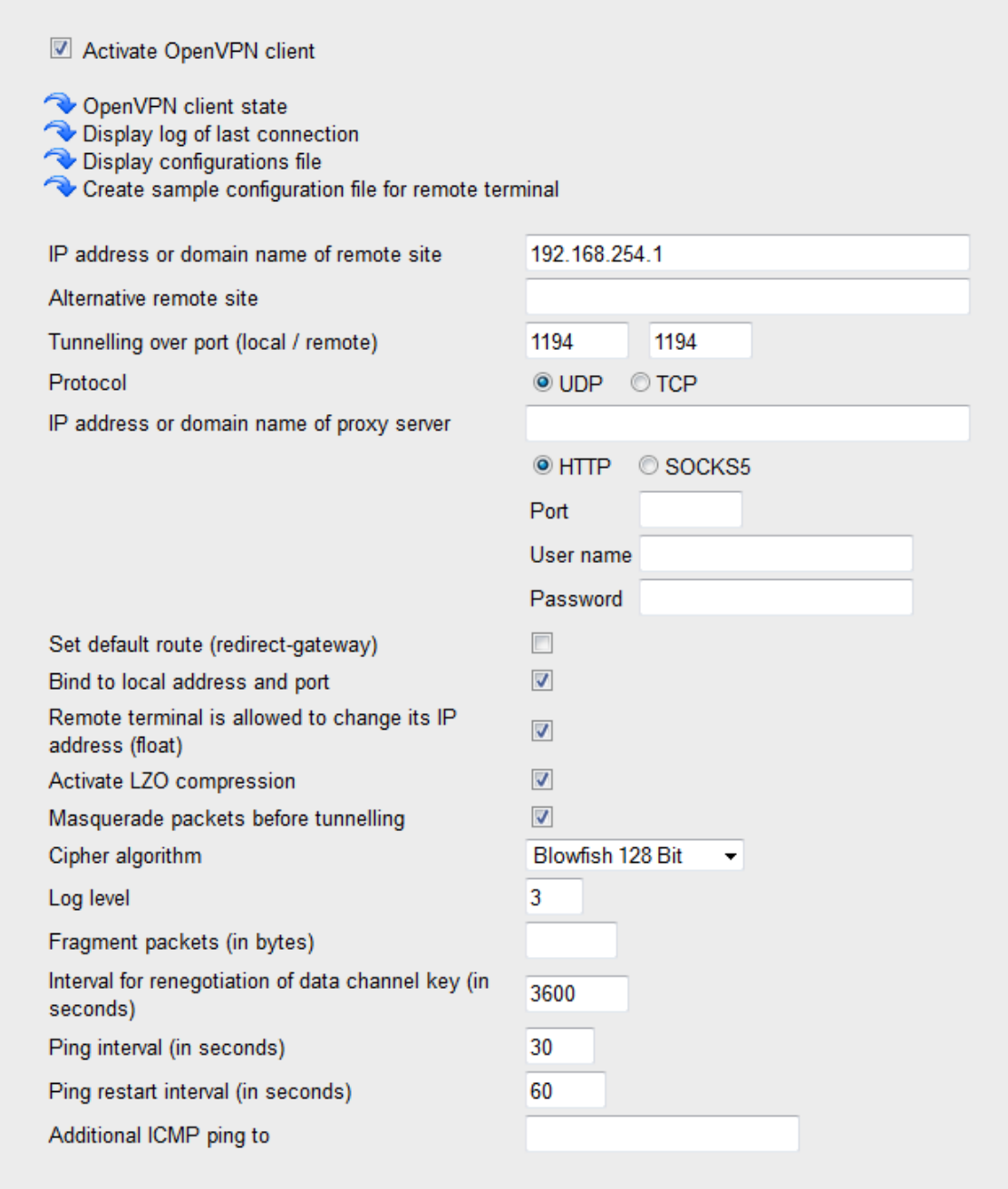



ⓘ *If the server has no fixed IP address, a DynDNS domain name can also be entered, which will then be resolved by the client. For this, DynDNS must be enabled in the DSL router (first example) or in the server (second example). Information about this can be found in the documentation of the respective devices. A DNS server must also be entered in the INSYS router for this.*

2. Select in the menu the page → OpenVPN client.

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

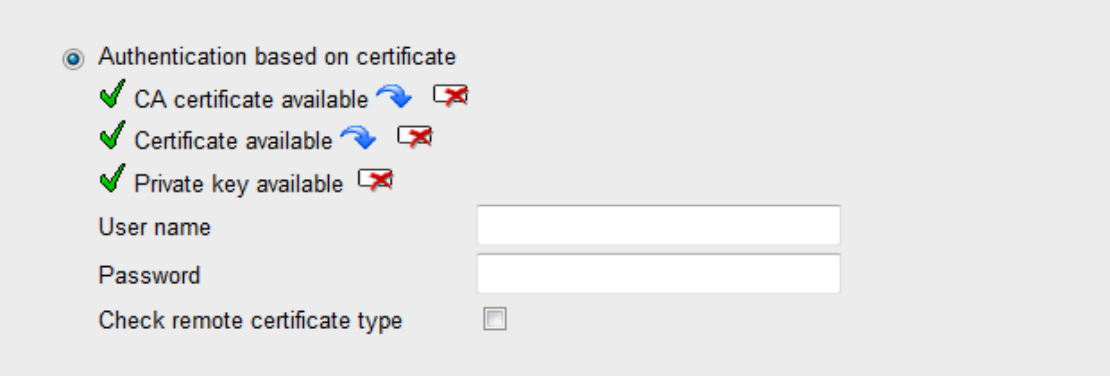
3. Check the check box "Activate OpenVPN client".
4. Enter the IP address accessible via the internet or the domain name of the OpenVPN server into "IP address or domain name of remote site".




5. Configure the further OpenVPN parameters according to the configuration of your server.

   ⓘ *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.*

6. Scroll down to → Authentication based on certificate.

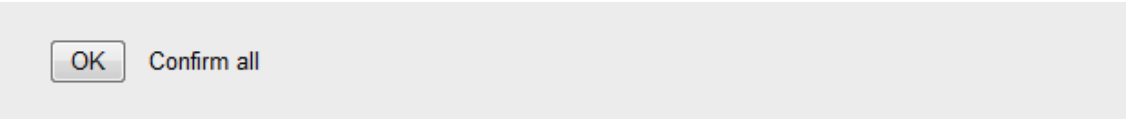



7. Select the "Authentication based on certificate" option.
8. Check "Check remote certificate type" if required.

   ⓘ *Client checks server certificate for certification by the common certification authority (CA certificate). This might not be essential and depends on the server.*

   ▶ *In addition to the authentication with certificates, the server might also require the authentication with user name / password.*

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




   ✓ The remote terminal for the connection set-up of the VPN client 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

**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