

REX300

Application examples

Edition 2 / 26.05.2010

HW 1 and FW 2.02 and higher



All rights are reserved, including those of translation, reprinting, and reproduction of this manual, or parts thereof. No part of this manual may be reproduced, processed, copied, or transmitted in any way whatsoever (photocopy, microfilm, or other method) without the express written permission of Systeme Helmholtz GmbH, not even for use as training material, or using electronic systems. All rights reserved in the case of a patent grant or registration of a utility model or design.

Copyright © 2010 by

Systeme Helmholtz GmbH

Hannberger Weg 2, 91091 Grossenseebach, Germany

Note:

We have checked the content of this manual for conformity with the hardware and software described. Nevertheless, because deviations cannot be ruled out, we cannot accept any liability for complete conformity. The information in this manual is regularly updated. When using purchased products, please heed the latest version of the manual, which can be viewed in the Internet at www.helmholz.de, from where it can also be downloaded.

Our customers are important to us. We are always glad to receive suggestions for improvement and ideas.

Revision history of this document:

Edition	Date	Revision
1	28.01.2010	First edition
2	26.05.2010	VPN applications added, minor changes

Contents

1	Overview	7
1.1	Application and function description	7
1.2	Information in the figures	7
2	Overview of the Web interface	8
2.1	Menu structure	8
2.2	Menu overview	8
3	Active Internet connection scenarios	11
3.1	Internet connection via analog/ISDN/EDGE modem	11
3.1.1	Internet connection via an analog modem	11
3.1.2	Internet connection via EDGE Modem	14
4	Passive Internet connection scenarios	17
4.1	REX 300 behind an Internet gateway	17
4.2	REX 300 with a public IP address	19
5	Access to the REX 300 via the Internet	21
5.1	IP address via e-mail	21
5.2	DNS name resolution	23
6	Point-to-point connections	24
6.1	Analog direct connection	24
6.2	GSM direct connection	26
6.3	Setting up a dial-up connection	28
7	VPN (Client-Router)	33
7.1	OpenVPN (with wizard)	33
8	VPN (Router-Router)	40
8.1	OpenVPN (with wizard)	40
8.1.1	Setting up the OpenVPN server (REX 300)	40
8.1.2	OpenVPN Client	44
9	Certificates	50
9.1	Overview of certificates	50
9.2	Creating certificates	50
9.2.1	Creating a root certificate	51

9.2.2	Creating a client certificate	56
9.3	Creating CRL files (certificate revocation lists)	62
9.4	Importing certificates under Windows XP	64
10	Troubleshooting	67
10.1	Firmware update	67
10.2	Frequently asked questions	69
11	Important Information about VPN	70
11.1	Basic information	70
11.2	OpenVPN	70
11.2.1	Ports	70
11.2.2	Proxyserver	70
11.2.3	Encryption methods	70
12	List of Sources	71

1 Overview

1.1 Application and function description

The REX 300 is intended to be used as an Ethernet router for the remote maintenance of S7-300 and S7-400 systems. It has an integrated MPI/DP interface. This MPI/DP interface supports MPI and PROFIBUS with up to 12 Mbps. The REX 300 enables remote servicing of the S7 systems via the Internet. Depending on the available connection to the Internet, the REX 300 is obtainable with various integrated modems or integrated interfaces. It can establish the Internet connection via an analog, ISDN, or GPRS/EDGE modem. Moreover, an external DSL modem can be connected to the REX 300 devices with a WAN interface. The WAN interface can be used through an Internet connection already provided through a server or a gateway.

This document is intended as a supplement to the “*REX 300*” Quickstart Guide and Manual.

It is intended to provide the user with step-by-step support with setting up the connection.



Please pay attention to the information in the figures

1.2 Information in the figures

In the printed figures, important settings and notes for the user are highlighted in red.

2 Overview of the Web interface

The following text provides an overview of the Web interface integrated in the REX 300.

2.1 Menu structure

The web user interface of the REX 300, is divided into a main menu on the left and a corresponding submenu at the top of your browser window. The following Figure 2-1 shows the menu structure.

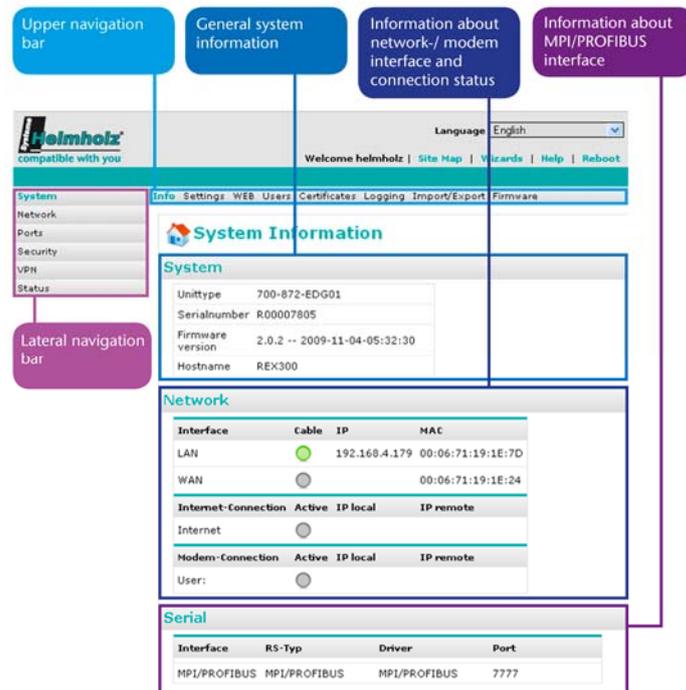


Fig. 2-1: Menu structure

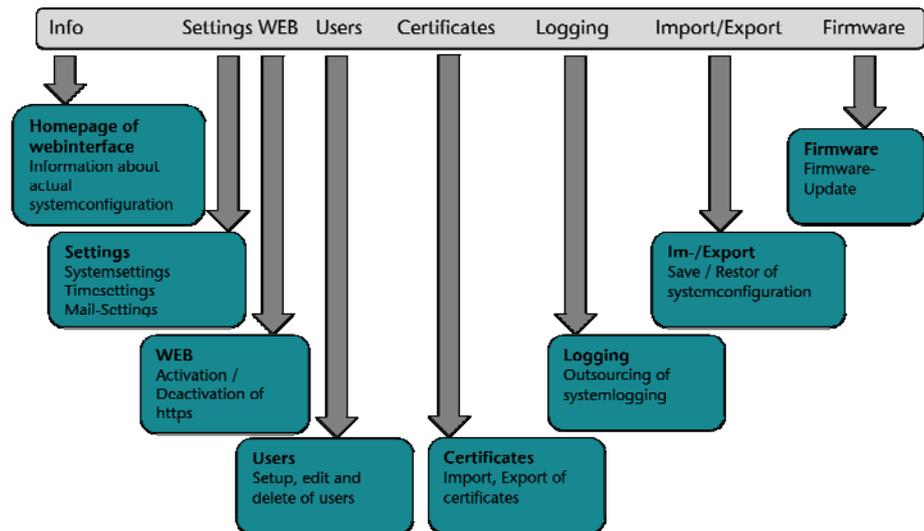
2.2 Menu overview

The following figures show the menus available to you in the REX 300. The following submenus of the main menus are explained:

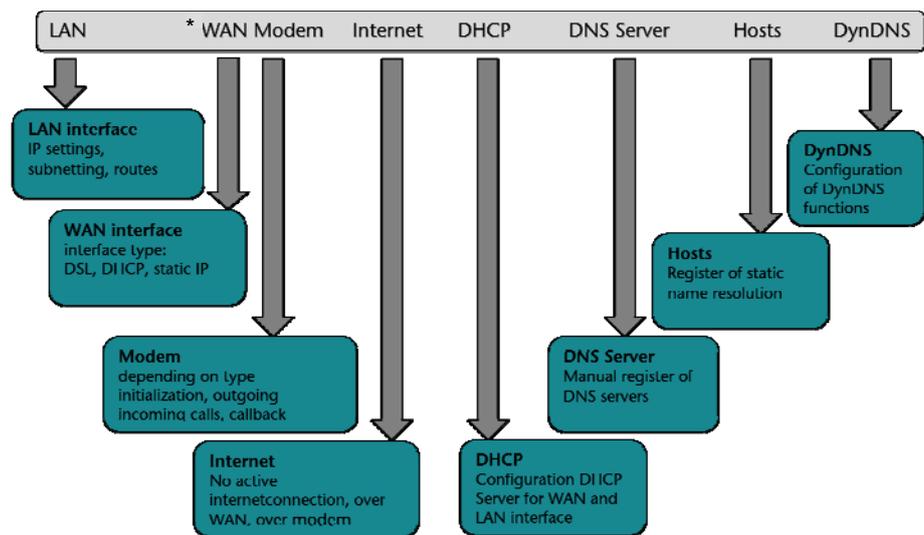
- System,
- Network,
- Interfaces,
- Security settings
- VPN.

The Status main menu with its various submenus provides general information about the devices and is primarily used for diagnostics.

System menu:

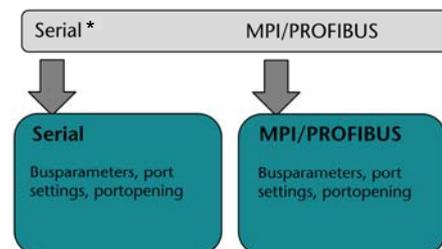


Network menu:



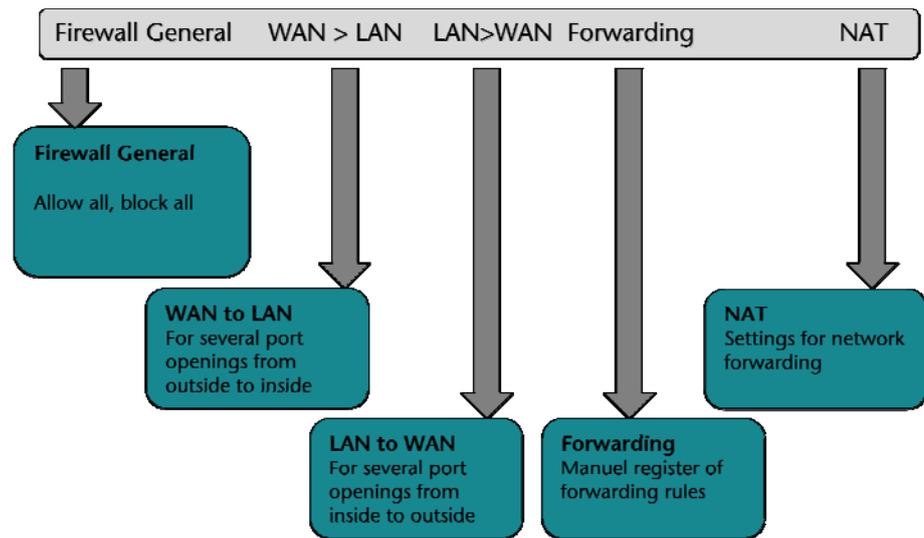
* for WAN devices only

Interfaces menu:

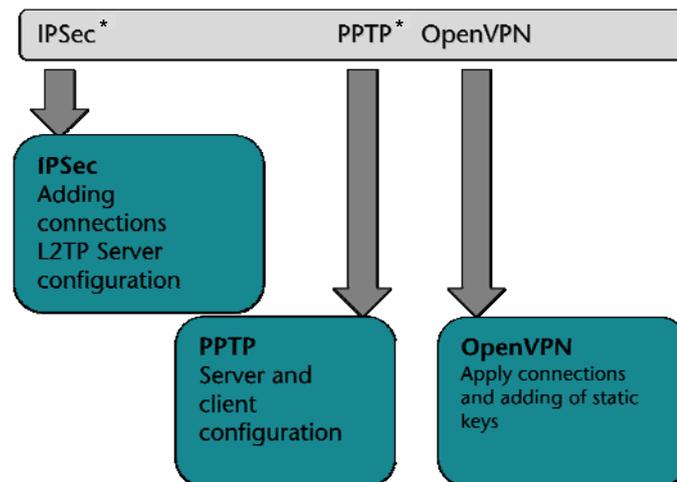


* for WAN devices only

Security settings menu:



VPN menu:



* for VPN/WAN devices only

3 Active Internet connection scenarios

The steps explained in this manual are all performed manually. Configuration of the LAN, Internet, and VPN connection is also possible using the wizard integrated into the web interface.

The following steps must be performed in the sequence described:

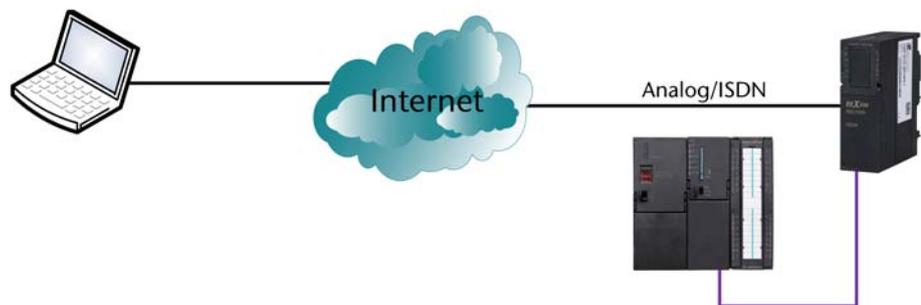
3.1 Internet connection via analog/ISDN/EDGE modem

This section explains the connection with the Internet via the various modems.

The prerequisite of the Internet connections show is an analog or ISDN phone line (Fig. 3-1-1), or a SIM card with enabled data service for GPRS communication.

3.1.1 Internet connection via an analog modem

Fig. 3-1-1: Internet via an analog or ISDN line



Step-by-step instructions:

1. It is first necessary to connect the device to an analog phone line. The analog phone line is connected via the RJ socket under the front hatch.

Fig. 3-1-2: Modem socket on the REX 300



2. Now it is necessary to communicate to the device via the web interface to inform it how the Internet connection will be established.
3. To establish the Internet connection via an analog phone line, it is necessary to enter an Internet-by-call provider in

the device. This is entered under menu item Network > Modem.

4. Under this menu item, it is important to enter the phone number of the Internet-by-call provider, the user names, and the password. This data is usually found on the web site of the provider.

The screenshot displays the Helmholtz System Modem Configuration interface. The top navigation bar includes the Helmholtz logo, a language dropdown set to English, and links for Welcome, Site Map, Wizards, Help, and Reboot. A secondary navigation bar lists System, LAN, WAN, Modem, Internet, DHCP, DNS Server, Hosts, and DynDNS. A left sidebar contains Network, Ports, Security, VPN, and Status. The main content area is titled 'Modem Configuration' and 'Modem Settings'. It features a form with the following fields: Modem Type (ANALOG), Modem Init (+GCI=FD), and another Modem Init (X3). Below these are three tabs: Outgoing, Incoming, and Call Back. The Outgoing tab is selected, showing fields for Phone Number (0.019193384), User (egal), Password (****), Authentication via PAP (checked), Authentication via CHAP (checked), and Timeout Dialout (300). A 'Save Changes' button is located at the bottom right of the form.

Fig. 3-1-3: Settings on the Modem tab

- Now, because the modem is configured, settings still have to be entered under menu item Network > Internet. Here, it is possible to set that the Internet connection will be established via the modem. It is also possible to define when the Internet connection will be established. In this example, it is possible to activate call-back by the device to establish the Internet connection. This is done with the dial-out key or by a call on the device. If call-back is activated, the modem disconnects after four ring tones and then dials the stored Internet-by-call number. (Fig. 3-1-4)

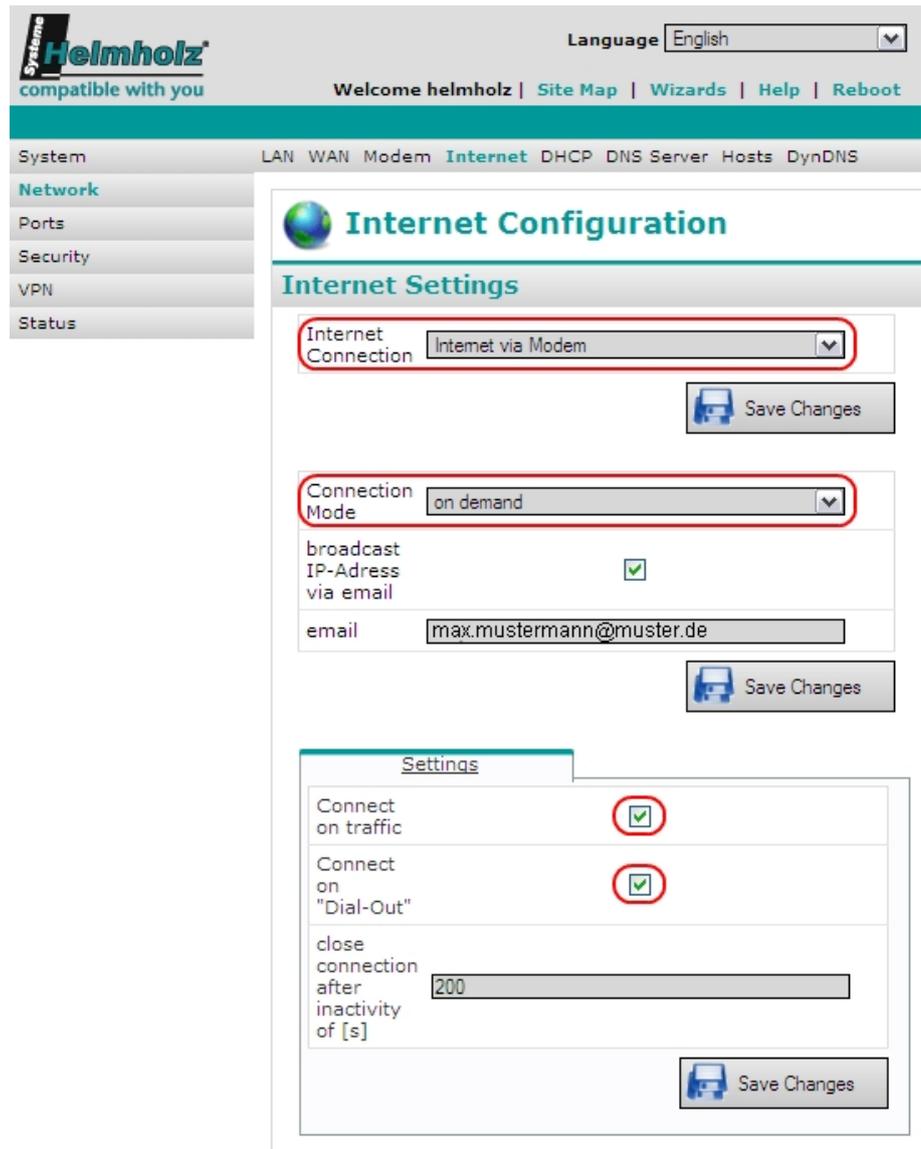
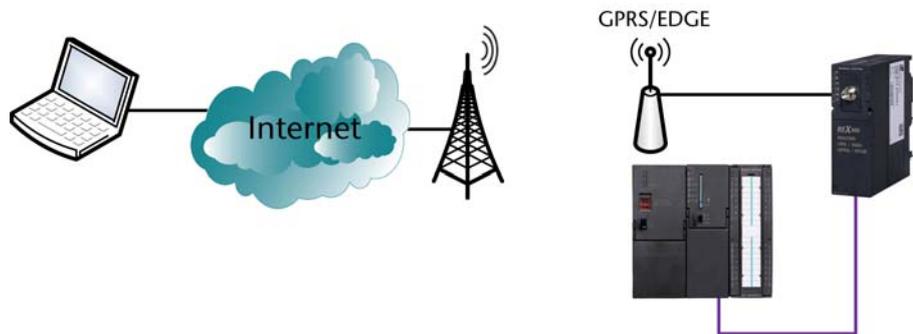


Fig. 3-1-4: Settings on the Internet tab

- How the device is accessed from the Internet is explained in a general explanation in Section 5.

3.1.2 Internet connection via EDGE Modem

Fig. 3-1-2: Internet with SIM card via GSM (GPRS/EDGE)



Step-by-step instructions:

1. First it is necessary to insert a SIM card on which a data service is activated. The providers supported by the integrated wizard are T-Mobile, Vodafone, Eplus, and O2. The relevant parameters can be set manually. This is done with the setting "Other provider." This example explains how the settings are made for a T-Mobile card from Germany (manually).

Provider dial-in data:

Provider (German)	T-Mobile	Vodafone	EPlus	O2
Phone number	*99***1#	*99***1#	*99***1#	*99***1#
User	any	blank	eplus	blank
Password	any	blank	gprs	blank
Data also apply to:	Congstar klarmobil callmobile REWE simply Tangens	Milleni.com PAYBACK smobil	BASE Blau MEDION-Mobile simyo uboot vybemobile	Fonic

2. If the device is equipped with a SIM card and the web interface has been opened, it is necessary to enter the following settings with menu items Network > Modem. (Fig. 3-1-3)

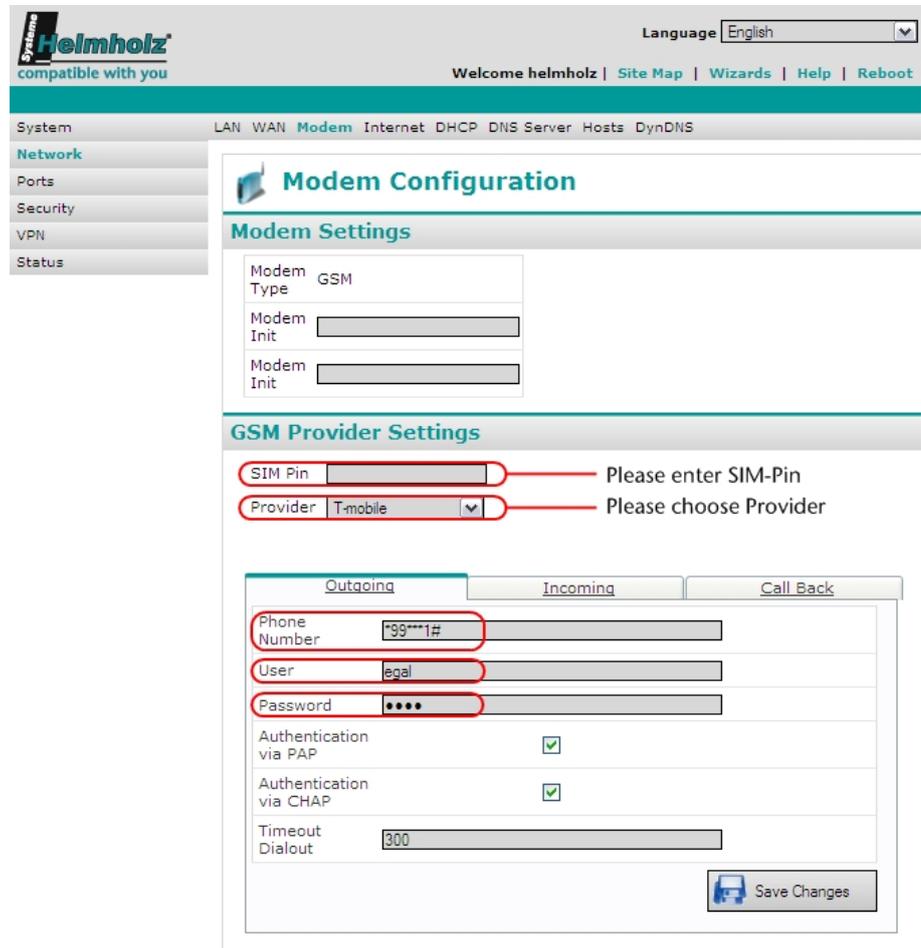


Fig. 3-1-3: Settings on the Modem tab



If the provider you want is not in the list of providers, set the phone number, user, APN, and password manually by choosing "Other provider" as the provider!

- Under menu item System > Internet, you can now define whether the Internet connection will remain permanently or only be established when required. The setting “on demand,” for example, permits establishment of an Internet connection after a call. That is, if you call the mobile number of the SIM card, 4 ring tones are allowed to elapse; the REX 300 then hangs up and dials into the Internet within 40 seconds. The Internet connection via modem must remain activated for this. (Fig. 3-1-4)

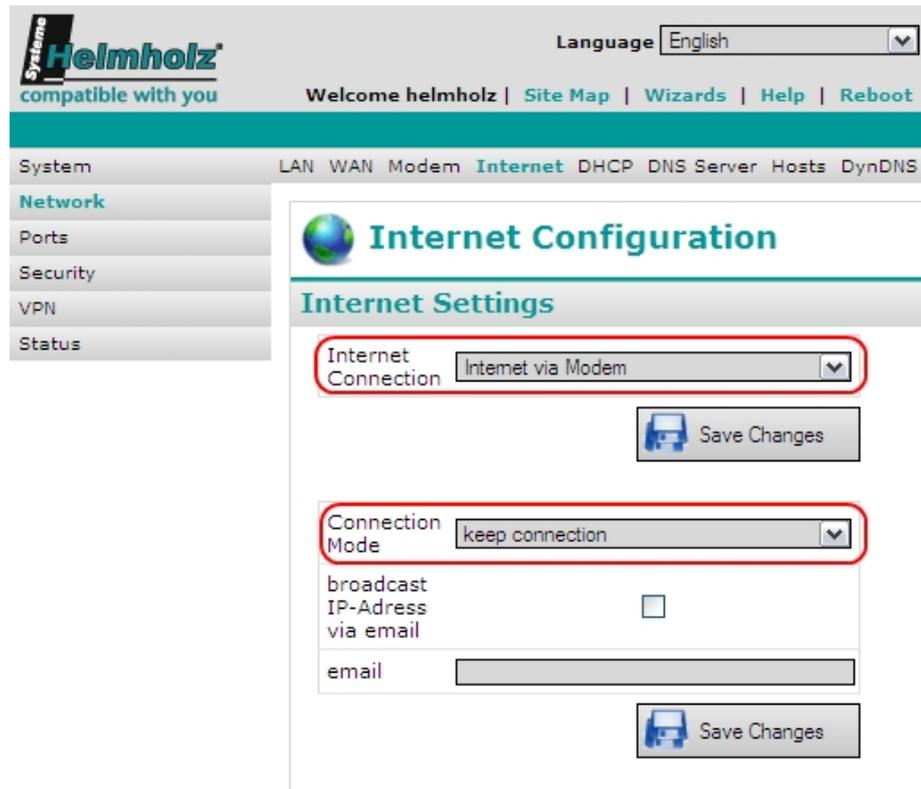


Fig. 3-1-4: Settings on the Internet tab

- How the device is accessed from the Internet is shown in the general explanation in Section 5.

4 Passive Internet connection scenarios

The following steps must be performed in the sequence described:

For the REX 300, a passive Internet connection is a connection through a device that provides an Internet connection. The REX 300 uses this Internet connection and therefore does not establish the connection itself.

A passive Internet connection is only supported by REX 300 with a WAN interface.

4.1 REX 300 behind an Internet gateway

This particular case means for the user that relevant settings must be made in the Internet gateway for a VPN connection to be established, for example. This refers to port redirections to internal IP addresses. It is shown below how the settings must be made in the REX 300 and not in the corresponding Internet gateway. Only the responsible administrator can usually make the settings of the Internet gateway.

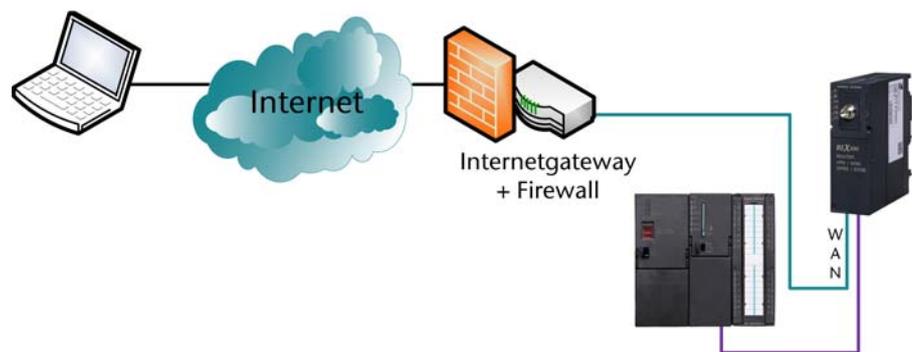


Fig. 4-1-1: REX behind an Internet gateway

Step-by-step instructions:

1. It is necessary for the WAN interface to be able to establish a connection with the Internet gateway. This connection can, of course, also be established via multiple switches or hubs.

- Under menu item Network > WAN, the settings for the WAN interface must be made. Here, the IP address, subnet mask, and gateway IP address can be set. Moreover, the WAN interface can be configured in such a way that the REX 300 automatically receives the parameters from a DHCP server. (Fig. 4-1-2)

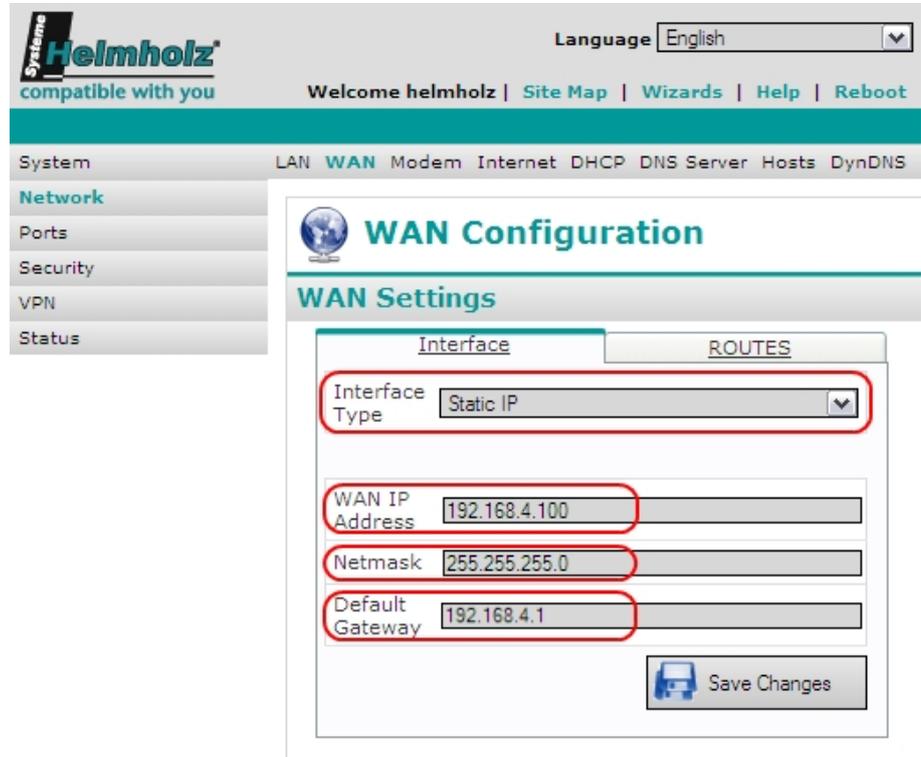


Fig. 4-1-2: Settings on the WAN tab

- In this example, the Internet gateway has the IP address 192.168.4.1 and the REX 300 has 192.168.4.100.
- Configuration of the Internet connection is performed under menu item Network > Internet and must look as shown in the figure. Because the REX 300 uses the Internet connection of another device, the Internet connection type is "No internetconnection" in this case. (Fig. 4-1-3)



Fig. 4-1-3: Settings on the Internet tab

- Now, the necessary settings have been made in the REX 300. Depending on the system implementation, the Internet gateway or the firewall now has to be configured to establish a VPN connection. Section 7 explains what port enables have to be set up for this purpose.

4.2 REX 300 with a public IP address

This connection scenario is similar to the previous scenario. The difference is that the device uses a public IP address and is not protected by an additional firewall. It is still protected by the internal REX 300 firewall.

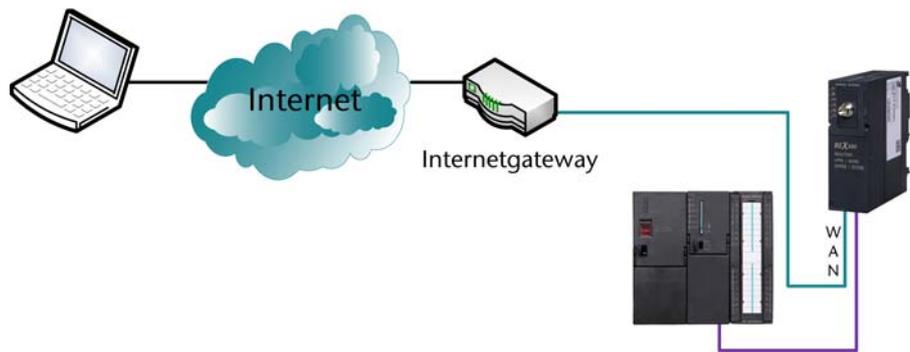


Fig. 4-2-1: REX 300 with a public IP address

Step-by-step instructions:

- The WAN interface must be able to establish a connection with the Internet gateway. This connection can, of course, be routed through multiple switches or hubs.
- Under menu item Network > WAN, the settings for the WAN interface must be made. Here, the IP address, subnet mask, and gateway IP address can be set. Moreover, the WAN interface can be configured in such a way that the REX 300 automatically receives the parameters from a DHCP server. (Fig. 4-2-2)

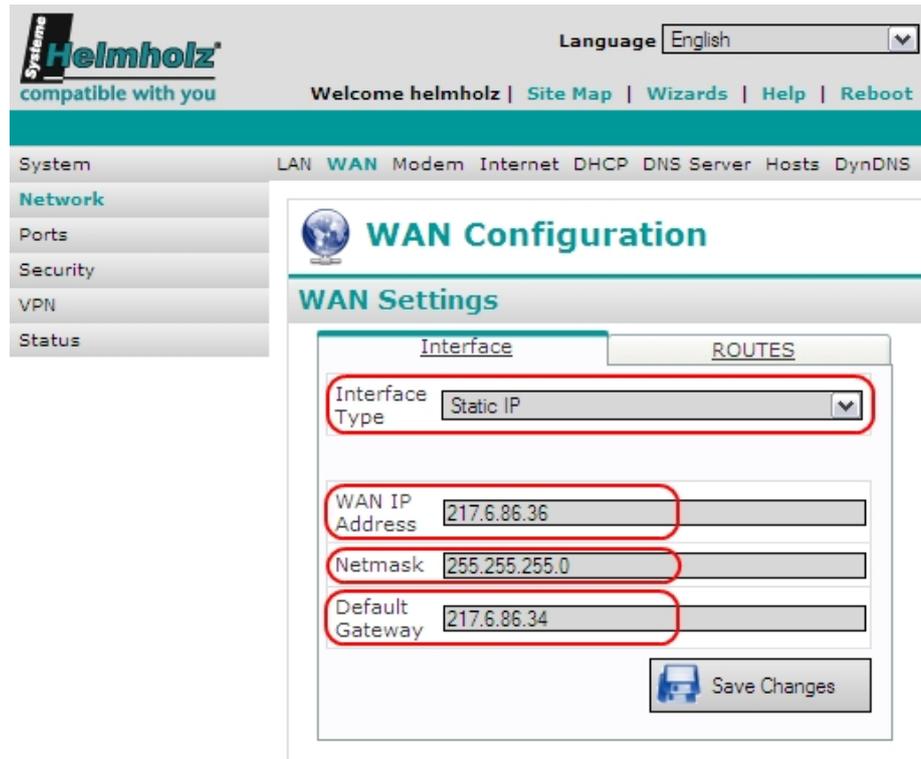


Fig. 4-2-2: Settings on the WAN tab

3. The REX 300 can be accessed directly via a public IP address via the relevant gateway (here: 217.6.86.34) in the Internet and is not in an internal network.
4. Configuration of the Internet connection is performed under menu item Network > Internet and must look as shown in the figure. Because the REX 300 uses the Internet connection of another device, the Internet connection type is "No internetconnection." (Fig. 4-2-3)

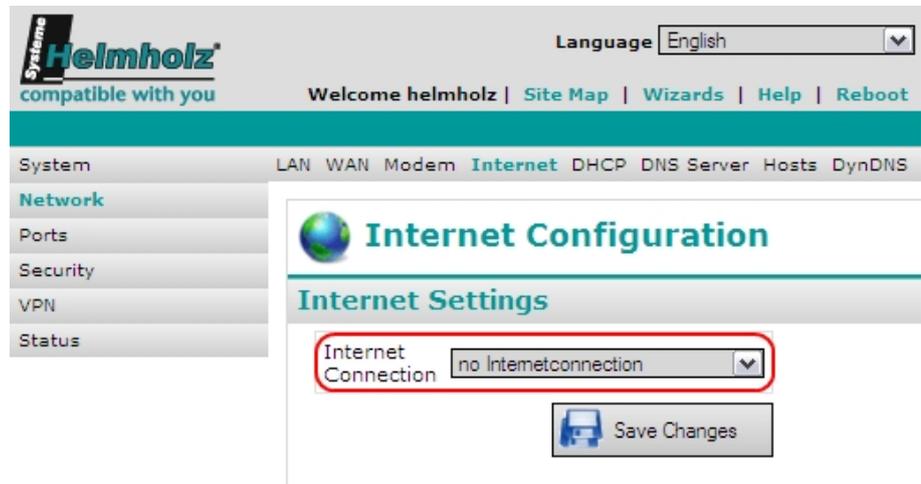


Fig. 4-2-3: Settings on the Internet tab

6. Now, the necessary settings have been made in the REX 300. Depending on the system implementation, the Internet gateway now has to be configured to establish a VPN connection. Section 7 explains what port enables have to be set up.

5 Access to the REX 300 via the Internet

For the following functions it is necessary for the REX 300 to have already established the Internet connection.

5.1 IP address via e-mail

Systeme Helmholtz GmbH offers the service of sending e-mails via a server that is provided free of charge. This free service allows you to find out the IP address that the REX 300 has obtained from the Internet Service Provider. The REX 300 sends an e-mail containing the IP address to the e-mail address you specified via the server of Systeme Helmholtz GmbH.

The necessary settings are preconfigured on delivery. That is, you do not have to set anything except the e-mail address to which the e-mail is to be sent. You can set your e-mail address under menu item Network > Internet for an Internet connection via modem or WAN.

Fig. 5-1-1: Settings on the Internet – e-mail with IP tab

The screenshot shows the Helmholtz web interface for Internet Configuration. The page title is "Internet Configuration" and the sub-section is "Internet Settings". The "Internet Connection" is set to "Internet via Modem". The "Connection Mode" is set to "keep connection". The "broadcast IP-Address via email" checkbox is checked and highlighted with a red box. The "email" field is empty. There are "Save Changes" buttons for both sections.

Setting	Value
Internet Connection	Internet via Modem
Connection Mode	keep connection
broadcast IP-Address via email	<input checked="" type="checkbox"/>
email	

You can also deactivate this automatic e-mail function and use your own server. You will find this function in the menu System > Settings > “Activate automatic e-mail settings.” (Fig. 5-1-2)

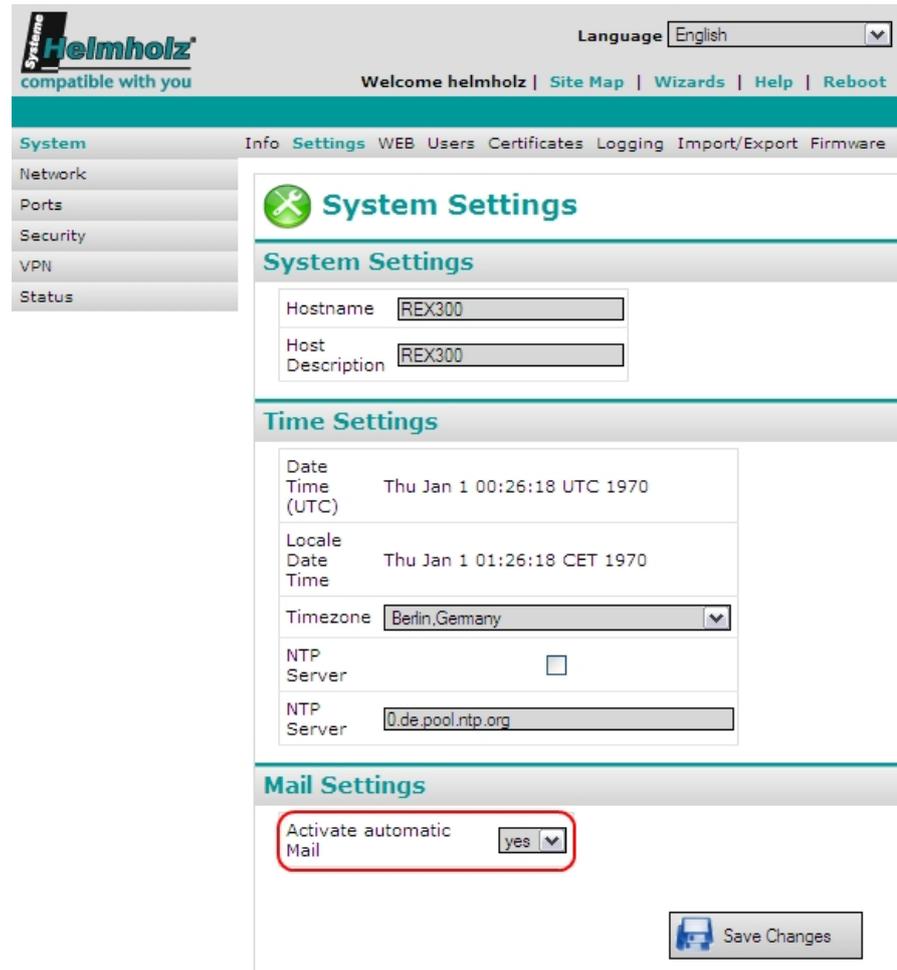


Fig. 5-1-2: IP address via e-mail

A manual setting would look like this. (Fig. 5-1-3)

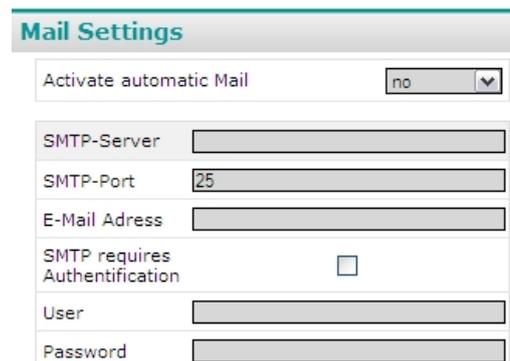


Fig. 5-1-3: Manual e-mail server settings

The IP address or your e-mail server and the e-mail address of the REX 300 now have to be entered under SMTP server. If authentication is necessary, a user and password have to be entered in addition.

5.2 DNS name resolution

To reach the REX 300 even more simply from the Internet, Systeme Helmholtz GmbH allows you to perform DNS name resolution using a free service.

That means that the IP address that is assigned to the REX 300 for an active Internet connection is converted to a permanent name. The REX 300 can then be reached by this name in the Internet. The necessary settings are preset in the REX 300. However, manual settings can also be made to be able to use, for example, other service providers for this function. You will find the settings under Network > DynDNS (Fig. 5-2-1)

Fig. 5-2-1: DNS service

The screenshot shows the web interface for configuring DynDNS on a Systeme Helmholtz device. The top navigation bar includes 'System', 'LAN', 'WAN', 'Modem', 'Internet', 'DHCP', 'DNS Server', 'Hosts', and 'DynDNS'. The left sidebar lists 'Network', 'Ports', 'Security', 'VPN', and 'Status'. The main content area is titled 'DynDNS Configuration' and 'Systeme Helmholtz DynDNS Service'. It displays the unit's access URL: 'R00007805.REX300.my-rex.net'. Below this, there is a checkbox for 'Enable System Dynamic DNS' which is checked. A 'Save Changes' button is visible. Further down, there is a section for 'public DynDNS Service' with fields for 'Enable' (unchecked), 'Provider' (set to 'dyn dns'), 'User', 'Password', 'Host Name', and 'Interval [s]'. A second 'Save Changes' button is located at the bottom of this section.

In this example, the REX 300 would be accessible via the name R00007821.REX300.my-rex.net. In the lower part of the display, manual settings are possible if a public DNS provider is to be used. The device name can be set in the menu System > Settings "Hostname"

Step-by-step instructions:

1. The integrated modem must be configured to permit PPP dialing under the menu item Network > Modem. (Fig. 6-1-2)



If you want to use a ISDN PPP connection you must enter "B10" in the "Modem Init"-Field.

The screenshot displays the 'Modem Configuration' interface. At the top, there's a navigation bar with 'System', 'LAN', 'WAN', 'Modem', 'Internet', 'DHCP', 'DNS Server', 'Hosts', and 'DynDNS'. The 'Modem' tab is active. Below this, the 'Modem Settings' section includes:

- Modem Type: ANALOG
- Modem Init: +GCI=FD
- Modem Init: X3

The 'Incoming' tab is selected, showing:

- Dialin enable:
- PPP Server IP-Address (here): 192.168.0.101
- PPP Client IP-Address: 192.168.0.102
- Dialin Authentication: every User with dialin rights
- Authentication via PAP:
- Authentication via CHAP:
- close connection after inactivity of [s]: 300

A 'Save Changes' button is located at the bottom right of the form.

Fig. 6-1-2: Settings on the Modem tab

2. On this page, it is also possible to set whether dial-in is to be permitted to just a certain user or to all users from the user list with dial-in rights.
3. The server-side (REX 300) connection is now parameterized. To be able to access the REX 300, it is necessary to set up a data telecommunication connection in your operating system. You will find a general explanation for this in Section 6.3.

6.2 GSM direct connection

Via this connection path, it is possible to access the MPI and PROFIBUS or LAN interface of the REX 300 independently of a connection with the Internet. In the following example, a PC with a modem connection is used as the client. For the PPP connection with a GSM modem, the CSD client must be enabled on the SIM card in the REX 300. This standard modem service usually has to be activated separately for each network provider. The CSD service limits the transmission rate for direct connections via the GSM network to 9.6 Kbps.

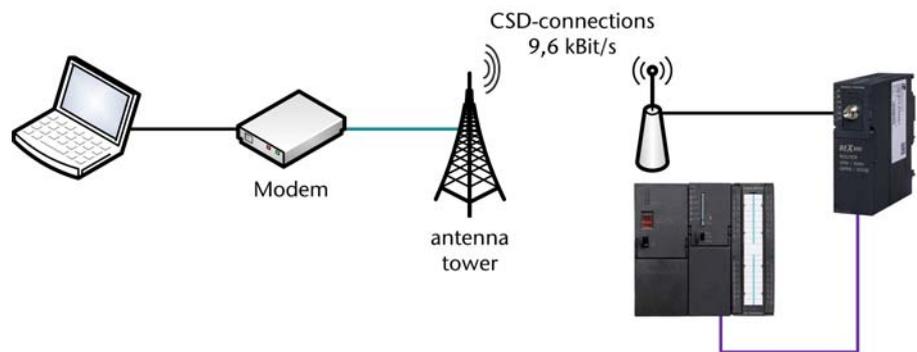


Fig. 6-2-1: GSM point-to-point connection

Step-by-step instructions:

1. The integrated modem must be configured to permit PPP dial-in under menu item Network > Modem. (Fig. 6-2-2)

The screenshot displays the Helmholtz Systems web interface for Modem Configuration. The top navigation bar includes 'System', 'LAN', 'WAN', 'Modem', 'Internet', 'DHCP', 'DNS Server', 'Hosts', and 'DynDNS'. The left sidebar lists 'Network', 'Ports', 'Security', 'VPN', and 'Status'. The main content area is titled 'Modem Configuration' and is divided into two sections: 'Modem Settings' and 'GSM Provider Settings'.
In the 'Modem Settings' section, the 'Modem Type' is set to 'GSM'. There are two 'Modem Init' input fields.
The 'GSM Provider Settings' section includes a 'SIM Pin' field with the value '1111' and a 'Provider' dropdown menu set to 'T-mobile'. Below this are three tabs: 'Outgoing', 'Incoming', and 'Call Back'. The 'Incoming' tab is selected, and the 'Dialin enable' checkbox is checked and circled in red. Other settings in this tab include:
- 'PPP Server IP-Address (here)': 192.168.0.101
- 'PPP Client IP-Address': 192.168.0.102
- 'Dialin Authentication': every User with dialin rights (dropdown)
- 'Authentication via PAP': checked
- 'Authentication via CHAP': checked
- 'close connection after inactivity of [s]': 300
A 'Save Changes' button is located at the bottom right of the form.

Fig. 6-2-2: Settings on the Modem tab

2. On this page, it is also possible to set whether dial-in will be permitted to just a particular user or to all users with dial-in rights in the user list (System > Users).
3. Now the server-side (REX 300) connection is parameterized and a dial-up connection can be set up in your operating system. You will find a general explanation for this in Section 6.3.

6.3 Setting up a dial-up connection

This Section tells you how to set up a dial-up connection for your direct connection with the REX 300 under Window XP.

Step-by-step instructions:

1. You must first start the *“New Connection Wizard”* under Start > Settings > Control Panel > Network Connection with the item *“Create a new connection.”*
2. Now click *“Next”* in the open window



3. In the next step, select “*Connect to the network at my workplace*” and then click “*Next.*”



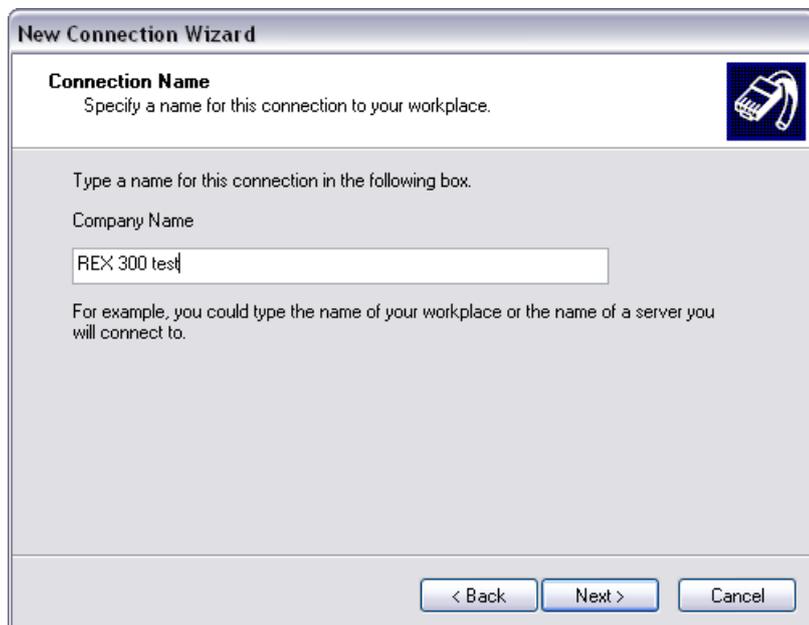
4. In the following window, select the item “*Dial-up connection*” and confirm the dialog box with “*Next.*”



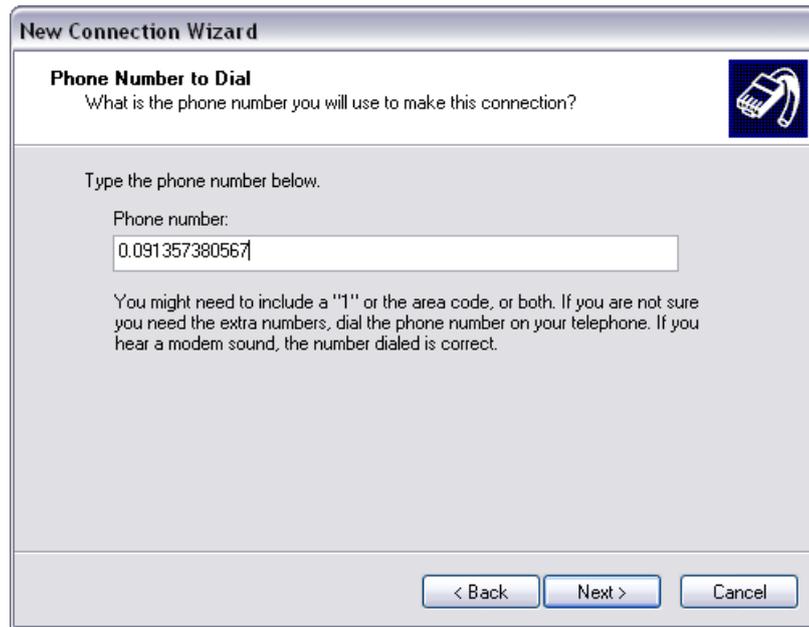
5. In the following dialog box, if you have installed several modems, you must select the modem with which the connection is to be opened and confirm the dialog box with "Next."



6. Now enter a name for your new connection, for example, "REX 300 Test."



7. Enter the phone number at which the REX 300 can be reached and confirm the dialog box with "Next."



8. Click "Finish." The connection has now been set up.



9. Now you can either open the connection by double-clicking on an icon on the desktop, if one was placed there, or you can open the connection by clicking the menu item Start > Settings > Control Panel > Network Connections.



10. In the connection dialog box, you have to enter the user name and the password that you defined for the relevant user in the web interface. The factory setting is, for example
- User name: helmholz
Password: router



11. Finally, click the “Dial” button to make the connection.

7 VPN (Client-Router)

The steps described here are intended to help you set up a VPN connection for your REX 300. These steps apply to client-to-router connections.

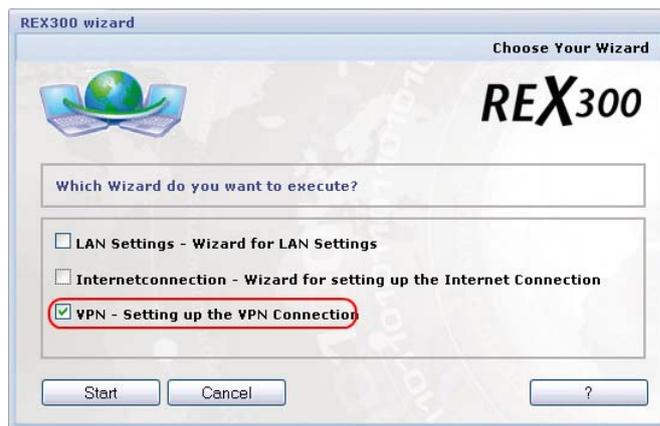


7.1 OpenVPN (with wizard)

How you configure an OpenVPN connection with the integrated wizard is described here. This is done as follows:

1. Call the Web interface of the REX 300. If your REX 300 still has the factory settings, you can call it by entering IP address 192.168.0.100 in your Browser.
2. The display shown in Fig. 7-1-1 should now be visible to you.

Fig. 7-1-1
Selecting the VPN
wizard



Select the “VPN – Setting up the VPN Tunnel” wizard in this display. The VPN wizard is executed when you click the “Start” button.

3. If you have not yet executed the Internet wizard or if you have set the Internet connection by hand, this warning (Fig. 7-1-2) will be displayed. If you have not yet defined how the Internet connection is to be established, please do this before you perform the next steps (see Sections 3 and 4).

Fig. 7-1-2
Notice, have you already run the Internet wizard?



4. Information and a welcome greeting are now displayed. All you need to do here is click the "Next >" button.

Fig. 7-1-3
Welcome display of the VPN wizard



5. In the screen form that now opens you must select the type of connection you wish to configure. In this example, we have chosen the Client Router connection. Now click the "Next >" button again.

Fig. 7-1-4
Selecting the VPN connection type



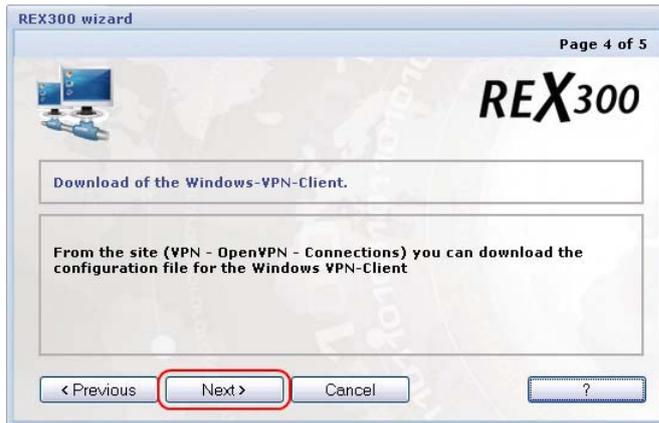
- Now you must select a key for the encryption. If you have not already imported a key into the device manually you can also use the “*Wizard_Static_Key*.” This is a randomly generated key. Now click the “*Next >*” button again.

Fig. 7-1-5
Selecting the static key



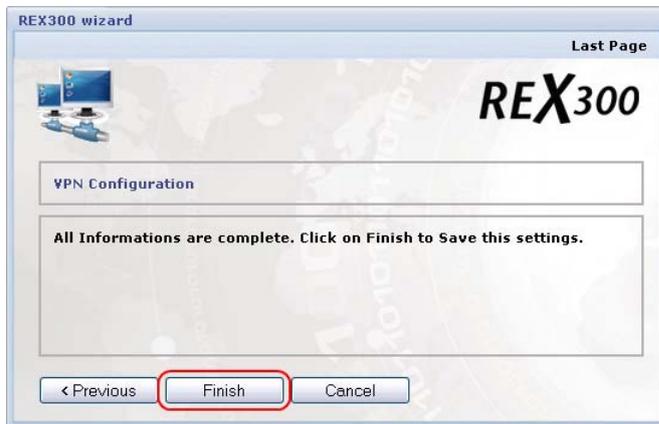
- A message now informs you that you can download the relevant configuration file from the VPN – OpenVPN menu. You can confirm this dialog box by clicking the “*Next >*” button.

Fig. 7-1-6
Indication of the
configuration files



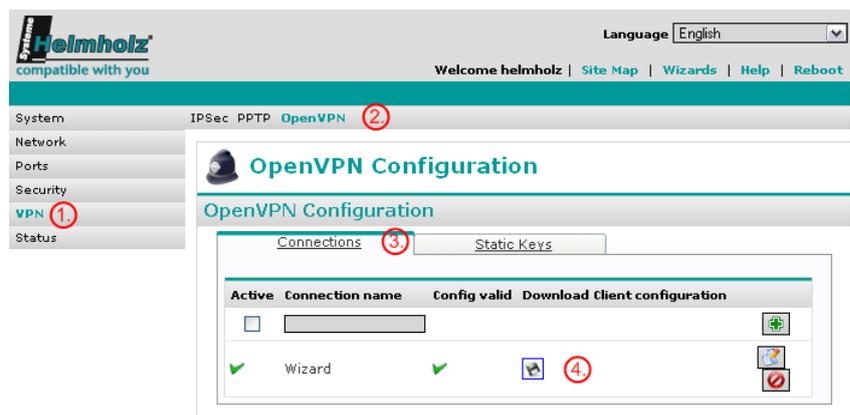
- Confirm the following message box with “*Finish.*”

Fig. 7-1-7
Finish dialog box



9. The REX 300 now applies the configuration. This process takes approx. 30 seconds. You will recognize whether the device has completed the task when a green checkmark is displayed in front of the VPN wizard in the wizard screen form.
10. Configuration of the REX 300 is now complete. You must now set up your PC for the VPN connection.
If you have already installed OpenVPN, continue with step 13. If you have not, perform the following steps.
11. Install the OpenVPN software, if you have not already done so, from the included product CD. Please confirm the dialog boxes of the installation software with “Weiter >” or “Next >”. Furthermore, you must accept the “License Agreement” with “I Agree”; as soon as you have answered all the questions correctly, you can install the software on your computer with the “Install” button.
12. If installation has been successful you will find folder C:\Program Files\OpenVPN\config on your drive if you have selected the default installation folder for OpenVPN. You must copy two files into this folder so that the software knows to which OpenVPN device (server or REX 300) you wish to connect. You can download the files from the REX 300. To do that, select menu items **VPN – OpenVPN** (1)(2) with tab card “Connections” (3) and “Static Keys”. You can download two files on these two tab cards. These are the “Wizard.ovpn” file and the “Wizard_Static_key” file. To be able to download the files, you must click the “Floppy Disk” button (4) in the screen form concerned. The file in question is prepared and you can then download it with the blue underscored link (5).

Fig. 7-1-10
Downloading the
configuration and key
file



You can now store the file in folder C:\Program Files\OpenVPN\config\ by right-clicking the blue underscored link (5) and left-clicking “Save link as...” (6)

Fig. 7-1-11
Saving the configuration file

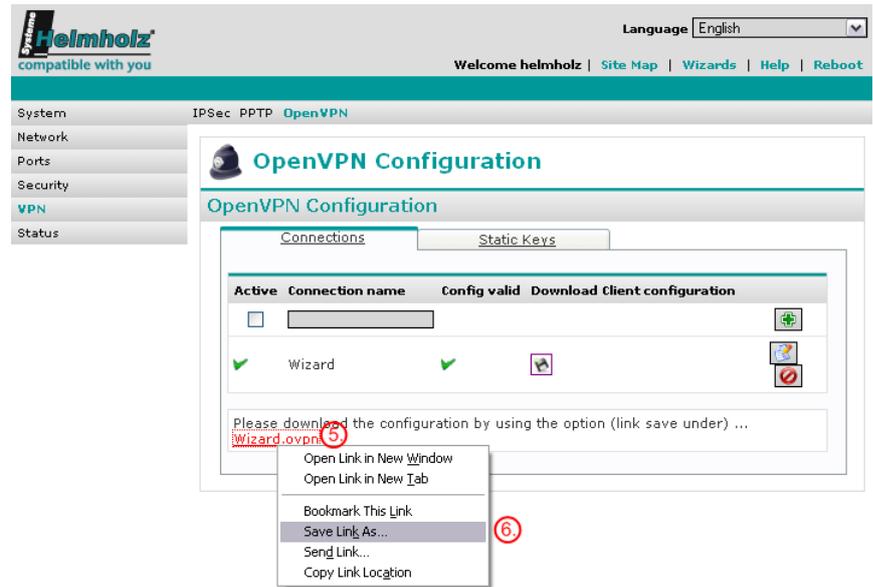
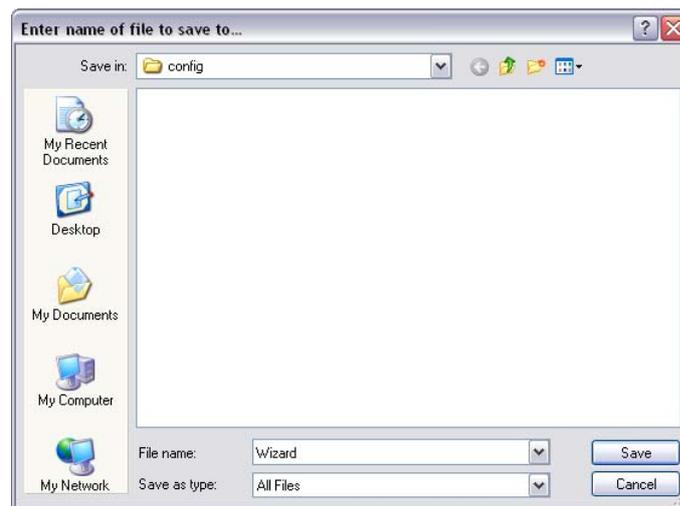


Fig. 7-1-12
Saving dialog box of the browser



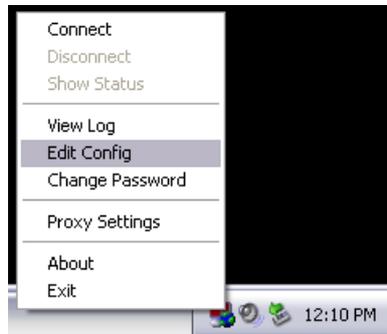
- Now, if you have also stored the “Wizard_Static_Key” file in this folder, you can start the OpenVPN software with “Start>Programs>OpenVPN>OpenVPN GUI”. You should now find the following icon bottom right in your task bar.

Fig. 7-1-13
View of OpenVPN in the inactive state



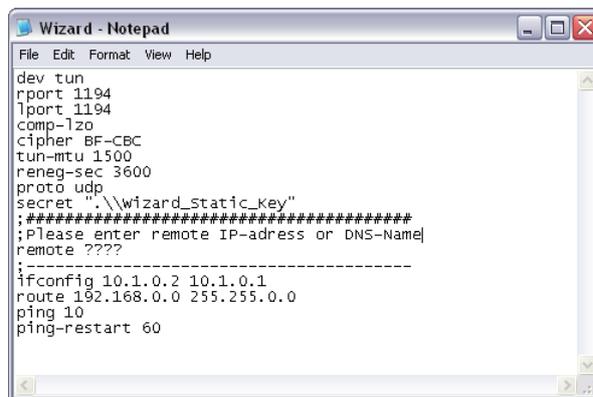
- You can open the context menu of the software by right-mouse clicking the OpenVPN icon. Here you can establish the connection, change the configuration, and execute various other actions. Click *“Edit Config”* to edit the *“Wizard.ovpn”* file.

Fig. 7-1-14
Adapting the configuration



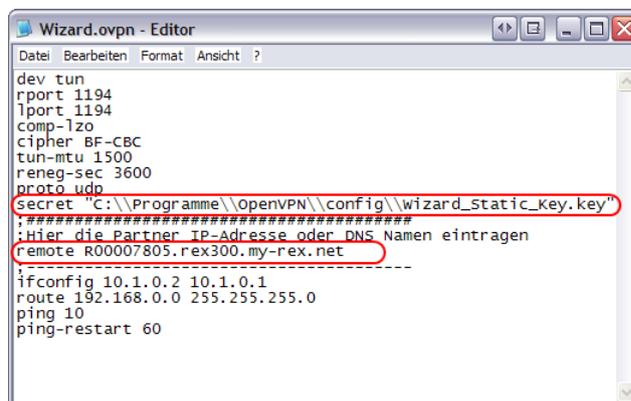
- A window displaying the contents of the *“Wizard.ovpn”* file should now open. You can make the necessary changes here.

Abb. Fig. 7-1-15
Configuration file in its original state



- So that your PC knows which address to make a connection to and which file transmission is to be encrypted, you must enter two more things here. First, under item *“secret,”* you must enter the path to the *“Wizard_Static_Key”* file and secondly, you must specify to which Internet address, this is item *“remote,”* the OpenVPN connection is to be established. An example is given in the following figure.

Fig. 7-1-16
Configuration after entering secret and remote.
Please pay attention to the double backslash when entering the path.



17. The configuration task is completed when you save the file. You can now try to establish a connection. Single right-click the OpenVPN icon on your task bar to open the context menu and left-click "*Connect.*" OpenVPN will now try to establish a VPN connection to the remote station you entered. This is indicated by the OpenVPN icon changing from red to yellow.

Fig. 7-1-17
OpenVPN connection
establishment



18. Once everything is correctly configured and no obstacles exist, such as disabled ports in any firewalls, the VPN connection will be established. This is indicated to you by the icon changing from yellow to green.

Fig. 7-1-18
OpenVPN connection
established



19. Now the VPN connection is correctly established and you can, for example, open the Web interface and/or address the MPI/PROFIBUS interface via the LAN IP address of the REX 300.

Now that the VPN connection has been established, you can reach all devices that are connected to the LAN interface of the REX 300 via the LAN-IP address. If you want to use the MPI/PROFIBUS interface of your REX 300, you will find a step-by-step explanation in the accompanying QuickStart Guide.

20. If you want to break the connection, single right-click the green icon once again and then select "*Disconnect.*" Now the icon changes again from green to red and the connection is disconnected.

8 VPN (Router-Router)

The steps described here are intended to help you set up a VPN connection for your REX 300. These steps describe the router-to-router connection.

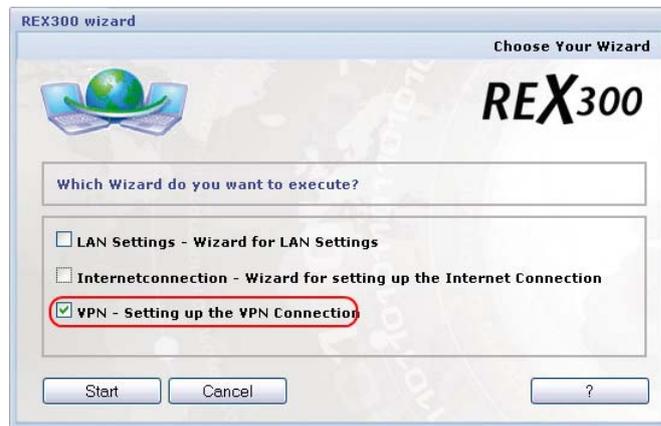
8.1 OpenVPN (with wizard)

How you configure an OpenVPN connection with the integrated wizard is described here. This is done as follows:

8.1.1 Setting up the OpenVPN server (REX 300)

1. Call up the Web interface of the REX 300 that you wish to set up as the OpenVPN server. If your REX 300 still has the factory settings, you can call it by entering IP address 192.168.0.100 in your Browser.
2. The display shown in Fig. 8-1-1-1 should now be visible to you.

Fig. 8-1-1-1
Selecting the VPN
wizard



Select the “VPN – Setting up the VPN Tunnel” wizard in this display. The VPN wizard is executed when you click the “Start” button.

3. If you have not yet executed the Internet wizard or if you have set the Internet connection by hand, this warning (Fig. 8-1-1-2) will be displayed. If you have not yet defined how the Internet connection is to be established, please do this before you perform the next steps (see Sections 3 and 4).

Fig. 8-1-1-2
Notice, have you already run the Internet wizard?



4. Confirm the following message box with "Next >."

Fig. 8-1-1-3
Welcome display of the VPN wizard



5. In the screen form that now opens you must select the type of connection you wish to configure. In this example we have used the router-to-router connection "Connection between 2 Networks". Now click the "Next >" button again.

Fig. 8-1-1-4
Selecting the VPN connection type



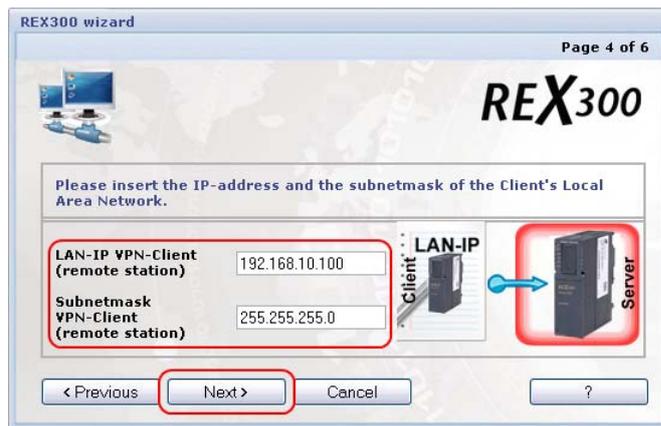
6. In the next screen form you must define that the REX 300 is to be configured as a VPN server. Now click the “Next >” button again.

Fig. 8-1-1-5
Selecting which VPN node is to be configured.



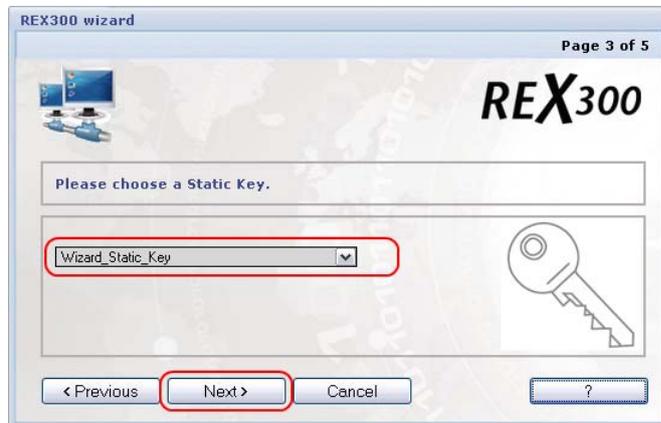
7. In the screen form shown here, you must enter the IP address and subnet mask of the LAN interface of your REX 300 that you want to connect to this VPN server (REX 300). Now click the “Next >” button again.

Fig. 8-1-1-6
Entry of the LAN parameters of the VPN client.



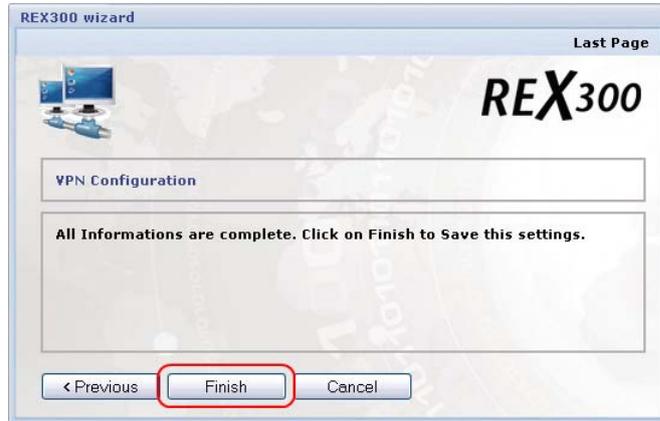
8. Now you must select a key for the encryption. If you have not already imported a key into the device manually you can also use the “Wizard_Static_Key”. This is a randomly generated key. Now click the “Next >” button again.

Fig. 8-1-1-7
Selecting the static key.



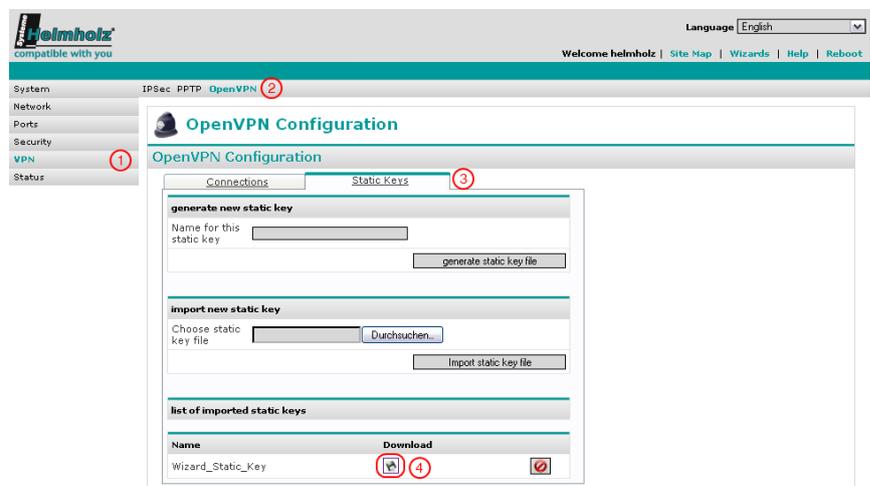
- Finally, you will see that all the important information is available and that you can apply the settings with the “Finish” button. Confirm this dialog box with the “Finish” button.

Fig. 8-1-1-8
Finish dialog box



- The REX 300 will now apply the configuration. This process lasts approx. 30 seconds. You will recognize whether the device has completed the task when a green checkmark is displayed in front of the VPN wizard in the wizard screen form.
- Configuration of the REX 300 VPN server is now complete. You must now set up a second REX 300 for the client VPN connection.
- To ensure that the REX 300 VPN client can operate together with your REX 300 VPN server you must ensure that both REX 300s use the same static key for encryption. You must download this key from the REX 300 you first configured. In this example it was the REX 300 VPN-Server To do that, go to the “Static keys” (3) tab card with menu items VPN – OpenVPN (1) and (2). To be able to download the file, you must click the “Floppy Disk” button (4) in the screen form concerned.

Fig. 8-1-1-9
Downloading the static key file.



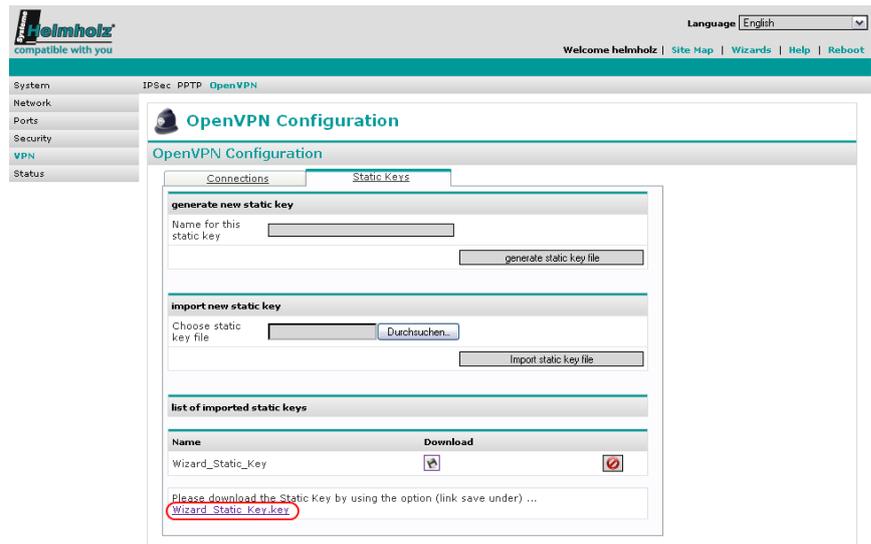
This action prepares the file in question, which you can then download via the blue underscored link and selecting

“Save link as...” from the context menu to store the file on your PC, for example.

Fig. 8-1-1-10
Downloading the static
key file.



*Please save the file
without a file extension!*



13. Now continue with Section 8.1.2 to configure the REX 300 VPN Client.

8.1.2 OpenVPN Client

Please remember that you must first adapt the IP address of your REX 300 VPN Client to the IP address you defined as the LAN-IP remote station in Chapter 8.1.1.

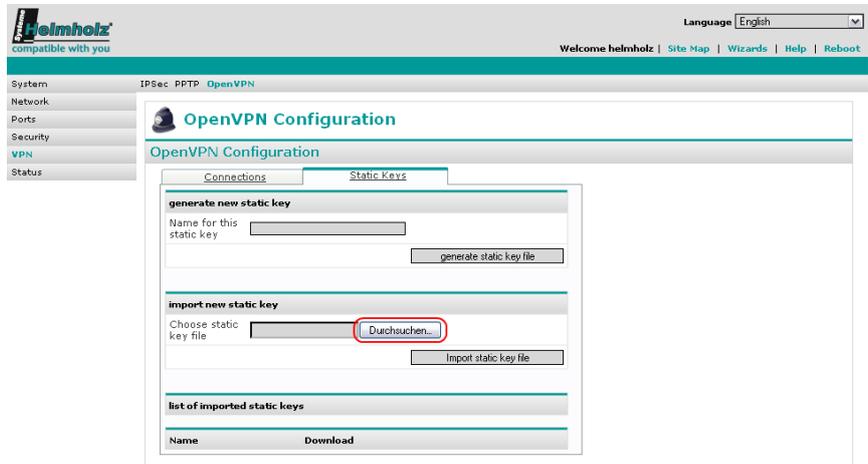
1. Call the Web interface of the REX 300 that you wish to set up as the OpenVPN Client. If your REX 300 still has the factory settings, you can call it by entering IP address 192.168.0.100 in your Browser.
2. As mentioned above, you should now adapt the IP address of your REX 300 either via the integrated wizard or via **Network – LAN**.

- Before you can execute the VPN wizard you must import the static key that you previously used for the VPN server into the REX 300 VPN client. To do that, go to the "Static keys" tab card with menu items VPN – **OpenVPN**. Now click the "Browse..." button to import into the REX 300 the static key that you saved to your PC.

Fig. 8-1-2-1
Importing the static key file.

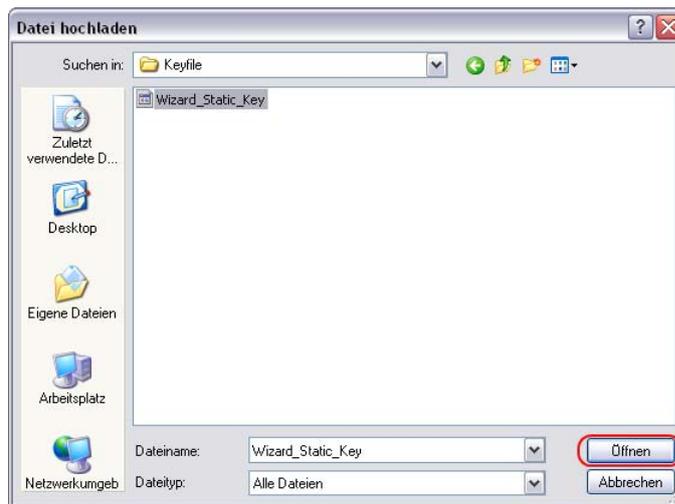


Please import the Key file without a file extension.



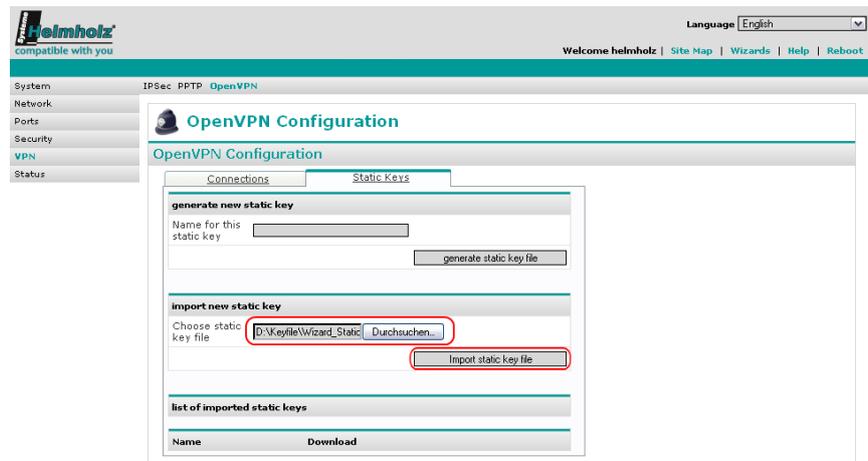
- Now you must select the key file on your PC and transfer it to the Web interface using the "Open" button.

Fig. 8-1-2-2
Selecting the static key file.



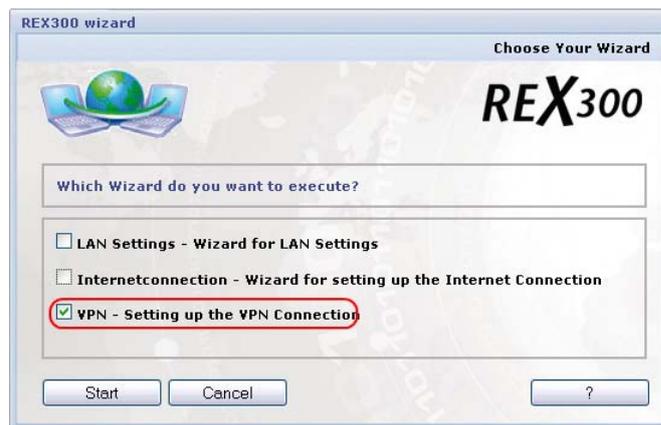
5. The file path to the key file is now in the Web interface and you can import the file into the REX 300 with the “Import static key file” button.

Fig. 8-1-2-3
Importing the static key
file.



6. Now you can start the VPN wizard via the wizard menu.
7. The display shown in Fig. 8-1-2-4 should now be visible to you.

Fig. 8-1-2-4
Selecting the VPN
wizard



Select the “VPN – Setting up the VPN Tunnel” wizard in this display. The VPN wizard is executed when you click the “Start” button.

8. If you have not yet executed the Internet wizard or if you have set the Internet connection by hand, this warning (Fig. 8-1-2-5) will be displayed. If you have not yet defined how the Internet connection is to be established, please do this before you perform the next steps (see Sections 3 and 4).

Fig. 8-1-2-5
Notice, have you already run the Internet wizard?



9. Confirm the following message box with "Next >."

Abb. 8-1-2-6
Welcome display of the VPN wizard



10. In the screen form that now opens you must select the type of connection you wish to configure. In this example we have used the router-to-router connection "Connection between 2 Networks". Now click the "Next >" button again.

Fig. 8-1-2-7
Selecting the VPN connection type



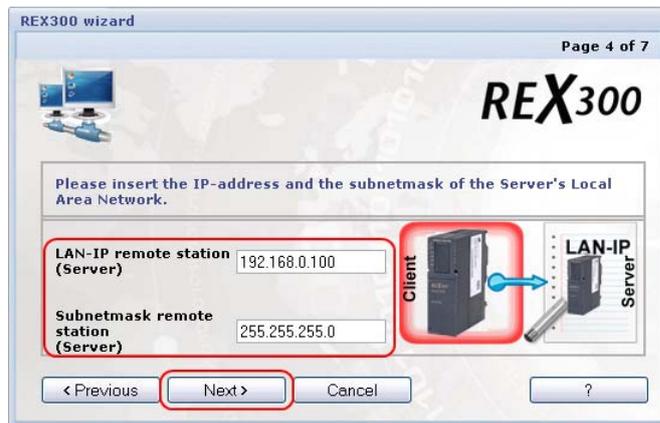
11. In the next screen form, you must define that the REX 300 is to be configured as a VPN Client. Now click the “Next >” button again.

Fig. 8-1-2-8
Selecting which VPN node is to be configured.



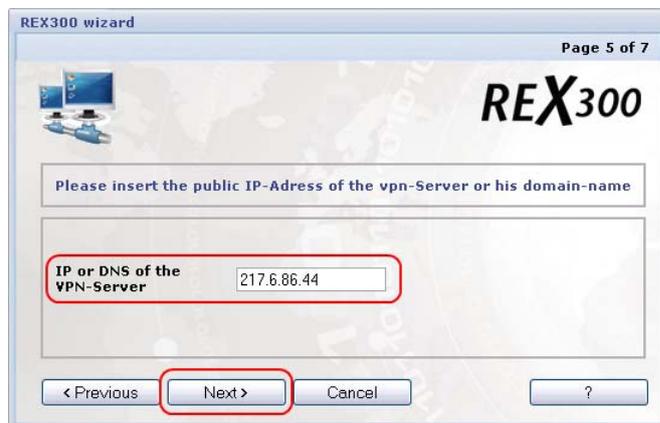
12. In the next screen form, you must enter the LAN parameters of the REX 300 VPN server. Now click the “Next >” button again.

Fig. 8-1-2-9
Entry of the LAN IP addresses of the remote station (server).



13. In the next dialog box, you enter the IP address or name that the REX 300 VPN server will be known by in the Internet. Now click the “Next >” button again.

Fig. 8-1-2-10
Entry of the public IP address or the name of the VPN server.



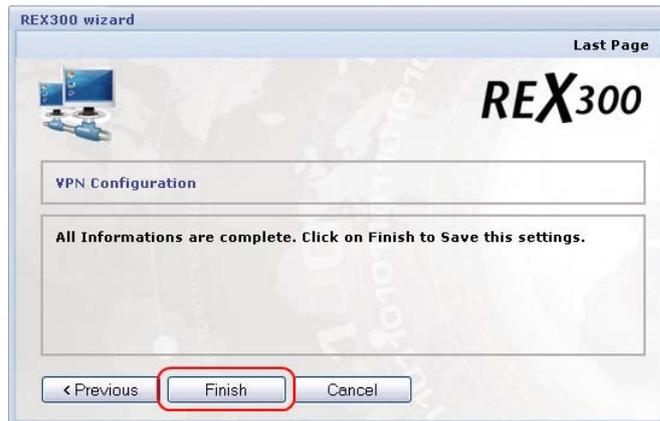
14. Now define the static key that is to be used for encryption or connecting. Please remember that the key on the VPN server and that on the VPN client must match. The key that you previously imported from the server to the client is displayed here. Now click the “Next >” button again.

Fig. 8-1-2-11
Selecting the static key
file.



15. Now you are told that all the important information is available and that you can apply the settings with the “Finish” button. Confirm this dialog box with the “Finish” button.

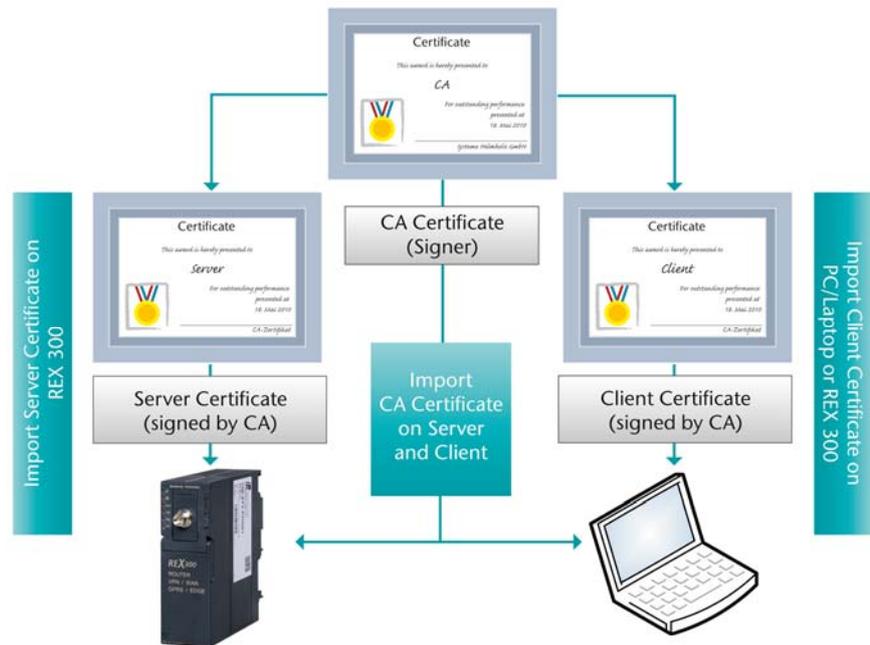
Fig. 8-1-2-12
Finish dialog box



16. The REX 300 will now apply the configuration. This process lasts approx. 30 seconds. You can see whether the device has completed the task if a green checkmark is displayed in front of the VPN wizard in the wizard screen form.
17. Configuration of the REX 300 VPN client is now complete. Now you can test the connection. The OpenVPN wizard configures the VPN connection so that it constantly tries to establish a connection. You can manually set the connection to start with the “Dial Out” key, for example. You will find this setting in the VPN – OpenVPN menu when you edit the active connection.

9 Certificates

9.1 Overview of certificates



Each participant in a VPN connection must have two certificates. Such a certificate must be signed by a so-called CA certificate (root certificate). Each participant must own such a CA certificate as well as a “server” or “client” certificate. In our case, the server is the REX 300. The client is either a PC/laptop or another REX 300. The certificates are needed to establish a secure VPN tunnel and are used to authenticate the VPN participants. If a participant either has no certificate or an invalid certificate it will not be possible to establish a VPN tunnel between the two devices when authentication of the REX 300 is set to “X.509.”

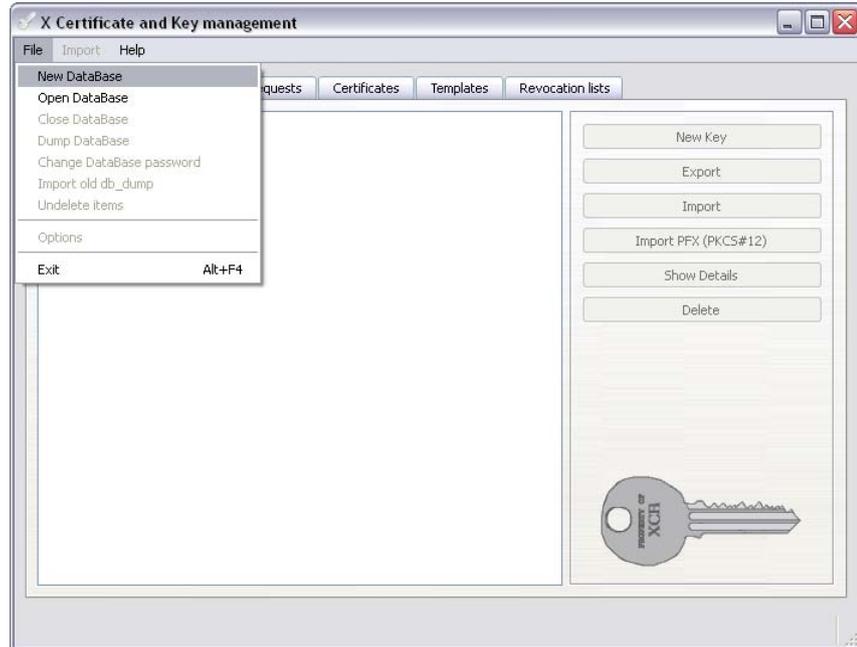
Please read the following sections to find out how to create certificates.

9.2 Creating certificates

To create certificates, we suggest using the freely available program XCA written by Christian Hohnstädt. This program allows you to create both X.509 certificates and the necessary private keys in a simple way.

The program is available free of charge from <http://sourceforge.net/projects/xca> and install it in the normal way under Windows (NT/2000/XP/VISTA) (execute the file with the extension .exe).

When you start XCA for the first time, you must first create a new database for managing your certificates. To do that, select “File” and then “New DataBase”.



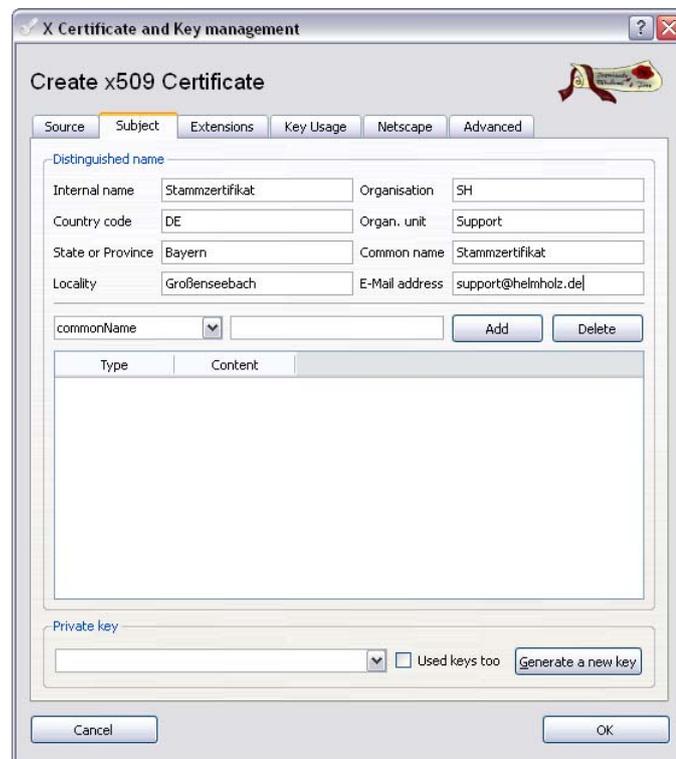
When you have chosen a name, memory location, and password for your new database, you can open it and create your first root certificate (CA certificate).

9.2.1 Creating a root certificate

To create a root certificate click on the “Certificates” tab card and then on “New certificate” to open the following dialog box:



You should first change the signature algorithm to MD 5 so that the certificate is compatible with the REX 300. Now select the “Subject” tab card and make the certificate settings.



On the Subject tab card, complete the “Internal Name“ to “E-Mail address” fields. The Subject settings can later be used as the ID for VPN via IPSec. Now you must select "Generate a new key" to create a new private key.



You must use key type RSA. You can choose any key length and, of course, name. The longer the key, the more secure it will be, encryption will be more computationally intensive.

The “Extensions” tab card is where you make the settings for the type and validity of the certificate.

The screenshot shows the 'Create x509 Certificate' dialog box with the 'Extensions' tab selected. The 'Basic constraints' section has 'Type' set to 'Certification Authority' and 'Critical' checked. The 'Key identifier' section has 'Subject Key Identifier' checked. The 'Validity' section has 'Not before' set to '2010-06-10 11:51' and 'Not after' set to '2011-06-10 11:51'. The 'Time range' section has '20' selected in the list box and 'Years' selected in the dropdown. There are 'Edit' buttons for 'subject alternative name', 'issuer alternative name', 'CRL distribution point', and 'Authority Info Access'. 'Cancel' and 'OK' buttons are at the bottom.

Basic constraints

Type = Certification Authority (CA)

Set a checkmark for the option **Critical**

Key identifier

Set a checkmark for Subject Key Identifier

Validity

You can enter the precise starting and end dates in the fields provided or use the adjacent Time Range field.

Time Range

In the list box on the far right, select the numerical values Days, Months, or Years. See the list below for how long individual certificates should be valid for:

- Personal certificates should be valid for 1 (one) year.
- Server (SSL) certificates should also be valid for 1 (one) year.
- Router certificates should be valid for 1 (one) year (if they are external routers) or 10 (ten) years (if they are internal routers).
- CA certificates should also have a long validity period (for example > 10 years).

Click “*Apply*” to apply the settings made under Time Range.

Subject alternative name

The alternative name of the owner is a list of alternative names for the owner of the certificate; these names can be RFC822 name (e-mail), DNS name, X.400 addresses, EDI name, URLs, or IP addresses, in fact, any structured name scheme can be used. For PKIX this extension is critical if the subject field in the certificate is empty.

Issuer alternative name

The same applies to the alternative name of the issuer as to the alternative name of the owner.

CRL distribution point

To be able to use a public distribution point for certificate revocation lists, the LDAP or HTTP address of the certificate revocation list must be entered. An address must always be preceded by a URL (universal resource indicator, for example, URL: <http://www.helmholz.de>). A colon is used as the field separator. If you have local revocation lists, you do not require this option.

Authority Info Access

This PKIX extension defines how further information and services of the issuing CA can be used. It provides a way of accessing further information via the CA (further guidelines, root certificates,...) or online verification services (e.g. OCSP). It is convenient for the verifying application if for certificate applications such as Secure Mail (S/MIME) the end certificate specifies in this extension where the next highest CA certificate can be retrieved if the full certificate path has not been sent.

On the “Key Usage” tab card you can select a key and an extended key. Both keys should be non-critical, that is, you should not check the two Critical checkboxes.

Select the following values in the left column if you want to create a root certificate:

- Certificate Sign
- CRL Sign

With these two options, your root certificate can sign the client certificates and the certificate revocation lists.

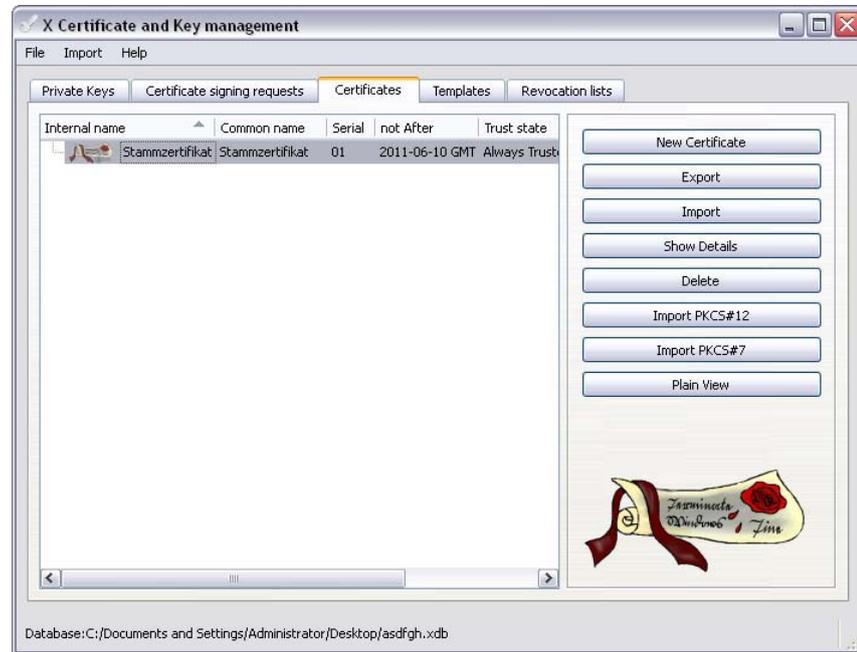


You can now click "OK" to complete the root certificate.

You have now successfully created your root certificate and you can use it to create and sign further certificates.

9.2.2 Creating a client certificate

To create a certificate that is signed by this CA, on the “Certificates” tab card mark the root certificate that you just created and click “New Certificate” again.



The following dialog box now opens.

Origin

First of all we must specify that our root certificate is to be used for signatures. Again, you must set the signature algorithm MD5.



In the default setting, our root certificate is already selected for the signature.

Again, enter the data for the client certificate in the fields “Internal name” to “E-mail address”.



Then create a key for the client certificate. This key should be the same length as the key of the root certificate.



Extensions:

As your client certificate does not have to sign any other certificates, enter the certificate type “End Entity”).

Basic constraints

Type = End Entity

Key identifier

Set a checkmark for Subject Key Identifier

Validity

You can enter the precise starting and end dates in the fields provided or use the adjacent Time Range field.

Time Range

In the list box on the far right, select the numerical values Days, Months, or Years. See the list below for how long individual certificates should be valid for:

- Personal certificates should be valid for 1 (one) year.
- Server (SSL) certificates should also be valid for 1 (one) year.
- Router certificates should be valid for 1 (one) year (if they are external routers) or 10 (ten) years (if they are internal routers).
- CA certificates should also have a long validity period (for example > 10 years).

Apply the values of the Time Range with “Apply”.

Subject alternative name

The alternative name of the owner is a list of alternative names for the owner of the certificate; these names can be RFC822 name (e-mail), DNS name, X.400 addresses, EDI name, URLs or IP addresses, in fact, any structured name scheme can be used. For PKIX this extension is critical if the subject field in the certificate is empty.

Issuer alternative name

The same applies to the alternative name of the issuer as to the alternative name of the owner.

CRL distribution point

To be able to use a public distribution point for certificate revocation lists, the LDAP or HTTP address of the certificate revocation list must be entered. An address must always be preceded by a URI (universal resource indicator, for example, URL: <http://www.helmholz.de>). A colon is used as the field separator. If you have local certificate revocation lists, you do not require this option.

Authority Info Access

This PKIX extension defines how further information and services of the issuing CA can be used. It provides a way of accessing further information via the CA (further guidelines, root certificates,...) or online verification services (e.g. OCSP). It is convenient for the verifying application if for certificate applications such as Secure Mail (S/MIME) the end certificate specifies in this extension where the next highest CA certificate can be called up if the full certificate path has not been sent.

If you are creating a client certificate as an end instance you will not need any of options provided here. You can go directly to the next tab card.

If you require additional security, you can additionally select the option SSL Server or SSL Client, depending on the role of the VPN participants (client or server).

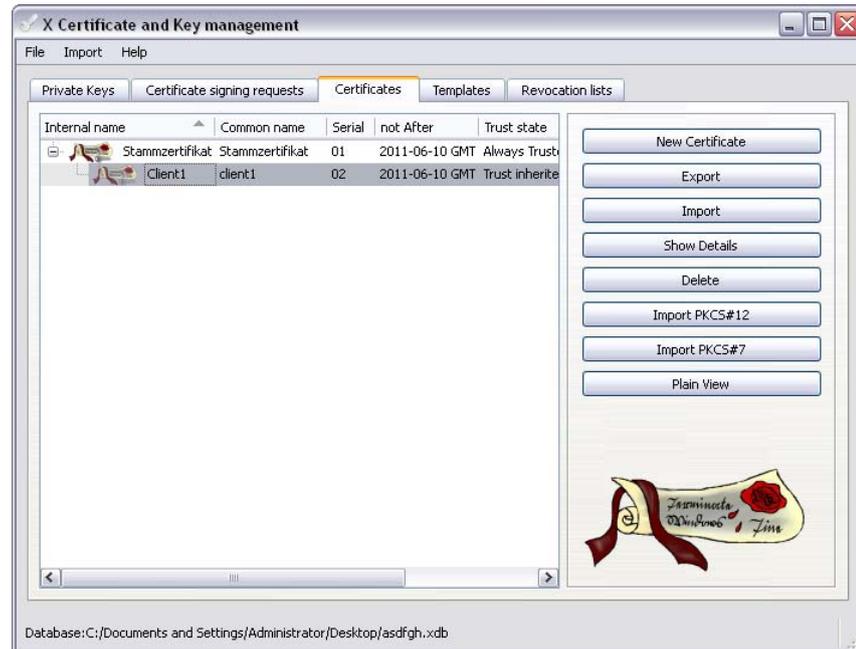
This has the advantage that for OpenVPN it is possible to query whether a VPN server is additionally provided with SSL. This option can also be activated in the REX 300. This topic and the setting options are dealt with in more detail in the section on OpenVPN in the manual. If you equip your client certificate with both options, both a VPN client and a VPN server can be provided with the certificate.



No settings have to be made for IP-Sec on the "Netscape" tab card.

If OpenVPN is used with the option "Remote station must be a TTL-Server" activated, only the option "SSL-Server" has to be selected for the server certificate. See also the screenshot above.

Now the certificates you created must be made accessible in the “Certificates” tab card of the first dialog box by marking the certificate in question and clicking “Export.”



In the next menu, you can define a storage location on your computer for the certificate and a format for the certificate file.



So that your client can authenticate with the client certificate, in addition to this client certificate it also requires the matching private key. As shown in Fig. x, export the client certificate in the format PKCS #12 with Certificate chain. Click “OK” to store the client certificate at the location previously specified. The client certificate now has the extension .p12.

The root certificate must be exported in PEM format (file extension .crt).

These certificates can now be imported into the REX 300 router via the Web interface (cf. REX 300 manual: Section System Certificates)

9.3 Creating CRL files (certificate revocation lists)

If you want to withdraw the right to use the VPN tunnel from an employee, please read the following section and create a certificate revocation list.

To do this, start up the XCA software again. Open the database containing the certificates of your employee. To declare a certificate invalid, right-click it once to open the following menu:



Now select “Revoke” as shown. The certificate entry is marked with a red question mark and is now invalid.

In the next step, right-click the associated root certificate. The following dialog box opens:



You can now create a revocation list via menu item “CA → “Generate CRL” as shown in the figure above. Again, choose MD5 for “Hash Algorithm”. For extensions, no options have to be activated by a checkmark. The CRL must now be exported and imported into the REX 300.

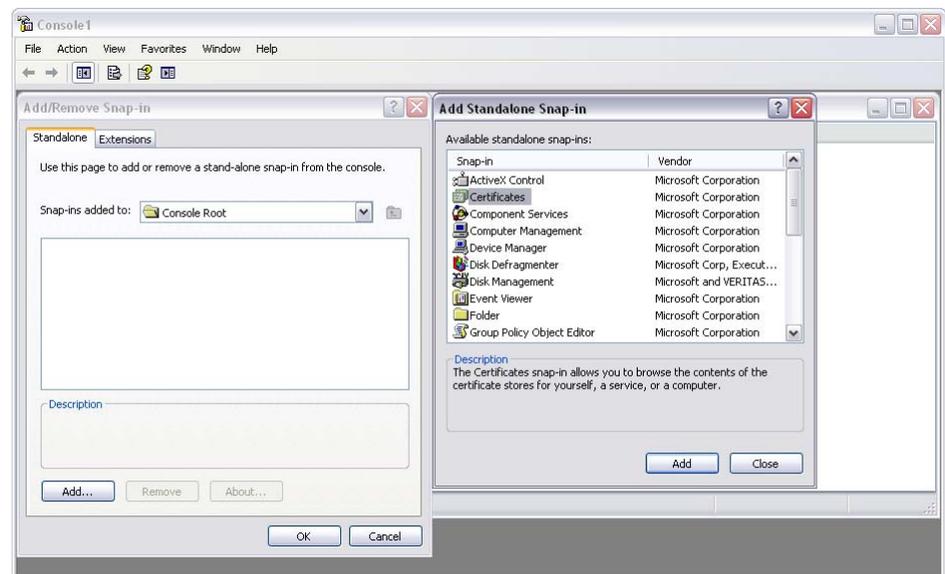
Proceed as follows to export:



On the “Revocation lists” tab card you can now see the revocation list you just created. Mark it and then click “Export.” Select .pem as the export format. Confirm with “OK” after you have chosen a suitable storage location. You can now import this list via the **System – Certificates** menu item on the Web interface of the REX 300. When you restart the VPN connections and the REX 300 the CRL will be activated and it will no longer be possible to establish a tunnel with the invalid certificate.

9.4 Importing certificates under Windows XP

To import any certificates you have completed, you must create a so-called certificate management console. Enter “MMC” under “Start → Run”. Then select “File - Add/Remove Snap-In” and in the dialog box that then opens select “Add.” You can now select “Certificates” from the list of available snap-ins.



In the next step, select “Computer account”:

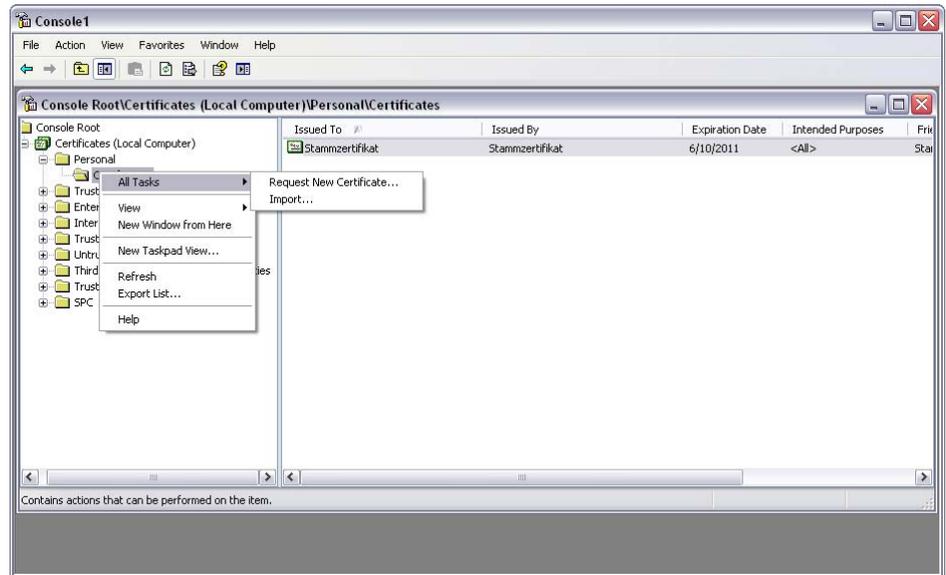


In the following dialog box select “This snap-in will always manage” “Local computer: (the computer this console is running on)”.

Once you have created the certificate consoles as described above, you can import a certificate.

First open the dialog box shown below by right-clicking “Certificates (Local Computer) → Certificates” and import the certificate that will identify the client. Make sure you select the “.p12” file. Enter the password for the p12 file and then click *Next*. In the next dialog box, select “Automatically select the certificate store based on the type of certificate.” When you click “Finish” the required certificates will be imported.

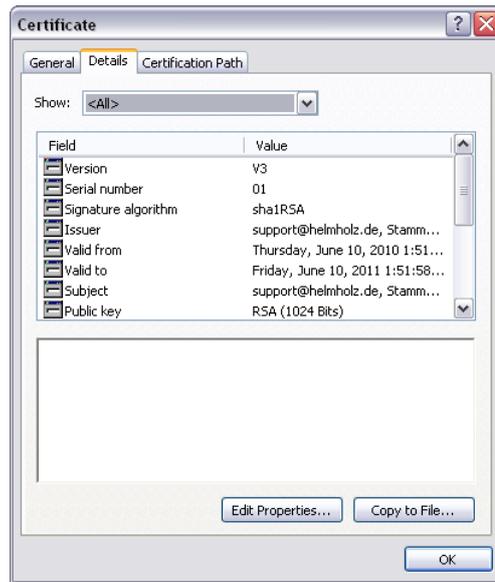
No more certificates have to be imported. The CA certificate is automatically imported with the rest. It is not absolutely necessary to save the console you created.



Double-click a certificate to open its properties. On the “General” tab card, you can check, for instance, which CA issued the certificate, how long the certificate will be valid for, and whether you own a private key for this certificate. This item is very important for the use of certificates in Web server publications.



More information about the issued certificate is given on the “Details” tab card.



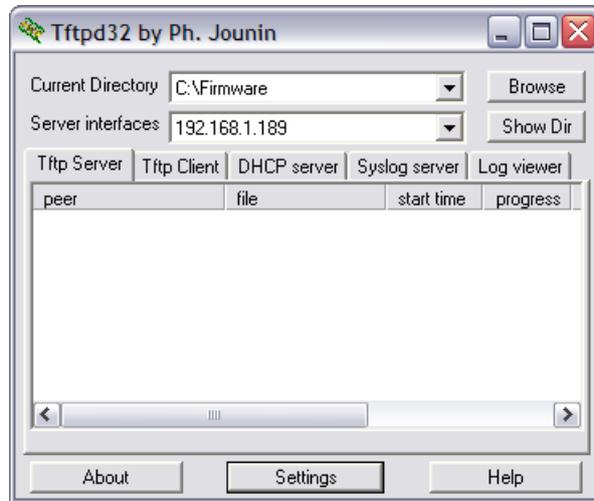
10 Troubleshooting

If a problem is not described here and this manual does not provide any information on how to remedy it, the support service of Systeme Helmholtz GmbH will gladly help you to solve the problem.

10.1 Firmware update

1. Download the latest firmware file from www.helmholz.de. You will find it in the download area. (Download > REX 300 > image.bin)
2. Start or install the software TFTP32 from www.helmholz.de. You will find it in the download area (Download > REX 300 > TFTP32.zip)

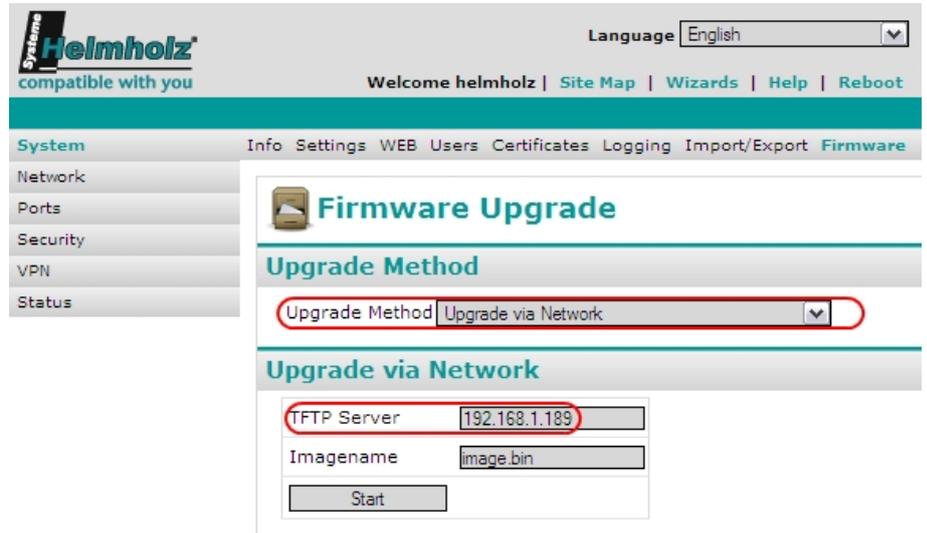
Fig. 10-1-1: TFTP32 software



3. Place the image.bin file in a folder of your choice. (in this case: C:\Firmware) You must specify this folder in the program TFTP32 under TFTP Server in "Current Directory."
4. Open the web interface of the REX 300 in your browser.

- Open the menu item System > Firmware and choose the upgrade method “Upgrade via network” and, under TFTP server, specify the IP address of your computer on which the TFTP software is started. (Fig. 02.01.10)

Fig. 10-1-2: Firmware update method selection



- With a mouse click on the “Start” button, the message “Do NOT switch off the device!” is displayed. (Fig. 10-1-3)

Fig. 10-1-3: Firmware update warning



- With a further mouse click on the “Start” button, the firmware update is performed. When uploading of the image.bin file has been completed, the device will start the update mechanism and prompt you to restart the device. You can either do that via the web interface or by disconnecting the power supply.
- After the device has been restarted, the latest firmware version will be on the device.

10.2 Frequently asked questions

Q: Which ports have to be enabled or redirected for a passive Internet connection for OpenVPN in the factory setting?

A: In the relevant firewall, the UDP port 1194 must be enabled or redirected.

Q: Which ports have to be enabled or redirected for a passive Internet connection for IPsec in the factory setting?

A: In the relevant firewall, the UDP port 500 or 4500 must be enabled or redirected.

Q: Which ports have to be enabled or redirected for a passive Internet connection for PPTP in the factory setting?

A: In the relevant firewall, the TCP port 1723 must be enabled or redirected.

Q: Is it possible to establish a VPN test connection with a REX 300 in your company?

A: Yes. You will find the necessary files (OpenVPN configuration script and Static Key) on www.helmholz.de under Download > REX 300 > OpenVPN Testverbindung.zip. You will also find a picture of the configuration there.

Q: Does REX 300 have to be entered in my hardware config?

A: No

Q: How can I access the web interface of the REX 300 over the Internet?

A: You must enable port 80 in menu Security settings – WAN > LAN. You will find a more detailed description in Section 7.4 of the manual (900-87x-REX300).

Q: What must I pay attention to when using a REX 300 GPRS/EDGE?

A: Please make sure that it is possible to receive a dynamic IP address for the REX 300 with your cell phone contract and that incoming data are received according to this contract.

11 Important Information about VPN

This section explains important information about VPN connections in more detail.

11.1 Basic information

VPN connections from a client PC to a REX 300, which corresponds to the VPN server, can only be established if the Internet connection is permitted to send incoming data to the REX 300. That means that if your Internet connection is disabled for incoming data traffic, you cannot establish a VPN connection to your REX 300.

VPN connections allow you to access the LAN interface of the REX 300. For you this means that once you have established a VPN connection, you must work with the IP address area of the LAN interface of the REX 300. Example: A REX 300 with LAN-IP address 192.168.0.100 can be accessed via the Internet. The VPN connection from your PC (for example, LAN-IP address 192.168.1.100) to the REX 300 has already been established. If you now want to access the Web interface of the REX 300, for example, you must enter 192.168.0.100 in your Browser. VPN ensures that the request to the IP 192.168.0.100 is sent via the Internet through the VPN tunnel to the REX 300. The REX 300 will then transmit the data of the Web interface to you so that you can use it. The same applies if you want to use the MP/PROFIBUS interface. When you use VPN you must enter the LAN-IP address of the REX 300 in our NETLink driver to be able to access the MPI/PROFIBUS interface via VPN.

11.2 OpenVPN

11.2.1 Ports

In the case of OpenVPN you can, if you want, define the ports for the VPN connection. The standard port is 1194. If you want change this to Port 80 you must make sure you set another port for the Web interface under System – Web, as otherwise the Web interface can no longer be opened.

11.2.2 Proxyserver

For OpenVPN you can also select a proxy server as the Internet access point. For that you must reset the protocol of OpenVPN to TCP as most proxy servers do not allow the UDP protocol. This also requires you to make a change in the .ovpn file on your PC that you use for the connection to your REX 300. Instead of “*proto udp*,” you must enter “*proto tcp-client*” in the .ovpn file.

11.2.3 Encryption methods

You can choose two different methods of encryption. You can either use the predefined key or X.509 certificates. If you use a predefined key, be aware that you cannot simultaneously make an OpenVPN connection to an OpenVPN server.



Remember that TCP is slightly slower!

12 List of Sources