

# Description of Parameters

high security remote access

## NCP Secure Enterprise Suite

**NCP**

SECURE COMMUNICATIONS



# **Secure Enterprise Suite Parameters**

## Support

NCP offers support for all international users by means of Fax and Internet Mail.

### Fax Hotline Number

+49 911 99 68 458

### Internet Mail Address

support@ncp-e.com

When contacting NCP with your problems or queries please include the following information:

- exact product name
- serial number
- Version number
- Accurate description of your problem
- Any error message(s)

NCP will do its best to respond as soon as possible, but we do not guarantee a fixed response period.



Network  
Communications  
Products engineering GmbH

### GERMANY

Headquarters:  
Dombühler Straße 2  
D-90449 Nürnberg  
Tel.: +49-911-99680  
Fax: +49 - 911 - 9968 299  
Internet <http://www.ncp-e.com>  
E-mail: [info@ncp-e.com](mailto:info@ncp-e.com)

## Copyright

*Considerable care has been taken in the preparation and publication of this manual, errors in content, typographical or otherwise may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP as desired.*

*NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or use for any particular purpose. Furthermore NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes.*

*This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH, Dombühler Str. 2, D - 90449 Nürnberg, Germany.*

*All trademarks or registered trademarks appearing in this manual belong to their respective owners.*

© NCP engineering, April 2012



# Enterprise Suite Parameters



In this document all configuration parameters of the profile settings and the IPsec configuration of the Secure Enterprise Suite are described.

The order of the parameter descriptions was adjusted to the profiles in Enterprise Client on the order of the configuration fields.

All parameters are listed in the **Index**.

On the following page **the configuration fields of the profile settings** are listed. From this page the configuration fields can be directly selected per mouse click without needing to page through the document. A mouse click on the Enterprise Client icons directs you back to this page.\*



Per mouse click on one of the boldly printed red terms, you jump to the respectively given position in this documentation.



Should the icon for a NCP-PDF be installed (left) next to the red term, then the corresponding further-reaching document will be opened with a mouse click, assuming it is found in the same directory as the parameter description.



The easiest way to receive the desired information is via the **Enterprise Suite Navigation**. All available documents about your product are recorded in this pdf file.

Starting from navigator, you can jump directly into all relevant documents and download them from the NCP homepage in case they are not yet saved in your navigator directory.

*\* Please observe that not all parameters and configuration fields must always be displayed in the user interface of your secure client. On the one hand they will be automatically displayed or hidden according to the respectively selected linking medium (e.g. Modem oder HTTP Logon). On the other hand individual configuration fields or parameters, which you do not need for your work with the client, can be hidden by your system administrator..*

## Configuration Modes and Online Help



Profile settings can be configured using one of three different configuration modes. (See **Configuration Modes**)

When OK is pressed any changes made to the configuration of the currently selected profile will become effective, regardless of which configuration mode is selected. The changes will be then reflected across all three modes.

When a profile is first opened, the default values are displayed in a single configuration window.

From then on, five further configuration windows can be opened using the “Extended” button and then closed using the “Standard” button. “Expert” mode shows the current settings of all available parameters.

The configuration mode selected when the last “Edit” operation was finished will be re-opened when a subsequent edit is started.

### Standard Configuration

The Standard Configuration displays the most important parameters (about communication medium, network connection, VPN gateway access data and HA support)

### Extended Configuration

The Extended Configuration displays additional parameter fields associated with Advanced IPsec Settings, L2TP capabilities, Split Tunneling, Connections and Authentication Options.

### Expert Mode

In Expert Mode every setting of every parameter in the Client software can be modified. To do this a list of parameters is displayed in the RH window folder and the appropriate setting for a parameter can be selected as required. **Expert mode is blocked in the default settings in Secure Enterprise Management!**

### Online Help

The Online Help system mirrors the structure of Expert Mode, i.e. it displays text associated with each configuration parameter, independent of the configuration mode that is selected.

# Configuration Fields of the Profile Settings

**Basic Settings**

**Dial-Up Network**

**Modem**

**GPRS / 3G**

**HTTP Logon**

**Line Management**

**Callback**

**Security**

**Advanced**

**Pre-authentication**

**VPN Tunneling**

**Advanced IPsec Options**

**IPsec Address Assignment**

**Split Tunneling**

**HA Support**

**DNS / Management**

**Certificate Check**

**Link Firewall**

## IPsec Configuration

**IKE Policy**

**IPsec Policy**

**Index**

## Basic Settings



The client software allows the creation of individual profiles, which can be configured according to the user requirements. In order to distinguish between profile settings, a name must be initially given for the profile in this parameter field. Subsequently the connection medium to the remote station can be more precisely defined.

### Profil Name

When you define a new profile, you should initially enter a distinctive name for the profile ( e.g. IBM London). The name may contain any desired letters as well as numbers and may be up to 39 characters including spaces.

### Communication Medium



The selection button can be specifically used to set the communication medium for each profile, assuming you have connected the corresponding hardware and installed it in your system. The following communication media can be set:

#### ISDN

Hardware: ISDN hardware  
(card, ISDN box or PCMCIA card)  
with Capi 2.0 support;  
Network: ISDN fixed network;  
Remote stations: ISDN hardware;

#### Modem

Hardware: Asynchronous modems (PCMCIA modem, GSM card) with Com Port support;  
Network: PSTN (also GSM and GPRS);  
Remote stations: Modem or ISDN card with digital modem;

#### LAN (over IP)

Hardware: LAN adapter;  
Network: Ethernet based LAN;

#### xDSL (PPP over Ethernet)

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

#### xDSL (AVM - PPP over CAPI)

The communication medium can be selected if an AVM Fritz! DSL card is used. In the field “call

number (target)” in the group “network dial-up” AVM-specific initialization commands can additionally be entered for the connection using CAPI. Under the Windows operating systems it is however recommended to use the standard “xDSL (PPPoE)”, since it allows for direct communication with the card via the network interface. When using the AVM Fritz! DSL card no separate additional network card is required.

Network: xDSL;

Remote stations: Access Router in xDSL;

### GPRS / 3G

Select this medium if the dial-up should be carried out using the mobile wireless network (GPRS or 3G). For this purpose, observe the guidelines given under **Mobile Computing** und **Secure Client Monitor**.



### PPTP

Microsoft Point-to-Point Tunnel Protocol;  
Connected hardware: Ethernet-Adapter, xDSL-Modem;  
Network: xDSL;  
Remote stations: Access Router in xDSL;

Should this protocol be selected then the IP address of the access router must be entered in xDSL in the parameter field **Dial-Up Network** under “PPTP Endpoint”.

### Wi-Fi

Hardware: Wi-Fi adapter;  
Network: Wireless network;  
Remote stations: Access point;

The Wi-Fi adapter can be operated under Windows 2000/XP and Vista with the connection type “Wi-Fi”. In the monitor menu the item “Wi-Fi settings” specifically appears, in which the access data to the wireless network can be stored in a profile. Should this “Wi-Fi configuration be activated”, then the management tool of the Wi-Fi card must be deactivated. (Alternatively the management tool of the Wi-Fi card can also be used, then the Wi-Fi configuration is deactivated in the monitor menu.)

Should the connection type Wi-Fi be set for a target system in the telephone book, then a further interface will be displayed under the graphical field of the client monitor, on which the field strength and the Wi-Fi network is displayed. See **Mobile Computing** and **Secure Client Monitor**.



## External Dialer

Should the connection type “Ext. dialer” (over the external dialer) be set, then pushing the “connection” button starts a preconfigured EXE-file (e.g. the iPass dialer). Using the EXE file, the connection is established with the Internet and subsequently the VPN dial-up of the client is initiated using “RWSCMD/connect”. The NCP dialer works under this configuration in the LAN mode.



This connection type only functions when the dial-up in the parameter field “connection control” is switched to “manual”.

Depending on the installed dialer (iPass or T-Online) the EXE file of the dialer must be entered for the entry “ExeName” in the configuration file EXTDIAL.INI. In order to avoid specifying the complete path for the dialer in the DAT file, the path can be optionally read from the registry and entered in the INI file. The exact wording of the heading of the dialer, paying attention to capital and small letters, must be entered in the INI file under “caption”.

Example of the INI file for iPass. The installation path is found in the registry under “InstallPath” “Software \Ipass \iPassConnectEngine”):

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

## Automatic Media Detection



Automatic media detection can only be used when alternately communication media are available.

## Default Profile after System Reboot

Normally the client monitor is opened after a new start with the last used profile. Should this function be activated, then after a new start of the system the profile which belongs to it will always be loaded, independent of which profile was last used.

## Use Windows Dial-up Networking

For the dial-up on the ISP (Internet Service Provider) the microsoft remote transmission dialer can be used. This is always necessary when the dial-up point requires a dial-up script. The remote transmission dialer supports this script. In the parameter window “Network dial-up” the script file is subsequently entered by inputting the path and name of the script file which is running (see below script file).

### never

With the “never” setting the Dialer of the client is used exclusively to dial-in.

### only for script dial-in

If the data communications dialer will be used “only for script dial-in”, then select this option. For a dial-in point that does not require a script, the system automatically switches to the Dialer of the client.

### always

If the data communications dialer will always be used, then the appropriate setting must be made.

In the parameter folder Dial-Up Network the **RAS Script File** must be entered including its path and name. The script file you receive from your provider.

(Using an international phonebook the script file will be entered automatically and cannot be modified anymore.)



## Automatic Media Detection



If different communication media are used alternately, e.g. LAN or Wi-Fi (within the corporate network) or modem and ISDN (during remote access), manual selection of the profile with the respective communication medium is rendered superfluous, provided the profile with communication medium LAN has been changed to a profile with automatic media detection and a profile for each alternatively available communication medium like modem, ISDN, DSL or GPRS/3G is available.

### Configuration Instruction

1. Configure a profile for LAN or Wi-Fi to the VPN gateway within your corporate network. For this you need the IP address of the VPN gateway and your authentication data (i.a. VPN user ID; VPN password) and possibly the certificate configuration.
2. Change the communication medium from LAN or Wi-Fi to "automatic media detection". (A connection to the VPN gateway within the corporate network has to be possible with this configuration!)
3. Configure an alternative profile which contains all access data for the internet service provider and the parameter for an alternative communication medium. Then define this profile as "profile for automatic media detection".
4. The alternative profile may be copied for further alternative communication media. Only media specific parameter changes need to be made in these profiles.
5. Please take care, that prior to connection set-up the profile with the communication medium "automatic media detection" has to be selected.

### Profile for Automatic Media Detection

With the activation of this function this profile is automatically linked with the profile for automatic media detection and is automatically used for a potential connection establishment in the case of availability of the corresponding medium.

## Seamless Roaming



**Seamless Roaming** is configured by using two Link Profiles in the Profile Settings. The communication medium of one Link Profile with a LAN connection to the gateway is changed to "Automatic Media Detection" and the switch "Seamless Roaming" set; a connection to the gateway via GPRS / 3G is defined in a second Link Profile and this is activated with "Profile for Automatic Media Detection".



See the description of **Seamless Roaming!**

### Disconnect the logical VPN tunnel when the connection is broken

When a break occurs in the physical communication medium connection used to establish a VPN tunnel, the existing VPN tunnel remains established, for an unspecified length of time. Thus the tunnel remains logically active while the new physical connection is being established.



See the description of **Seamless Roaming!**

### Maintain mobile wireless network connection with Seamless Roaming

If Seamless Roaming has been enabled for a set of profiles with different media types, this option defines whether or not the Wi-Fi or UMTS / 3G connection remains intact during the changeover from one media type to another. This option must only be set on the "Profile for Automatic Media Detection".



See the description of **Seamless Roaming!**

## Dial-Up Network



The data for the dial-up network are evaluated using this parameter field. It contains User ID and Password which are needed for the PPP negotiation to the Internet service provider (ISP).

In the connection type “PPP over Ethernet” the parameter field “phone number” is eliminated. The parameter field does not appear at all if the client is operated in the connection type “LAN over IP”.



When using the communication medium GPRS / UMTS for mobile Computing refer to the description **Secure Client Mobile Computing**.

### Username

With the username you identify yourself to the Network Access Server (NAS), when you want to establish a connection to the remote station. The username can be up to 255 characters long. In the normal case, you will be assigned a username from the destination system, since you must also be recognized from there. You receive it from your head office, from the Internet Service Provider or the system administrator.

### Password

You need the password to be able to identify yourself to the Network Access Server (NAS) when the connection is established. The password may be up to 128 characters long. In the normal case, you will be assigned a user name from the destination system, since you must also be recognized from there. You receive it from your head office, from the Internet Service Provider or the system administrator.



Note: If profiles are configured for the “automatic media detection”, it is compulsory that an (NAS) password be entered for all of these profiles, otherwise the connection cannot be established.

When you enter the password, all characters will be displayed as stars (\*) in order to prevent undesired monitoring. It is important that you enter the password exactly as specified and pay attention to small and capital letters.



Note: In case you haven't activated the parameter “save password”, the following applies: Even if you have chosen the connection mode “automatic”, you must establish the connection the first time manually. In the process you will be asked for the password. For every further automatic dial-up this password will be automatically assumed until you reboot the PC or change the profile.

## Save Password

This parameter must be activated (clicked on) if you desire that the password (insofar as it is entered) be saved. Otherwise the passwords will be deleted as soon as the PC is booted or a profile is changed. The activated function is standard.



Important : Please observe that in the case of saved passwords, each person can work with your client software - even if he doesn't know the passwords.

## Destination Phone Number

In the case of a switched connection the phone number for the destination must be entered. This phone number must be exactly entered as if you would call this telephone number manually. This means you must observe all the necessary area codes: Country code, city code, extension numbers, etc. The phone number can contain a total of up to 30 characters.

Do not however enter the outside line access, even if you are connected to an interphone system! The outside line access is entered under the monitor menu item “configuration” and, thus, has validity for all profiles.

*Examples: You want to establish a connection from Germany to England*

00 (for the international connection, if you are calling from Germany)

44 (this is the country code for England)

171 (area code for London)

1234567 (the number you wish to reach)

In accordance with this example the following number is saved in the profile settings and used for the dial-up: 00441711234567.



Note: If a remote station wants to establish a connection to your PC with callback, the client requires this phone number in this field in order to be able to accept the call in accordance with the selected callback mode.

## Alternative Phone Numbers

It is possible that the destination system is a Network Access Server (NAS) which is equipped with several connections for various phone numbers. In this case it is recommended to enter alternative phone numbers - in case for example the first number is busy. The alternative phone numbers are attached to the first number, separated with only a colon or semicolon. A maximum of 8 alternative phone numbers are supported.

The first number is the standard phone number and is always selected first. If no connection can be established because it is busy, then the second number will be dialed, etc.



**Important :** Please observe that the dial-up can only function if the protocol properties for the connections of the alternative phone numbers are equivalent.

### PPTP Endpoint

This parameter is only displayed if the basic settings of the communication medium PPTP are selected. Should this protocol be selected then the IP address of the access router must be entered in xDSL.



In Expert Mode the IP address is entered under "Destination Phone Number".

### RAS Script File

If you use the Microsoft remote transmission dialer, enter here the script file under the entry for path and names. (See above Basic settings /Dial-up via Windows remote transmission.



### Support of the international dial-up for diverse service providers (only for Enterprise Clients)

The following providers provide foreign telephone books with the corresponding dial-up points, which are supported by the Secure Client: Gric, InfoNet, iPass, T-Online and UUNet. Should a foreign telephone book be used, then the software module for "International dialing" must be installed. (You can receive this module upon request from NCP.)

The selection of the desired telephone book is carried out in the setup program, In order to use the phone number of the international dial-up in the telephone book, the respective name of the provider must be entered instead of the "Destination Phone Number".

Provider	"Destination Phone Number"
T-Online	T-Online
UUNet	UUNET
InfoNet	INFONET
Gric	GRIC

## Modem



*This parameter field appears exclusively if you have selected “Modem” as the communication medium. All required parameters for this communication medium are gathered here.*



*Please observe that your modem has already been installed before the configuration. Normally you already have an (integrated) modem installed on your computer or notebook. Using the assistant for a new profile, now create a new entry with the communication medium modem. In this way you can already select your modem in this assistant from a selection box. All associated parameters are thereby automatically assumed by the client software, so that you do not need a configuration in this parameter field.*

### Com Port

Should modems already be installed, then the Com Port which was set during the installation will be automatically assumed as soon as the corresponding device is selected under “Modem Type”.

### Baud Rate

The baud rate describes the transmission speed between Com Port and modem. It is automatically assumed with the selected modem type. Should the baud rate of the modem not correspond to one of the available values here, select the next highest baud rate. The following baud rates can be selected: 1200, 2400, 4800, 9600, 19200, 38400, 57600 and 115200.

### Release Com Port

If you use an analog modem for your client, it can be desirable that the Com Port be released for other applications after the ending of the communication (e.g. fax). In this case, set the parameter to “on”. As long as the parameter in the standard setting remains at “off”, the Com Port will be exclusively used by the client software.

### Modem Type



The devices, which you have configured in the Windows system control under “Modems”, are made available for selection for this configuration field. Depending which modem you select, the associated parameters “Com Port” and “Modem Init. String” will be automatically assumed in the configuration fields from the driver databank of the system.

### Modem Init. String

Insofar as your modem is correctly installed in the Windows system, the corresponding “modem init. String” will be automatically assumed by this field. In exceptional cases the string can be expanded with (Hayes) commands.

Every AT command within the initialization string must be concluded with <cr>, since otherwise the command will not be transmitted. This means that in every case the init-string must be concluded with <cr>.

### Dial Prefix

This is an optional field. If the modem is correctly installed and the software is available as standard driver, then no entry must be made here. The dial prefix is only necessary in rare exceptions. Consult for this purpose the modem handbook. In the following, several examples for dial prefix:

ATDT  
ATDP  
ATDI  
ATDX

## GPRS / 3G



If you use the communication medium GPRS / 3G, this parameter folder appears. Please also refer to the description

### Enterprise Client Mobile Computing.

This folder has three configuration modes to choose from. As default setting you can select your provider from the provider list. (If your provider is not on the list, you can edit the provider list with the respective data. It is stored in the installation directory as APN.INI file.)

In the second configuration mode, the APN is read from your SIM card. The third configuration mode is user defined and all data has to be entered manually.

### Country

In the “Provider list” mode, select the country in which you are currently located. The most important providers will then be displayed. The Provider List is editable and stored as APN.ini in the installation directory.

### Provider

In the configuration mode with the Provider List, the most important providers in a particular country can be selected. (If your provider is not listed in the display, the list can be extended with the details of your provider; edit the APN.ini file in the installation directory). When a provider is selected the associated parameters, when present in the list, are automatically set into the configuration.

### APN

You obtain the APN from your provider. It can either be entered manually or read from the provider list. It is “web.vodafone.de” for Vodafone and “internet.t-d1.de” for T-Mobile. The APN (Access Point Name) is usually used for administration purposes.

### Dial-up Number

Enter a defined string of characters as “dial-up number” depending on your SIM card and provider. This string of characters tells the 3G card which type of connection has to be set up. Usually this string is \*99#. (If the connection cannot be established, please contact the hotline of your service provider).

### User ID, Password

Enter user ID and password, both of which can be freely assigned and function as access data for your ISP. This only applies if you use the automatic mode or the user defined configuration mode. If you have received a specified user ID and password from your service provider, use these. With Vodafone and T-Mobile any string of characters is sufficient.

### User ID, Password

Enter user ID and password, both of which can be freely assigned and function as access data for your ISP. This only applies if you use the automatic mode or the user defined configuration mode. If you have received a specified user ID and password from your service provider, use these. With Vodafone and T-Mobile any string of characters is sufficient.



### Forced Password Prompt at 3G Connection Setup

Usually, no distinct user ID or password are required when setting up an Internet connection via 3G. If the 3G connection requires the user to enter a user ID or password, because the company’s internet access has an APN or provider of its own, for example, the user identification prompt can be automatically displayed in a new window.

In order to use the forced password prompt, enter <pwreq> (including angle brackets) in the password configuration field in the “GPRS / 3G” configuration of the secure clients’ profile settings for the GPRS / 3G connection.

### SIM PIN

Use a SIM card for GPRS and 3G or enter your PIN for this card in this field. If no SIM PIN has been entered it is prompted during connection set up with this profile. You can decide whether it is to be saved for this profile.

If you use a cell phone, the PIN has already been entered during switching it on.

## HTTP Logon



With the settings in this parameter field the automatic HTTP Logon can be carried out. The centrally created logon script and the stored logon data can be taken over by Access Point (Hotspot) without opening a browser window.

The logon on Hotspots is automated in the following manner: with a dial-up to the access point from there an HTTP redirect to the client (with a website for logon) is carried out. Instead of a browser start for HTTP authentication, the authentication occurs automatically in the background with the entries made here.



Please observe that the connection using a Hotspot operator is subject to fees. You must agree to the terms and conditions of the Hotspot operator if the connection should be established.

For the script-controlled logon a script from the installation directory  
`<install>\scripts\samples`  
 can be accordingly adapted for other Hotspots.



With the connection type Wi-Fi the authentication data for the Hotspot from the Wi-Fi setting will be assumed, and respectively if these are deactivated, from the management tool of the Wi-Fi card.

### User ID | HTTP Logon

This is the user name, which you received from your Hotspot operator.

### Password | HTTP Logon

This is the password, which you received from your Hotspot operator. The password is entered with encoding (with \*).

### Save Password | HTTP Logon

After the password has been entered, it can be saved.

### HTTP Authentication Script | HTTP Logon

After clicking on the search button [...] the stored logon script can be selected here.

In order to be able to check incoming certificates in the HTTP authentication, the variable CACERT-DIT must have been placed in the script. Furthermore, the contents of the WEB server certificate can also be checked. Additional variables are available for this purpose:

CACERTVERIFY\_SUBJECT  
 checks the contents of the subject (e.g. cn=WEB Server 1)

CACERTVERIFY\_ISSUER  
 Checks the content of the issuer

CACERTVERIFY\_FINGERPRINT  
 Checks the MD5 fingerprint of the issuer certificate

Should the contents of the variable not agree with the entered certificate, the SSL connection will not be established and a log-signal will be displayed on the monitor.



## Line Management



*In this parameter field you specify how the dial-up should proceed and set the time-out values. In addition you can activate compression and specify the type of the compression. With compression the data throughput can be increased by the factors 3 to 5, depending on which data are involved.*

*Should the communication medium ISDN be used, the channel bundling can be activated. Please observe that the channel bundling can only function if both the client and the remote station are equipped with the same number of possible B channels.*

### Connection Mode

Three methods are available for the establishment of a connection to the remote station. (Here pay attention to the description *Secure-Client-Monitor-d.pdf*):

**automatic** (default) This means that the client software automatically establishes the connection. The separation of the connection occurs according to your system protocol, corresponding to the requirements of the application and corresponding to additional settings in the profile.

**manual** This means that the connection to the remote station must be established manually. A separation of the connection occurs according to the set value for the time-out.

**alternating** If this method is selected, the connection must initially be established manually. Subsequently the method changes according to the connection establishment:

- should the connection be ended with time-out, then the connection will be automatically established with the next demand,
- should the connection be released manually, then it must also be reestablished manually.

Should the time-out be set to zero (0), i.e. should no time-out be set, then you must in any case separate the connection manually.



**Important:** Should you set the dial-up to “manual”, then you should activate the time-out in order to automate the dial-up. Otherwise unnecessary connection costs could arise for you.

### Keep IP Address when connecting manually

Should a connection be separated – also due to time-out – then the client loses the IP address by default, which the VPN Gateway had assigned to him from the company network for the session. If the function

“maintain the IP-address with manual dial-up” is activated, then the client keeps the IP address after the ending of the connection to the next manual dial-up, so that the logical connection remains uninterrupted.



**Note:** This functionality can only be used for manual or alternating connection modes.

### Connect at Boot

In some cases it can be desirable that the connection to a specified remote station already be established during the boot phase. This is of particular interest to the users who would like to boot their remote client PC in the same way as their office PC, which is connected via a LAN. Please observe that in this case the remote PC must be preconfigured in such a way that the LAN client is involved in the boot process.

If you want to activate “Connect at Boot”, switch this feature to “on”. The standard setting is “off”.

### Inactivity Timeout

With this parameter, the time frame is determined that must elapse after the last data movement (received or sent) before a connection termination automatically occurs. The value is input in seconds between 0 and 65535. The standard value is “100”.

If your connection (ISDN or analog) receives a charge impulse, then the client software uses the impulse interval in order to determine the optimal time of the connection termination regarding the value you have set. The time-out which optimized according to the charge cycle runs in the background and helps to reduce the connection costs.

**Note:** In order to activate the time-out, it is necessary to enter a value between 1 and 65535. The value “0” means that the separation of the connection must be carried out manually.

**Important:** The timer for the selected time interval is not activated until no more data movement or hand shaking is present in the line.

### Timeout Direction

With this parameter you determine for which transmission direction the timeout should apply. Three different settings are possible:

**TxRx** (default) The client pays attention to both the end of the sent (out) as well as the received (in) data before the timer is invoked.

**Tx** Only the sending direction (out) is observed.

**Rx** Only the receiving direction (in) is observed.

## Compression

With this parameter you determine the type of the utilized compression. Three settings are possible:

**off** (default)

**STAC** (without History)

**STAC with History** Cisco compatible



Important: The type of compression selected here must also be supported by Network Access Server (NAS).



Please observe that this is not the compression of a transmission with IPsec data. The IPsec compression is set on another place. With Entry Client under the expanded IPsec settings of the profiles, with Enterprise Client under the suggestions for the IPsec guidelines.

Please consult your Internet provider or your system administrator for further information.

## PPP Multilink



When using PPP Multilink (for ISDN) the client software can bundle up to 8 ISDN B channels. In order to use this function in the full scope, both the PC and the remote station must however be equipped with the required number of So-interfaces (4).

With dynamic link connection you indeed raise the costs for each connected B channel. At the same time, however, the costs are minimized to the same degree because the transmission time is correspondingly shortened!

With this parameter you determine how the link connection should occur. Three options are available:

**off** (default)

**Tx** Links are connected corresponding to the bit rate of the outgoing data.

**Rx** Links are connected corresponding to the bit rate of the incoming data.

**TxRx** Links are connected according the bit rate of both the incoming and the outgoing data.

## Multilink Threshold

The value of this parameter informs the client software of the bit rate, beyond which a further link (channel) should be connected. The value corresponds to percents of the maximum bit rate. Possible values are 1 to 100 (percent). The standard value is "20". This setting applies for transmitter and recipient.

## OTP Token

When a One-Time-Password (OTP) Token is used, then the PIN and password of the tokens can be entered and used instead of the standard "User ID" and "Password".

The use of the OTP is defined as follows:

**off** (default) OTP is not used

**NAS Dial-up** If the OTP Token is to be used for accessing a NAS, then the "Password" parameter field located in the parameter folder "Dial-Up Network" will be set to inactive.

**VPN Dial-up** If the OTP Token is to be used for accessing the VPN Gateway, then the "VPN Password" parameter field located in the "VPN parameter" folder will be set to inactive.



When dialing in, a dialog window will be displayed prompting for the **Onetime-Password for VPN-Access**, which requires that the PIN and Onetime-Password be entered.

If messages are sent from the ACE server because of the RSA token, then these messages are displayed on the monitor in an input field (for example "Expiration of the valid PIN").



## Callback



*The callback function can only be used for dial-up connections via the communication medium ISDN or modem!*

### Callback for outgoing connections (Gateway calls back)

#### Prerequisites

The type of the callback depends on the rights of the client, which are assigned to him (using his User ID and password) from the central Gateway.

In the case of a centrally designed callback option, a differentiation can be made between two methods, which are supported by most Gateways. Gateway determines which of the methods will be used:

**1. Fixed Callback**, which is always executed to a client with a fixed phone number. This callback method is for example preferred if the teleworker always communicates from the home office.

**2. Variable Callback** is then used when the phone number changes (varies). This method is for example preferred by mobile teleworkers who often change location.

#### Negotiate Callback

You activate the PPP callback negotiation only if a callback should occur from Gateway and the Gateway uses the callback mode PPP callback. Only then can you also enter a callback number.

#### Callback Phone Number

Here you enter the complete phone number of the client (max. 30 places) for a variable callback. This phone number is transmitted with the PPP negotiation for all dial-ups from the client to the Gateway.



For a fixed callback the callback number must not be entered, since it is stored on the Gateway.

### Callback for incoming connections (Client calls back)

#### Callback Method

This parameter is only required for the callback which the client software executes to the Gateway. The following methods are available:

**off** (standard setting) The client software does not execute a callback.

**PPP** (RFC 1570 conform) is supported by most Gateways.

**NCP** (specific) can be used with the Secure Enterprise Server.

**COSO** (Charge-One-Side-Only) also low level or D channel callback. In the ISDN D channel the client does not incur any (local) charges. COSO is also Cisco compatible.

The client software executes the callback to the phonenumber which was entered in the network dial-up parameter field for **Destination Phone Number**.

In the process the client software must also identify itself to the Gateway. This occurs with username and password in the parameter field "Dial-up Network".



Please consult your system administrator with further questions about this topic.

## Security



In the parameter field “Security” all the configuration parameters for L2Sec and IPsec for the application in remote access environments are collected. Depending on the set safety mode, L2Sec or IPsec, further parametrization can be carried out, whereby IPsec can be driven in both an L2TP tunnel (over L2TP) as well as without L2TP tunnel (native IPsec, also IPsec tunneling).

**L2Sec:** The security mode “L2Sec” was always used as the standard in earlier versions of the secure software when one of the offered encryption types was selected! In earlier versions of the secure software this configuration field was called “Encryption”.

**IPsec native or IPsec over L2TP:** Insofar as IPsec is used for remote access, the Secure Policy Database (SPD) is dynamically constructed according to the specifications of the parameters set here (see description **IPsec-Functionality**). All IP packets for this goal are processed using the dynamic SPD.



**Encryption:** With the encryption important datasets of a computer network and system are protected. Above all in the transmission of sensitive data through public networks which anyone can use, the encoding is of great significance. In the secure client software a series of safety mechanisms are implemented to prevent the access by unauthorized persons and to exclude an unauthorized usage. Although standards of encryption exist (DES or AES), no sufficient safety standards have been developed up to now which also assure comparably high security for the interoperability between various systems. Therefore it is imperative that the remote station of the Secure Client supports the correspondingly equal standards. Furthermore NCP is trying to implement newly available encoding standard.

## Security Mode

Here you can stipulate the security standard for a connection, L2Sec or IPsec (over L2TP). Please observe that only with L2Sec alongside IP packets, NetBios, IPX and SNA data can be transmitted.

### inactive

Encryption and authentication are deactivated.

### L2Sec

NCP standard. All security negotiations are carried out encoded and secure in an end-to-end tunnel (layer 2) between client and secure server. **L2Sec** can be used when **L2TP** has been selected as VPN protocol.



### IPsec

This mode is preconfigured when the **VPN protocol IPsec** (IPsec native) has been selected. Additionally with this option the standard “IPsec in Tunnelmode” (layer 3) can be used when the **VPN protocol L2TP** has been selected. This will cause **IPsec over L2TP** using every provider layer 2 media type between client and secure server (these are all communication media of the client with L2TP).



## Certificate Configuration

A certificate which was initiated using the certificate configuration of the client monitor can be selected here for the encoding and authentication in the security mode L2Sec or for the extended authentication in the security mode IPsec. (see description **Certificates**.)



Should several certificate configurations be created, then the desired certificate can be selected for this profile using the name of the certificate configuration. (see below **Extended Authentication** and **VPN User ID**).

### none

No certificate is used for data encoding and authentication.

### Standard PKI Configuration

The certificate configuration of a client older than version 9.1 will in case of an update to this version automatically be converted to the standard PKI configuration. The standard PKI configuration will also be set up after a first installation of version 9.1 if a test connection with certificate is established.

## Encryption (L2Sec)

In this field you specify whether an encoding should be implemented in the security mode L2Sec and which type of encryption should be used.

### none

Encryption not active (standard)

### assigned by destination

Depending on the encryption technology of the Gateway (destination system) the data will be transmitted in code to Blowfish 128 /448 or triple DES.

### SSSL with certificate

The establishment of a connection with this encoding is only possible if a valid PIN has previously been entered. The type of encoding (like also Blowfish and 3DES under “assigned by destination”) is established by the central gateway.

## Static Key | Security

The key can only be entered if the encryption has previously been activated. The key must be coordinated with the configuration of the remote station (gateway). It is a string with 16 hexadecimal numbers which are separated by periods(.). Standard is:

00.11.22.33.44.55.66.77.88.99.AA.BB.CC.DD.EE.FF

## Pre-shared Key | Security

The pre-shared key is a string of any characters up to a maximum length of 255 characters. The pre-shared key must only be entered if a connection with “IPsec Tunneling” to an external IPsec Gateway should be constructed and this remote station is expected as IKE policy “Pre-shared Key”.

## Policies



**For the selection of the policies please also observe the description of the IPsec configuration. The policies are delivered with the client software as standard. The policies can be modified insofar as the IPsec client should use special policies. For this click on [IPsec Configuration](#).**

## IKE Policy | Security

The IKE policy is selected from the listbox. (pre-configured policies: “Pre-shared Key” and “RSA-Signature”). All IKE policies which were created during the IPsec configuration are listed by name in the list box.

### automatic Mode

In this case the configuration of the IKE policy via the IPsec configuration can be eliminated.

### Pre-shared Key

This preconfigured policy can be used without PKI support. The same “pre-shared key” is used on both sides (see above “Pre-shared Key”).

### RSA Signature

This preconfigured policy can only be implemented with PKI support. The use of the RSA signature as additional strengthened authentication is only useful when using a smart card or a soft certificate.

## IPsec Policy | Security

The IPsec policy is selected from the listbox. (pre-configured policies: “ESP - 3DES - MD5”). All IPsec policies which were created during the IPsec configuration are listed by name in the list box.

### automatic Mode

In this case the configuration of the IKE policy via the IPsec configuration can be eliminated.

### ESP - 3DES - MD5

Should this preconfigured IPsec policy be selected, the same policy with its suggestions must be valid for all users. This means that the same suggestions for the policies must be provided on both the client and server side.

## Exchange Mode | Security

The exchange mode specifies the manner in which the Internet key exchange should take place. Two different methods are available, the main mode, also identity protection mode, and the aggressive mode. The methods differ in the number of messages and their encoding (see **IPsec Functionality**).



### Main Mode

In the main mode (standard setting) six messages are sent via the control channel, whereby the last two, which contain the user ID, the certificate, the signature and if applicable a hash value, are encoded – therefore also “Identity Protection Mode”.

### Aggressive Mode

In the aggressive mode only three messages are sent without encoding through the control channel.



*Corresponding to the security modulus IPsec detailed safety settings can also be undertaken.*

## IKE ID Type | Security

With native IPsec outgoing and incoming connections are differentiated. The value which the initiator has selected for an outgoing connection must be selected at the remote station as ID for incoming connections. The following ID types can be selected:

- IP address
- Fully Qualified Domain Name
- Fully Qualified Username
- IP subnet address
- ASN1 Distinguished Name
- ASN1 group name
- String for group identification

### IKE ID | Security

The value which the IPsec-initiator has selected for an outgoing connection must be selected at the remote station as ID for incoming connections.

The associated ID must be entered as a string according to the ID type.

## Advanced



*The settings in this parameter field are dependent on the Network Access Server of the respective remote station. In order to obtain additional information, consult your system administrator or your Internet Service Provider.*

### Deny incoming connections

This feature is checked in the default setting and for that reason no connection to this computer may be established from a computer within the connected network.

If this check mark is removed, a connection, initiated by a different computer, may be set up and the remote side may access the computer.



Please note that it is only sensible to remove this check mark if the computer is accessed by a defined remote side, i.e. from the corporate network. Otherwise, removing this check mark annihilates the protection of the firewall's stateful inspection technology. This means, that everybody within the network has the possibility to access the computer via the Client Software.

### Permit IP Broadcast

You decide with this parameter whether the client software should allow the transmission of IP broadcasts. IP broadcasts are used for example if a LAN client (such as the client software) searches for a file server in the network. In the case of the client the network would be a remote LAN, on which the client is connected.

IP broadcasts are disabled if the field is not clicked on (standard).

You must permit IP broadcasts if you are using DHCP in order to be able to request an IP address from the destination system.

### NetBIOS over IP

This parameter removes a filter which disables Microsoft NetBIOS frames. This is always purposeful if you, for example, use Microsoft networking via the client.

This filter is set in the standard setting, i.e. the check button is not marked with a check so that Microsoft NetBIOS frames are disabled so that they do not unnecessarily burden the data traffic. If you mark the check button with a check, then NetBIOS frames over IP is allowed.

### Prioritize Voice over IP (VoIP)

Should this client be used for communication with Voice over IP, then this function should be activated in order to send and receive the speech data without delays or distortions.

### MAC Address

The MAC address is the address of the network adapter in LAN. It can be used for the purpose of identification (DHCP). It is an address with 6 hexadecimal numbers which are separated by periods(.).

The standard address is 00.00.00.00.00.00



Please consult your Internet provider or your system administrator about this parameter.

## Pre-authentication



*This configuration field is only important for the communication media “LAN” or “Wi-Fi” or if an external dialer is used or the profile was configured for the automatic media detection. The type of authentication required before the tunnel construction depends on the respective network.*

*Please observe in the Wi-Fi that the connection via a Hotspot operator is subject to charges and you must agree to the terms and conditions of the Hotspot operator when the connection should be established. Also observe the descriptions of the **Basic Settings** and the **Communication Medium**.*



### EAP Authentication

If the client needs to authenticate with EAP (Extensible Authentication Protocol), then this function must be activated. It has the effect that for this profile the EAP configuration must be used in the monitor menu under “EAP Options”.

Please observe that the EAP configuration in the monitor menu is valid for all profiles and must be actively switched on if this link-specific setting should be effective.

EAP is then used if an Access Point is used for the wireless LAN which is capable of 802.1x and demands a corresponding authentication.

However, EAP can also be used if the client wants to have access by means of a router to another network segment of the company network.

EAP generally prevents an unauthorized user from logging into LAN via the hardware interface.

After configuration of the EAP a status display must appear in the graphics field of the monitor. Should this not be the case then the EAP configuration must be actively switched on in the monitor menu. The EAP can be restored by means of a double click on the EAP symbol. Subsequently the EAP negotiation reoccurs.



For this also see the description **Secure-Client-Monitor**.

### HTTP Authentication

This function must be activated for the automatic HTTP authentication on the Access Point (Hotspot).

In this way a further configuration field is added in the profile settings, in which the authentication data can be entered. (For this click on HTTP Logon)



In the event of a link with the connection type Wi-Fi, the **HTTP Logon** is not connected!



Instead the activation of this function has the effect that for this profile the authentication data from the Wi-Fi settings in the monitor menu are used.



For this observe the description **Wi-Fi and Hotspot Logon**.



## VPN Tunneling



These parameters are only important if a tunnel should be constructed between the client and the VPN Gateway, i.e. the destination system supports IPsec or L2TP. The respective settings are dependent on the Network Access Server of the destination system (VPN Gateway). If you are uncertain about the respective setting, please consult your system administrator or your Internet Service Provider.

### VPN Protocol

#### not used

No tunnel is constructed between the client and the destination system.

#### L2TP

You specify with this switch whether the L2TP protocol (layer 2 tunneling protocol) should be used. Using this protocol you can additionally switch either the security mode **L2Sec** or **IPsec**. When using the security mode IPsec with L2TP refer to the description **IPsec over L2TP**.



#### IPsec-Tunneling

Should IPsec tunneling as VPN protocol be selected, then the native IPsec connection will be established to a pure IPsec Gateway without a layer 2 tunnel (L2TP).



**When using native IPsec observe the description of the IPsec Configuration and the description IPsec Functionality.**

### Connection to pure IPsec Gateways



*In the selection of IPsec Tunneling you will be advised that the following settings are automatically made in the security configuration field:*

Security mode = IPsec

IKE policy = automatic mode

IPsec Policy = automatic mode

Exchange mode = main mode

*These automatically made settings can also be modified according to the requirements of the IPsec Gateway. (For this, click on **Security**.) Moreover the following should be observed for the usage of IPsec tunneling:*

*The parameters IKE ID type and IKE ID are faded into the configuration field Security for configuration. Corresponding to the specifications from the remote station the automatically made setting “specified from remote station” can be changed as IKE policy to pre-shared key or RSA signature (certificate). If the remote station expects pre-shared key, then the code must be entered in the field. (The pre-shared key must in this case be identical for all clients.)*

*IP addresses and DNS server are assigned using the protocol IKE config mode (Draft 2) (currently compatible only against Cisco). All previous WAN interfaces can be used for the NAS dial-up. (Click on **IPsec Address Assignment**.)*

*Should IPsec tunneling be used, then the authentication occurs in the standard setting of the Enterprise Client via extended authentication (XAUTH protocol, draft 6). [Extended Authentication can be switched off in the **Advanced IPsec Options** configuration field.] For this the following parameters must be set:*

VPN User ID = Username of the IPsec user

VPN Password = Password of the IPsec user

Use VPN User ID and Password from = optional  
(see below)

*With IPsec tunneling DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background, in case this is supported by the remote station. With DPD the client checks in specified intervals whether the remote station is still active. In the case of inactive remote stations an automatic disconnection occurs. The usage of NAT Traversal occurs automatically with the IPsec client and is always necessary when a device with network address translation is used on the remote side.*

### VPN User ID

You obtain the user names for the VPN Gateway from your system administrator. The name may be up to 255 characters long.

### VPN Password

You obtain the password for the VPN Gateway from your system administrator. The password may be up to 128 characters long.

## VPN Suffix

The “VPN Suffix” facilitates the creation of groups in Secure Enterprise Management (SEM). The central administrator may configure an environment variable for the “VPN Suffix” or the “VPN User ID”, e.g. %userdomain% or %username%, respectively. This variable is then automatically used by the Client as a “VPN Suffix”.

The user ID for VPN tunneling is made up of “VPN User ID” plus “VPN Suffix”. However the user only has to enter the “VPN User ID”. Based on the VPN suffix, the gateway recognizes which group the user belongs to.

### Environment Variable USERNAME

The user’s USERNAME variable will be used as the VPN Suffix if the string %USERNAME% is entered in the profile’s “VPN Suffix” field. However, if this environment variable is not set then the contents of the profile setting “VPN Suffix” field will be used unaltered.

## Tunnel Secret

This is a password which is needed for the tunnel construction. The tunnel will be constructed only if this password agrees with VPN Gateway and the VPN client. The password may be up to 16 characters long.

## Gateway (Tunnel Endpoint)

The address of the Gateway must be entered at this location. You will obtain it from your administrator either as an IP address or as a name string.

### IP address

If the Gateway is equipped with a fixed official IP address, the IP address can be entered.

### Name string

If the Gateway obtains alternating IP addresses from an Internet Service Provider, then the name string is entered here. It involves thereby the DNS name of the Gateway, which was stored in the DynDNS Service Provider.

In the same syntax, a second Gateway can be entered, separated from the first with a semicolon.

### Separate IPsec Gateway for Enterprise Clients

Should a L2TP tunnel be constructed, then this is the endpoint of the L2TP tunnel.

Should IPsec over L2TP be used, thus both a layer 3 and a layer 2 tunnel be constructed, then this is the endpoint for both tunnels, insofar as no connection should be established to a separate IPsec Gateway with the layer 3 tunnel.

Should a separate Gateway be used for IPsec, then the IP address entered here is the tunnel endpoint for the L2TP tunnel and the tunnel endpoint or the address of the IPsec Gateway will be entered in the **Advanced IPsec Options** configuration field.

## VPN Tunnel Authentication Data

The following entries can be read out and used as access data for a VPN:

### Configuration

This means that VPN user name and VPN password from this configuration field are used for VPN authentication.

### Certificate (email)

This means that instead of VPN user name and VPN password the e-mail entry of the certificate is used.

### Certificate (common name)

This means that instead of VPN user name and VPN password the user entry of the certificate is used.

### Certificate (Serial number)

This means that instead of VPN user name and VPN password the serial number of the certificate is used.

### Certificate field (Universal Principal Name, UPN)

This means that instead of “User Name” and “Password”, the Universal Principal Name (Registered-Name@Domain-Name) is used, assuming that the attribute is present in the certificate.



Please keep in mind that this also applies for the usage of **Extended Authentication** with IPsec connections.



For this purpose, compare the above description **Connection to pure IPsec Gateways** and the description of extended authentication in the configuration field **Advanced IPsec Options**. (For this, click here.)



For this purpose observe the description of **Certificates**.



## Advanced IPsec Options



With the usage of the security mode IPsec the configuration field is displayed. With these parameters, settings for a client-server connection can be established in the case of usage of native IPsec and IPsec over L2TP. If IPsec over L2TP is used, then a different destination address can be given here for the layer 3 IPsec tunnel than for the layer 2 L2TP tunnel, so that a proprietary IPsec Gateway can be used which doesn't originate from NCP.

### Disable DPD (Dead Peer Detection)

DPD can be deactivated with this function..

DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background, insofar as the destination gateway supports this. The IPsec client uses DPD in order to check at routine intervals, which can be set in seconds, whether the remote station is still active. If this is not the case, then an automatic disconnection occurs.



With DPD (Dead Peer Detection) the VPN Gateway active (according to the defined time interval) is "pinged" and the tunnel deactivated (independent of the actual data transfer) if no reply is received from the gateway or the timeout has expired (independent of data traffic).

### Destination Address IPsec Gateway

In the case of connections with IPsec over L2TP separate destination addresses to the respective Gateways can be given for the layer 3 and the layer 2 tunnels. At this point the endpoint of the layer 3 tunnel or the destination address of the IPsec Gateway can be entered. The tunnel endpoint (destination) for the layer 2 tunnel is entered in the configuration field **VPN Tunneling**. (For this, click here.)

Should no separate destination address for the IPsec Gateway be entered here, then the tunnel endpoint (destination) will also be used for the IPsec Gateway, which must be entered in any case.

In the case of connections with native IPsec this option is grayed out, since the tunnel endpoint (destination) from the configuration field "tunnel parameters" is used as the destination address for the IPsec Gateway.

The extended authentication can only be used for connections of the Enterprise Client with IPsec native and is activated for this tunnel protocol as standard. It can be deactivated in this configuration field.

### Extended Authentication (XAUTH)

In order to be able to natively use extended authentication (XAUTH protocol, draft 6) with IPsec, it must be supported by IPsec Gateway. If XAUTH is not supported by Gateway, then it must be deactivated here, since otherwise no connection will be made.

If XAUTH is supported by Gateway, then the extended authentication (XAUTH) remains activated. In addition to the pre-shared key, the following parameters from the configuration field "tunnel parameters" are then still used for authentication:

#### VPN Username

User name of the IPsec user. The name may be up to 255 characters long.

#### VPN Password

Password of the IPsec user. The password may be up to 128 characters long.

The VPN user name and VPN password are entered in the configuration field **VPN Tunneling**, where alternatively it can also be specified that they be read out from a certificate configuration. (For this, click here.)

### Standard IPsec / UDP Encapsulation

The alternative use of standard IPsec (port 500) and UDP encapsulation is possible.

With UDP encapsulation only the Port 4500 must be activated on the external Firewall (different with NAT Traversal or UDP 500 with ESP). If the UDP encapsulation is used, then the port can be freely selected.

Port 4500 is set as default for IPsec with UDP; Port 500 for IPsec without UDP.

The NCP Gateway detects automatically UDP encapsulation.

### VPN Path Finder

The prerequisite of the VPN Path Finder is a NCP gateway (>=V.8) as remote destination. There, an alternative port has to be configured in the VPN / IPsec settings.

As soon as default IPsec via port 500 is not possible or UDP encapsulation via a freely configurable port is not possible, the VPN Path Finder automatically uses the alternative connection protocol TCP encapsulation with SSL Header (Port 443).

This is important if only HTTPS port 443 is available for the client and a connection solely based on IPsec is not possible, this is the case, for example, in a hotel or at a hotspot.



If a connection is established using VPN Path Finder (i.e. using port 443), the monitor displays this via an icon in its **state display** (below and to the right of the HQ / gateway).

If a proxy server is to be placed ahead for this connection, it can be set and configurations can be made in the configuration menu under “Proxy for VPN Path Finder”.

### Anti-replay Protection

The delayed arrival of IP packets could imply that these are corrupt; if this function (based on RFC 2406) is enabled, such packets are discarded.

## IPsec Address Assignment



*With the usage of native IPsec, the IP addresses of the client can be assigned in various manners which can be configured here.*

### 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.



[This standard setting is automatically used for the Enterprise Client if the tunnel protocol IPsec is selected, as described in **VPN Tunneling**].

All previous WAN interfaces can be used for the NAS dial-up.

With “IPsec Tunneling” **DPD** (Dead Peer Detection) and **NAT-T** (NAT Traversal) are automatically executed in the background, in case this is supported by the remote station. With **DPD** the client checks in specified intervals whether the remote station is still active. In the case of inactive remote stations an automatic disconnection occurs.

The usage of **NAT Traversal** occurs automatically with the client and is always necessary when a device with network address translation is used from the side of the destination system.

#### 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 for the Entry Client]

#### manual IP address

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

#### DHCP using 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.

## Split Tunneling



*In this folder you can define the IP network(s) to which the client should communicate via tunneling.*

*If you have made no entries, data will be transferred only in tunnel mode.*

*If an entry exists, data will be transferred in tunnel mode only to the networks which are entered in this folder. Other connections will be established directly via the selected dial-in medium. In this case you can toggle between your company's VPN gateway using tunneling and the internet without tunneling.*

By clicking on the button "New", you can enter IP addresses and net masks in the window which appears.

### 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.

If you do not make an entry in this list all IP packets will be sent via the VPN tunnel.

Note: Be sure that IP addresses entered in this field are not the same subnet as the gateway.

### Remote IP Net Masks

In this window enter the address(es) and net-mask(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.

### Full Local Network Enclosure Mode

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

## HA Support



The parameters of this configuration field is only important for the Enterprise Client, since only Enterprise Client supports the high availability services.

*This parameter field is only important if the destination system is an HA server (high availability), which forwards the tunnel emergence depending on the configuration to the VPN Gateways. Moreover this configuration field only appears in the profile settings if a VPN protocol for the connection to the remote station has been selected.*

### DVE Functionality

A DVE (Dynamic VPN Endpoint) can be used for Load balancing or as Backup of a Virtual Private Network with two VPN-Gateways. With DVE it is assured depending on the configuration in HA manager that no bottleneck occurs in the tunnel construction. Depending on the load emergence HA server will change between the tunnel endpoints of the VPN Gateway for the tunnel construction. (For this purpose observe the description **HA-Function**).

### Activation

The DVE functionality is switched on with this parameter (Dynamic Virtual Endpoint). Thereupon the tunnel endpoint (destination) is hidden in the Tunnel parameter configuration field. Instead of this, the IP address of the HA server (first / second HA server) must be specified. Depending on the configuration, this HA server guides the tunnel further on one of the VPN Gateways.

### First / Second HA Server

Enter the IP address of the HA server here. You obtain the address from your system administrator.

### DVE Secret

Enter the password for the connection of the DVE client to the destination system (DVE server) here. You obtain it from your system administrator.

### Use last assigned Gateway

If “IP Address from Pool” is selected on the gateway and an HA-Server with load balancing is being used, the Client should always be connected to the Gateway that last assigned it an IP Address from its IP Pool. To assure this, please activate this feature.

Note: Only use this function if an HA server is used with load balancing. It must not be used together with HA systems in failsafe mode.

## DNS / Management



*In this parameter field the server which was automatically assigned through the PPP negotiation can be replaced by an alternative server. For this purpose the DNS mode must be set in the network settings of the operating system.*



*In accordance with your requirements you can assign one or two DNS or WINS servers. The primary server is used as the default server. If no alternative server has been defined, then the server assigned via PPP will be used.*

### DNS Server

#### First / Second DNS Server

The initially entered DNS server is used instead of the server which was established by the PPP negotiation. The second DNS server serves as backup DNS server.

### Domain Name

This is the Domain Name which is otherwise transferred per DHCP to the system in the network settings.



**This parameter is only important for the Enterprise Client. The Enterprise Client can be centrally managed and can obtain automatic updates from the management system. Normally the contact to the management system is established by NCP using a VPN Gateway. This IP address is only necessary if the remote station is not an NCP Gateway.**

### Management Server

The IP address of the NCP Secure Enterprise Manager SEM (precisely: Enterprise Management Server) must be entered here, if the Gateway of the remote station is not an NCP Gateway and thus no NCP management server can be automatically disclosed using the PPP negotiation.



Should the IP address of a management server be entered, although the remote station is an NCP Gateway, then the management server of the NCP Secure Enterprise Management, which is disclosed during the PPP negotiation between NCP Gateway and NCP Secure Client, is used independently of the entered IP address. The entered IP address is ignored in this case.

## Certificate Check



The entries which must be present in a certificate of the remote station (secure server) can be set in this configuration field for each link profile on the Secure Client.

For this purpose observe the description of **Certificates**.

### Incoming Certificate's Subject

All user attributes, insofar as known and using wild cards, can be input as entries of the user certificate of the remote station (server). For this purpose compare which entries are listed for the user in the monitor connection menu under “display incoming certificate”.

Use the abbreviations of the attribute types. The abbreviations of the attribute types for certificate entries have the following meaning:

```

cn      = Common Name
s       = Surname
g       = Givenname
t       = Title
o       = Organisation
ou      = Organisation Unit
c       = Country
st      = State
l       = Location
email   = E-mail
sn      = Serialnumber in the subject's
         area
  
```

(This is not the certificate serial number!)

*Example::*

```
cn=VPNGW*, o=NCP, c=de
```

The common name of the Security Server is only checked up to the Wild card “\*”. All following positions can be arbitrary, for example 1 - 5 as numbering. In this case, the organization unit must always be NCP and the country Germany.

### Incoming Certificate's Issuer

All issuer attributes, insofar as known and using wild cards, can be input as entries of the user certificate of the remote station (server). For this purpose compare which entries are listed for the issuer in the monitor connection menu under “display incoming certificate”. The abbreviation of the attribute types for certificate entries have the same meaning as above under “Users of the incoming certificate”.

*Example:*

```
cn=NCP engineering GmbH
```

The common name of the issuer is checked here.

### Issuer's Certificate Fingerprint



In order to prevent an unauthorized party, who imitates the trustworthy CA, from using a faked issuer certificate, the fingerprint of the issuer, insofar as known, can additionally be entered.

### Use SHA1 Fingerprint

The algorithm for the creation of the fingerprint can be either MD5 (Message Digit 5) or SHA1 (Secure Hash Algorithm 1).

## Link Firewall



The link Firewall can be used for all network adapters and for RAS connections. The activated Firewall is presented in the graphical interface of the client or in the task bar as symbol (Wall with arrow).

(For this also see **Secure-Client-Monitor**.)

The fundamental task of a Firewall is to prevent risks from other or external networks (Internet) from expanding into one's own network. For this reason a Firewall is also installed on the crossover between company network and the Internet. It checks all incoming and outgoing data packets and decides on the basis of previously set configurations whether or not a data packet can pass.

The Firewall to be activated here works under the principle of stateful

inspection. Stateful inspection is the Firewall technology with the currently highest possible safety standard for Internet connections and thus the company network. Security is assured in two aspects. On the one hand unauthorized access to data and resources in the central data network is prevented. On the other hand it monitors the respective status of all existing Internet connections as control instance. Moreover the stateful inspection Firewall detects whether a connection has opened "daughter connections", such as with FTP or Netmeeting, whose packets also must be forwarded. A stateful inspection connection constitutes a direct conduit for the communication partner, which may only be used for data exchange corresponding to the agreed upon rules.



(For this also see **Secure-Client-Personal-Firewall**)

### Stateful Inspection

#### off

The security mechanisms of the Firewall are not used.

#### always

The safety mechanisms of the Firewall are always used, i.e. the PC is protected against unauthorized access even when no connection is established.

#### when connected

The PC is not vulnerable if a connection exists.

### Only Tunneling 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. Any other data traffic will be rejected.

### In Combination with Microsoft's RAS Dialer only Tunneling Permitted

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



Please observe that when using the Link Firewall the complete IP traffic is accordingly locked - even if the client monitor is not started. This can have the result that for example a printer which is addressed in the local network via IP doesn't react.



## IPsec Configuration of the Secure Client



The most important settings for an IPsec connection are made in the configuration fields of the profile settings and were already described above. It involves the following parameters,

which can be activated with a mouse click in the corresponding configuration field (the configuration field is given in parenthesis behind the parameter):

**IPsec Tunneling** (VPN Tunneling)

**Exchange Mode** (Security)

**IKE ID-Type and IKE ID** (Security)

**IKE Policy and IPsec Policy** (Security)\*

**Gateway (Tunnel Endpoint)** (VPN Tunneling)

**Destination Address IPsec Gateway** (Advanced IPsec Options)

**Assignment of the Private IP Address** (IPsec Address Assignment)

**Access Data for XAUTH** (VPN Tunneling)

**Deactivate DPD** (Advanced IPsec Options)

**IPsec Compression** (IPsec Configuration)\*

**PFS / DH Group** (IPsec Configuration)\*

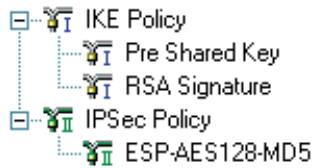
*\* Only parameters  
which are designated  
with a star\* can be set*

As a rule the IPsec configuration is only needed if an adaptation of the IKE or IPsec policy must be made because no policy from the client suggestion list suits the IPsec configuration on the Gateway. Insofar as the standard setting of the policy “specified by remote station” is used, the client suggests a list of policies, from which merely one suggestion must fit the policy configuration on the Gateway

in order to be able to establish a correct IPsec connection to the Gateway. This suggestion list as well as an explanation of it and most of the aforementioned parameters can be found in the document **IPsec Functionality and Configuration**.



The IPsec configuration is opened with the menu item “IPsec” in the monitor configuration menu.



In the window which opens you will find two configuration nodes, one to the IKE policy and one to the IPsec policy. The policies “Pre-shared key” and “RSA signature” lie

beneath the IKE policy. You may select these instead of the **standard setting “automatic mode”**. (Observe for this the **guidelines about the proposal lists for IKE Policies**). You will find the policy “ESP-3DES-MD5” under the IPsec policy. You may also select these instead of the standard setting “automatic mode”. (Observe for this the **guidelines about the proposal lists for IPsec Policies**).

You do not yet require an IPsec configuration to change this standard setting! It can be made in the respective configuration field! (see previous page)

In compliance with the **IKE Policy** the authentication negotiation between client (IPsec initiator) and remote station is carried out and an encoded control channel is established between them.

It is determined in compliance with the **IPsec Policy** how the usage data should be processed in accordance with the IPsec protocol.

## Editing the Policies

In order to edit the (standard) values within the policies, i.e. to set or modify parameters to conform to the connection requirements of the remote station, select the policy with the mouse, whose values you would like to change – the buttons for operation then become active.

### Configure

In order to modify a policy, select the name of the policy whose values you would like to change with the mouse and click on “configure”. Then open the corresponding configuration field.

### New Entry

If you would like to create a policy, select one of the policies and click on “new entry.” The new policy will be created. All parameters are set to standard values except for the name.

### Copy

In order to copy the parameter settings of a policy which has already been defined, mark the policy to be copied and click on “copy”. Thereupon the parameter field will be opened. Now change the name and then click on Ok. The new policy has now been created. The parameter values are identical to those that were copied except for the name.

### Delete

If you want to delete a policy from the configuration tree, select it and click on “delete.” The policy is thus permanently deleted from the IPsec configuration.

### Close

When you close the IPsec field, you return to the monitor. The data will remain as they were configured.

### Saving

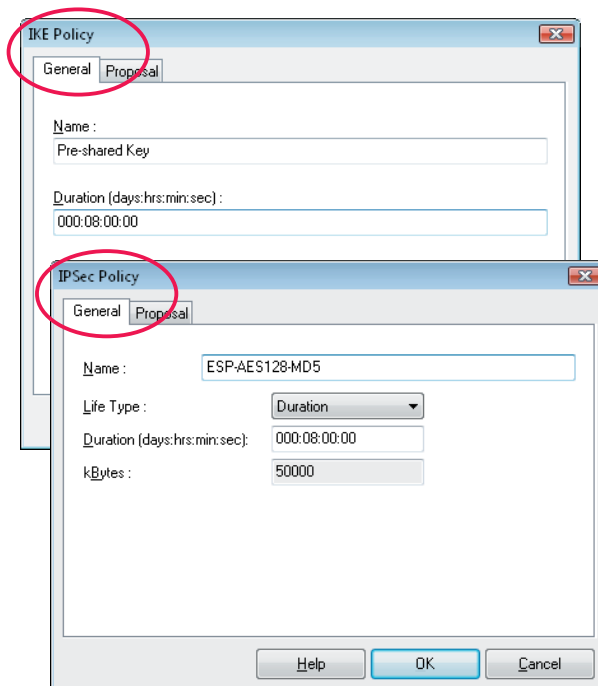
Every change in the IPsec configuration is saved with “OK”.

## Policy Lifetime / General



When you open the settings of a policy on Enterprise Client, initially the general parameters are displayed, which have validity for all suggestions of this policy. These include the policy name - in the standard setting “pre-shared key” or “RSA signature” – under which the proposals are collected, but also the settings for the validity of this policy.

## General



The policy validity is determined on the Enterprise Client in the configuration window General specifically per individual policy, distinguished also according to IKE and IPsec policy. (Illustration above)

### Life Type

Specifies which criteria are used to determine the type of code validity, according to duration, transmitted kBytes or **both**. With every new SA negotiation the counter is reset. (For this see SA negotiation and policies in the PDF file IPsec Functionality and Policies.)

### Duration

The quantity of the kBytes or the size of the time span can be specifically set.

### kBytes

The quantity of the kBytes or the size of the time span can be specifically set.

### Name

Give this policy a name. Using this name the policy can be selected with Enterprise Client in the configuration field Security.

On the Entry Client the policy name is entered directly in the respective policy configuration (see below).

## IKE Policy / Proposals



These parameters in this field apply to phase 1 of the Internet Key Exchange (IKE) with which the control channel for the SA negotiation is established.

The IKE policies which you configure here are listed for selection.

Two IKE policies which are delivered with the software as standard differ functionally: “Pre-shared Key” and “RSA-Signature”. Every policy lists at least one proposal for authentication and encoding algorithm (IKE policy, authentication, encoding), i.e. a policy can consist of various proposals.

The same policies including the associated proposals should apply for all users. This means the same proposals should be available for the policies both on the client side and on the central system.

### Authentication | IKE Policy

Before the control channel for the phase-1 negotiation (IKE Security Association) can be established, an authentication must have occurred on both sides.

#### Pre-shared Key

The joint Pre-shared key is used for mutual authentication.

The pre-shared key is specified on Enterprise Client under **Security**.

#### RSA Signature

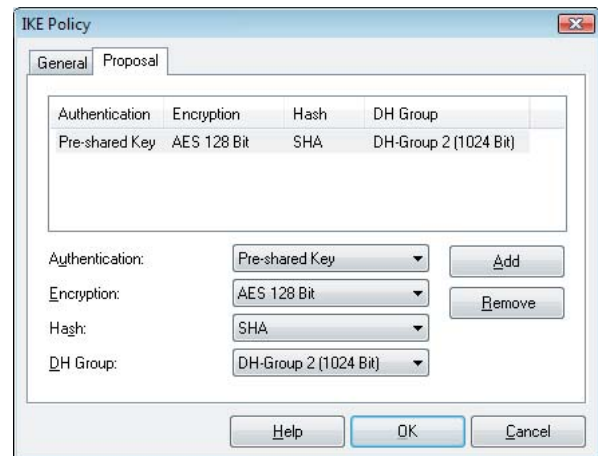
For mutual authentication a certificate is used that you have configured for the “Extended Authentication” (XAUTH). In Main Mode the certificate will be additionally encrypted. This is only possible with PKI support of the system.

### Encryption | IKE Policy

The symmetrical encoding of the messages 5 and 6 in the control channel is carried out according to one of the optional encoding algorithms, insofar as the main mode (identity protection mode) is navigated.

There is a choice of: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

The exchange mode in the configuration field **Security** is set on the Enterprise Client.



Ill. above: IKE policy on the Enterprise Client.

### Hash | IKE Policy

Mode how the hash value is formed using the ID or the certificate of the messages in the control channel.

There is a choice of: MD5 (Message Digest, Version 5), SHA (Secure Hash Algorithm), SHA 256, SHA 384 and SHA 512 Bit

### DH Group | IKE Policy

The selection of the available Diffie-Hellman groups determines the degree of security of the Internet Key Exchange in the control channel (phase 1) after the later symmetrical key is created. The higher the DH group the more secure the Key Exchange.

## IPsec Policy / Proposals



The parameters in this field apply to phase 2 of the SA negotiation.

The IPsec policies which you configure here are listed for selection for the internally created SPD.

Only an IPsec policy with ESP (Encapsulating Security Payload) is delivered with the software as standard. Since the IPsec mode with AH security is unsuitable for flexible remote access, only one IPsec policy with ESP protocol is delivered. Every IPsec policy lists at least one proposal for IPsec protocol and authentication, i.e. a policy can consist of various proposals.

The same policies including the associated proposals should apply for all users. This means the same proposals should be available for the policies both on the client side and on the central system.

### Protocol | IPsec Policy

The firmly set standard value is ESP.

#### IPsec Compression

The data transmission with IPsec can be compressed in the same way as with a transfer without IPsec. This allows for a maximum three-fold increase of the throughput. After selection of "IPsec compression", a choice between LZS and deflate compression can be made as transformation.



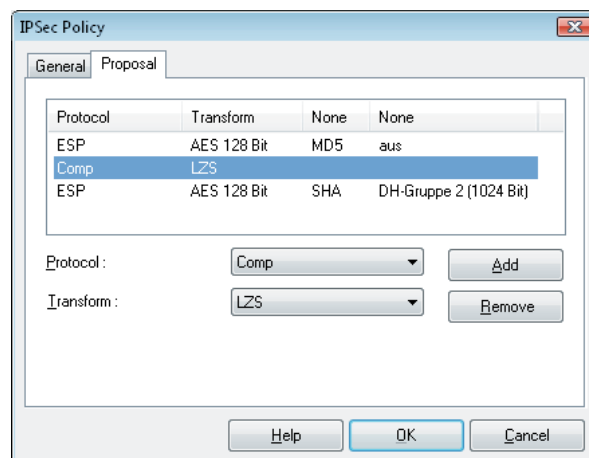
The IPsec compression does not become active for the proposals of the IPsec policy of the client until the proposal list is concluded with the proposal of compression.

### Transformation / Encryption | IPsec Policy

For the security protocol ESP it can be defined here how the encryption with ESP should occur.

There is a choice of the same encryption algorithms as for layer 2: none (NULL) DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

After selection of "IPsec compression", a choice between LZS and deflate compression can be made as transformation.



Ill. above: IPsec Policy on the Enterprise Client with IPsec compression. The compression applies in this example for the proposal ESP- AES 128 Bit - MD5. The following proposal of the policy is sent uncompressed.

### Authentication | IPsec Policy

For the security protocol ESP the mode of the authentication can be specially set. There is a choice of: MD5 (Message Digest, Version 5), SHA (Secure Hash Algorithm), SHA 256, SHA 384 and SHA 512 Bit.

### PFS / DH Group

The selection of one of the available Diffie Hellman groups determines that a complete key exchange (PFS) should additionally occur in phase 2 with the SA negotiation.

The standard setting is "none". The following DH groups are possible:

DH-Group 1 (768 Bit)  
DH-Group 2 (1024 Bit)  
DH-Group 5 (1536 Bit)



# Index

Anti-replay Protection . . . . .	26	IPsec Policy   Security . . . . .	19
Activation . . . . .	29	Issuer's Certificat Fingerprint . . . . .	31
Alternative Phone Numbers . . . . .	10	Keep IPAddress when connecting manually . . . . .	15
APN . . . . .	13	MAC Address . . . . .	21
Assignment of the Private IP Address . . . . .	27	Management Server . . . . .	30
Authentication   IKE Policy . . . . .	36	Modem Init. String . . . . .	12
Authentication   IPsec Policy . . . . .	37	Modem Type . . . . .	12
Automatic Media Detection /		Multilink Threshold . . . . .	16
Configuration Instruction . . . . .	9	Negotiate Callback . . . . .	17
Baud Rate . . . . .	12	NetBIOS over IP . . . . .	21
Callback Method . . . . .	17	Only Tunneling Permitted . . . . .	32
Callback Phone Number . . . . .	17	OTP Token . . . . .	16
Certificate Configuration . . . . .	18	Password   HTTP Logon . . . . .	14
Com Port . . . . .	12	Password . . . . .	10
Communication Medium . . . . .	7	Permit IP Broadcast . . . . .	21
Compression . . . . .	16	PFS / DH Group . . . . .	37
Connect at Boot . . . . .	15	PPP Multilink . . . . .	16
Connection Mode . . . . .	15	PPTP Endpoint . . . . .	11
Connection to pure IPsec Gateways . . . . .	23	Pre-shared Key   Security . . . . .	19
Default Profile after System Reboot . . . . .	8	Prioritize Voice over IP (VoIP) . . . . .	21
Deny incoming connections . . . . .	21	Profil Name . . . . .	7
Destination Address IPsec Gateway . . . . .	25	Profile for Automatic Media Detection . . . . .	9
Destination Phone Number . . . . .	10	Protocol   IPsec Policy . . . . .	37
DH Group   IKE Policy . . . . .	36	RAS Script File . . . . .	11
Dial Prefix . . . . .	12	Release Com Port . . . . .	12
Dial-up Number . . . . .	13	Remote IP Net Masks . . . . .	28
Disable DPD (Dead Peer Detection) . . . . .	25	Remote Networks . . . . .	28
DNS Server . . . . .	30	Save Password   HTTP Logon . . . . .	14
Domain Name . . . . .	30	Save Password . . . . .	10
DVE Functionality . . . . .	29	Security Mode . . . . .	18
DVE Secret . . . . .	29	SIM PIN . . . . .	13
EAP Authentication . . . . .	22	Standard IPsec / UDP Encapsulation . . . . .	25
Encryption (L2Sec) . . . . .	19	Stateful Inspection . . . . .	32
Encryption   IKE Policy . . . . .	36	Static Key  Security . . . . .	19
Exchange Mode   Security . . . . .	20	Timeout Direction . . . . .	15
Extended Authentication (XAUTH) . . . . .	25	Transformation / Encryption   IPsec Policy . . . . .	37
First / Second HA Server . . . . .	29	Tunnel Secret . . . . .	24
Full Local Network Enclosure Mode . . . . .	28	Use last assigned Gateway . . . . .	29
Gateway (Tunnel Endpoint) . . . . .	24	Use SHA1 Fingerprint . . . . .	31
Hash   IKE Policy . . . . .	36	Use Windows Dial-up Networking . . . . .	8
HTTP Authentication Script   HTTP Logon . . . . .	14	User ID   HTTP Logon . . . . .	14
HTTP Authentication . . . . .	22	User ID, Password . . . . .	13
IKE ID   Security . . . . .	20	Username . . . . .	10
IKE ID Type   Security . . . . .	20	VPN Password . . . . .	23
IKE Policy   Security . . . . .	19	VPN Path Finder . . . . .	25
In Combination with Microsoft's RAS Dialer		VPN Protocol . . . . .	23
only Tunneling Permitted . . . . .	32	VPN Suffix . . . . .	24
Inactivity Timeout . . . . .	15	VPN Tunnel Authentication Data . . . . .	24
Incoming Certificate's Issuer . . . . .	31	VPN User ID . . . . .	23
Incoming Certificate's Subject . . . . .	31		



## Seamless Roaming

**Disconnect the logical VPN tunnel when the connection is broken**

**Maintain mobile wireless network connection with Seamless Roaming**