



. . . c o n n e c t i n g y o u r b u s i n e s s

LANCOM Advanced VPN Client

Version 2.22 (Windows)

Version 1.00 (Mac OS X)

- Handbuch
- Manual

LANCOM Advanced VPN Client

Version 2.22 (Windows)

Version 1.00 (Mac OS X)

© 2010 LANCOM Systems GmbH, Wuerselen (Germany). All rights reserved.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software included with this product is subject to written permission by LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

All explanations and documents for registration of the products you find in the appendix of this documentation, if they were present at the time of printing.

Trademarks

Windows®, Windows XP® and Microsoft® are registered trademarks of Microsoft, Corp.

Apple, Apple logo, Macintosh, PowerMac, iMac, MacBook, iPhone, Mac OS, Leopard, Snow Leopard, Mac and the Mac logo are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

The LANCOM Systems logo, LCOS and the name LANCOM are registered trademarks of LANCOM Systems GmbH. All other names mentioned may be trademarks or registered trademarks of their respective owners.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit <http://www.openssl.org/>.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom.de

Wuerselen, June 2010

Contents

1 Product Description	8
1.1 LANCOM Advanced VPN Client	8
1.2 Performance range	8
1.3 Important notices	9
1.4 Client Monitor - graphical user interface (GUI)	10
1.5 Dialer	10
1.6 Line Management	10
1.7 Personal Firewall	10
1.8 PKI Support	11
1.8.1 Public-key infrastructure	11
1.8.2 Smart Card	12
2 Installation	13
2.1 Installation Prerequisites	13
2.1.1 System Requirements	13
2.1.2 Remote Destination	13
2.1.3 Local System	13
ISDN adapter (ISDN)	13
Modem or data card	13
Direct support of UMTS/HSDPA or GPRS data cards	14
LAN adapter (LAN)	14
LANCOM LANCAP	14
xDSL modem (PPPoE/PPTP)	14
WLAN adapter (WLAN)	14
Automatic Media Detection	15
2.1.4 Prerequisites for Strong Security	16
2.1.5 Smart Card Reader (CT-API-conform)	16
2.1.6 Smart Cards	17
2.1.7 Soft Certificates and Tokens (PKCS#12)	17
2.1.8 Smart Card or Tokens (PKCS#11)	17
2.2 Installing and activating the Advanced VPN Client	18
2.2.1 Activation	18
2.2.2 Online Activation	19
2.2.3 Offline Activation	20

3 Client Monitor	23
3.1 Using the Client Monitor	23
3.1.1 Connection [menu]	24
Connect	24
Disconnect	25
Hotspot Logon	25
Connection Info	26
Available Communication Media	27
Certificates [view]	27
Enter PIN	31
Reset PIN	33
Change PIN	33
Call Control Statistics	33
Call Control Reset	34
Exit	34
3.1.2 Configuration [menu]	34
Profile Settings [Menu]	35
Firewall Settings	37
WLAN-Settings	47
Outside Line Prefix	50
Certificates [Configuration]	51
Call Control Manager [Configuration]	56
EAP Settings [Configuration]	62
Logon Options	63
Configuration Locks	64
Profile Import	66
HotSpot	66
Profile Settings Backup	67
3.1.3 Log	67
Logbook	68
3.1.4 Window [Menu]	69
Show Profiles	69
Show Buttons	69
Show Statistics	69
Always on top	69
Autostart	69
Minimize when closing	70
Minimize when connected	70
Language	70
3.1.5 Help	71

4 Profile Settings [Parameters]	72
4.1 Basic Settings	73
4.1.1 Profile name	73
4.1.2 Connection type	73
4.1.3 Communication medium	74
4.1.4 Use Microsoft RAS-Dialer	76
4.1.5 Use this phonebook entry after every system reboot	76
4.2 Dial-Up Network	76
4.2.1 Username [Dial-Up Network]	77
4.2.2 Password [Dial-Up Network]	77
4.2.3 Destination phone number	77
4.2.4 Save password	78
4.2.5 RAS script file	79
4.3 Connection via Modem	79
4.3.1 Modem	79
4.3.2 COM Port	79
4.3.3 Baud Rate	80
4.3.4 Release Com Port	80
4.3.5 Modem Init. String	80
4.3.6 Dial Prefix	80
4.3.7 APN	81
4.3.8 SIM PIN	81
4.4 HTTP Logon [Parameters]	81
4.4.1 User ID [HTTP Logon]	81
4.4.2 Password [HTTP Logon]	81
4.4.3 Save password [HTTP Logon]	82
4.4.4 HTTP authentication script [HTTP Logon]	82
4.5 Line Management	82
4.5.1 Connection Mode	82
4.5.2 Inactivity Timeout	83
4.5.3 Prioritise Voice over IP (VoIP)	84
4.5.4 PPP Multilink	84
4.5.5 Multilink Threshold	85
4.5.6 EAP authentication	85
4.5.7 HTTP authentication	85

4.6	IPSec General Settings	86
4.6.1	Gateway	87
4.6.2	IKE Policy	87
4.6.3	IPSec Policy	88
4.6.4	Policy lifetimes	88
4.6.5	Policy editor	89
4.6.6	Exch. mode	92
4.6.7	PFS group	93
4.6.8	Use IP compression (LZS)	93
4.6.9	Disable DPD (Dead Peer Detection)	93
4.7	Extended IPSec options	93
	Use IP compression (LZS)	93
	Disable DPD (Dead Peer Detection)	93
	Force UDP encapsulation	94
4.8	Identity	94
4.8.1	Type [Identity]	94
4.8.2	Type [Identity]	95
4.8.3	ID [Identity]	95
4.8.4	Use pre-shared key	95
4.8.5	Use extended authentication (XAUTH)	95
4.8.6	Use access data from configuration	96
4.8.7	Username [Identity]	96
4.8.8	Password [Identity]	96
4.9	IP Address Assignment	97
4.9.1	Assignment of the private IP Address	97
	Use IKE Config Mode	97
	Use local IP address	97
	Use manual IP address	98
	DHCP over IPSec	98
4.9.2	DNS / WINS server	98
4.9.3	DNS server	98
4.9.4	WINS server	98
4.9.5	Domain name	98
4.10	Remote Networks	98
4.10.1	Network addresses [Remote Networks]	99
4.10.2	Subnet masks	99
4.10.3	Apply tunneling security for local networks	99

4.11	Certificate Check	100
4.11.1	Incoming certificate's subject	100
4.11.2	Incoming certificate's Issuer	101
4.11.3	Issuer's certificate fingerprint	102
4.11.4	Use SHA1 fingerprint	102
4.11.5	Further certificate checks	102
4.12	Link Firewall	104
4.12.1	Enable Stateful Inspection	105
4.12.2	Only communication within the tunnel permitted	105
4.12.3	Enable NetBios over IP	105
4.12.4	If Microsoft's dialer in use only communication within the tunnel is permitted	106
4.13	Setting up a UMTS or GPRS profile	106
4.13.1	Alternative ways to connect via UMTS or GPRS	106
4.13.2	Setting up communication via the mobile telephone provider's software	107
4.13.3	Setting up a direct connection over LANCOM Advanced VPN Client	109
4.13.4	Dial-in information for various mobile telephone providers	112
5	Establishing a Connection	113
5.1	Establishing a Connection to the destination system	113
5.1.1	Automatic connection	113
5.1.2	Manual connection	113
5.1.3	Variable connection	114
5.2	Connect	114
5.3	Client Logon	116
5.4	Passwords and User Names	117
5.4.1	User ID for NAS Dial-Up	117
5.4.2	Username and Password for VPN-Login	117
5.5	Disconnection and error	118
5.6	Disconnect	118
5.7	Disconnect (the Monitor)	118

1 Product Description

1.1 LANCOM Advanced VPN Client

The LANCOM Advanced VPN Client can be used in arbitrary VPN environments. It communicates based on standard IPSec protocols with VPN gateways different manufacturers. The LANCOM Advanced VPN Client emulates an Ethernet LAN adapter and provides additional performance features to allow customers' entrance into an integrated remote access VPN solution.

The LANCOM Advanced VPN Client features:

- Support of all common MS Windows desktop operating systems (only for Windows systems)
- Communication over all supported networks (LANCOM LANCAPI too) (only for Windows systems)
- Integrated Personal Firewall for more security.
- Dialer protection (no threat through 0190- or 0900-Dialers) (only for Windows systems)
- More performance via ISDN channel bundling (only for Windows systems)
- Save connection charges (controll of costs and connections)
- „Friendly-Net“ detection for situation dependent firewall rules
- Automatic Hot-Spot detection (only for Windows systems)
- Ease of use (graphical user interface)
- VPN Path Finder

1.2 Performance range

The IPSec client supports all major operating systems (Windows 2000, 2003 Server, XP, CE (on request) and Mac OS X 10.5 Leopard (Intel only) or Mac OS X 10.6 Snow Leopard). Connecting to the corporate network is media-type independent, e.g. in addition to ISDN, PSTN analog telephone network, GSM, GPRS, UMTS and xDSL, wired LAN technologies and wireless LANS (WLANS) 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 (Windows only)
- In the corporate headquarters via LAN

- On the road at hotspots and at customer sites via WLAN or GPRS/UMTS (Windows only)
- In the home office via xDSL, cable, or ISDN (Windows only)



All further information only apply to Windows systems. Differences from Mac versions will be labeled.

1.3 Important notices

EN

- ① This manual describes the function range of the LANCOM Advanced VPN Client on basis of the software releases 2.22.
- ② If the computer is not connected with the Internet, for example via local network access (LAN, WLAN or LANCAP), then an Internet connection must be established first (e.g. by logging in at a WLAN hotspot). Further, the client can independently control Internet access via: analog modems, DSL modems (PPPoE), ISDN-, GPRS- or UMTS cards. Unlike connections over the Internet that are secured by VPN, direct dialed connections (e.g. ISDN card or LANCAP, analog modem, HSCSD mobile telephone) generally do not need to be encrypted.
- ③ The LANCOM Advanced VPN Client software is available at a fee. Under www.lancom.de/download and on the LANCOM CD you will find a 30-day demo version of the LANCOM Advanced VPN Client. After 30 days, this demo version can be upgraded to a full version with the appropriate licence. The sale of the full version is only possible via LANCOM partners (distribution, specialist resellers and system vendors). Use the following item numbers when ordering the licence for Windows (XP, 2000, Me or 98SE):
 - 61600 LANCOM Advanced VPN Client (single licence)
 - 61601 LANCOM Advanced VPN Client (10 licences)
 - 61602 LANCOM Advanced VPN Client (25 licences)



The simultaneous use of a single licence number on multiple systems is not permitted under licensing law.

- ④ The simultaneous dialing-in of VPN clients that do not have the necessary licence numbers (i.e. when in demo mode) is limited to three. The LANCOM Advanced VPN Clients that are logged into the VPN are displayed by the LANCOM LANmonitor.

- ⑤ If the VPN-LAN interface (LANCOM Advanced VPN Client) is manually deactivated by the network administration (Device manager), the system must be rebooted. Repeating the manual reactivation also requires a manual restart of the operating system.

1.4 Client Monitor - graphical user interface (GUI)

The graphical user interface 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.

1.5 Dialer

Only available for Windows systems.

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"

1.6 Line Management

Only available for Windows systems.

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 transparency 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.

1.7 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.

Besides the LANCOM Advanced VPN Client includes a application layer firewall and friendly net detection. With the application layer firewall filter rules can be linked with certain applications. Situation-dependent filter rules can be activated and/or deactivated with the friendly net detection. Strict rules can be defined e.g. for the connection to a public Hot Spot, which are loosened with the choice at a trustworthy network.

1.8 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 corporate network. The IPSec client becomes part of a Public Key Infrastructure (PKI). LANCOM Router support Pre-Shared-Keys and digital certificates as of LCOS 5.00.

1.8.1 Public-key infrastructure

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 communicate. 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.

1.8.2 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.

1.9 VPN Path Finder

In some environments it is impossible to establish a secured VPN connection over an existing Internet connection due to an interim firewall that blocks the ports used by IPsec. To be able to set up an IPsec-secured VPN connection in such a situation, the LANCOM Advanced VPN Client supports the technology known as VPN Pathfinder.

The first attempt always tries to establish data communications with standard IPsec. If the connection cannot be established (e.g. because IKE port 500 is blocked by a cellular network), then an attempt is then automatically made to establish a connection that encapsulates the IPsec VPN in an additional SSL header (port 443, like https).

2 Installation

2.1 Installation Prerequisites

2.1.1 System Requirements

In order to be able to communicate with the Client Software it is essential to have either Microsoft Windows 2000, XP/Vista or Mac OS X 10.5 Leopard (Intel only) or Mac OS X 10.6 Snow Leopard installed on your PC.

During the installation you are asked to have your CDs or DVDs ready, as these will be needed for updating your PC's driver database files. Please insert these when prompted to do so.

2.1.2 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), GPRS, UMTS, LAN over IP, WLAN over IPsec or PPP over Ethernet (PPPoE).

2.1.3 Local System

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

ISDN adapter (ISDN)

Only available for Windows systems.

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.

Modem or data card

Only available for Windows systems.

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, UMTS 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.

Direct support of UMTS/HSDPA or GPRS data cards

Only available for Windows systems.

The LANCOM Advanced VPN Client supports the direct use of data cards for notebooks, as they are offered by various mobile network vendors. The dial-in parameters can be entered directly to the profile settings.

Further information concerning configuring a mobile online account via UMTS or GPRS can be found under 'Setting up a UMTS or GPRS profile'

LAN adapter (LAN)

When the Link Type 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.

Adapters for a wireless LAN (WLAN adapter) are handled nearly like normal LAN adapters. "WLAN over IPSec" must also be selected for WLAN.

LANCOM LANCAP

Only available for Windows systems.

If you use LANCOM LANCAP to connect to the Internet, please consider the following:

- If the stateful inspection firewall is in use as well, the setting "only communication within the tunnel permitted" must remain off, otherwise the LANCAP server in the local network can no longer be accessed.
- With the stateful inspection firewall switched off, the Internet and VPN communication will work without further changes to the settings.

xDSL modem (PPPoE/PPTP)

Only available for Windows systems.

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.

WLAN adapter (WLAN)

Only available for Windows systems.

The WLAN adapter is 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 'Connection type' →Page 73.

Automatic Media Detection

Only available for Windows systems.

If various link types could be used, the client detects automatically which link type actually can be used and 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 'Communication medium' →Page 74.

2.1.4 Prerequisites for Strong Security

If you are using the Client Software which provides support for X.509 certificates (Strong Security version of the Client), 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.

2.1.5 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 web site) 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 WINDOWS\SYSTEM directory (Windows 95/98) or in the SYSTEM32 directory (Windows NT/2000). Enter the name of the connected Smart Card reader as "ReaderName" (xyz) and the name of the installed driver as DLLWIN95 or DLLWINNT respectively. 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!

Module name = 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 -> Certificate -> Smart Card reader". Now you select that Smart Card reader.

2.1.6 Smart Cards

Currently, the following Smart Cards are supported:

- Signtrust
- NetKey 2000
- TC Trust (CardOS M4)

2.1.7 Soft Certificates and Tokens (PKCS#12)

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

2.1.8 Smart Card or Tokens (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 windows\system directory (Windows 95/98) or system32 directory (Windows NT/2000), with an ASCII editor 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".

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 under "Configuration-> Certificates -> Configuration -> Smart Card reader". Now select this Smart Card reader or token.

2.2 Installing and activating the Advanced VPN Client

To install the LANCOM Advanced VPN Client insert the program CD supplied with the device into your CD-ROM drive. The setup program should start automatically within seconds; if not, please manually execute the "autostart.exe" in the root directory of the CD. A Wizard starts that will guide you through the installation. Select 'Standard Installation'.

If a previous version of the client is already installed, it will be detected and updated automatically.



To complete the installation, you will need to restart the device.

Activation

Once the device has been restarted, the LANCOM Advanced VPN Client installation is complete. You can test the LANCOM Advanced VPN Client for 30 days before activation. Once the client has been started, the main window appears.

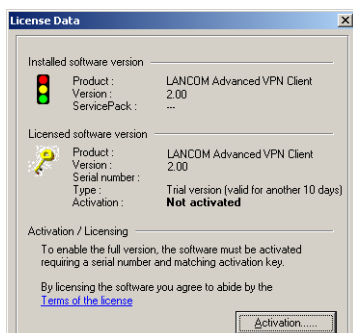



The product must be activated in order to make use of the complete set of features after the 30-day trial period has expired. There are three possible scenarios here:

- This is the first installation with the purchase of a full license.
- A software and license upgrade from a previous version with the purchase of a new license.
- A software update for the sole purpose of bug fixing. You retain your previous license. In this case, the new client version is installed but the user only has access to the functionality of the previous version.


In every case the following steps must be taken:

- 1 Click on **Activation** in the main window. A dialog then appears which shows your current version number and the license used.



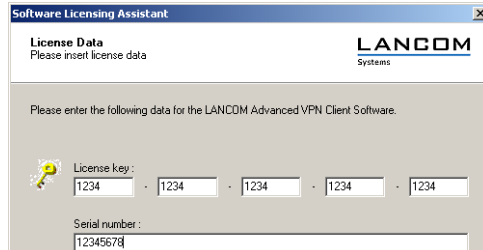
 Alternatively, this dialog can be accessed via the menu item **Help ► License data and activation**.

- 2 Click on **Activation** again here. You can activate your product online or offline.

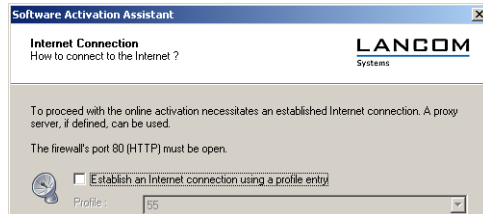
 An Internet connection is required for "Offline Activation" as well.

Online Activation

- 1 If you select Online Activation, enter your license data in the following dialog. You received this information when you purchased your LANCOM Advanced VPN Client.



- 2 The client must now establish a connection to the LANCOM server.

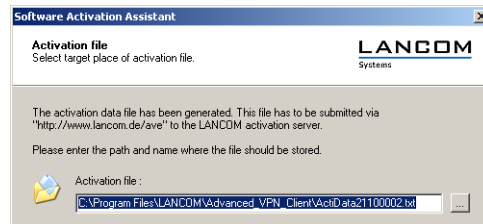


If you are already using an older version of LANCOM Advanced VPN Client, then you can use your previous configured user profiles to connect to the Internet. As soon as the computer is connected to the Internet, it automatically connects to the LANCOM server. No further action is necessary to carry out the activation and the process terminates automatically upon completion.

Offline Activation

- 1 If you have selected Offline Activation, you will need to enter your license data and serial number when activating. These are then verified and

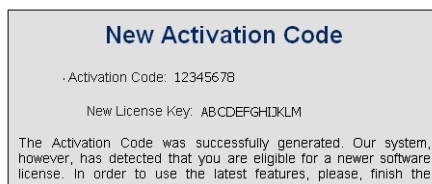
stored in a file on the hard drive. You may select the name of the file freely providing that it is a text file (.txt).



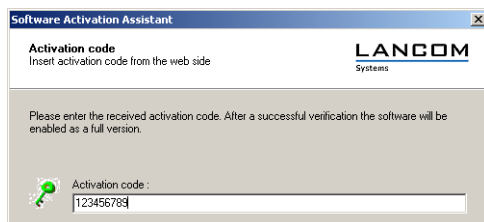
- 2 Your license data is included in this activation file. This file must be transferred to the LANCOM server for activation. Start your browser and open the www.lancom.de/avc/activation website.



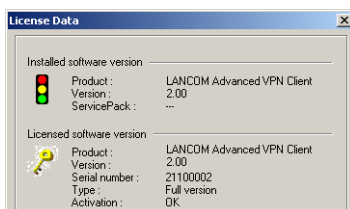
- 3 Click on **Search** and select the activation file that was just created. Then click **Send**. The LANCOM server will now process the activation file. You will now be forwarded to a website where you will be able to view your activation code. Print this page or make a note of the code listed here.



- 4 Switch back to LANCOM Advanced VPN Client and click on **Activation** in the main window. Enter the code that you printed or made a note of in the following dialog.



- 5 Once the activation code has been entered, the product activation is complete and you can use the LANCOM Advanced VPN Client as specified within the scope of your license.
- 6 Depending on the license you purchased, the license and version number will now appear.



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 > LANCOM > LANCOM Advanced VPN Client**. 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.

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 Phonebook and associated Destination and Security parameters

3.1 Using the Client Monitor

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

- Connection [menu]
- Configuration [menu]
- Log [menu]
- Window [menu]
- Help

3.1.1 Connection [menu]

This pull-down menu "Connection" contains the following menu items:

- Connect
- Disconnect
- HotSpot Logon (Windows only)
- Multifunction card (Windows only)
- Connection Info
- Available Communication Media (Windows only)
- Certificates [View]
- Enter PIN
- Reset PIN
- Change PIN
- Call Control Statistics
- Call Control Reset
- Exit

Connect

This command is used to initiate a connection. A connection can only be made if a destination has been properly defined and selected in the Phonebook (see -> Phonebook, General). The selected destination system is displayed in the "Destination" 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 Destination in the Line Management folder of the Phonebook as well as the Link Type being used (-> see Phonebook, Line Management, Connection Mode).

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.

Hotspot Logon

Only available for Windows systems.



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 concerning access to WLANs).

The LANCOM Advanced VPN Client 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. During 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.

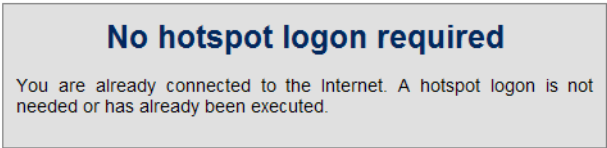


At present the clients hotspot access works only with those hotspots, that redirect inquiries with the help of browsers to the homepage of the public WLAN provider (for example T-Mobile or Eurospot).

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. If hotspot logon has not been executed by the client the user gets the message "HotSpot could not be found". In this case it must be checked whether a general problem exists in conjunction with the implemented mechanisms relative to the hotspot operator.

The configuration for hotspot logon is executed via the Monitor menu "Configuration / Hotspot Logon". 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.lancom.de>. A window with the following message will appear:



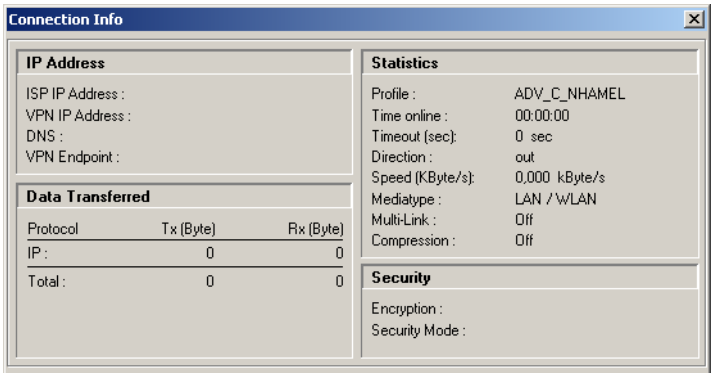
This text can be changed by the administrator by entering the address of a different HTML start page in the form "<http://www.mycompany.de/error.html>".

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 login to the hotspot operator.
- If the user has not reached a website, then the Microsoft error message "...not found" will be displayed.

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.

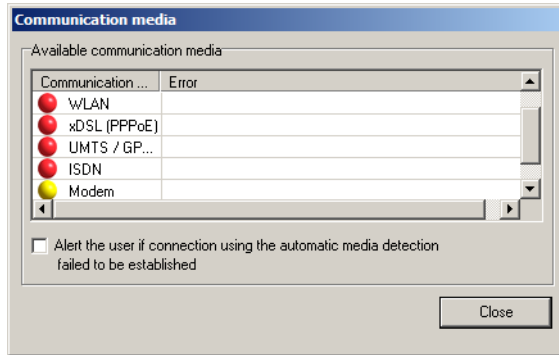


The information in the connection info window is "read-only" and has no influence on the functionality of the IPSec client.

Available Communication Media

Only available for Windows systems.

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.

Certificates [view]

In the "Connection" menu you will find the entry "Certificates", which consists of the following submenus: "View Issuer Certificate", "View User Certificate", "View incoming Certificate" and "CA Certificates".

Normally a Certification Authority (CA) issues certificates, in accordance with X.509 standards. These certificates may be implemented on a Smart Card or alternatively in a PKCS#12 file (soft certificate).

■ 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.

Certification 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 - View Issuer Certificate).

Serial number: The serial number of the certificates can be compared with the registered numbers 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. 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 Windows directory NCPLE\CACERTS\, then no verification takes place.

General

In the general display you find the information about certificate user and issuer (these are identical for an issuer certificate), as well as the serial number, the information about the period of validity, and the fingerprint.

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.

■ Display CA Certificates

Multiple issuer certificates are supported with the new client software (multiple CA support). The issuer certificates must be collected in the Windows directory NCPLE\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 NCPLE\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 Windows directory NCPLE\CACERTS\, then a connection that implements certificates is not permitted.

General

In the general display you find the information about certificate user and issuer (these are identical for an issuer certificate), as well as the serial number, the information about the period of validity, and the fingerprint.

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.

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 selected the menu item "Connection - Enter PIN", then the PIN (at least 6 digits) can be entered in the open entry field, and confirmed with "OK". The digits of the PIN are displayed as asterisks "*" on the screen.

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 omitted in the case of repeated manual connection establishment, if this has been configured (see -> Configuration, Certificates).

If you have configured the VPN/PKI 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.

If the Secure Client has been configured for the use of a soft certificate (see -> Configuration, Certificates), then no symbol appears in the status field.

If the PIN has been correctly entered, then this fact is indicated in the monitor interface by a green check mark behind "PIN".



Incorrect entries and incorrect PINs are acknowledged with the error message "Incorrect PIN!" after approximately 3 seconds. At this point a connection establishment is not possible.

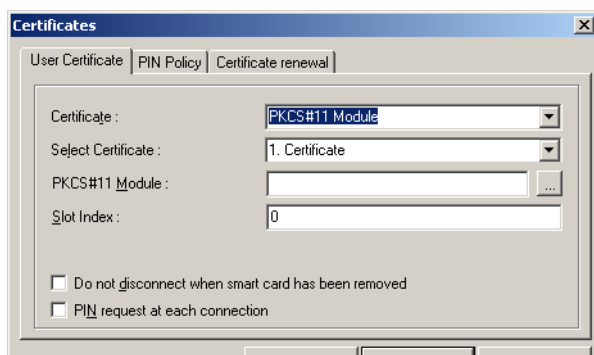
Please note that a Smart Card or a token can be blocked after multiple incorrect PIN entries. In this case, please contact your remote administrator.

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



An established connection will, by default, be disconnected if the Smart Card or token is removed during the operation.

This behavior can be changed, and is determined by whether or not the "Do not disconnect when Smart Card is removed" has been enabled. This toggle can be found in the main menu of the monitor: Configuration -> Certificates..



The policies for PIN entry can be specified in the main menu under "Configuration -> Certificates" (see -> Configuration, Certificates, PIN Policies). These policies must also be observed when the PIN is changed (see -> Connection, Change PIN).



The PIN for a smart card or a certificate can be changed under the "Change PIN" menu item, if the correct PIN has been correctly entered prior to this. This menu item will not be activated without the prior entry of a valid PIN.

Reset PIN

This menu item is active only when the PIN has been entered correctly, i. e. the certificate is used for the connection to be established.

If you reset the PIN this certificate could not be used to establish a connection anymore until the correct PIN is entered again.

Change PIN

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 "**".

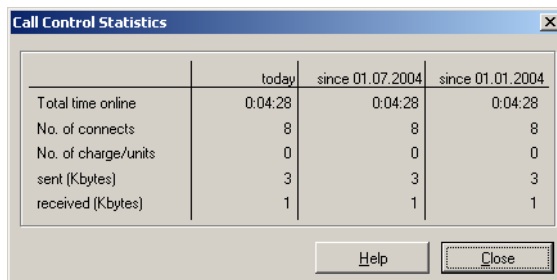
Then enter your new PIN and confirm it by repeating it in the last entry field. With a click on "OK" you have changed your PIN.

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".

Call Control Statistics

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.



	today	since 01.07.2004	since 01.01.2004
Total time online	0:04:28	0:04:28	0:04:28
No. of connects	8	8	8
No. of charge/units	0	0	0
sent (Kbytes)	3	3	3
received (Kbytes)	1	1	1

Help Close

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".

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.



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!

3.1.2 Configuration [menu]

This pull-down menu "Configuration" contains the following menu items:

- Profile Settings [Menu]
- Extended Firewall Settings [Menu]
- WLAN-Settings (Windows only)
- Outside Line Prefix (Windows only)
- Certificates [Configuration]
- Call Control Manager [Configuration] (Windows only)
- EAP Settings [Configuration] (Windows only)
- Logon Options (Windows only)
- Configuration Locks
- Profile Settings Backup
- Profile Import
- HotSpot (Windows only)

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 creat-

ing 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..

Profile Settings [Menu]

Entries in the profile settings

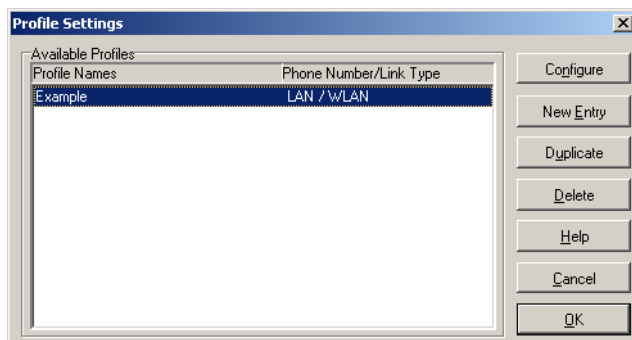


After installing the Secure Client for the first time it will be necessary to define a profile for your requirements in the profile settings. For this purpose there is a "Configuration Assistant", which will walk you through the configuration steps of a profile. In this way the first profile will be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

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 accord-

ing 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.

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:

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

■ 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 - Destination

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 Profile 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.

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.



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 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.



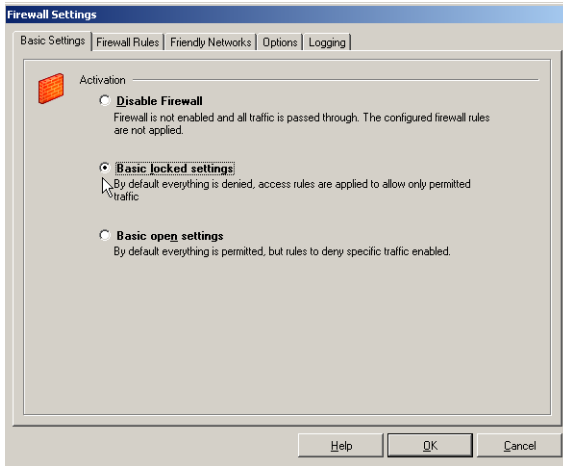
Please note that the link-based firewall settings take priority over the global firewall settings at activation. For instance if the Link Firewall is set to "Always" and "Only allow communication in the tunnel", then in spite of global configuration rules that may possibly be different, only one tunnel 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.

■ Basic Settings

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.



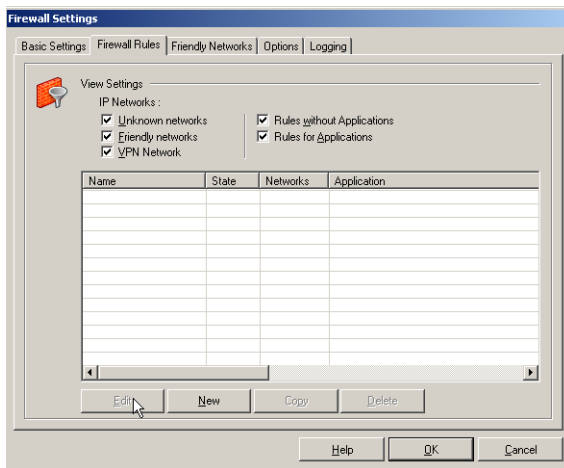
In the blocked basic setting mode in a convenient manner an L2Sec/IPSec tunnel connection is released. For this, the data traffic can be globally permitted in the configuration field "Options", via VPN protocols (L2Sec, IPSec).

- **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.

Firewall rules

The rules for the extended firewall are brought together in this configuration field.

[View Settings](#)

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 without Applications
- Rules with 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.

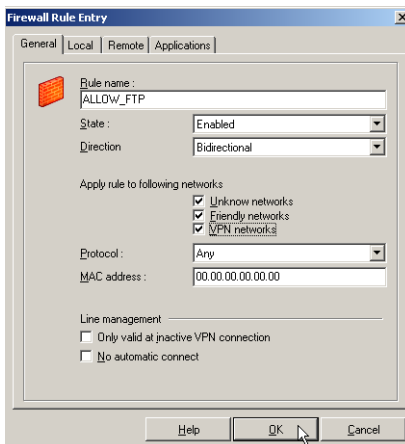
Creating a firewall rule

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.

General

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).

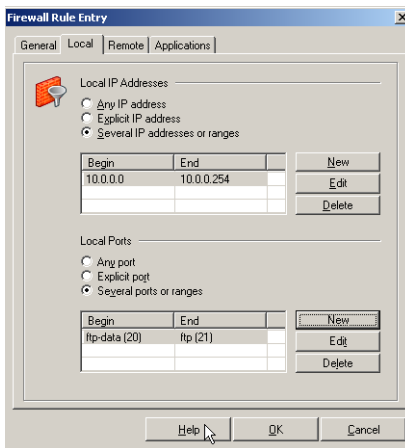
- **Apply rule to following networks:** When creating a rule, at first do not assign it to any network. A rule can only be saved if the desired allocation has been made and if a name has been assigned.
 - **Unknown networks:** are all networks (IP network interfaces), that can neither be allocated to 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 "Fire-wall 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.
- **MAC address:** The MAC address is worldwide unique and only allows data packets for incoming connections that originate from the gateway that has this MAC address. For an outgoing connection specifying the MAC address of the target gateway ensures that the client can only set-up a connection to this destination gateway. After setting-up a VPN connection via this gateway the client has access to the corporate network depending on the configured link profile. This is a very restrictive rule that can only be used in very special situations.

Local

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).

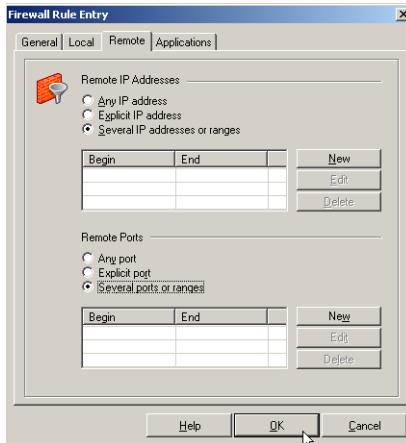
Remote

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.



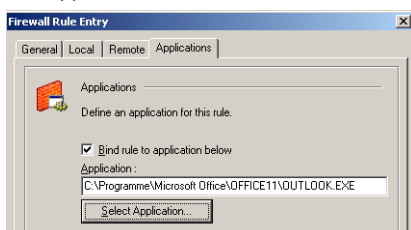
- **All IP addresses:** permits communication with any IP address of the other side, without limitation.
- **Unique IP address:** only allows communication with the IP address on the other side specified here.
- **Multiple IP addresses / IP ranges:** permits communication with different IP address on 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).

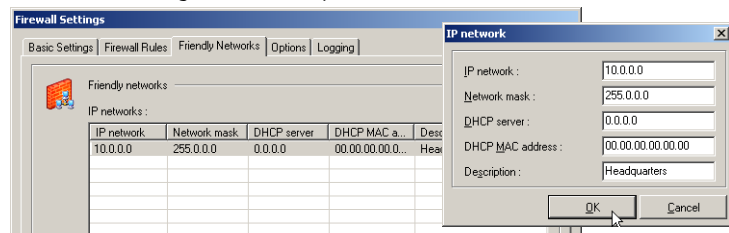
Applications

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.



Friendly Networks

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).

Options

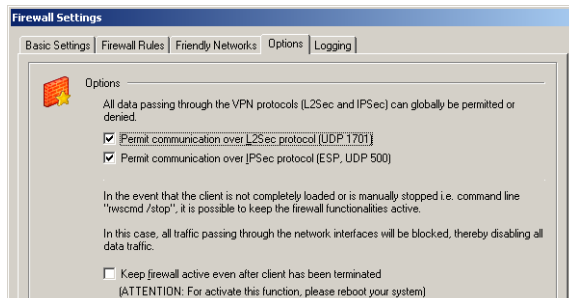
[Data traffic via VPN protocols](#)

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.

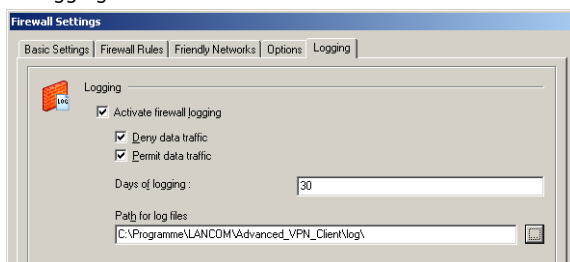
If the above mentioned function is not used and the client is stopped, then the firewall will also be deactivated.

Logging

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: <Installation directory>\log>.

The log files for the firewall are written in pure text format and are named Firewallymmdd.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.

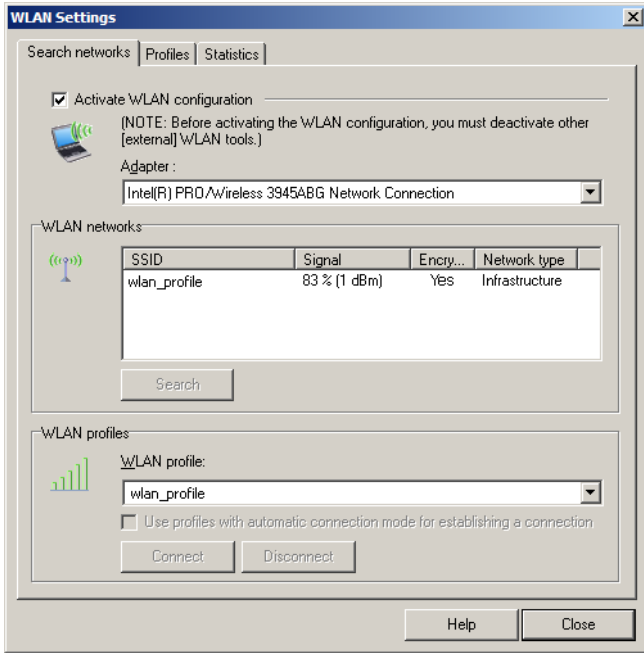
The log files are written at each start of the firewall. The maximum number is maintained in the log directory, as has been entered as number of the "Days for logging".



WLAN-Settings

The WLAN adapter can be operated with the connection type "WLAN" (see (r) Phonebook / Parameters / Destination system). In the monitor menu "Config-

uration / 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

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 / Signal / 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. 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 profile](#) / General).



WLAN profile

A previously created [WLAN profile](#) can be selected for the according (scanned) network. By clicking on the "Connect" button the connection is set up.

■ WLAN profile

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.

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.

Encryption [WLAN profile]

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

IP addresses [WLAN profile]

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)).

Authentication [WLAN profile]

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

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

Outside Line Prefix

Only available for Windows systems.

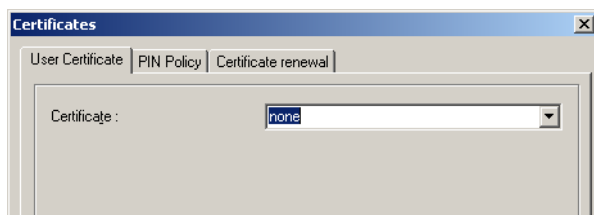
A special number or dial prefix is generally required when communicating via a PBX in order to acquire an outside line. This could, for example, be a 0 (zero) or 9 or any other number(s) depending on the PBX in use at your location. The

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) of the profile, particularly when travelling.

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.



■ User Certificate

Certificate: By choosing "Certificate" from the submenu you can determine whether or not you want to use the certificate and thus use the "Extended Authentication".

None: The default value is "None", meaning that certificates will not be used.

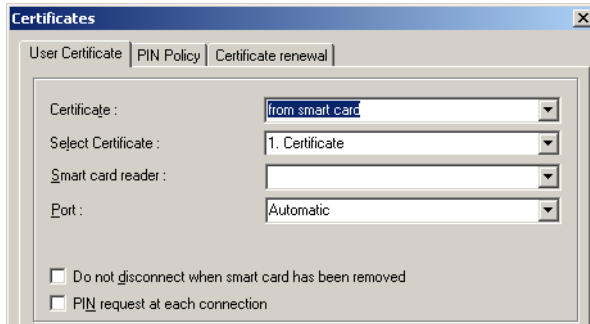
from PKCS#12 File: In order to use a Soft Certificate select "from PKCS#12 File" and then define the directory (path) in which the PKCS#12 file is stored for access purposes. Normally you will receive this file (encrypted) from your network administrator or your CA (Certification Authority).

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: With an ASCII Editor edit the file NCPPKI.CONF, which is located in the Directory \WINDOWS\SYSTEM (Windows 95/98) or in the Directory SYSTEM32 (Windows NT/2000) 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. (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:

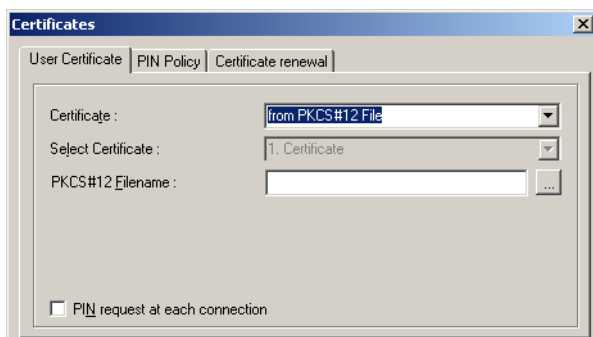
1. Certificate ... 3.: (Standard = 1) Up to 3 different certificates, located on the Smart Card, can be selected from the list. The number of certificates on the Smart Card is dependent on the Registration Authority that has issued the Smart Card. For further information please contact your System Administrator. The Smart Cards issued by Signtrust and NetKey 2000 come with three certificates:

- 7 for digital signing
- 8 for encryption and decryption
- 9 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. Instead of entering the entire directory name, it can be dynamically defined, e.g.

%SYSTEMROOT%\ncpleuser1.p12 %SYSTEMDRIVE%\winxxx\ncpleuser1.p12



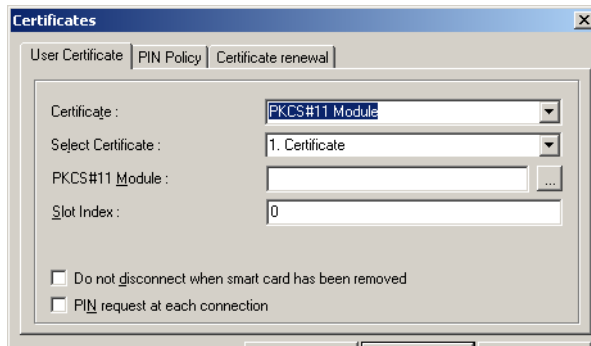
Important: The strings for the File Name can be entered with variables. This simplifies in particular the handling of the configuration files

with the Client Manager, because the same strings including environment variables can be entered for all Users.

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. Instead of entering the entire directory name, it can be dynamically defined, e.g.

```
%SYSTEMROOT%\ncple\pkcs#11.dll %SYSTEMDRIVE%\winxxx\ncple\ pkcs#11.dll
```



Important: The strings for the File Name can be entered with variables. This simplifies in particular the handling of the configuration files with the Client Manager, because the same strings including environment variables can be entered for all Users.

Do not disconnect when Smart Card is removed (new parameter)

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.

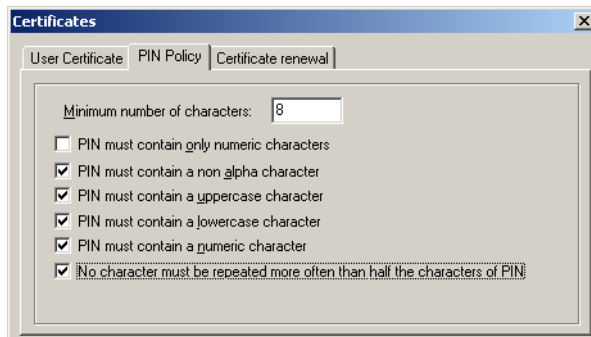
■ PIN Policy

Minimum number of characters

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..

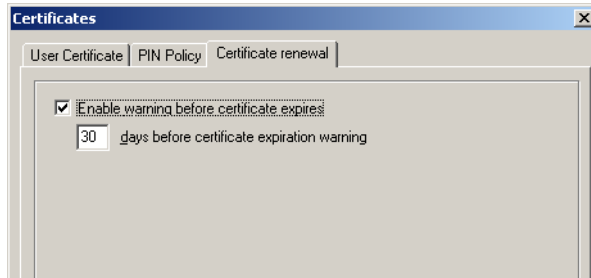


The specified policies are displayed when the PIN is changed, and the policies that are only fulfilled at entry are highlighted in green (see - > Change PIN).

■ Certificate renewal

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..



Call Control Manager [Configuration]

Only available for Windows systems.

■ Budget Manager

Functions of the Budget Manager

The budget manager is a component of the Secure Client "Call Control Manager" and serves predominately for voluntary monitoring. It measures and monitors the data volume estimation during a certain time span or the time run out online within this time span (e.g. within a month), to the extent that the connection has been built via a media type supported by the NCP Dialer. If no parameter locks are created by the administrator in the client software, the user can set the budget limits himself.

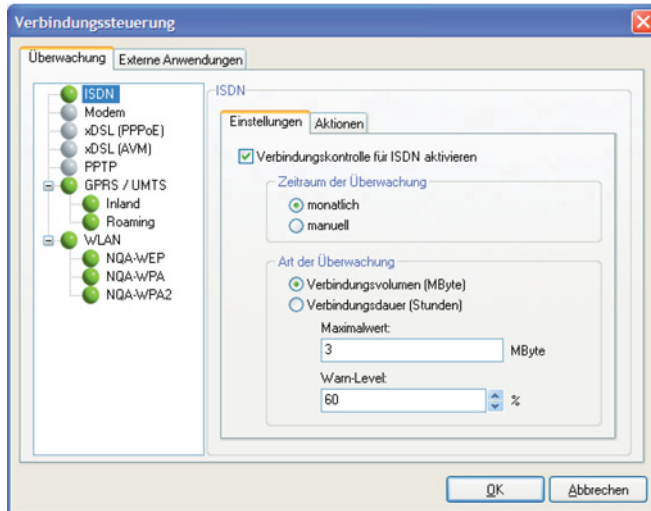
Should a limit be exceeded and a connection establishment is no longer possible, the user must contact his administrator, to the extent that parameter blocks are set. The parameter blocks must be unmade; only thereafter can the user conduct a new configuration, to the extent that the Enterprise Client is used, new profile settings is obtained from the management system.

Budget Limitation according to Volume or Time online

The corresponding settings, whether data volume or time online that should be measured during a month or other determined time period, can be done via the monitor menu "Configuration / Call Control Manager".

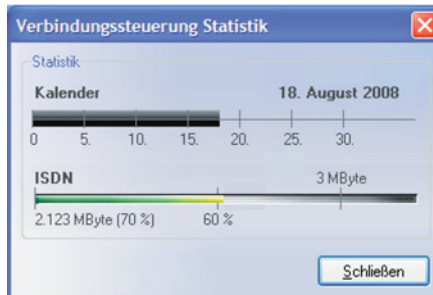
For all connection media supported by the NCP Dialer, each type of calculation can be determined separately, whether the (monthly) connection volume or the time of connection were measured. So for example, a maximum connec-

tion time per month for ISDN or WLAN and a maximum connection volume per month for GPRS / UMTS can be specified.



Budget Manager Statistics

The statistics show at the current date, how much of the maximum budget have already been used in hours or bytes, since the first of the current month or since the start of monitoring. Limits can be set here, in order to trigger certain actions.



Smaller Budgets for Mobile Computing

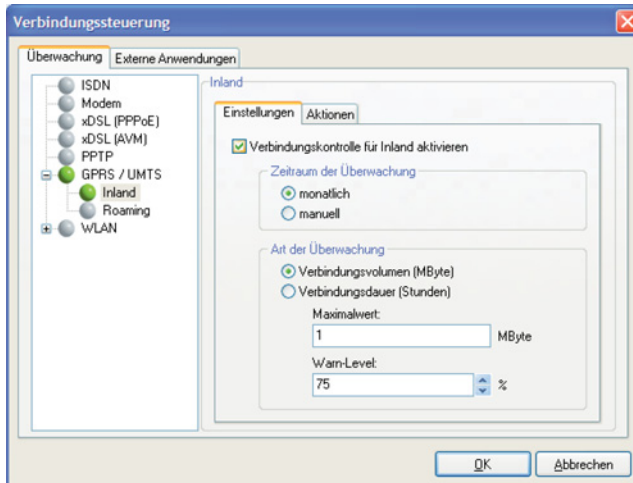
If a limited budget is available for a limited time period, for example for the time of a hotel stay, the starting time point can be set manually. Additionally, the statistic is opened via the monitor menu "Connection" and pressed for the selected type of connection of the reset button. Thereby, the starting time

point is determined from which the specified budget is posted. (Pressing the reset button again starts the connection control again with the same specification and deletes the previous connection records.)



Avoid costly Roaming

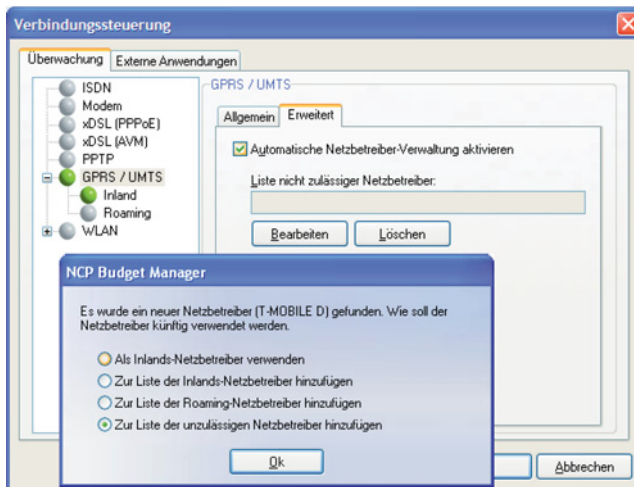
For the media type GPRS / UMTS, the connection control is activated separately for inland (home) and roaming connections. (See illustration left) Unnecessary roaming with GPRS / UMTS connections, e.g. in border areas, can largely be excluded through targeted security inquiries. In this way, lists of permissible inland network operations and permissible roaming network operators can be created that permit the selection of the most favourable and the exclusion of undesirable providers from the beginning on in a convenient way..



Automatic Provider Management

If automatic provider management is activated, the user for each new provider not yet known to the system is asked in which new provider's list this provider should be recorded. In the list of inland network operators, of the roaming network operators or denied impermissible network operators. The list of network operators to be denied can be handled under "Upgrading" at any time, for example in order to delete a provider and to record it in another list.

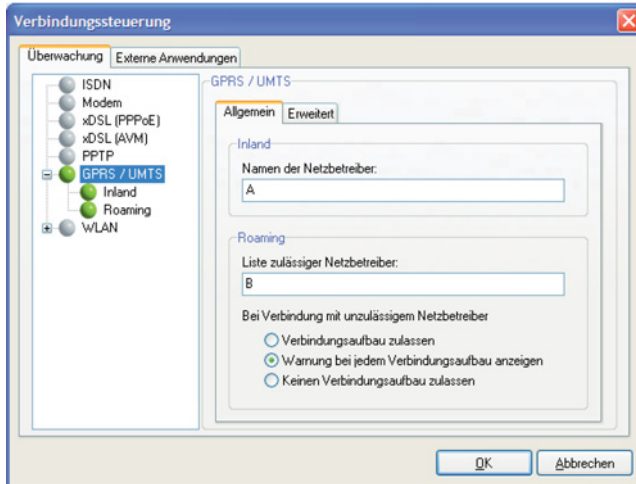
If automatic provider management is not used, a provider the system does not yet recognize is handled as an impermissible network operator and connection establishment is made via this provider according to the options for impermissible network operator specified under the settings "General"..



Inland Network Operator and Roaming Network Operator

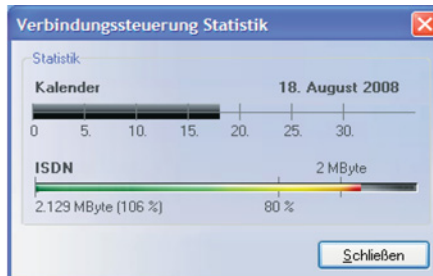
Like the connection control, which is activated separately for inland connections and roaming connections, separated lists for permissible inland network operator and roaming operators are conducted. Via these lists that are conducted in the settings "General", the provider selection is automated. Each provider, that the user has entered via the automated network operator administration or manually in one of the lists under "inland" or "roaming", is used for connection establishment as soon as the system recognizes it. Yet

unknown providers are handled according to the setting for impermissible network operators.



Budget Statistics and automated Warnings

The user obtains an overview of his (monthly) budget in the statistics regarding connection control. The statistic shows, with the current date, how much of the maximum exhausted budget in hours or bytes already have been used since the first of the current month or since the start of monitoring. Here you also can see limits that can be set in order to trigger certain actions..



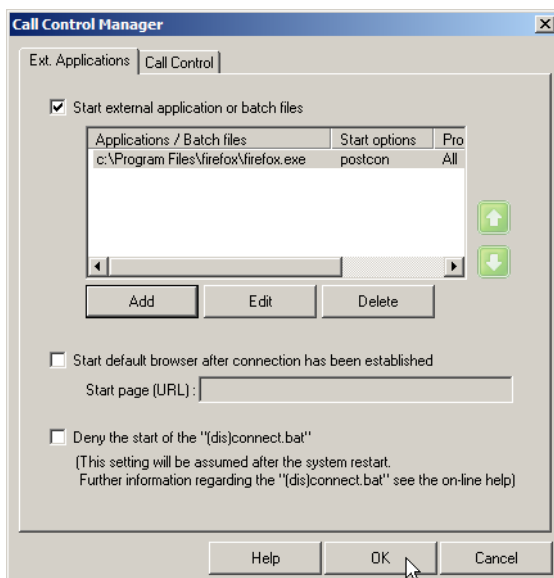
The actions are individually determined like the connection control for each medium . Therefore, a warning can be issued after a percent use of determined connection volume or the maximum connection time that makes one alert that the budget is soon exhausted. Or, after the budget is exhausted, no connection is permissible for this month.

If the budget display in the statistic is clearly more rapid than the balance display for the calendar, the assigned budget is not sufficient. The budget display is coloured yellow after reaching the warning area, red after reaching the maximum value. If establishment of the connection is no longer permissible after exceeding the maximum value, the corresponding report appears on the client monitor.

■ External Applications

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 directory and file name of the browser.

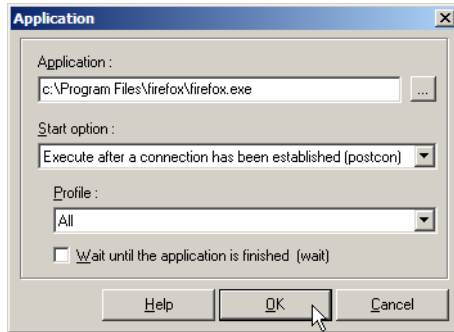


After you have selected the function “Start external applications or batch files” you can select an application or batch file from the computer via the “Add” button that, this application or batch file will be loaded depending on the start option.

- 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 function should always be activated if execution of the cited batch files with administrator rights (system rights) is not necessarily required for a desired application.

■ Call Control Manager [Configuration]

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).

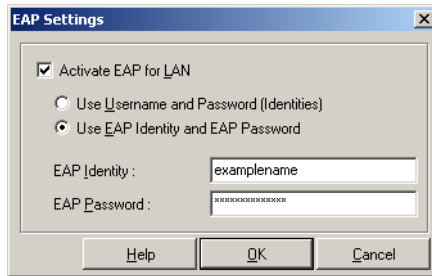
EAP Settings [Configuration]

Only available for Windows systems.

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



Use of the Extended Authentication Protocol Message Digest version 5 (EAP MD5) can be specified via the main menu of the monitor under "Configuration - EAP Settings". 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 MD5). You can use either "VPN User ID" with "VPN Password" 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%

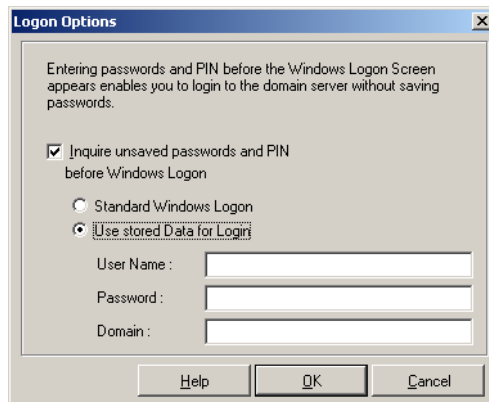
Logon Options

Only available for Windows systems.

This option is only available under Windows NT, Windows 2000 and Windows XP.

Select this menu item enable domain logon next time the machine started. You may choose to save your domain logon credentials locally, or simply enter them when prompted to do so. An attempt to establish a VPN connection will be made during the boot process in order to logon to the domain. The VPN connection is then necessary in order to reach the domain controller. When establishing the connection you may be required to enter your password, if this was not "saved" under password in the Phonebook.

Once the Client has established a connection to the destination, you will be able to sign-on to the remote domain. This sign-on (domain logon) process, because it is done through the VPN tunnel, is encrypted.



You must reboot your PC after making any changes to the "Logon Options".

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 blocks]

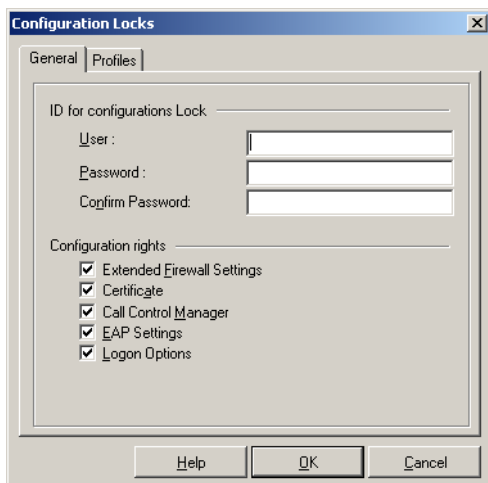
In order to effectively specify the configuration blocks, identification must be entered, which consists of "User ID" and "Password". The password must be confirmed thereafter.



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.

EN

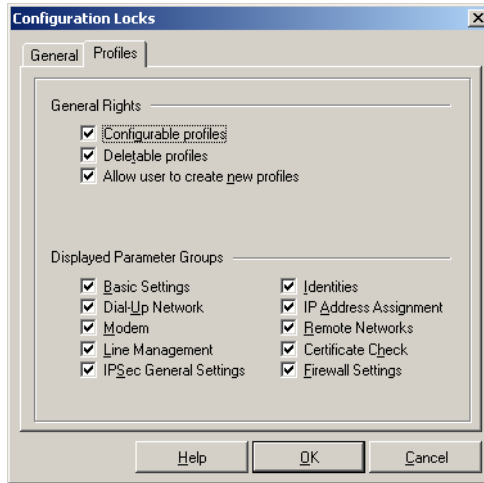


■ Profiles [Configuration Locks]

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

■ General rights

■ Visible profile parameter fields

**General rights**

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.

Profile Import

With this function profiles can be imported. 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.

HotSpot

The following settings for HotSpot Logon 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.

The alternative browser can be especially configured for the requirements at hotspots. Specifically no proxy server will be installed and all active elements (Java, JavaScript, ActiveX) will be deactivated. (The alternative browser is not part of the Client software!)

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.mycompany.de/error.html.`

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.

3.1.3 Log

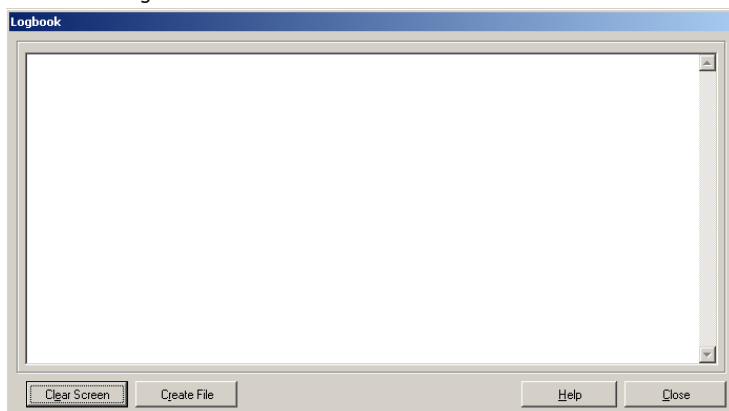
This feature automatically logs (records) all communication transactions (but not the data) going via the Client. Selecting the Log function will open the window of the logbook. The contents of the log are stored in memory and are accessible until such a time that you (re)boot your PC.

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=month, 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

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.

3.1.4 Window [Menu]

This feature lets you influence the way in which the monitor is displayed on your screen. During normal operation you will probably want to deactivate "Show Details" in order to reduce the window size. The following features are found in the "Window" pull-down menu:

- Show Profiles
- Show Buttons
- Show Statistics
- Show WLAN state
- Always on top
- Autostart
- Minimize when closing
- Minimize when connected
- Language

Show Profiles

When "Show Profiles" is activated the configured destinations could be selected by clicking on the listed names.

Show Buttons

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

Alternatively, when those buttons are not displayed, you can establish or terminate a connection with the right mouse click menu.

Show Statistics

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

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.

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.

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 accruing, 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.

Minimize when connected

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

Language

The client software has been designed for international language support. The default language is English. In order to choose a language, click on "Lan-

guage" in the Window pulldown menu and then select the desired language. In the near future the client will have additional language support.

3.1.5 Help

Clicking on "Help" opens a window displaying a table of contents for all available Help Text.

Clicking on "Info" opens a window displaying the Secure Client version installed on your PC.

4 Profile Settings [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.

Upon clicking "Profile Settings" in the monitor menu, the menu is opened with an overview of the defined profiles and the phonenumbers of the assigned destinations. 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". Enabling the "Configuration Assistant", which assists in the creation of a new profile definition. All other parameters will be assigned default values.

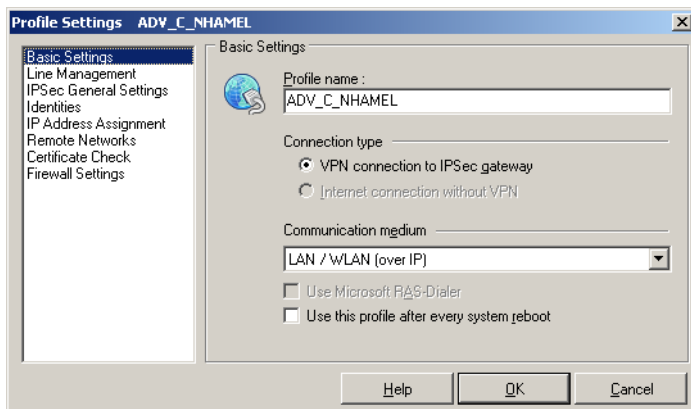
To edit these default values, in order to fulfill the requirements of the profile, select the desired profile and then "Configure" to gain access to the individual parameters. (See -> Profile Settings - Configure). In order to duplicate a profile click on "Duplicate". In order to delete a profile click on "Delete".

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 -> Phonebook, Configure). Within the configuration folder the connection parameters pertaining to this profile can be configured.

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

4.1 Basic Settings

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



-> see following parameters:

- Profile name
- Connection type
- Communication medium
- Use Microsoft RAS-Dialer
- Use this phonebook entry after every system reboot

4.1.1 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).

4.1.2 Connection type

Only available for Windows systems.

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.

4.1.3 Communication medium

Only available for Windows systems.

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 adapters or UMTS/GPRS adapters with software from the manufacturer or provider (see 'Setting up a UMTS or GPRS profile' →Page 106)

Networks: Ethernet or Token Ring based LAN

WLAN (over IPsec)

Hardware: WLAN adapter

Networks: Wireless LAN

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 phone-book, 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).

xDSL (PPPoE):

Hardware: Ethernet adapter;

Networks: Broadband (e.g. ADSL);

Remote destination: Access Router in the xDSL

GPRS/UMTS

Select this dial-up media for access via the mobile telephone network (GPRS/UMTS) (as an alternative to using the the manufacturer's / provider's software supplied with the UMTS/GPRS card). In this case please observe the notes about installation requirements for 'Modem or data card' →Page 13 and notes about configuration under 'Setting up a UMTS or GPRS profile' →Page 106.

PPTP Microsoft Point-to-Point Tunnel Protocol;

Hardware: Ethernet adapter, xDSL modem;

Networks: xDSL;

Remote destinations: Access Router in the xDSL;

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.

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.

4.1.4 Use Microsoft RAS-Dialer

Only available for Windows systems.

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

4.1.5 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.

4.2 Dial-Up Network

Only available for Windows systems.

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).



Note: 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.

-> see following parameters:

- Username [Dial-Up Network]
- Password [Dial-Up Network]
- Destination phone number
- Save password
- RAS script file

EN

4.2.1 Username [Dial-Up Network]

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.

4.2.2 Password [Dial-Up Network]

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.

4.2.3 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"

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.

4.2.4 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.

4.2.5 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.

4.3 Connection via Modem

Only available for Windows systems.

4.3.1 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.

4.3.2 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

4.3.3 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 and 115200

4.3.4 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.

4.3.5 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).

4.3.6 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

4.3.7 APN

The APN (Access Point Name) is required for the GPRS/UMTS and UMTS dial-in. You obtain this name from your provider. The APN is used particularly for administrative purposes.

4.3.8 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.

4.4 HTTP Logon [Parameters]

Only available for Windows systems.

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.

If the access point executes an HTTP redirect, then user name and password entry is not necessary in a browser window. Instead the authentication data are entered here.

For script driven logon you can use a script from the installation directory
\\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.

4.4.1 User ID [HTTP Logon]

This is the user name that you have obtained from your HotSpot operator.

4.4.2 Password [HTTP Logon]

This is the password that you have obtained from your HotSpot operator. The password is concealed with asterisks (*) when entered.

4.4.3 Save password [HTTP Logon]

After the password has been entered it can be saved

4.4.4 HTTP authentication script [HTTP Logon]

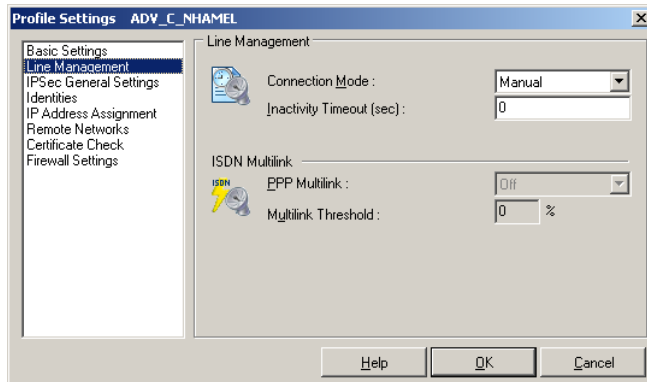
Click on the Browse button [...] to select the saved logon script.

4.5 Line Management

Only available for Windows systems.

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 (NAS) that you are communicating with support the same number of channels.



-> see following parameters:

- Connection Mode
- Inactivity Timeout
- PPP Multilink (only possible with communication medium "ISDN")
- Multilink Threshold (only possible with communication medium "ISDN")

4.5.1 Connection Mode

You can define how the client builds a link via the profile to the destination. There are three Modes to select from:

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 than zero (0). If the Inactivity Timeout is set to zero then you must manually disconnect.

automatic (default) = Means that the Secure Client will automatically activate a connection in accordance with your application program requirements to the destination selected in the Phonebook. A disconnect also occurs automatically, provided that the Inactivity Timeout parameter is set to any value other than zero.

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.

4.5.2 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.

4.5.3 Prioritise Voice over IP (VoIP)

If the client is being used for VoIP communication this function should be activated in order to transmit and receive the voice-data without delays or distortion.

For VoIP-Prioritisation defined ports are being monitored for incoming or outgoing connections. Should such a connection be established, the bandwidth for FTP and SMB-Protocol will be reduced. On closing the connection the original bandwidth will be restored.

4.5.4 PPP Multilink



Only for ISDN

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.

4.5.5 Multilink Threshold



Only for ISDN

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.

4.5.6 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.

4.5.7 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 -> HTTP Logon).

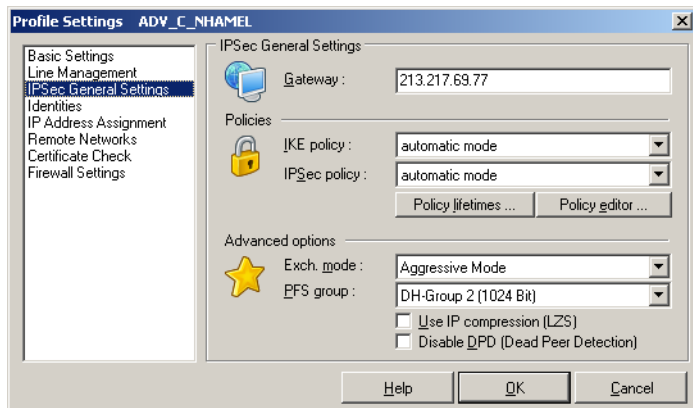
The HTTP logon is not switched on in the phonebook for a link with the connection type WLAN! Instead, activation of this function causes the authentication data from the WLAN settings in the Monitor menu to be used for this destination system.



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.

4.6 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.



-> see following parameters:

- Gateway
- IKE Policy
- IPSec Policy
- Policy lifetimes

- Policy editor
- Exch. mode
- PFS group
- Use IP compression (LZS)
- Disable DPD (Dead Peer Detection)

4.6.1 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.

4.6.2 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.

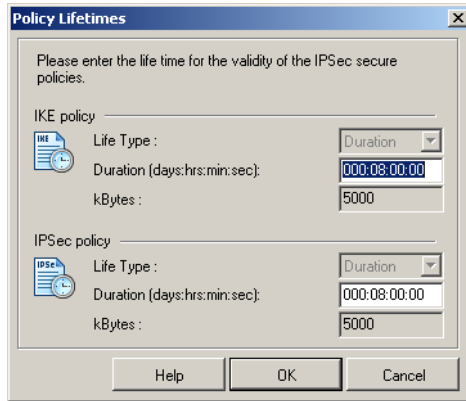
Pre-shared Key: This preconfigured policy can be used without PKI support. The same "Static Key" is used on both sides (see -> Pre-shared key, Shared secret in the parameter folder "Identity").

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.

4.6.3 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.

4.6.4 Policy lifetimes



The lifetime of the policies defined here are applicable to all the policies.

Life Type

Determines the criteria for key validation based either on duration or transferred bytes or both. The counter is reset for each new SA negotiation.

■ Duration [Lifetimes]

The number of Kbytes or the size of the time interval can be adjusted.

■ kBytes [Lifetimes]

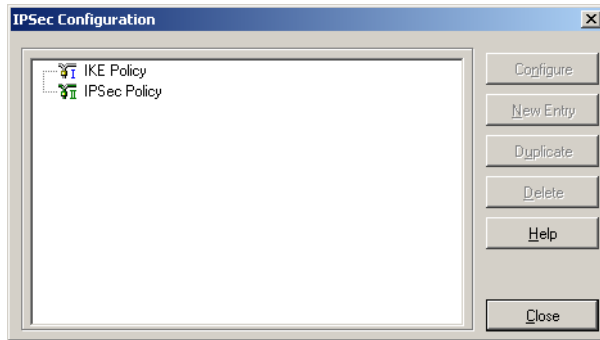
The number of Kbytes or the size of the time interval can be adjusted.

4.6.5 Policy editor

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. Any recorded data remain as configured.

■ IKE Policy

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".

Parameters:

- Policy Name [IKE Policy]
- Authentication [IKE Policy]
- Encryption [IKE Policy]
- Encryption [IKE Policy]
- Hash [IKE Policy]
- DH Group [IKE Policy]

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 ("Iden-

tity Protection Mode") is used. Choices are DES, Triple DES, Blowfish, AES 128, AES 192, and AES 256.

Hash [IKE-Richtlinie]

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) and SHA (Secure Hash Algorithm).

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

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".

Parameters:

- Policy Name [IPsec Policy]
- Protocol [IPsec Policy]
- Transform [IPsec Policy]
- Authentication [IPsec Policy]

Policy Name [IPsec Policy]

Give this policy a name over which an SPD can later be allocated.

Protocol [IPsec Policy]

The IPsec Policies differ essentially according to the two security protocols, AH or ESP, that cancel each other out in tunnel mode. The fixed default value is

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.

Authentication [IPSec Policy]

The authentication mode can be specifically set here for the security protocol ESP. Choices are: MD5 and SHA.

4.6.6 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.

4.6.7 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".

4.6.8 Use IP compression (LZS)

The data can be compressed in order to increase transmission rates. By enabling compression the throughput can be increased to up 3 times that the regular transmissions without compression.

4.6.9 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.

4.7 Extended IPsec options

Use IP compression (LZS)

The data can be compressed in order to increase transmission rates. By enabling 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

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).

Standard for IPsec with UDP is port 4500, for IPsec without UDP it is port 500. The NCP Gateway detects UDP encapsulation automatically.

VPN Path Finder

Via VPN Path Finder one can use IPsec connections behind firewalls, even if their port settings do not allow the use of IPsec (e.g. in hotels).

The VPN Path Finder automatically switches to the alternative connection protocol TCP Encapsulation with SSL Header (port 443), once the standard IPsec via port 500 and accordingly UDP Encapsulation is not available. This is important if the client can only use the https port 443 and no stand alone IPsec connection is available.

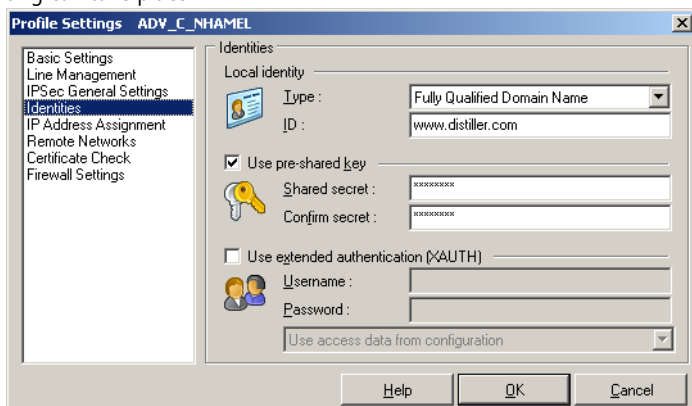
It is also possible to connect a proxy server first if required.



VPN Path Finder technology only works if the remote is a LANCOM VPN router operating LCOS version 8.0 or higher.

4.8 Identity

According to the security mode setting IPSec a more detailed parameter setting can take place.



4.8.1 Type [Identity]

According to the security mode setting IPSec a more detailed parameter setting can take place.

-> see following parameters:

- Type [Identity]
- ID [Identity]
- Use pre-shared key
- Use extended authentication (XAUTH)
- Username [Identity]
- Password [Identity]
- Use access data from configuration

4.8.2 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 (corresponds with the user's email address)
- Fully Qualified Username
- IP Subnet Address
- ASN1 Distinguished Name
- ASN1 Group Name
- Free String used to identify Groups

4.8.3 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.

4.8.4 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.

4.8.5 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

4.8.6 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.

4.8.7 Username [Identity]

Contact your System Administrator for your "Username". The name can be up to 256 characters long.



TNote: This parameter pertains only to accessing the gateway at the remote site.

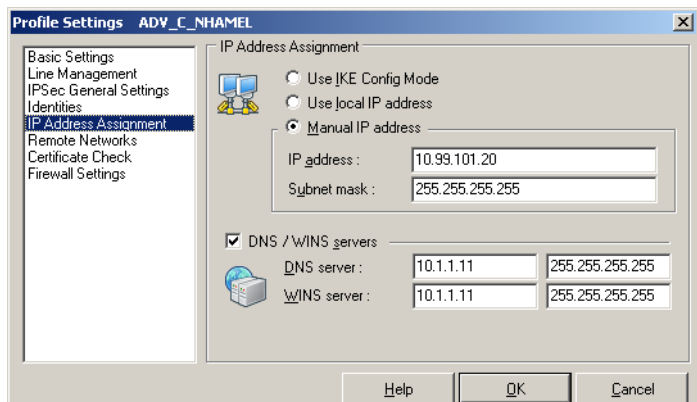
4.8.8 Password [Identity]

Contact your System Administrator for your "Password" for XAUTH. The password can be up to 256 characters long.



TNote: This parameter pertains only to accessing the gateway at the remote site.

4.9 IP Address Assignment



4.9.1 Assignment of the private IP Address

It can be specified in this parameter field how the IP address should be assigned.

Use IKE Config Mode

With IKE config mode (Draft 2) the IP addresses of the client, the DNS and WINS servers as well as the domain name are dynamically assigned. All previous WAN interfaces can be used for the NAS dial-up.

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

Use local IP address

In this case the current IP addresses (also DHCP) which are configured in the network settings of the PC are used for the IPSec client. (This is the standard setting.)

Use manual IP address

This is the IP address and the subnet template which can be freely entered here. In this case the addresses which are entered here are used, regardless of the configuration in the network settings.

DHCP over IPSec

As an alternative to the usage of IKE config mode, a DHCP server of the Gateway can also be used. In the process the IP address is assigned to the client via the VPN tunnel in a DHCP negotiation.

4.9.2 DNS / WINS server

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.

4.9.3 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. .

4.9.4 WINS server

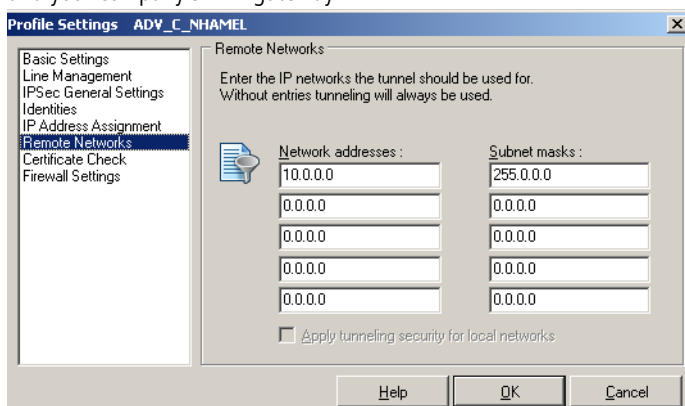
The IP address of the WINS server entered will be the one used instead of the WINS Server assigned during the PPP negotiation.

4.9.5 Domain name

This is the domain name, which otherwise is transferred to the system per DHCP in the network settings.

4.10 Remote 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.



Note: This is also referred to as "Split Tunneling".

4.10.1 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.

4.10.2 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.

4.10.3 Apply tunneling security for local networks

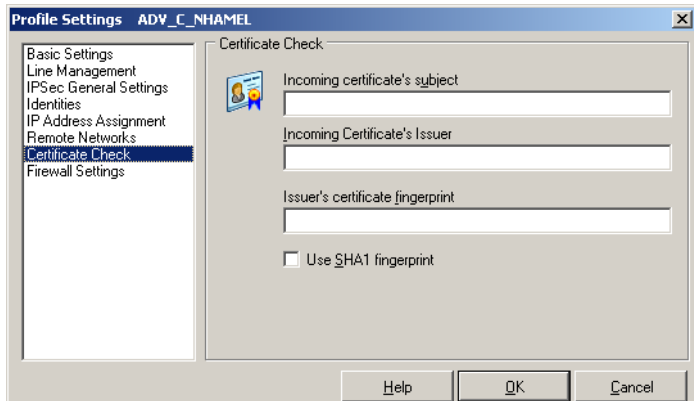
If you wish to encrypt the local LAN traffic by means of VPN tunneling enable this function.

4.11 Certificate Check

Checking the certificate contents

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 following topics:

- Incoming certificate's subject
- Incoming certificate's Issuer
- Issuer's certificate fingerprint
- Use SHA1 fingerprint
- Further certificate checks

4.11.1 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
- g = Given name
- t = Title
- o = Organization / Company
- ou = Organizational Unit / Department
- c = Country
- st = State / Province

- l = Location / City

- 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.

4.11.2 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

- g = Given name

- t = Title

- o = Organization / Company

- ou = Organizational Unit / Department

- c = Country

- st = State / Province

- l = Location / City

- email = E-mail

Example: cn=ABC GmbH. Only the common name of the issuer is verified here.

4.11.3 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.

4.11.4 Use SHA1 fingerprint

Der Algorithmus zur Erzeugung des Fingerprints kann MD5 (Message Digit 5) oder SHA1 (Secure Hash Algorithm 1) sein.

4.11.5 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 \ncple\cacerts\ Windows directory. 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 client determines the issuer, then searches the issuer certificate, first on Smart Card or in the PKCS#12 file, and then in the NCPL\CACERTS\ directory. 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.



Exception: For a server callback 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.

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 \ncple\crls\ Windows directory. 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 \ncple\arls\ Windows directory.

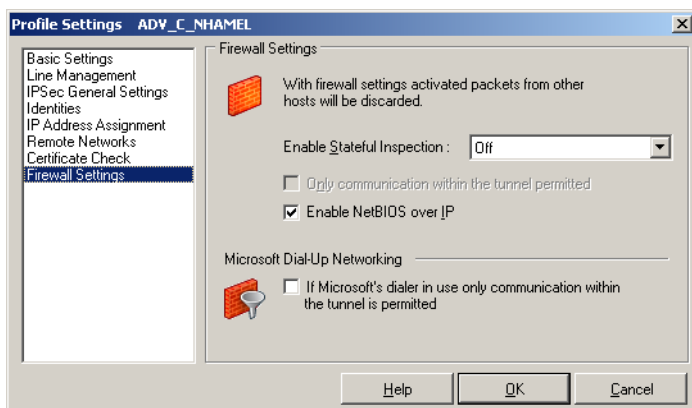
If incoming certificates are contained in the CRL or ARL lists, then the connection is not permitted.

If CRLs or ARLs are not present, then no check takes place in this regard.

4.12 Link Firewall

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 highest 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 the protocols UDP, TCP, FTP (active and passive) and ICMP - whose packets 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..



4.12.1 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.

4.12.2 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.



Please consider that if the LANCOM LANCAPI is in use as well, this must remain off, otherwise the LANCAPI server in the local network can no longer be used.

4.12.3 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.

4.12.4 If Microsoft's dialer in use only communication within the tunnel is permitted

Only available for Windows systems.

When using the Client Monitor this function prevents communication to the Internet via the RAS Dialer.

4.13 Setting up a UMTS or GPRS profile

Only available for Windows systems.

Even when you are travelling, the LANCOM Advanced VPN Client gives you the benefit of secure connections from your notebook to your own network or that at the headquarters. A highly convenient method is to use a special data card for communications via the UMTS or GPRS standard as offered by most of the major mobile telephone providers.

4.13.1 Alternative ways to connect via UMTS or GPRS

The LANCOM Advanced VPN Client can be configured in two different ways to use this type of data card to establish a connection:

- The data card is operated with the software provided by the operator of the mobile telephone system. This software is initially used to establish a connection to the Internet. The profile in LANCOM Advanced VPN Client then uses this Internet connection as a "LAN connection".

The profile is set up with the appropriate communication medium 'LAN (over IP)' and the necessary VPN parameters; no further information is required to establish the connection.

The advantages of this method:

- Easy configuration of the profile in LANCOM Advanced VPN Client
- The status information provided by the mobile telephone system provider is available (selected network, signal strength, transfer volumes, statistics, etc.)

A disadvantage with this scenario is that the connection has to be started and terminated manually.

- The alternative is to operate the data card with LANCOM Advanced VPN Client directly. In this case, the VPN information and the parameters necessary for connection establishment via the data card are entered into the connection profile.

The particular advantage of this method: After setting up the profile in LANCOM Advanced VPN Client, you can automatically start your UMTS or GPRS connection at the same time as starting the VPN connection. The current network status for the data card is not available, however.



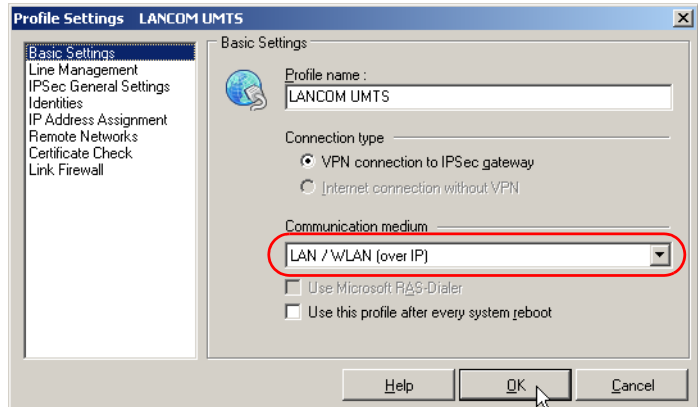
The direct control of the data card requires the appropriate modem driver to be installed. This driver is set up during the installation of the operating software from the mobile telephone provider.

4.13.2 Setting up communication via the mobile telephone provider's software

This is how to set up a new profile for UMTS or GPRS connections that use the operating software from the mobile telephone provider:

- ① Install the data card in your computer as described in the supplier's instructions and ensure that a connection can be established correctly.

- ② In LANCOM Advanced VPN Client, create a new profile with the parameters necessary for the VPN connection.
- ③ To do this, select the communication medium as 'LAN / WLAN (over IP)'. A connection that exists via a UMTS or GPRS data card is used by LANCOM Advanced VPN Client as a LAN connection that is the basis for a VPN tunnel.

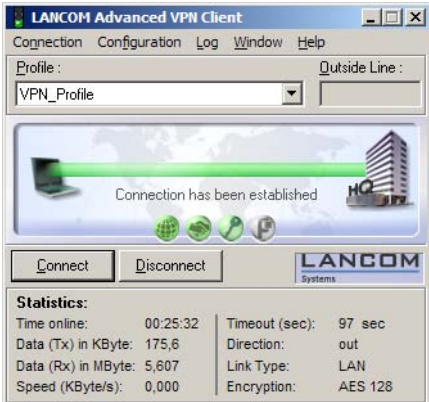


- ④ If possible, test the establishment of a VPN tunnel over a "true" LAN or WAN connection (e.g. an Ethernet connection to the Internet, or similar).
- ⑤ Then you can disable all connections to the Internet (via Ethernet, ISDN, etc.) and then re-start the UMTS or GPRS connection using the operating

software from the mobile telephone provider (illustrated example: Vodafone).




- ⑥ As soon as the Internet connection via the UMTS or GRPS data card has been established, start the connection with the LANCOM Advanced VPN Client.



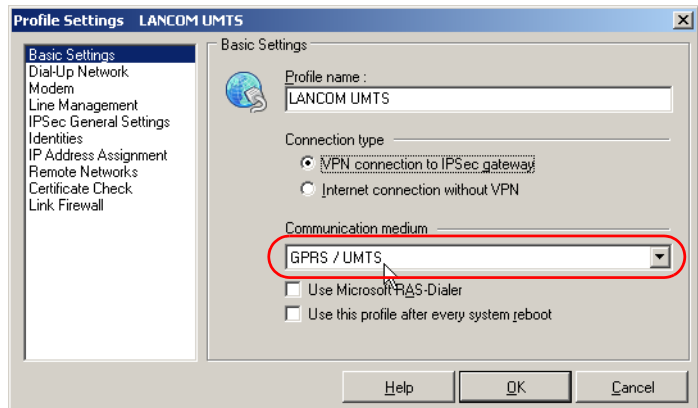
4.13.3 Setting up a direct connection over LANCOM Advanced VPN Client

This is how to set up a new profile to control the UMTS or GPRS data card directly:

- ① Install the data card in your computer as described in the supplier's instructions and ensure that a connection can be established correctly.
- ② In LANCOM Advanced VPN Client, create a new profile with the parameters necessary for the VPN connection.

 Leave the UMTS or GPRS data card in the PCMCIA slot while you are setting up the connection profile to ensure that the modem can be selected for the configuration.

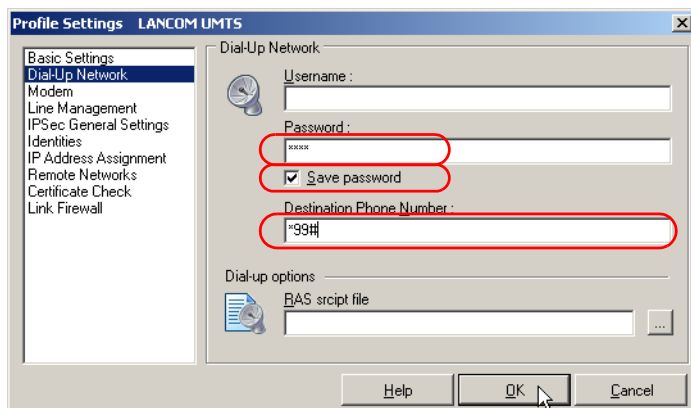
- ③ Select the communication medium as 'GPRS / UMTS'. The UMTS or GPRS data card functions to provide a modem connection that the LANCOM Advanced VPN Client can then use to establish a VPN tunnel.



- ④ In the 'Dial Up Network' area, enter the information required for dialing-in to the server at your mobile telephone provider (see 'Dial-in information for various mobile telephone providers' → Page 113).

Make sure that you enter the telephone number. The password (the PIN number for the SIM card in the UMTS or GPRS data card) can optionally

be entered as the password. Storing this password in the profile means that it won't be requested when making a connection.

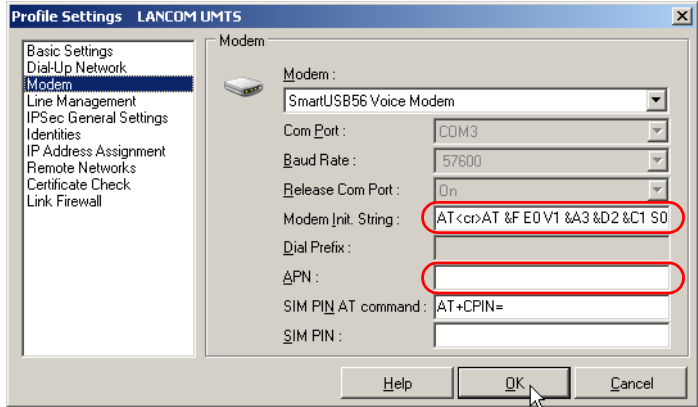


- ⑤ The in area 'Modem', select the modem driver that was installed along with the UMTS or GPRS data card. Enter the required modem init string. This init string generally consists of the following elements:
- ☐ AT+F<cr> (resets the modem firmware to its default values)
 - ☐ AT+CGDCONT=1, "IP", (commences the entry of the mobile telephone provider's APN)
 - ☐ web.vodafone.de (APN of the mobile telephone service provider)



Depending on the data card model, further information may be necessary for the init string. Information about the required init string can be found in the documentation with your data card or directly from your mobile telephone provider.

APN and SIM can be entered into the following fields.



Further APNs from various mobile telephone providers can be found under 'Dial-in information for various mobile telephone providers' → Page 113.

- ⑥ Once the profile is fully set up with the VPN parameters and UMTS or GPRS information, a single click on the **Connect** button in the LANCOM Advanced VPN Client is all you need. The client the initially establishes the connection via the UMTS or GPRS data card and then it automatically sets up the VPN tunnel to the selected VPN gateway.



4.13.4 Dial-in information for various mobile telephone providers

Mobile tele- phone operator	T-Mobile	Vodafone	E-Plus	O2 Genion
Telephone number	*99#	*99#	*99#	*99#
User name	(any)	(any)	eplus	(any)
Password	(any)	(any)	(any)	(any)
DNS server	193.254.160.1	139.7.30.125	212.23.97.2	195.182.96.28
Alternative DNS server	0.0.0.0	139.7.30.126	212.23.97.3	195.182.96.61
Modem command (init string)	+cgdcont=1, "IP", "internet.t-t-d1.de"	+cgdcont=1, "IP", "web.vodafone.de"	+cgdcont=1, "IP", "internet.eplus.de"	+cgdcont=1, "IP", "internet" ("internet.interkom.de" for pre-paid O2 Loop)

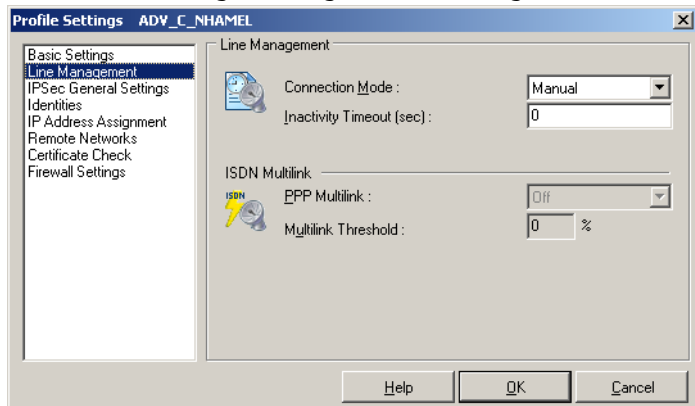
5 Establishing a Connection

5.1 Establishing a Connection to the destination system

The client software allows the definition of many different target systems which can be named and configured according to requirements.

To define a target system, click on **Configuration > Profile-Settings** in the menu bar. A Window with the profile-settings will now appear and show all previously defined targets

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 under **Configuration > Profile Settings > Configure > Line Management**.



5.1.1 Automatic connection

The Client works on the principle of LAN emulation, whereas with Microsoft RAS, every connection has to be established manually. You are only required to start the according application (Email, Internet Browser, Terminal Emulation, etc.) The connection will then be established automatically, using the parameters of the target system.

5.1.2 Manual connection

It is also possible to manually connect to the chosen target.

This is done by clicking on “Connection” in the Monitor and than selecting “Connect”.

5.1.3 Variable connection

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:

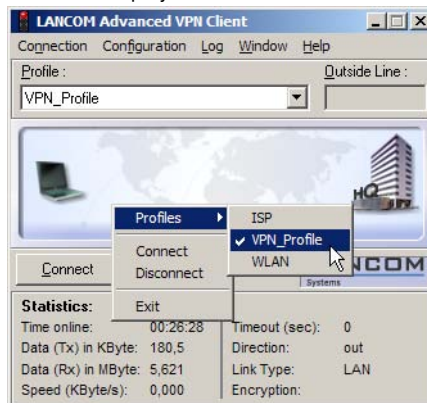
- If the connection was terminated as a result of a timeout, then the following connection will be automatically initiated as required.
- On the other hand if the connection was terminated manually, then the following connection must then also be established manually.

5.2 Connect

Independent of the connection mode, the monitor always displays, if being visible in foreground.

The connection status as explained in the following example:

First step is to select a destination system to connect to – click the right mouse button to display the menu.



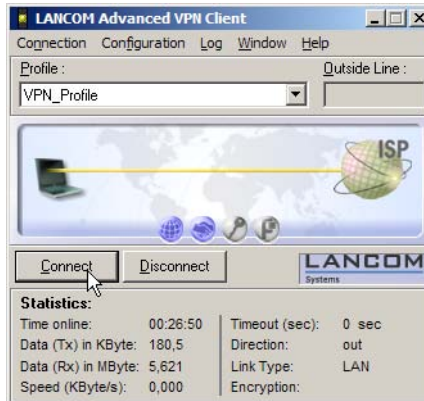
Afterwards the connection is being established- in this case manually through the menu appearing on right-click.

If the use of a (Soft-) Certificate was configured – as on the trial-connection with SSL – you first have to enter the PIN.

Then a link to the Internet Service Provider (ISP) is built indicated by a yellow line. The dial-up negotiation is displayed with a symbol representing a globe

and the authentication status with a handshake. Upon doing so the symbols change according to the current status.

- light blue = Link building stage
- dark blue = Stage passed
- green = successfully negotiated stage.



The successfully passed stages are displayed by minimized symbols.

Upon a successful authenticated connection with the ISP/Network Access Server (green line and green handshake symbol) ...



... a tunnel is built indicated by a new yellow bar and the second dial-up to the VPN Gateway starts. Here authentication is necessary as well. In addition under the use of Test connection SSL an encryption (key) is configured.

If the configuration of the destination system is set to utilize compression, you can configure compression as well.

If the last stage of the link built (here encryption resp. decryption) is successfully passed, the traffic light switches to green...

... as well as the tunneling. Now a connection is established.!



Please note that green traffic lights indicates that a link is built and that communication costs are being incurred!

5.3 Client Logon

Only available for Windows systems.

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).

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.

If the use of a (Soft-) Certificate was configured – like example destination Test connection SSL – you first have to enter the PIN.

The following stations of the link built in the same procedure as described above under "Connect"...

... until the connection is established.

5.4 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. The password ID can include up to 256 characters. Normally the password will be assigned to you by your Destination since the target-system has to be able to identify you. You will receive the password from your HQ, your internet service provider or your system administrator.

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 note that in case of a saved password anyone is in a position to work with your client software- even if he does not know your password.

5.4.1 User ID for NAS Dial-Up

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)

5.4.2 Username and Password for VPN-Login

Usernames and passwords for the login at the VPN-gateway (see > Tunnel parameters) can be completely entered upon configuration of the target system. They remain available for VPN-Login even after a boot-process. If they are not entered they will be asked for in a dialog on VPN-Logon.

5.5 Disconnection and error

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")

5.6 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.

5.7 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 explicitly for a prompt.



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!