# FEC Secure IPSec Client

Version 2.0
February 2007

**Copyright**

**Trademarks**

How to reach Funkwerk
Enterprise Communications:
Funkwerk Enterprise
Communication GmbH
Suedwestpark 94
D-90449 Nuremberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

**Liability**

While every effort has been made to ensure the accurancy of all information in this manual, Funkwerk Enterprise Communications GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of ist terms of scale and delivery.

The information in this manual is subject to change without notice. Additional information can be found at www.funkwerk-ec.com.

# Contents

# 1. Product Overview

This manual describes Installation, Configuration, Features and User Interface of the FEC Secure IPSec Client and its Components.

The FEC IPSec Client Software works according to the principle of Ethernet LAN emulation and supports the routable protocol TCP/IP.

Additional information on upgrades and product variants are available on the website www.funkwerk-ec.com

## 1.1 Using this manual

The structure of this manual is presented below to help you quickly find what you need in this documentation.

The manual is subdivided into seven larger sections that offer step-by-step descriptions, or that describe the structure of the graphic user interface according to the respective object. Two appendices providing additional information and definitions of specialized terms follow these sections.

| | |
|---|---|
| Chapter 1: | Product overview with brief description of the performance range of the software |
| Chapter 2: | Installation instructions |
| Chapter 3: | Description of the graphic user interface |
| Chapter 4: | Description of the configuration possibilities |
| Chapter 5: | Description of the parameters listed in the profile settings |
| Chapter 6: | Description of a connection establishment |
| Chapter 7: | Examples and explanations, particularly for IPsec |
| | Glossary with abbreviations and terms |
| | Index |

Cross references appear in the text in parenthesis and cite the reference with the title, or after a comma, with the subtitle.

An exclamation mark in the margin indicates that the text so marked is of particular significance.

Naturally the software also offers context-sensitive help.

## 1.2 FEC Secure IPSec Client – Universal Solution for Secure VPN Solutions

The FEC Secure IPSec Client can be used in any VPN environment. The client communicates on the basis of the IPSec standard with the gateways provided by a wide variety of vendors and is the alternative to the uniform IPSec client technology offered on the market. The client software emulates an Ethernet LAN adapter. The client has additional features that introduce the user into a holistic remote access VPN solution.

***The IPSec Client offers:***

☑ Support of all major operating systems

☑ Dial-in over all transmission networks

☑ Compatibility with VPN gateways from a wide variety of vendors*

☑ Integrated personal firewall for more security

☑ Dialer protection (no misuse by third parties)

☑ Higher speed in the ISDN (channel-bundling)

☑ Saving telephone charges (charges and connection management)

☑ Convenient operation (graphic interface)

## 1.3 Performance range

The IPSec client supports all major operating systems (Windows 2000, Windows XP and Windows Vista). Connecting to the corporate network is media-type independent, e.g. in addition to ISDN, PSTN analog telephone network, GSM, GPRS, and xDSL, LAN technologies such as WLAN (on the corporate campus and hotspots) or local area networks (branch office network) are also supported. A possible scenario: an employee must access the corporate network from various locations with one and the same end device:

– in the branch office via WLAN
– in the corporate headquarters via LAN
– on the road at hotspots and at customer sites via WLAN or GPRS
– in the home office via xDSL, cable, or ISDN

### 1.3.1 Client Monitor – graphical user interface (GUI)

The graphical user interface (see →Client Monitor) of the IPSec client provides transparency during the dial-in process and data transfer. Among other things it provides information on actual data throughput.

The user knows whether his PC is online at all times, and if necessary what charges have been incurred.

### 1.3.2 Dialer

The system’s own dialer replaces the otherwise usual Microsoft Dialer. This offers advantages in several areas:

– intelligent line management (Short Hold Mode) in dial-up networks
– controlling the bandwidth (channel bundling) in the ISDN
– integrated personal firewall mechanism
– protection against “automatic dialers”

### 1.3.3 Line Management

In order to guarantee fast and cost effective data communications over public networks, all products include various automated processes and features for efficient Line Management, such as: Inactivity Timeout (Short Hold), Multilink support (Channel Bundling), Data Compression, Filtering, Spoofing, Local Termination etc. Optimal economy of scale achieved through intelligent features that minimize transmission times and connection costs.

This takes care of optimized costs transparence and a better overview: It allows the system administrator to determine certain limits for remote connections (e.g. maximum connection time, maximum number of connections established and units of charge) as well as automatic monitoring of the same by having the connection control in operation.

### 1.3.4 Personal Firewall

The IPSec client provides all the personal firewall functionalities to fully secure the workstation against attacks from the Internet, wireless LAN, or the local network. This shield consists of IP-NAT (Network Address Translation) and various IP-protocol filters. NAT is a security standard that prevents exposing the internal private IP address to the Internet by translating it to a legal or public IP address, thus enabling the host (e.g. user PC) to communicate safely across the Internet. Incoming packets are checked for precisely defined properties (address and protocol) in accordance a sophisticated filter, which rejects those that match the defined parameters. Source ports are also screened to prevent any masquerading. In other words: The Internet port of the respective computer is thoroughly protected, and the building of any unwanted links is prevented.

### 1.3.5 PKI Support

Strong authentication through digital certificates as soft certificates (PKCS#12) or on smart cards (PKCS#11, CT-API, PC/SC) increases the security for the PC as well as the corporate network. The IPSec client becomes part of a Public Key Infrastructure (PKI).

## Public Key Infrastruktur

PKI consists of a combination of standards, products, guidelines, and procedures. As such it provides the basic security platform for eCommerce business transactions, so those users (un)known to each other can safely com-municate. PKI is a globally recognized and applied technology for security. PKI includes the use of digital certificates that act as personal “electronic ID’s” and are issued by a Certificate Authority (CA) or Trust Center. Security experts and the IETF (Internet Engineering Task Force) have concluded that an effective protection against man-in-the-middle attacks can only be achieved by using Smart Cards with certificates.

Thus, a trust relationship, as we know it in the traditional world of paper-based business, can also be established in the world of global electronic information exchange. A digital signature in combination with data encryption is the electronic equivalent to a written signature and proves the validity and origin of messages in a similarly secure manner.

## Smart Card

Smart Cards are the ideal enhancement for high security Remote Access solutions. They provide two-fold security for Log-in purposes, which includes the PIN (Personal Identification Number) as well as the actual possession of the Smart Card itself. The User identifies himself as the Smart Card’s rightful owner by entering its assigned PIN (Strong Security). The PIN substitutes the entering of Password and User-ID (basis for Single-Sign-On). The User identifies himself only to the Smart Card. The validation against the network is negotiated between the Smart Card and the corresponding Security (Authentication) system. All security related processes are executed inside the card, thus not in the PC. Smart Cards also provide the technological basis for multi-functional applications, e.g. Company Card, etc.. Biometric processes can also be integrated.

# 2. Installation

A Setup program performs the installation of the client software quickly and smoothly. The following text describes the procedures for installing the client software under Windows 2000, Windows XP and Windows Vista.

**Prior to executing Setup be sure that the following prerequisites are fulfilled.**

# 2.1 Installation Prerequisites

## Operation System

In order to be able to communicate with the client software it is essential to have either Microsoft Windows 2000, Windows XP or Windows Vista installed on your PC (min. 128 MB RAM). During the installation you are asked to have your or disks ready, as these will be need-ed for updating your PC’s driver database files. Please insert these when prompted to do so.

## Remote Destination

The parameters of the remote destination must be entered in the profile settings. In order to communicate with the remote destination it must support one of the following media types: ISDN, PSTN (analog modem), LAN over IP, WLAN or PPP over Ethernet.

## Lokales System

One of the following communication devices and its respective drivers must be properly installed on the client software PC.

### ■ ISDN adapter (ISDN)

The device (e.g. internal or external adapter) must support the ISDN CAPI 2.0 Kernel Mode standard. When using PPP Multilink the software can bundle up to 8 ISDN B-Channels. Any ISDN device supporting the ISDN CAPI 2.0 can be used. Please check your device to be sure that such a driver is available. The client software does not support TAPI based ISDN devices.

### ■ Analog Modem (Modem)

The client software can communicate with any industry standard analog PC modem, provided that it and the modem drivers have been properly installed and the modem initialization string and the COM port definition for the modem is correct. The modem has to support Hayes AT commands.

Mobile (cellular) telephones can also be used for data communication, after the associated software has been installed that presents itself to the client precisely as if it were an analog modem. The serial interface, IR (infrared) interface, or Bluetooth can be used as interface between mobile phone and PC. The opposite side must have the appropriate dial-in platform depending on the transfer rate (GSM, v.110, GPRS or HSCSD). The initialization string in the Secure Client modem configuration must be obtained from the ISP or the manufacturer of the mobile (cellular) phone.

### LAN adapter (LAN over IP)

When the communication medium LAN has been defined the Client Software may be used as a IPSec client in a LAN that communicates across a LAN network and associated router to a central site VPN Gateway. When defined as a LAN Client, the Client Software can also be used as a VPN or VPN/PKI plugin for Microsoft's RAS (Dial-Up Network) client.

### xDSL Broadband Device (PPPoE)

Cable modems, splitters (e.g. for ADSL), etc. can be used in conjunction with PPP over Ethernet (PPPoE), which is supported by the Client Software.

### xDSL (AVM - PPP over CAPI)

If an AVM Fritz DSL card is to be used then this communication medium may be selected. AVM specific initialization strings may be entered in the field "Destination phone number" ("Dial-Up Network" group) for the connection.
It is recommended to use the standard setting "xDSL (PPPoE)" with Windows operating systems as this provides direct communication over the network interfaces.
No additional network card is necessary with the AVM Fritz! DSL card.

### Multifunction Card (GPRS/UMTS)

If you are using a multi-function card, special features of the mobile computing can be used depending on the card characteristics (see the appendix of the handbook "Mobile Computing). Due to the direct support of the multi-function card for UMTS/GPRS/WLAN through the Secure Client, installation of management software from the card implemented, is not necessary. The VPN connection is established via the integrated NCP Dialer independent of the Microsoft data communications network.
Currently supported multi-function cards:

– T-Mobile Multimedia NetCard
– Vodafone Mobile Connect Card
– KPN Mobile Connect Card
– T-Mobile DSL card 1800
– integrated Card of the Lenovo Notebooks (Sierra Chipset)
– Vodafone EasyBox USB-Adapter for UMTS/GPRS

## ■ WLAN adapter (WLAN)

Under Windows 2000/XP and Windows Vista the WLAN adapter can be operated with the link type “WLAN”. In the monitor menu the special “WLAN settings” menu item is displayed where the access data for the wireless network can be saved in a profile. If this “WLAN configuration” is activated, then the management tool of the WLAN card, or the Microsoft tool must be deactivated. (Alternatively the management tool of the WLAN card or the Microsoft tool can be used as well.)

If the link type WLAN is set for the destination system in the phonebook, then under the graphic field of the Client Monitor an additional area is shown where the field strength and the WLAN network are displayed.

Please read the description of the parameters “Link Type” in the section “Configuration parameters / Profile Settings”.

## ■ Automatic Media Detection

If various link types could be used, the client detects automatically which link type actally can be used und selects the fastest one.

On the basis of a pre-configured destination system, those link types that are currently available for the Client PC are detected and implemented, and if multiple alternative transmission paths are available, the fastest will be selected automatically. The link type priority is specified in the following sequence in a search routine: 1. LAN, 2. WLAN, 3. DSL, 4. UMTS/GPRS, 5. ISDN, 6. MODEM.

The configuration is executed in the phonebook with the link type “Automatic media detection” under “Destination system”. If desired, all destination systems for the VPN gateway that are pre-configured for this Client PC can be assigned to this automatic media detection. This renders manual selection of a medium (WLAN, UMTS, LAN, DSL, ISDN, MODEM) from the profile entries superfluous. Input data for the connection to the ISP are transferred from the available profile entries in a manner that is transparent for the user.

Please note the description “Destination System / Link Type”.

## Prerequisites for Strong Security

If you are using the client software with certificates (X.509), then the following prerequisites must be fulfilled:

- ### TCP/IP

The protocol TCP/IP must be installed on your PC.

- ### Smart Card Reader

The client software supports all Smart Card readers that are PC/SC conform. Subsequently such readers will only be entered in the client software Smart Card reader list after the Smart Card reader including the associated driver software has been installed on the PC. The client software detects the Smart Card reader automatically after the PC has been booted. The Smart Card reader can then be selected as described above and used accordingly.

In order to use the features of the Smart Card, configure the Smart Card by selecting “Configuration → Certificates” in the pull-down menu of the client software Monitor. When you insert your Smart Card in the Smart Card reader, you can enter your PIN.

- ### Smart Card Reader (CT-API conform)

Please note the following instructions when using a Smart Card reader that is CT-API conform:

☑ The current software includes drivers for the Smart Card readers SCM Swapsmart and SCM 1x0 (PIN Pad reader). These Smart Card readers can be set in the Monitor under “Configuration → Certificates”. If, however, the Smart Card reader does not work with the drivers, which are included in the software, or a Smart Card reader is to be used, which does not show up in the configuration selection of supported readers, then ask the supplier or producer of the Smart Card (or the respective website) reader for the current hardware driver and install it. In this case the client software requires some modifications:

Use an ASCII editor to edit the NCPPKI.CONF file. You find this file in the installation directory. Enter the name of the connected Smart Card reader as “ReaderName” (xyz) and the name of the installed driver as DLLWIN95 or DLLWINNT respectively. For operating systems based on Windows NT like Windows 2000 and Windows XP the modulname DLLWINNT has to be used. (The default name for CT-API conform drivers is CT32.DLL.)

Important: Only those drivers that have been appropriately set with “visible = 1” will be displayed in the list!

| | | | | |
|---|---|---|---|---|
| Modulname | = | SCM Swapsmart (CT-API) | → | xyz |
| DLLWIN95 | = | scm20098.dll | → | ct32.dll |
| DLLWINNT | = | scm200nt.dll | → | ct32.dll |

☑ After rebooting the PC the new “ReaderName” is displayed in the Monitor under “Configuration → Certificates → Smart Card reader”. Now you select that Smart Card reader.

## Smart Cards

Currently, the following Smart Cards are supported:

– Signtrust
– NetKey 2000
– TC Trust (CardOS M4)
– Telesec PKS SigG

## Soft Certificates (PKCS#12)

Instead of a Smart Card you can also use soft certificates or tokens.

## Smart Cards or Token (PKCS#11)

Drivers in the form of a PKCS#11 library are supplied with the software for the card reader or token. This driver software must first be installed. Then the NCPPKI.CONF file must be edited.

☑ Edit the NCPPKI.CONF file located in the installation directory by entering the name of the connected reader or token (xyz) as “module name”. The name of the DLL must be entered as PKCS#11-DLL. The associated “Slotindex” is manufacturer-dependant (standard = 0).

Important: Only those drivers are visible in the list that have been set to visible with “visible = 1”.

```
Modulname      = xyz
PKCS#11-DLL    = Name of the DLL
Slotindex      =
```

☑ After rebooting the PC the new “ReaderName” is displayed in the Monitor under “Configuration → Certificates → Smart Card reader”. Now you select that Smart Card reader.

## 2.2 Installing the Client Software

The actual version and later versions of the Client will be tested by the quality assurance only according to the operation systems Windows 2000, Windows XP and Windows Vista. Full functionality cannot be garanteed when using the client under Windows NT, Windows 98 or older Windows versions.

The initial installation steps for the Client Software are almost the same for Windows 2000, Windows XP and Windows Vista. Please note that there are some differences when installing from a hard disk, CD or removable disk.

You can obtain the software as EXE file by downloading it from the website under www.funkwerk-ec.com.

### *Installation and Licensing*

First the FEC Secure IPSec Client is installed as a test version. If you posess a license, you can enter the license data after a reboot of the software by selecting the monitor menu option “License Info and Activation”. The test version is valid for 30 days. Without software activation or licensing it will no longer be possible to setup a connection after this 30-day period expires. When 10-days validity remain, a message box will be displayed to remind you that the software has not yet been licensed. For licensing the software please refer to the chapter “Licensing” in the handbook.

### *Please note when installing the Software under Windows XP*

Microsoft Windows XP informs the user as soon as a driver software is being installed which is not licensed by Microsoft. Windows XP runs a Microsoft specific “compatibility test” and warns the user not to install the software. This test does not check the compatibility of the software with Windows XP. Since the client software is not licensed by Microsoft, the warning occurs when the client is installed on a Windows XP machine. What to do:

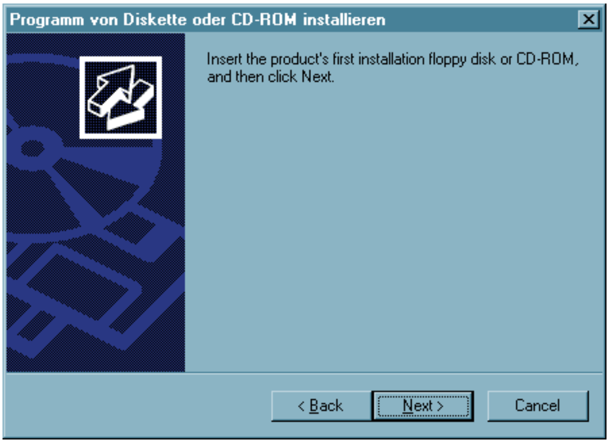
☑ You can modify the Windows XP default settings so that any software can be installed without the Microsoft compatibility check. Open the Windows Control Panel and then “System (Properies) - Driver Signing”. Set the install procedure to “Install the software anyway and dont’t ask for my approval”!

☑ You can ignore the warning when installing the client. After the warning pops up you click on “proceed Installation” Windows XP will let you install the client adapter. The installation will not have any negative effect on the operating system.

## 2.2.1 Default Installation

First you copy the EXE file you have got with a download or with the CD onto the hard disk of your PC. The filename of the EXE file displays the number of the verion and build number of the software, e. g.:
`FEC_EntryCl_Win32_200_030.EXE`

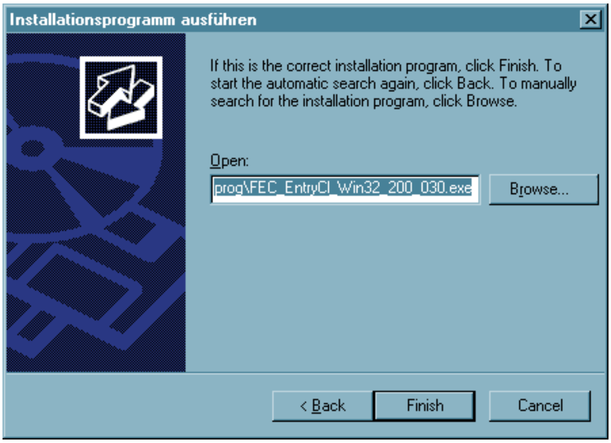
To install the software select in the windows main menu ”Start → Settings → Control Panel.” Select “Add/Remove Programs” in the Control Panel and then click on the “Install” button.



Programm von Diskette oder CD-ROM installieren

Insert the product's first installation floppy disk or CD-ROM, and then click Next.

Click on “Next” when the window on the left hand appears.

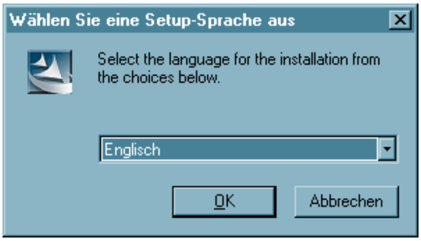


Installationsprogramm ausführen

If this is the correct installation program, click Finish. To start the automatic search again, click Back. To manually search for the installation program, click Browse.

Open: prog\FEC_EntryCl_Win32_200_030.exe

When the following window appears click on “Browse” to select the EXE file and click on “Finish”.



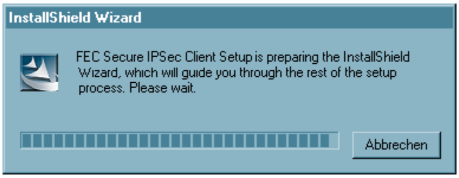
Wählen Sie eine Setup-Sprache aus

Select the language for the installation from the choices below.

Englisch

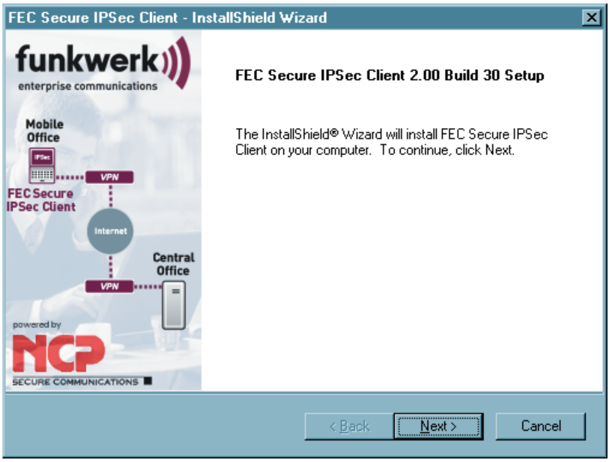
A window appears where you can select the language to be used for the installation and then click “OK”.

→ *continue next page*


InstallShield Wizard

FEC Secure IPSec Client Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.

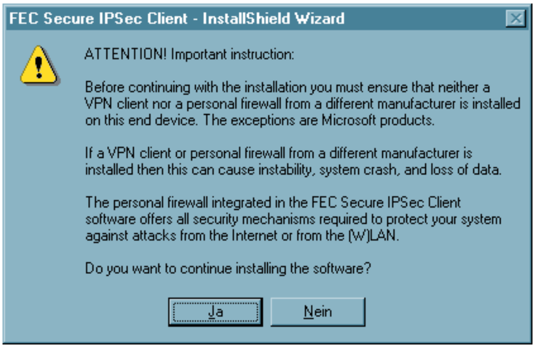
The “Install Shield Assistant” is now started. It will guide you through the installation.


FEC Secure IPSec Client - InstallShield Wizard

FEC Secure IPSec Client 2.00 Build 30 Setup

The InstallShield® Wizard will install FEC Secure IPSec Client on your computer. To continue, click Next.

Read the terms of the Software License Agreement carefully and click on “Next”.


FEC Secure IPSec Client - InstallShield Wizard

ATTENTION! Important instruction:

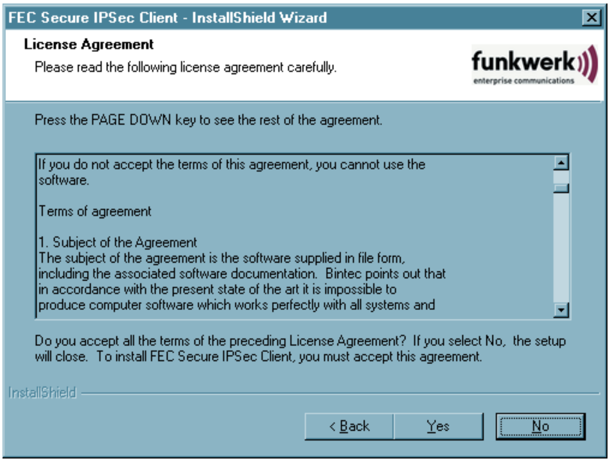
Before continuing with the installation you must ensure that neither a VPN client nor a personal firewall from a different manufacturer is installed on this end device. The exceptions are Microsoft products.

If a VPN client or personal firewall from a different manufacturer is installed then this can cause instability, system crash, and loss of data.

The personal firewall integrated in the FEC Secure IPSec Client software offers all security mechanisms required to protect your system against attacks from the Internet or from the (W)LAN.

Do you want to continue installing the software?

Note the following message and deactivate any VPN Client and Personal Firwall of another manufacturer to avoid data loss.


FEC Secure IPSec Client - InstallShield Wizard

**License Agreement**

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

If you do not accept the terms of this agreement, you cannot use the software.

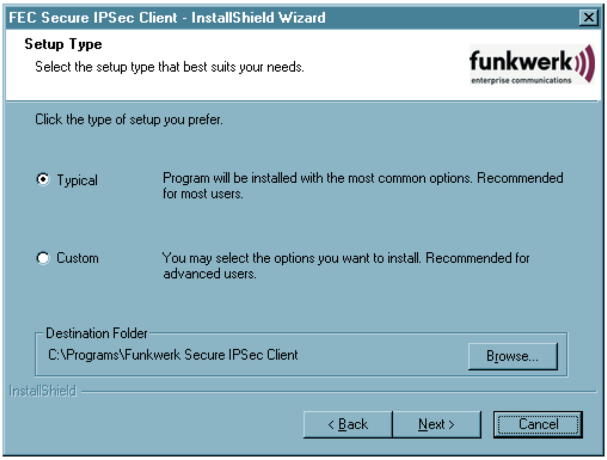
Terms of agreement

1. Subject of the Agreement
The subject of the agreement is the software supplied in file form, including the associated software documentation. Bintec points out that in accordance with the present state of the art it is impossible to produce computer software which works perfectly with all systems and

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install FEC Secure IPSec Client, you must accept this agreement.

The next window displayes the software Licensed Agreement. In order to proceed with the installation of the licensed version click on “Yes”. Clicking “No” will stop the installation process.

→ *continue next page*


FEC Secure IPSec Client - InstallShield Wizard

**Setup Type**

Select the setup type that best suits your needs.

Click the type of setup you prefer.

● Typical — Program will be installed with the most common options. Recommended for most users.

○ Custom — You may select the options you want to install. Recommended for advanced users.

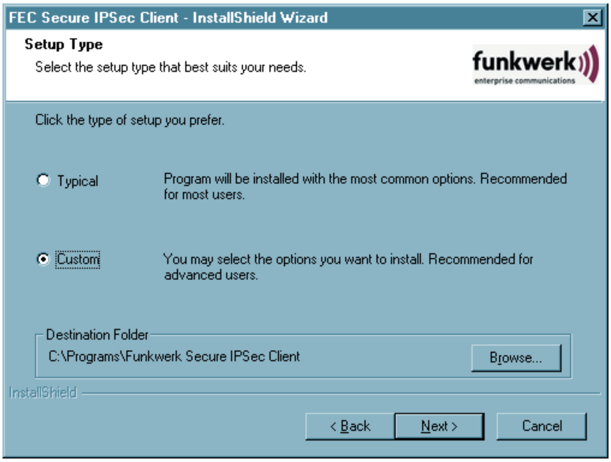
Destination Folder: C:\Programs\Funkwerk Secure IPSec Client

Default directory for installation* is: Programs\ Funkwerk Secure IPSec Client

Undependently of “Typical” or “Custom” installation you can select any folder for the software installation by clicking on “Browse”. This is particularly important if the user should have no rights on the system root directory.

If you select “**Typical**” in this window the installation will continue automatically and the setup is finished.

* Under Windows Vista it could also be:
Program Files\Funkwerk Secure IPSec Client


FEC Secure IPSec Client - InstallShield Wizard

**Setup Type**

Select the setup type that best suits your needs.

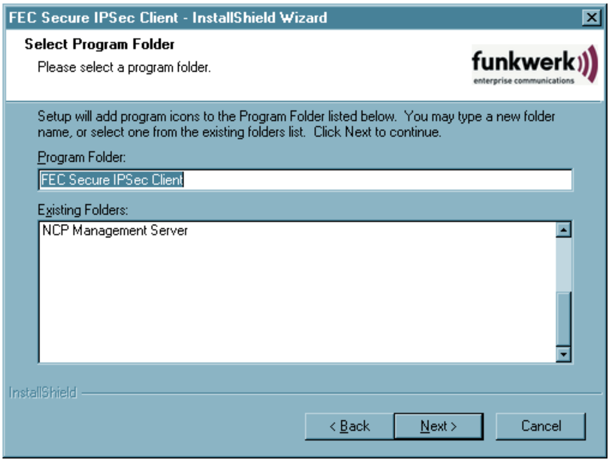
Click the type of setup you prefer.

○ Typical — Program will be installed with the most common options. Recommended for most users.

● Custom — You may select the options you want to install. Recommended for advanced users.

Destination Folder: C:\Programs\Funkwerk Secure IPSec Client

Selecting the “**Custom**“ Installation you can define settings according to your requirements.


FEC Secure IPSec Client - InstallShield Wizard

**Select Program Folder**

Please select a program folder.

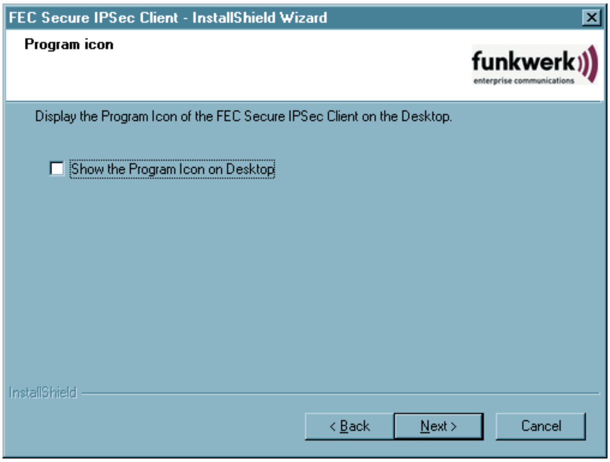
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

Program Folder: FEC Secure IPSec Client

Existing Folders:
NCP Management Server

In the following window of the “Custom" installation you define the programmfolder for the client software. (Default setting “FEC Secure IPSec Client”)

→ *continue next page*



FEC Secure IPSec Client - InstallShield Wizard

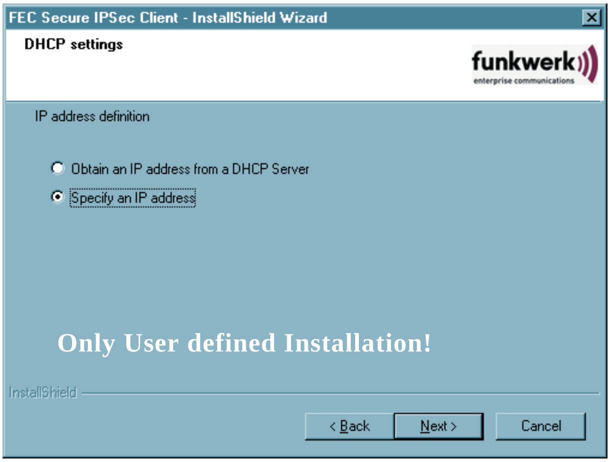
**Program icon**

Display the Program Icon of the FEC Secure IPSec Client on the Desktop.

□ Show the Program Icon on Desktop

Moreover you can have the program icon displayed on the desktop.

Please contact your system administrator or your internet service provider for additional information about your communication gateway.



FEC Secure IPSec Client - InstallShield Wizard

**DHCP settings**

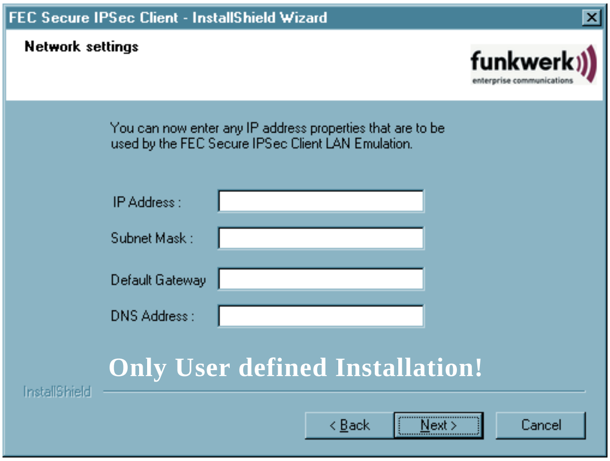
IP address definition

○ Obtain an IP address from a DHCP Server

● Specify an IP address

Only User defined Installation!

Communication with DHCP (Dynamic Host Control Protocol) means that a temporary IP Address will be assigned automatically for each communication session. If required, click on “Obtain an IP Address from DHCP Server”.



FEC Secure IPSec Client - InstallShield Wizard

**Network settings**

You can now enter any IP address properties that are to be used by the FEC Secure IPSec Client LAN Emulation.

IP Address :

Subnet Mask :

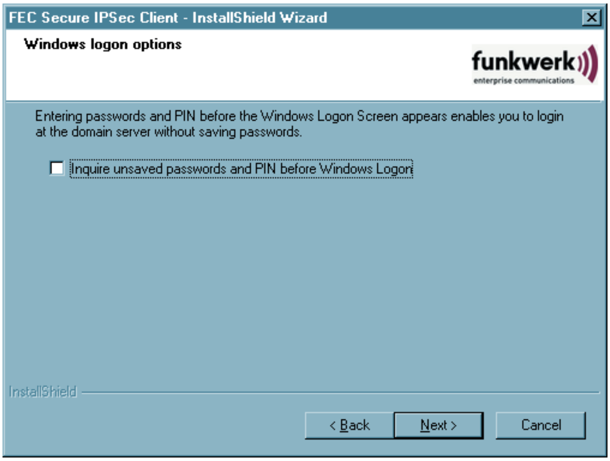
Default Gateway

DNS Address :

Only User defined Installation!

If you “Specify an IP Address”, enter the IP address in this window. Default Gateway: If a network adapter with a Default Gateway is already installed, you will have to delete this Default Gateway Address. It is not possible to have more than one network adapter with a Default Gateway. DNS Address: You should only enter a DNS Address if you have been assigned one from your system administrator or ISP.

→ *continue next page*


FEC Secure IPSec Client - InstallShield Wizard

Windows logon options

Entering passwords and PIN before the Windows Logon Screen appears enables you to login at the domain server without saving passwords.

□ Inquire unsaved passwords and PIN before Windows Logon

Thereafter you can define whether a logon to a remote domain should occur after establishing a connection to the remote destination's NAS, which may necessitate entering the PIN for your certificate and/or your Password (if not already stored in the Client Software). After establishing a connection to the remote destination's NAS, you can logon to the remote domain. This logon will be encrypted.

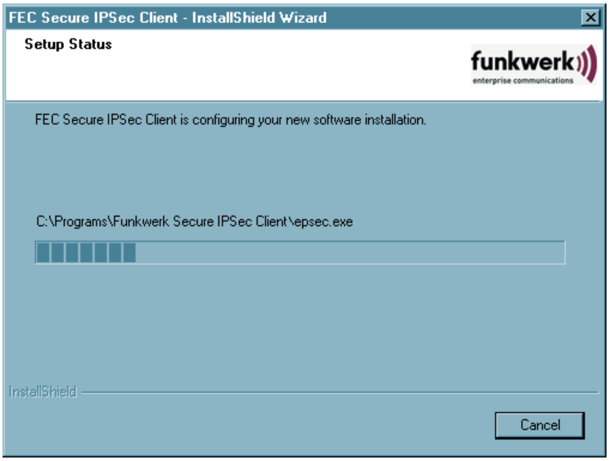
Please note: Activate this option before the Windows logon, thus the NCP Gina will also be automatically installed. The logon options can also be used only if the NCP Gina is installed after the Windows Gina - which is possible in this setup window. These logon options can be set via the Monitor menu of the Client under "Configuration".

If the logon option is not activated here, and if it will be used at a later point in time, then the NCP Gina can be permanently installed after this setup using the command

```
rwscmd /ginainstall
```

See the description "Secure Client Services" in this regard, in the appendix of this manual.

Now the data will be loaded and copied.


FEC Secure IPSec Client - InstallShield Wizard

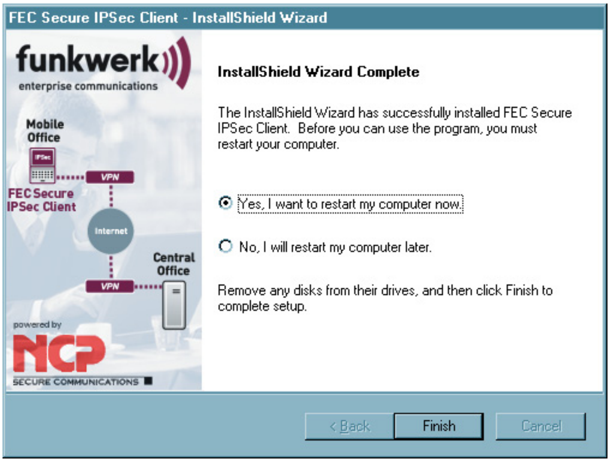
Setup Status

FEC Secure IPSec Client is configuring your new software installation.

C:\Programs\Funkwerk Secure IPSec Client\epsec.exe

There after the associated network components will be installed.

→ *continue next page*



**InstallShield Wizard Complete**

The InstallShield Wizard has successfully installed FEC Secure IPSec Client. Before you can use the program, you must restart your computer.

● Yes, I want to restart my computer now.

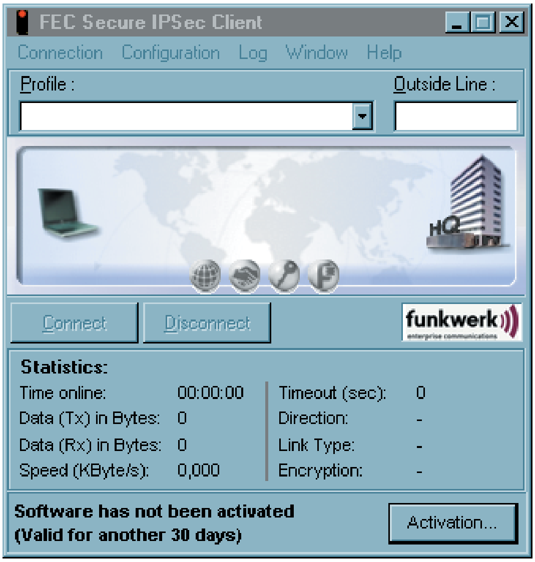
○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

This completes the installation of the Client Software. Click the “Finish” button. Before using the Client Software it is necessary to reboot your PC. Click on “Yes, I want to restart my computer now” and then click on “Finish” to reboot your PC.

## 2.3 Before starting

After installing, the Client Monitor is displayed on the screen of your PC. To use the client you first have to generate an entry in the profile settings, what means that you have to define a profile according to a destination system to which an IPSec connection can be established.

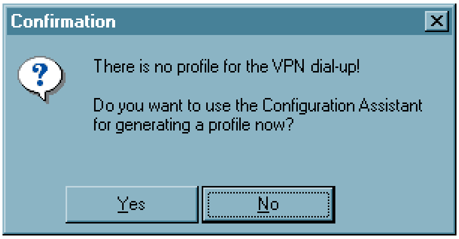


Statistics:

Time online: 00:00:00
Data (Tx) in Bytes: 0
Data (Rx) in Bytes: 0
Speed (KByte/s): 0,000

Timeout (sec): 0
Direction: -
Link Type: -
Encryption: -

**Software has not been activated**
**(Valid for another 30 days)**



There is no profile for the VPN dial-up!

Do you want to use the Configuration Assistant for generating a profile now?

If you click on “Yes” in the confirmation window, you can use the offered assistant. The assistant can also be started later. Therefore you activate the menu item “Profile Settings” in the main menu of the monitor under “Configuration” (see → 4. Configuration, Profile Settings).

For further configuration refer the descriptions under “4. Profile Settings” and “5. Configuration Parameters, IPSec General Settings”. Only if a profile has been defined, a connection to the according destination system can be established. See “ 6. Establishing a Connection”.

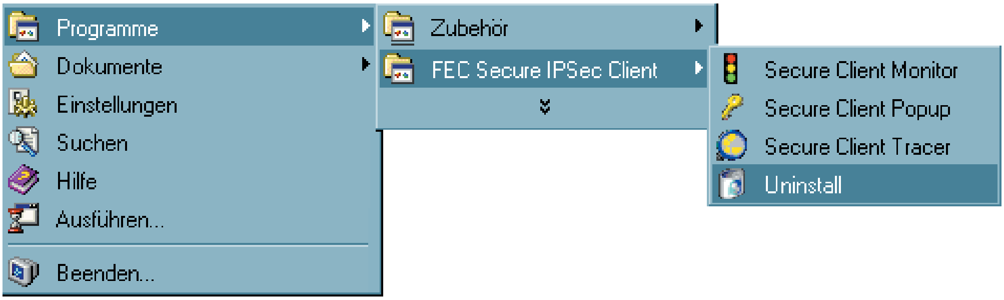
For activating the software refer to the section “4.5 Help” and “4.6 Licensing” in this manual.

In order to guarantee the proper functionality of your IPSec Client Funkwerk Enterprise Communications offers a public VPN test access. A detailed step-by-step guidance how to use this test access and how to set the needed configurations correctly can be found on the websites at www.funkwerk-ec.com.

## 2.4 Uninstalling

There are two methods to remove the software from your machine:

1. Navigate to, and select the Uninstall option from the Windows Start Menu in the “FEC Secure IPSec Client” program group (see illustration below).



A confirmation request will be made- if confirmed, the Uninstall Shield will commence with removing the software from the system.

2. Using the “Start → Settings → Control Panel → Add/Remove Software” option select the client from the list of programs and Windows components currently installed on the system. Click “Change/Remove” button to run the Uninstall Shield and remove all the software from your system.

Important: After the removal of the software components, the profile and configuration settings are still saved and can be restored in the event a newer version of the client is installed. In order to completely delete everything; manually remove the installation directory.

## 2.5 Project Logo

The logo is displayed in a panel of the Client over the entire width of the Monitor at the very bottom. An ini file (ProjectLogo.ini) must be created for the logo, where the following can be entered:

– Project logo for small fonts
– Project logo for large fonts
– Info text (ToolTip) if the cursor is positioned on the logo
– HTML file if there is mouse click on the logo.

For the installation a “ProjectLogo.ini” is copied into the installation directory that contains further explanations for creating the logo.

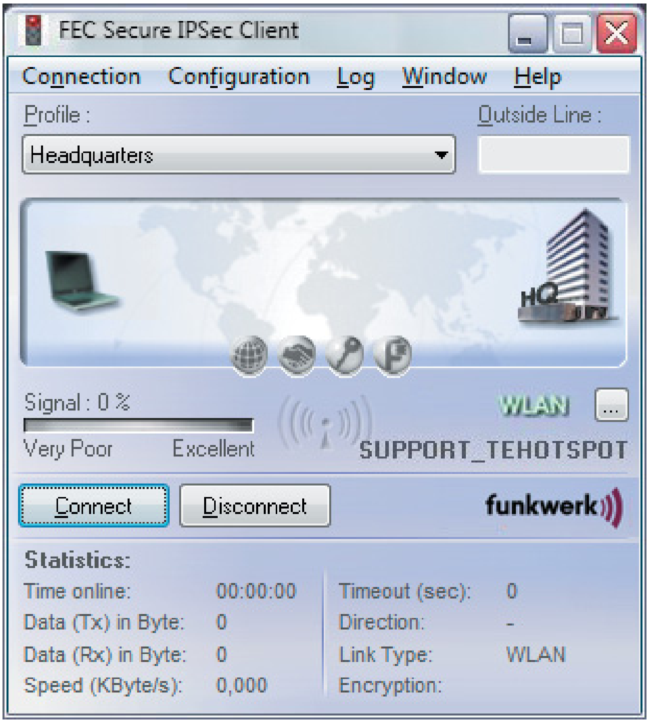
```
===============================================================
ProjectLogo.ini
===============================================================
[GENERAL]
Picture_96=
Picture_120=
ToolTip1=
HtmlLocal=

# Picture_96
# ==========
# Bitmap of the project logo for view with small fonts (96 DPI)
# Height: 24 pixels (minimal)
# Width: 328 pixels (precise)
# If a path is not specified, then the file is searched in the
# current directory of the Secure Client.
#
# e.g. Picture_96=C:\Programs\Funkwerk Secure IPSec Client\
#                                         MyProjectPicture.bmp
#
# Picture_120
# ==========
# Bitmap of the project logo for view with large fonts (120 DPI)
# Height: 29 pixels (minimal)
# Width: 404 pixels (precise)
# If a path is not specified, then the file is searched in the
# current directory of the Secure Client.
#
# e.g. Picture_96=C:\Programs\Funkwerk Secure IPSec Client\
#                                         MyProjectPicture.bmp
#
# ToolTip[1] ... ToolTip[X]
# =========================
# Info text for the ToolTip of the project logo.
# For each line in the info text a ToolTip entry with
# consecutive number (ToolTip[x]) must be created.
#
# e.g. ToolTip1=the info text for the project logo
# ToolTip2=--------------------
# ToolTip3=third  line ...
# ToolTip4=fourth line ...
#
# HtmlLocal
# =========
# HTML file that will be displayed, if there is a mouse click
# on the project logo. The file must be available locally on
# the computer. If a path is not specified, then the file is
# searched in the current directory of the Secure Client.
#
# e.g. HtmlLocal=C:\Programs\Funkwerk Secure IPSec Client\
#                                         MyProjectInfo.html
```

# 3. Client Monitor

Once you have installed the Client the Monitor should appear automatically on PCs screen. To manually display the Monitor click on: Start → Programs → FEC Secure IPSec Client → Secure Client Monitor. The Client Monitor will be loaded and displayed on the screen or in the task bar.

Note: When the monitor is loaded it will either be displayed on the screen (as well as the taskbar) or if it is not displayed but loaded it appears in the taskbar.



Profile : Headquarters

Outside Line :

Signal : 0 %

Very Poor Excellent

SUPPORT_TEHOTSPOT

Statistics:

| | | | |
|---|---|---|---|
| Time online: | 00:00:00 | Timeout (sec): | 0 |
| Data (Tx) in Byte: | 0 | Direction: | - |
| Data (Rx) in Byte: | 0 | Link Type: | WLAN |
| Speed (KByte/s): | 0,000 | Encryption: | |

***The Client Monitor serves 4 important purposes:***

☑ to display the current communications status

☑ for selection of Link Type

☑ for definition of Call Control parameters

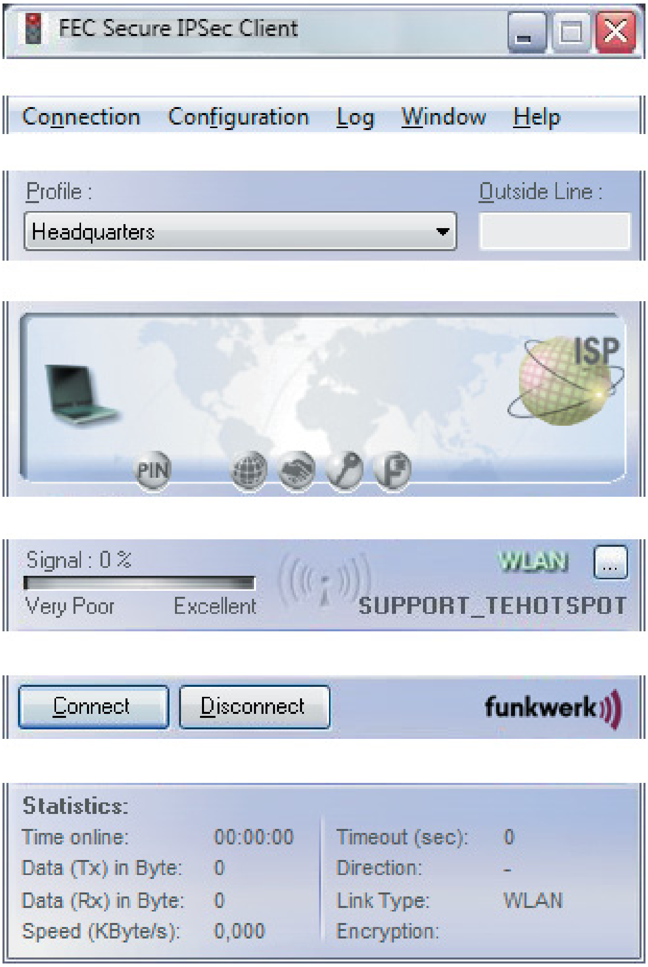
☑ for definition of Profiles and associated Destination and Security parameters

# 3.1 The Client Monitor User Interface

## 3.1.1 Operation and Display Field

The Client Monitor consists of:

- □ A title header indicating the security version of the client,
- □ the main menu bar,
- □ A display of the currently selected Profile and a window for Outside Line Prefix if so needed,
- □ the graphic status field, displaying the communication status,
- □ The field that displays signal strength only opens for connection types UMTS/GPRS/WLAN,
- □ the button bar with "connect" and "disconnect"
- □ and the statistics field



Profile : Headquarters

Outside Line :

Signal : 0 %

Very Poor Excellent

SUPPORT_TEHOTSPOT

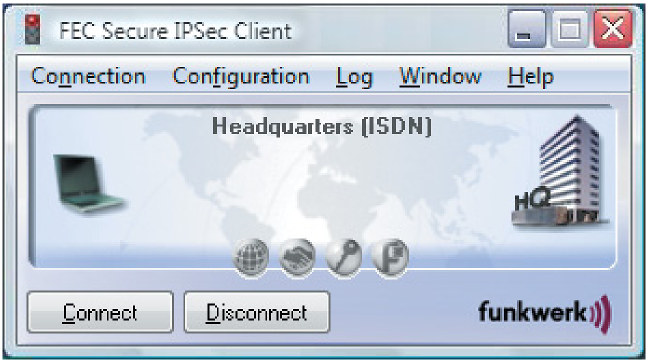
Statistics:

| | | | |
|---|---|---|---|
| Time online: | 00:00:00 | Timeout (sec): | 0 |
| Data (Tx) in Byte: | 0 | Direction: | - |
| Data (Rx) in Byte: | 0 | Link Type: | WLAN |
| Speed (KByte/s): | 0,000 | Encryption: | |

The user interface is conform Windows standards, and operation is similar to that of other Windows applications. The monitor can either be operated by using pull down menus from the menu bar, or by using buttons from the button bar, or via the context menu (right mouse button).

## 3.1.2 The Apperance of the Monitors

The monitor can be displayed in different sizes according to the setup in “Window” from the monitor menu (see → 4.4 Window).



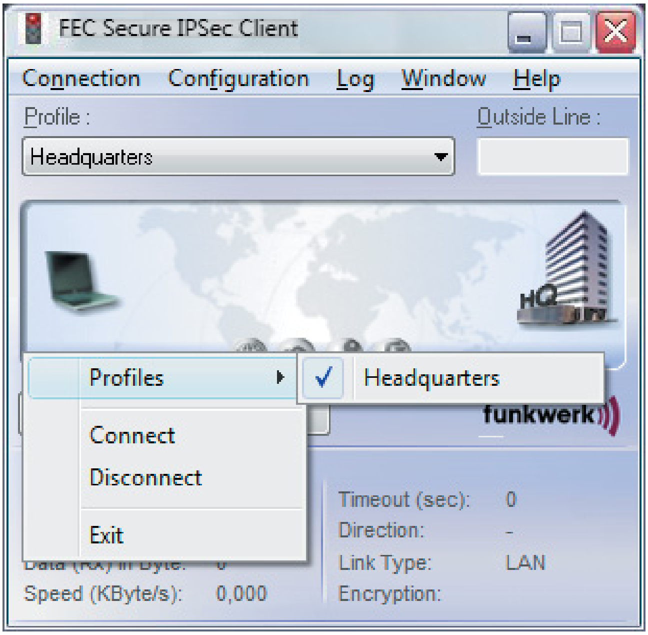
The Link Type is shown in the statistic window or can be entered by defining the profile so that is displayed in the status field as well.

### *Modification of the Interface*

The monitor appearance can be modified by the administrator. This is particularly relevant for the menu choices “Link Information”, “Certificates”, “Link Control” and “Logon Options”. Also the administrator can suppress profile parameter fields and can suppress individual parameters or set them to “non configurable”. The suppressed and deactivated features and parameters simplify software operation, they do not influence the performance of the software or your work. Refer the section 4.2 Configuration, 4.2.9 Configuration Locks.

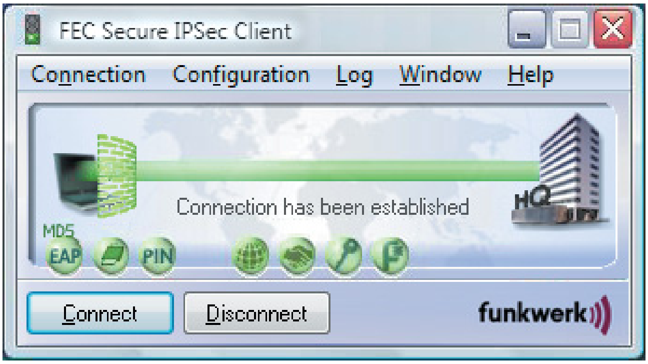
## 3.1.3 Dialing-up und selecting the Destination system

Once the software has been installed and a profile has been configured correctly (see → 4.2 Configuration), you are ready for dialing up to the selected destination.



The profile can be selected in two ways: either from the pull-down menu, or from the pop-up menu invoked by clicking on the right mouse button. (see illustration)

In order to establish a connection it is therefore not necessary to start the client monitor itself or to dial-up manually. The only software that must be started is the desired application software (Email, Internet browser, terminal emulation, etc.). The connection will then be established automatically (see → Line Management, Connection Mode, automatically).


FEC Secure IPSec Client
Connection Configuration Log Window Help
Connection has been established
HQ
MD5
EAP
PIN
Connect
Disconnect
funkwerk

It is also possible to manually establish the connection to a selected destination by selecting “Connection” in the main menu and click on “connect” Alternatively you can click on the “connect” button in the tool bar.

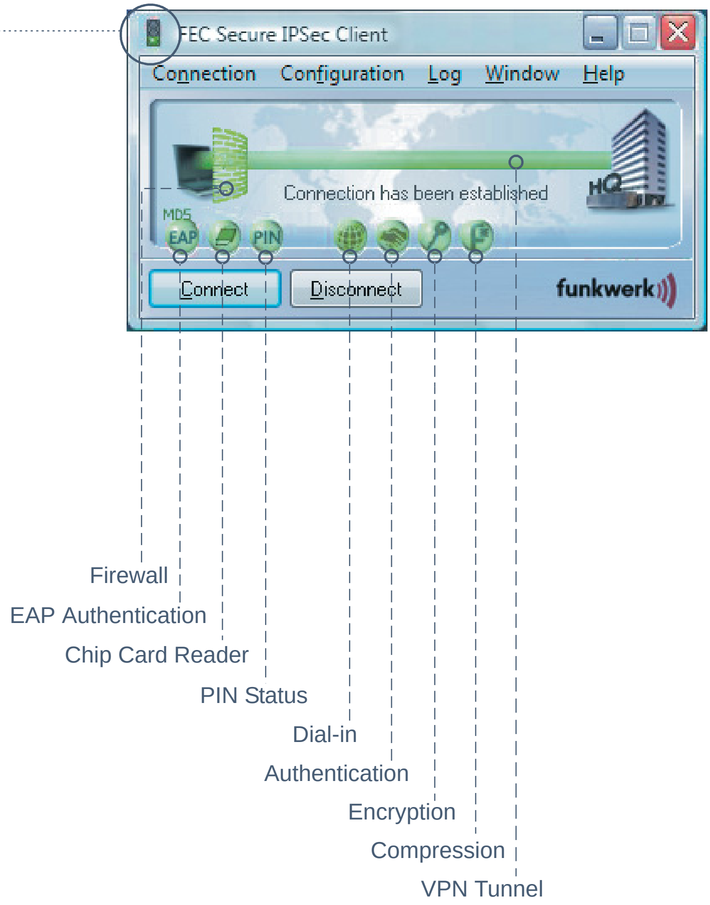
When the connection is established (see → illustration above), the monitor displays a thick green bar from the Client to the Server under which the text “Connection is established” is displayed. At the same time, the traffic lights change from red to green. The green traffic light denotes an established connection and occuring costs.

## 3.1.4 Symbols of the Monitor

The Client's Monitor interface has been informatively designed with icons. They provide information about the current status of the connection or about specific configured features via appearance and color.

The traffic light icon is always visible when the Client starts. If you minimize (close) the Monitor, this icon will be displayed in the taskbar. Double click on this icon to re-open the Monitor. The traffic light icon only disappears when the Monitor is closed.

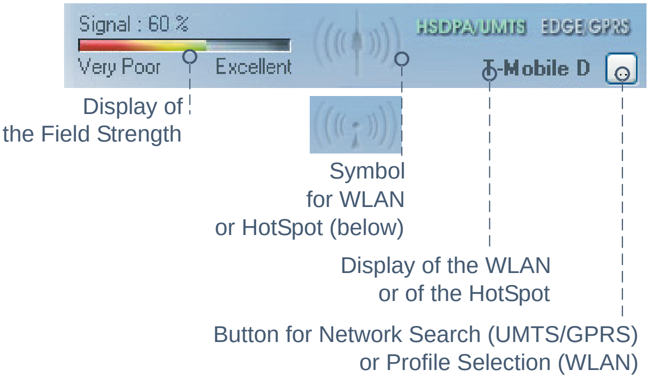
The other icons are described in details on the following pages.



Connection has been established

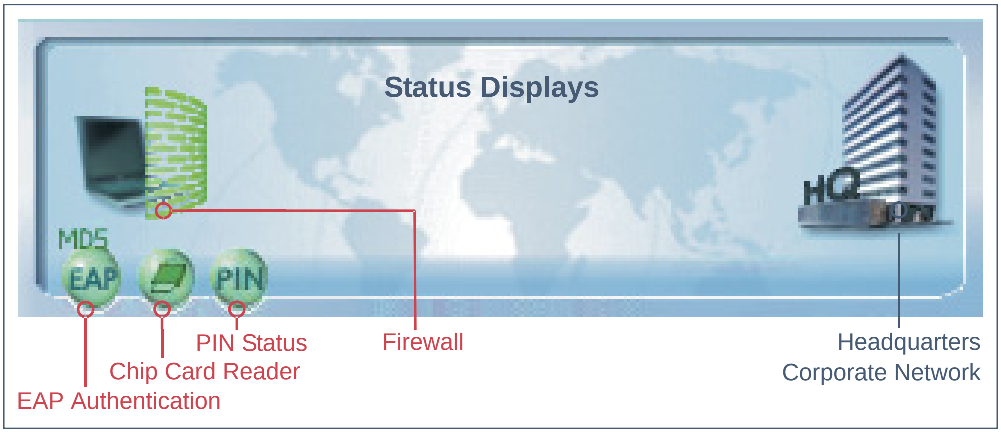
In addition either WLAN panel or a UMTS / GPRS panel will be displayed in the monitor depending on configuration and installation of a multifunction card.

In the UMTS / GPRS panel you can select the desired data transmission process by clicking on the respective label. Then the icon will be displayed in green.



## 3.1.5 Status Displays

The graphic field of the Client Monitor displays different icons depending on the configuration; these icons can take on different status settings depending on the phases of the connection setup. Tooltips provide brief comments relative to function when you move the cursor over one of the icons. The status displays are described below in the sequence in which they are shown in the illustration below, from left to right.



### EAP Authentication

If an extended authentication via the Extensible Authentication Protocol (EAP) has been activated in the “EAP options” then this will be displayed via the EAP icon. The color **yellow** indicates the EAP negotiation phase, **red** indicates unsuccessful authentication, **green** indicates successful authentication with EAP. Double click on the EAP icon to reset the EAP. Then a new EAP negotiation will be executed automatically.

If the Client is successfully authenticated relative to a network component, the opposite side will indicate which protocol was used; this information is always displayed with a **green** icon and the designation MD5 or TLS.

If an EAP icon is displayed in **red** and the connection has been set up nonetheless; this means that EAP has been configured in the Client, however the network component does not require EAP.

### Chip Card Reader

If a smart card reader has been installed and configured (see Monitor menu -> Configuration / Certificate), then its icon will be displayed in **blue**.

If the smart card is inserted in the reader, this icon will be displayed in **green**.

## PIN Status

A PIN icon in **gray** always means that the system is still waiting for the PIN to be entered for the respectively configured certificate. Double click on this icon to open the dialog for entering the PIN. An incorrect PIN is acknowledged with an error message, and remaining number of possible PIN entry attempts will be reduced.

After successfully entering the PIN the icon will be displayed in **green**. This color indicates that the entered PIN is valid, even if a connection has not been set up. If you want to ensure that unauthorized persons cannot establish a connection in your absence, then the PIN must be reset (see Monitor menu -> Reset Connection / PIN) or the “PIN query function for each connection setup” must be activated under “Configuration / Certificate. In the latter case the dialog for PIN entry will not be displayed after double clicking on the grey icon, it will only be displayed after connection setup.

## Firewall

The firewall icon is always visible if a firewall is activated. If the global firewall (Personal Firewall) with defined rules is active, and the link-specific firewall is not active, then the icon will be displayed in **red** without arrows.

If the administrator has specified a Friendly Net (Friendly Net Detection), and if the Client is in a friendly net, then the firewall icon will be displayed in the color **green**. Friendly Net Detection specifications are made in the Monitor Configuration menu under “Settings / Friendly Nets”, either by specifying static network routes, or by activating automatic Friendly Net Detection. In this regard, see the description under “Firewall Settings / Configuration Field - Friendly Nets”.

If Link Firewall is activated, the icon will be displayed with arrows, regardless of whether the global firewall is active or inactive.

If the Link Firewall has been switched active in the Phonebook with “Activate Stateful Inspection -> Always” and the system is configured so that communication is only allowed in the tunnel then the firewall icon will be displayed with **two red arrows**.

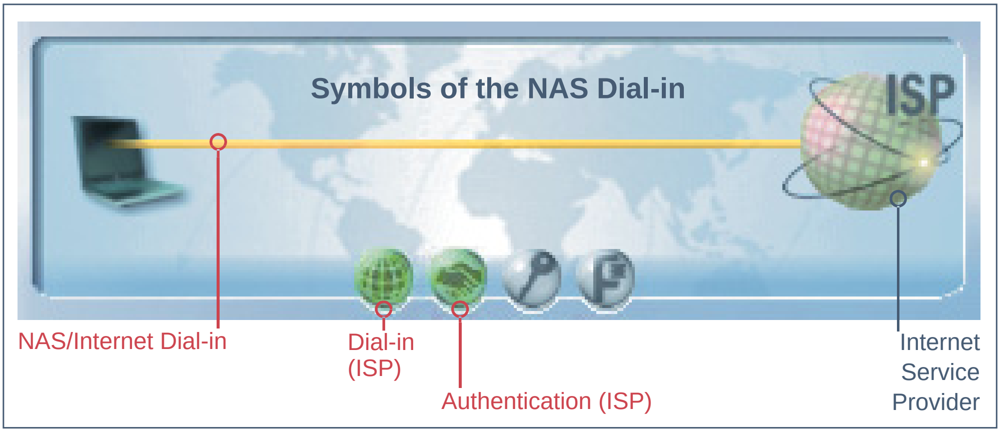
If the option “Only allow communication in the tunnel” is switched off then the icon will be displayed with **one green arrow and one red arrow**.

If Stateful Inspection is only activated for an existing connection then arrow icons are only displayed after a connection setup.

The **arrow symbols** appear **in front of a green firewall**, if in addition to Link Firewall options, a Friendly Net where the Client is currently located has been defined in the global firewall.

## 3.1.6 Connection Setup Symbols

In addition to the status displays the graphic field of the Client Monitor also includes connection set up icons.



### Symbols of the NAS Dial-in

If a dial-in to the Network Access Server or Internet Service Provider (ISP) is taking place on the Internet then the dial-in connection will be indicated by a thin yellow line. The dial-in is concluded and the connection to the ISP is established when the thin connection line is displayed in green.

The colors of the NAS dial-in icons change color concurrently with the start of the connection setup.

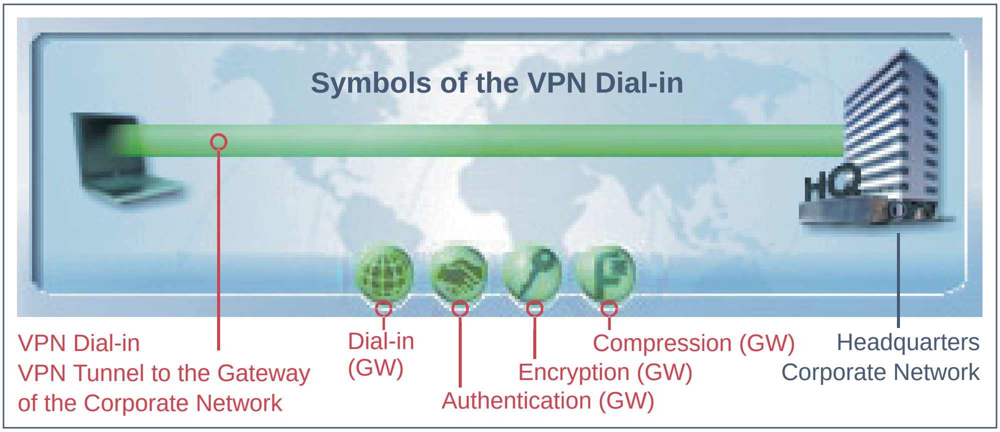
Dial-in to the ISP is displayed with a green globe; authentication at the ISP is indicated with a handshake. During the connection setup its color changes from gray to blue , then flashes green, and finally is displayed as constant green to indicate successful connection set up.

The parameters for NAS dial-in are located in the profile settings under “Network Dial-In”. If the profile will be used for “Automatic Media Detection” (see -> Profile Settings / Basic Settings), then it is strictly required that you enter a user ID and a password under “Network Dial-In”.

### Symbols of the VPN Dial-in

After NAS dial-in is concluded, the VPN dial-in to the corporate gateway can take place. In this process the dial-in connection will be symbolized with a thick yellow line. If the dial-in is concluded and the connection to the VPN Gateway is successfully established then the thin connection line will be displayed in green.

The colors of the VPN dial-in icons change color concurrently with the start of the connection setup to the gateway. Dial-in and authentication on the VPN gateway are displayed in precisely the same manner as they are displayed for NAS dial-in. In addition there are icons for key negotiation (keys) and compression (pliers), if configuration of these icons is prescribed from the gateway side.



The colors of the icons change from gray to black, then flash green, and finally are displayed as constant green to indicate successful connection set up. In this regard the dial-in and authentication processes on the gateway must always be executed; encryption and compression are optional. From left to right the VPN dial-in icons are:

**Dial-in on the VPN Gateway:**
The target address of the VPN gateway is specified in the profile settings under “IPSec Settings / Gateway”.

**Authentication on the VPN Gateway:**
The necessary parameters are in the profile settings under “Identity”. “Extended Authentication (XAUTH)” is always used. User ID and password are either read from the configuration under these parameters, or they are read from the certificate. A certificate that will be used is configured in the Monitor menu under “Configuration / Certificates”, and the issuer certificate of the gateway that will be selected must agree with the user certificate.

**Encryption:**
Either a pre-shared key or the private key from a certificate are used for encryption. Both alternatives are set in the profile settings under “Identity”. If the pre-shared key is used, then the “Shared Secret” must be entered here. If the “pre-shared key” is not used then the certificate will be used automatically. The gateway specifies which encryption will be used.

**Compression:**
Compression is only used if it is also supported by the gateway. You make the compression settings in the profile settings under “Use Extended IPSec Options / IP Compression”.

# 4. Using the Client Monitor

The description follows the menu items in the menu bar.

The menu-bar consists of the following items from left to right:

□ Connection

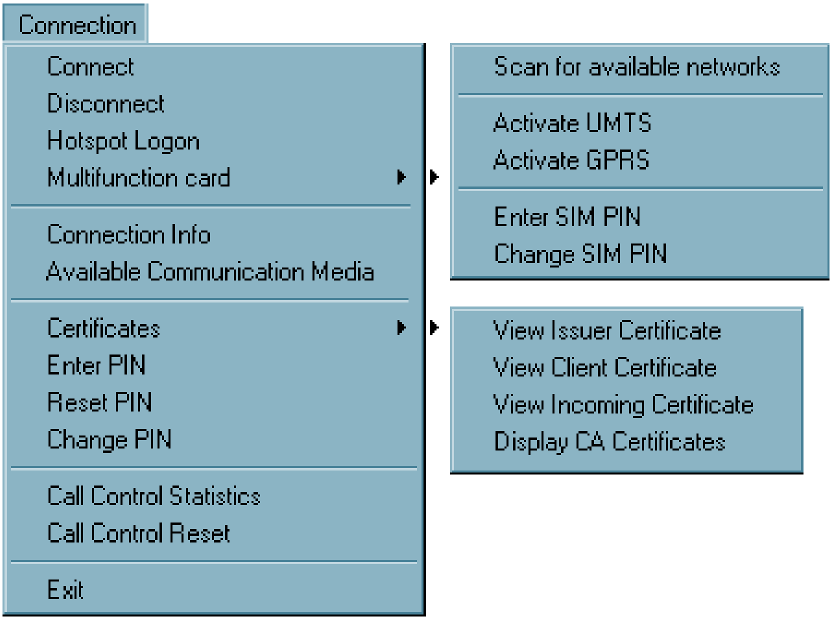
□ Configuration

□ Log

□ Window

□ Help

## 4.1 Connection



With this choice you will find commands for Link establishment and Link break-off. You will also find information windows displaying the current link establishment and the implemented certificates. In addition Link control statistics can be read here and if required the Link control barrier can be deleted if a threshold value that you have set is exceeded.

### 4.1.1 Connect

This command is used to initiate a connection. A connection can only be made if a profile has been properly defined and selected in the Profile Settings (see → Profile Settings, Basic Settings). The selected profile is displayed in the “Profile” field of the monitor.

Selecting the function “Connect” the connection will be established manually to the destination system. Whether the link is built manually or automatically depends on the “Connection Mode” defined for the profile in the Line Management folder of the profile settings as well as the Link Type being used (see → Profile Settings, Line Management, Connection Mode).

### 4.1.2 Disconnect

A connection can be terminated manually by clicking on “Disconnect” in the Connection pull-down menu or by clicking the right mouse button. As soon as the connection has been terminated, the “traffic light” switches from green to red.

### 4.1.3 HotSpot Logon

Requirements: The user must be in the receiving range of a hotspot, with an activated WLAN card. There must be a connection to the hotspot and the wireless adapter must have an assigned IP-address. (Windows XP provides you with the needed configurations concernig access to WLANs).

The clients firewall makes sure that only the IP-address assignment is being done by DHCP without any further possibilities of access to or from the WLAN. The firewall has intelligent automated processes for clearing the ports of one or more https so as to make logins and -outs to the hotspot available. Durig this process only data traffic to the hotspot server is possible. In this way a public WLAN can only be used for connecting VPN to the central data network, direct internet access is excluded. For opening the homepage of a hotspot in the browser a possible existing proxy-configuration must be deactivated.

At present the clients hotspot access works only with those hotspots, that redirect inquiries with the help of browsers to the homepage of the public WLAN provider (for example T-Mobile or Eurospot).

Under previously described conditions a click on the menu option “Hotspot Logon” opens the website to log into the standard browser. After entering the access data the VPN-connection to, for example, the company’s headquarters can be established and safe communication is possible.

After this menu option has been selected different connection messages will be displayed on the screen:

– If the user is already connected to the Internet he will be connected with the start page http://www.ncp.de. A window with the following message will appear:

“You are already connected to the Internet. Hotspot logon is not necessary or has already been executed.”

This text can be changed by the administrator by entering the address of a different HTML start page in the form
`http://www.mycompagnie.de/error.html`
And the text of error.html is changed accordingly.

– If the user is not yet logged on, then a window will be displayed requesting the user to enter user ID and password for logon to the hotspot operator.

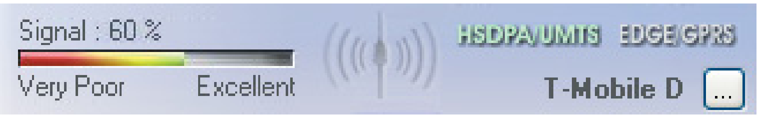
– If the user has not reached a website, then the Microsoft error message “...not found” will be displayed.

## 4.1.4 Multifunction Card

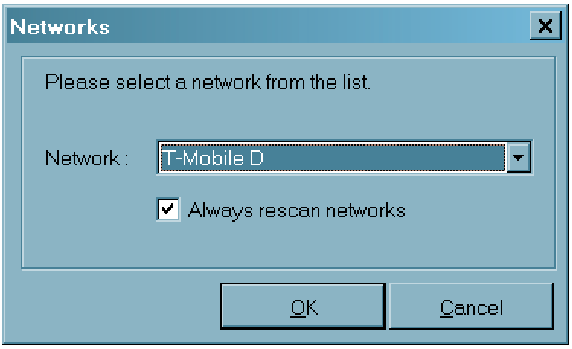
This menu item is displayed after a multifunction card has been installed (see the Appendix in this manual). In addition the field with the display for UMTS / GPRS will be displayed in the Monitor and the WLAN panel will be hidden (see “Monitor icons” above).

### ■ Network Search

After the monitor starts, the installed multifunction card automatically searches for a wireless network and displays it with the appropriate field strength as soon as it is found (T-Online in the Fig. below). Another network search can be triggered by selecting the menu item or by clicking on the button for “Network Search”.



If the field strength is insufficient, the card will automatically switch over from UMTS as data transmission technology to GPRS, and the connection will remain intact. When the field strength increases, the card will automatically switch back.


Networks

Please select a network from the list.

Network : T-Mobile D

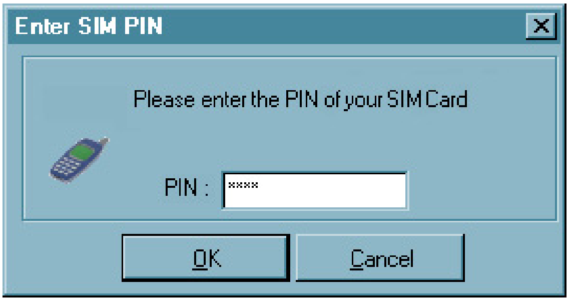
☑ Always rescan networks

If a network search was executed, the window for network selection will be displayed (left). The desired network can be selected from a list. If you do not desire another network search each time the Monitor is called, is then this function, which is active by default, must be switched off via the Check button.

## Activate GPRS / UMTS

The data transmission technology can also be changed manually. To do this click on the text with the desired transmission technology, or select this menu item. When changing the medium manually the connection will first be disconnected. The connection will then be re-established automatically, if “Automatic Connection Set Up” has been installed in the Phonebook.

## Enter SIM PIN


Enter SIM PIN

Please enter the PIN of your SIM Card

PIN : ****

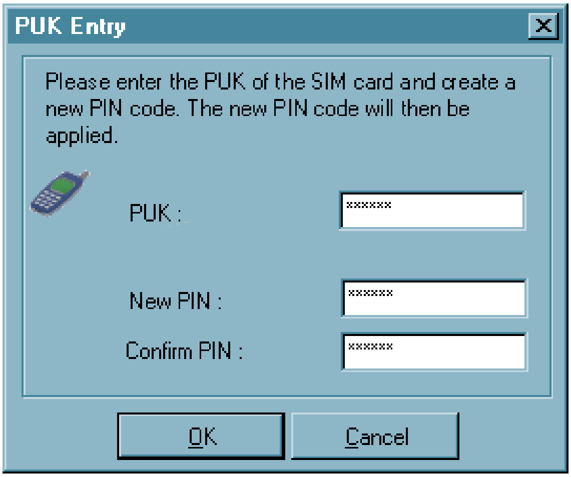
The dialog for entering the SIM PIN is automatically displayed for a connection setup.

Use this menu item to also enter the SIM PIN even before a connection setup.

## Change SIM PIN

You can only change the SIM PIN if the previous SIM PIN has been entered correctly.

### PUK Entry



PUK Entry

Please enter the PUK of the SIM card and create a new PIN code. The new PIN code will then be applied.

PUK : ******

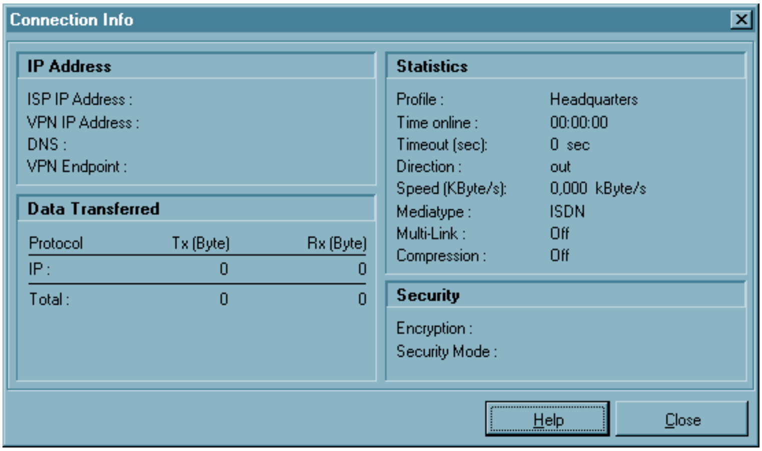
New PIN : ******

Confirm PIN : ******

After three incorrect attempts to enter the SIM PIN the window for entering the PUK (Personal Unblocking Key), which accompanies the SIM card, will be displayed. After correctly entering the PUK you will be able to enter a new SIM PIN.

## 4.1.5 Connection Info

Upon selecting the menu parameter “Connection Info” link statistics are displayed. The window also displays the type of security features being used as well as the IP addresses that have been assigned between the IPSec client and the destination resulting from the PPP negotiation. The information in the connection info window is “read-only” and has no influence on the functionality of the IPSec client.



Connection Info

IP Address

ISP IP Address :
VPN IP Address :
DNS :
VPN Endpoint :

Data Transferred

| Protocol | Tx (Byte) | Rx (Byte) |
|---|---|---|
| IP : | 0 | 0 |
| Total : | 0 | 0 |

Statistics

| | |
|---|---|
| Profile : | Headquarters |
| Time online : | 00:00:00 |
| Timeout (sec): | 0 sec |
| Direction : | out |
| Speed (KByte/s): | 0,000 kByte/s |
| Mediatype : | ISDN |
| Multi-Link : | Off |
| Compression : | Off |

Security

Encryption :
Security Mode :

The field “Connection Info” could be suppressed by the administrator. In this case the menu item could not be activated.

If the connection info is faded, the most important information concerning data transfere, statistic and security can be seen in the statistic field of the monitor (see → Window, Show Statistics).

## Time Online

Time Online indicates the total amount of time that the PC is actually connected to the destination, regardless of any timeouts (disconnects). The value is reset to zero (0) either as a result of (re)booting your PC or when you change the destination.

## Timeout

The Client Monitor displays the time remaining until the next timeout (disconnect) occurs, which begins immediately following the last exchange of data over the Link (including any handshaking). (See → Phonebook, Line Management).

## Direction

Direction indicates the current direction of communications as follows:
Out = outbound or outgoing call is currently being executed.
In = inbound or incoming call is currently taking place.

## Speed

The displayed number varies according to the current data throughput.

## Multilink

If a connection is established via several ISDN-B channels, the statistic showes “on”.

## Media Type

The following Media Types are supported: ISDN, Modem, LAN over IP, xDSL (PPPoE), xDSL (AVM - PPP over Capi), GPRS and PPTP.

## Compression

Compression is always defined by the gateway. IPSec compression is displayed with “IPSec Compression (LZS)”.

## Encryption

The used encryption type is diasplayed. Following types of encryption are supported: AES, Blowfish, 3DES. The encryption type is assigned by the central site (gateway).

### Key exchange

Display what Session Key exchange method is used:

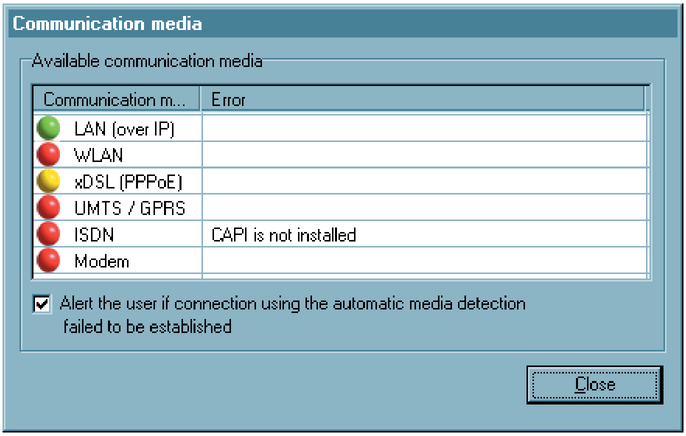
Static Key = The same Static Key must be used at both endpoints of communication. It is entered under “Profile Settings → Identity”

IKE (IPSec) = To transfer the Session Key, the encrypted Control Channel of Phase 1 negociation is used.

### Rx and Tx Bytes

Rx and Tx Bytes indicates the amount of data being sent (out) and received (in) for each protocol and for each communications session. The amount of data is expressed in Bytes (1 byte = 1 character). The total amount of data sent and received for all protocols is also displayed.

## 4.1.6 Available Communication Media



| Communication m... | Error |
|---|---|
| 🟢 LAN (over IP) | |
| 🔴 WLAN | |
| 🟡 xDSL (PPPoE) | |
| 🔴 UMTS / GPRS | |
| 🔴 ISDN | CAPI is not installed |
| 🔴 Modem | |

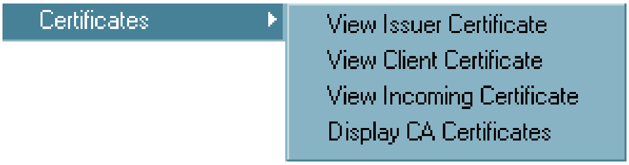
☑ Alert the user if connection using the automatic media detection failed to be established

The purpose of this window is only to inform about the available communication media and the currently used communication medium. On the basis of a pre-configured destination system, those link types that are currently available for the Client PC are detected and implemented, and if multiple alternative transmission paths are available, the fastest will be selected automatically.

The available communication media are displayed with yellow signal lamps and the automatically selected with a green signal lamp.

For configuration purposes note the description of “Automatic Media Detection” in the parameterfolder “Destination System” of the phonebook.

## 4.1.7 Certificates



In the pulldown menu “Connection” you will find the entry “Certificates” which consists of the following submenus “Configuration”, “View Issuer Certificate”, “View Client Certificate”, “View Incoming Certificate” and “Display CA Certificate”.

Certificates are normally created by a CA (Certification Authority) utilizing some sort of PKI-based architecture and they may be implemented on a Smart Card in addition to a digital signature(s). Such Smart Cards represent an individual “personal identity card”.

### ■ View Issuer Certificate

In order to view the Issuer Certificate select “Connection → Certificate → View Issuer Certificate”. Upon doing so the individual assigned data will be displayed (read-only) for your review purposes.

Certificate Authority (CA) = The CA and the issuer of a Issuer Certificate are normally identical (self-signed certificate). The CA of the Issuer Certificate has to be identical with the CA of the Client Certificate (see → View Client Certificate).

Serial Number = The serial number of the certificate can be compared with the registered serial number in the Revocation List of the Certification Authority.

Validity = The validity of certificates is limited. Normally the validity of a Issuer Certificate is longer than the validity of a Client Certificate. Upon expiration of the Issuer Certificate, the validity of the Client Certificate of the same CA expires as well.

Fingerprint = Hash value. The Hash value is the signature of the certificate. The Hash value is encrypted with the private key of the CA.

## View Client Certificate

In order to view the Client Certificate select “Connection → Certificate → View Client Certificate”. Upon doing so the individual assigned data will be displayed (read-only) for your review purposes.

Certification Authority (CA) = The CA and the issuer of a Client Certificate is normally identical (self-signed certificate). The CA of the Client Certificate has to be identical with the CA of the Issuer Certificate (see → Issuer Client Certificate).

Serial Number = The serial number of the certificates can be compared with the registered numbers in the Revocation List of the Certification Authority. (see → strong Radius Authentication)

Validity = The validity of certificates is limited. Normally the validity of a Issuer Certificate is longer than the validity of a Client Certificate. The expiration of validity erases the functionality of certificates.

Fingerprint = Hash value. The Hash value is the signature of the certificate. The Hash value is encrypted with the private key of the CA.

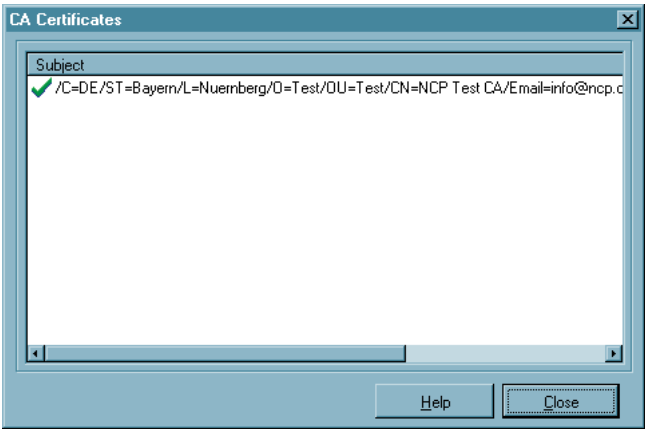
## View incoming Certificate

Display of the certificate that is communicated in the SSL negotiation from the other side (Secure Server). You can see, for example, whether you have accepted the issuer displayed here in the list of your CA certificates (see below).

If the incoming user certificate is one of the CAs not known from the list “Display CA Certificates”, then the connection will not take place.

If no certificates are stored in the installation directory under CACERTS\, then no verification takes place.

## Display CA Certificates



| Subject |
|---|
| ✓ /C=DE/ST=Bayern/L=Nuernberg/O=Test/OU=Test/CN=NCP Test CA/Email=info@ncp.c |

Multiple issuer certificates are supported with the client software (multiple CA support). The issuer certificates must be collected in the installation directory under CACERTS\ for this. In the client monitor the list of CA certificates read in is displayed under the menu item “Connection → Certificates → Display CA Certificates”,

If the issuer certificate of another side is received, then the client determines the issuer, then searches for the issuer certificate, first on Smart Card or in the PKCS#12 file, and then in the CACERTS\ directory.

If the issuer certificate is not known, then the connection will not be established (No Root Certificate found). If no CA certificates are present in the installation directory under CACERTS\, then a connection that implements certificates is not permitted.

## Display and analysis of extensions for incoming certificates and CA certificates

Certificates can contain extensions. These serve for the linking of additional attributes with users or public keys, that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written in the certificate by the issuing certification authority.

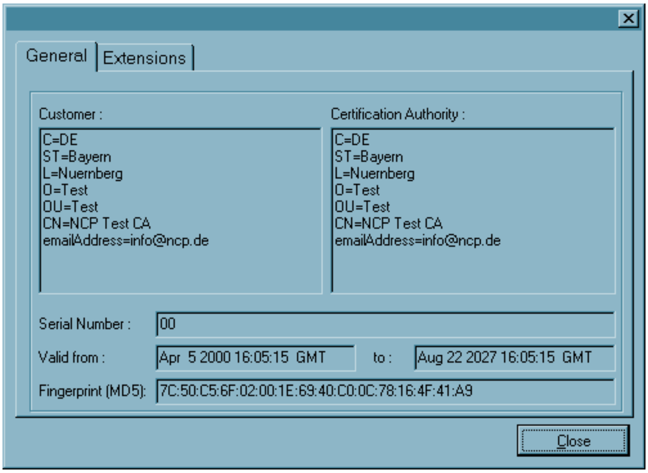
Three extensions are significant for the IPSec client and the gateway:

☑ extendedKeyUsage

☑ subjectKeyIdentifier

☑ authorityKeyIdentifier

### *Display of extensions*



Customer :

C=DE
ST=Bayern
L=Nuernberg
O=Test
OU=Test
CN=NCP Test CA
emailAddress=info@ncp.de

Certification Authority :

C=DE
ST=Bayern
L=Nuernberg
O=Test
OU=Test
CN=NCP Test CA
emailAddress=info@ncp.de

Serial Number : 00

Valid from : Apr 5 2000 16:05:15 GMT to : Aug 22 2027 16:05:15 GMT

Fingerprint (MD5): 7C:50:C5:6F:02:00:1E:69:40:C0:0C:78:16:4F:41:A9

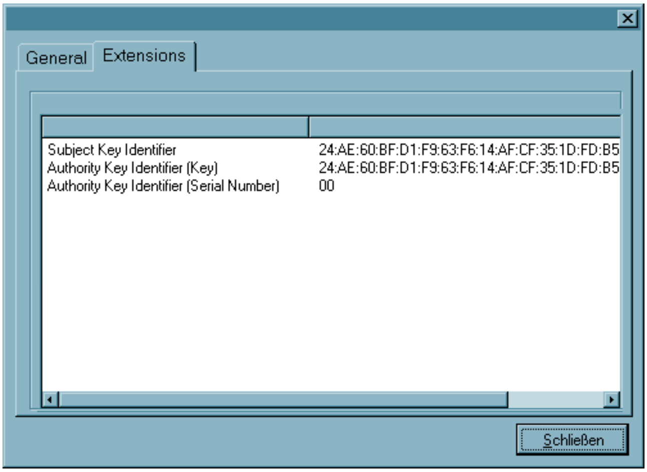
To display the extensions of an incoming or CA certificate you have to proceed as follows:

The Ca certificate which extension should be displayed, has to be opened by a doubble click in the window of Ca certificates. Upon doing so the  next window with general information is opened.

For the incoming certificate this window is already opened  after “View incoming certificate” was selected in the certificate menu.

The window “General” displays the general certificate data

The window “Extensions” displays the certificate extensions if available.



| | |
|---|---|
| Subject Key Identifier | 24:AE:60:BF:D1:F9:63:F6:14:AF:CF:35:1D:FD:B5 |
| Authority Key Identifier (Key) | 24:AE:60:BF:D1:F9:63:F6:14:AF:CF:35:1D:FD:B5 |
| Authority Key Identifier (Serial Number) | 00 |

### *Extension checks*

**KeyUsage**

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted:
– Digital Signature
– Key Encipherment (key transport, key management)
– Key Agreement (key exchange process)
If one of the bits is not set, then the connection is interrupted.

**extendedKeyUsage**

If the extendedKeyUsage extension is present in an incoming user certificate, then the Secure Client checks whether the defined extended application intent is “SSL Server Authentication”. If the incoming certificate is not intended for server authentication the connection will be refused. If this extension is not present in the certificate, it will be ignored.

Please note that the SSL server authentication is direction-dependent. This means that the initiator of the tunnel establishment checks the incoming certificate of the other side, which, if the extendedKeyUsage extension is present, must contain the intended purpose “SSL Server Authentication”. This applies also for a callback to the Client via VPN.

Exception: For a server call-back to the client after a direct dial-up, without VPN but with PKI, the server checks the client certificate for the extendedKeyUsage extension. If this is present, then the intended purpose “SSL Server Authentication” must be contained otherwise the connection will be rejected. If this extension is not present in the certificate it will be ignored.

**subjectKeyIdentifier / authorityKeyIdentifier**

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer’s public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA certificate is found then the connection is rejected.

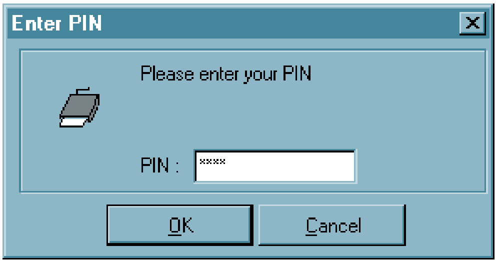
**CDP (Certificate Distribution Point)**

The URL for downloading an CRL is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is setup, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid the connection is disconnected. During this process the CRL is stored in the CRLS\ directory, under the common name of the CA.

## 4.1.8 Enter PIN

The PIN entry can be executed before establishing a connection, after the monitor has been started. If a connection requiring a certificate is established at a later time, then the PIN entry can be omitted – unless the configuration for the certificate requests it (see → Configuration, Certificates).

If you have configured the IPSec client for the use of a Smart Card or of a PKCS#11 module (see →Configuration, Certificates), then a light blue symbol for the Smart Card appears in the status field. If you have inserted your Smart Card in the card reader, the symbol color changes from light blue to green.


Enter PIN

Please enter your PIN

PIN : ****

If the PIN has not been entered before a connection establishment, then the PIN entry dialog appears when the first connection requiring the use of a certificate is to be established to a destination at the latest. Thereafter the PIN entry can be comitted in the case of repeated manual connection establishment, if this has been configured (see →Configuration, Certificates).

Using a soft certificate the PINcan have of 4 digits. Using a Smart Card it must have at least 6 digits.

Incorrect entries and incorrect PINs are acknowledged with the error message “Incorrect PIN!” after approximatly 3 seconds. At this point a connection establishment is not possible. Please note that a Smart Card or a token can be blocked after multiple incorrect PIN entries. In this case, please contact your remote administrator. An established connection will, by default, be disconnected if the Smart Card or token is removed during the operation.

The connection establishment can only be executed after correct PIN entry.

### *Safeguarding PIN Use*

If you activate the function, “PIN request at each connection”, in the certificate configuration, then the PIN can no longer be entered via the “Enter PIN” Monitor menu option. The menu option “Enter PIN” is thus switched to inactive automatically. This ensures that the PIN will only be queried and can only be entered directly before the connection is set-up.

Activate this function to prevent an unauthorized user from setting up an undesired connection if the PIN has already been entered.

Likewise, if the “Change PIN” function has been switched active, then the PIN that has already been requested in other function contexts is no longer used – i.e. when setting up a connection, or in the “Enter PIN” connection menu. Instead you can always select the menu option “Change PIN” and the new PIN will be automatically reset immediately after the change.

☞ This ensures that when configuring “PIN query at every connection set-up” on an unauthorized Client Monitor, a PIN entered previously by an unauthorized user cannot be used at anytime to set-up a connection.

## 4.1.9 Reset PIN

This menu item can be selected for deleting the PIN, for making the valid PIN useless to other users. It can be helpful for example if you leave your client temporary or if the user changes. Afterwards a valid PIN must be reentered again for authentication.

- **PIN State Symbol Visible in the Client Monitor.**

If a valid PIN is entered this is symbolized by a green check next to the PIN display in the client monitor. If the PIN has not yet been entered correctly the green check will not appear.

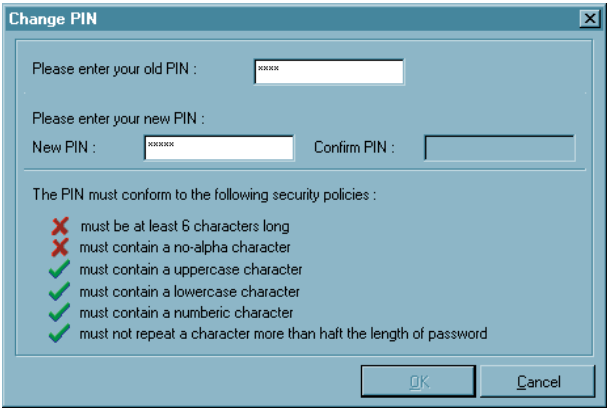
- **PIN Handling after Logoff or Sleep Mode**

When a user logs off Windows NT/2000/XP the PIN cache is cleared and must be reentered at next logon. When the machine enters sleep mode the PIN cache is also cleared.

- **Displaying ACE Server Messages for RSA-Token**

If messages are sent by the ACE server because of the RSA token they will be displayed on the monitor in an input field (for example “Expiration of valid PIN”).

## 4.1.10 Change PIN



Please enter your old PIN : ****

Please enter your new PIN :

New PIN : ***** Confirm PIN :

The PIN must conform to the following security policies :

- ✗ must be at least 6 characters long
- ✗ must contain a no-alpha character
- ✓ must contain a uppercase character
- ✓ must contain a lowercase character
- ✓ must contain a numberic character
- ✓ must not repeat a character more than haft the length of password

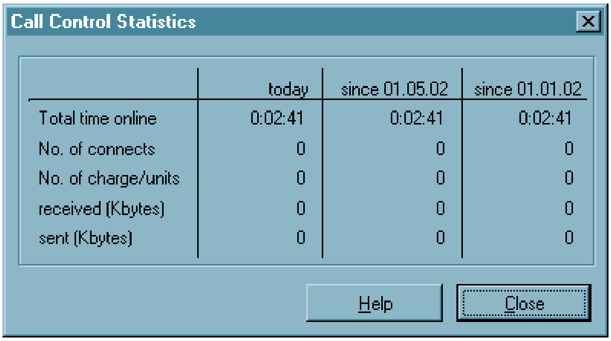
The PIN for a Smart Card or for a soft certificate can be changed under the menu item “Change PIN”, if the correct PIN number has previously been entered. This menu item will not be activated without the previous entry of a valid PIN number.

For security reasons, after opening this dialog the still valid PIN must be entered a second time. This is to insure PIN change for the authorized user only. The digits of the PIN are displayed in this entry field, and in the next entry fields as asterisks “*”.

Then enter your new PIN and confirm it by repeating it in the last entry field. With a click on “OK” you have changed your PIN. PIN policies that need to be complied with are displayed under the entry field. They can be set in the main menu under “Certificate →PIN Policies”.

By entering a new PIN the red X will change to a green check as soon as the guidelines are fulfilled. (see illustration above)

### 4.1.11 Call Control Statistics



Call Control Statistics

|  | today | since 01.05.02 | since 01.01.02 |
|---|---|---|---|
| Total time online | 0:02:41 | 0:02:41 | 0:02:41 |
| No. of connects | 0 | 0 | 0 |
| No. of charge/units | 0 | 0 | 0 |
| received (Kbytes) | 0 | 0 | 0 |
| sent (Kbytes) | 0 | 0 | 0 |

Call Control Statistics provide you with an overview of your communications on a daily, monthly and yearly basis. It accurately displays the following information:

- total time online
- total number of connects (outgoing calls)
- total number of charge/units (if available)
- total amount of data (expressed in Bytes) sent and received

### 4.1.12 Call Control Reset

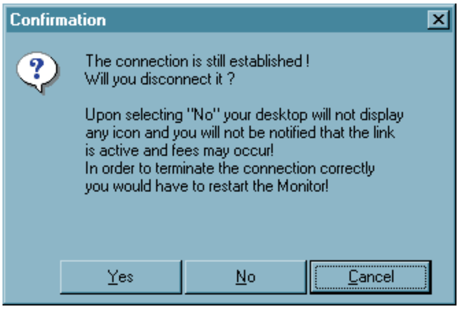
If the “Limits” defined in the Call Control Manager have been exceeded, the IPSec client issues a “Warning Message” and blocks any further communications until such time that the “Call Control Reset” has been activated (see → “Connection” pull-down menu in the Monitor).

A connection can only be established after clicking “Call Control Reset”.

### 4.1.13 Exit (Disconnect the Monitor)

Have you already disconnected the link, a click on this menu item or on the “Disconnect” button closes the monitor.

If the connection is still established, with a click on this menu item or on the “Disconnect” button the monitor can be closed as well. Please note that closing the Monitor does not automatically terminate the connection. If the link should be established although the monitor is closed and fees may occur, the software asks you explicitly for a prompt.

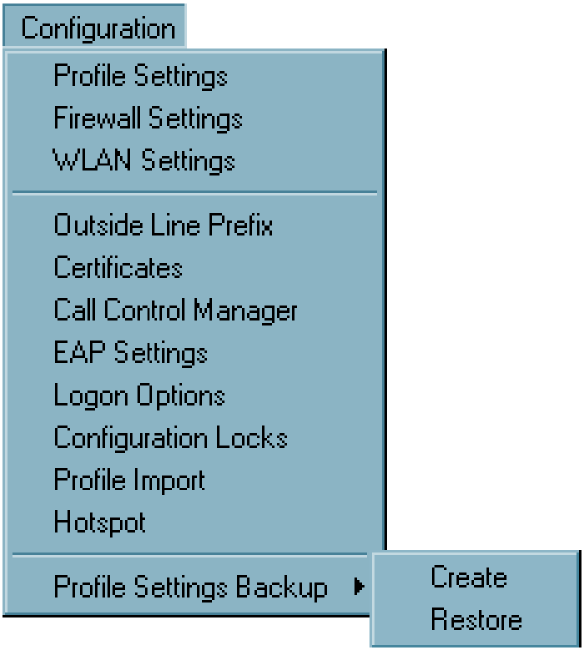


The connection is still established !
Will you disconnect it ?

Upon selecting "No" your desktop will not display any icon and you will not be notified that the link is active and fees may occur!
In order to terminate the connection correctly you would have to restart the Monitor!

Upon selecting “No” your desktop will not display any icon and you will not be notified that the link is active and fees may occur! In order to terminate the connection correctly you would have to restart the Monitor!

## 4.2 Configuration



You can specify all settings for work with the IPSec Client, which should work longer than one session, with this menu choice. Specifically this means creating profiles, configuration for IPSec links, choosing communication media, as well as obtaining an outside line for connections to telecommunications systems.

In addition you can individually configure precisely how certificates should be used, how the call control manager should work and which configuration rights the user receives.

In order to guarantee the proper functionality of your IPSec client Funkwerk Enterprise Communications offers a public VPN test access. A detailed step-by-step guidance how to use this test access and how to set the needed configurations correctly can be found on the websites at www.funkwerk-ec.com.

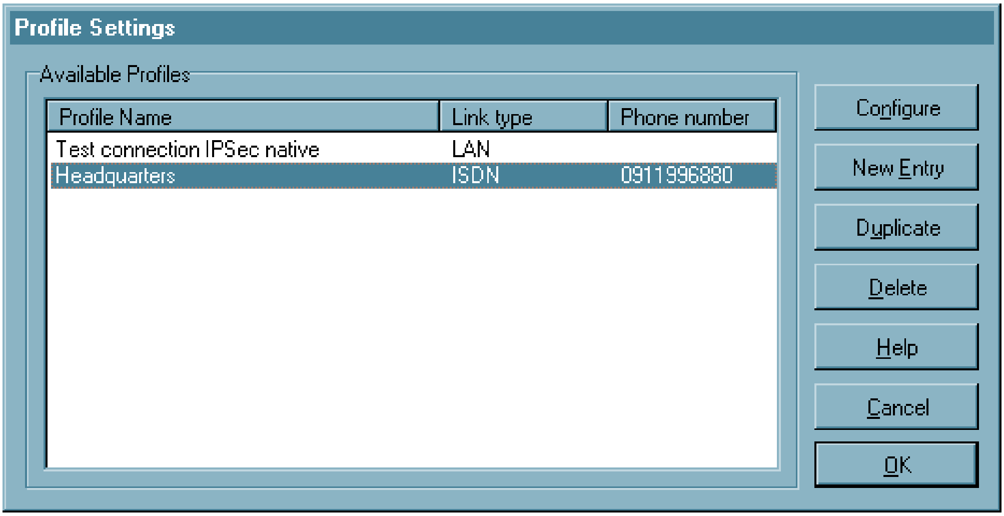
## 4.2.1 Profile Settings

### ■ Entries in the profile settings

After installing the Secure Client for the first time it will be necessary to define a profile for your requirements in the profile settings. For this purpose there is a “Configuration Assistant”, which will walk you through the configuration steps of a profile. In this way the first profile will be created.

The profile settings provide the basis for defining and configuring destinations (profiles) which can be modified or reconfigured at any time according to requirements.

Upon clicking “Profile Settings” in the Monitor menu “Configuration” the menu is opened and displays an overview of the defined profiles and their respective names and the telephone numbers of the according destinations.



Profile Settings

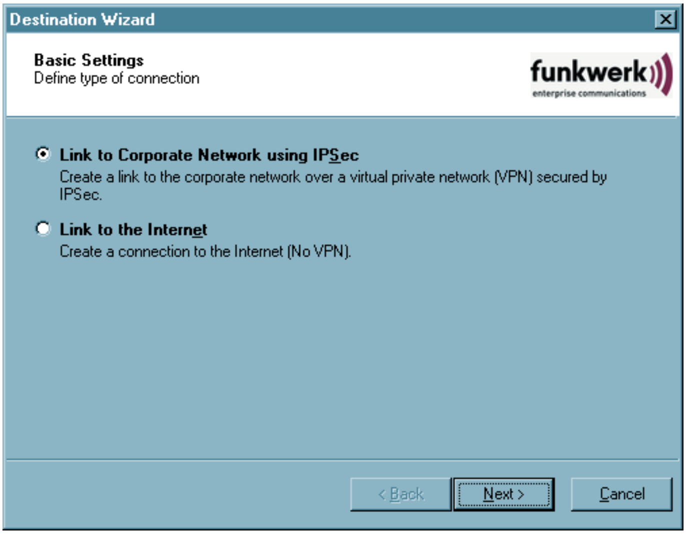
Available Profiles

| Profile Name | Link type | Phone number |
|---|---|---|
| Test connection IPSec native | LAN | |
| Headquarters | ISDN | 0911996880 |

*There is also a toolbar with the following function buttons: Configure, New Entry, Duplicate, Delete, OK, Help and Cancel.*

### ■ New Entry – Profile

In order to define a new Destination, click on “Profile Settings”. When the window opens click on “New Entry”. Upon doing so the “Configuration Assistant” opens and walks you through the configuration of a new Profile according to your requirements. Upon entering all items in the assistant the new profile is entered in the Profile Settings based on these parameters. All other parameters are assigned a default value.



Basic Settings
Define type of connection

● Link to Corporate Network using IPSec
Create a link to the corporate network over a virtual private network (VPN) secured by IPSec.

○ Link to the Internet
Create a connection to the Internet (No VPN).

*Using the configuration assistant, connections can be quickly established with the Internet or to the corporate network. The profile is created after a few configuration questions, in accordance with the selection of the desired basic setting.*

Below are the required data for the configuration:

**Link to Corporate Network using IPSec:**

→ Profile Name
→ Link Type
→ Access data for Internet Service Provider (User ID, Password, Phone Number)
→ VPN-Gateway selection (Tunnel Endpoint IP address)
→ Access data for VPN Gateway (XAUTH, User ID, Password)
→ IPSec Configuration (Exch. Mode, PFS Group, Compression)
→ Static key (Preshared Key), without certificate (IKE ID Type, IKE ID)
→ IP Address Assignment (IP address of the client, DNS/WINS Server)
→ Firewall Settings

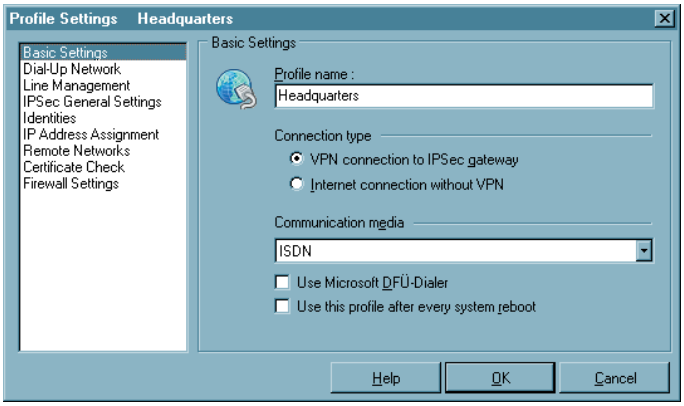
**Link to the Internet:**

→ Profile Name
→ Link Type
→ Access data for Internet Service Providers (User ID, Password, Phone Number)

The new profile is displayed now in a list of profiles with its assigned name. If no further parameter settings are necessary you can close the profile settings by clicking on “Ok”. The new profile is immediately available in the monitor. It can be selected in the monitor and via the menu “Connection → Connect” a connection to the relating destination can be established.

## Configure – Profile

If you want to change any default profile data and parameters, start by selecting the appropriate profile and then click on the “Configure” button. Upon doing so a folder opens and displays a list of the following parameter folders on the left side:



Profile Settings    Headquarters

- Basic Settings
- Dial-Up Network
- Line Management
- IPSec General Settings
- Identities
- IP Address Assignment
- Remote Networks
- Certificate Check
- Firewall Settings

Basic Settings

Profile name : Headquarters

Connection type

● VPN connection to IPSec gateway

○ Internet connection without VPN

Communication media: ISDN

□ Use Microsoft DFÜ-Dialer

□ Use this profile after every system reboot

*Basic Settings*
*Dial-Up Network*
*Modem*
*Line Management*
*IPSec General Settings*
*Identity*
*IP Address Assignment*
*Remote Networks*
*Certificate Check*
*Firewall Settings*

Upon selecting one of the folders the associated parameters will be displayed (see → 5. Configuration Parameters).

## Ok – Profile

Upon clicking “OK” in the configuration window the configuration of a profile is concluded. The new or modified profile is available in the monitor. It can be selected in the monitor and via the menu “Connection → Connect” a connection to the relating destination can be established.

## Duplicate – Profil

You may want to use an existing profile for the basis of a new profile, perhaps however with slight modifications. In order to do so first select the profile to be duplicated and then click on the “Duplicate” button. Upon doing so the “Basic Settings” parameter folder will open. You must now enter a new name for the profile and then click on “OK”. A new profile is now created with parameters identical to the profile that was duplicated except for the Proflie Name.

Important: It is not possible to have 2 or more profiles with identical names. Each profile must be assigned its own unique name.

## Delete – Profile

If you want to delete a profile select the appropriate profile and then click on the “Delete” button.

### 4.2.2 Firewall Settings

All firewall mechanisms are optimized for Remote Access applications and are activated when the computer is started. This means that in contrast to VPN solutions with autonomous firewall, the teleworkstation is already protected against attacks before actual VPN utilization.

The Personal Firewall also offers complete protection of the end device, even if the client software is deactivated. All firewall rules can be centrally specified by the administrator, and compliance with these rules can be forced. The prerequisite in this case is the central NCP Secure Enterprise Management system, which is used to configure the Client, which can be permanently specified as unchangeable for the user.

**Please note that the firewall settings are globally valid, i.e. they apply for all destination systems in the telephone book.**

On the other hand the Link Firewall Setting that is made in the telephone book can only be effective for the associated telephone book entry (destination system) and the connection to this destination system.

### Firewall properties

The firewall works in accordance with the principle of packet filtering, in conjunction with Stateful Packet Inspection (SPI). The firewall checks all incoming and outgoing data packets and decides whether a packet will be forwarded or rejected on the basis of the configured rules.

Security is ensured in two ways. First unauthorized access to data and resources in the central data network is prevented. Secondly the respective status of existing connections is monitored via Stateful Inspection. Moreover the firewall can detect whether a connection has opened “Spawned connections” – as is the case with FTP or Netmeeting for example – whose packets likewise must be forwarded. If a rule is defined for an outgoing connection, which permits an access, then the rule automatically applies for the corresponding return packets. For the communication partner a Stateful Inspection connection is represented as a direct line, which can only be used for an exchange of data that corresponds to the agreed rules.

The firewall rules can be configured dynamically, i.e. it is not necessary to stop the software or restart the system.

The firewall settings in the configuration menu of the Client Monitor permit a more precise specification of firewall filtering rules. They have a global effect. This means that regardless of the currently selected destination system, the rules of the extended firewall settings are always worked through first, before the firewall rules from the telephone book are applied.

A combination of the global and link based firewall can be quite effective in certain scenarios. However generally, the global setting possibilities should be able to cover virtually all requirements.

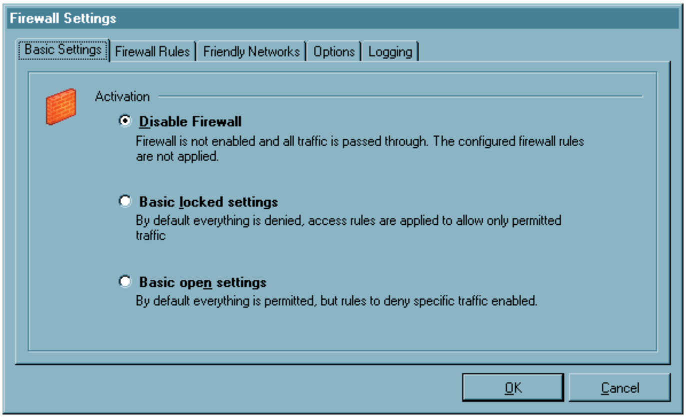
Please note that the link-based firewall settings take priority over the global firewall settings at activation. For instance if the Link Firewall is set to “Always” and “Only allow communication in the tunnel”, then in spite of global configuration rules that may possibly be different, only one tunnel can be set-up for communication. All other traffic will be rejected by the Link Firewall.

### Configuration of the firewall settings

The filter rules of the firewall can be defined application-based as well as (additionally) address-oriented, relative to friendly/unknown networks.

To avoid any conflict between the rules of the Link Firewall in the phonebook and the global firewall, we recommend to switch off the Link Firewall when using the advanced global firewall. The IP addresses of the respective links (to the VPN gateway) can be inserted in the filter rules of the global firewall.

## Configurationfield Basic Settings



● Disable Firewall
Firewall is not enabled and all traffic is passed through. The configured firewall rules are not applied.

○ Basic locked settings
By default everything is denied, access rules are applied to allow only permitted traffic

○ Basic open settings
By default everything is permitted, but rules to deny specific traffic enabled.

*In the basic settings you decide how the extended firewall settings will be used.*

### *Disable Firewall*

If the extended firewall is deactivated, then only the firewall configured in the telephone book will be used. This means that all data packets will only be worked through via the security mechanisms of this connection-oriented firewall, if they have been configured.

### *Basic locked settings (recommended)*

If this setting is selected, then the security mechanisms of the firewall are always active. This means that without additionally configured rules all IP data traffic will be suppressed. The exception are the data packets that are permitted (permitted through) by the separately created active firewall rules (Permit Filter). If a characteristic of a data packet meets the definition of a firewall rule, then at this point the work through of the filter rules is ended and the IP packet is forwarded.

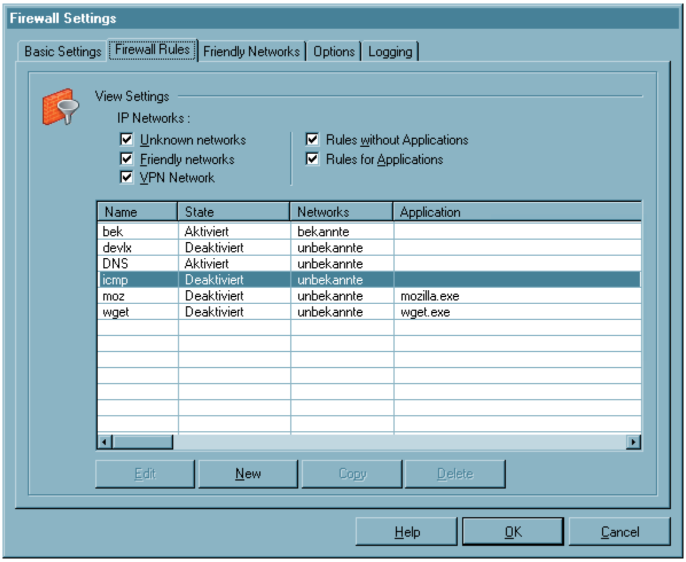
In the blocked basic setting mode in a convenient manner an L2Sec/IPSec tunnel connection is released. For this, the data traffic can be globally permitted in the configuration field “Options”, via VPN protocols (L2Sec, IPSec).

### *Basic open settings*

In the open base setting all IP packets are first permitted. Without additional filter rules all IP packets are forwarded.

The exception are the data packets that are filtered out (not permitted through) by the separately created active firewall rules (Deny Filter). If one of the characteristics of an IP packet coming into the server/client meets the definition of a Deny Filter, then at this point the working through of filtering rules ends, and the IP packet will not be forwarded. Data packets that do not meet a suitable Deny Filter are forwarded.

## Configurationfield Firewall Rules



View Settings

IP Networks :

☑ Unknown networks
☑ Friendly networks
☑ VPN Network

☑ Rules without Applications
☑ Rules for Applications

| Name | State | Networks | Application |
|---|---|---|---|
| bek | Aktiviert | bekannte | |
| devlx | Deaktiviert | unbekannte | |
| DNS | Aktiviert | unbekannte | |
| icmp | Deaktiviert | unbekannte | |
| moz | Deaktiviert | unbekannte | mozilla.exe |
| wget | Deaktiviert | unbekannte | wget.exe |

*The rules for the extended firewall are brought together in this configuration field. The display options are all active by default and correspond to the selected networks, for which the respective rule can be defined, and whether this rule will be valid regardless of application:*

– Unknown networks
– Friendly networks
– VPN networks
– Rules with applications
– without applications

*These selection fields for the displays of rules are only for overview purposes and have no effect on the application of a filter rule. The most important characteristics are displayed for each defined rule:*

– Name
– State
– Networks
– Application

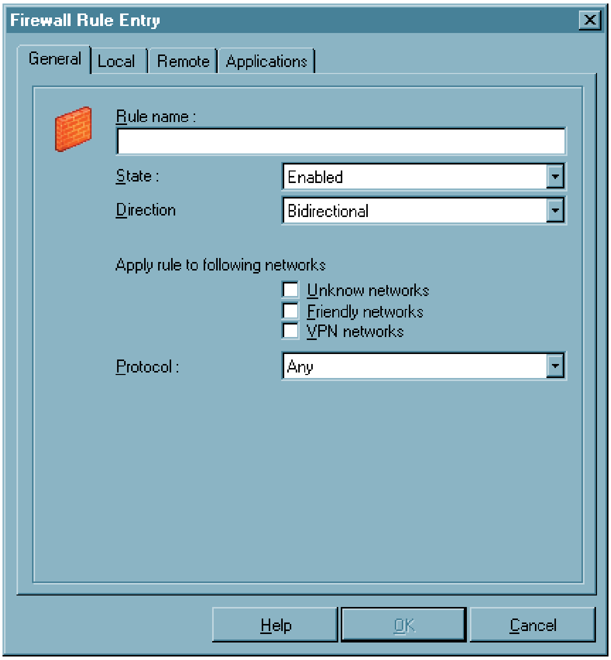
Clicking on these characteristic buttons sorts the displayed rules.

### *Creating a firewall rule*

Use the buttons underneath the display line to generate or edit the rules. To create a firewall rule click on “New”. A filter rule is created via four configuration areas or tabs:

– General: In this configuration field you specify the network and the protocol for which the rule will apply.
– Local: Enter the values of the local ports and IP addresses in this configuration field.
– Remote: Enter the port and address values of the other side in the remote field.
– Applications: In this configuration field the rule can be assigned to one or more applications.

## Firewall rule / General


Firewall Rule Entry

General | Local | Remote | Applications

Rule name :

State : Enabled

Direction Bidirectional

Apply rule to following networks

□ Unknow networks
□ Friendly networks
□ VPN networks

Protocol : Any

*The created rule is always executed as an exception to the basic setting (see -> Basic Settings).*

### Rule name

The rule appears under this name in the display list.

### State

The rule will only be applied to data packets, if the status is “active”.

### Direction

With the direction you specify whether this rule will apply for incoming or outgoing data packets. According to the Stateful Inspection principle, data packets are received that come in from a destination, to which data packets may be sent and vice versa. However Stateful Inspection is only used for TCP/IP protocols (UDP, TCP).

You can switch to “incoming” for instance if a connection will be set-up from the remote side (e.g. for “incoming calls” or administrator accesses).

The “bi-directional” setting is only practical if Stateful Inspection is not available, e.g. for the ICMP protocol (for a ping).

### Apply rule to following networks

When creating a rule, at first do not assign it to any network. A rule can only be saved if the desired allocation has been made and if a name has been assigned.
*Unknown networks*
– are all networks (IP network interfaces), that can neither be allocated to a known nor VPN. These include for example connections via the Microsoft remote data transmission network or also direct or unencrypted connections with the integrated dialer of the client, as well as Hotspot WLAN connections. If a rule will apply for unknown networks then this option must be activated.

*Known networks*
– are defined in the tab of the same name in the “Firewall settings” window. If a rule will apply for known networks then this option must be activated.
*VPN networks*
– are all L2Sec or IPSec connections in the set-up condition. Moreover under this group there are also all encrypted direct dial-in connections via the client’s integrated dialer. If a rule will apply for VPN networks then this option must be activated.

**Protocol**

Select the appropriate protocol depending on the application:

TCP, UDP, ICMP, GRE, ESP, AH, IGRP, RSVP, IPv6 or IPv4, all

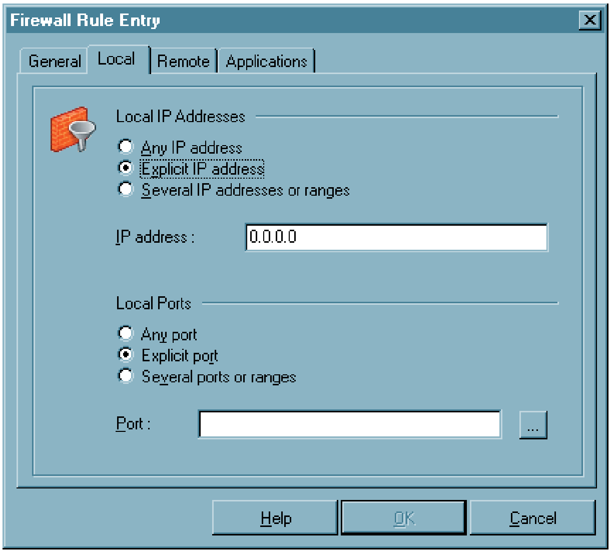
**Line management**

Use this parameter to influence the type of connection.

For example, you select the option that the rule configured here “is only valid at inactive VPN connection”, if you an Internet connection with concurrently present VPN connection to be excluded, otherwise the Internet connections to unknown networks should be allowed. For this, this rule for “unknown networks” must be used, i.e. this rule must permit access to unknown networks.

The option, “no automatic connect” is only practical if in the telephone book the connection set-up has been set to “automatic” in the “Line Management” parameter field. For the data packets defined via this rule, automatic connection set-up does not take place when activating this function, it does for other data packets.

## Firewall rule / Local



Firewall Rule Entry

General | Local | Remote | Applications

Local IP Addresses

○ Any IP address
● Explicit IP address
○ Several IP addresses or ranges

IP address : 0.0.0.0

Local Ports

○ Any port
● Explicit port
○ Several ports or ranges

Port :

*On this tab the filter are set for the local IP addresses and IP ports.*

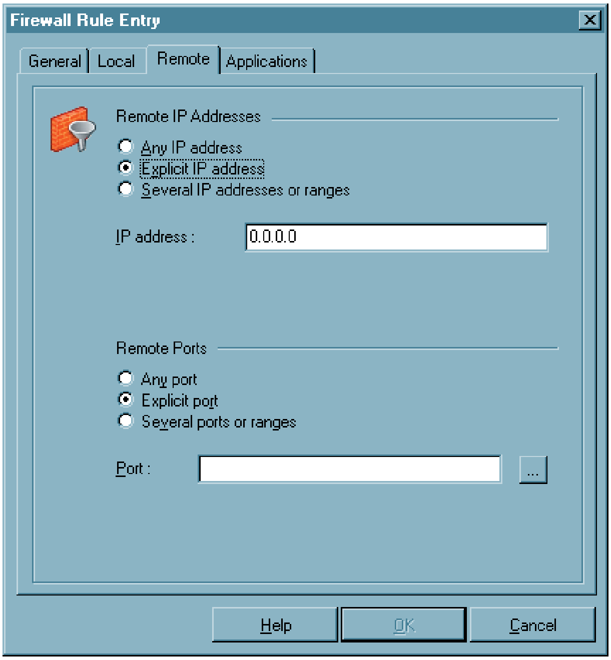
If the basic setting is blocked then those data packets will be let through to the outside by the firewall whose source address agrees with the address under “Local IP address” or is within the range of validity. Of the incoming data packets those are let through whose destination address agrees with the address under “Local IP addresses” or is within the validity area.

The same is true for blocked basic setting with the IP ports. Those data packets are permitted outside by the firewall whose source port falls under the definition of the local port. Of the incoming data packets those are let through whose destination port falls under the definition of the local port.

*All IP addresses*
– includes all source IP addresses of outgoing packets or destination IP addresses of incoming packets, regardless of the local network adapter.
*Unique IP address*
– is the IP address defined for the local network adapter. It can be assigned to the address of the Ethernet card, the WLAN card, or it can also be assigned to the VPN adapter.
*Multiple IP addresses*
– designates an address range or pool. For example this can be the IP address pool, from which the address assigned by the DHCP server to the client originates.

*All ports*
– allows communication via all source ports for outgoing packets and destination ports for incoming ports.
*Unique port*
– This setting should only be used if this system makes a server service available (e.g. remote desktop on port 3389).
*Multiple ports*
– This setting should only be used if the local ports can be combined in a range, that is required by a services that will be made available on this system (e.g. FTP ports 20/21).

## Firewall rule / Remote



Remote IP Addresses

○ Any IP address
● Explicit IP address
○ Several IP addresses or ranges

IP address : 0.0.0.0

Remote Ports

○ Any port
● Explicit port
○ Several ports or ranges

Port :

*On this tab the filters are set for the remote IP addresses and IP ports.*

If the basic setting is blocked then those data packets will be let through to the outside by the firewall whose destination address agrees with the address under “Local IP address” or is within the range of validity. Of the incoming data packets those are let through whose source address agrees with the address under “Local IP addresses” or is within the validity area.

The same is true for blocked basic setting with the IP ports. Those data packets are permitted outside by the firewall whose destination port falls under the definition of the local port. Of the incoming data packets those are let through whose source port falls under the definition of the local port.

With the settings under remote IP address you can specify the remote IP addresses with which the system may communicate.

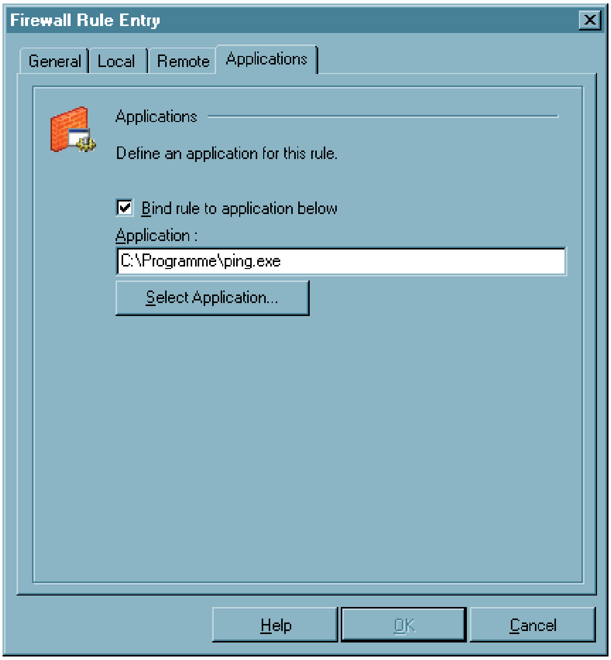
*All IP addresses*
– permits communication with any IP address of the other side, without limitation.
*Unique IP address*
– only allows communication with the IP address on the other side specified here.
*Multiple IP addresses / IP ranges*
– permits communication with different IP address on the other side according to the entries.

With the settings under remote ports, you can specify the ports via communication with remote systems is permitted.

*All ports*
– sets no limitations whatsoever relative to destination port for outgoing packets or source port for incoming packets.

*Unique port*
– only allow communication via the specified port, if this port if it is present al destination port in the outgoing data packet, or if it is present a source port in the incoming packet. If for example a rule only permits Telnet to a different system, then port 23 must be entered here.
*Multiple ports / ranges*
– can be used if multiple ports will be used for a rule (e.g. FTP port 20/21).

## Firewall rule/ Applications



Applications

Define an application for this rule.

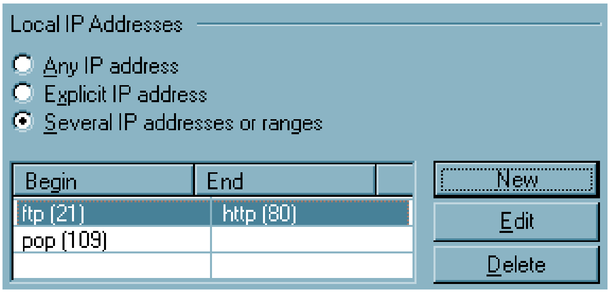
☑ Bind rule to application below

Application : C:\Programme\ping.exe

Assign rule to a certain application

– this means that with blocked (basic setting) for this application a connection is possible. It is selected via the “Select application” button a local installed application, such as ping.exe, thus only this application can communicate. In this case according to this rule only pings can be executed.

In this example you should also note that ICMP is permitted from the protocol.



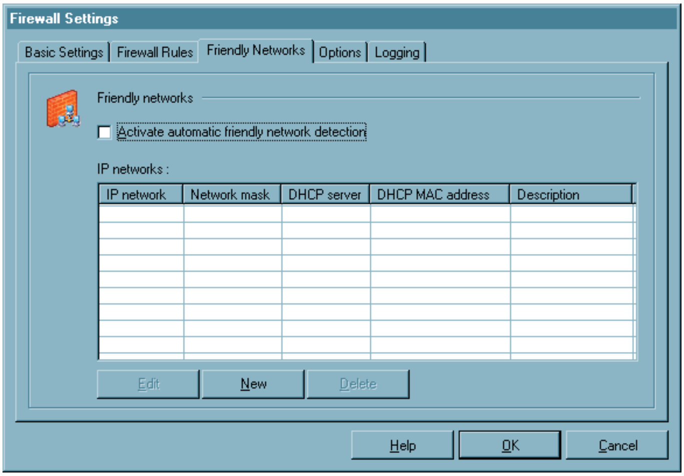
Local IP Addresses

○ Any IP address
○ Explicit IP address
● Several IP addresses or ranges

| Begin | End |
|---|---|
| ftp (21) | http (80) |
| pop (109) | |

Please note that the assigned Port has als to be selected. For e-mail application port 80.

## Configurationsfield Friendly Networks



Firewall Settings

Basic Settings | Firewall Rules | Friendly Networks | Options | Logging

Friendly networks

☐ Activate automatic friendly network detection

IP networks :

| IP network | Network mask | DHCP server | DHCP MAC address | Description |
|---|---|---|---|---|

If in “Firewall rules” you have defined in the configuration field, that a rule will be applied to connections with known network, then this rule is always used, if a network can be identified as known network according to the criteria that is entered here, e.g. the LAN adapter is in a known network.

The LAN adapter of the client is considered to be in a known network if:

**[IP network and Network mask]**

– the IP address of the LAN adapter originates from the specified network range. If for example the IP network 192.168.254.0 is specified with the mask 255.255.255.0, then the address 192.168.254.10 would effect an allocation to the known network.

**[DHCP server]**

– the IP address has been assigned by the DHCP server that has the IP address specified here;

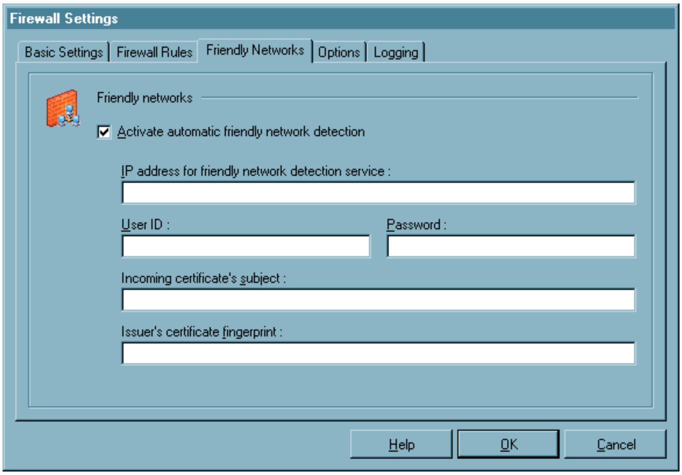
**[DHCP MAC address]**

– if this DHCP server has the MAC address specified here. This option can only be used if the DHCP server is located in the same IP subnet as the DHCP client.
The more of these conditions that are fulfilled the more precise the verification that a known network is involved.
The allocation of an adapter to unknown or known network is automatically logged in the log window of the Client Monitor and in the log file of the firewall (see -> Logging).

**Activate automatic friendly network detection**

About automatic friendly network detection please refer the parameter field on the following page.

## Automatic detection of Friendly Nets



Firewall Settings

Basic Settings | Firewall Rules | Friendly Networks | Options | Logging

Friendly networks

☑ Activate automatic friendly network detection

IP address for friendly network detection service :

User ID :

Password :

Incoming certificate's subject :

Issuer's certificate fingerprint :

The administrator centrally specifies what constitutes a Friendly Net. A Friendly Net is indicated in the monitor by the Firewall icon, which is green as soon as the Client has dialed-in to a Friendly Net.

### IP address of the Friendly Net detection service

A Friendly Net Detection Server (FNDS) is required; this is an NCP software component that must be installed in a network that is defined as “Friendly Net”. This Friendly Net Detection Server must be reachable via IP, and its IP address must be entered here.To increase redundancy the IP address of a second FND server can be entered after the first IP address, after a comma. The IP address of the first available FND server will be selected automatically for friendly net detection.

### User ID, Password (FNDS)

The Friendly Net Detection Server is authenticated via MD5 or TLS. The user ID and password entered here must agree with those that have been stored on the FNDS.

### Incoming certificate’s subject (user)

The incoming certificate of the FNDS is checked for this string. It a Friendly Net only if there is agreement.

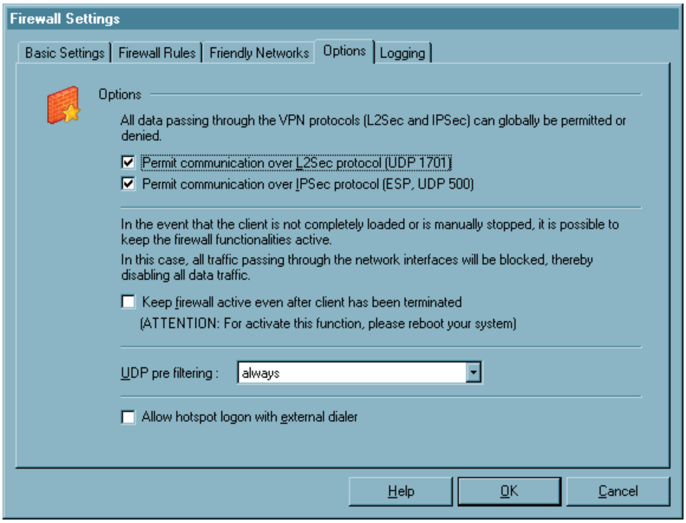
### Issuer’s certificate fingerprint

In order to offer maximum security against counterfeiting, the fingerprint of the issuer certificate must be capable of verification. It must agree with the hash value entered here.

### *Friendly Net Detection via TLS*

If the Friendly Net will be detected via TLS, (including authentication via the issuer certificate fingerprint), then this issuer certificate must be located in the “CaCerts” program directory, and its fingerprint must agree with the fingerprint configured here.

## Configurationsfield Options



Firewall Settings

Options

All data passing through the VPN protocols (L2Sec and IPSec) can globally be permitted or denied.

☑ Permit communication over L2Sec protocol (UDP 1701)

☑ Permit communication over IPSec protocol (ESP, UDP 500)

In the event that the client is not completely loaded or is manually stopped, it is possible to keep the firewall functionalities active.

In this case, all traffic passing through the network interfaces will be blocked, thereby disabling all data traffic.

□ Keep firewall active even after client has been terminated

(ATTENTION: For activate this function, please reboot your system)

UDP pre filtering : always

□ Allow hotspot logon with external dialer

With blocked basic setting the set-up of VPN connections via the “Options” tab can be globally permitted. The following protocols and ports required for the tunnel set-up are released per generated filter:

For L2Sec:
UDP 1701 (L2TP),
UDP 67 (DHCPS),
UDP 68 (DHCPC)

For IPSec:
UDP 500 (IKE ISAKMP),
IP-protocol 50 (ESP),
UDP 4500 (NAT-T),
UDP 67 (DHCPS),
UDP 68 (DHCPC)

This global definition saves you the set-up of dedicated single rules for the respective VPN variants.

Please note that only the tunnel set-up is enabled with this. If no additional rules exist for VPN networks, that permit a communication in the tunnel, then no data transfer can occur via the VPN connection.

### Continue to activate firewall with stopped client

The firewall can also be active if the client is stopped, if this function is selected. In this state however each incoming and outgoing communication is suppressed, so that no data traffic at all is possible, as long as the client is deactivated.

If the above mentioned function is not used and the client is stopped, then the firewall will also be deactivated.

### UDP Pre-filtering

In the default setting when you start the Client (independent of the Firewall) UDP pakkets will be filtered out so that a connection to the Client PC from the outside is not possible. If you start an application with server function on the Client PC, which is based on UDP data transfer (e. g. terminal applications or NTP), then this default setting can have a disturbing effect on data communication. Consequently this default setting can be switched off, or it can be limited to UDP packets of unknown networks.

Always: Default setting. In this switch position when you start the Client no UDP pakkets reach the Client PC.

Only for unknown networks: In this switch position UPD filtering will discard all pakkets from unknown networks.

Off: If the filter is switched off, all UDP packets reach the Client PC. This setting should only be used if problems occur with an application.

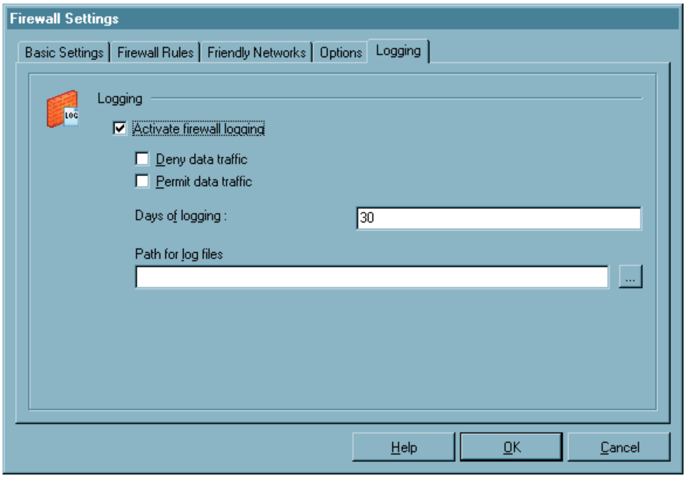
### Allow HotSpot logon for external dialers

If this function is activated, then HotSpot logon can be executed via an external dialer. You must call the command line interface rwscmd.exe for this. (See the description in the “Services” Appendix in this manual for more information in this regard!) With the command

```
rwscmd /logonhotspot [Timeout]
```

the firewall will be released for ports 80 (HTTP) and 443 (HTTPS). This generates a dynamic rule that allows data traffic until the transferred timeout (in seconds) has elapsed.

## Configurationsfield Logging


Firewall Settings

Basic Settings | Firewall Rules | Friendly Networks | Options | Logging

Logging

☑ Activate firewall logging

□ Deny data traffic

□ Permit data traffic

Days of logging : 30

Path for log files

The activities of the firewall are written to log file depending on the setting. The default location of the “Output directory for log files” is in the installation directory under \log.

The log files for the firewall are written in pure text format and are named Firewallyymmdd.log. They contain a description of “rejected data traffic” and or “Permitted data traffic”. If neither of these options has been selected then only status information on the firewall will be logged.

The log files are written at each start of the firewall. The maximum number is maintained in the log directory, as has been entered as number of the “Days for logging”.

Note: Activating the Logging will decrease the performance. For each packet corresponding to this setting, an according log text has to be written.

## 4.2.3 WLAN Settings

### *Integrated WLAN configuration*

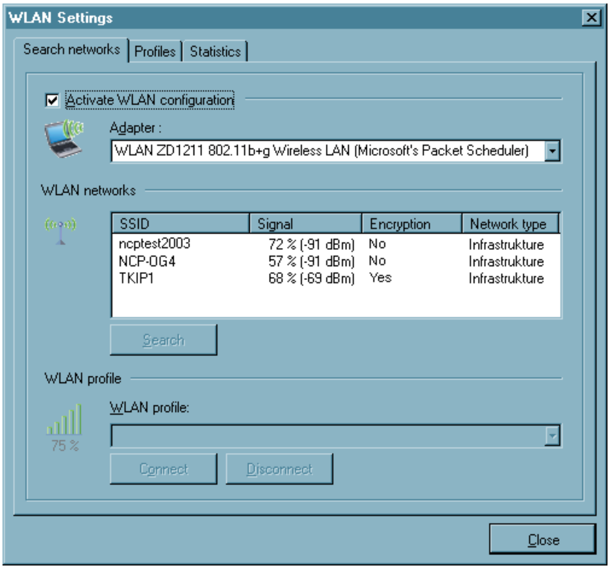
Under Windows 2000/XP and Windows Vista the WLAN adapter can be operated with the connection type “WLAN” (see → Phonebook / Parameters / Destination system). In the monitor menu “Configuration / WLAN settings” the access data for the wireless network can be saved in a profile.

### *WLAN Automation*

In the “WLAN Settings” under “WLAN Profile” select the profile with which a connection will be setup to the access point. Other than the profile selected here, there are other profiles that can be used for dialing into the access point, if these have been configured with the connection type “Automatic”, and if the function “Use profiles with automatic connection type for connection setup” has been activated in the “WLAN” settings.

In other words, multiple profiles have been created with the connection type “Automatic” and if the function “Use profiles with automatic connection type for connection setup” is used then the last selected profile will be referenced for a possible connection setup. If the SSID does not match, so that a connection to the access point cannot be setup with this profile, then subsequently the profiles that have been referenced as “automatically” configured will be referenced for the connection setup and the appropriate SSID will be used.

### Search networks



☑ Activate WLAN configuration

Adapter : WLAN ZD1211 802.11b+g Wireless LAN (Microsoft's Packet Scheduler)

WLAN networks

| SSID | Signal | Encryption | Network type |
|---|---|---|---|
| ncptest2003 | 72 % (-91 dBm) | No | Infrastrukture |
| NCP-OG4 | 57 % (-91 dBm) | No | Infrastrukture |
| TKIP1 | 68 % (-69 dBm) | Yes | Infrastrukture |

WLAN profile

WLAN profile:

75 %

If this “WLAN Configuration” is activated, then the management tool of the WLAN card must be deactivated. (Alternatively the management tool of the WLAN card can also be used; in this case the WLAN configuration in the monitor menu must be deactivated.)

**Adapter**

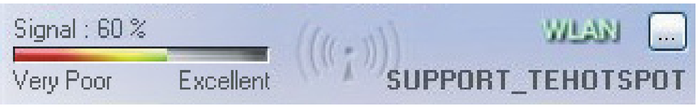
If a WLAN adapter is installed, then it will be displayed.

### WLAN networks

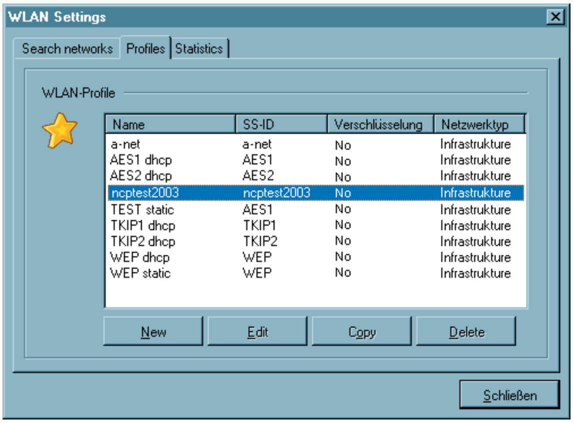
After an automatic scan process that takes a few seconds, (this can also be triggered manually by clicking on the “Scan” button), the currently available networks will be displayed with data on SSID, field strength, encryption, and network type. These values can be configured accordingly in an associated profile:

**SSID**
**Field strength**
**Encryption**
**Network type**

The name for the SSID (Standard Security) is assigned by the network operator and is displayed under the graphic field of the Monitor, in the same manner as the field strength (Fig. below). After double clicking on the network to be selected the SSID is automatically transferred into a WLAN profile for this adapter, if a profile has not yet been created for this network (see below → WLAN Profiles / General).



## WLAN Profiles

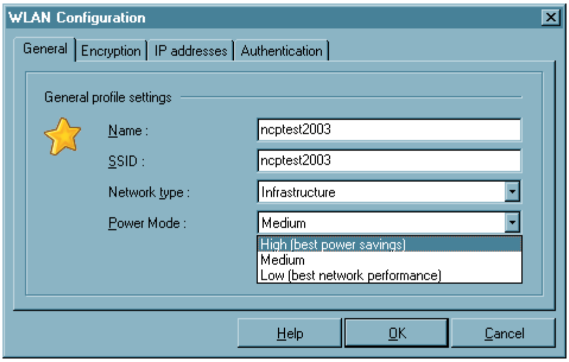


| Name | SS-ID | Verschlüsselung | Netzwerktyp |
|---|---|---|---|
| a-net | a-net | No | Infrastrukture |
| AES1 dhcp | AES1 | No | Infrastrukture |
| AES2 dhcp | AES2 | No | Infrastrukture |
| ncptest2003 | ncptest2003 | No | Infrastrukture |
| TEST static | AES1 | No | Infrastrukture |
| TKIP1 dhcp | TKIP1 | No | Infrastrukture |
| TKIP2 dhcp | TKIP2 | No | Infrastrukture |
| WEP dhcp | WEP | No | Infrastrukture |
| WEP static | WEP | No | Infrastrukture |

Previously created profiles for the adapter selected above are displayed in a list. Network type, encryption, and SSID must agree with the above network parameters. A new profile is generated by clicking on the “New” button, or by double clicking on the corresponding network in the previous window, or by clicking on the right mouse button. Profiles can also be edited or deleted via the buttons.

### General Profile Settings

The name can be freely assigned, and for a new profile generation after double clicking on the scanned network, it is initially identical with the SSID of this network. The procedure is the same with the network type, which must be identical with the network type that is sent in the broadcast of the wireless network.



General profile settings

Name : ncptest2003

SSID : ncptest2003

Network type : Infrastructure

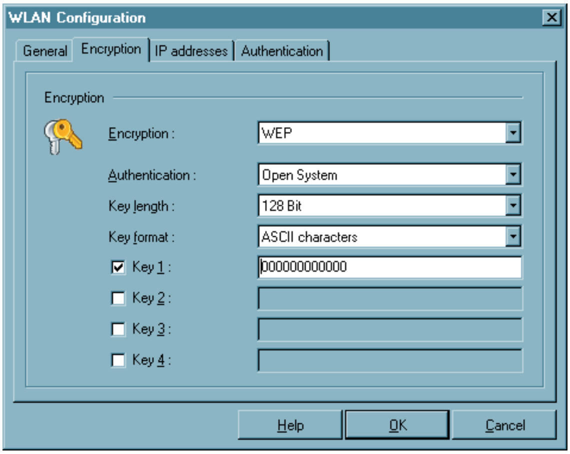
Power Mode : Medium

High (best power savings)
Medium
Low (best network performance)

The network type must then be switched to “Ad-hoc” manually if you want to set-up a profile for a direct connection from PC to PC. If the WLAN adapter permits this then the Energy Mode can be selected for it.

If the connection type of the selected profile is switched to “Automatic”, this profile can be used for the WLAN autimation (see above).

## Encryption



Encryption

Encryption : WEP

Authentication : Open System

Key length : 128 Bit

Key format : ASCII characters

☑ Key 1 : 000000000000

☐ Key 2 :

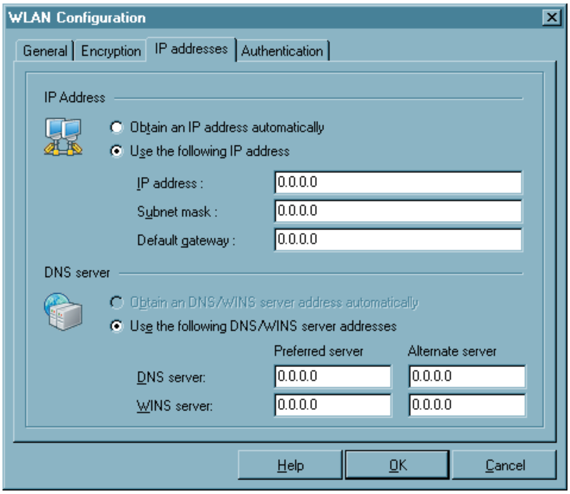
☐ Key 3 :

☐ Key 4 :

The encryption mechanism must be specified by the Access Point (WLAN router) and communicated by the administrator.

If WPA is used with EAP (TLS), then the EAP options must be activated in the configuration menu of the monitor and a certificate must be configured (in the monitor menu under “Configuration / Certificates”).

## IP Addresses



IP Address

○ Obtain an IP address automatically

● Use the following IP address

IP address : 0.0.0.0

Subnet mask : 0.0.0.0

Default gateway : 0.0.0.0

DNS server

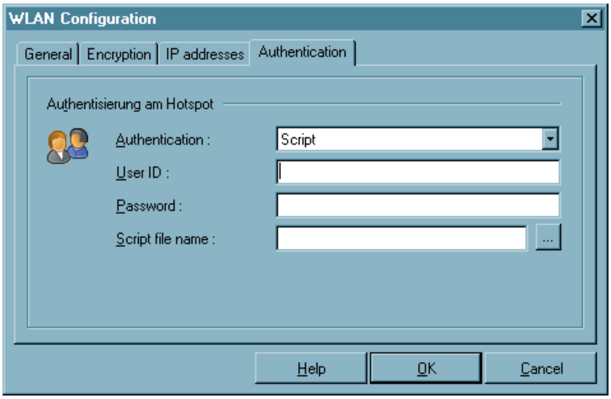
○ Obtain an DNS/WINS server address automatically

● Use the following DNS/WINS server addresses

| | Preferred server | Alternate server |
|---|---|---|
| DNS server: | 0.0.0.0 | 0.0.0.0 |
| WINS server: | 0.0.0.0 | 0.0.0.0 |

Configure the IP address of the WLAN card in this window.

The settings made here are only effective if the WLAN configuration has been activated as described above. In this case the configuration entered here will be transferred into the Microsoft configuration of the network connections. (See → Network connections / Properties of Internet protocol (TCP/IP)).



Authentisierung am Hotspot

Authentication : Script

User ID :

Password :

Script file name : ...

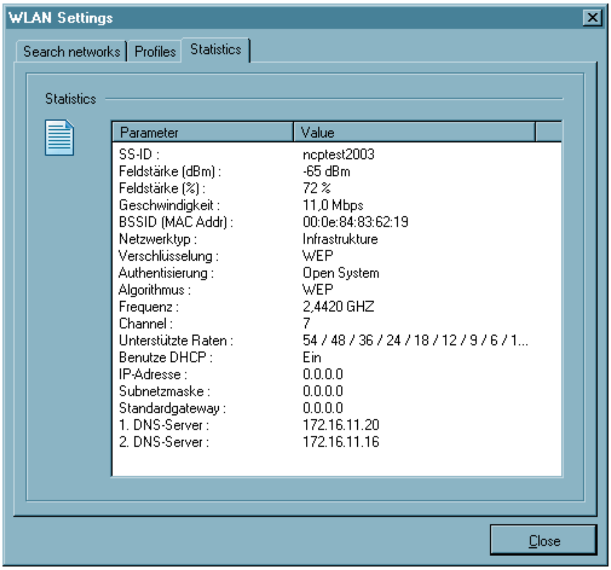
### Authentication

The access data for the HotSpot must be entered in this window. These user data are only used for this WLAN profile.

Authentication can be executed by entering user ID and password, or via script. The script automates the logon to the HotSpot operator.

Please note that there are charges associated with the connection via a HotSpot operator. You must agree to the terms and conditions of the HotSpot operator in order to set up the connection.

## Statistics



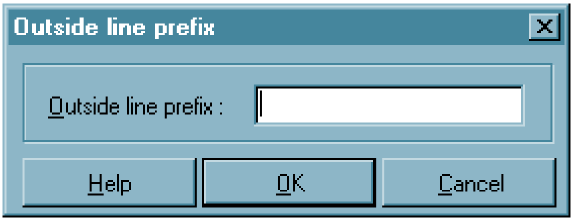
Statistics

| Parameter | Value |
|---|---|
| SS-ID : | ncptest2003 |
| Feldstärke (dBm) : | -65 dBm |
| Feldstärke (%) : | 72 % |
| Geschwindigkeit : | 11,0 Mbps |
| BSSID (MAC Addr) : | 00:0e:84:83:62:19 |
| Netzwerktyp : | Infrastrukture |
| Verschlüsselung : | WEP |
| Authentisierung : | Open System |
| Algorithmus : | WEP |
| Frequenz : | 2,4420 GHZ |
| Channel : | 7 |
| Unterstützte Raten : | 54 / 48 / 36 / 24 / 18 / 12 / 9 / 6 / 1... |
| Benutze DHCP : | Ein |
| IP-Adresse : | 0.0.0.0 |
| Subnetzmaske : | 0.0.0.0 |
| Standardgateway : | 0.0.0.0 |
| 1. DNS-Server : | 172.16.11.20 |
| 2. DNS-Server : | 172.16.11.16 |

The statistics window for the WLAN settings shows the status of the connection to the Access Point in plain text.

The statistics window completes the graphical displays in the monitor with additional data. The connection state is not concerned!

## 4.2.4 Outside Line Prefix



A special number or dial prefix is generally required when communicating via a PBX in order to acquire an outside line. The number entered in this field, depending on the type of PBX, will then be used for all outgoing calls until changed or deleted. This eliminates the need for modifying the destination phone number(s) in the phonebook, particularly when travelling.

The outside line prefix within the graphical user interface or the logon is limited to the numbers 0 to 9 and the characters “#" and “*”.

By entering the comma “,” you can configure a dial pause through  the outside line.

### 4.2.5 Certificates |Configuration

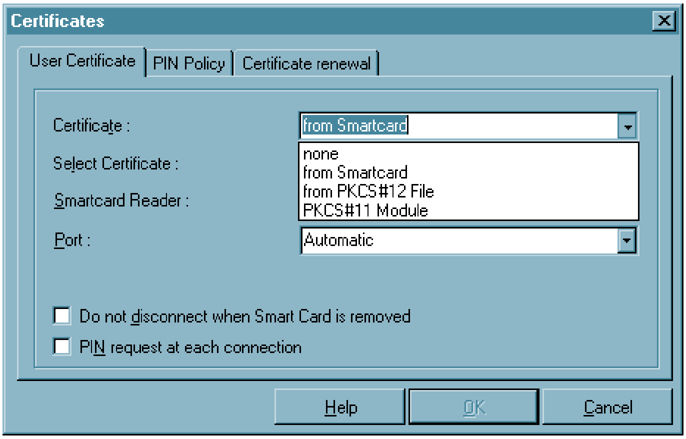
By clicking on the menu item “Configuration – Certificates” you can first determine whether you want to use the certificates, and thus the “Extended Authentication”, and where you want to store the user certificates. The PIN entry policies and the interval of validity are specified in a second parameter field.

Certificates are normally created by a CA (Certification Authority) utilizing some sort of PKI-based architecture and they may be implemented on a Smart Card in addition to a digital signature(s). Such Smart Cards represent an individual “personal identity card”. You can use certificates with the length of the private key up to 2048 Bits.

The system monitors whether the PKCS#12 file is present. If, for example, this file is stored on USB stick or an SD card, then after pulling out the SD card the PIN is reset and an existing connection is disconnected. This process corresponds to the “Connection disconnect when smart card is removed”, which can be set when using a smart card, under “Configuration, Certificates” in the monitor menu. If the SD card is later re-inserted, then the connection can be restored, after another PIN entry.

The environment variables (users) of the operating system can be inserted in the certificate configuration. The variables are changed when closing the dialog, and when copying the telephone book, and they are written back into the configuration. If an environment variable does not exist, then it is removed from the path when converted, and a log entry is written into the logbook. If a % sign (syntax), is missing then the variable remains, and a log entry is written, as above.

## User Certificate | Configuration



Certificate : from Smartcard

Select Certificate :

Smartcard Reader :

Port : Automatic

none
from Smartcard
from PKCS#12 File
PKCS#11 Module

□ Do not disconnect when Smart Card is removed

□ PIN request at each connection

### *Certificate*

By clicking on the menu item “Configuration – Certificates” you can first determine whether you want to use the certificates, and thus the “Extended Authentication”, and where you want to store the user certificates.

The PIN entry policies and the interval of validity are specified in a second parameter field.

**None:** By choosing “Certificate” from the submenu you can determine whether or not you want to use the certificate and thus use the “Extended Authentication”. The default value is “None”.

**from PKCS#12 File:** In order to use a Soft Certificate select “from PKCS#12 File” and then define the directory (path) in which the PKCS#12 file is stored for access purposes. Normally you will receive this file (encrypted) from your network administrator or your CA (Certification Authority).

**from Smart Card:** In order to use Smart Card based Certificates select “from Smart Card” and then select the Smart Card Reader from the list of supported Smart Card Readers. (see also → Enter PIN)

**PKCS#11-Module:** Select “PKCS#11-Module” from the list in conjunction with “Extended Authentication” in order for the respective Certificate to be read from a Smart Card in a Smart Card Reader or from a Token.

### *Smart Card Reader*

In order to use the Smart Card's Certificate with your card reader, select the respective Smart Card reader from the list (see also → PIN Entry).

#### Smart Card Reader (PC/SC conform)

The Client Software automatically supports all PC/SC conform Smart Card readers. The Client software automatically recognizes the Smart Card reader each time the PC is re-booted. Thereafter the installed Smart Card reader can be selected and used as required.

#### Smart Card reader (CT-API conform)

Together with the current Client Software the following drivers are included for: SCM Swapsmart and SCM 1x0 (PIN Pad reader). In the event that the Smart Card reader does not work together the drivers that are included or another Smart Card reader is installed, then please contact the respective manufacturer. Also make the following settings in the Client Software: Edit the file NCPPKI.CONF, which is located in the installation directory by entering the "ReaderName" of the Smart Card reader (xyz) connected to your PC and enter as DLLWIN95 or DLLWINNT the name of the installed driver. For operating systems based on Windows NT like Windows 2000 and Windows XP the modulname DLLWINNT has to be used. (The default name for CT-API conform drivers is CT32.DLL).

Important: Only those drivers that have been appropriately set with "visible = 1" will be displayed in the list!

```
ReaderName = SCM Swapsmart (CT-API) -> xyz
DLLWIN95   = scm20098.dll           -> ct32.dll
DLLWINNT   = scm200nt.dll           -> ct32.dll
```

The "ReaderName" will be displayed in the Monitor Menu after re-booting.

### *Port*

If the Installation has been executed correctly, the card reader will automatically be assigned a port. Should problems arise, COM Ports 1-4 can be manually assigned.

### Certificate Selection

1. Certificate ... 3.: (Standard = 1) Up to 3 different certificates, located on the Smart Card, can be selected from the list. The number of certificates on the Smart Card is dependent on the Registration Authority that has issued the Smart Card. For further information please contact your System Administrator.

The Smart Cards issued by Signtrust and NetKey 2000 come with three certificates:
(1) for digital signing,
(2) for encryption and decryption,
(3) for Authentication (optional with NetKey 2000)

### PKCS#12 File Name

If you are using the PKCS#12 format, then you will receive a file from your system administrator that must be copied to your PC's hard disk. In this case enter the path and filename of the PKCS#12 file or alternatively after clicking the selection button select the file.

### PKCS#11 Module

If you are using the PKCS#11 format, then you will receive a DLL from your Smart Card reader manufacturer that must be copied to your PC's hard disk. In this case enter the path and filename of the driver.

Edit the NCPPKI.CONF file located in the installation directory by entering the name of the connected reader or token (xyz) as "module name". The name of the DLL must be entered as PKCS#11-DLL. The associated "Slotindex" is manufacturer-dependant (standard = 0).

```
Module name    = xyz
PKCS#11-DLL  = Name of the DLL
Slotindex        =
```

After a boot process the "Module name" you entered appears in the monitor menu if the file NCPPKI.CONF for the drivers have been set to visible with "visible = 1".

You can use an assistant to search for installed PKCS#11 modules and then select the desired module with the associated slot. For this click the button "PKCS#11-Module".

### *Do not disconnect when Smart Card is removed*

The connection is not necessarily broken off when the Smart Card is removed. Whether “Do not disconnect when Smart Card is removed” occurs is set via the main menu of the monitor under the menu item “Configuration – Certificates”.

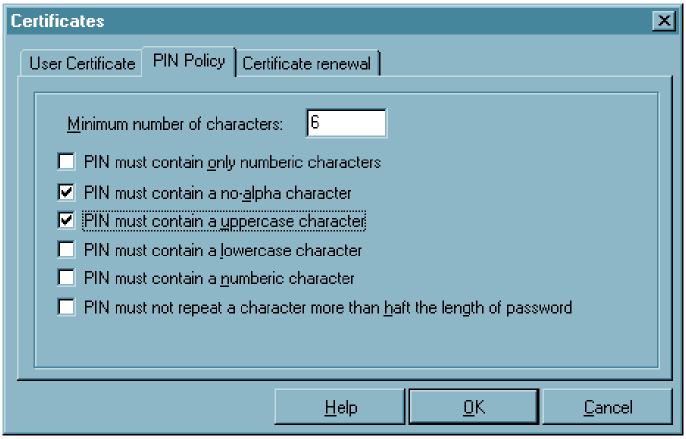
### *PIN request at each manual connect*

Default: If this function is not used, the PIN request is displayed only for the first connect of the VPN/PKI Client.

If this function is activated, the PIN will be requested at each connect.

Important: If the monitor has not started, then no PIN dialog will take place. In this case, the connection will be established without renewed PIN entry in the case of an automatic connection establishment.

## PIN Policy



Minimum number of characters: 6

☐ PIN must contain only numberic characters
☑ PIN must contain a no-alpha character
☑ PIN must contain a uppercase character
☐ PIN must contain a lowercase character
☐ PIN must contain a numberic character
☐ PIN must not repeat a character more than haft the length of password

You can specify PIN guidelines that must be complied with during PIN entry or PIN modification.

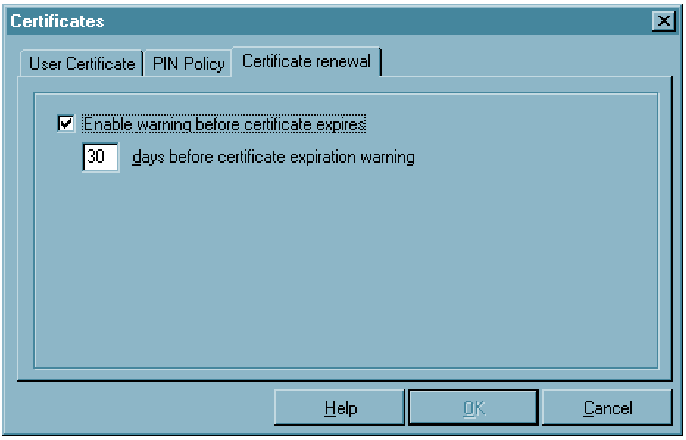
### *Minimum number of characters*

Standard is a 6-digit PIN. An 8-digit PIN is recommended for security reasons.

### *Further policies*

It is recommended to implement all PIN policies, other than the one specifying that only numbers may be contained. Additionally, the PIN should not begin with a number.The specified policies are displayed when the PIN is changed, and the policies that are only fulfilled at entry are highlighted in green (see → Change PIN).

## Certificate renewal



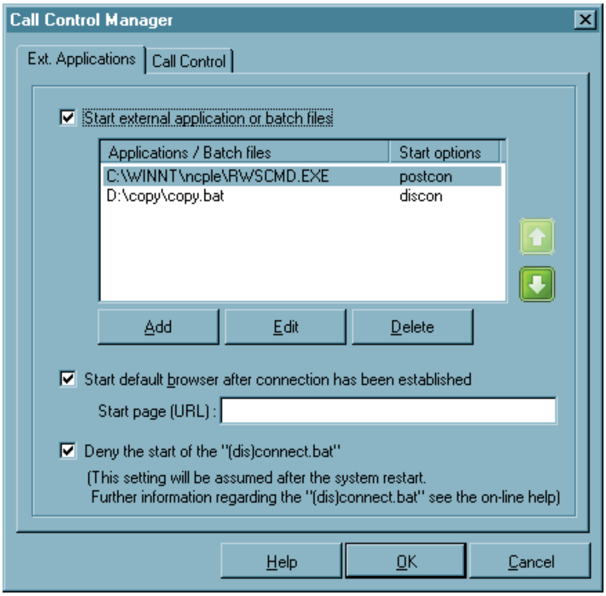
☑ Enable warning before certificate expires

30 days before certificate expiration warning

In this configuration field you can specify whether a message is given out that warns of the expiration of validity, and you can specify how many days before the certificate validity expiration this message should go out. As soon as the set time frame before expiration goes into effect, a message will appear each time a certificate is used, indicating the expiration date of the certificate.

## 4.2.6 Call Control Manager | Configuration

### ■ External Applications



☑ Start external application or batch files

| Applications / Batch files | Start options |
|---|---|
| C:\WINNT\ncple\RWSCMD.EXE | postcon |
| D:\copy\copy.bat | discon |

☑ Start default browser after connection has been established

Start page (URL) :

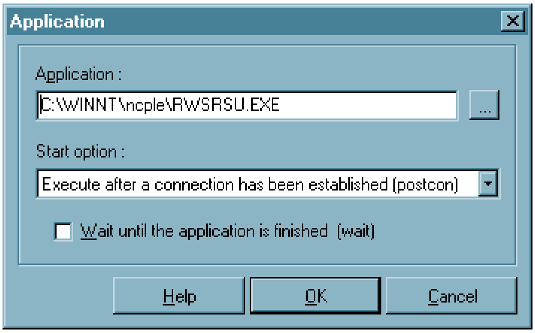
☑ Deny the start of the "(dis)connect.bat"

(This setting will be assumed after the system restart. Further information regarding the "(dis)connect.bat" see the on-line help)

Use this configuration to start applications or batch files, depending on the Client Monitor. The external applications are added as described below. The sequence, in which they are called, from top to bottom, can be changed with the green arrow keys.

If you want to start the standard browser after connection set-up, then activate this function and enter the website of the browser.

After you have selected the function “Start external applications or batch files” you can select an application or batch file from the computer via the “Add” button that, this application or batch file will be loaded depending on the start option.



Application : C:\WINNT\ncple\RWSRSU.EXE

Start option : Execute after a connection has been established (postcon)

☐ Wait until the application is finished (wait)

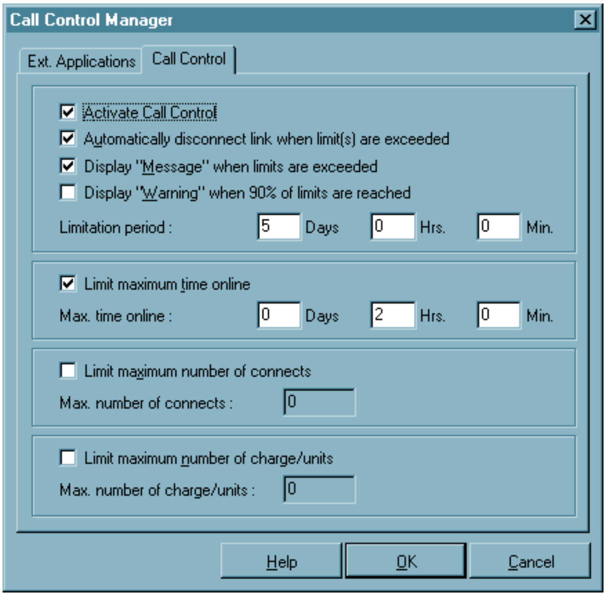
– Execute before connection has been established (precon)
– Execute after connection has been established (postcon)
– Execute after connection has been disconnected (discon)

The wait function “Wait until application has been executed and ended” can then be relevant if a series of batch files will be executed one after the other.

**Deny the start of the “(dis)connect.bat”**

**This fuction should always be activated** if execution of the cited batch files with administrator rights (system rights) is not necessarily required for a desired application. (Please see the description in the “Services” Appendix in the manual). The applications (batch files) for which user rights are adequate, can be started in the Monitor menu “External Applications...” (see above).

## Call Control



Call Control Manager

☑ Activate Call Control
☑ Automatically disconnect link when limit(s) are exceeded
☑ Display "Message" when limits are exceeded
☐ Display "Warning" when 90% of limits are reached

Limitation period : 5 Days 0 Hrs. 0 Min.

☑ Limit maximum time online

Max. time online : 0 Days 2 Hrs. 0 Min.

☐ Limit maximum number of connects

Max. number of connects : 0

☐ Limit maximum number of charge/units

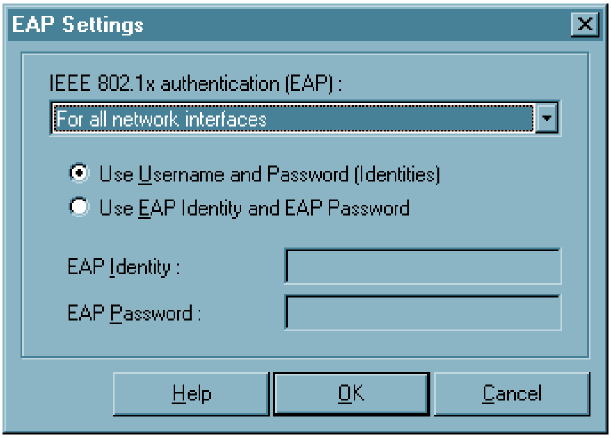
Max. number of charge/units : 0

The Call Control Manager is a feature devised to help control and limit communication costs. The following “Limit” factors can be defined:

– the maximum time online
– the maximum number of connects (outgoing calls)
– the maximum number of charge/units that may be incurred.

The time period for which these limits are to adhere to may also be defined. It is possible to define that a “Warning Message” be displayed upon reaching 90% of any limit. In the event that the set “Limit(s)” are exceeded, the link will be automatically disconnected and a “Warning Message” will be displayed in the monitor. Any further communications is denied until the “Call Control Reset” is activated (see →“Connection” pull-down menu in the monitor).

## 4.2.7 EAP Settings



IEEE 802.1x authentication (EAP) : For all network interfaces

● Use Username and Password (Identities)

○ Use EAP Identity and EAP Password

EAP Identity :

EAP Password :

You can specify whether EAP authentication will only be executed via WLAN cards, LAN cards, or via all network cards, in the “EAP Options” of the Monitor menu. The setting made here applies globally for all phonebook entries. In an activation box the EAP authentication can be set as follows:

– Deactivated
– For all network cards
– Only for WLAN cards
– Only for LAN cards

This protocol can then be used if a switch, a hub, or if an access point is used, which support 802.1x and the according Authentication Mode for the access to the wireless LAN.

You can prevent unauthorized users from getting into the LAN via the hardware interface with the Extended Authentication Protocol (EAP MP5).

You can use either “Username” with “Password” (from the configuration field “Identity”) or your own “EAP User ID” with an “EAP Password”.

Certificate content can be automatically transferred if in the Phonebook under “Tunnel parameters” VPN User ID and VPN Password are transferred from the certificate, and if “Use VPN User ID and VPN Password” is activated in the EAP options.

For EAP-TLS (with certificate) now the EAP user name can be directly referenced from the certificate configuration. The following content of the configured certificate can be used by entering the appropriate placeholders in the EAP configuration:

```
Commonname : %CERT_CN%
E-mail     : %CERT_EMAIL%
```

After configuration of the certificate these placeholders are entered in the monitor menu under: Configuration / EAP Options / User ID and Password. Double click on the EAP icon to reset the EAP. Subsequently a new EAP negotiation will be executed automatically.

## 4.2.8 Logon Options

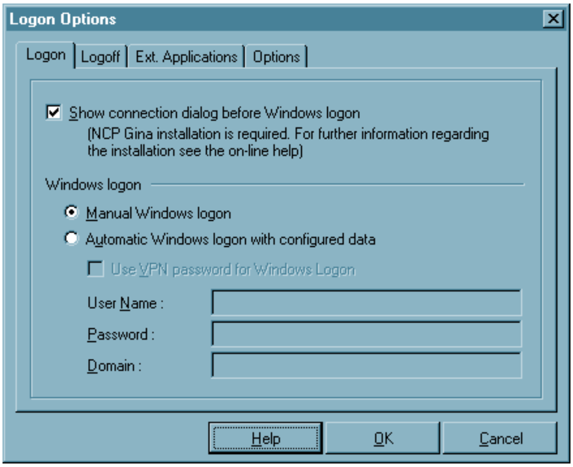
The logon options are only effective when the computer has booted.

### Logon

Because the connection setup to the gateway occurs prior to the Windows logon, the logon to the remote domain is already encrypted and the firewall is activated.

**Show connection dialog befor Windows logon**

The NCP Gina dialogs can be hidden via the Monitor menu without de-installing the Gina. Thus Gina concatenations that may possibly be necessary for the respective work environment remain intact. If you want to display the Gina dialog, then note that the NCP Gina must be installed in any case. This can be done in three ways:



☑ Show connection dialog before Windows logon
(NCP Gina installation is required. For further information regarding the installation see the on-line help)

Windows logon

● Manual Windows logon

○ Automatic Windows logon with configured data

□ Use VPN password for Windows Logon

User Name :

Password :

Domain :

– With the software installation, here the system asks the user if he wants to use the Windows logon via the NCP Gina. If yes, it will be installed.
– Retroactive installation is possible via the command line interface rwscmd.exe, likewise retroactive de-installation is also possible.
– The Gina is also installed if an appropriate phonebook is provided via Secure Enterprise Management.

If the Gina dialog does not appear then the connection to the domain server cannot be set-up via the NCP Gina. In other words you must have the “Display dialog for connection before Windows logon” so that in the boot phase the connection to the VPN gateway can already be set-up. For this connection set-up you must enter access data for the network dial-in, or PIN and SIM PIN must be entered before the Windows logon.

**Windows logon**

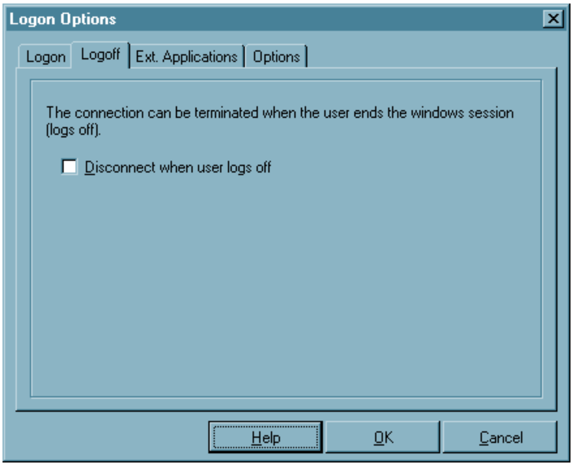
The following Windows logon can be executed automatically or manually depending on configuration.

“Execute manually” means that the user must enter his logon data manually in the Windows logon screen.
“Automatically” means that the Client software will transfer the data entered here to the Microsoft Gina without user intervention.

If you use the logon option with callback then “Negotiate PPP callback” must be activated (see → parameter field “Callback” in the Phonebook).

To select the destination with the logon option please see the section “Setup a connection - Client logon” and the Appendix for Mobile Computing.

## Logoff



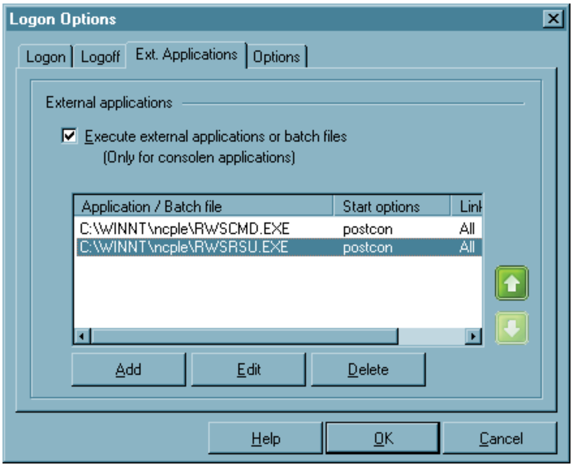
The connection can be terminated when the user ends the windows session (logs off).

□ Disconnect when user logs off

The Client connection to the VPN Gateway or ISP can be maintained when a Windows logon is executed.

This permits a change of Windows users on the computer, without having to disconnect the VPN connection.

## External applications



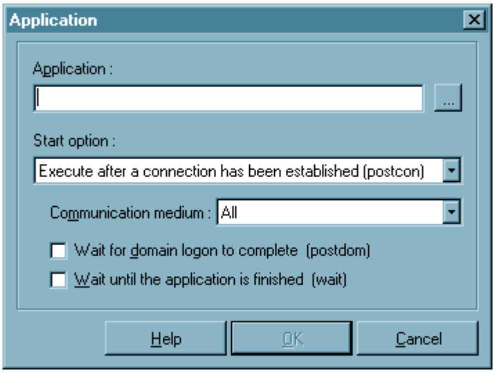
External applications

☑ Execute external applications or batch files
(Only for consolen applications)

| Application / Batch file | Start options | Lin |
|---|---|---|
| C:\WINNT\ncple\RWSCMD.EXE | postcon | All |
| C:\WINNT\ncple\RWSRSU.EXE | postcon | All |

Use this configuration field to start applications or batch files, depending on the Client Monitor (no Windows programs!).

The external applications are added as described on the next page. The call sequence from top to bottom can be changed with the green arrow keys.


Application

Application :

Start option : Execute after a connection has been established (postcon)

Communication medium : All

□ Wait for domain logon to complete (postdom)

□ Wait until the application is finished (wait)

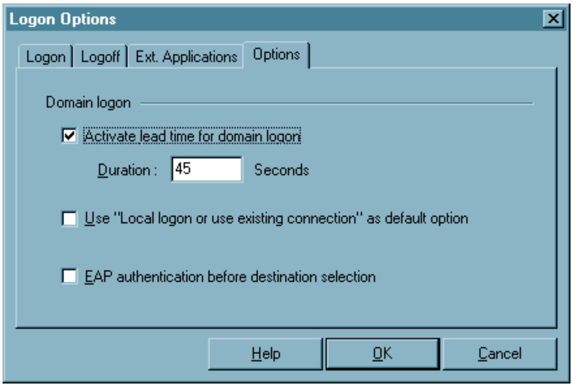
After you have selected the function "Start external applications or batch file" you can select an application or batch file from the computer (see previous page), this application of batch file is then loaded depending on the start option:

- Execute before a connection has been established (precon)
- Execute after a connection has been established (postcon)

In addition, the application can be started depending on the connection type of the destination system that is selected in the Gina dialog. The application always starts if the connection type "All" has been selected.

"Wait for domain preparation (postdom)" means that after the initialization period, the application will be started immediately. The wait function "Wait until application has been executed and ended" can then be relevant if a series of batch files will be executed one after the other.

## Options


Logon Options

Domain logon

☑ Activate lead time for domain logon

Duration : 45 Seconds

□ Use "Local logon or use existing connection" as default option

□ EAP authentication before destination selection

Windows requires a certain initialization time between network logon and domain logon. This preparation time for the domain logon can be activated and set here. The Windows logon will only be executed after the connection setup, after the initialization time set here has elapsed. The standard value is 45 seconds and can be changed as needed.

**Perform EAP authentication prior to destination selection**

The standard situation is that EAP authentication takes place prior to establishing the connection to the VPN gateway. If EAP will be used without subsequently setting up a connection via the Client (pure EAP Client) then this function must be activated. If EAP with certificate is implemented, then the PIN dialog for authentication appears on the network components. Thereafter the destination can be selected. If the function is not activated then EAP authentication will only be executed after the destination has been selected.

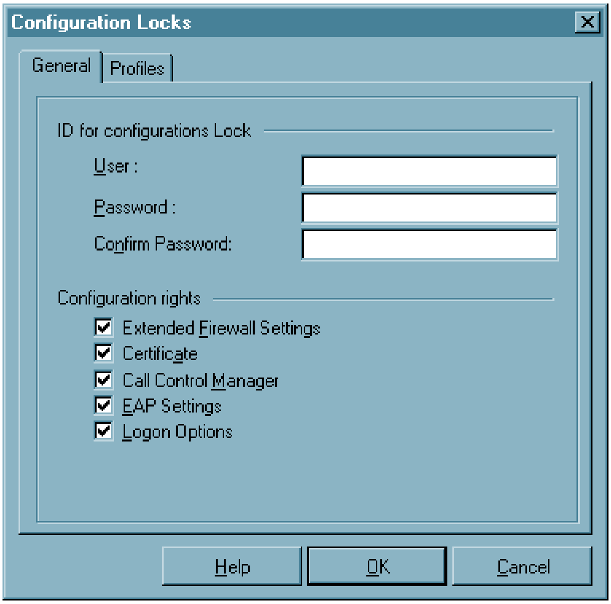
Using the Logon Options refer also the appendix "Mobile Computing via GPRS/UMTS".

## 4.2.9 Configuration Locks

Use configuration locks to modify the configuration main menu in the monitor in such a way that the user can no longer modify the pre-set configurations, or so that selected parameter fields are no longer visible for the user.

The configuration locks are enabled after applying the defined settings with “OK”. Clicking the cancel button the default settings will be used.

### ■ General | Configuration Locks



Configuration Locks

ID for configurations Lock

User :

Password :

Confirm Password:

Configuration rights

☑ Extended Firewall Settings

☑ Certificate

☑ Call Control Manager

☑ EAP Settings

☑ Logon Options

In order to effectively specify the configuration blocks, identification must be entered, which consists of “User ID” and “Password”. The password must be confirmed thereafter.

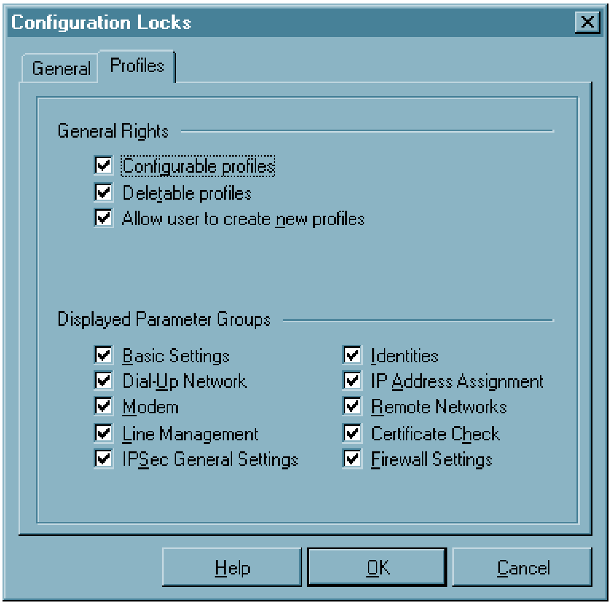
Please note that identification is absolutely necessary for the configuration block, in order to activate the blocks, or to cancel the configuration blocks. If the identification is forgotten there is no other possibility to cancel the blocks!

Now authorization to open menu items under the main menu item, “Configuration”, can be limited for the user. As standard, the user can open all menu items and edit the configurations. If the check mark is removed from the respective menu item with a mouse click, then the user can no longer open this menu item.

## Profiles | Configuration Locks

The editing rights for the parameters in the profile settings are divided into two groups:

– General rights
– Visible profile parameter fields



General Rights

☑ Configurable profiles
☑ Deletable profiles
☑ Allow user to create new profiles

Displayed Parameter Groups

☑ Basic Settings
☑ Dial-Up Network
☑ Modem
☑ Line Management
☑ IPSec General Settings
☑ Identities
☑ IP Address Assignment
☑ Remote Networks
☑ Certificate Check
☑ Firewall Settings

### *General rights*

The general rights refer only to (configuration of) the profiles. If you specify “Profiles may be created”, then “Profiles may be configured”, however remains excluded, thus while new profiles can indeed be defined with the assistant, subsequent modification of individual parameters will then no longer be possible.

### *Visible profile parameter fields*

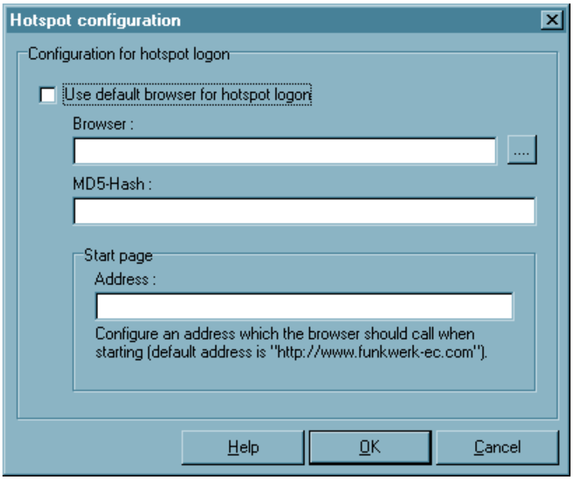
The parameter fields of the profile settings can be suppressed for the user.

Please note as well that parameters of a non-visible field cannot be configured.

## 4.2.10 Profile Import

With this function profile settings can be imported by the client. The profile settings to be imported can be created as INI-file by the destination system or edited by hand. You will find the files IMPORT_D.TXT and IMPORT_E.TXT in the installation directory for example. In those files the syntax and the values of the parameters are described.

## 4.2.11 HotSpot



Hotspot configuration

Configuration for hotspot logon

□ Use default browser for hotspot logon

Browser :

MD5-Hash :

Start page

Address :

Configure an address which the browser should call when starting (default address is "http://www.funkwerk-ec.com").

The configuration for hotspot logon is executed via this menue option. The following settings are possible:

– “Use standard browser for hotspot logon” is the default setting. If the check mark is removed from the checkbox then a different browser can be specified in the form:
`%PROGDIR%\Mozilla\Firefox\firefox.exe.`
In addition the MD5 hash value of the browser exe file can be determined and entered in the “MD5 Hash” field. In this manner the system ensures that a hotspot connection is only realized with this browser.

– Under “Start Page / Address” the start page described above is entered in the form:
`http://www.mycompagnie.de/error.html.`

## 4.2.12 Profile Settings Backup

If a secure profile setting has not yet been generated, for instance in the case of a first installation, then a first profile setting (NCPPHONE.SAV) will automatically be created.

- **Create**

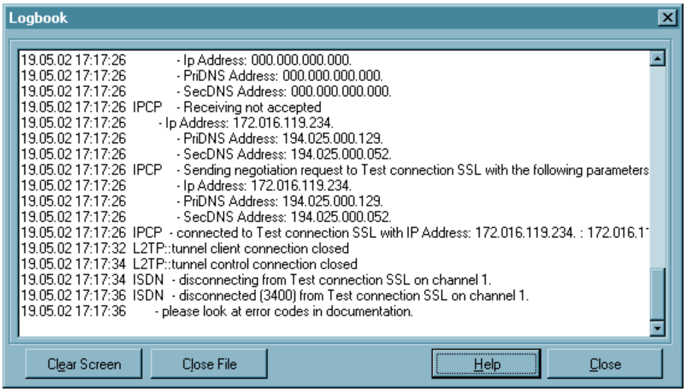
A profile setting backup will be created after each click on the “Create” menu item, and after a confirmation question, that contains the configuration up to this point.

- **Restore**

The last profile setting backup will be read in after each click on “Restore”. Thus, changes in the configuration that have been made since the last profile setting backup will be lost.

## 4.3 Log

This feature automatically logs (records) all communication transactions (but not the data) going via the Client. Selecting the Log function will open the window of the logbook.



```
19.05.02 17:17:26         - Ip Address: 000.000.000.000.
19.05.02 17:17:26         - PriDNS Address: 000.000.000.000.
19.05.02 17:17:26         - SecDNS Address: 000.000.000.000.
19.05.02 17:17:26 IPCP    - Receiving not accepted
19.05.02 17:17:26       - Ip Address: 172.016.119.234.
19.05.02 17:17:26         - PriDNS Address: 194.025.000.129.
19.05.02 17:17:26         - SecDNS Address: 194.025.000.052.
19.05.02 17:17:26 IPCP    - Sending negotiation request to Test connection SSL with the following parameters
19.05.02 17:17:26         - Ip Address: 172.016.119.234.
19.05.02 17:17:26         - PriDNS Address: 194.025.000.129.
19.05.02 17:17:26         - SecDNS Address: 194.025.000.052.
19.05.02 17:17:26 IPCP  - connected to Test connection SSL with IP Address: 172.016.119.234. : 172.016.1
19.05.02 17:17:32 L2TP::tunnel client connection closed
19.05.02 17:17:34 L2TP::tunnel control connection closed
19.05.02 17:17:34 ISDN  - disconnecting from Test connection SSL on channel 1.
19.05.02 17:17:36 ISDN  - disconnected (3400) from Test connection SSL on channel 1.
19.05.02 17:17:36       - please look at error codes in documentation.
```

The contents of the log are stored in memory and are accessible until such a time that you (re)boot your PC.

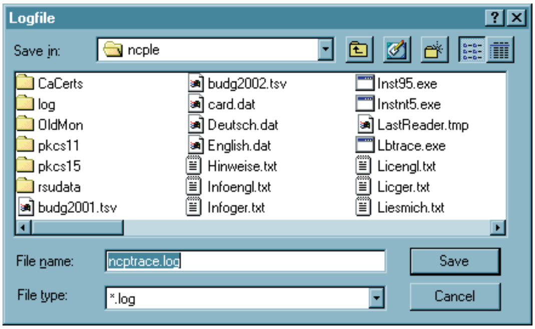
Alternatively, if required, the log can also be written (stored) to a file. The log function automatically stores all actions of the Client for a period of seven days. Log files older than 7 online days will be automatically deleted. This is where the log files are stored and are named NCPyymmdd.LOG (yy=year, mm=mouth, dd=date). The file can be opened and analyzed with a text editor.

### Logbook

The buttons of the “Logbook” window have the following functions:

– Create File
– Close File
– Clear Screen
– Close – Logbook

#### *Create File*



Save in: ncple

File name: ncptrace.log

File type: *.log

Clicking this button will open a window where you can enter the name and path of the file to be created for the log feature to write (record) to (default name = ncptrace.log).

All communication transactions (but not the data) will then be written to the file until such a time that the “Close File” command is initiated. Creating a log file will enable you to make a more detailed review or analysis of your communication transactions over a longer period of time.

### *Close File*

Clicking on the “Close” button will close the file that was established with “Create File”. Once the file has been closed it can then be used to make a detailed review or analysis of the communication transactions that have been stored.

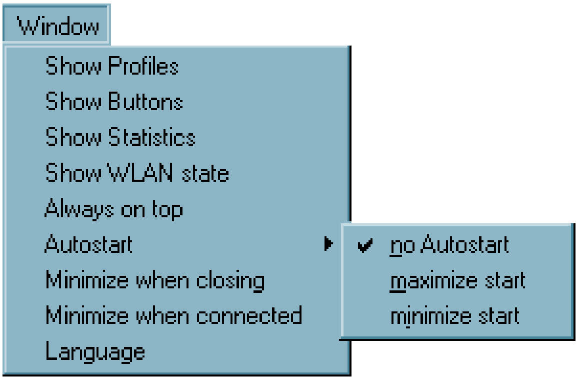
### *Clear Screen*

Clicking this button will delete the contents of the log screen and empty the buffers.

### *Close – Logbook*

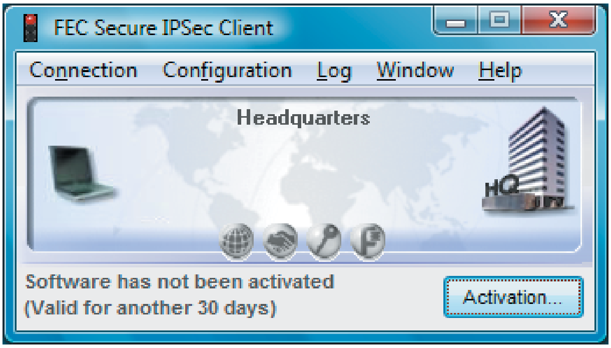
When you click on “Close” the logbook closes and returns to the monitor. Any recorded data remains unchanged.

## 4.4 Windows



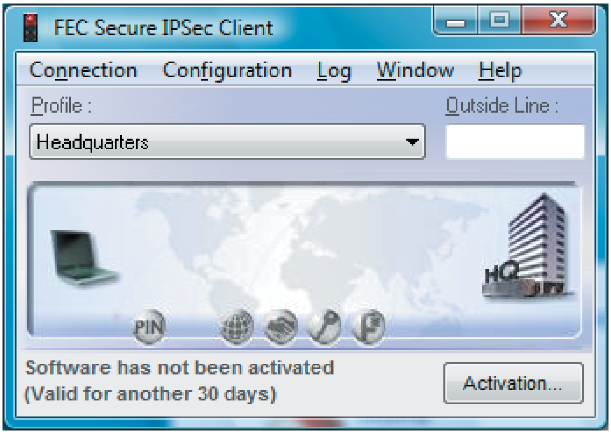
This feature lets you influence the way in which the monitor is displayed on your screen.

### 4.4.1 Show Profiles



Software has not been activated
(Valid for another 30 days)

Left side the minimized representation.



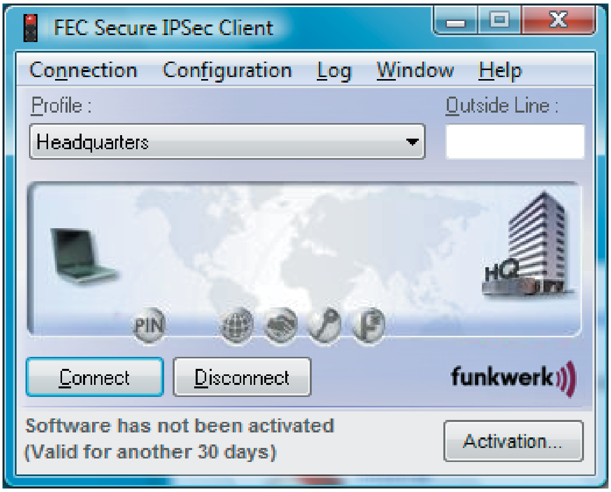
Profile : Headquarters

Outside Line :

Software has not been activated
(Valid for another 30 days)

When “Show Profiles” is activated the configured destinations could be selected by clicking on the listed names (picture left side).

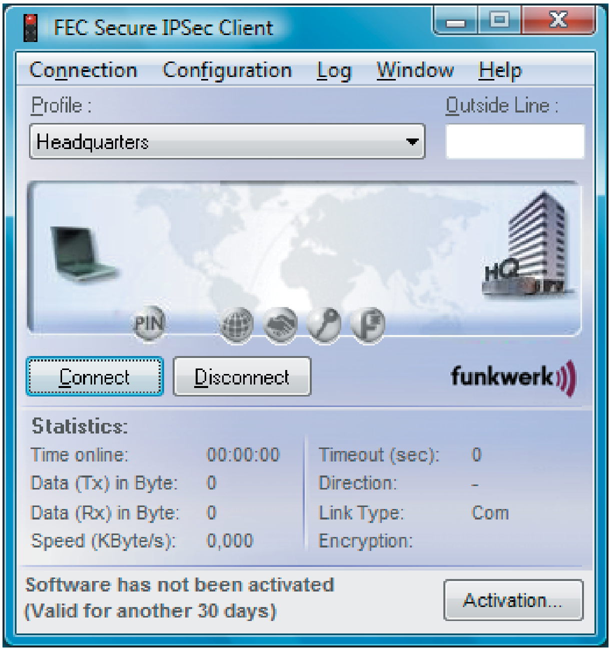
## 4.4.2 Show Buttons



Software has not been activated
(Valid for another 30 days)

When “Show Buttons” is activated the buttons concerning to “Connect” and “Disconnect” are displayed therefore the size of the window is larger.

## 4.4.3 Show Statistics



Statistics:

| | | | |
|---|---|---|---|
| Time online: | 00:00:00 | Timeout (sec): | 0 |
| Data (Tx) in Byte: | 0 | Direction: | - |
| Data (Rx) in Byte: | 0 | Link Type: | Com |
| Speed (KByte/s): | 0,000 | Encryption: | |

Software has not been activated
(Valid for another 30 days)

When “Show Statistics” is activated all information available from the monitor is displayed; the size of the window will be larger.

### 4.4.4 Show WLAN Status

Undepending on the connection medium of the current link profile, in the Monitor menu “window” under “Show WLAN status”, you can open or close a separate field for graphic display of WLAN field strength, if a WLAN configuration has been activated in the the Monitor menu “Configuration”, under “WLAN settings”. If a multifunction card has been configured, then the menu item “WLAN panel” is not active.

### 4.4.5 Always on top

When “Always on Top” is activated the monitor will always be displayed in the foreground of your desktop regardless of what application is currently active.

### 4.4.6 Autostart

This menu item allows to set the monitor to be started after booting. Use this menu item to set the following options:

□ no Autostart: after booting do not automatically start the system

□ minimize start: after booting start the monitor and minimize the display

□ maximize start: after booting start the monitor and display it in its normal size

If you require the use of the IPSec client often and need the information displayed on the monitor, you should select the Autostart option “maximize start”. It is, however, not mandatory for communicating with the destination to start the monitor.

### 4.4.7 Minimize when closing

If the monitor is closed during an existing connection via the close button [x] in the upper right hand side of the (active) titel bar [Alt + F4], then a message window alerts you that no icon (tray icon) will appear in the task bar, this means that the user then cannot recognize on his screen whether connection charges are accrueing, how long connection charges will accrue, or whether the connection has already ended.

(In this case, the monitor must be restarted to determine the status of the connection and to correctly end the connection.)

The “Minimize when closing” menu item has been added under “Window”. If this menu item is active, then the monitor is only minimized when closing via the [x] in the (active) titel bat or via [Alt + F4]. Clicking on the close button [x] in the header has the same effect in this setting as clicking on the minimize button [-] in the (active) titel bar.

(The possible destination system can be read and the connection can be established or terminated with a right mouse click on the icon, or the monitor can also be ended if the connection is terminated.

By clicking “Disconnect” in the connection menu the monitor can be terminated.

### 4.4.8 Minimize when connected

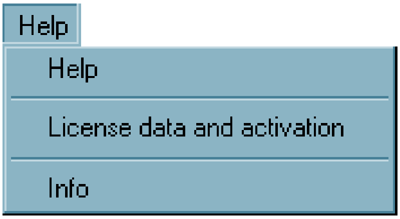
If this menu item is activated the monitor will be minimized when the connection is established successfully.

Closing the monitor is only possible via the main menu “Connection – Exit”.

### 4.4.9 Language

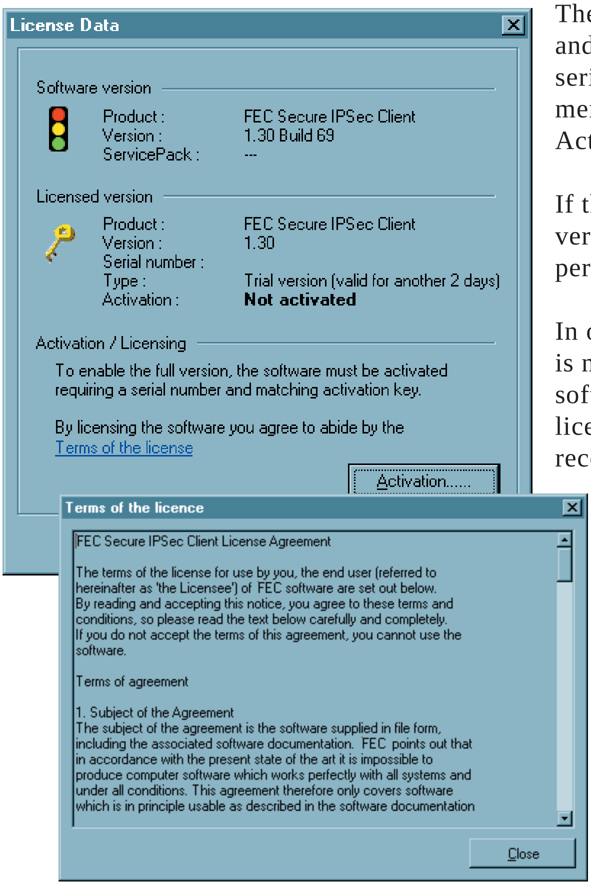
The client software has been designed for international language support. The default language is English. In order to choose a language, click on “Language” in the Window pulldown menu and then select the desired language. In the near future the client will have additional language support.

# 4.5 Help



*Select the "Help" menu option to open the online help context-independently with Table of Contents and Index. Moreover you can enter the license key and read the version number of the software here.*

## 4.5.1 License Data and Activation



License Data

Software version

Product : FEC Secure IPSec Client
Version : 1.30 Build 69
ServicePack : ---

Licensed version

Product : FEC Secure IPSec Client
Version : 1.30
Serial number :
Type : Trial version (valid for another 2 days)
Activation : **Not activated**

Activation / Licensing

To enable the full version, the software must be activated requiring a serial number and matching activation key.

By licensing the software you agree to abide by the Terms of the license

Terms of the licence

FEC Secure IPSec Client License Agreement

The terms of the license for use by you, the end user (referred to hereinafter as 'the Licensee') of FEC software are set out below. By reading and accepting this notice, you agree to these terms and conditions, so please read the text below carefully and completely. If you do not accept the terms of this agreement, you cannot use the software.

Terms of agreement

1. Subject of the Agreement
The subject of the agreement is the software supplied in file form, including the associated software documentation. FEC points out that in accordance with the present state of the art it is impossible to produce computer software which works perfectly with all systems and under all conditions. This agreement therefore only covers software which is in principle usable as described in the software documentation

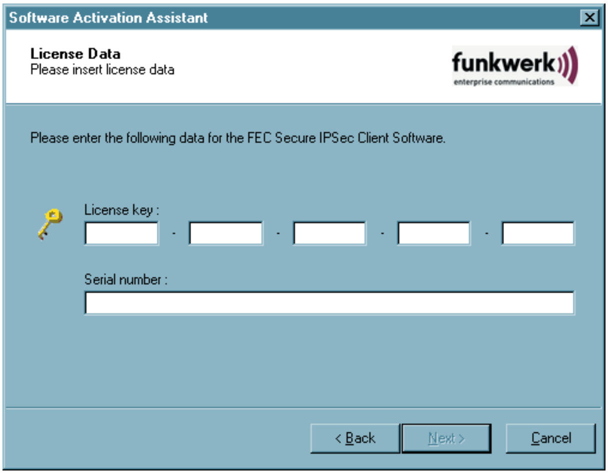
The software version implemented, and possibly the licensed version with serial number, are shown under the menu option "License Data and Activation".

If the software is used as a test version, then the remaining validity period is displayed in the popup.

In order to use a valid full version that is not subject to time restrictions, the software must be released with the license key and serial number received.

The licensing process for the software requires your acceptance of the license conditions; these conditions can be viewed via mouse click.

The license data can be entered either online or offline via an assistant. Please refer to the chapter "Licensing".



Software Activation Assistant

License Data
Please insert license data

Please enter the following data for the FEC Secure IPSec Client Software.

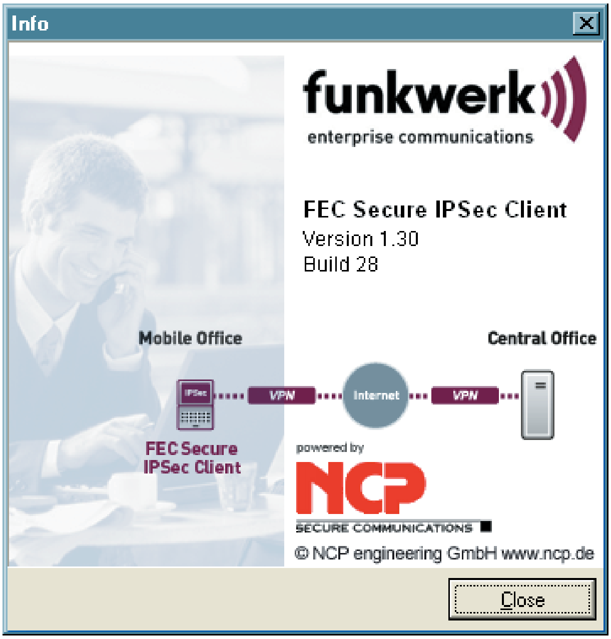
License key : ____ - ____ - ____ - ____ - ____

Serial number : ____

License key and serial number can be entered after you have clicked on the licensing button.

Later the correctly entered license data is no longer displayed at this point.

## 4.5.2 Info



Info

FEC Secure IPSec Client
Version 1.30
Build 28

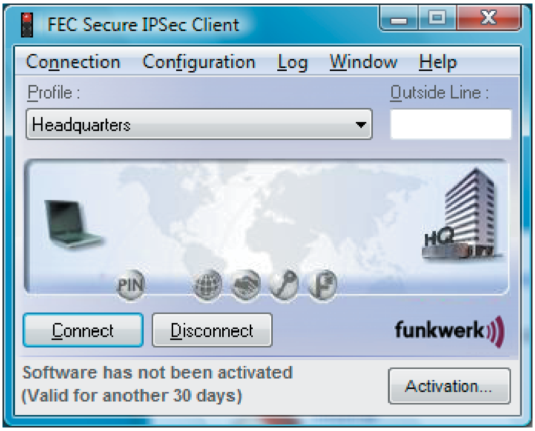
© NCP engineering GmbH www.ncp.de

The info window shows the product designation and the version number of the software you are using.

## 4.6 Licensing

In the “Help” Monitor menu, under the menu option “License Data and Activation”, the software version implemented, and possibly the licensed version with serial number, are shown.

The Client software is always installed first as a test version, if Client software has not yet been installed, or if there is a previously installed older version, then the software has not yet been activated. This also applies if the older version has already been licensed – then this older version will be reset to the status of a test version, and the license data must be re-entered within 30 days via the activation dialog.



Software has not been activated
(Valid for another 30 days)

The time remaining until software activation, i.e. the validity period of the test version, is displayed in the message bar of the monitor next to the activation button.

In order to use a full version with no time limitations the software must be released in the activation dialog with the license key and the serial number that you have received. With activation you accept the license conditions that you can view in the activation dialog after clicking on the appropriate button.

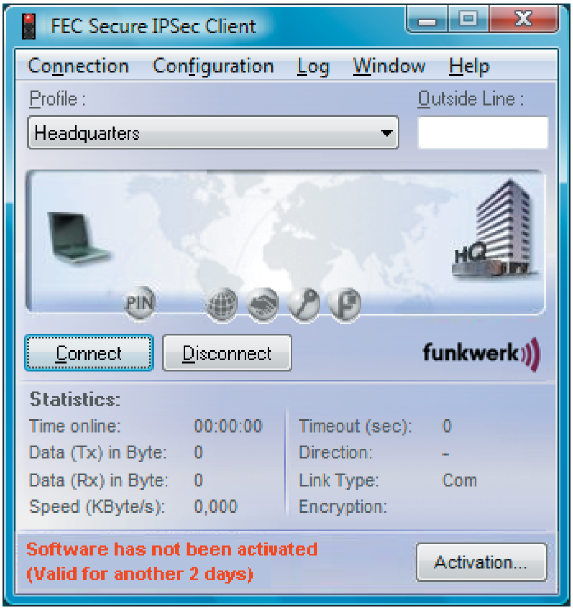
The activation dialog can be opened via the activation button in the message bar of the monitor, as well as the via the monitor menu “Help / License info and activation”. The license data can be entered either online or offline via a wizard.

In the offline variant, a file that is generated after entering the license key and serial number must be sent to the web server, and the activation key that is then displayed on the website must be noted. This activation key can be entered in the licensing window of the Monitor menu at a later point in time.

In the online variant, an assistant forwards the licensing data to the web server immediately after entry and thus the software is immediately released.

## 4.6.1 Test Version Validity Period

The test version is valid for 30 days. Without software activation or licensing it will no longer be possible to setup a connection after this 30-day period expires.



Statistics:

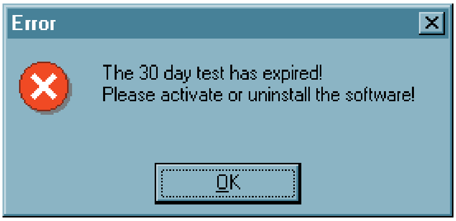
| | | | |
|---|---|---|---|
| Time online: | 00:00:00 | Timeout (sec): | 0 |
| Data (Tx) in Byte: | 0 | Direction: | - |
| Data (Rx) in Byte: | 0 | Link Type: | Com |
| Speed (KByte/s): | 0,000 | Encryption: | |

Software has not been activated
(Valid for another 2 days)

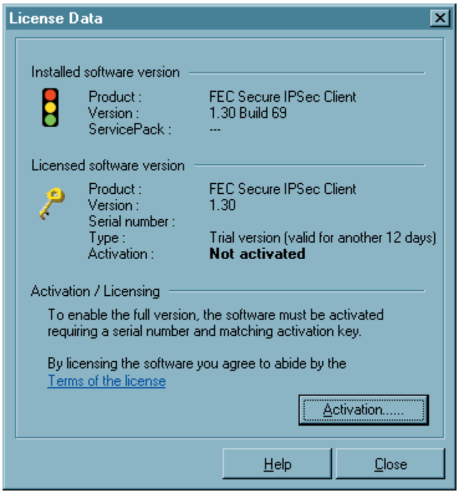
After installation, each time the software is started the validity period will be shown in the popup window. Moreover in a footer of the Monitor the system will display how long the test version can still be used, and when 10-days validity remain, a message box will be displayed to remind you that the software has not yet been licensed. This message box will appear once a day.

If the test phase has expired, then only those connections to destination systems can be setup with the IPSec Client software that are used for software activation/licensing. Thus one of the profiles of the IPSec Client can be used to set-up an Internet connection for licensing purposes.

## 4.6.2 Software Activation



The 30 day test has expired!
Please activate or uninstall the software!



Installed software version

Product : FEC Secure IPSec Client
Version : 1.30 Build 69
ServicePack : ---

Licensed software version

Product : FEC Secure IPSec Client
Version : 1.30
Serial number :
Type : Trial version (valid for another 12 days)
Activation : **Not activated**

Activation / Licensing

To enable the full version, the software must be activated requiring a serial number and matching activation key.

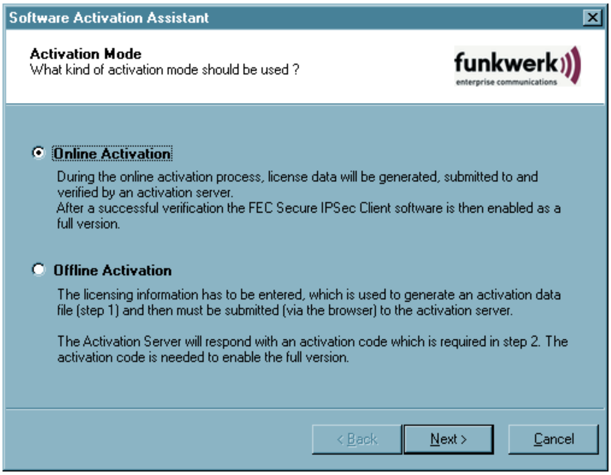
By licensing the software you agree to abide by the Terms of the license

At the latest when the test phase has expired the software must be either activated or de-installed. For activation, select the menu option “License info and activation” in the monitor menu “Help”.

Here you can see which software version you have and how the software is licensed, i.e. you can see that the test version has expired and that the software has not yet been activated/licensed.

Click on the license conditions to display the license agreement text. By activating/ licensing the software you accept the license conditions.

Click on the “Activation” button to license the software.



**Activation Mode**
What kind of activation mode should be used ?

● **Online Activation**

During the online activation process, license data will be generated, submitted to and verified by an activation server.
After a successful verification the FEC Secure IPSec Client software is then enabled as a full version.

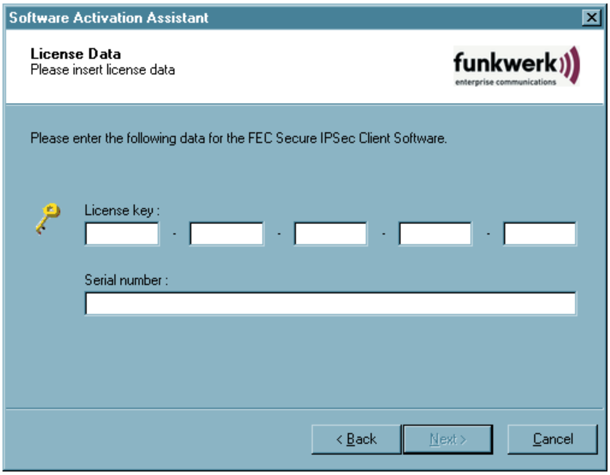
○ **Offline Activation**

The licensing information has to be entered, which is used to generate an activation data file (step 1) and then must be submitted (via the browser) to the activation server.

The Activation Server will respond with an activation code which is required in step 2. The activation code is needed to enable the full version.

In the window that appears you can select an online variant or an offline variant.

In the offline variant, a file that is generated after entering the license key and serial number must be sent to the web server, and the activation key that is then displayed on the website must be noted. In the online variant, an assistant forwards the licensing data to the web server immediately after entry and thus the software is immediately released.


Software Activation Assistant

License Data
Please insert license data

Please enter the following data for the FEC Secure IPSec Client Software.

License key : ____ - ____ - ____ - ____ - ____

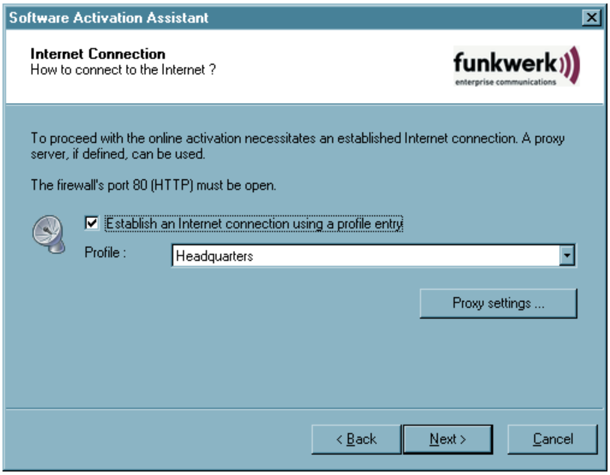
Serial number :

After selecting the type of activation the license data will be entered in the appropriate fields. Click on “Next”!

## Online Variant

With the online variant the license data will be transmitted to the Activation Server via an Internet connection. This Internet connection can either be established via the Data Communications Dialer, via DSL, or via the IPSec Client.

If the Internet connection is not set-up via the IPSec Client, then the connection must first be established in order to then start the activation assistant via the Monitor menu option, “Help” / License info and activation".


Software Activation Assistant

Internet Connection
How to connect to the Internet ?

To proceed with the online activation necessitates an established Internet connection. A proxy server, if defined, can be used.

The firewall's port 80 (HTTP) must be open.

☑ Establish an Internet connection using a profile entry

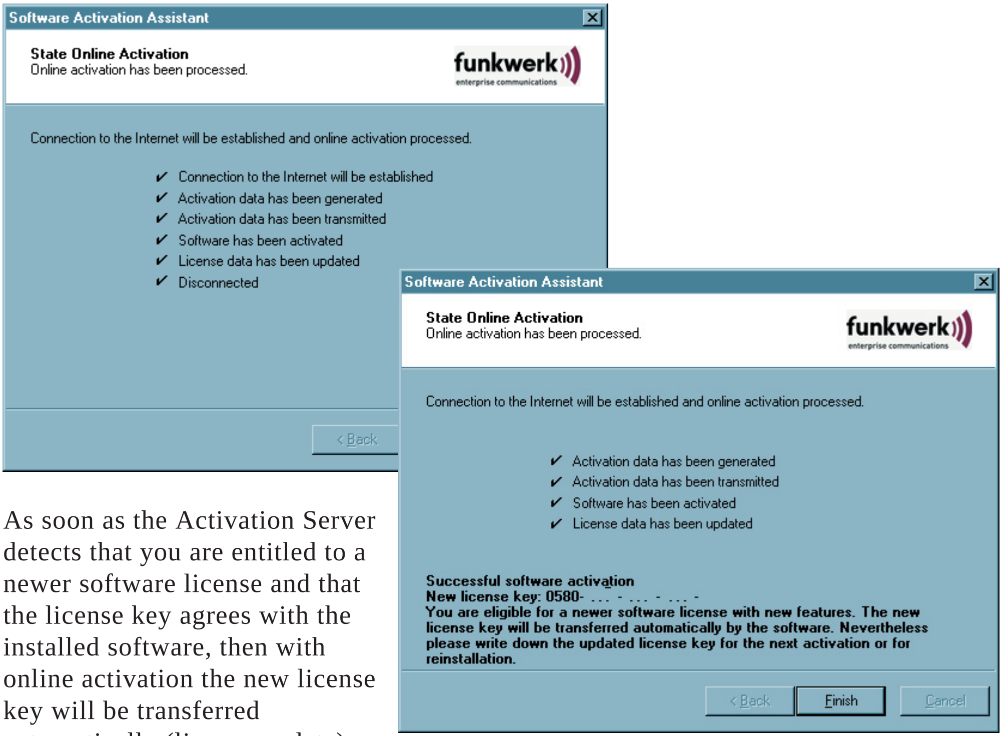
Profile : Headquarters

If the IPSec Client is used to set-up the connection on the Internet, then a suitable profile must first be established for the IPSec Client. Ensure in this regard that port 80 is released (for HTTP) if the firewall is activated. (If a proxy server will be configured in the operating system, then these settings can be transferred.)

After the profile has been selected, click on “Next”.

The Internet connection via the IPSec Client does not have to be set-up prior to activation. It is set-up automatically after the desired existing profile has been selected in the assistant for software activation, and after clicking on the "Next" button.

The software is activated automatically in the specified sequence.



Software Activation Assistant

**State Online Activation**
Online activation has been processed.

Connection to the Internet will be established and online activation processed.

- ✓ Connection to the Internet will be established
- ✓ Activation data has been generated
- ✓ Activation data has been transmitted
- ✓ Software has been activated
- ✓ License data has been updated
- ✓ Disconnected

Software Activation Assistant

**State Online Activation**
Online activation has been processed.

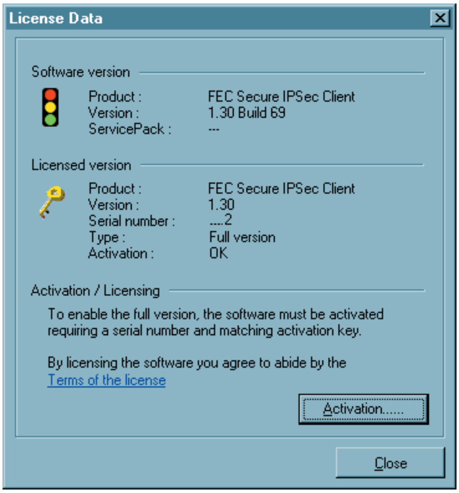
Connection to the Internet will be established and online activation processed.

- ✓ Activation data has been generated
- ✓ Activation data has been transmitted
- ✓ Software has been activated
- ✓ License data has been updated

**Successful software activation**
**New license key: 0580- . . . - . . . - . . . -**
**You are eligible for a newer software license with new features. The new license key will be transferred automatically by the software. Nevertheless please write down the updated license key for the next activation or for reinstallation.**

As soon as the Activation Server detects that you are entitled to a newer software license and that the license key agrees with the installed software, then with online activation the new license key will be transferred automatically (license update), and thus the new features of the software will be released.*

** Please see the section "Updates" at the end of this section for more information in this regard.*



License Data

Software version

| | |
|---|---|
| Product : | FEC Secure IPSec Client |
| Version : | 1.30 Build 69 |
| ServicePack : | --- |

Licensed version

| | |
|---|---|
| Product : | FEC Secure IPSec Client |
| Version : | 1.30 |
| Serial number : | ....2 |
| Type : | Full version |
| Activation : | OK |

Activation / Licensing

To enable the full version, the software must be activated requiring a serial number and matching activation key.

By licensing the software you agree to abide by the Terms of the license

After concluding the activation process, in the window for the license data you can see that you now have a correctly activated full version.

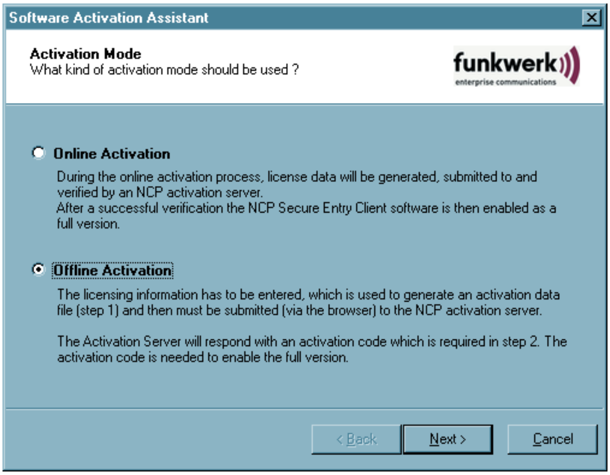
The number of the software version and of the licensed version can differ if the licensing is only valid for an older version, otherwise the licenses must be updated with a newer license key. To do this click on the "Licensing" button. See the description at the end of the offline variant for more information in this regard.

## Offline Variant

The offline variant is executed in two steps. In the first step a file that is generated after entering the license key and serial number is sent to the Web Server. The URL is:

`http://www.funkwerk-ec.com/onlineservices_en`

Then an activation key will be shown on the web site, and you must note this number in order to enter the license key in the licensing window of the Monitor menu in a second step, which can also be executed at a later point in time.


Software Activation Assistant
funkwerk enterprise communications
< Back
Next >
Cancel

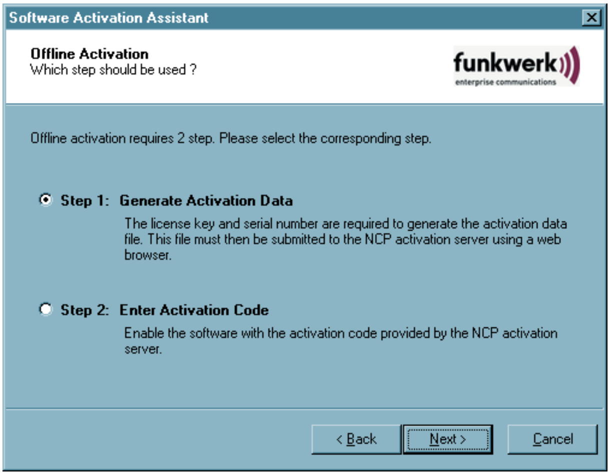
**Activation Mode**
What kind of activation mode should be used ?

○ **Online Activation**
During the online activation process, license data will be generated, submitted to and verified by an NCP activation server.
After a successful verification the NCP Secure Entry Client software is then enabled as a full version.

● **Offline Activation**
The licensing information has to be entered, which is used to generate an activation data file (step 1) and then must be submitted (via the browser) to the NCP activation server.

The Activation Server will respond with an activation code which is required in step 2. The activation code is needed to enable the full version.

Start the offline variant via the monitor menu “Help / License Data and Activation”, and select this variant in the first window of the Activation Assistant. Click on “Next”.


Software Activation Assistant
funkwerk enterprise communications
< Back
Next >
Cancel

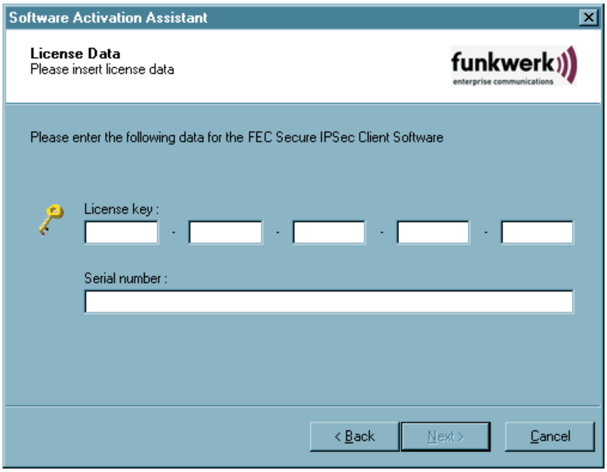
**Offline Activation**
Which step should be used ?

Offline activation requires 2 step. Please select the corresponding step.

● **Step 1: Generate Activation Data**
The license key and serial number are required to generate the activation data file. This file must then be submitted to the NCP activation server using a web browser.

○ **Step 2: Enter Activation Code**
Enable the software with the activation code provided by the NCP activation server.

In the second window of the Activation Assistant the two steps of the offline activation process are explained. The first step, creation of the activation file is selected automatically. Click on “Next”!



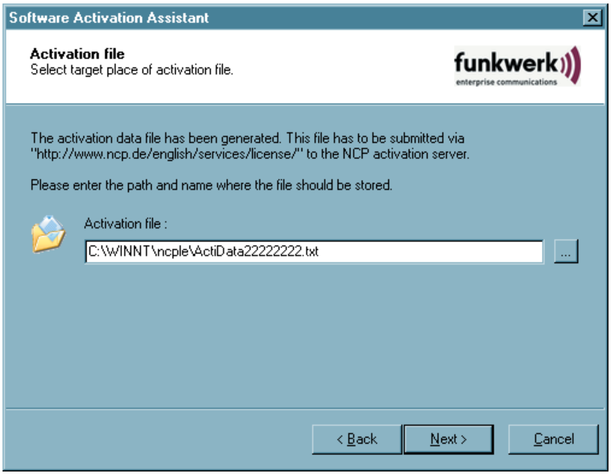
**License Data**
Please insert license data

Please enter the following data for the FEC Secure IPSec Client Software

License key : ________ - ________ - ________ - ________ - ________

Serial number : ________

In the following window enter the license data and click on “Next”.



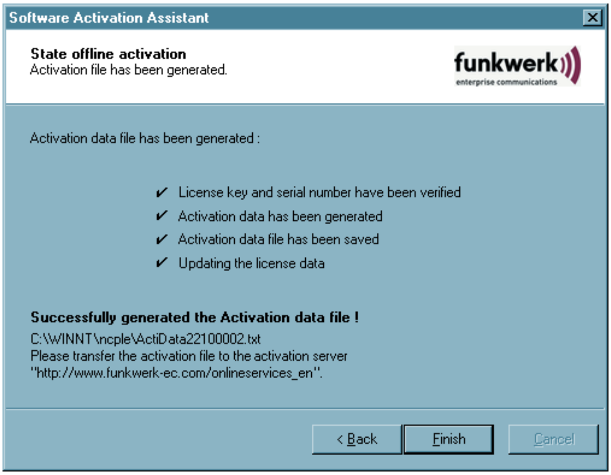
**Activation file**
Select target place of activation file.

The activation data file has been generated. This file has to be submitted via "http://www.ncp.de/english/services/license/" to the NCP activation server.

Please enter the path and name where the file should be stored.

Activation file : C:\WINNT\ncple\ActiData22222222.txt

Enter name and path for the activation file. The default is the installation directory of the software and the name ActiData.txt (with serial number).



**State offline activation**
Activation file has been generated.

Activation data file has been generated :

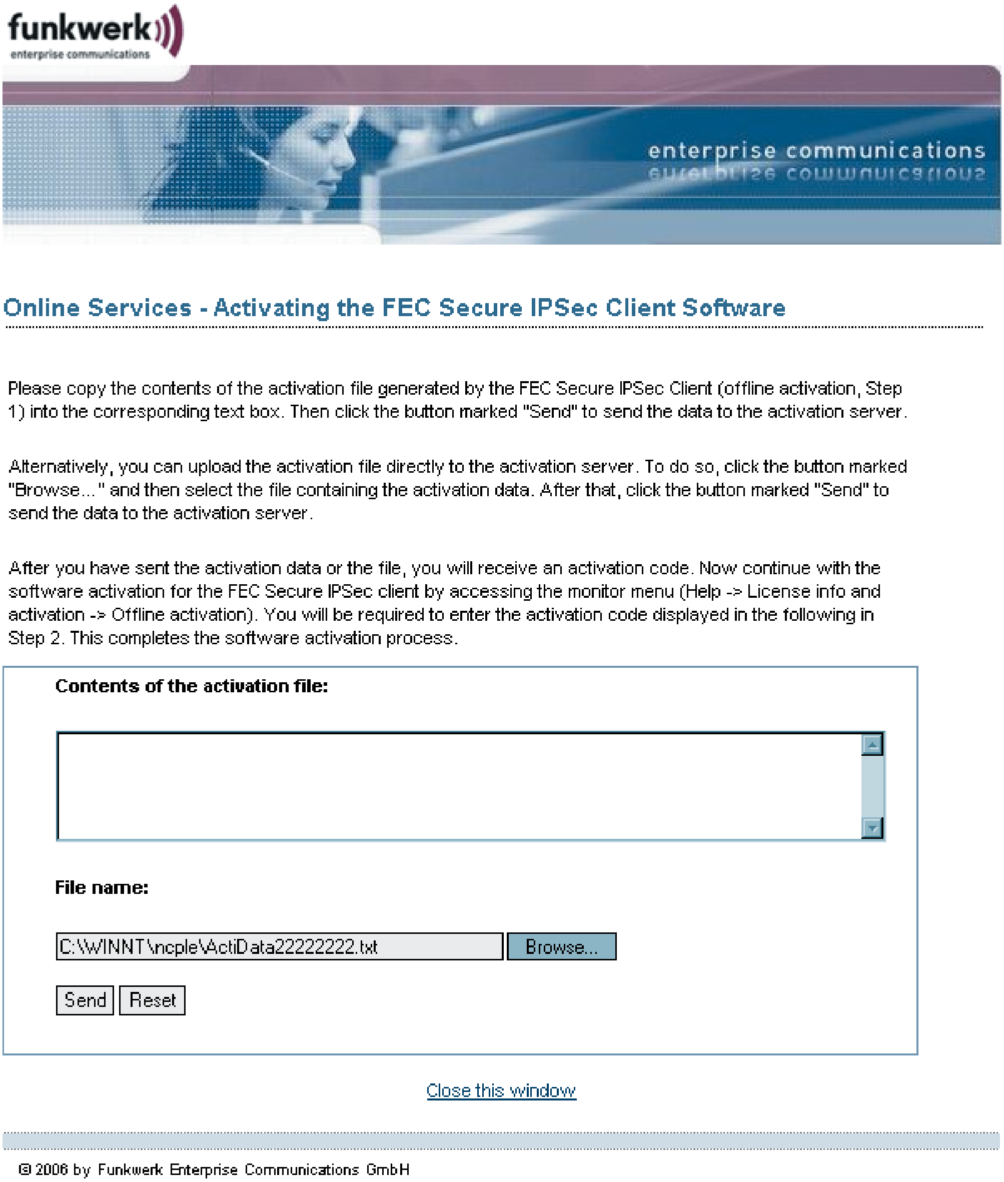
- ✓ License key and serial number have been verified
- ✓ Activation data has been generated
- ✓ Activation data file has been saved
- ✓ Updating the license data

**Successfully generated the Activation data file !**
C:\WINNT\ncple\ActiData22100002.txt
Please transfer the activation file to the activation server "http://www.funkwerk-ec.com/onlineservices_en".

Now the activation file is created and this file must be transferred to the Activation Server.

For this the following web site must be called:

`http://www.funkwerk-ec.com/onlineservices_en`



Online Services - Activating the FEC Secure IPSec Client Software

Please copy the contents of the activation file generated by the FEC Secure IPSec Client (offline activation, Step 1) into the corresponding text box. Then click the button marked "Send" to send the data to the activation server.

Alternatively, you can upload the activation file directly to the activation server. To do so, click the button marked "Browse..." and then select the file containing the activation data. After that, click the button marked "Send" to send the data to the activation server.

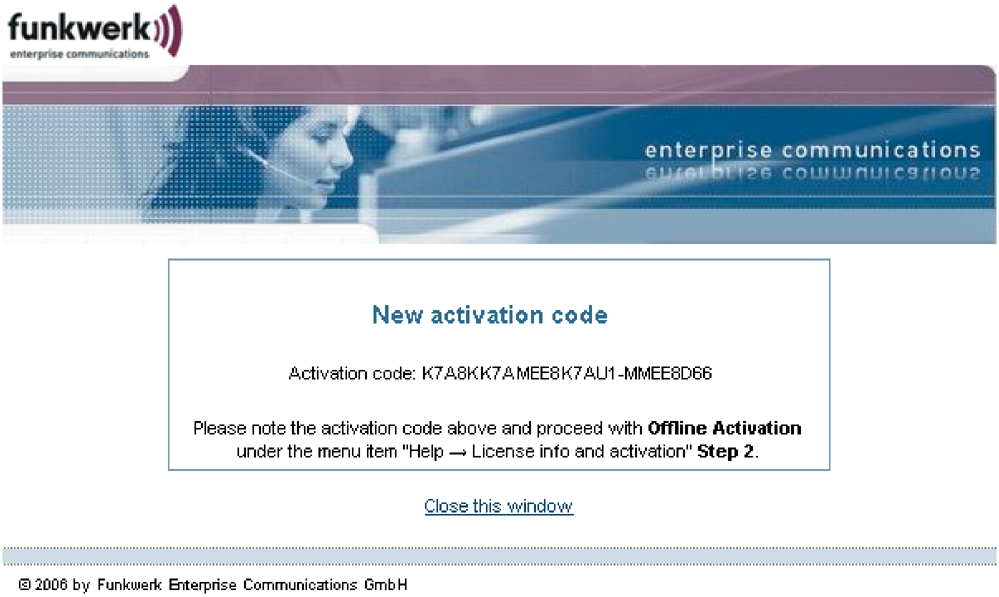
After you have sent the activation data or the file, you will receive an activation code. Now continue with the software activation for the FEC Secure IPSec client by accessing the monitor menu (Help -> License info and activation -> Offline activation). You will be required to enter the activation code displayed in the following in Step 2. This completes the software activation process.

Contents of the activation file:

File name: C:\WINNT\ncple\ActiData22222222.txt

© 2006 by Funkwerk Enterprise Communications GmbH

There are two ways to transfer the activation file to the Activation Server. Either copy the content of the activation file with Copy & Paste, after you have opened the activation file with the Notepad (ASCII editor), into the window that is open on the web site, or click on the “Browse” button and select the activation file. Click on “Send”!



New activation code

Activation code: K7A8KK7AMEE8K7AU1-MMEE8D66

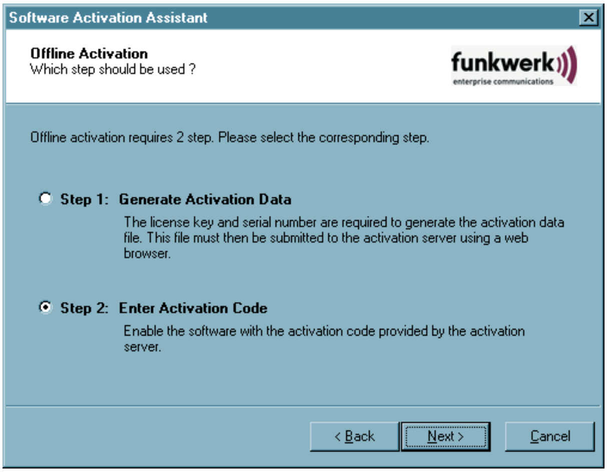
Please note the activation code above and proceed with **Offline Activation** under the menu item "Help → License info and activation" **Step 2**.

Close this window

© 2006 by Funkwerk Enterprise Communications GmbH

Then the activation code will be generated and displayed on the web site. Note the activation code and continue the activation process under the menu option “Help” / License info and activation", by executing the second step of the activation in the offline variant.

IF the Activation Server detects that you are entitled to a newer software license and that the license key agrees with the installed software, then with the online activation the new license key will be displayed automatically. If you want to activate the new features then note the new license key, conclude the activation process, and then use the new license key. (Please see the section “Scenarios” at the end of this section for more information in this regard.)



Software Activation Assistant

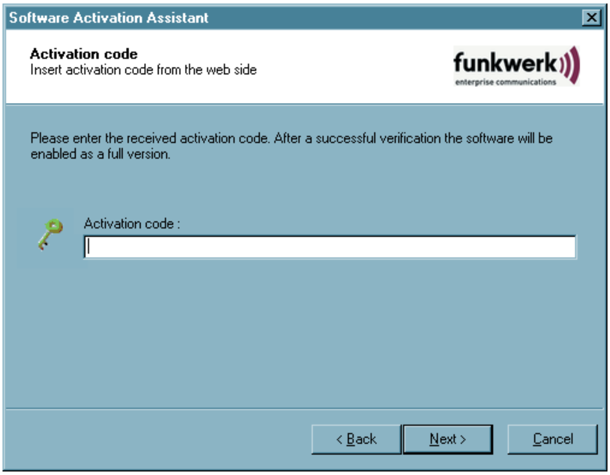
**Offline Activation**
Which step should be used ?

Offline activation requires 2 step. Please select the corresponding step.

○ **Step 1: Generate Activation Data**
The license key and serial number are required to generate the activation data file. This file must then be submitted to the activation server using a web browser.

● **Step 2: Enter Activation Code**
Enable the software with the activation code provided by the activation server.

The second step of the offline variant is triggered via the Monitor menu “Help” “License info and activation”. After the offline variant has been selected, select the second step.



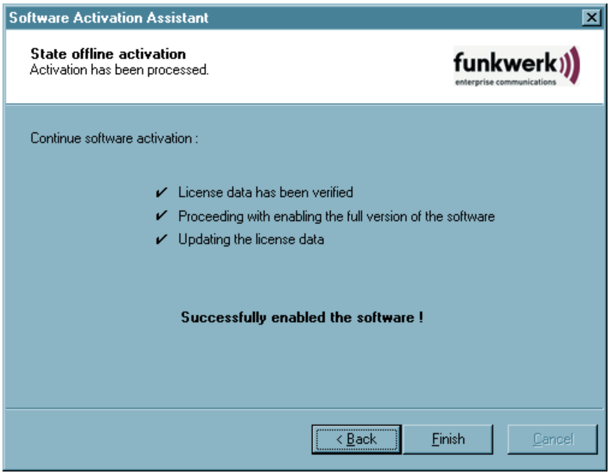
Software Activation Assistant

**Activation code**
Insert activation code from the web side

Please enter the received activation code. After a successful verification the software will be enabled as a full version.

Activation code :

An Activation Assistant window will open where you can enter the activation code. After you have entered the activation code you can click on “Next”.



Software Activation Assistant

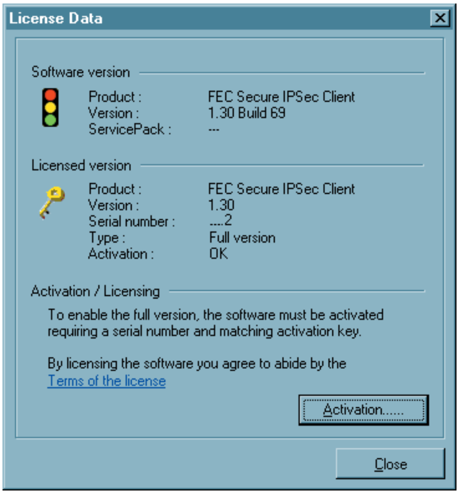
**State offline activation**
Activation has been processed.

Continue software activation :

✓ License data has been verified
✓ Proceeding with enabling the full version of the software
✓ Updating the license data

**Successfully enabled the software !**

Offline activation is concluded with the following window.



License Data

Software version

Product : FEC Secure IPSec Client
Version : 1.30 Build 69
ServicePack : ---

Licensed version

Product : FEC Secure IPSec Client
Version : 1.30
Serial number : ....2
Type : Full version
Activation : OK

Activation / Licensing

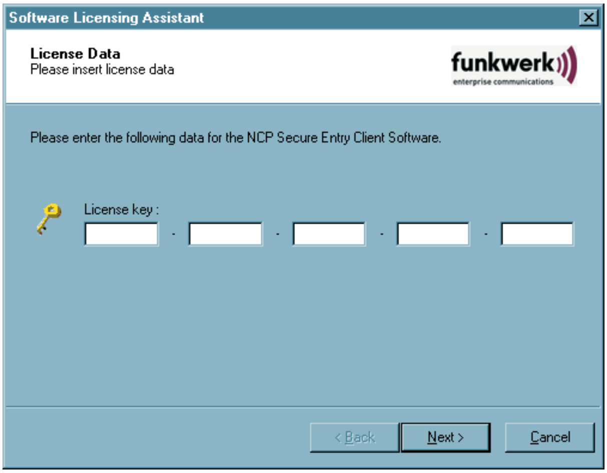
To enable the full version, the software must be activated requiring a serial number and matching activation key.

By licensing the software you agree to abide by the Terms of the license

After concluding the activation process, you will see that you now have a correctly activated full version, in the window for the license data.

The number of the software version and the number of the licensed version can differ if the licensing is only valid for an older version.

If you have received a new license key from the Activation Server during the offline activation process (see above in the display of the activation code), then enter this license key for a license update, by clicking on the “Licensing” button.



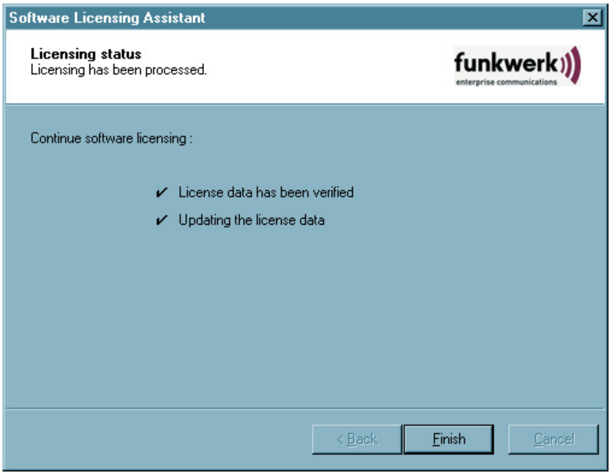
Software Licensing Assistant

**License Data**
Please insert license data

Please enter the following data for the NCP Secure Entry Client Software.

License key : _____ - _____ - _____ - _____ - _____

In next window of the Assistant, enter the new license key and click on “Next”.



Software Licensing Assistant

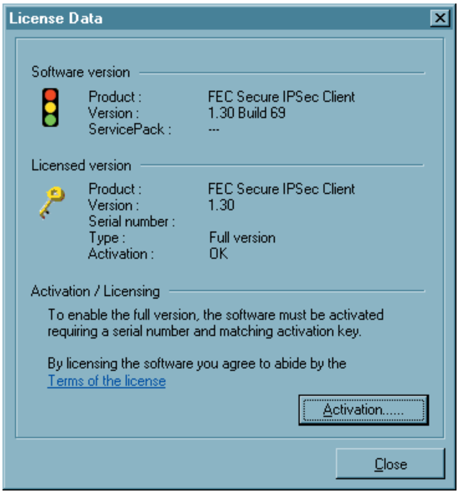
**Licensing status**
Licensing has been processed.

Continue software licensing :

✓ License data has been verified
✓ Updating the license data

The license data will be verified and then transferred.

Click on “Finished” when the verification has been concluded.



Software version

Product : FEC Secure IPSec Client
Version : 1.30 Build 69
ServicePack : ---

Licensed version

Product : FEC Secure IPSec Client
Version : 1.30
Serial number :
Type : Full version
Activation : OK

Activation / Licensing

To enable the full version, the software must be activated requiring a serial number and matching activation key.

By licensing the software you agree to abide by the Terms of the license

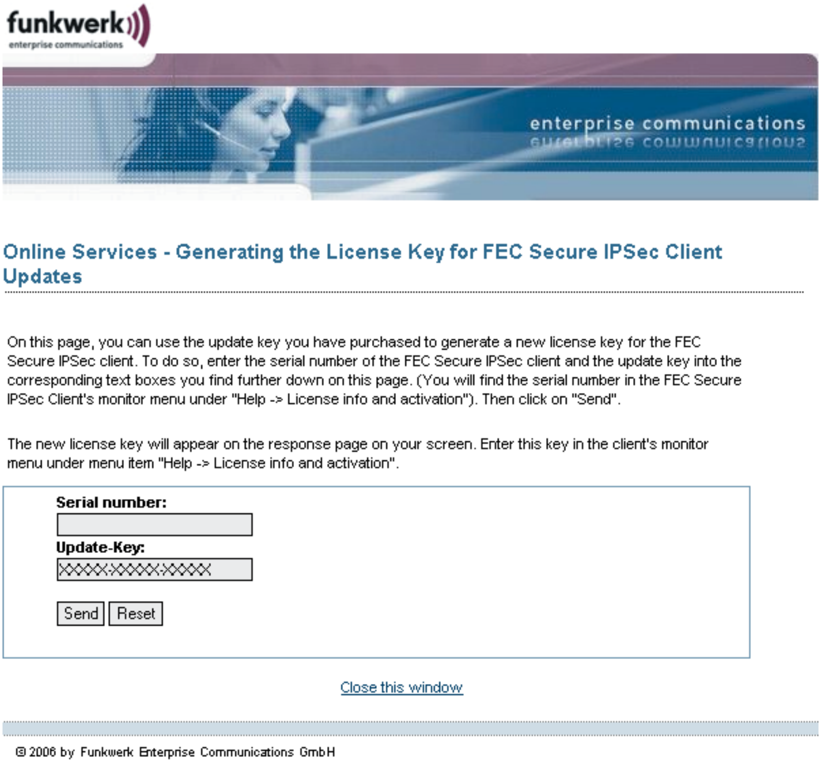
In the window with the license data you will see that the number of the software version and the number of the licensed version now agree.

## 4.7 Updates

Information on the performance range of the latest software is always available on the web site of Funkwerk Enterprise Communications:
`http://www.funkwerk-ec.com/onlineservices_en`

The software update is always available free of charge if the newer version is a service release, which contains bug fixes, an extension of hardware support and compatibility extensions. You can download this software from the website at any time.

The software update always costs money if the newer version is a major release, which is indicated by the change on the first decimal place. For example: If a version 1.11 is installed and the next software version has the number 1.30 then a software update from 1.11 to 1.30, as well as use of the new features, will cost money. The new features can be used without activation with a new license key, as soon as the new software has been installed. The new license key is generated by entering the serial number and the update key that can be purchased from the reseller. On the page shown below you can use the update key to generate a new license key for the FEC Secure IPSec Client.



Online Services - Generating the License Key for FEC Secure IPSec Client Updates

On this page, you can use the update key you have purchased to generate a new license key for the FEC Secure IPSec client. To do so, enter the serial number of the FEC Secure IPSec client and the update key into the corresponding text boxes you find further down on this page. (You will find the serial number in the FEC Secure IPSec Client's monitor menu under "Help -> License info and activation"). Then click on "Send".

The new license key will appear on the response page on your screen. Enter this key in the client's monitor menu under menu item "Help -> License info and activation".

Serial number:

Update-Key: XXXXX-XXXXX-XXXXX

© 2006 by Funkwerk Enterprise Communications GmbH

# 5. Configuration Parameters

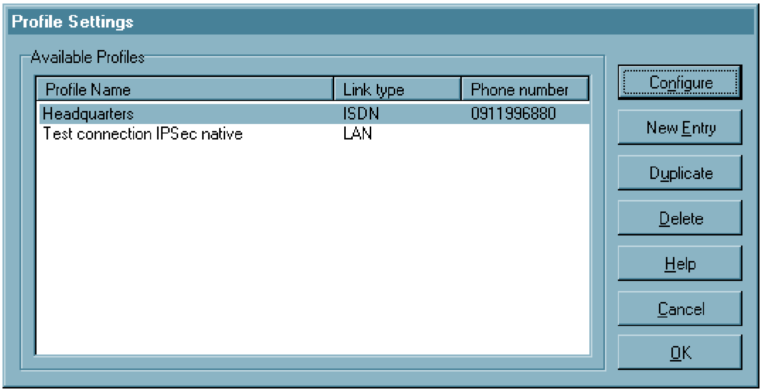
With the IPSec client you can define and configure numerous individual profiles for corresponding destinations, in accordance with your communication requirements.

In this section all parameter descriptions are listed and they are arranged in the same sequential order as displayed in the monitor.

In order to guarantee the proper functionality of your IPSec client Funkwerk Enterprise Communications offers a public VPN test access. A detailed step-by-step guidance how to use this test access and how to set the needed configurations correctly can be found on the websites at www.funkwerk-ec.com.

## 5.1 Profile Settings

Upon clicking “Profile Settings” in the monitor menu, the menu is opened with an overview of the definied profiles and the phonenumbers of the assigned destinations.



Profile Settings

Available Profiles

| Profile Name | Link type | Phone number |
|---|---|---|
| Headquarters | ISDN | 0911996880 |
| Test connection IPSec native | LAN | |

The buttons located to the right can be used to add, remove, copy and modify the entries of the profiles.

In order to define a new profile click on “Profile Settings” in the monitor menu under “Configuration”. Upon doing so the menu opens displaying any defined profiles. Click on “New Entry”. Enabeling the “Configuration Assistant”, which assists in the creation of a new profile definition. All other parameters will be assigned default values.

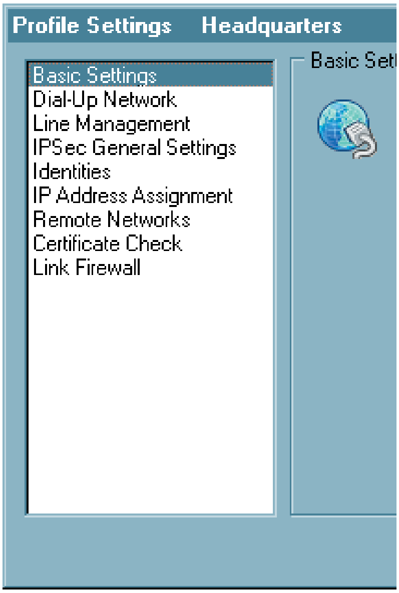
To edit these default values, in order to fulfill the requirements of the profile, select the desired profile and then “Configure” to gain access to the individual parameters. (See → Profile Settings, Configure)

In order to duplicate a profile click on “Duplicate”

In order to delete a profile click on “Delete”.

## Parameterfolders:

Parameters which specify the connection via the profile to the destinations, are found in the configuration folders. The name of the profile appears in the titel bar (see → Profile Settings, Configure). Within the configuration folder the connection parameters pretaining to this profile can be configured.



Profile Settings Headquarters

Basic Settings
Dial-Up Network
Line Management
IPSec General Settings
Identities
IP Address Assignment
Remote Networks
Certificate Check
Link Firewall

1 ***Basic Settings***

2 ***Dial-Up Network***

3 ***HTTP Logon***

4 ***Modem***

5 ***Line Management***

6 ***IPSec General Settings***

7 ***Advanced IPSec Settings***

8 ***Identities***

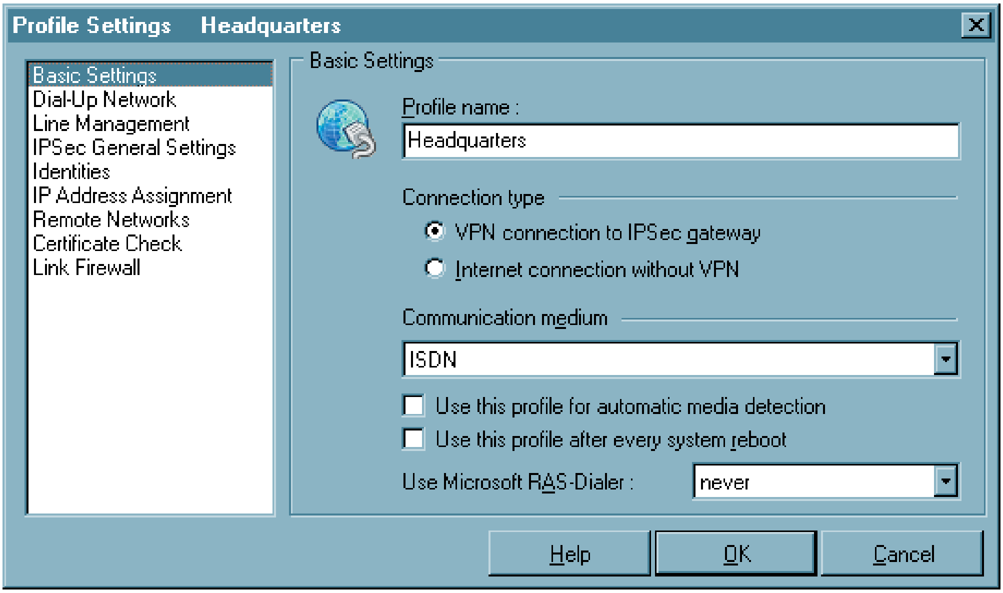
9 ***IP Address Assignment***

10 ***Remote Networks***

11 ***Certificate Check***

12 ***Link Firewall***

### 5.1.1 Basic Settings



Basic Settings

Profile name : Headquarters

Connection type

● VPN connection to IPSec gateway

○ Internet connection without VPN

Communication medium

ISDN

□ Use this profile for automatic media detection

□ Use this profile after every system reboot

Use Microsoft RAS-Dialer : never

In the folder “General” enter “Profile name”, the “Communication type” and the “Communication medium” you wish to use and is available to Windows.

*Parameters:*

- □ Profil name
- □ Connection type
- □ Communication medium
- □ Use this entry for automatic media detection
- □ Use Microsoft RAS-Dialer
- □ Use this phonebook entry after every system reboot

## Profile name

When entering new profiles you should enter a unique name for each profile. The profile name may include any character or number as desired up to a maximum of 39 characters (including spaces).

## Connection type

Alternatively there are two connection types available with the IPSec client:

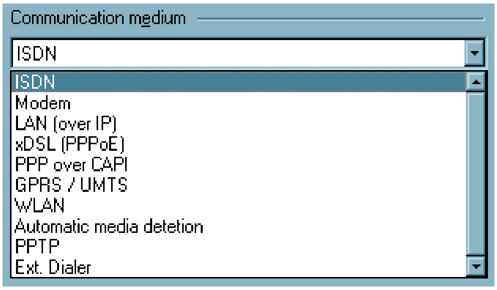
***VPN to IPSec correspondent:***

In this case you dial into the corporate network (or into the gateway) with the IPSec client. A VPN tunnel is set up for this.

***Internet connection without VPN:***

In this case only use the IPSec client for dialing into the Internet. Here the Network Address Translation (IPNAT) continues to be used in background so that only those data packets are accepted that have been requested.

## Communication medium



Communication medium

ISDN

You can select the communication medium for each profile, provided that you have the required device installed on your PC and recognized by Windows.

***ISDN:***

Hardware: ISDN device;
Network: ISDN;
Remote destination: appropriate ISDN support;

***Modem:***

Hardware: Asynchronous modem (PCMCIA modem, GSM adapter)
with COM Port support;
Network: PSTN (also GSM);
Remote destination: Modem or ISDN device with digital modem;

### *LAN (over IP)*

Hardware: LAN adapter;
Networks: Ethernet or Token Ring based LAN;

### *xDSL (PPPoE)*

Hardware: Ethernet adapter;
Networks: Broadband (e.g. ADSL);
Remote destination: Access Router in the xDSL;

### *xDSL (AVM – PPP over CAPI)*

If an AVM Fritz DSL card is to be used then this communication medium may be selected. AVM specific initialization strings may be entered in the field “Destination Phone Number” (“Dial-Up Network” group) for the connection. It is recommended to use the standard setting “xDSL (PPPoE)” with Windows operating systems as this provides direct communication over the network interfaces. No additional network card is necessary with the AVM Fritz! DSL card.

Networks: Broadband (e.g. ADSL);
Remote Destination: Access Router in the xDSL

### *GPRS / UMTS*

If a mobile (cellular) telephones is to be used (GRPS) then this communication medium may be selected. Note the description under “Installation Prerequisites” to “Analog modem”.

### *PPTP*

Microsoft Point-to-Point Tunnel Protocol;
Hardware: Ethernet-Adapter, xDSL Modem;
Networka: xDSL;
Remote destinations: Access Router in the xDSL;

### WLAN

Hardware: WLAN adapter;
Networks: WLAN;
Other sides: Access Point;

Under Windows 2000/XP/Vista the WLAN adapter can be operated with the connection type “WLAN”. In the monitor menu the special “WLAN settings” menu option is displayed where the access data for the wireless network can be saved in a profile. If this “WLAN configuration” is activated, then the management tool of the WLAN card must be deactivated. (Alternatively the management tool of the WLAN card can also be used; in this case the WLAN configuration in the Monitor menu must be deactivated.)

If the connection type WLAN is set for the destination system in the phonebook, then under the graphic field of the Client Monitor an additional area is shown where field strength and the WLAN network are displayed (see -> WLAN Settings).

### Ext. Dialer

If this connection type is set, then a pre-configured EXE file (e.g. the iPass dialer) will start when you press the “Connect” button. This EXE file must first set-up the connection to the Internet and then trigger the set-up of the VPN connection to the client via “RWSCMD / connect”. In this case our dialer works in LAN mode.

This connection type will only work with manual connection setup.

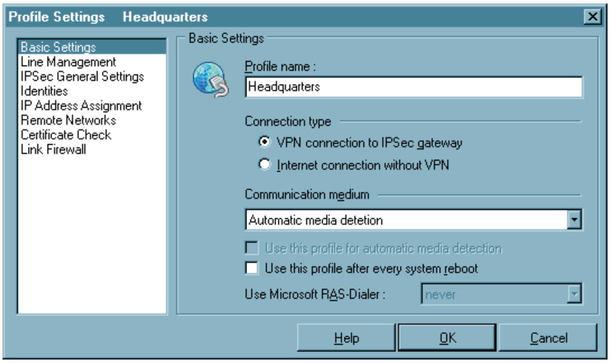
With connection type “Ext. Dialer” in order not save yourself the trouble of entering the complete path for the dialer in the DAT file, alternatively the path can be read out of the registry. Two new INI entries have been created to detect the path for the dialer. Under “DialerExec” the EXE name of the dialer is all that must still be entered.

Example for Ipass:
The installation path of the Ipass dialer, “Software\Ipass\iPassConnectEngine” is located in the registry, under “InstallPath”. The EXE file must be entered manually:

```
DialerInstallPathKey   = Software\Ipass\iPassConnectEngine
DialerInstallPathValue = InstallPath
DialerExec             = IPassConnectGUI.exe
Caption                = iPassConnect
```

### *Automatic media detection*

If different connection types are used in alternation, such as modem and ISDN, then manual selection of the destination system with the respectively available connection medium is not necessary, if a destination system has been configured for “Automatic media detection”, and in each case a destination system with the alternatively available connection types, such as modem and ISDN has been selected.


Profile Settings Headquarters

Basic Settings
Line Management
IPSec General Settings
Identities
IP Address Assignment
Remote Networks
Certificate Check
Link Firewall

Basic Settings

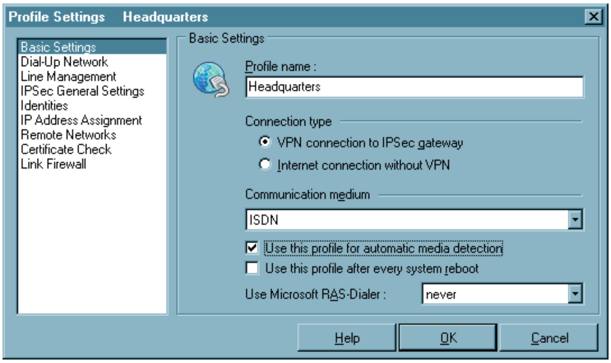
Profile name : Headquarters

Connection type
● VPN connection to IPSec gateway
○ Internet connection without VPN

Communication medium: Automatic media detetion

□ Use this profile for automatic media detection
□ Use this profile after every system reboot

Use Microsoft RAS-Dialer : never


Profile Settings Headquarters

Basic Settings
Dial-Up Network
Line Management
IPSec General Settings
Identities
IP Address Assignment
Remote Networks
Certificate Check
Link Firewall

Basic Settings

Profile name : Headquarters

Connection type
● VPN connection to IPSec gateway
○ Internet connection without VPN

Communication medium: ISDN

☑ Use this profile for automatic media detection
□ Use this profile after every system reboot

Use Microsoft RAS-Dialer : never

In this regard ensure that the destination system with automatic media detection is configured with all parameters necessary for the connection to the VPN Gateway (particularly the IP address of the VPN gateway), on the other hand the destination systems with the alternative connection types must be configured in such a manner that each desired connection type (possibly the modem parameters as well) is set and the function “Entry for automatic media detection” is activated.

In addition for the respective connection medium the input data to the ISP must be set in the “Network dial-in parameter field.

For connection setup the Client automatically detects which connection types are currently available and selects the fastest of these, and if there are multiple alternative transmission paths it automatically selects the fastest. The connection type priority is specified in the following sequence in a search routine: 1. LAN, 2. WLAN, 3. DSL, 4. UMTS/GPRS, 5. ISDN, 6. MODEM. The incoming data for the connection for the ISP are transferred from the phonebook entries that have been configured for automatic media detection.

## ■ Use this profile after every system reboot

Normally after a restart the Client Monitor opens with the last profile used. If this function is activated, then the profile referred to here is loaded after a system re-start, regardless of which profile was last used.

In order to setup a connection, this profile can also be selected manually. assumed that the VPN parameters have been configured correctly.

- **Use this phonebook entry after every system reboot**

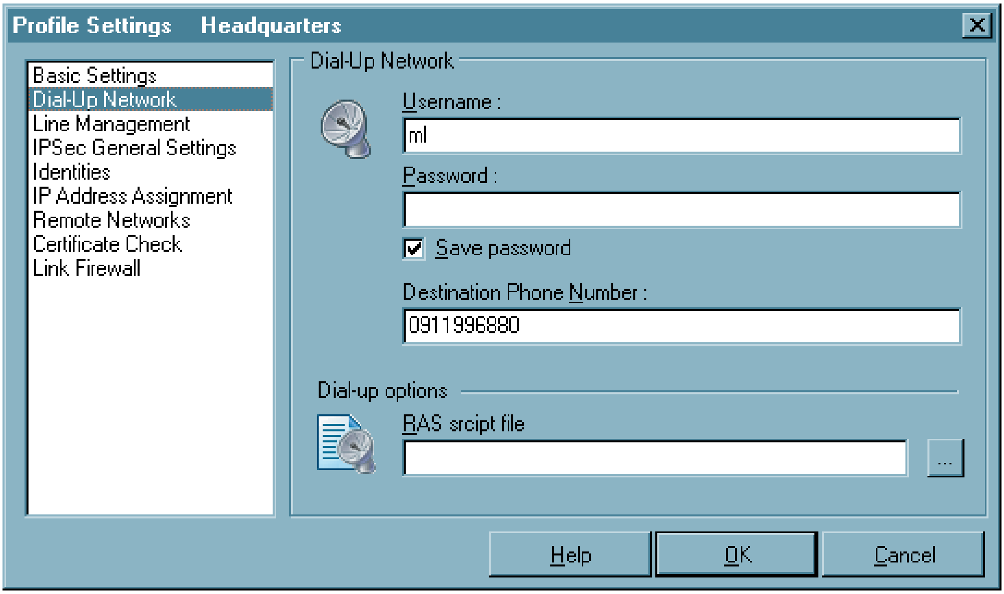
Normally after a restart the Client Monitor opens with the last profile used. If this function is activated, then the profile referred to here is loaded after a system re-start, regardless of which profile was last used.

- **Use Microsoft RAS-Dialer**

Microsoft's RAS Dial-Up Networking can be used for dialing in to an ISP. This is necessary when then access point requires a dial-up script. The RAS Dial-Up Networking supports this script. The option "Use Microsoft RAS Dialer" is located in the Client's Phonebook under Destination. The RAS Script file including its path and name can be entered in the parameter folder "Dial-Up Network" (see -> RAS Script file).

With the "Never" setting the NCP Dialer is used exclusively to dial-in. If the data communications dialer will be used "only for script dial-in", then select this option. For a dial-in point that does not require a script, the system automatically switches to the NCP Dialer. If the data communications dialer will always be used, then the appropriate setting must be made.

## 5.1.2 Dial-Up Network



Profile Settings Headquarters

Basic Settings
Dial-Up Network
Line Management
IPSec General Settings
Identities
IP Address Assignment
Remote Networks
Certificate Check
Link Firewall

Dial-Up Network

Username : ml

Password :

☑ Save password

Destination Phone Number : 0911996880

Dial-up options

RAS srcipt file

This folder contains the parameters Username and Password, which are needed to properly identify you when accessing the destination. From a technical standpoint these two items are included as part of the PPP negotiation to the ISP (Internet Service Provider). If the Communication media “LAN over IP” has been selected, then this folder will not appear since these parameters are not relevant for LAN operation.

***Parameters:***

- □ Username
- □ Password
- □ Save password
- □ Destination phone number
- □ Alternate destination phone numbers
- □ RAS script file

## Username

This parameter is used to identify yourself to the remote Network Access System (NAS) when establishing a connection to your destination, or alternatively to your Internet Service Provider (ISP) if you are communicating across the Internet. The username may consist of up to 254 characters. Normally the username will be assigned to you by your destination (e.g. your company Headquarters, User Help Desk, Internet Service Provider, etc.), because it must be supported and accepted by the NAS, Radius or LDAP server for authentication purposes.

## Password

This parameter is used for identifying yourself to your Internet Service Provider (ISP) if the Internet is used. The password can include up to 128 characters. Normally the password will be assigned to you by your destination (e.g. your company Headquarters, User Help Desk, Internet Service Provider, etc.), because it must be supported and accepted by the NAS, RADIUS or LDAP Server for authentication purposes.

Upon entering your password all characters will be displayed as an asterisk (*) in order to keep them from being detected by someone else. Therefore it is necessary to be very careful that you enter your password exactly the way in which it was assigned to you (also with regards to the use of upper case and lower case characters).

If the user chooses not to enter and save the password he will be prompted to manually enter it with every connection attempt.

## Save password

This parameter should be activated when it is desired that the Password (if entered) is to be stored. Otherwise it will be removed from memory when (re)booting the PC or changing the profile. Default is the activated function.

Important: For security purposes you must be aware that should some unauthorized person use your PC, they will be able to use your password. Therefore caution should be used when your PC is left unattended.

## Destination phone number

You must define a phone number for those destinations using ISDN/PSTN/GSM otherwise the Client will not be able to dial up and establish a connection to the destination or ISP. The phone number must be entered exactly in the same manner as if you were dialing the number from a telephone. You must enter any required prefixes, country codes, area codes, extensions, etc. etc.

In order to acquire an outside line when communicating via a PBX it is necessary to define an “Outside Line Prefix” (see → Outside Line Prefix) in the monitor menu “Configuration”.

*Example: Making a connection from Germany to UK:*
00 (gets you an international line when dialing from Germany)
44 (this is the country code for United Kingdom)
171 (prefix for London)
1234567 (the number you want to reach)

The following number will be used by the Client for dialing purposes and it will be displayed in the Phonebook as follows: 00441711234567.
The destination phonenumber may include up to 30 characters.

## Alternate destination phone numbers

It could be that the destination you want to communicate with uses a Network Access System (NAS) that is equipped with multiple phone numbers. If this is the case, then it may be useful to enter more than one phone number for the destination if for example the primary Destination Phone Number is occupied. The alternate destination phone number(s) can be entered following the primary destination phone number and separated by a colon (:).

A maximum of 30 digits can be entered in the Destination phone number field. The IPSec client supports a maximum of 8 alternate phone numbers.

Example: 00441711234567:00441719876543

The first number is the primary Destination Phone Number and will always be dialed first. The second number is the Alternate Destination phone number and will be dialed when a connection to the primary number is not possible.

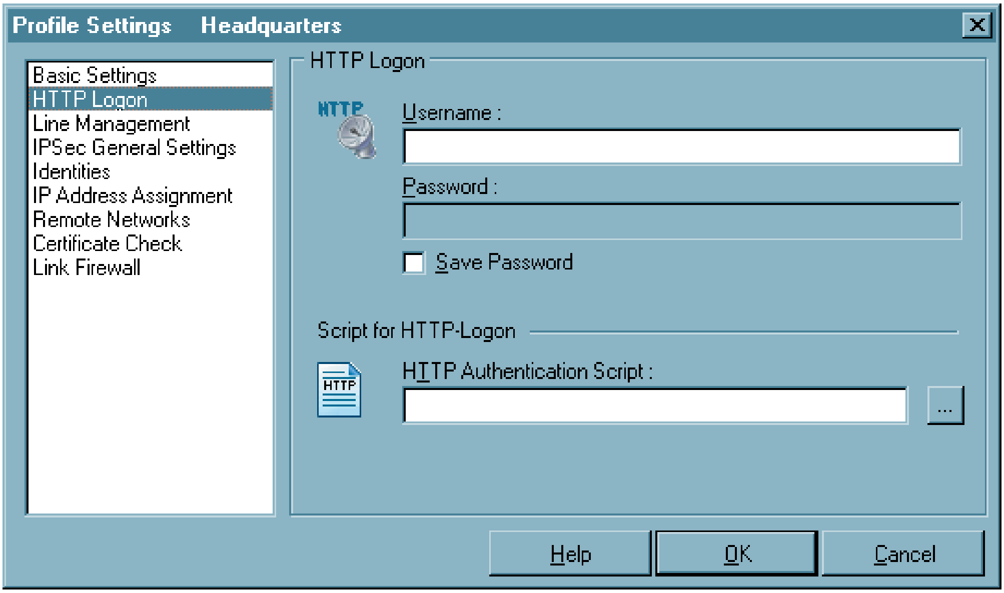
Important: This will only work if the protocol settings associated with alternate Destination phone number are the same as the primary Destination phone number

## RAS script file

If Microsoft’s RAS Dial-Up networking is to be used, the RAS script file including its path and name must be entered.

(See → Basic Settings, Use Micosoft RAS-Dialer)

### 5.1.3 HTTP Logon



The automatic HTTP logon can be executed automatically with the settings in this parameter field. Centrally created logon scripts and the stored logon data can be transferred from the access point hotspot without opening a browser window.

Please note that there are charges associated with the connection via a HotSpot operator. You must agree to the terms and conditions of the HotSpot operator in order to set up the connection.

***Parameters:***

□ User name | HTTP Logon

□ Password | HTTP Logon

□ Save Password | HTTP Logon

□ HTTP Authentication Script | HTTP Logon

The logon at the HotSpot is automated with these data. This is executed as follows; for a connection setup to the Access Point an HTTP redirect to the Client with a website for logon is executed from the Access Point. Instead of a browser start for HTTP authentication, the authentication occurs automatically in background, with the entries made here.

For script driven logon you can use a script from the installation directory
`<install>\scripts\samples`
and you can modify it for other HotSpots

For the WLAN connection type the authentication data for the HotSpot are transferred from the WLAN settings.

### Username | HTTP Logon

This is the user name that you have obtained from your HotSpot operator.

### Password | HTTP Logon

This is the password that you have obtained from your HotSpot operator. The password is concealed with asterisks (*) when entered.

### Save Password | HTTP Logon

After the password has been entered it can be saved

### HTTP Authentication Script | HTTP Logon

Click on the Browse button [...] to select the saved logon script.

Incoming certificates can be verified with HTTP authentication. For this the variable CACERTDIR must have been set in the script. In addition WEB server certificate content can also be verified. Additional variables are available in this regard:

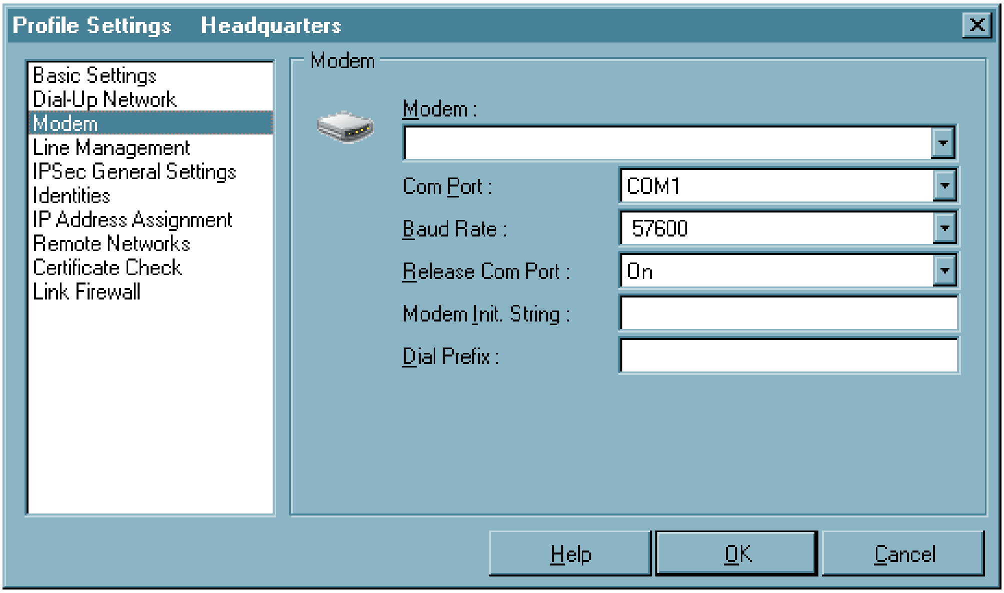
`CACERTVERIFY_SUBJECT`
Checks the content of the subject (e.g. cn=WEB Server 1)

`CACERTVERIFY_ISSUER`
Checks the content of the issuer

`CACERTVERIFY_FINGERPRINT`
Checks the MD5 fingerprint of the issuer certificate

If the content of the variable does not agree with the entered certificate, then the SSL connection will not be established and a log message will be output in the Monitor.

### 5.1.4 Modem



Modem :

Com Port : COM1

Baud Rate : 57600

Release Com Port : On

Modem Init. String :

Dial Prefix :

This parameter field is only displayed if your selected communication medium is “Modem”. All necessary parameters for this link type are listed here.

*Parameters:*

□ Modem

□ COM Port

□ Baud Rate

□ Release COM Port

□ Modem Init. String

□ Dial Prefix

□ APN

□ SIM PIN

### ■ Modem

This field will view the modem(s) installed on your PC. Select the required modem.

Selecting a Modem causes the corresponding COM Port and Modem Init. String for this Modem to be automatically entered in the appropriate Phonebook Link Definition parameter fields.

All other parameters for this communication media can be configured in the control panel of your PC.

Note: We recommend that you install your Modem prior to installing and configuring the Secure Client. In this case the Secure Client will automatically use the driver and values installed with the Modem.

### ■ COM Port

In this field you can define the COM Port to be used by your Modem. Normally when you install a Modem under Windows the COM Port will be defined during the installation of the Modem. If you then select Modem under the Link Definition field, the COM Port already assigned to the Modem will be automatically enter in the COM Port field.

Note: We recommend that you first select the appropriate modem in the field “Modem”. Thereafter the Secure Client will automatically import and use the pre-defined COM Port.

### ■ Baud Rate

Baud Rate refers to the transmission rate between the PC’s Com Port and the Modem. If for example your Modem is able to transmit data at 14.4 Kbits, then the Baud Rate should be set to 19200 (factory default setting).

The following rates may be selected:
1200, 2400, 4800, 9600, 19200, 38400, 57600 und 115200

### ■ Release Com Port

If you are using an analog modem for communications in conjunction with the IPSec client, it may be desirable upon conclusion of each communications session to release the Com Port for other communication applications (e.g. Fax, Answering Machine). As long as this parameter is set to “OFF” (factory default setting), the Com Port will be assigned exclusively to the Secure Client, and no other application will be able to use it.

## Modem Init. String

AT commands can be required, depending on the mobile (cellular) phone or modem and the link mode. For these commands, refer to the respective user manual or obtain the information from your telco or provider. Complete each command with <cr> (Carriage Return).

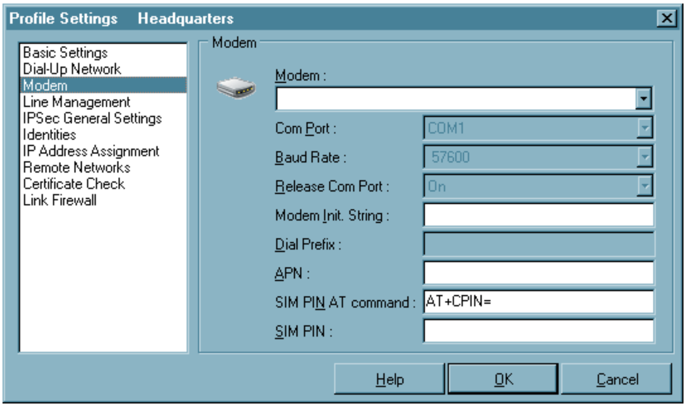
## Dial Prefix

This field is optional. Normally it will not be necessary to enter anything in this field, provided that your modem has been properly installed and is available to the client as a standard communications driver. However, if it is desirable to enter a “Dial Prefix”, refer to your Modem manual for more detailed information.

Following are some examples of Dial Prefixes:
ATDT
ATDP
ATDI
ATDX

## APN

The APN (Access Point Name) is required for the GPRS and UMTS dial-in. You obtain this name from your provider. The APN is used particularly for administrative purposes.

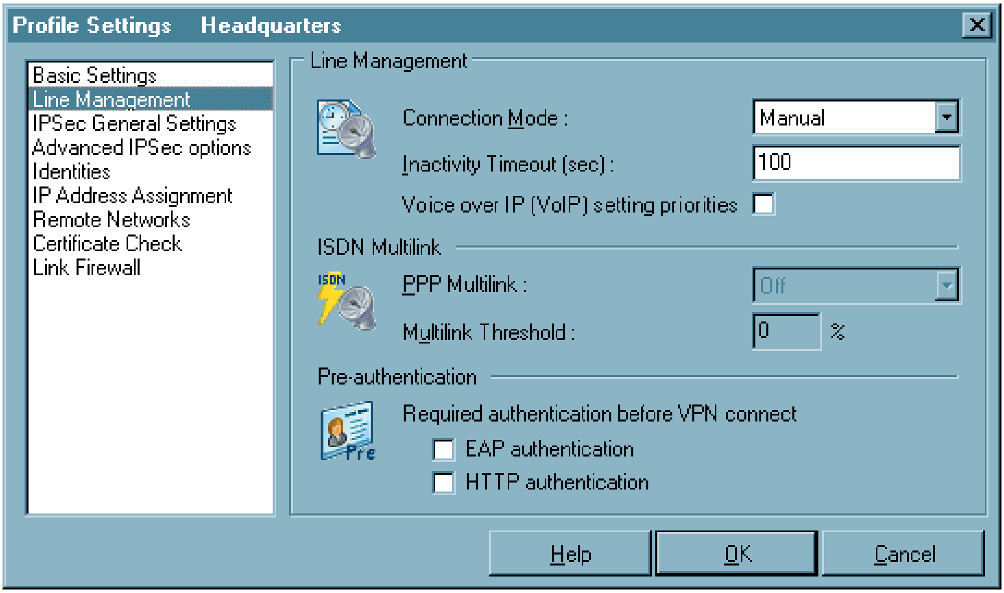


Modem :
Com Port : COM1
Baud Rate : 57600
Release Com Port : On
Modem Init. String :
Dial Prefix :
APN :
SIM PIN AT command : AT+CPIN=
SIM PIN :

## SIM PIN

If you use an SIM plug-in card for GPRS (UMTS also), then enter the PIN for this card here. If you use a mobile phone, then this PIN must be entered on the mobile phone.

## 5.1.5 Line Management



Profile Settings Headquarters

- Basic Settings
- Line Management
- IPSec General Settings
- Advanced IPSec options
- Identities
- IP Address Assignment
- Remote Networks
- Certificate Check
- Link Firewall

Line Management

Connection Mode : Manual

Inactivity Timeout (sec) : 100

Voice over IP (VoIP) setting priorities □

ISDN Multilink

PPP Multilink : Off

Multilink Threshold : 0 %

Pre-authentication

Required authentication before VPN connect

□ EAP authentication

□ HTTP authentication

In the “Line Management” you can define the Connection Mode as well as Timeout values used for automatically disconnecting the link.

If the client is using the communication medium ISDN you can activate channel bundling in this folder. In order for channel bundling to work requires that your PC be equipped with a communications device that supports multiple ISDN B-Channels. It is also necessary that the Network Access System that you are communicating with supports the same number of channels.
The required authentication before VPN connect is assigned by the network of the hotspot operator.

***Parameters:***

□ Connection Mode

□ Inactivity Timeout

□ Voice over IP (VoIP) setting priorities

□ PPP Multilink

□ Multilink Threshold

□ EAP Authentication

□ HTTPAuthentication

## Connection Mode

You can define how the client builds a link via the profile to the destination. There are three Modes to select from:

automatic = (default) Means that the Secure Client will automatically activate a connection in accordance with your application program requirements to the profile setting. A disconnect also occurs automatically, provided that the Inactivity Timeout parameter is set to any value other then zero.

manual = Means that you must manually activate a connection. Disconnect will be activated by the Inactivity Timeout provided that this parameter has been set to any value other the zero (0).

variable = When this mode is selected, the connection must be established "manually". Subsequently, the mode adapts according to the manner in which the connection was terminated:
– If the connection was terminated as a result of a timeout, then the following connection will be automatically initiated as required.
– If the connection was terminated manually, then the following connection must also be established manually.

Important: When setting the Connection Mode to "Manual" you should also set the Inactivity Timeout parameter to any value other than zero (0) in order for an automatic disconnect to be made. Otherwise you may incur unnecessary communication costs if a Disconnect is not executed.

## Inactivity Timeout

This parameter is for setting the time delay to be used following the last transmission of data before automatically executing disconnect. Time is expressed in seconds. Possible settings are from 1 to 65356 seconds. The default value is "100"..

If your communications connection (regardless of link type) receives a Charge/Unit impulse from the network provider, this will be used by the Secure Client Timeout feature for achieving an optimal disconnect time with regard to the value set in the Inactivity Timeout. This optimized timeout feature will further help to reduce communication costs.

Note: In order for the Inactivity Timeout to be activated it is necessary to enter any value from 1 to 65356. The value "0" (zero) means that no automatic timeout (disconnect) will be executed. When the Inactivity Timeout is set to "0" (zero) you must manually execute Disconnect.

Important: The Inactivity Timer only begins counting down after the last data transmission and after any communications handshaking has stopped.

### Voice over IP (VoIP) setting priorities

If this Client is used for communication with Voice over IP, then this function should be activated in order to send and receive the voice data without delay and without distortion.

### PPP Multilink

When using PPP Multilink the Secure Client can bundle up to 8 ISDN B-Channels, therefore in order to take advantage of this your PC must be equipped with the necessary number of ISDN BRI (Basic Rate Interface) ports.

In order for Multilink to work requires that your PC be equipped with an ISDN device that supports multiple ISDN B-Channels. It is also necessary that the Network Access System (NAS) that you are communicating with support Multilink operation. When using PPP Multilink additional costs will be incurred for each B-Channel used.

This parameter defines how additional links will be added if requested. There are 3 possible settings:

| | |
|---|---|
| off | (default setting) |
| Tx | (links are added according to the bit rate demanded by the transmitter) |
| Rx | (links are added according to the bit rate demanded by the receiver) |
| TxRx | (links are added according to the bit rate demanded by both transmitter and receiver. |

### Multilink Threshold

This parameter tells the client the bit rate (as a percent of the current bit rate) at which a new link (B-Channel) is to be added. Possible settings are from 1 to 100. The default setting is “20". The Threshold setting is common to both transmitter and receiver.

In order for this value to be activated it is necessary to have Tx, Rx or TxRx under PPP Multilink selected.

Important: In order for PPP Multilink to work it must be supported by the destination’s Network Access System.+

## EAP authentication

If the Client must authenticate itself at the Access Point (HotSpot) with EAP (Extensible Authentication Protocol), then this function must be activated. It means that for this destination system the EAP configuration in the Monitor menu under “EAP options” will be used.

Please note that the EAP configuration in the monitor menu is valid for all destination systems and must be switched active if this link-specific setting will be effective.

EAP is used if an Access Point is used for the wireless LAN that is 802.1x capable, and it demands a corresponding authentication. This can prevent unauthorized users from plugging into the LAN via the hardware interface.

After configuration of the EAP a status display must appear in the graphic field of the Monitor. If this is not the case then the EAP configuration must be switched active in the Monitor menu. Double click on the EAP icon to reset the EAP. Then the EAP is renegotiated.

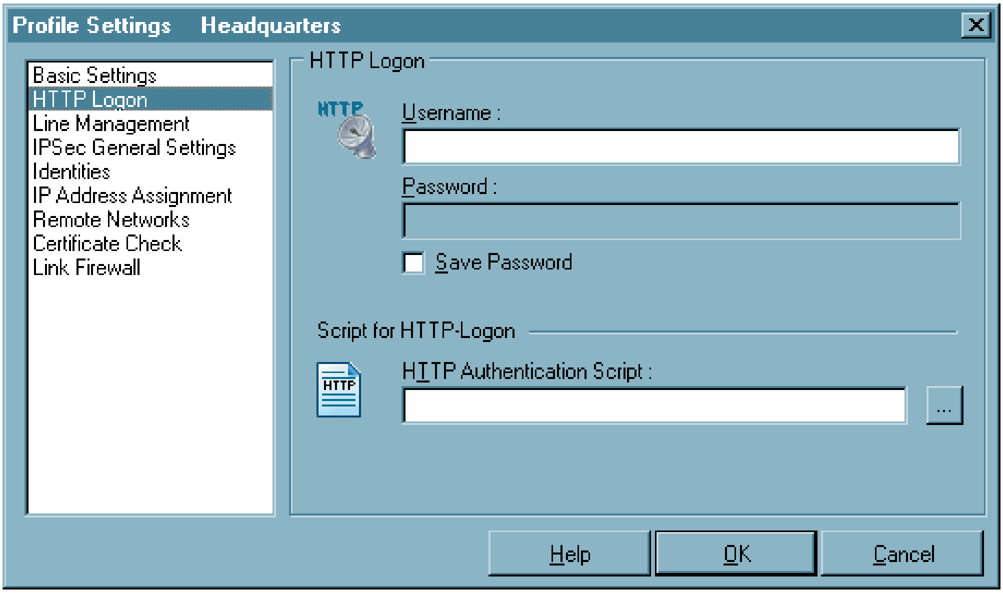
## HTTP authentication

This function must be activated for automatic HTTP authentication at the access point (HotSpot).

For this an additional parameter field “HTTP Logon” must be switched on in the phonebook, where the authentication data can be entered thereafter (see -> Next parameter field).

The HTTP logon is not switched on in the phonebook for a link with the connection type WLAN! Instead, activation of this function causes the authentication data from the WLAN settings in the Monitor menu to be used for this destination system.

## 5.1.6 IPSec General Settings



In this parameter folder you enter the IP address of the gateway. Furthermore you determine the policies to be used for the IPSec connection in the negotiation of phase 1 and 2. Using the automatic mode, the client accepts the policies assigned by the gateway. Should the client use its own policies as the initiator of the connection, you have to configure them with the policy editor. The advanced options could be used according to the requirements of the gateway.

***Parameters:***

- □ Gateway
- □ IKE Policy
- □ IPSec Policy
- □ Policy lifetimes
- □ Policy editor
- □ Exch. mode
- □ PFS group

## Gateway

This is the IP address of the IPSec gateway. You receive the address from your administrator as an IP number, if the gateway has a permanent official IP address - or as a string “hostname” that is mapped to a dynamic IP address from the Internet Service Provider.

IP address: The address is 32 bits long and consists of four numbers separated by periods.

Name (String): Enter the name which you have received from your administrator. This is the DNS Name of this gateway which is stored by the DynDNS service provider.

## IKE Policy

The IKE policy is selected from the list box. All IKE policies that you set up with the policy editor are listed under IKE policy. The policies appear in the box with the name that you specified in the configuration.

You will find two pre-configured policies in the policy editor under IKE policy as “Pre-shared Key” and “RSA Signature”. Contents and name of these policies can be changed at any time, i.e. new policies can be added. Every policy lists at least one proposal for authentication and encryption algorithms (see → IKE Policy (editing)). This means that a policy consists of different proposals. There are functional differences between these two IKE policies by using a static key or an RSA signature (see → Examples and Explanations, IPSec, IKE Modes).

☞ The same policies with their affiliated proposals should be valid for all users. This means that on the client side, as well as on the server side, the same proposals for the policies should be available.

Automatic mode: In this case it is not necessary to configure the IKE policy in the “IPSec Configuration”. It will be assigned by the remote site.

Pre-shared Key: This preconfigured policy can be used without PKI support. The same “Static Key” is used on both sides (see → Pre-shared key, Shared secret in the parameter folder “Identity”).

RSA Signature: This preconfigured policy can only be set with PKI support. Implementation of the RSA signature as additional strong authentication only makes sense when using a Smart Card or a soft certificate.

## IPSec Policy

The IPSec policy is selected from the List box. All IPSec policies that you set up with the policy editor are listed under IPSec policy. The policies appear in the box with the name that you specified in the configuration.

Two IPSec policies differ according to the IPSec security protocol AH (Authentication Header) or ESP (Encapsulating Security payload. Because the IPSec mode with AH security is totally unsuitable for flexible remote access, only an IPSec policy with ESP protocol, “ESP - 3DES - MD5", is preconfigured and comes standard with the software (see → Examples and Explanations, IPSec, AH and ESP).

Every policy lists at least one proposal for authentication and encryption algorithms (see → IPSec Policy (editing)). This means that a policy consists of different proposals.

The same policies with their affiliated proposals should be valid for all users. This means that on the client side, as well as on the server side, the same proposals for the policies should be available.

Automatic mode: In this case it is not necessary to configure the IPSec policy with the policy editor. It will be assigned by the destination.

ESP - 3DES - MD5 (or other policy name): When selecting the name of the pre-configured IPSec policy the same policies with their affiliated proposals should be valid for all users. This means that on the client side, as well as on the server side, the same proposals for the policies should be available.

## Exch. mode

The Exchange Mode determines how the “Internet Key Exchange” should proceed. Two different modes are available; Main Mode also referred to as Identity Protection Mode and the Aggressive Mode. These modes are differentiated by the number of messages and by their encryption.

Main Mode: in Main Mode (standard setting) six messages are sent over the Control Channel and the last two messages are encrypted. The last two messages contain the username, the signature or a hash value. This is why it is also known as Identity Protection Mode.

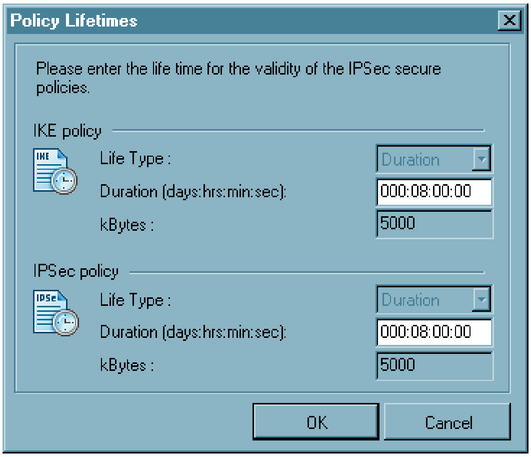
Aggressive Mode: in Aggressive Mode only three messages are sent over the Control Channel and nothing is encrypted.

## PFS group

With the selection of one of the offered Diffie Hellman groups it is determined whether a complete Diffie Hellman, (DH Group), key exchange (PFS, Perfect Forward Secrecy) should occur in Phase 2 in addition to the SA negotiation. The Standard is “none”.

### *Policy lifetimes*

*The lifetime of the policies defined here are applicable to all the policies.*



**Policy Lifetimes**

Please enter the life time for the validity of the IPSec secure policies.

IKE policy

Life Type : Duration

Duration (days:hrs:min:sec): 000:08:00:00

kBytes : 5000

IPSec policy

Life Type : Duration

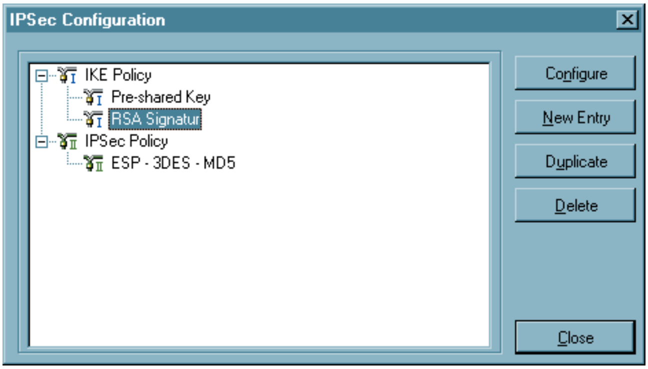
Duration (days:hrs:min:sec): 000:08:00:00

kBytes : 5000

- **Duration**

The number of Kbytes or the size of the time interval can be adjusted.

### *Policy editor*



**IPSec Configuration**

This menu item is clicked for configuring policies and, if necessary, a static Secure Policy Database. A configuration window will open displaying the branch with the policies and the Secure Policy Database as well as buttons for operation in the right-hand part of the configuration window.

Use the mouse to select the policy whose values are to be modified. The buttons will then be active. The (default) values of the policies can be edited, i.e. the parameters can be set or modified according to the requirements for the link to the defined destination

*Configure*
If you want to change any Policy or SPD data and parameters, start by selecting the appropriate name and then click on the “Configure” button. Upon doing so a folder opens and displays the IPSec parameters.

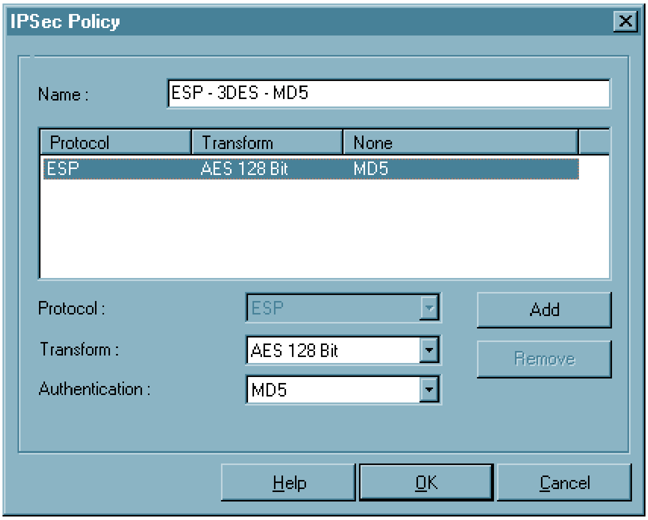
*New Entry*
In order to define a new Policy or SPD, select one of the Policies or the SPD and click on “New Entry”. The new Policy/SPD is entered. All parameters are assigned a default value except the Name.

*Duplicate*
You may want to use an existing Policy or SPD for the basis of a new one, however with some slight modifications. In order to do so first select the Policy or SPD to be duplicated and then click on the “Duplicate” button. Upon doing so a parameter folder will open. You must now enter a new name for this group and then click on “OK”. A new Policy or SPD is now created with parameters identical to those that were duplicated except for the Name.

*Delete*
If you want to delete a Policy or SPD from the IPSec configuration tree select the appropriate group and then click on the “Delete” button. Upon executing “Delete” the Policy or SPD will be permanently deleted.

*Close*
When you click on “Close” the IPSec folder closes and returns to the Monitor.

### *IKE Policy (edit)*



IPSec Policy

Name : ESP - 3DES - MD5

| Protocol | Transform | None |
|---|---|---|
| ESP | AES 128 Bit | MD5 |

Protocol : ESP
Transform : AES 128 Bit
Authentication : MD5

The parameters in this field relate to phase 1 of the Internet Key Exchange (IKE) with which the control channel for the SA negotiation was established. You determine the IKE mode (Exchange Mode), main mode or aggressive mode, in the Phonebook under “IPSec General Settings”.

The IKE policies that you configure here will be listed for the policy selection.

Contents and name of these policies can be changed at any time, i.e. new policies can be added. Every policy lists at least one proposal for authentication and encryption algorithms. This means that any policy can consist of several proposals.

The same policies with their affiliated proposals should be valid for all users. This means that on the client side, as well as on the server side, the same proposals for the policies should be available.

You can extend the list of proposals or delete a proposal from the proposal list by using the buttons “Add” and “Remove”.

## Policy Name | IKE Policy

Give this policy a name over which later an SPD can be allocated.

## Authentication | IKE Policy

Both sides must have been successfully authenticated in order to establish a control channel for phase 1 (IKE Security Association).

The authentication mode is limited to the use of pre-shared keys. This means for mutual authentication a static key is used. You define this key in the parameter folder “Identity”.

## Encryption | IKE Policy

Symmetrical encryption of messages 5 and 6 in the control channel occurs according to one of the optional encryption algorithms if Main Mode (“Identity Protection Mode”) is used. Choices are DES, 3DES, Blowfish, AES 128, AES 192, and AES 256.

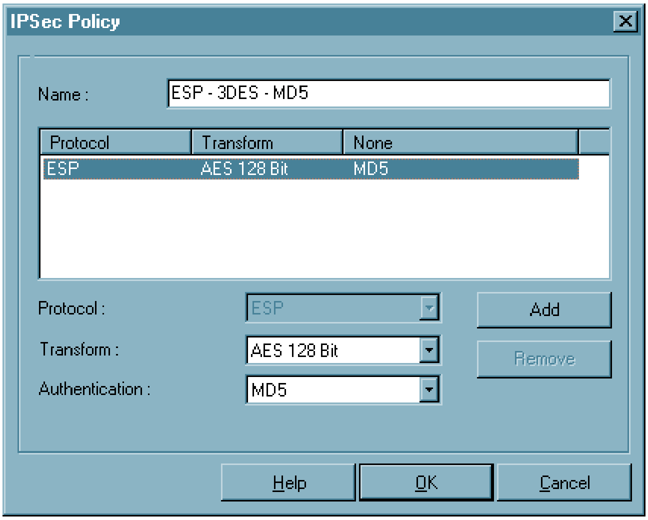
## Hash | IKE Policy

This is mode that determines how the hash value over the ID is formed, or in other words this determines which hash algorithm is used in the IKE negotiation. Choices are: MD5 (Message Digest, version 5), SHA (Secure Hash Algorithm), SHA 256, SHA 384 and SHA 512-bit.

## DH Group | IKE Policy

The selection of one of the offered Diffie Hellman groups determines the level of security for the key exchange in the control channel. Later a symmetrical key will be generated according to this selection. The higher the DH group the more secure the key exchange will be.

### *IPSec Policy (edit)*


IPSec Policy

Name : ESP - 3DES - MD5

| Protocol | Transform | None |
|---|---|---|
| ESP | AES 128 Bit | MD5 |

Protocol : ESP

Transform : AES 128 Bit

Authentication : MD5

The IPSec policies (Phase 2 parameters) that you configure here will be listed for the policy selection.

The same policies with their affiliated proposals should be valid for all users. This means that on the client side, as well as on the server side, the same proposals for the policies should be available.

You can extend the list of proposals or delete a proposal from the Proposal List by using the buttons "Add" and "Remove".

- ## Policy Name | IPSec Policy

Give this policy a name over which an SPD can later be allocated.

- ## Protocol | IPSec Policy

The fixed default value is ESP.

- ## Transform | IPSec Policy

One can specify which encryption algorithms (DES, Triple DES, Blowfish, AES 128, AES 192, and AES 256) are to be used within the ESP (Encrypted Security Payload). Multiple IPSec proposals with different security combinations can be defined.

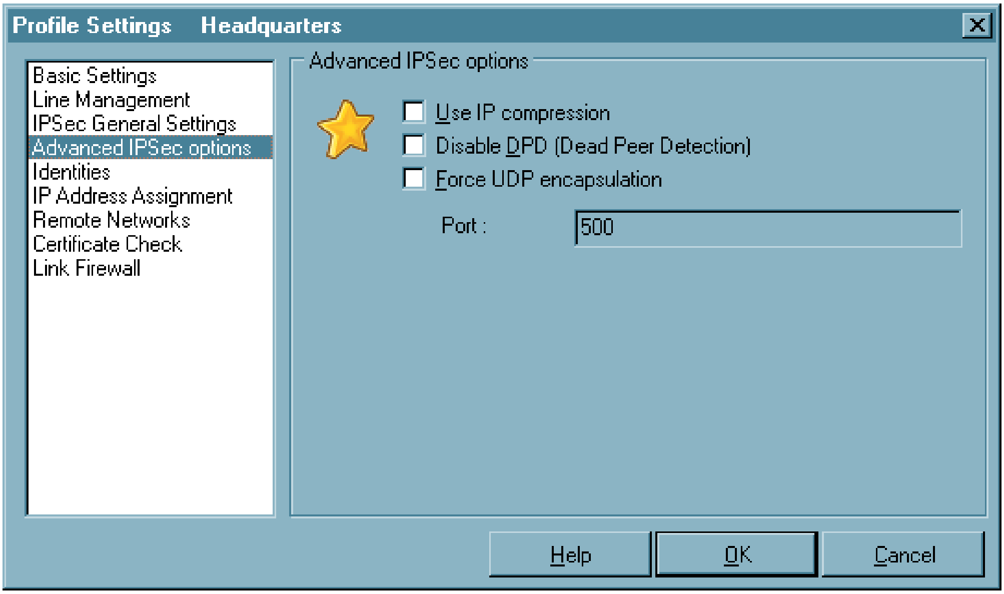
- ## Transformation (Comp) | IPSec Policy

IPSec compression. The data transmission with IPSec can also be compressed as in transfer without IPSec. This enables a maximum threefold increase in throughput. After selecting the "Comp" (compression) protocol you can select between LZS and deflate compression.

- ## Authentication | IPSec Policy

The authentication mode can be specifically set here for the security protocol ESP. Choices are: MD5, SHA, SHA 256, SHA 384 and SHA 512-bit

### 5.1.7 Advanced IPSec Options


Profile Settings Headquarters

Advanced IPSec options

□ Use IP compression

□ Disable DPD (Dead Peer Detection)

□ Force UDP encapsulation

Port : 500

*In this filed you can enter further IPSec settings.*

***Parameters:***

□ Use IP compression (LZS)

□ Disable DPD (Dead Peer Detection)

□ Force UDP Encapsulation

### Use IP compression (LZS)

The data can be compressed in order to increase transmission rates. By enabeling compression the throughput can be increased to up 3 times that the regular transmissions without compression.

### Disable DPD (Dead Peer Detection)

DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background if supported by the destination gateway. The IPSec client uses DPD to check, in regular intervals, whether the other side is still active. If the other side is inactive, then an automatic connection-disconnect occurs.

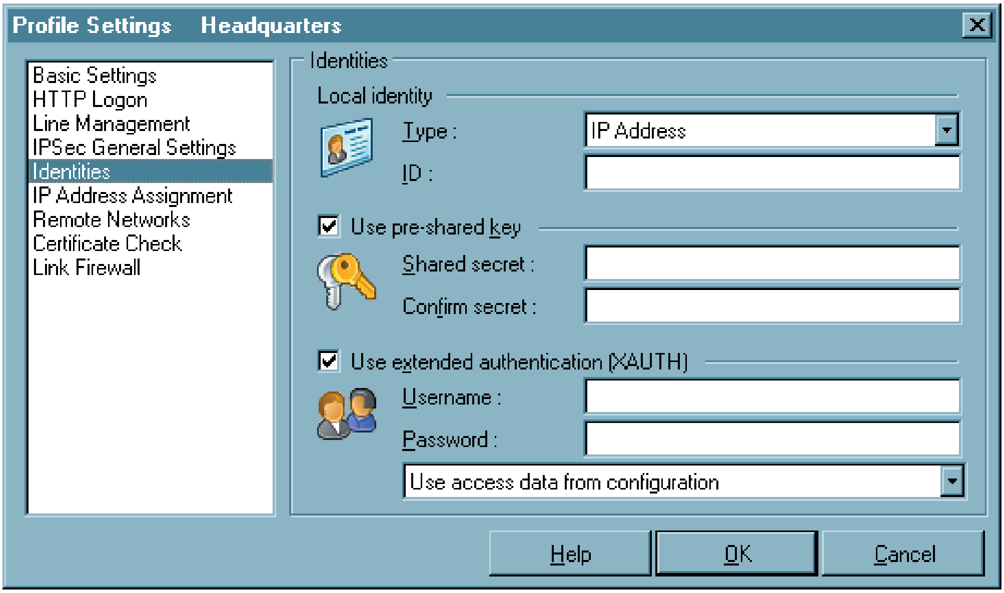
With this function you can disable DPD.

### Force UDP Encapsulation (Port 4500)

With UDP encapsulation only port 4500 should be released on the external firewall, (this is different than the situation with NAT Traversal or UDP 500 with ESP). The NCP Gateway detects UDP encapsulation automatically.

If UDP encapsulation is used then the port can be freely selected. Standard for IPSec with UPD is port 4500, for IPSec without UDP port 500.

## 5.1.8 Identities



Local identity

Type : IP Address

ID :

☑ Use pre-shared key

Shared secret :

Confirm secret :

☑ Use extended authentication (XAUTH)

Username :

Password :

Use access data from configuration

According to the security mode setting IPSec a more detailed parameter setting can take place.

***Parameters:***

□ Type | Identity

□ ID | Identity

□ Use pre-shared key

□ Use extended authentication (XAUTH)

□ Username | Identity

□ Password | Identity

□ Use access data from configuration

## Type | Identity

For IPSec there is a differentiation of incoming and outgoing connections. The value that the initiator selected as ID for outgoing connection must also be selected by the recipient as the ID for incoming connection.

The following ID Types are available:
– IP Address
– Fully Qualified Domain Name
– Fully Qualified Username
(entspricht der E-Mail-Adresse des Benutzers)
– IP Subnet Address
– ASN1 Distinguished Name
– ASN1 Group Name
– Free String used to identify Groups

## ID | Identity

For IPSec there is a differentiation of incoming and outgoing connections. The value that the initiator selected as ID for outgoing connection must also be selected by the recipient as the ID for incoming connection.

According to the selected ID type the character string i.e. the address range (with minus "-") must be entered in this field.

## Use pre-shared key

The pre-shared key is a string of the max. length of 255 characters. Any (alpha)numeric characters can be used. If the other side expects a pre-shared key during the IKE negotiation, then this key must be entered in the field "Shared secret".

Please confirm the shared secret in the field below. The same pre-shared (static) key must be used at both end points of the communication.

## Use extended authentication (XAUTH)

The authentication for "IPSec Tunneling" can be dealt with utilizing extended authentication (XAUTH protocol, Draft 6). If "XAUTH" is to be used, and supported by the gateway, enable "Use extended authentication (XAUTH)". In addition to pre-shared key, username and password can be defined:

Username = Username of the IPSec user

Password = Password of the IPSec user

## Username | Identity

Contact your System Administrator for your “Username”. The name can be up to 256 characters long.

Note: This parameter pertains only to accessing the gateway at the remote site.

## Password | Identity

Contact your System Administrator for your “Password” for XAUTH. The password can be up to 256 characters long.

Note: This parameter pertains only to accessing the gateway at the remote site.

## Use access data from configuration

You can select one of the following methods for authenticating the VPN tunnel against the gateway:

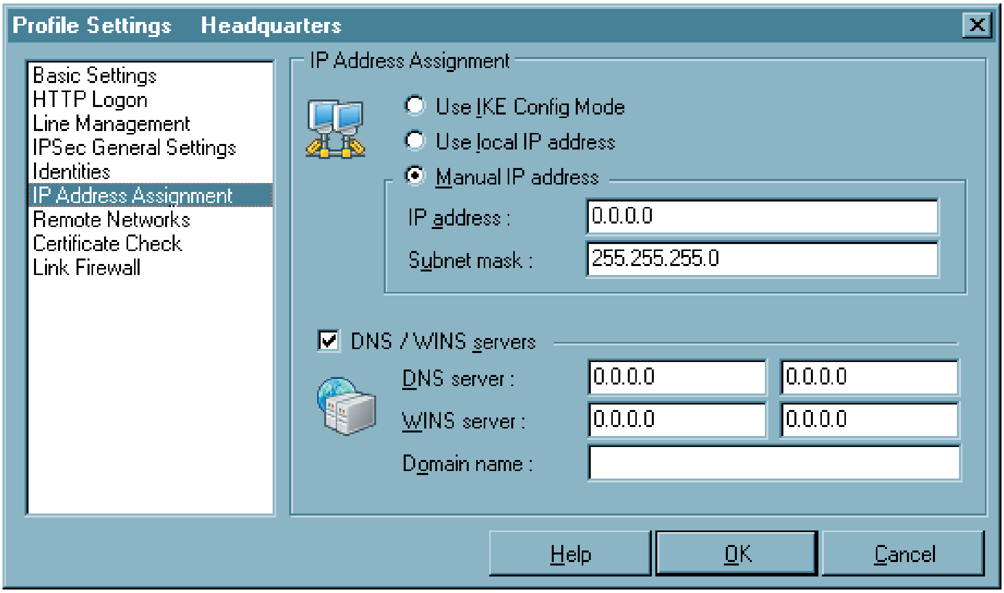
Use access data from configuration:
The VPN tunnel will be authenticated based on the User ID and Password entered in the respective fields above.

Use access data from certificate field “e-mail”:
The VPN tunnel will be authenticated based on the contents of E-Mail field of the selected certificate.

Use access data from certificate field “cn”:
The VPN tunnel will be authenticated based on the contents of “Customer” field of the selected certificate.

Use access data from certificate field “serial no.”:
The VPN tunnel will be authenticated based on the contents of “Serial No.” field of the selected certificate.

## 5.1.9 IP Address Assignment



Profile Settings Headquarters

Basic Settings
HTTP Logon
Line Management
IPSec General Settings
Identities
IP Address Assignment
Remote Networks
Certificate Check
Link Firewall

IP Address Assignment

○ Use IKE Config Mode
○ Use local IP address
● Manual IP address

IP address : 0.0.0.0
Subnet mask : 255.255.255.0

☑ DNS / WINS servers

DNS server : 0.0.0.0 0.0.0.0
WINS server : 0.0.0.0 0.0.0.0
Domain name :

In this parameterfield you can determine how to assign IP addresses. Moreover the server, assigned automatically by the PPP negotiation, can be changed with an alternativ server. Therefore the network settigs of the operation system must be switched to DNS mode.

***Parameters:***

□ Use IKE Config Mode

□ Use local IP address

□ Manual IP address

□ DNS/WINS

□ DNS server

□ WINS server

□ Domain Name

- **Use IKE Config Mode**

IP addresses and DNS servers are assigned via the IKE Config Mode protocol (Draft 2). All WAN interfaces can be used for the NAS dial-in.

DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background for “IPSec Tunneling” if supported by the destination gateway. The IPSec client uses DPD to check, in regular intervals, whether the other side is still active. If the other side is inactive, then an automatic connection-disconnect occurs. Using NAT Traversal is automatic with the IPSec client and is always necessary if network address translation is used on the side of the destination system device.

- **Use local IP address**

In this case the currently configured IP address (DHCP as well) of the PC is used for the IPSec client.

- **Manual IP address**

This is the IP address and the subnet mask; these can be freely entered here. In this case the address entered here is used, regardless of the configuration in the network settings.

- **DNS/WINS**

IKE Config Mode, if configured and available, enables dynamic assignment of client IP addresses, DNS / WINS server addresses and domain name.

Activating this function you can define an alternative DNS Server as opposed to using the one that is automatically assigned during the PPP negotiation to the NAS/ISP.

- **DNS server**

The IP address of the DNS server entered will be the one used instead of the DNS server assigned during the PPP negotiation.

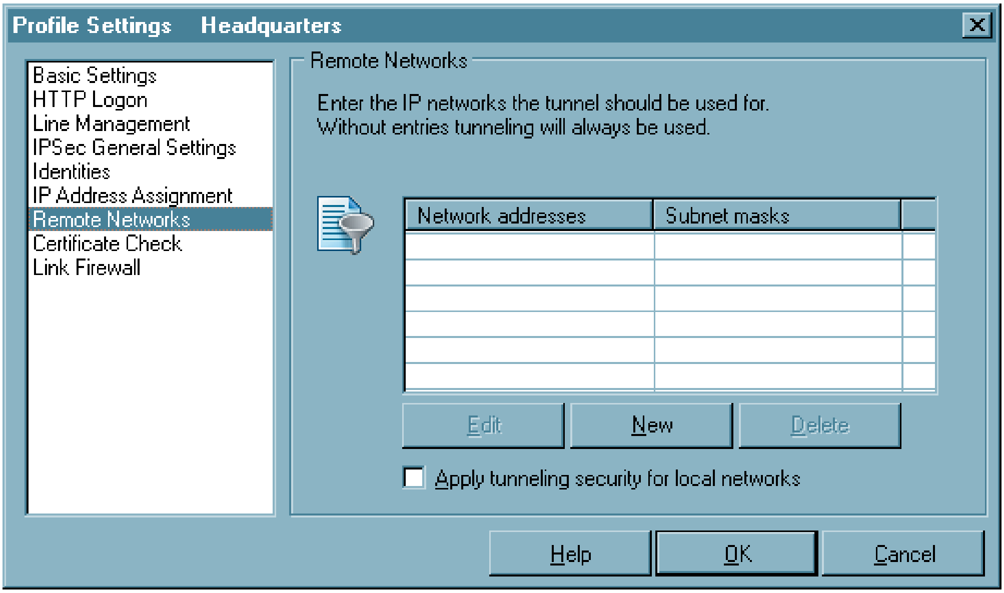
- **WINS server**

The IP address of the WINS server entered will be the one used instead of the WINS Server assigned during the PPP negotiation.

- **Domain Name**

This is the domain name, which otherwise is transferred to the system per DHCP in the network settings.

## 5.1.10 Remote Networks


Profile Settings Headquarters

Remote Networks

Enter the IP networks the tunnel should be used for.
Without entries tunneling will always be used.

| Network addresses | Subnet masks |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |

□ Apply tunneling security for local networks

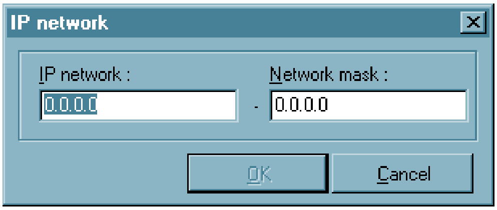
In this folder you can precisely define the IP Network(s) to which the Client can communicate with via VPN tunnels. If you are using tunneling and you have made no entries in this folder, then your communications will always be established only to the tunnel end-point (VPN gateway). However if you would like to alternatively communicate with your central site using tunneling as well as the Internet, then you must define the IP Networks in your company that you wish to communicate with. Then you can toggle between the Internet and your company's VPN gateway. This is also referred to as "Split Tunneling".

***Parameters:***

□ Network addresses | Remote Networks

□ Subnet masks

□ Apply tunneling security for local networks



IP network

IP network : 0.0.0.0

Network mask : 0.0.0.0

Click on the “New” button to enter the IP address of the network and the netwok mask in the window that will appear (left).

## Network addresses | Remote Networks

In this window enter the address of the IP Network(s) that you want to reach via the gateway. These addresses are available from your administrator.

Note: Be sure that IP addresses entered in this field are not the same subnet as the gateway.

## Subnet masks

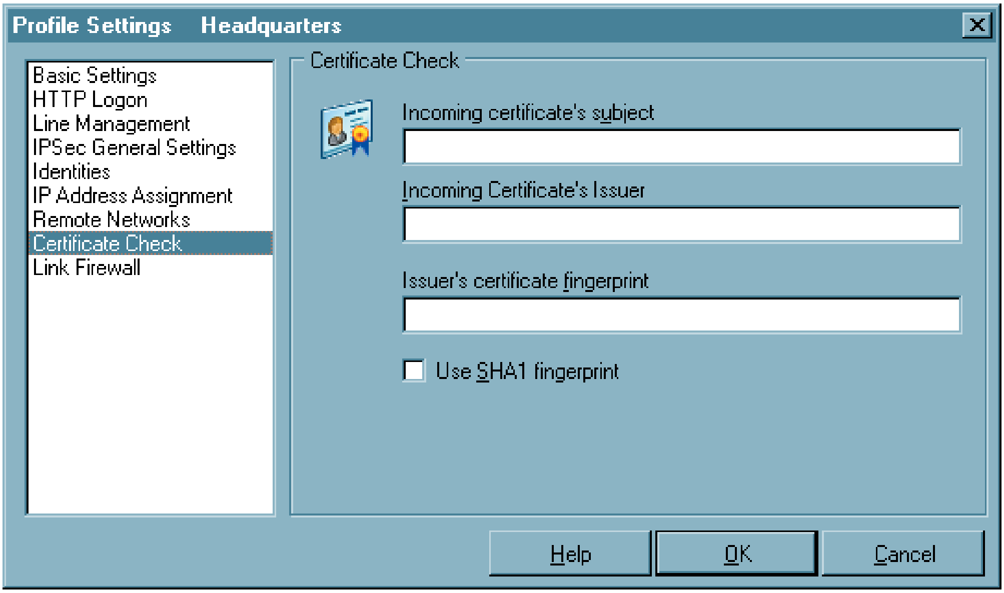
In this window enter the address(es) and netmask(s) of IP Network(s) that you want to reach via the gateway. These addresses are available from your administrator.

Note: Be sure that IP addresses entered in this field are not the same subnet as the gateway.

## Apply tunneling security for local networks

If you wish to encrypt the local LAN traffic by means of VPN tunneling enable this function.

## 5.1.11 Certificate Check



Incoming certificate's subject:

Incoming Certificate's Issuer:

Issuer's certificate fingerprint:

☐ Use SHA1 fingerprint

You can specify in the “Certificate Check” parameter field, per destination system, which entries must be present in a certificate from the other side (Secure Server) (see → Display Incoming Certificate, General). See also → Further Certificate Checks.

**See also:**

- ☐ Incoming certificate’s subject
- ☐ Incoming certificate’s Issuer
- ☐ Issuer’s certificate fingerprint
- ☐ Use SHA1 fingerprint
- ☐ Further certificate checks

## Incoming certificate’s subject

All attributes of the user, to the extent known - even with wildcards -, can be used as user certificate entries of the other side (server). In this regard compare the entries that are always listed under users for “Display Incoming Certificates”.

Use the attribute name abbreviations for this. The attribute type abbreviations for certificate entries have the following meaning:

```
cn     = Common Name / Name
s      = Surname / Nachname
g      = Givenname / Vorname
t      = Title / Titel
o      = Organisation / Firma
ou     = Organization Unit / Abteilung
c      = Country / Land
st     = State / Bundesland, Provinz
l      = Location / Stadt, Ort
email  = E-mail
```

Example:

```
cn=VPNGW*, o=ABC, c=de
```

The common name of the security server is verified here only until the wildcard “*”. All following positions can be as desired, like 1 - 5 as numbering. The organizational unit must always be ABC in this case and Germany must be the country.

## Incoming certificate’s Issuer

All attributes of the user, to the extent known - even with wildcards -, can be used as user certificate entries of the other side (server). In this regard compare the entries that are always listed under users for “Display Incoming Certificates”.

Use the attribute name abbreviations for this. The attribute type abbreviations for certificate entries have the following meaning:

```
cn     = Common Name / Name
s      = Surname / Nachname
g      = Givenname / Vorname
t      = Title / Titel
o      = Organisation / Firma
ou     = Organization Unit / Abteilung
c      = Country / Land
st     = State / Bundesland, Provinz
l      = Location / Stadt, Ort
email  = E-mail
```

Example:
`cn=ABC GmbH`
Only the common name of the issuer is verified here.

## Issuer’s certificate fingerprint

To prevent an unauthorized person that imitates a trusted CA, from using a counterfeited issuer certificate, the issuer’s fingerprint can also be entered if it is known.

## Use SHA1 fingerprint

The algorithm for fingerprint generation can be either MD5 (Message Digest version 5) or SHA1 (Secure Hash Algorithm 1).

### *Further certificate checks*

In addition to the certificate verification according to content a certificate check is executed on the Secure Client in many respects.

**1. Selection of the CA Certificates**

The corporate network administrator specifies which issuers of certificates can be trusted. This is done by copying the CA certificates of his choice into the installation directory under CACERTS\. The copying over can be automated with diskettes in a software distribution, if the issuer certificates are located in the root directory of the first diskette at the installation. Afterwards issuer certificates can be automatically distributed via the Secure Management Server (see → Management Server Manual), or if the user has the requisite write authorizations in the designated directory - they can be set by the user himself (see → Display CA Certificates.

The formats *.pem and *.crt are supported for issuer certificates. They can be viewed in the monitor under the menu item “Connection / Certificates / Display CA Certificates”.

If the issuer certificate of another side is received, then the client determines the issuer, then searches the issuer certificate, first on Smart Card or in the PKCS#12 file, and then in the installation directory under CACERTS\. If the issuer certificate cannot be located, then the connection cannot be established.

If no issuer certificates are present, then no connection will be permitted.

### 2. Check of Certificate Extensions

Certificates can contain extensions. These serve for the linking of additional attributes with users or public keys, that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written in the certificate by the issuing certification authority.

Three extensions are significant for the Secure Client and the Secure Server:
– extendedKeyUsage
– subjectKeyIdentifier
– authorityKeyIdentifier

*extendedKeyUsage:*

If the extendedKeyUsage extension is present in an incoming user certificate, then the Secure Client checks whether the defined extended application intent is “SSL Server Authentication”. If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Please note that the SSL server authentication is direction dependent. This means that the initiator of the tunnel establishment checks the incoming certificate of the other side, if the extendedKeyUsage extension is present, then the intended purpose must contain “SSL Server Authentication”. This applies as well for callback to the Client via VPN.

*subjectKeyIdentifier / authorityKeyIdentifier:*

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer’s public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA certificate is found then the connection is rejected.

The keyidentifier designates the public key of the certification authority and thus not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determining a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

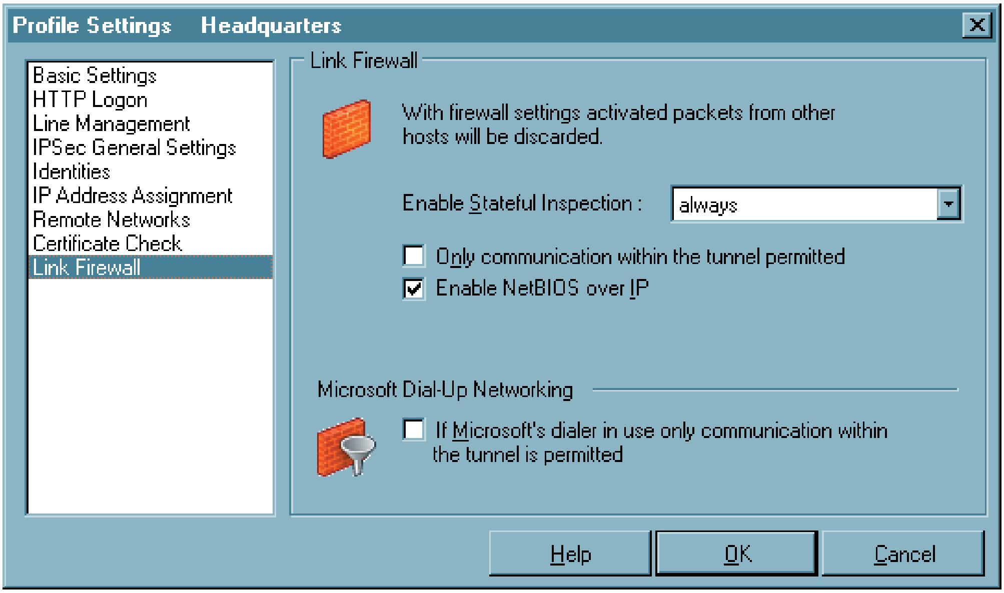
### 3. Checking Revocation Lists

The Secure Server can be provided with the associated CRL (Certificate Revocation List) for each issuer certificate. It will be copied into the installation directory under CRLS\. If a CRL is present, then the Secure Client checks the incoming certificates to see if they are listed in the CRL. The same applies for an ARL (Authority Revocation List) that must be copied into the ARLS\ directory.

If incoming certificates are contained in the CRL or ARL lists, then the connection is not permitted.

If CRLs or ARLs are not present, then no check takes place in this regard.

## 5.1.12 Link Firewall



With firewall settings activated packets from other hosts will be discarded.

Enable Stateful Inspection : always

☐ Only communication within the tunnel permitted

☑ Enable NetBIOS over IP

☐ If Microsoft's dialer in use only communication within the tunnel is permitted

The Link Firewall configuration field with extended configuration possibilities is included in this client. The firewall settings can also be used to protect the RAS connections. The activated firewall is displayed on the monitor as a symbol (wall with arrow). A firewall's fundamental task is to prevent hazards from the Internet from spreading within the corporate network. This is why a firewall is also installed at the junction between corporate network and the Internet. It checks all incoming and outgoing data packets and decides whether a data packet will be permitted through or not, on the basis of previously specified configurations. The implemented technology is Stateful Inspection. Stateful Inspection is a very recent firewall technology and offers the high-est security available today for Internet connections and thus the corporate network. Security is insured from two perspectives. On one hand, this functionality prevents unauthorized access to data and resources in the central data network. On the other hand it monitors the respective status of all existing Internet connections as a control instance. Additionally, the Stateful Inspection firewall recognizes whether a connection has opened; "spawned connections" - such as is the case with FTP or Netmeeting - whose pakkets likewise must be forwarded. The Stateful Inspection connection presents itself as a direct line to the communication partner that may only be used for a data exchange that corresponds to one of the agreed upon rules.

***Parameters:***

☐ Enable Stateful Inspection

☐ Only communication within the tunnel permitted

☐ Enable NetBios over IP

☐ If Microsoft's dialer in use only communication within the tunnel is permitted

### Enable Stateful Inspection

off: The firewall’s security mechanisms will not be used.

always: The firewall’s security mechanisms will always be used, this means the PC is protected from unauthorized accesses even if no connection is established.

when connected: The PC is not vulnerable if a connection exists.

### Only communication within the tunnel permitted

Only communication within the tunnel permitted: This function can also be switched on with activated firewall to additionally filter IP packets so that only VPN connections are possible.

### Enable NetBios over IP

This parameter switches off a filter, which prevents NetBios frames from being transmitted over IP links.

The default setting is “Off”, meaning that NetBios frames are filtered will be filtered out of the data stream.

When this parameter is activated, NetBios frames will be included in the data stream over IP. This may be desirable when using Microsoft Networking in conjunction with the Secure Client.

### If Microsoft’s dialer in use only communication within the tunnel is permitted

When using the Client Monitor this function prevents communication to the Internet via the RAS Dialer.

# 6. Establishing a Connection

In order to guarantee the proper functionality of your IPSec client Funkwerk offers a public VPN test access. A detailed step-by-step guidance how to use this test access and how to set the needed configurations correctly can be found on the Funkwerk websites at www.funkwerk-ec.com.

## Establishing a Connection to the destination system

Provided the software is installed properly and the profile parameters are configured correctly a dial-up to the destination system can take place. Part of the configuration is to define the mode with which this connection is to be established. There are three modes to select from: automatic, manual and variable. You define the connection mode of the destination system in the Phonebook under "Line Management – Connection Mode".

### *Automatic (default):*

The Client works on the principle of LAN emulation, whereas with Microsoft RAS, every connection has to be established manually. This means that the Secure Client will automatically activate a connection in accordance with your application program requirements to the destination selected in the Phonebook.

### *Manual:*

This means that you must manually activate a Connect. This is done by clicking on "Connection" in the Monitor and than selecting "Connect".

### *Variable:*

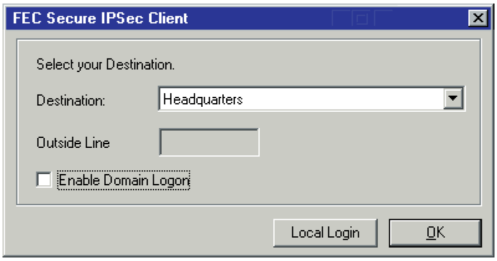
When this mode is selected, the connection must be established "manually". Subsequently, the mode adapts according to the manner in which the connection was terminated:
– If the connection was terminated as a result of a timeout, then the following connection will be automatically initiated as required.
– On the other hand if the connection was terminated manually, then the following connection must then also be established manually.

## Connect

Independent of the connection mode, the monitor always displays the connection status as explained in the section 3.1.6 Symbols of the Dial-in.

## Client Logon

If the Client Logon to the Network Access Server occurs before the Windows Logon to the remote domain, ("Logon Options" (see → Monitor, Logon Options), the connection is established in the same way as described under "Connect" (see above).



FEC Secure IPSec Client

Select your Destination.

Destination: Headquarters

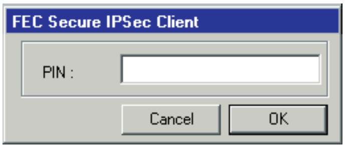
Outside Line

□ Enable Domain Logon

To initiate a link to be built, select the destination system to connect to and then click on the OK button.

Local logoff:
With a click on this button the link build is stopped.

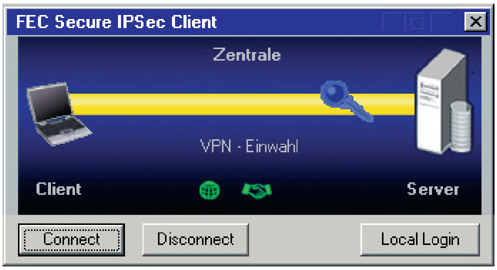
Activate Domain Logon: With this option a safe WAN domain logon is possible, even if the logoff was not executed correctly. The logon takes some seconds. This function is not necessary if the shut down of the PC was made correctly and mapped drivers were disconnected properly.



FEC Secure IPSec Client

PIN :

If the use of a (Soft-) Certificate was configured – like example destination Test connection SSL – you first have to enter the PIN.

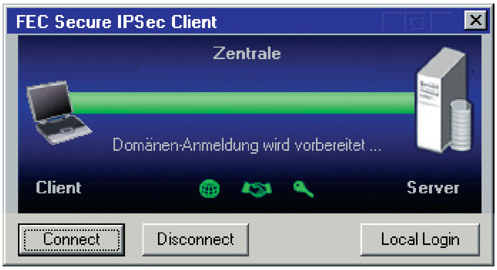


FEC Secure IPSec Client

Zentrale

VPN - Einwahl

The following stations of the link built in the same procerure as described above under 3.1.6 Symbols of the Dial-in.



FEC Secure IPSec Client

Zentrale

Domänen-Anmeldung wird vorbereitet ...

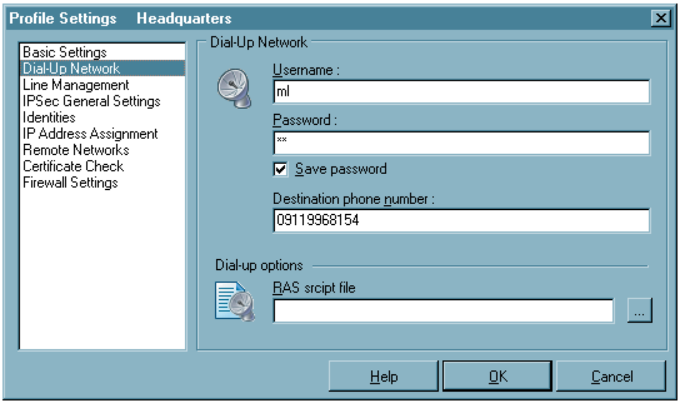
## Passwords and User Names

The password (see → Dial-Up Network, Password) is used for identifying yourself to the remote Network Access System (NAS) when establishing a connection to your Destination, or alternatively to your Internet Service Provider (ISP) if you are communicating across the Internet. The password ID can include up to 256 characters. Normally the password will be assigned to you by your Destination (e.g. your company Headquarters, User Help Desk, Internet Service Provider, etc.), because it must be supported and accepted by the NAS, for authentication purposes. Upon entering your password all characters will be displayed as an asterisk (*) in order to keep them from being overlooked by someone else. Therefore it is necessary to be very careful that you enter your password exactly the way in which it was assigned to you (pay attention to upper case and lower case characters).

Even if you selected “automatically” as connection mode (see → “Establishing a Connection to the destination system”), you have to establish the first connection manually and enter the password. For every additional automatically established connection the password is adopted automatically, until you reboot your PC or you select a different destination system. This means that even though the function “Save Password”(see → Dial-Up Network) was not activated, automatic connections can still be made where this cached password is used to authenticate. When (re)booting your PC the once entered password is then deleted (Please notice → Logon Options).

If you do not want to delete the password when (re)booting your PC you have to activate the function “Save Password” (see → Dial-Up Network). Please notice that for security reasons you must be aware that should some unauthorized person use your PC, they will be able to use your password. Therefore caution should be used when your PC is unattended.

### *User ID for NAS Dial-Up*



Username : ml

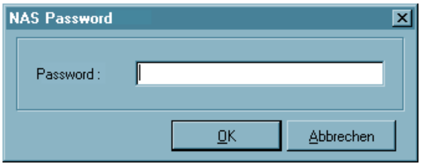
Password : **

☑ Save password

Destination phone number : 09119968154

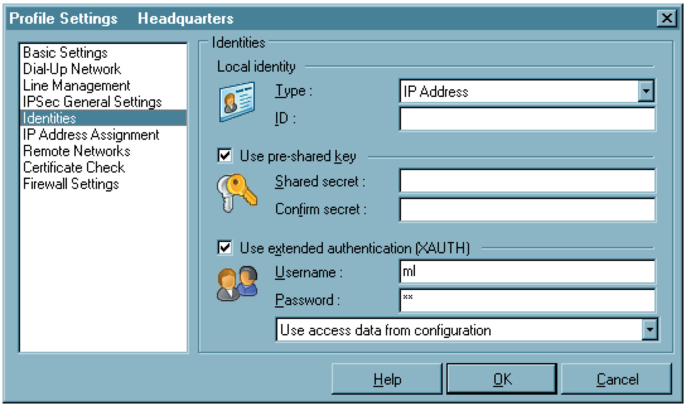
If the Password has not been entered or saved it will be requested in a seperate window.

The “User Name”of the Dial-Up Network must always be entered in the configuration of the profile. Without this User ID a dial-up to the NAS is impossible (see → Dial-Up Network)



Password :

### *User Name and Password for Extended Authentication*



Identities

Local identity

Type : IP Address

ID :

☑ Use pre-shared key

Shared secret :

Confirm secret :

☑ Use extended authentication (XAUTH)

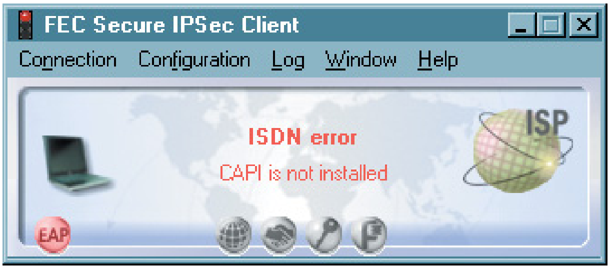
Username : ml

Password : **

Use access data from configuration

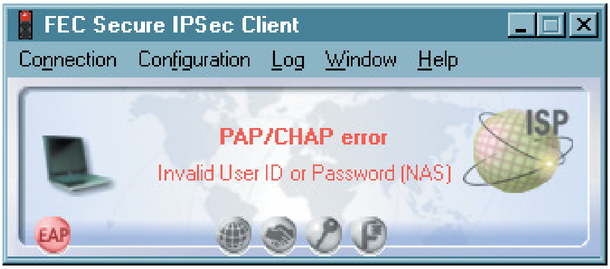
If you use Extended Authentication, User Name and Password must be entered in the configuration folder of the profile. Otherwise the establishing of a connection will not be successful (see → Profile Settings, Identities, Use extended authentication (XAUTH)).

## Disconnection and error



ISDN error

CAPI is not installed



PAP/CHAP error

Invalid User ID or Password (NAS)

If an error occurs, a connection will not be established and the reason is displayed in the monitor (please notice the passage “ISDN CAPI Error Codes“)

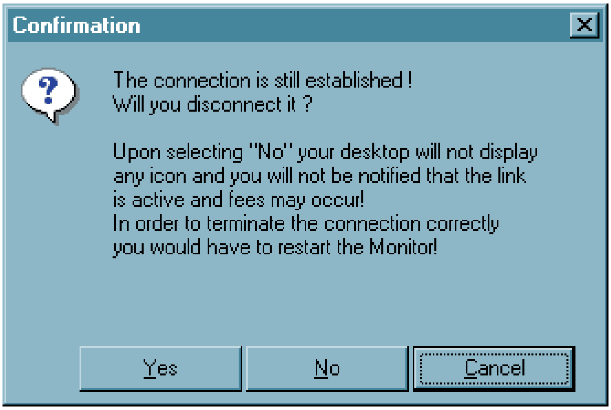
## Disconnect

With the function “Disconnect” a connection can be manually terminated. If you want to keep the possibility to disconnect manually you have to set the connection mode to “manually” and deactivate the active Timeout by setting it to zero (0) ( → Connection Mode).

If the connection is terminated, the color of connection line changes until it disappears and the lamps of the traffic light changes from green to red during the period of offline.

## Disconnect (the Monitor)

If the connection is still established, with a click on this menu item or on the “Disconnect” button, the monitor can be closed as well. Please note that the connection is not automatically terminated by closing the Monitor. If the link should be established although the monitor is closed and fees may occur , the software asks you explicitelly for a prompt (see picture )



Confirmation

The connection is still established !
Will you disconnect it ?

Upon selecting "No" your desktop will not display any icon and you will not be notified that the link is active and fees may occur!
In order to terminate the connection correctly you would have to restart the Monitor!

**Upon selecting “No” your desktop will not display any icon and you will not be notified that the link is active and fees may occur! In order to terminate the connection correctly you would have to restart the Monitor!**

# 7. Examples and Explanations

This section of the handbook discusses some essential routing concepts. The Secure Client configuration is illustrated with several different examples.

# 7.1 IP Functions

To correctly configure an IP network, you must adhere to the procedure for IP addressing. Below you will find some guidelines and terminology. For additional information about IP networks the standard literature is recommended.

## 7.1.1 IP Network Devices

IP addresses are assigned to the component interfaces of an IP network. These components are also called hosts or computers. Multiple networked components (e.g. routers) may also be allocated to various addresses. The term host-address marks the IP address of the host of an IP process, regardless of the actual physical structure of the components or the interfaces.

## 7.1.2 IP Address Structure

IP addresses have a length of four octets, 32 bits (4 bytes) and are written in dotted decimal or hexadecimal notation. E.g.:

```
198.10.6.27 or
C6.0A.06.1B or
0xC6.0x0A.0x06.0x1B
```

The addresses are divided into a network segment, which identifies the network, and a local address, the host segment, identifying the host of the network. All hosts within a unique network share the same host segment. All devices inside a unique network share the same network segment. Each also has a unique host segment.

There are three classes of Internet addresses each is used according to how many bytes the IP address uses for network segment and host segment.

*Class A*, large networks: network numbers 1 - 127

For class A addresses the highest bit is equal to zero, the next seven bits represent the network segment and the remaining 24 bits represent the host segment.

The network segment needs 1 byte (max. 126 different networks)

The host segment needs 3 bytes (max. 2 to the 24th power = 16.777.216 various hosts).

In this manner a maximum of 127 different networks, each with maximum of 16.777.216 different hosts may be addressed.

*Class B*, mid-size networks: network numbers 128 -191

For class B addresses the two highest bits have the values 1 and 0, the following 14 bits represent the network segment and the remaining 16 bits represent the host segment

The network segment needs 2 Byte (max. 16.384 various networks)

The host segment needs 2 bytes (max. 2 to the 16th power = 65.526 different hosts)

In this manner a maximum of 16.384 different networks, each with maximum of 65.526 different hosts may be addressed.

C*lass C*, small networks: network numbers 192 - 223

For class C addresses the three highest bits have the values 1, 1 and 0, the following 21 bits represent the network segment and the remaining 8 bits represent the host segment.

The network segment needs 3 bytes (max. 2.097.152 various hosts)

The host segment needs 1 byte (max 256 various hosts)

In this manner a maximum of 2.097.152 various networks, each with maximum of. 256 different hosts may be addressed.

e.g.:

```
                Network          Host
Class A:   122. | 087.   156.   045
Class B:   162.   143. | 085.   132
Class C:   195.   076.   212. | 024
```

Please note, when assigning the addresses, that each physical host must be able to use several IP addresses. A workstation can function with one IP address. A router needs an IP address for each interface however at least two – one for the connection to the local network (LAN IP Address) and one for the connection to the WAN side.

### 7.1.3 Subnet Masks

In a wide area network various physically separated nets (LANs) may belong to the same network (WAN) with the same network number. On the basis of the network number alone no router can decide if it should create a connection to a physically different network within the WAN or not. Thus the network (WAN) must be subdivided into smaller segments (LANS) that each receive their own address block. Each address block of the individual physical networks is designated as a subnet. Through this subdivision of a network into subnets the hierarchy network and computer is extended to a hierarchy of network, subnet, and computer.

This extended hierarchy makes it easier to locate a computer in the total network (WAN).  An example using the telephone nomenclature can illustrate how this works. The area code designates in which area the telephone is located. This hierarchy insures also a certain access security. For example a computer on a subnet will not automatically have access to the resources of another subnet. Or to use a specific case a production worker does not have access to the personnel department data provided that the subnet masks have been selected according to corporate departments.

The subnet mask indicates the location of the subnet field in an IP address. The subnet mask is a binary 32-bit-number like an IP address. It has a “1" in every position of the network segment and an IP address (according to the network class within the first to the third octet). The next octet shows the position of the subnet field. The digits 1 adjacent to the subnet field indicate the subnet bits. All remaining positions with ”0" remain for the host segment.

**Examples**

*Example 1:*

The subnet mask is used for the interpretation of the IP address. Accordingly an address 135.96.7.230 with the mask 255.255.255.0 may be interpreted as follows: The network has the address 135.96.0.0, the subnet has the number 7, the host number 230. An IP address with 135.96.4 belongs a to a different subnet (4) on the same network.

Binary representation:

```
135.96.7.230     = 10000111 11000000 | 00000111 | 11100110
135.96.4.190     = 10100000 10010101 | 00000100 | 10111110
255.255.255.0    = 11111111 11111111 | 11111111 | 00000000
                   Network           | Subnet   |
255.255.248.0    = 11111111 11111111 | 11111|000  00000000
```

If the net mask did not have a standard value of 255.255.255.0 in the example shown above, but rather an IP address of 255.255.248.0 then the IP addresses would be located in the same subnet, and routing would not take place.

*Example 2:*

Two IP addresses with 160.149.115.8 and 160.149.117.201 and the subnet mask 255.255.252.0 are located in the same network, but belong to different subnets.

Binary description:

```
160.149.115.8   = 10100000 10010101 | 011100|11 00001000
160.149.117.201 = 10100000 10010101 | 011101|01 11001001
255.255.252.0   = 11111111 11111111 | 111111|00 00000000
                  network           | subnet|
```

The choice of a suitable subnet mask depends on the network class, the quality of the possible subnets, their quantity and their growth potential. For planning purposes please refer to the standard tables or to a subnet calculator.

Subnet tables class C:

| Subnet bits | Host bits | netmask | subnets | host |
|---|---|---|---|---|
| 2 | 6 | 255.255.255.192 | 2 | 62 |
| 3 | 5 | 255.255.255.224 | 6 | 30 |
| 4 | 4 | 255.255.255.240 | 14 | 14 |
| 5 | 3 | 255.255.255.248 | 30 | 6 |
| 6 | 2 | 255.255.255.252 | 62 | 2 |

(Calculation: 2 to the power of n minus 2 = quantity of subnets / computers
where n is the quantity of subnets / host bits)

With the subnet mask 255.255.255.240 a class C network is divided into subnets. This net mask allows a total of 14 subnets each with a maximum of 14 computers.

```
255.255.255.240  11111111 11111111 11111111 | 1111 | 0000
199.  9. 99.130 11000111 00001001 01100011 | 1000 | 0010  Subnet-Nummer 8
199.  9. 99.146 11000111 00001001 01100011 | 1001 | 0010  Subnet-Nummer 9
                 Netzwerk                   |Subnet| Host
```

## Standard masks

Subnet mask for class A:255.  0.  0.    0

Subnet mask for class B:255. 255.  0.    0

Subnet mask for class C:255. 255. 255.    0

### ■ Reserved addresses

Some IP addresses may not be assigned to network devices. These include the network or subnet address and the circular address for networks ref. subnets. Network addresses consist of network number and the host field filled with binary 0’s (e.g. 200.1.2.0, 162.66.0.0., 10.0.0.0) – also Loop Back, there is no transmission into the network. The circular address consists of network numbers and the host segment with binary 1’s (e.g. 200.1.2.255, 162.66.255.255., 10.255.255.255) – therefore also an “All One Broadcast”, all components of a network will be addressed.

*Example:*

| | |
|---|---|
| 198.10.2.255 | addressed to all stations in the network 198.10.2. |
| 255.255.255.255 | addressed to all stations of all connected nets |
| 0.0.0.0 | All Zero Broadcast: invalid address. |

Please note that this is often used for standard settings.

## 7.1.4 Using IP Addresses:

□ Each address in your enterprise-wide network should be unique. Make sure that this is the case when connecting to the Internet or linking new networks.

□ Use a logical, comprehensible addressing scheme, e.g. organized according to administrative units, buildings, departments etc.

□ For connection to the Internet, you will need an official, unique, Internet address.

□ If possible, do not assign any addresses in which the network or host segment end in “0". This might lead to misinterpretations and to undefined errors in the network.

□ Subnet masks will only be evaluated by the Internet protocol, if the network numbers of all communication partners are the same.

The subnet masks have network segments of different length just as do the address classes.

## 7.2 Security

Configuration parameters for IPSec for implementation in remote access environments are collected in the parameter field “IPSec General Settings”. This section describes some possibilities of configuration.

### 7.2.1 IPSec – Overview

IPSec can only be implemented for IP data traffic. The IPSec specification includes not only Layer 3 tunneling but also includes all necessary security mechanisms like strong authentication, key exchange and encryption.

The IPSec RFC’s (2401-2409) permit the development of a VPN with specified IP security. IPSec tunneling and security are thoroughly described making a complete VPN framework available. In principle it is possible to use vendor-independent components. For site-to-site VPN’s the gateways may be supplied by different manufacturers, for end-to-site gateways the clients may be supplied by another manufacturer.

The establishment of a connection to IPSec traffic is based on the Internet Key Exchange Protocol (IKE).

- **IPSec – General Functional Description**

In every IP host (client or gateway) that supports IPSec there is an IPSec module i.e. an IPSec engine. This module examines each packet for certain characteristics in order to apply the appropriate security negotiation to it.

Testing of the outgoing IP packets from the IP stack occurs relative to a Secure Policy database (SPD). With this all configured SPDs will be processed. (When using the IPSec Client, the SPDs are only stored at the central site gateway.)

The SPD consists of multiple entries (SPD entries), which in turn contain a filter portion. The filter portion or Selector of an SPD entry consists primarily of IP addresses, UPD, and TCP ports as well as other IP header-specific entries. If the values of an IP packet agree with the values from the SPD entry Selector portion, then further determination as to what should be done with this IP packet is made from the SPD Entries. The packet can simply be allowed through (permitted), or discarded, or certain security policies of the IPSec process can be imposed on the packet. These security policies are also described in the SPD entry.

If, in this manner, it is determined that an IP packet is linked with an SPD entry that triggers an IPSec process, then it will be examined to see whether a security association (SA) exists for this SPD entry. If an SA does not yet exist then first an authentication and a key exchange will take place before the negotiation of an SA (see below → IPSec Negotiation Phase 1)

After the SA negotiation, negotiations follow for data packet encryption (ESP) and/or authentication (AH) of the data packets.

The SA describes which security protocol should be used. ESP (Encapsulating Security Payload) supports the encryption and authentication of IP packets. AH (Authentication Header) supports only the authentication of IP packets. The SA also describes the operating mode in which the security protocol should be used either Tunnel or Transport mode. In Tunnel mode an IP header is inserted, in Transport mode the original header is used. Additionally the SA describes which algorithm will be used for authentication, which encryption method (for ESP) and which key should be used. Of course the other side should work according to the same SA.

If the SA is negotiated, then each packet will be processed according to the operating mode and protocol, either Tunnel or Transport, and either ESP or AH respectively. The IPSec Client uses always the IP protocol in Tunnel mode.

### 7.2.2 Firewall Settings

The firewall settings consists mainly of IP addresses, UDP and TCP ports, as well as other IP header-specific entries. If the values of an IP packet agree with values from the selector portion, then further determinations from the SPD entries specify how to proceed with this IP packet.

Following, the entries for configuring the IPSec Client:

□ Command

permit, deny, disabled

□ IP Protocol

This is the transport protocol that can be ICMP, TCCP, or UDP. One of these offered protocols can be selected or (any) can be used.

□ Source IP address

This can be a simple IP address or an address range. The latter is necessary if a shared SA, behind a firewall, supports multiple output systems for example.

□ Destination IP address

This can be a simple IP address or an address range. The latter is necessary if a shared SA, behind a firewall, supports multiple output systems for example.

□ Source Port

These can be either individual TCP or UDP port numbers or a range of port numbers. You determine the port numbers with allocated service by using the Select button [...].

□ Destination Port

These can be either individual TCP or UDP port numbers or a range of port numbers. You determine the port numbers with allocated service by using the Select button [...].

### 7.2.3 SA Negotiation and Policies

In order to initiate the IPSec filter process the SA must first have been negotiated. One SA negotiation takes place for the phase 1 (IKE policy) and at least two (for incoming and outgoing connection) for phase 2 (IPSec policy). [For every destination network (see → Profile Settings, Remote Networks) two SAs are also negotiated.].

- **Phase 1 (IKE Policy)**

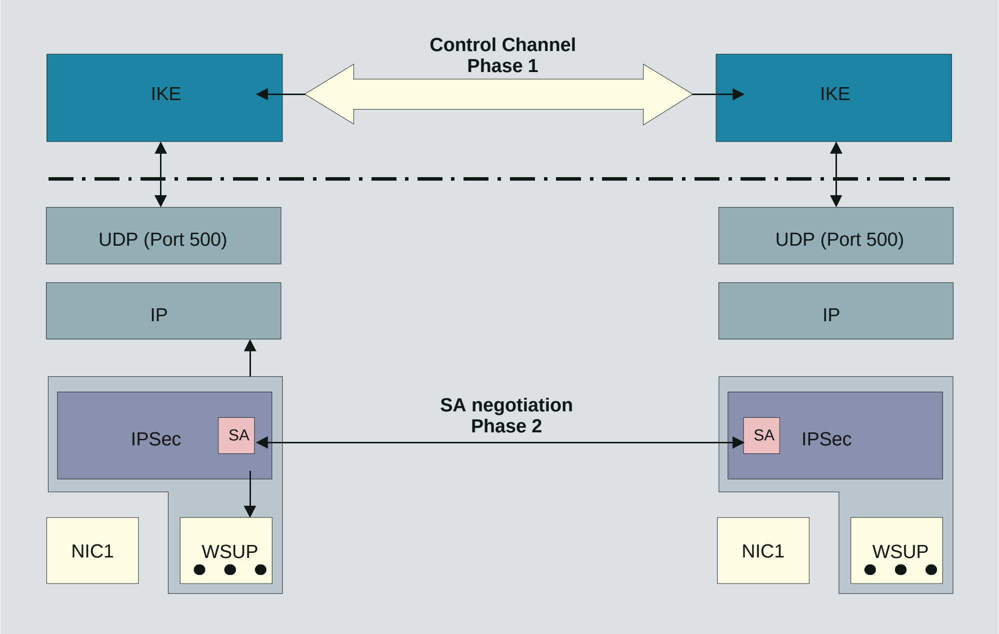
IPSec establishes the control channel in tunnel mode over the IKE protocol to the IP address of the secure gateway. In Transport mode it is established directly to the IP Address of the other side.

You define parameters to determine encryption and authentication type over the IKE protocol in the IKE Policies. Thus an authentication can be achieved via a pre-shared key or RSA signature. (These IKE guidelines are referenced in the IPSec editor.)

- **Phase 2 (IPSec Policy)**

The SA negotiation is concluded over the control channel. From the IPSec engine the SA is handed-off to the IKE protocol that it transmits over the control channel to the IPSec engine.

### Control Channel and SA Negotiation



*Description of the Graphic:*

*The SA must first have been negotiated in order for the IPSec process to start. This SA negotiation takes place once per SPD (which can be created for different ports, addresses, and protocols). This SA negotiation requires a control channel.*

*First the client must create a Layer 2 (PPP) link to the provider. With this link the client is assigned a new IP address each time he dials in. The IPSec module in the client receives an IP frame with the destination address of the corporate network. An SPD entry for this IP frame will be found but no SA exists at this time. The IPSec module then issues a request to the IKE module to negotiate an SA. Thus the requested security policies as present in the SPD entry are handed off to the IKE module. Negotiating an IPSec-Security Association (IPSec-SA) is considered a Phase 2 negotiation. However before an IPSec-SA can be negotiated with the other side (Secure Server) a kind of control channel from the client to the Secure Server (VPN) gateway must first exist. This control channel is established via the Phase 1 negotiation whose result is an IKE- Security Association (IKE-SA). Thus the Phase 1 negotiation undertakes the complete authentication of the client relative to the Secure Server and generates an encrypted control channel. Then the Phase 2 negotiation (IPSec-SA) can immediately take place over this control channel. The Phase 1 negotiation is a handshake over which the exchange of certificates is possible and it contains key exchange for the control channel.*

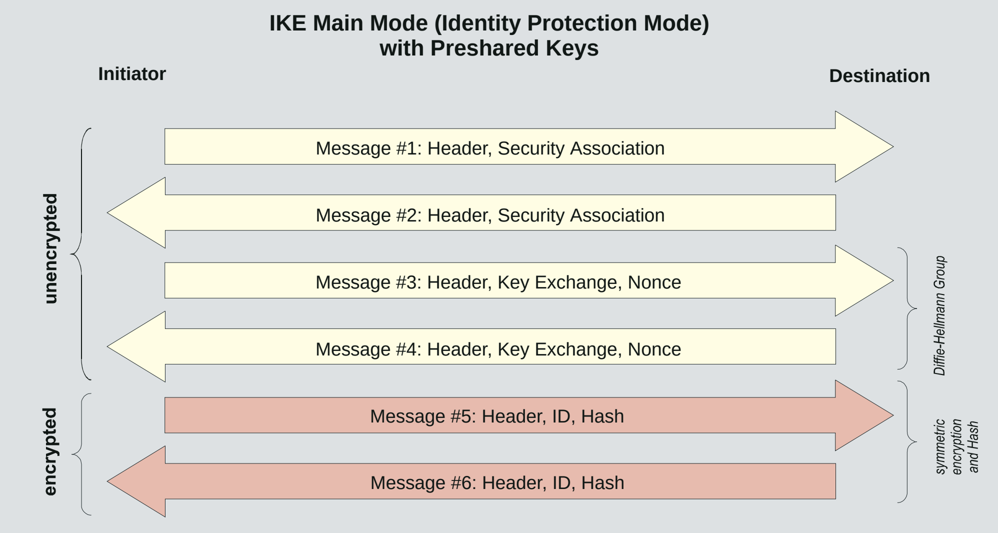
## IKE Modes

Essentially two types of IKE policies can be configured. They differ according to the type of authentication, which can be either over Pre-shared Key or RSA signature. Each of the two types of Internet Key Exchange can be executed in two different modes. These are; Main Mode also referred to as Identity Protection Mode or Aggressive Mode. These modes are differentiated by the number of messages and by the encryption.

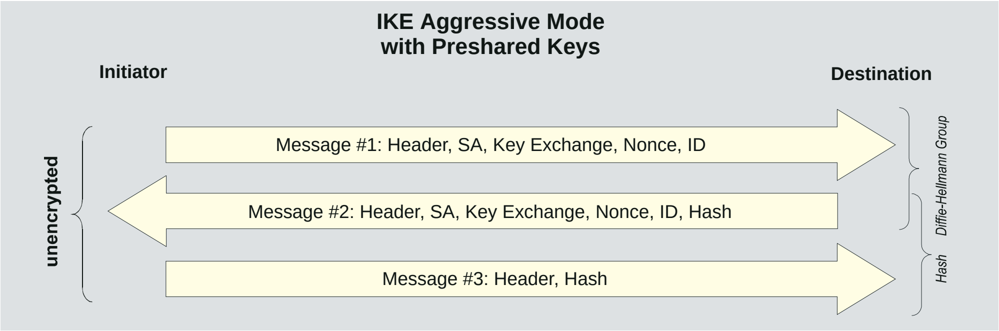
In Main Mode (standard setting) six messages are sent over the Control Channel and the last two messages are encrypted. The last two messages contain the user ID, the signature, the certificate and, if required, a hash value. This is why it is also known as Identity Protection Mode.

In Aggressive Mode only three messages are sent over the Control Channel and nothing is encrypted.

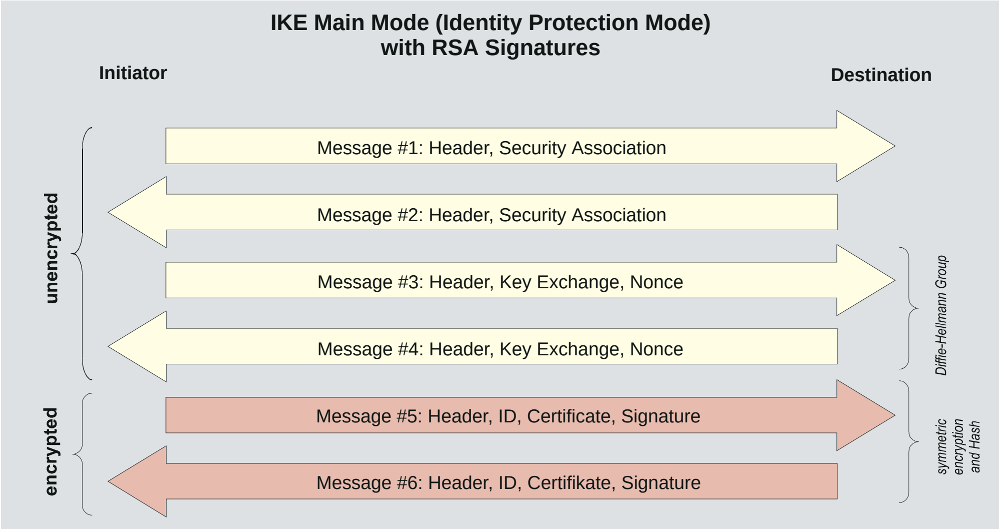
You determine the IKE mode (Exchange Mode), Main Mode or Aggressive Mode “Security” parameter fields under “Link Profiles” (for a dynamic SPD) and under “IPSec, Secure Policy Database” (for a static SPD). (See also → Exchange Mode).


IKE Main Mode (Identity Protection Mode)
with Preshared Keys
Initiator
Destination
Message #1: Header, Security Association
Message #2: Header, Security Association
Message #3: Header, Key Exchange, Nonce
Message #4: Header, Key Exchange, Nonce
Message #5: Header, ID, Hash
Message #6: Header, ID, Hash
unencrypted
encrypted
Diffie-Hellmann Group
symmetric
encryption
and Hash

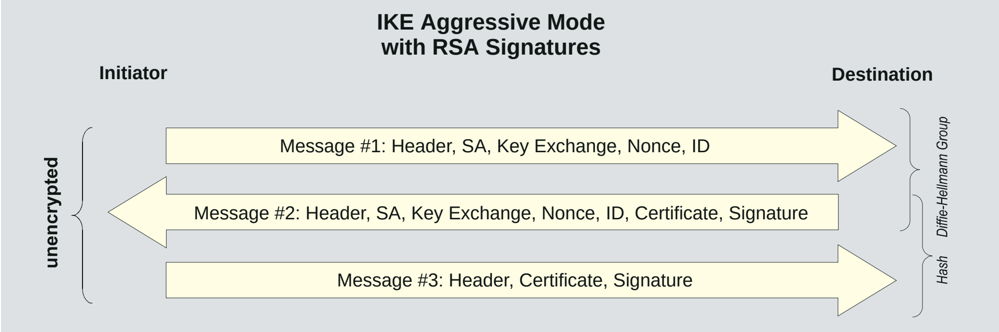
*If the pre-shared key method is used in Main Mode then the client on the VPN/Gateway must be clearly identifiable by his IP address. This is because the pre-shared key will be introduced into the symmetric key calculation and encrypted before the transfer of any other information that could identify the client. However a client dialing in to the provider is not identifiable by an IP address because he receives a new one with each dial in. This means that in Main Mode only the same pre-shared key can be given out which weakens the authentication.*



*One possibility to avoid a general pre-shared key would be to use the Aggressive Mode (see above graphic), however in this case the client ID is not encrypted.*


IKE Main Mode (Identity Protection Mode)
with RSA Signatures
Initiator
Destination
unencrypted
encrypted
Message #1: Header, Security Association
Message #2: Header, Security Association
Message #3: Header, Key Exchange, Nonce
Message #4: Header, Key Exchange, Nonce
Message #5: Header, ID, Certificate, Signature
Message #6: Header, ID, Certifikate, Signature
Diffie-Hellmann Group
symmetric encryption and Hash

*If RSA signatures have been set (Graphic above and below), then this means that certificates will be used and thus pre-configuration of all "secrets" is no longer relevant.*


IKE Aggressive Mode
with RSA Signatures
Initiator
Destination
unencrypted
Message #1: Header, SA, Key Exchange, Nonce, ID
Message #2: Header, SA, Key Exchange, Nonce, ID, Certificate, Signature
Message #3: Header, Certificate, Signature
Diffie-Hellmann Group
Hash

### 7.2.4 IPSec Tunneling

The compatibility with other manufactures relies on the ability to conform to the IPSec RFC's and to some drafts (official or not). The IPSec Client running in IPSec compatible mode supports the following RFC's and drafts:

RFC 2104 - Keyed-Hashing for Message Authentication
RFC 2401 - Security Architecture for the Internet Protocol
RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH
RFC 2404 - The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2406 - IP Encapsulating Security Payload (ESP)
RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 - The Internet Key Exchange (IKE)
DRAFT - draft-beaulieu-ike-xauth-05 (XAUTH)
DRAFT - draft-dukes-ike-mode-cfg-02 (IKECFG)
DRAFT - draft-ietf-ipsec-dpd-01 (DPD)
DRAFT - draft-ietf-ipsec-nat-t-ike-01 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-02 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-03 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-05 (NAT-T)
DRAFT - draft-ietf-ipsec-udp-encaps-06 (UDP-ENCAP)

- **Implemented Algorithms for Phase 1 and 2:**

***Supported authentication methods for phase 1 (IKE policy)***

– RSA signature.

– PSK (Pre-shared Key)

***Supported symmetric encryption algorithms (phase 1 & 2)***

– DES.

– 3DES.

– AES-128, AES-192, AES-256.

***Supported asymmetric encryption algorithms (phase 1 & 2)***

– DH 1,2,5 ( Diffie-Hellmann )

– RSA

### *Supported hash algorithms*

– MD5

– SHA-1

### *Additional phase 2 support*

– PFS (Perfect Forward Secrecy)

– IPCOMP (LZS)

– Seamless re-keying

When a profile entry with IPSec tunneling is defined some defaults will be set automatically.

These defaults are:

– IKE phase 1 policies - Automatic Mode

– IKE phase 2 policies - Automatic Mode

– IKE phase 1 mode RSA - Main Mode.

– IKE phase 1 mode PSK - Aggressive Mode.

These policies and negotiation modi are set automatically but, alternatively they can be configured manually in the Phonebook. They can therefore be modified if necessary for other requirements.

## Default mode proposals

1. With the setting “Assigned by Destination” and the “Preshared Key” field left empty, the following proposals for the IKE policy will be sent to the destination by default and a certificate will be used for authentication (refer to → IKE Policy, Phase 1 Parameter):

Notation:

```
EA    = Encryption Algorithm (Verschlüsselung)
HASH  = Hash Algorithm (Hash)
AUTH  = Authentication Method (Authentisierung)
GROUP = Diffie-Hellmann Group Number (DH-Gruppe)
LT    = Life Type (Dauer)
LS    = Life Seconds (Dauer)
KL    = Key Length (Schlüssellänge)

EA      HASH AUTH      GROUP LT      LS    KL
AES_CBC SHA  XAUTH_RSA DH5   SECONDS 28800 256
AES_CBC MD5  XAUTH_RSA DH5   SECONDS 28800 256
AES_CBC SHA  RSA       DH5   SECONDS 28800 256
AES_CBC MD5  RSA       DH5   SECONDS 28800 256
AES_CBC SHA  XAUTH_RSA DH2   SECONDS 28800 256
AES_CBC MD5  XAUTH_RSA DH2   SECONDS 28800 256
AES_CBC SHA  RSA       DH2   SECONDS 28800 256
AES_CBC MD5  RSA       DH2   SECONDS 28800 256
AES_CBC SHA  XAUTH_RSA DH5   SECONDS 28800 192
AES_CBC MD5  XAUTH_RSA DH5   SECONDS 28800 192
AES_CBC SHA  RSA       DH5   SECONDS 28800 192
AES_CBC MD5  RSA       DH5   SECONDS 28800 192
AES_CBC SHA  XAUTH_RSA DH5   SECONDS 28800 128
AES_CBC MD5  XAUTH_RSA DH5   SECONDS 28800 128
AES_CBC SHA  RSA       DH5   SECONDS 28800 128
AES_CBC MD5  RSA       DH5   SECONDS 28800 128
AES_CBC SHA  XAUTH_RSA DH2   SECONDS 28800 128
AES_CBC MD5  XAUTH_RSA DH2   SECONDS 28800 128
AES_CBC SHA  RSA       DH2   SECONDS 28800 128
AES_CBC MD5  RSA       DH2   SECONDS 28800 128
DES3    SHA  XAUTH_RSA DH5   SECONDS 28800 0
DES3    MD5  XAUTH_RSA DH5   SECONDS 28800 0
DES3    SHA  RSA       DH5   SECONDS 28800 0
DES3    MD5  RSA       DH5   SECONDS 28800 0
DES3    SHA  XAUTH_RSA DH2   SECONDS 28800 0
DES3    MD5  XAUTH_RSA DH2   SECONDS 28800 0
DES3    SHA  RSA       DH2   SECONDS 28800 0
DES3    MD5  RSA       DH2   SECONDS 28800 0
```

If a specific IKE proposal is entered in the IPSec configuration of profile settings, the same proposal will automatically be generated with Extended Authentication and sent.

2. If a string is entered in the “Preshared Key” field, the following proposals for the IKE policy will be sent to the destination by default and no certificate will be used for authentication.

| EA | HASH | AUTH | GROUP | LT | LS | KL |
|---|---|---|---|---|---|---|
| AES_CBC | SHA | XAUTH_PSK | DH5 | SECONDS | 28800 | 256 |
| AES_CBC | MD5 | XAUTH_PSK | DH5 | SECONDS | 28800 | 256 |
| AES_CBC | SHA | PSK | DH5 | SECONDS | 28800 | 256 |
| AES_CBC | MD5 | PSK | DH5 | SECONDS | 28800 | 256 |
| AES_CBC | SHA | XAUTH_PSK | DH2 | SECONDS | 28800 | 256 |
| AES_CBC | MD5 | XAUTH_PSK | DH2 | SECONDS | 28800 | 256 |
| AES_CBC | SHA | PSK | DH2 | SECONDS | 28800 | 256 |
| AES_CBC | MD5 | PSK | DH2 | SECONDS | 28800 | 256 |
| AES_CBC | SHA | XAUTH_PSK | DH5 | SECONDS | 28800 | 192 |
| AES_CBC | MD5 | XAUTH_PSK | DH5 | SECONDS | 28800 | 192 |
| AES_CBC | SHA | PSK | DH5 | SECONDS | 28800 | 192 |
| AES_CBC | MD5 | PSK | DH5 | SECONDS | 28800 | 192 |
| AES_CBC | SHA | XAUTH_PSK | DH5 | SECONDS | 28800 | 128 |
| AES_CBC | MD5 | XAUTH_PSK | DH5 | SECONDS | 28800 | 128 |
| AES_CBC | SHA | PSK | DH5 | SECONDS | 28800 | 128 |
| AES_CBC | MD5 | PSK | DH5 | SECONDS | 28800 | 128 |
| AES_CBC | SHA | XAUTH_PSK | DH2 | SECONDS | 28800 | 128 |
| AES_CBC | MD5 | XAUTH_PSK | DH2 | SECONDS | 28800 | 128 |
| AES_CBC | SHA | PSK | DH2 | SECONDS | 28800 | 128 |
| AES_CBC | MD5 | PSK | DH2 | SECONDS | 28800 | 128 |
| DES3 | SHA | XAUTH_PSK | DH5 | SECONDS | 28800 | 0 |
| DES3 | MD5 | XAUTH_PSK | DH5 | SECONDS | 28800 | 0 |
| DES3 | SHA | PSK | DH5 | SECONDS | 28800 | 0 |
| DES3 | MD5 | PSK | DH5 | SECONDS | 28800 | 0 |
| DES3 | SHA | XAUTH_PSK | DH2 | SECONDS | 28800 | 0 |
| DES3 | MD5 | XAUTH_PSK | DH2 | SECONDS | 28800 | 0 |
| DES3 | SHA | PSK | DH2 | SECONDS | 28800 | 0 |
| DES3 | MD5 | PSK | DH2 | SECONDS | 28800 | 0 |

The client sends the following IPSEC (phase2) default proposals.

Notation:

```
PROTO   - Protocol (Protokoll)
TRANS   - Transform (Transformation (ESP))
LT      - Life Type (Dauer)
LS      - Life Seconds (Dauer)
KL      - Key Length (Schlüssellänge)
COMP    - IP Compression (Transformation (Comp))
```

| PROTO | TRANS | AUTH | LT | LS | KL | COMP | LZS |
|---|---|---|---|---|---|---|---|
| ESP | AES | MD5 | SECONDS | 28800 | 128 | Yes | Yes |
| ESP | AES | SHA | SECONDS | 28800 | 128 | Yes | Yes |
| ESP | AES | MD5 | SECONDS | 28800 | 128 | No | No |
| ESP | AES | SHA | SECONDS | 28800 | 128 | No | No |
| ESP | AES | MD5 | SECONDS | 28800 | 192 | Yes | Yes |
| ESP | AES | SHA | SECONDS | 28800 | 192 | Yes | Yes |
| ESP | AES | MD5 | SECONDS | 28800 | 192 | No | No |
| ESP | AES | SHA | SECONDS | 28800 | 192 | No | No |
| ESP | AES | MD5 | SECONDS | 28800 | 256 | Yes | Yes |
| ESP | AES | SHA | SECONDS | 28800 | 256 | Yes | Yes |
| ESP | AES | MD5 | SECONDS | 28800 | 256 | No | No |
| ESP | AES | SHA | SECONDS | 28800 | 256 | No | No |
| ESP | DES3 | MD5 | SECONDS | 28800 | 0 | Yes | Yes |
| ESP | DES3 | MD5 | SECONDS | 28800 | 0 | No | No |

## 7.2.5 Further Configuration

*Pre-shared Key* or *RSA Signature*: According to the defaults through the other side, the automatic setting “Automatic Mode” can be changed as IKE policy to, “Preshared Key” or “RSA Signature” (certificate). If the other side expects “Pre-shared key”, then the key must be entered in the field. (The “Preshared Key” must be identical for all clients in this case.)

*IP addresses* and *DNS server* are assigned via the IKE Config Mode protocol (Draft 2) (currently compatible only against Cisco). All previous WAN interfaces can be used for the NAS dial-in.

The *authentication* for IPSec Tunneling is handled via the XAUTH protocol (Draft 6). If “IPSec Tunneling” is used, then additionally the following parameters must still be set in the “Identities" configuration field:

| | | |
|---|---|---|
| Username | = | User Name of the IPSec user |
| Password | = | Password of the IPSec user |
| User access data from configuration | = | optional |

DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background for “IPSec Tunneling” when supported by the destination. The IPSec client uses DPD to check, in regular intervals, whether the other side is still active. If the other side is inactive, then an automatic connection-disconnect occurs. Using NAT Traversal is automatic with the IPSec client and is always necessary if network address translation is used on the side of the destination system device.

### ■ Basic configurations depending on the IPsec gateway

The configuration possibilities that you must be aware of depending on whether the Ipsec gateway supports Extended Authentication (XAUTH) and IKE config mode or not, are listed below.

#### *Gateway does not support XAUTH*

As initiator, the IPSec Client always suggests Extended Authentication as standard. This property cannot be configured. If the gateway does not support Extended Authentication, then it will not be executed.

#### *Gateway supports IKE config mode*

If the gateway supports the IKE config mode, the function “Use IKE Config Mode” in the paramaeter field “IP Address Assignment” could be activated.

### *Gateway does not support IKE config mode*

If the gateway does not support the IKE config mode, then two configurations are possible.

1. The IP address is defined as “Manual IP address” (see → Profile Settings, IP Address Assignment), the IP address must be entered which has been specified by the gateway or by the administrator.

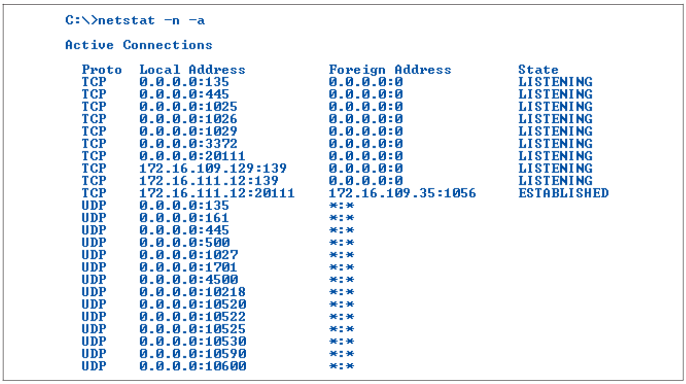
2. The function “Use local IP address” (see → Profile Settings, IP Address Assignment) causes the private IP address to be set equal to the public IP address, that the client gets per each Internet session from the provider, or if under the “LAN” connection type, the address that the LAN adapter has.

   If the “private IP address” has been set and the ”Type" is set to “IP address” in the parameter folder “Identities”, then there is no need to enter an IP address in the field for the “ID”. This is the only way to ensure that each current public IP address will be transferred to the gateway automatically for phase 1 identification.

## 7.2.6 IPsec ports for connection establishment and data traffic

Please note that the server requires exclusive access to UDP port 500. If NAT Traversal is used, then access to port 4500 is also required. Without NAT Traversal the IP protocol ESP (protocol ID 50) is used. Port 500, which is used for connection establishment under Windows systems, is used as standard by the IPsec policies. To change this, proceed as follows:

1. To determine which ports are currently being used by your system, you can enter the following command under the Command Prompt:
   `netstat -n -a`
   to display current network status.

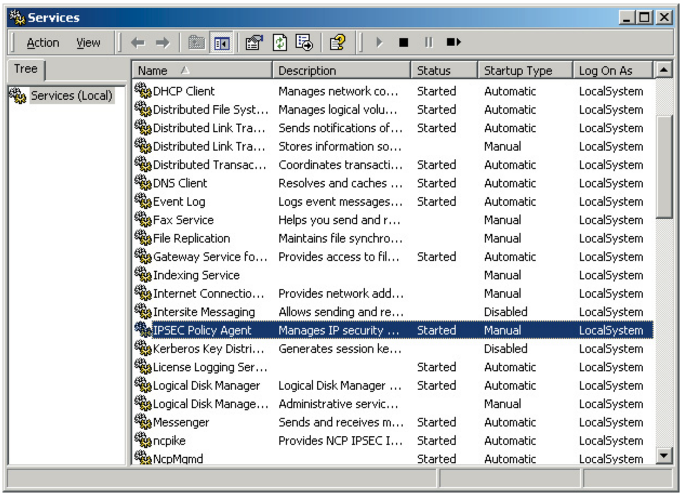


```
C:\>netstat -n -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:20111          0.0.0.0:0              LISTENING
  TCP    172.16.109.129:139     0.0.0.0:0              LISTENING
  TCP    172.16.111.12:139      0.0.0.0:0              LISTENING
  TCP    172.16.111.12:20111    172.16.109.35:1056     ESTABLISHED
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:161            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1027           *:*
  UDP    0.0.0.0:1701           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:10218          *:*
  UDP    0.0.0.0:10520          *:*
  UDP    0.0.0.0:10522          *:*
  UDP    0.0.0.0:10525          *:*
  UDP    0.0.0.0:10530          *:*
  UDP    0.0.0.0:10590          *:*
  UDP    0.0.0.0:10600          *:*
```

2. If the port is used, then the “System / Services - Administration” window must be opened in the Windows Start menu. The “IPsec policy agent” is highlighted in this window, the service stops and the “Autostart type” is set to “Manual”.



| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| DHCP Client | Manages network co... | Started | Automatic | LocalSystem |
| Distributed File Syst... | Manages logical volu... | Started | Automatic | LocalSystem |
| Distributed Link Tra... | Sends notifications of... | Started | Automatic | LocalSystem |
| Distributed Link Tra... | Stores information so... | | Manual | LocalSystem |
| Distributed Transac... | Coordinates transacti... | Started | Automatic | LocalSystem |
| DNS Client | Resolves and caches ... | Started | Automatic | LocalSystem |
| Event Log | Logs event messages... | Started | Automatic | LocalSystem |
| Fax Service | Helps you send and r... | | Manual | LocalSystem |
| File Replication | Maintains file synchro... | | Manual | LocalSystem |
| Gateway Service fo... | Provides access to fil... | Started | Automatic | LocalSystem |
| Indexing Service | | | Manual | LocalSystem |
| Internet Connectio... | Provides network add... | | Manual | LocalSystem |
| Intersite Messaging | Allows sending and re... | | Disabled | LocalSystem |
| IPSEC Policy Agent | Manages IP security ... | Started | Manual | LocalSystem |
| Kerberos Key Distri... | Generates session ke... | | Disabled | LocalSystem |
| License Logging Ser... | | Started | Automatic | LocalSystem |
| Logical Disk Manager | Logical Disk Manager ... | Started | Automatic | LocalSystem |
| Logical Disk Manage... | Administrative servic... | | Manual | LocalSystem |
| Messenger | Sends and receives m... | Started | Automatic | LocalSystem |
| ncpike | Provides NCP IPSEC I... | Started | Automatic | LocalSystem |
| NcpMgmd | | Started | Automatic | LocalSystem |

3. If the Autostart type change has been executed, then the command:
   `netstat -n -a`
   can be executed again. In this case UDP port 500 should no longer be listed under the active connections.

## 7.3 Certificate Checks

In addition to the certificate verification according to content a certificate check is executed on the Secure Client in many respects.

### 7.3.1 Selection of the CA Certificates

The corporate network administrator specifies which issuers of certificates can be trusted. This is done by copying the CA certificates of his choice into the installation directory under CACERTS\. The copying over can be automated with diskettes in a software distribution, if the issuer certificates are located in the root directory of the first diskette at the installation. Afterwards issuer certificates can be automatically distributed via the Secure Update Server (see → Update Server Manual), or if the user has the requisite write authorizations in the designated directory – they can be set by the user himself (see → Display CA Certificates.

The formats *.pem and *.crt are supported for issuer certificates. They can be viewed in the monitor under the menu item “Connection – Certificates – Display CA Certificates”.

If the issuer certificate of another side is received, then the IPSec Client determines the issuer, then searches the issuer certificate, first on Smart Card or PKCS#12, and then in the installation directory under CACERTS\. If the issuer certificate cannot be found, then the connection cannot be established. If no issuer certificates are present, then no connection will be permitted.

### 7.3.2 Check of Certificate Extensions

Certificates can experience extensions. These serve for the linking of additional attributes with users or public keys, that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written in the certificate by the issuing certificate authority.

Three extensions are significant for the Secure Client and the Secure Server:

□ extendedKeyUsage

□ subjectKeyIdentifier

□ authorityKeyIdentifier

- **extendedKeyUsage**

If the extendedKeyUsage extension is present in an incoming user certificate, then the Secure Client checks whether the defined extended application intent is “SSL Server Authentication”. If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Please note that the SSL server authentication is direction-dependent. This means that the initiator of the tunnel establishment checks the incoming certificate of the other side, if the extendedKeyUsage extension is present, then the intended purpose must contain “SSL Server Authentication”. This applies as well for callback to the Client via VPN.

Exception: For a server call-back to the client after a direct dial-up, without VPN but with PKI, the server checks the client certificate for the extendedKeyUsage extension. If this is present, then the intended purpose “SSL Server Authentication” must be contained otherwise the connection will be rejected. If this extension is not present in the certificate, then this will be ignored.

- **subjectKeyIdentifier / authorityKeyIdentifier**

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer’s public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA certificate is found then the connection is rejected.

The keyidentifier designates the public key of the certification authority and thus not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determining a certificate path.

In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

### 7.8.3 Checking Revocation Lists

The Secure Server can be provided with the associated CRL (Certificate Revocation List) for each issuer certificate. It will be copied into the installation directory under CRLS\. If a CRL is present, then the Secure Client checks the incoming certificates to see if they are listed in the CRL. The same applies for an ARL (Authority Revocation List) that must be copied into the installation directory under ARLS\ Windows directory.

## 7.4 Stateful Inspection Technology for the Firewall- Settings

The Stateful Inspection firewall technology can be used for all network adapters as well as for RAS connections. It is activated on the client in the telephone book under “Firewall settings” (see → Configuration parameters, Firewall settings). It is then active on the gateway if the “Protect LAN adapter” function has been switched on in the Server Manager under “Routing interfaces – General”.

The fundamental task of a firewall is to prevent hazards from other networks or external networks (Internet), from spreading in your own network. This is why a firewall is also installed at the junction between corporate network and the Internet, for instance. It checks all incoming and outgoing data packets and decides whether a data packet will be allowed through, or not, based on previously specified configurations.

Stateful Inspection is the Firewall technology that currently offers the highest possible security for Internet connections, and thus for the corporate network. Security is assured in two aspects. On one hand this functionality prevents unauthorized access to data and resources in the central data network. On the other hand, it monitors the status of all existing Internet connections as control instance. Furthermore the Stateful Inspection firewall recognizes whether a connection has opened “spawned connections” – as is the case for instance with FTP or Netmeeting – whose packets likewise must be forwarded. The Stateful Inspection Internet connection appears as a direct line to the communication partner, which may only be used for a data transfer according to the agreed upon rules. Alternative designations for Stateful Inspection are: Stateful Packet Filter, Dynamic Packet Filter, Smart Filtering, and Adaptive Screening.

Stateful Inspection conceptually unifies the protective possibilities of packet filter and application level gateways; this means it integrates the functions of both security processes as a hybrid and works on the network layer as well as on the user layer. With “condition-dependent packet filtering” not only are the Internet and transport layer taken into consideration, but the dependencies from the state of a connection are also taken into consideration. All current and initiated connections are stored with address and allocated port in a dynamic connection table. The Stateful Inspection filter decides which packets belong to which connection based on a specified raster (information). States can be: connection establishment, transfer, or connection disconnect, and they apply for TCP as well as for UDP connections. An example using a Telnet session: The state “Connection establishment” is defined in that user authentication has yet taken place. If the user has logged in with user name and password, then this connection is set to the “normal connection” state. Because the respective state of a connection is constantly monitored, access to the internal corporate network remains denied to unauthorized parties.

The advantage relative to static packet filters is that the decision whether an  Secure Gateway or Client will forward a packet or not, is not based on source address, destination address or ports. The security management also checks the state of the connection to a partner. Only those packets are forwarded that belong to an active connection. Data packets that cannot be assigned to an established connection are rejected and recorded in the log file. New connections can only be opened according to the configured rules.

In the simplest firewall function, only the incoming and outgoing connections are tested and monitored relative to the protocol (TCP/IP, UDP/IP, ICMP, IPX/SPX), the appropriate ports, and the participating computers. Connections are permitted or blocked depending on a specified system of rules. Further tests (such as content or transferred data) do not take place.

The Stateful Inspection filters are a further development of the dynamic packet filter and offer a more complex logic. The firewall checks whether a connection allowed on the port filter can also be established for the defined purpose.

The following additional information about a connection is also managed:

– Connection identification number
– State of the connection (such as establishment, data transfer, disconnect)
– Source address of the first packet
– Destination address of the first packet
– Interface through which the first packet came
– Interface through which the first packet was sent

Based on this information the filter can decide which subsequent packets belong to which connection. Thus a Stateful Inspection system can also eliminate the UDP problem. This involves the relative ease with which UDP packets can be forged, such as is the case with UDP-based DNS service. Because Stateful Inspection filters can note the current status and context information of a communication relationship, it is necessary that source and destination address as well as source and destination port, and also the DNS header in the query packet be included when saving the status and context information. The system executes an interpretation on the application layer.

Example: An incoming connection to port 21 of a computer is an FTP connection for a pure port filter. An additional test does not take place. On the other hand, the Stateful Inspection filter additionally checks whether the data transferred via this connection belong to an established FTP connection. If not, then the connection will be disconnected immediately. In addition, a Stateful Inspection filter is able to adapt rules depending on necessary communication processes. If, for example, an outgoing FTP connection is allowed, then the firewall also automatically enables the establishment of the associated reverse channel. The corresponding information (ports) is read out of the control connection.

One advantageous aspect of Stateful Inspection filters is the capability to check the data on all protocol layers (this means from the network layer to the application layer). Thus for example an FTP-GET can be allowed, however an FTP-PUT can be prohibited. A positive effect of the increased intelligence relative to conventional packet filters is the option of assembling individual packets during a communication relationship, and thus bring extended possibilities for user authentication to the application. Stateful Inspection filters are not immune to certain attacks that take place on the lower protocol layers as a consequence of the undependable separation of the network segments. Thus for instance, fragmented packets (usually from outside to inside) will be allowed through without further testing.

# Abbreviations and Technical Terms

**3DES**

TripleDES. Standard of Encryption with 112 Bits.

**AES**

Abbreviation for Advanced Encryption Standard. It is a European development of Belgian encryption experts Joan Daemen and Vincent Rijmen (“Rijndael algorithm”), and supercedes DES (Data Encryption Standard). This is an encryption algorithm that has key lengths of up to 256 bits. Thus N to the 256th power is the measuring unit for the number of possible keys that can be generated with this algorithm. In spite of increasing processor speeds it is expected that the AES algorithm will offer acceptable security for the next 30 years. AES will soon find wide distribution in VPN and SSL encryptions.

**AH**

Authentication Header RFC 2402

**Analog Interface**

This is an interface for connecting analog devices (e.g. modems, facsimile group 3 machines, analog telephones etc.). The current international standard connector for analog devices is RJ11.

**Asymmetric Encryption**

(Public Key Process) In an asymmetric encryption each participant has two keys: a secret private key and a public key. Both keys stand in a mathematically defined relationship to each other (2 Key Service). The participant’s private key is strictly secret; the public key is available to anyone. Key management is straightforward even with large numbers of participants. For example: Two keys per participant generate a total of 2000 keys to enable secure communication for 1000 participants in all sender-recipient combinations. RSA is the best-known asymmetric encryption process. The disadvantage of the asymmetric encryption process is that it is calculation-intensive and thus comparatively slow.

**Basic Connection**
**(So / BRI = Basic Rate Interface)**

A type of ISDN connection with So-interface. (“S” stands for subscriber interface: user interface). It consists of a D-Channel (bandwidth: 16 kBits/s) for controlling and two B-Channels (bandwidth: 64 kBits/s each) for data transmission.

**Basic Rate Interface (BRI)** An ISDN subscriber service that uses 2 B-Channels (64 Kbps) and 1 D-Channel (16 Kbps) to transmit data, audio, voice and video signals over a digital dial-up circuit. BRI's are available from your local PTT.

**BCP** Bridge Control Protocol

**BITS** Bump In The Stack - A type of IPSec implementation.

**BITW** Bump In The Wire - A type of IPSec implementation.

**Blowfish** Encryption Standard with 128/448 Bit

**Browser (Web Browser)** This is the user interface to the Internet. With its HTTP (Hypertext Transfer Protocol) capability it can handle different formats (for example HTML, GIF, CAD) that are required for a multi-media (sound and graphics) representation of the information.

**CA (Certification Authority)** Also Trust Center (for example D-trust, a combined undertaking of Debis and the Federal Printing Office). With PKI Manager Software a CA issues digital, signed confirmations (certificates) and stores them on a Smartcard (Chipcard). A CA can be a private service provider or a public institution. These certifying authorities do not need government permission and the private service provider or public institution is liable for the correctness of the certificates.

**CAPI** Common Application Program Interface. This interface is designated as a common ISDN API in ISDN and corresponds to the PCI interface (Programmable Communication Interface). The interface direct access to ISDN and the lower protocol layers (Layers 1-3). Higher-level protocols (applications) like telex and file transfer can be used regardless of the hardware platform implemented. There are two versions of CAPI, 1.1 and 2.0. The ISDN applications are programmed accordingly either for CAPI 1.1 or CAPI 2.0, or for the specific CAPI requirements. A hybrid CAPI allows implementation of application software for CAPI 1.1 as well as for CAPI 2.0 (see Hybrid CAPI).

**CCP**

Compression Control Protocol

**Certificates**

Certificates are issued by a CA (Certification Authority) with a PKI Manager (software) and stored on a Smartcard. This Smartcard contains digital signatures in addition to the Certificates. These digital signatures are equivalent to a digital personal identity card.

**CHAP**

Challenge Authentication Protocol

**CLI**

Calling Line Identification (Caller ID - Euro-ISDN)

**COSO**

Charge One Side Only. The low level callback is negotiated via D-Channel and uses call waiting via D-Channel. This method is very popular, because as opposed to PPP no local charge is assessed to the caller when dialing-up or connecting to the remote destination. The caller initiates the request for a connection on the ISDN D-Channel. The receiver establishes the connection and is charged.

**Cryptography**

Applications are encryption, electronic signature, authentication, and Hash Value Calculation. These are mathematical processes that are used with a key.

**CTAPI**

Interface to Smartcard Readers

**CUG**

Closed User Group (Euro-ISDN)

**DES**

Data Encryption Standard

**DHCP**

Communicating with DHCP (Dynamic Host Control Protocol) means that an IP Address is automatically assigned to you for every session.

**Directory Service**

Remote Accesses like Email addresses, telephone numbers etc. are stored in directories of various databases. Two problems are associated with this directory multiplicity, they are (1) large volumes of the same data must be captured many times (2) individual entries are not linked to each other. The maintenance required is enormous and inconsistencies cannot be ruled out. A standardized procedure is required that will facilitate the capture and maintenance of all information in a central directory. NCP Security Management supports the standardized protocols RADIUS (Remote Authorization dial-In User Service), and LDAP (Lightweight Directory Access Protocol). The latter insures access to centralized directory services.

**DMZ**

Demilitarized Zone - an area between the Firewall and the enterprise network with Web Servers, Email Servers and VPN Servers.

**DNS**

The Domain Name Server (DNS) makes the IP address available for an Internet session after dial-in with user name and password. It provides additional Internet routing in that it retranslates the given desired destination names into IP addresses and creates the connection to this address.

**DNS Server**

A computer with a database containing all relevant host computers (domain name addresses) and their corresponding IP addresses. When queried, the DNS Server responds by returning the IP address corresponding to the domain name address.

**D-Channel Protocol**

The D-Channel insures that terminals can communicate with the network. Among other things it monitors connection setup and breakdown. It includes Layers 2 and 3. HDLC is implemented on Layer 2 in ISDN for the logical data transfer. The actual D-Channel protocol resides on Layer 3. Currently DSS1 is available throughout Europe as D-Channel protocol.

**DSA**

Directory System Agent

**DSS1**

Abbreviation for the European standard Digital Subscriber System No.1. This is the European ISDN protocol for D-Channel.

**DUA**

Directory User Agent

**ECP**

Encryption Control Protocol

**EDI**

This is an abbreviation for Electronic Data Interchange, which is a set of standards for controlling the transmission of business documents (e.g. purchase orders and invoices) between computers.

**ESP**

Encapsulating Security Payload RFC 2406

**Euro-ISDN**

The International Telecommunications Union (ITU) standard for European ISDN, refers to the D-Channel Protocol DSS1 as well as various service features (e.g. Time & Charges, Completion of Calls to Busy Subscriber, Call Forwarding, Call Waiting, etc.). In Euro-ISDN the individual terminals are addressed with the D-Channel protocol DSS1 with the multiple subscriber number (MSN).

**Firewall**

A division between public network and private network. It is a protection mechanism that regulates the station access. A firewall computer seals off a network from unauthorized access, particularly from the WAN side. For example, authorization of incoming and outgoing connections is regulated by filtering out certain network participants and network services and by determining access rights. From the WAN perspective it is usually web servers, Email servers, and VPN servers that are located behind the firewall in the DMZ.

**FTP**

File Transfer Protocol. Based on TCP and TELNET (Port 21).

**FTP Server**

A fileserver that supports the File Transfer Protocol enabling users to download or upload files through the Internet or any other TCP/IP Network.

**GPRS**

Standard for fast handy communication

**GRE**

Generic Router Encapsulation. CISO specific tunneling protocol.

**GSM**

Global System Mobile. Standard for cellular communications

**Hash Value**

see Signature

**HBCI**

Standard for Smartcard Readers (Online Banking)

**HTTP**

Hypertext Transfer Protocol. (Port 80)

**Hybrid Encryption**

High performance and high security: Hybrid encryption combines the advantages of symmetric and asymmetric processes. While communication content is secured with fast symmetric algorithms, participant authentication and key exchange occur on the basis of asymmetric processes. Actual document data encryption is determined by a random number (session key) that is generated for each individual communication connection. This one-time key is encrypted with the recipient’s public key and the message is added. Then the recipient reconstructs the session key with his private key and decrypts the message.

**IETF**

Internet Engineering Task Force.

**IKE**

Internet Key Exchange, which is part of IPsec for secure key management, separate security association negotiation, and key management protocol RFC 2409.

**Internet**

The Internet is a worldwide open computer network. It is open to all. Every company and each individual can connect to the Internet and can communicate with all other connected users regardless of the computer platform or the respective network topology. A general shared network protocol is necessary to insure that data exchange between the different computers and networks is possible (see TCP/IP).

**Intranet**

A network within a company or organization employing applications associated with the Internet, such as Web pages, Web browsers, FTP Sites, E Mail, etc. However these are only accessible to those within the company or organization.

**IP Address**

Each computer in the Internet has an IP address (Internet Protocol Address) that clearly identifies it for as long as it is part of the Internet. An IP address is 32 bits long and consists of four numbers separated from each other by a dot. There are 8 bits available for each number thus it can take on 256 values. However the total number of possible IP addresses remains limited. The internet user thus does not receive a one-time non-modifiable number assigned to him, rather for every one of his sessions he gets the IP address that has not yet been assigned. The IP addresses are assigned for the duration of a time slice. This assignment of address is usually an automatic PPP negotiation over DHCP. Special programs can translate the IP address into a name. These programs run on a Domain Server.

**IP Network Address Translation** IP Network Address translation is already setup when the workstation software is installed and it is activated as default when a new destination system is created! When IP network address translation is used all transmitted frames are sent with the negotiated (PPP) IP address. The workstation software translates this official IP address into the system's own Internet address, or in the case of a workstation, into its own user defined IP address. In general it is possible with NAT to work in a LAN with unofficial IP addresses that are not valid in the Internet and, in spite of that fact, access the Internet from the LAN. To make this possible the unofficial IP addresses are translated into official IP addresses by the software. This saves official Internet addresses, that are not available in unlimited numbers on the one hand, and on the other hand NAT establishes a certain protection (Firewall) for the LAN.

**IPCP** Internet Protocol Control Protocol

**IPsec** IETF Standards: RFC's 2401-2412 (12/98)

**IPX** Internet Packet Exchange, Netware protocol from Novell

**IPXCP** Internetwork Packet Exchange Control Protocol

**ISDN** Integrated Services Digital Network. A digital network that integrates all narrow band communication services (for example telephone, telex, fax, teletext, videotext) consisting of channels with a transfer speed 64.000 bit/s. A basic connection in the so-called narrow band ISDN has three transmission channels: channel B1 64,000 bits/ s, B2 64,000 bits/s, D-Channel 16,000 bits/s. The total transmission rate is 144,000 bits/s. By the end of the millennium this network should be uniformly extended throughout Europe. The specifications for ISDN are worked out by ITU and CEPT.

**ISDN Adapter** The products of the NCP Arrow family are ISDN adapters. They make it possible to connect existing non-ISDN capable terminals to the ISDN network. The adapter handles the software and the hardware adaptation of the terminal interface to the ISDN interface (So). An ISDN adapter with Upo terminal interface enables the conversion of ISDN two wire interface Upo (range 3.5 km) on bus-capable ISDN 4 wire interface So (range 150 m) with ISDN TK equipment in accordance with Telekom Guidelines.

**ISP**
Internet Service Provider

**ISO/OSI Reference Model**
The ISO standardized model that describes communication in 7 layers (7. Application Layer, 6. Presentation Layer, 5. Session Layer, 4. Transport Layer, 3. Network Layer, 2. Data Link Layer, 1. Physical Layer). Data transmitted in a network are processed consecutively 7 -1 as above. The order is reversed on the receiver side.

**L2F**
Tunnel / VPN protocol Layer 2 Forwarding

**L2TP**
Tunnel / VPN protocol Layer 2 Tunneling Protocol

**L2Sec**
NCP designation, functional description in RFC 2716

**LCP**
Link Control Protocol

**LDAP**
Lightweight Directory Access Protocol (see Directory Service)

**MAC Address**
This stands for Medium Access Control Layer Address. It is a physical address in the network.

**MIB**
Management Information Base

**MD5**
Message Digit 5. Used to generate a hash value.

**Name**
Exact Internet name, it is supposed to make it easier for the users to work on the Internet. The names are entered in the Internet browser and are then translated into IP addresses by the Domain Server.

**NAS**
Network Access System

**NetBios**
Network Basic Input Output System an interface that offers datagram and stream-oriented communication.

**OCSP**
Abbreviation for Online Certificate Status Protocol. It is a protocol used for online verification of certificates.

**PAP**

PAP Password Authentication Protocol. Security mechanism inside the PP for authenticating the other side. PAP defines a method according to which the establishment of a connection whereby the rights of the sender are checked based on a user name and password. In this process the password is sent over the line in clear text. The recipient compares the parameters with his own data and if in agreement releases the connection.

**PBX**

An abbreviation for Private Branch Exchange, which is an automatic telephone switching system that enables users within a company to place calls to each other without having to go through the public telephone network. Users of course can also make calls and receive calls from the public telephone network.

**PC/SC**

Interface to Smartcard readers

**PEM**

An older form of Soft Certificates (without private key).

**Personal Firewall**

Client software security mechanisms combine tunneling processes and personal Firewalling, IP Network Address Translation (IP-NAT), as well as universal filter mechanisms. IP Nat is of central importance then it ensures that only outgoing connections from the computer to the Internet are possible. Incoming data packets are checked on the basis of refined filtering for precisely defined characteristics and are discarded if there is no agreement. This means that the Internet port of the respective computer is completely camouflaged and the establishment of undesired connections is impossible.

**PIN**

Personal Identification Number

**PKCS**

Abbreviation for Public Key Cryptography System, an encryption system with public key.

**PKCS#10**

A method defining how a certificate is transferred from the PKI manager to the CA (Certification Authority). Usually via Http - encrypted with SSL as Https.

**PKCS#11** Basis for Smartcard standards

**PKCS#12** Soft certificate. A standard that describes the data structure syntax.

**PKCS#15** Smartcard pointer description. Indicates where what will be found on the Smartcard

**PKI** This is used for Key Management. Transaction-based security requires a clear partner authentication by means of certificates that have been issued by a trustworthy PKI. Particularly for E-commerce PKI offers the framework for confidentiality (secrecy), Integrity (counterfeit security), authenticity (identity security) and indisputability.

**PoP** Point of Presence

**POP3** Protocol, used for downloading Emails. Counterpart to SMTP (Port 10).

**PPP** Point-to-Point Protocol. Transmission protocol in connection oriented networks.

**PPP negotiation** In a PPP negotiation the IP address is assigned automatically after the logon at the provider.

**PRI** Primary Rate Interface. (ISDN interface, primary multiplex S2m with 30 B-Channels and 2 D-Channels.

**Radius** Remote Authorization Dial-In User Service, see Directory Service

**RA** Registration Authority. For the most part the registering location is the site that accepts the certificate application. The RA is also the site where the loss or deterioration of a valid certificate is reported. It is also the site that issues revocation lists for certificates that have become invalid.

**RAS** Remote Access services. Company Specific (Microsoft) dial in help for Remote Access Routing Information Protocol, also routing mode.

**Revocation list** The revocation list includes client certificates that have been revoked or blacklisted. When a user for example notifies the CA that their Smartcard has been stolen, the certificate will be revoked by the CA and entered in the Revocation List. Certificates that expire will not be listed in a revocation list. Revocation Lists are regularly updated.

**RIP**

Routing Information Protocol, also Routing Mode

**RFC**

Request for Comment. Blueprint for a standard or a pre-standard that is in discussion and will be kept in the list of RFC’s as long as it proves itself in practice. Earlier forms of RFC’s are drafts.

**Routing Tables**

Routers require information about the best routes from the source to the destination for route selection in the network. With the routing table’s help these segments are calculated. With static routing the tables have been firmly defined. In dynamic routing the router receives information about the network through router information protocols (for example RIP, NLSP, OSPF) that is collected and continuously updated in self-learning router tables.

**RSA**

The first procedure that fulfilled the demands for public key cryptographics. Invented 1977 by Ron Rivest, Adi Shamier and Leonard Adlemann.

**SHA**

Secure Hash Algorithm, see also Signature

**Signature**

A digital signature requires the generation of a mathematical link between document and the secret personal signature key of the participant. The document sender generates a checksum or so-called Hash Value, this he in turn codifies with his secret key and thus creates a digital signature addition to the original document. The document recipient can check the signature with the sender’s public key by constructing on his side the Hash value from the message and comparing it to the encrypted signature. Because the sender’s signature is directly bound into the document every later modification would be noticed. Also interception or eavesdropping of the signature through data interception is to no avail. The digital signature cannot be emulated or copied because it uses the secret key. It is impossible to determine the secret key from the signature.

**Smartcard**

If you use the functionality of the Smartcard after CHAP Authentication (User ID and Password) then the Strong Authentication with the stored certificates on the Smartcard and the Gateway will be executed. Among other things the user certificate, the root certificate, and the secret private key, are stored on the Smartcard. The Smartcard can only be used with a valid PIN.

**SMTP**
Simple Mail Transport Protocol. Internet standard to distribute Email. Based on TCP (Port 25). It is text oriented.

**SNA**
Systems Network Architecture. Hierarchically oriented network for the control of terminals and for application access support in IBM host systems.

**SNMP**
Simple Network Management Protocol. Network management protocol based on UDP/IP.

**Source Routing**
The possibility to optimize route selection between bridges in Token-Ring networks. With SNA, route information hanging on the datablock is also transmitted. In this manner the confirmation route is also clearly manifest.

**SPD**
Security Policy Database

**SSL**
Secure Socket Layer. According to the SSL protocol Dynamic Key Exchange can be used. SSL, developed by Netscape, in the meantime has be-come the standard protocol for Dynamic Key Exchange

**SSLCP**
Secure Socket Layer Control Protocol

**STARCOS**
Operating system for Smartcards

**Symmetric Encryption**
Sender and recipient use the same key for symmetric encryption and decryption. Symmetric algorithms are very fast and very secure - only if the key transfer between the sender and the recipient is not endangered. If an unauthorized person is in possession of the key then this person can decrypt all messages. In other words using the key he will appear as the message sender. If for larger groups of participants symmetric encryption is to be used so that each participant can only read messages addressed to him, then an individual key is required for each sender-recipient pair. This results in a somewhat cumbersome key management. For example, for 1000 participants 499,500 different

keys are necessary (!) to support all possible relationships. Currently the best-known symmetric encryption is the DES algorithm.

**TCP/IP** An abbreviation for Transfer Control Protocol / Internet Protocol, which is a network protocol used by computers to communicate with each other. TCP/IP can be used in most any LAN or WAN, regardless of the underlying topology (Token Ring, Ethernet, X.25, ISDN, Frame Relay etc.). TCP/IP also includes various Internet standards: FTP: File Transfer Protocol (for File Transfer) / SMTP: Simple Mail Transport Protocol (for E Mail) / TELNET: Teletype Network (for Terminal Emulation) / RLOGIN: Remote Login (for remote control purposes)

**TECOS** Operating system for Smartcards (V. 1.2, 2.0)

**Token Ring** Ring structure network topology from IBM.

**UDP** User Data Protocol. This builds directly on the underlying Internet protocol. It was defined to also provide application processes with the direct possibility to send datagrams. UDP delivers over and above the capabilities of TCP/IP simply a port number and checksum of the data. Due to the lack of overhead such as receipts and security mechanisms it is particularly fast and efficient.

**UMTS** Universal Mobile Telecommunications Service. Future Standard for fast mobile phone communication.

**VPN** Virtual Private Network. A VPN can be implemented as a virtual network over all IP carrier networks - that means the Internet as well. Two specifications have crystallized for the realization of a VPN: L2F (Layer 2 Tunneling) and L2TP (Layer 2 Tunneling Protocol) both processes serve to establish a tunnel that can be considered a “virtual leased line”. In addition to IP frames also IPX data, SNA data, and NetBios data are transparently transmitted over such a logical connection. At the end of the tunnel the data packets must be interpreted and transformed into a DataStream on the basis of the protocol used.

**WAN**

Abbreviation for Wide Area Network, which is a communications network that connects networks that are separated geographically. (normally LAN = Local Area Network). WANs are normally provided by PTTs or Carriers and generally speaking offer high speed connection (64 Kbps - 2 Mbps or higher).

**WAP**

Wireless Application Protocol. Developed by Nokia, Ericsson and Motorola.

**WINS**

An abbreviation for Windows Internet Naming Service, which is a Windows NT Server method for linking a computer's host name to its address. This was the original Microsoft derivative of DNS, and is also referred to as INS = Internet Naming Service.

**X.25**

An ITU (International Telecommunications Union) recommendation that specifies the connection between an end device (e.g. PC or terminal) and a packet switched network. X.25 and is based on three definitions. (1) the physical connection between the end device and the network, (2) the transmission access protocol, and (3) the implementation of virtual circuits between network users. Together, these definitions specify a synchronous, full duplex end device (terminal) to network connection.

**X.509 v3**

A Standard of Certification

# Index