D-Link SecuriWall VPN Client

SECURIWALL™

Manual

D-Link®
Building Networks for People

Contents

Client Monitor

Once you have installed the D-Link SecuriWall VPN Client the graphical interface referred to as the Monitor should appear automatically on the PC's screen. To manually display the Monitor click:

Start → Programs → D-Link SecuriWall VPN Client → D-Link VPN Client Monitor

The Client Monitor will be loaded and displayed on the screen or in the task bar.

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

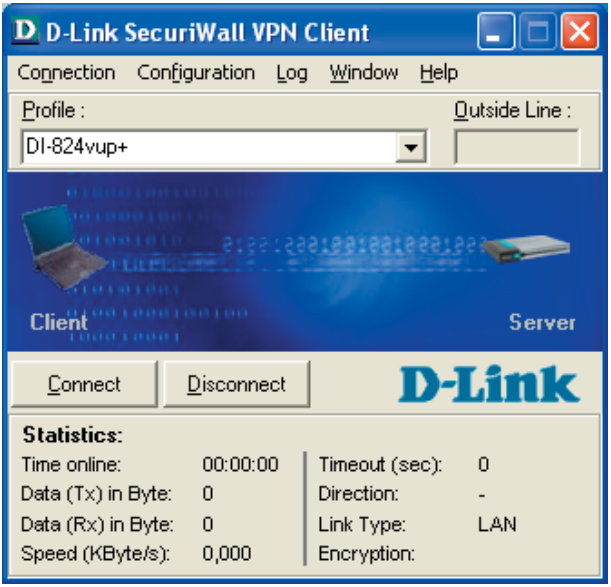
The Client Monitor serves 3 important purposes:

- to display the current communications status
- for selection of communication media
- for profile settings and associated destination and security parameters

Using the Client Monitor

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

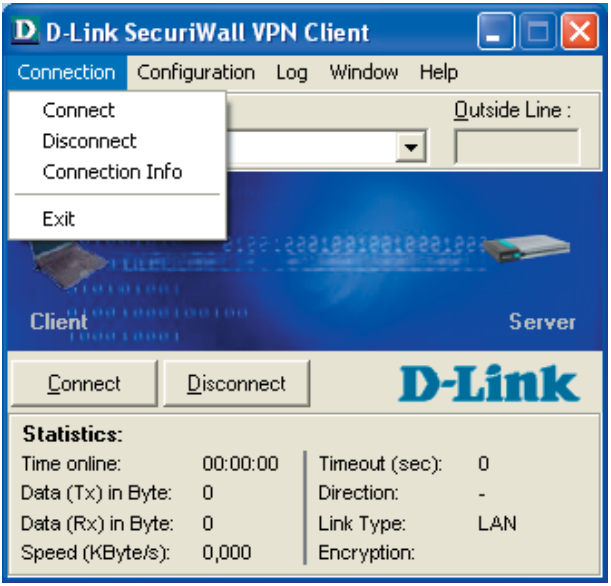
- Connection [Menu]
- Configuration [Menu]
- Log
- Window [Menu]
- Help



Connection

This pull-down menu “Connection” contains the following menu items:

- Connect
- Disconnect
- Connection Info
- Exit



Connect

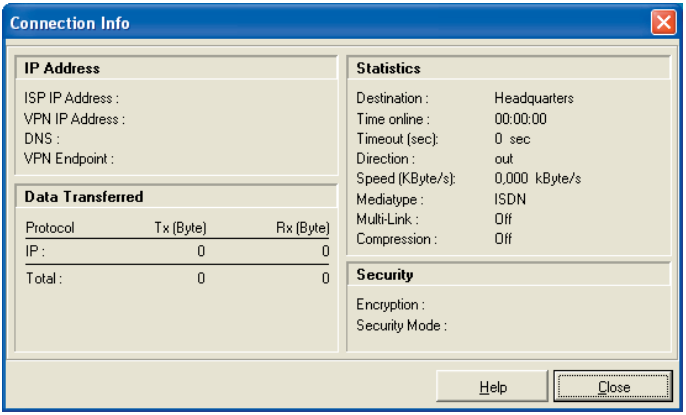
This command is used to initiate a connection. A connection can only be made if a profile has been properly defined and selected in the profile settings (see → Profile Settings). The selected profile is displayed in the “profile” field of the monitor. Or click the right mouse button to initiate the connection.

Disconnect

A connection can be terminated manually by clicking on “Disconnect” in the Connection pull-down Menu or by clicking the right mouse button.

Connection Info

To display the link/connection statistics, select “Connection Info” from the menu. The window also displays the type of security features being used as well as the IP addresses that have been assigned between the VPN 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 VPN Client.

Exit

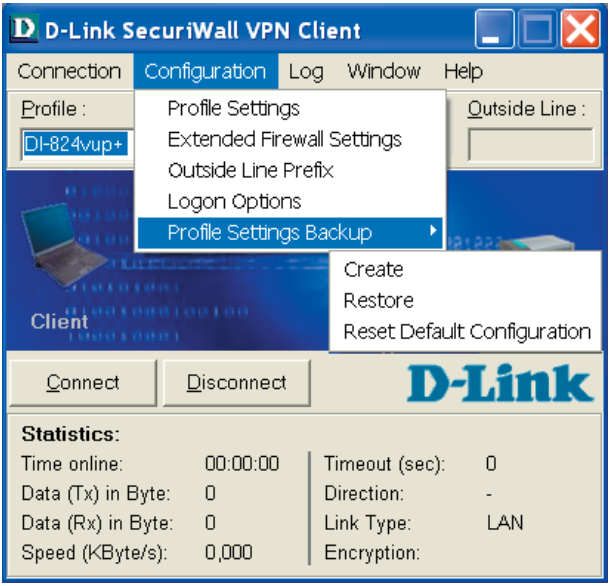
To close the Monitor, click on Exit. You will be prompted to close any existing connections, or you can leave the connections open; however, the monitor (the user interface) will be shutdown and the status of the link will no longer be visible.

Configuration

This pull-down menu “Configuration” contains the following menu items:

- Profile Settings
- Extended Firewall Settings
- Outside Line Prefix
- Logon Options
- Profile Settings Backup

Once the VPN Client is installed and the profile parameters are properly configured, a connection to the destination can be made.



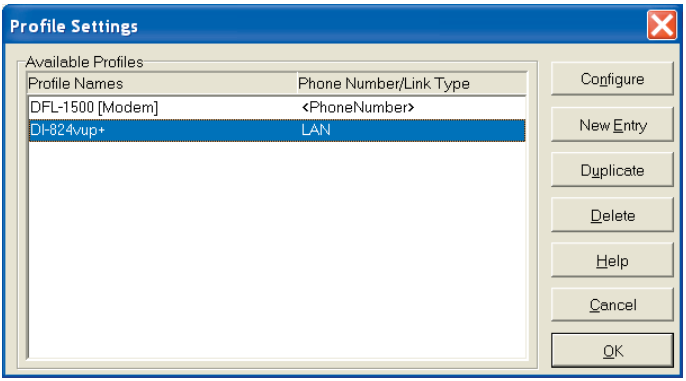
Profile Settings

Entries in the Profile Settings

A very important feature of the Client Monitor is the menu item Profile Settings, which provides the basis for defining and configuring profiles. Upon clicking this menu item in the Client Monitor menu, the profiles are opened displaying an overview of the defined profiles and their respective telephone numbers.

Note: After installing the VPN Client for the first time it will be necessary to define a profile for your requirements under the profile settings. For this purpose there is a “Configuration Assistant”, which will walk you through the configuration steps of defining a “profile”. In order to define a profile select “New Entry” in the profile settings. Once the profile has been completed it may be modified or re-configured at any time according to requirements.

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

At this point you should be able to establish a connection to your selected profile. However if necessary you can make additional parameter changes by selecting the desired profile and then clicking the “Configure” button in the profile settings.

Configure - Profile

If you want to change any 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:

- General
- Dial-Up Network
- IPSec General Settings
- Identities
- IP Address Assignment
- Remote Networks
- Firewall Settings

OK - Profile

In order to conclude the definition of a profile and to store all associated parameters click on the “OK” button in the respective folder and then click on “OK” in the main folder of the profile settings in order to select the profile which you desire to communicate with. The selected profile will now be used for a connection, either manually (via “Connection” and “Connect”) or automatically (launched by an application).

Duplicate - Profile

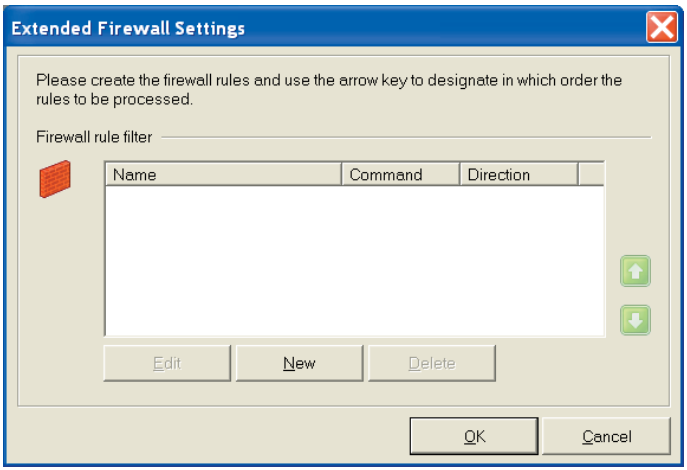
You may want to use an existing profile for a basis when defining a new profile. In order to do so, first select the profile to be duplicated and then click on the “Duplicate” button. Upon doing so the “General” parameter folder will open. Because each profile must have a unique name, you must now enter 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.

Delete - Profile

If you want to delete a profile from your profile settings select the appropriate profile and then click on the “Delete” button. Upon executing “Delete” the profile will be permanently deleted from the profile settings.

Extended Firewall Settings

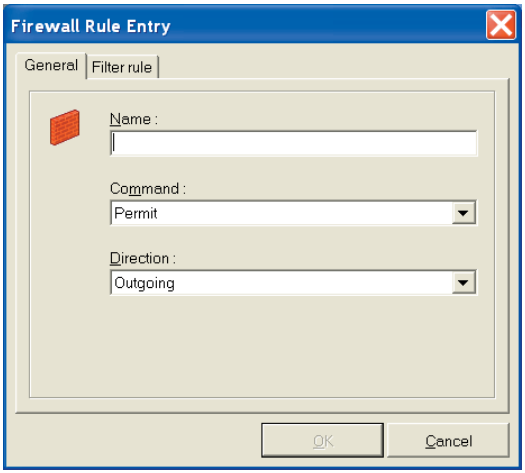
Use the filter editor to define filters to be applied to inbound and outbound traffic. Filters can be set for protoclos, network- and/or host IP addresses.



By clicking “New” you get the folders “General” and “Filter rule”.

General

Command / State



IPSec → is used for IP packets with addresses from the defined range, the IPSec security services are implemented.

Permit → IP packets with addresses from the defined range are allowed through without implementing the SPD.

Deny → all IP packets with addresses from the defined range will be discarded.

Disabled → this SPD is turned off and is not implemented for IPSec; it is not necessary to delete it.

Direction [Firewall]

Incoming = the setting “incoming” is chosen when Control Channel establishment and the IKE negotiation is initiated from the other side. (see → Examples and Explanations, IKE Modes)

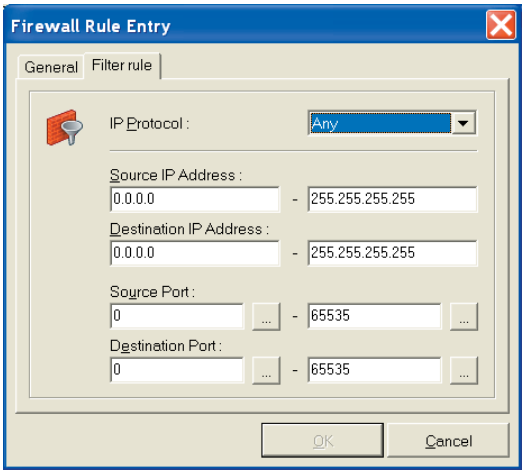
Outgoing = Control Channel establishment and IKE negotiation is initiated from this side.

Please note that establishment of the Control Channel must be authorized on the other side. In other words it must be configured as “incoming” on the other side.

The standard client configuration is “outgoing” so that for communication (with static SPD) it must be set as “incoming” on the server.

Filter rule

The filter portion or selector of an SPD entry consists of IP- and port addresses. If values of an IP packet agree with the values from the SPD entry selector portion, then it is determination is made in the Status as to what should next be done with this IP packet.



IP Protocol

This is the transport protocol, which can be ICMP, TCP, or UDP. One of these offered protocols can be selected or (any) can be used.

Source IP Address

This can be a host IP address or an address range.

Destination IP Address

This can be a host IP address or an address range.

Source Port

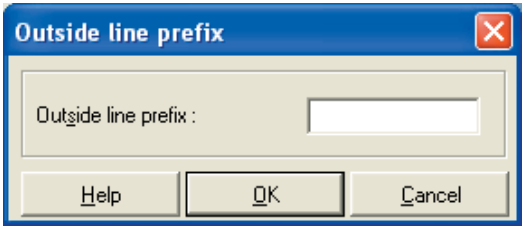
These can be either individual TCP or UDP port numbers or a range of port numbers. You determine the port numbers with allocated service by using the Select button [...].

Destination Port

These can be either individual TCP or UDP port numbers or a range of port numbers. You determine the port numbers with allocated service by using the Select button [...].

Outside Line Prefix

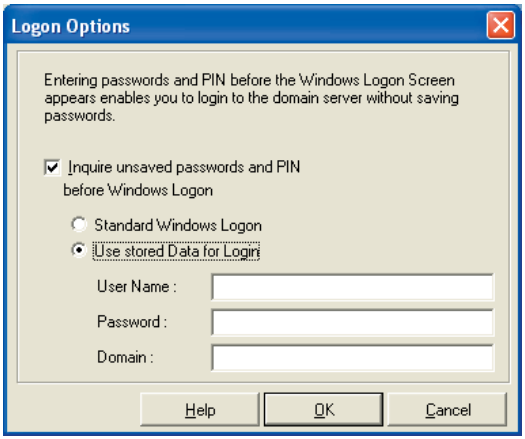
A special number or dial prefix is generally required when communicating via a PBX in order to acquire an outside line. This could, for example, be a 0 (zero) or 9 or any other number(s) depending on the PBX in use at your location.



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) in the profile settings, particularly when travelling.

Logon Options

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 profile settings.



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.

Note: You must reboot you PC after making any changes to the "Logon Options".

Profile Settings Backup

If a profile 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

When clicking “Create” menu item a back-up is automatically made of the profile settings.

Restore

If a profile setting needs to be restored to a version that was saved with the back-up feature,- one click on “Restore”. This will replace the current profile setting with the last known back-up. Changes since the last back-up will be lost!

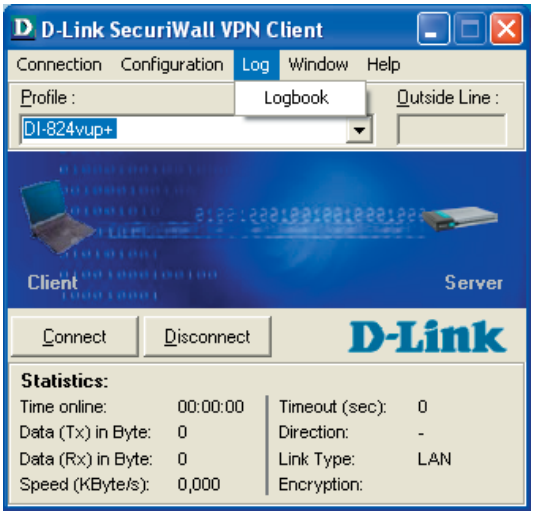
Reset Default Configuration

During the installation of the VPN Client a profile with default settings for the available VPN devices is automatically created. Selecting Reset Default Configuration will reset the configuration to these default values.

(To save individual configuration setting see “Profile Settings Backup”.)

Log

This feature automatically logs (records) all communication transactions (but not the data) going via the Client. This information may be valuable for troubleshooting problems or for analysis of your communication activities. The contents of the log are stored in memory and are accessible until such a time that you (re)boot your PC or until you click on the “Clear Screen” button. Alternatively, if required, the log can also be written (stored) to a file (see → Create File).

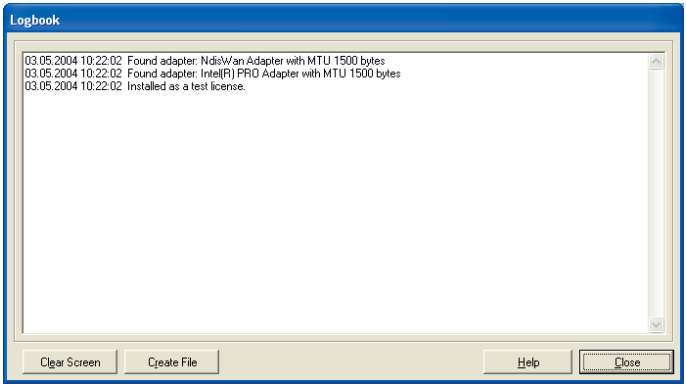


The log function automatically stores all actions of the Client for a period of seven days. Log files older than 7 online days will be automatically deleted. In the D-Link SecuriWall subdirectory (found in either Windows, or WINNT), there is a subdirectory called Log. This is where the log files are 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

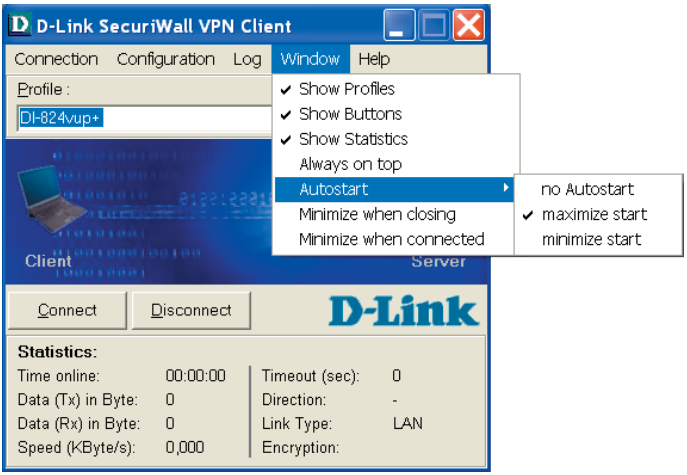
Clicking this button will delete the contents of the log screen and empty the buffers.

Close - Logbook

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

Window

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
- Always on top
- Autostart
- Minimize when closing
- Minimize when connected

Show Profile

When “Show Profiles” is activated the configured profiles 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.

Alternativly, 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

Click on “Always on Top” in order to activate or deactivate the display of the monitor. 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 VPN 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].

(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], and it appears as traffic light in the task bar, which displays the status of the connection. 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.

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

Minimize when connected

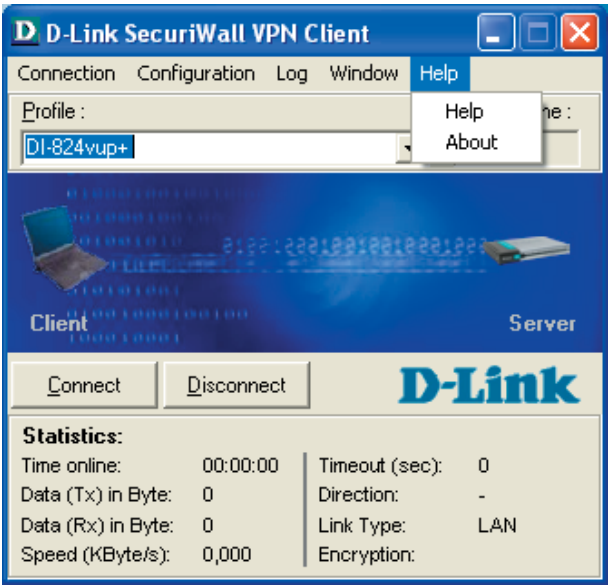
If this menu item is activated the monitor will be minimized when the connection is established successfully.

Help

Clicking on “Help” opens a window displaying a table of contents for all available help text.

About

Clicking on “About” opens a window displaying the Client version installed on your PC.



Configuration Parameters

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

Profile Settings

Upon clicking profile settings in the monitor menu, the list of profiles is opened and displays an overview of the defined profiles.

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

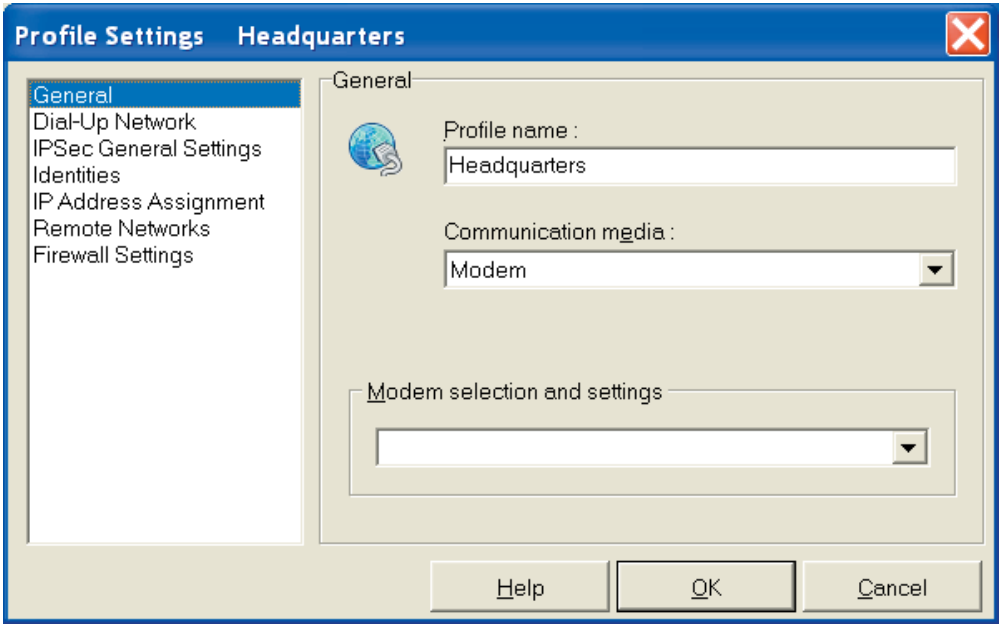
Parameters which specify the connection to the destinations, are found in the configuration folders (see → Profile Settings, Configure). Selecting an existing-, or creating a new profile entry opens the configuration folder. Within the configuration folder the connection parameters pretaining to this profile can be configured. The name of the destination appears in the titel bar.

- **General [Parameters]**
- **Dial-Up Network**
- **IPSec General Settings**
- **Identities**
- **IP Address Assignment**
- **Remote Networks**
- **Firewall Settings**

In the parameter folder “IPSec General Settings” there are two buttons needed to configure both IKE and IPSec policies:

- **Policy lifetimes**
- **Policy editor**

General [Parameters]



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

With the VPN Client you can define and configure numerous individual profiles, in accordance with your communication requirements.

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

To edit these default values, in order to fulfill the requirements of the destination, 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”.

Profile name

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

Communication media

You can select the communication media for communicating with individual profiles, provided that you have the required device installed on your PC and recognized by Windows.

ISDN

Hardware: ISDN device;

Network: ISDN;

Remote destination: appropriate ISDN support;

Modem

Hardware: Asynchronous modem (PCMCIA modem, GSM adapter) with COM Port support;

Network: PSTN (also GSM);

Remote destination: Modem or ISDN device with digital modem;

LAN (over IP)

Hardware: LAN adapter;

Networks: Ethernet or Token Ring based LAN;

xDSL (PPPoE) / PPPoE

Hardware: Ethernet adapter;

Networks: Broadband (e.g. ADSL);

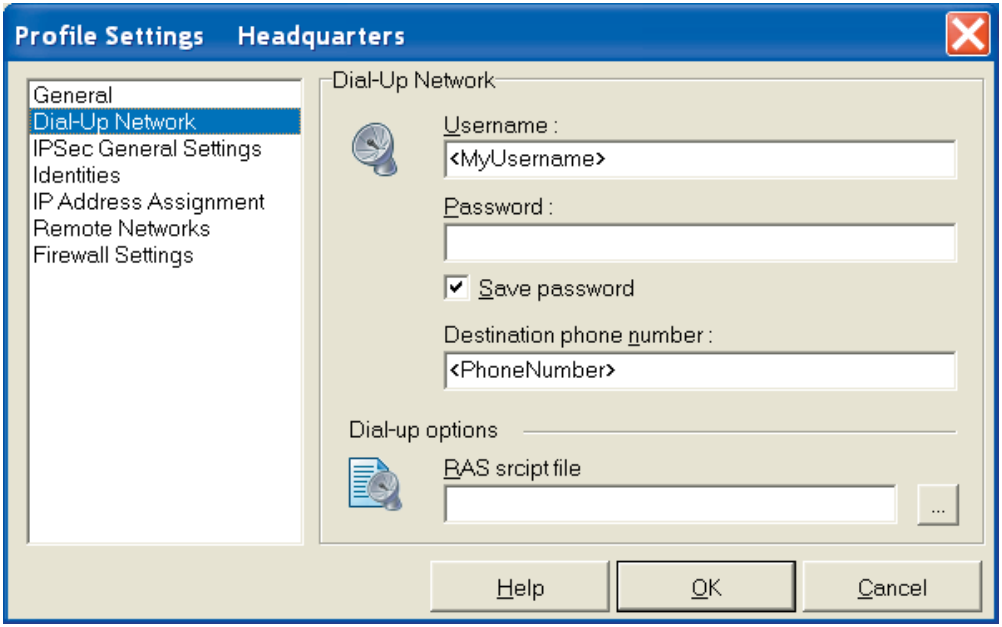
Remote destination: Access Router in the xDSL

Please note that the required hardware as well as the corresponding drivers must be installed according to the communication media you have selected.

Modem selection and settings

This parameter field is only displayed if your selected communication media is “Modem”. This field will view the modem(s) installed on your PC. Select the required modem. All other parameters for this communication media can be configured in the control panel of your PC.

Dial-Up Network



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.

Username [Dial-Up Network]

If the ISP requires a username it can be entered here.

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 256 characters. Normally the username will be assigned to you by your destination (e.g. your company Headquarters, User Help Desk, Internet Service Provider, etc.), because it must be supported and accepted by the NAS, RADIUS or LDAP server for authentication purposes.

Password [Dial-Up Network]

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

This parameter is used for identifying yourself to your Internet Service Provider (ISP) if the Internet is used. The password can include up to 256 characters. Normally the password will be assigned to you by your destination (e.g. your company Headquarters, User Help Desk, Internet Service Provider, etc.), because it must be supported and accepted by the NAS, 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).

Save password

If you wish the password to be stored and not be prompted for it everytime you wish to connect, enable “Save password”.

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

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

Destination phone number

You must define a phone number for those destinations using ISDN/PSTN/GSM otherwise the Client will not be able to dial up and establish a connection to the destination or ISP. The phone number must be entered exactly in the same manner as if you were dialing the number

from a telephone. You must enter any required prefixes, country codes, area codes, extensions, etc. etc.

In order to acquire an outside line when communicating via a PBX it is necessary to define an Outside Line Prefix (see → "Outside Line Prefix")

Example: Making a connection from Germany to UK:

Enter: 00 (gets you an international line when dialing from Germany)

Enter: 44 (this is the country code for United Kingdom)

Enter: 171 (prefix for London)

Enter: 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 profile 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 (:).

Note: A maximum of 30 digits can be entered in the Destination Phone Number field. The VPN Client supports a maximum of 8 alternate phone numbers.

Example: 00441711234567:00441719876543

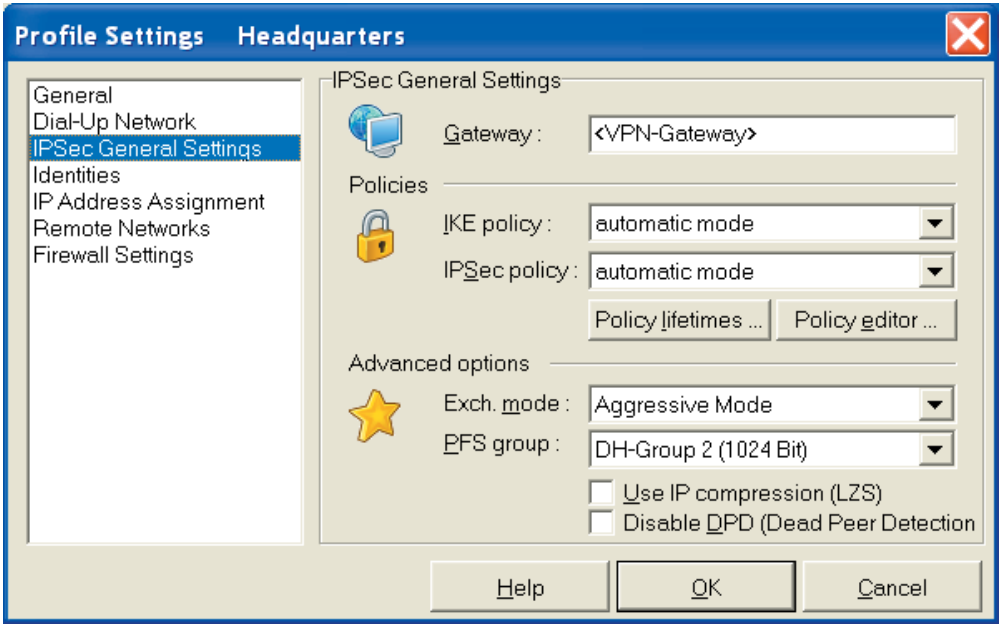
The first number is the primary Destination Phone Number and will always be dialed first. The second number is the Alternate Destination Phone Number and will be dialed when a connection to the primary number is not possible.

Important: This will only work if the protocol settings associated with alternate Destination Phone Number are the same as the primary Destination Phone Number.

RAS script file

Microsoft's RAS Dial-Up networking is to be used for dialing in to an ISP. When the access point requires a dial-up script the RAS script file including its path and name must be entered.

IPSec General Settings



Gateway

This is the IP address of the VPN 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.

IKE Policy

The IKE policy is selected from the list box. All IKE policies that you set up in the “IPSec Configuration” after clicking the button “Policy editor” are in the list box. The policies appear in the box with the name that you specified in the configuration.

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 destination.

Policy Name: When selecting the name of the pre-configured IKE policy the same pre-shared key must be used on both sides (see → Pre-shared key, Shared secret in the parameter folder “Identities”).

IPSec Policy

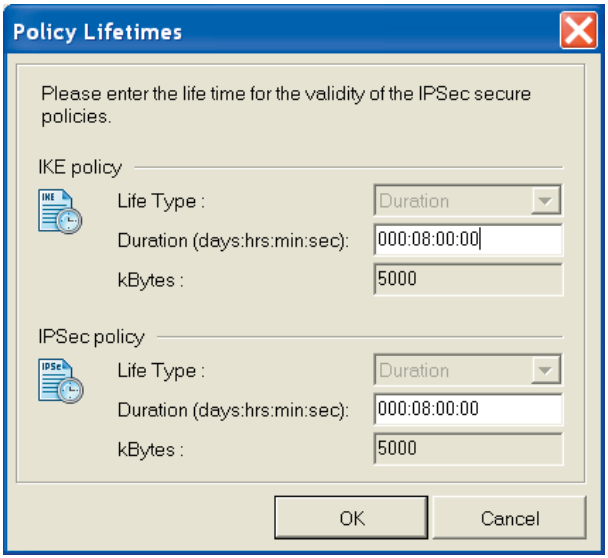
The IPSec policy is selected from the List box. All IPSec policies that you set up in the “IPSec Configuration” after clicking the button “Policy editor” are in the list box. The policies appear in the box with the name that you specified in the configuration.

automatic mode: In this case it is not necessary to configure the IPSec policy in the “IPSec Configuration”. It will be assigned by the destination.

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.

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

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

kBytes

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

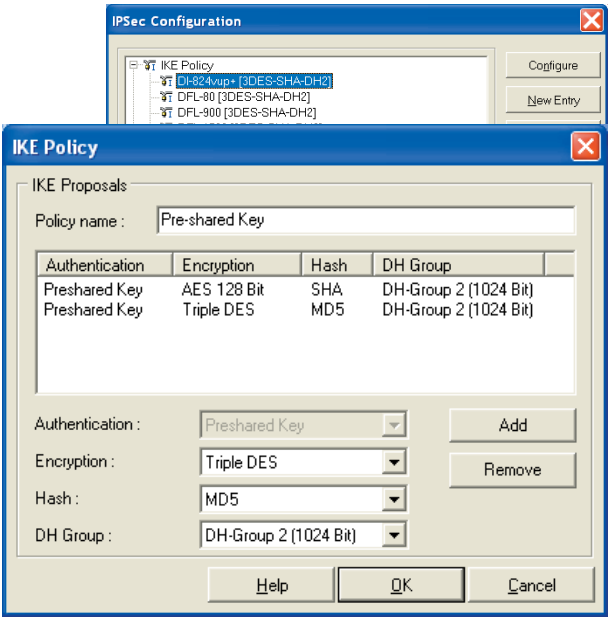
Policy editor

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 profile settings 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]
- 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 “Identities” (see → Pre-shared key, Shared secret).

Encryption [IKE Policy]

Symmetrical encryption of messages 5 and 6 in the control channel occurs according to one of the optional encryption algorithms if Main Mode (“Identity Protection Mode”) is used. Choices are DES, Triple DES, Blowfish, AES 128, AES 192, and AES 256.

Hash [IKE Policy]

This is mode that determines how the hash value over the ID is formed, or in other words this determines which hash algorithm is used in the IKE negotiation. Choices are: MD5 (Message Digest, version 5) and SHA (Secure Hash Algorithm)

DH Group [IKE Policy]

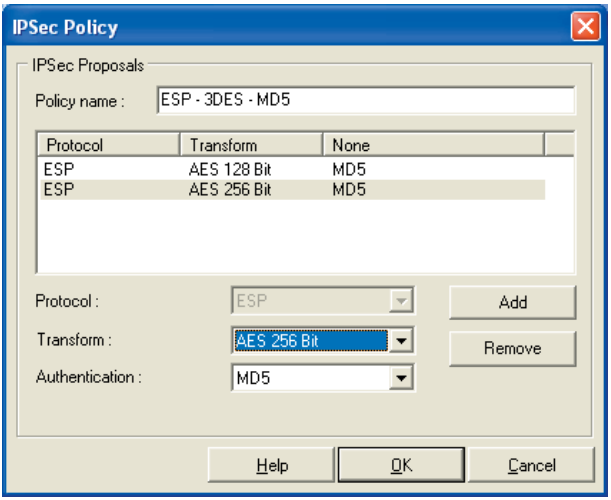
The selection of one of the offered Diffie Hellman groups determines the level of security for the key exchange in the control channel. Later a symmetrical key will be generated according to this selection. The higher the DH group the more secure the key exchange will be.

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]
- Transform [IPSec Policy]
- Authentication [IPSec Policy]

Policy Name [IPSec Policy]

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

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

Exchange mode

The Exchange Mode determines how the “Internet Key Exchange” should proceed. Two different modes are available; Main Mode also referred to as Identity Protection Mode and the Aggressive Mode. These modes are differentiated by the number of messages and by their encryption.

Main Mode: in Main Mode (standard setting) six messages are sent over the Control Channel and the last two messages are encrypted. The last two messages contain the username, the signature or a hash value. This is why it is also known as Identity Protection Mode.

Aggressive Mode: in Aggressive Mode only three messages are sent over the Control Channel and nothing is encrypted.

PFS group

With the selection of one of the offered Diffie Hellmann groups it is determined whether a complete Diffie Hellmann, (DH Group), key exchange (PFS, Perfect Forward Secrecy) should occur in Phase 2 in addition to the SA negotiation. The Standard is “none”.

Use IP compression

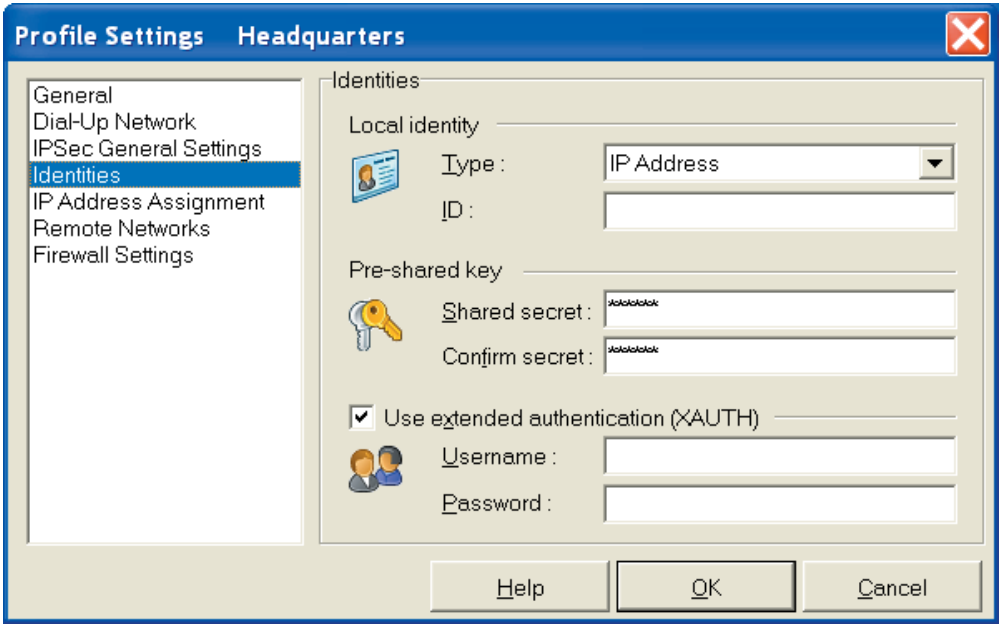
The data can be compressed in order to increase transmission rates. By enabeling compression the throughput can be increased to up 3 times that the regular transmissions without compression.

Disable DPD (Dead Peer Detection)

DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background if supported by the destination gateway. The IPSec client uses DPD to check, in regular intervals, whether the other side is still active. If the other side is inactive, then an automatic connection-disconnect occurs.

With this function you can disable DPD.

Identities



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

Type [Identities]

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
- Domain name
- User ID
- Subnet ID
- IP Address Range
- X.500 Distinguished name
- X.500 General Name
- Key ID

ID [Identities]

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.

Pre-shared Key

The pre-shared key is a string of the max. length of 255 characters. Any (alpha)numeric characters can be used. If the other side expects a pre-shared key during the IKE negotiation, then this key must be entered in the field "Shared secret".

Please confirm the shared secret in the field below. The same pre-shared (static) key must be used at both end points of the communication.

Use extended authentication (XAUTH)

The authentication for "IPSec Tunneling" can be dealt with utilizing extended authentication (XAUTH protocol, Draft 6). If "XAUTH" is to be used, and supported by the VPN gateway, enable "Use extended authentication (XAUTH)". In addition to pre-shared key, username and password can be defined:

Username = Username of the IPSec user

Password = Password of the IPSec user

Username [Identities]

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

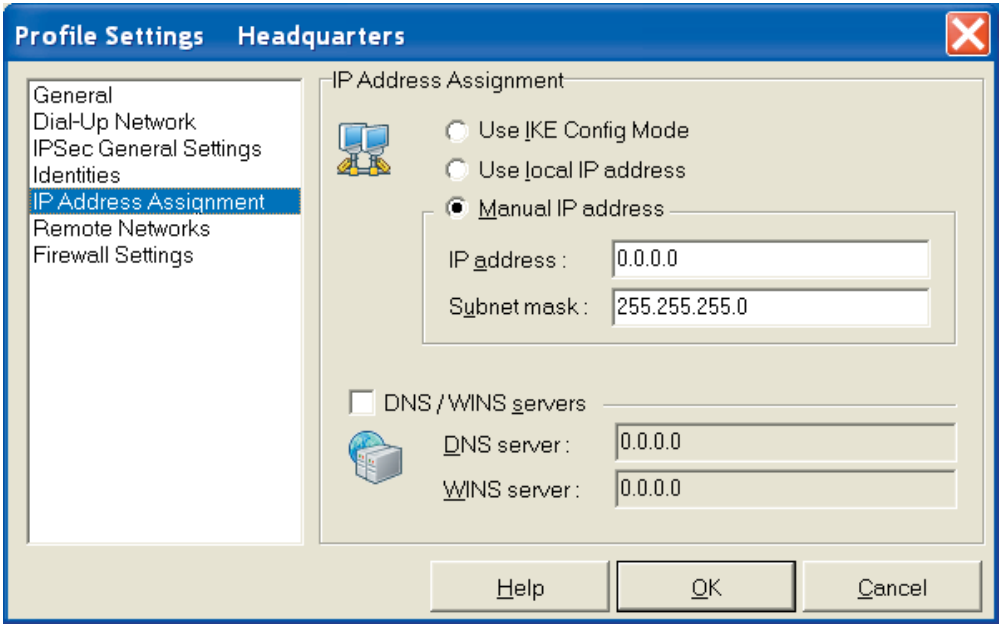
Note: This parameter pertains only to accessing the VPN gateway at the remote destination.

Password [Identities]

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

Note: This parameter pertains only to accessing the VPN gateway at the remote destination.

IP Address Assignment



Use IKE Config Mode

IP addresses and DNS servers are assigned via the IKE Config Mode protocol (Draft 2). All WAN interfaces can be used for the NAS dial-in.

DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background for "IPSec Tunneling" if supported by the destination gateway. The IPSec client uses DPD to check, in regular intervals, whether the other side is still active. If the other side is inactive, then an automatic connection-disconnect occurs. Using NAT Traversal is automatic with the IPSec client and is always necessary if network address translation is used on the side of the destination system device.

Use local IP address

Use the IP address currently assigned to your network adapter.

Manual IP address

This is the IP address of the workstation.

DNS / WINS servers

IKE Config Mode, if configured and available, enables dynamic assignment of client IP addresses, DNS / WINS server addresses and domain name.

Activating this function you can define an alternative DNS Server as opposed to using the one that is automatically assigned during the PPP negotiation to the NAS/ISP.

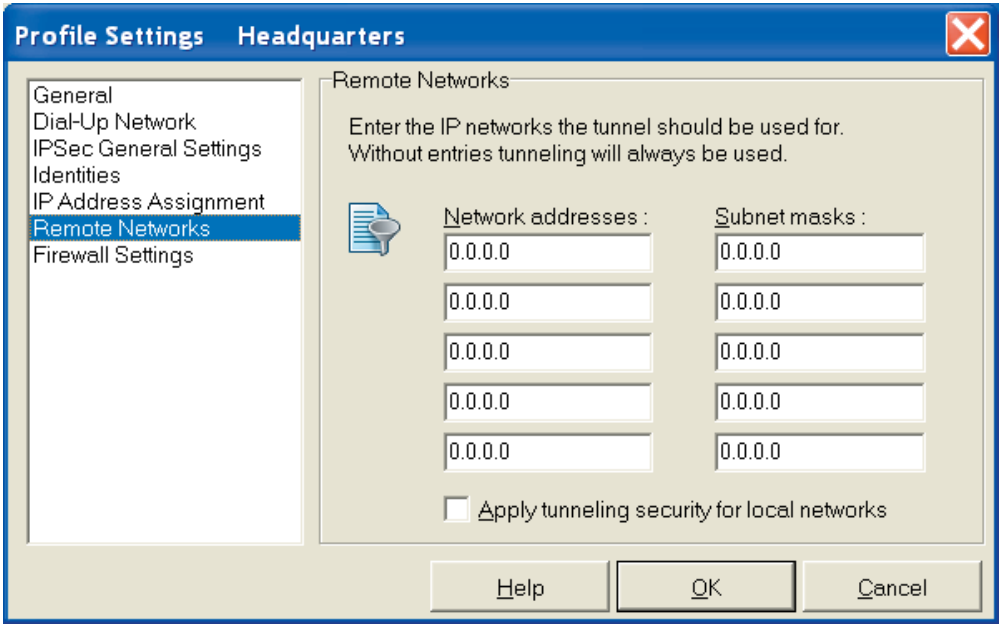
DNS server

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

WINS server

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

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".

Network addresses [Remote Networks]

In this window enter the address of the IP Network(s) that you want to reach via the VPN 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 VPN gateway.

Subnet masks

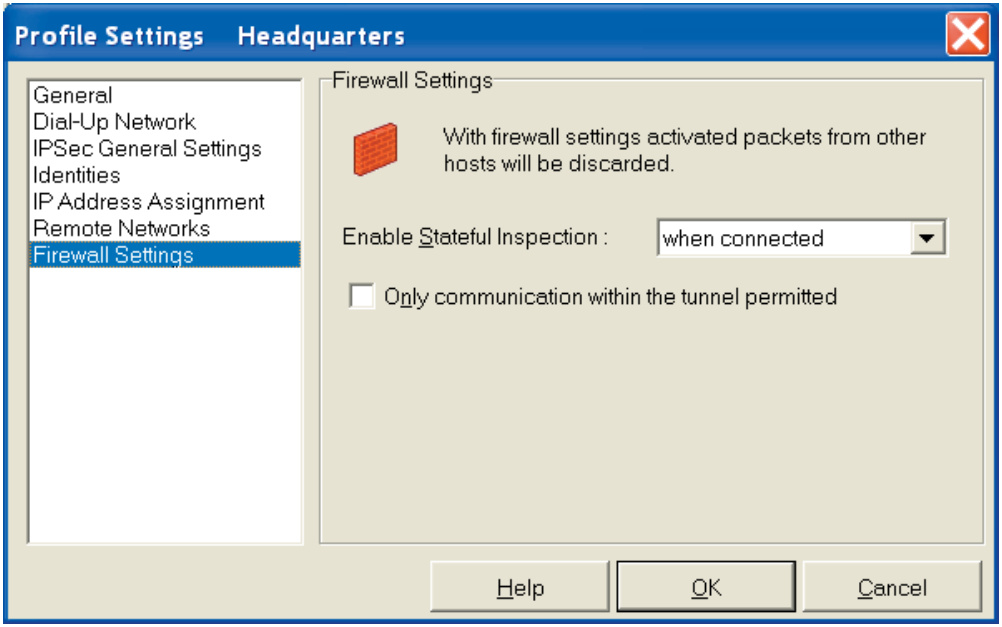
In this window enter the address(es) and netmask(s) of IP Network(s) that you want to reach via the VPN gateway. These addresses are available from your administrator.

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

Apply tunneling security for local networks

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

Firewall Settings



The “Firewall settings” 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 FTP or Netmeeting - 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.

Enable Stateful Inspection

off: The firewall's security mechanisms will not be used.

always: The firewall's security mechanisms will always be used, this means the PC is protected from unauthorized accesses even if no connection is established.

when connected: The PC is not vulnerable if a connection exists.

Only communication within the tunnel permitted: This function can also be switched on with activated firewall to additionally filter IP packets so that only VPN connections are possible.

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.

Establishing a Connection

Establishing a Connection to the destination system

In order to establish a VPN connection to the D-Link or other VPN Gateway, you must define the parameters in a configuration entry called a “Profile”. You can store several configurations each with unique username, passwords, VPN Gateways, connection methods as separate entries.

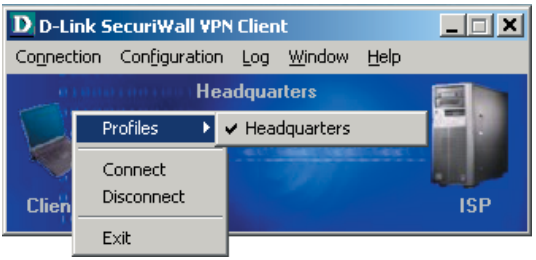
Click on “Configure - Profile Settings” in the menu bar to define a destination or profile entry, and the dialog box of the Profile Settings opens displaying the pre-configured profiles.

Provided the software is installed properly and the profile parameters are configured correctly a connection to the destination system can take place.

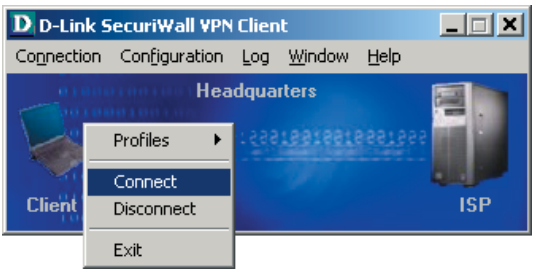
Connect

The monitor displays the connection status as explained in the following example where a connection is first created to an ISP, and then a VPN tunnel created to the D-Link SecuriWall appliance:

First step is to select a profile for a destination to connect to - click the right mouse button to display the menu, or select the profile name you wish to use.



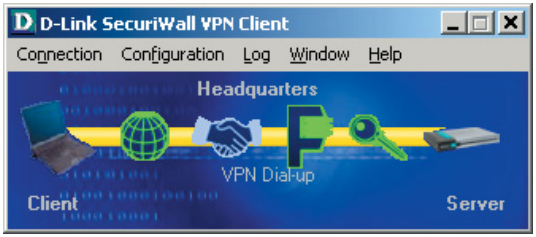
To then establish a connection click the right mouse button to display the menu and then select “Connect”.



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. The symbols change color as each phase is negotiated; the colors indicate the status:

light blue = link building stage
dark blue = stage passed
green = successfully negotiated stage

The different phases, if successfully negotiated are displayed by minimized symbols.



Upon a successful authenticated connection with the ISP/Network Access Server a tunnel is built indicated by a new yellow bar and the second “dial-up” to the VPN Gateway is started. Authentication now depends on what type of IKE-negotiation has been configured. One can use a Pre-shared key or (if supported) XAUTH. Contact your administrator for more details how to authenticate the VPN connection.

If the configuration of the profile is set to utilize compression, and this is supported by the destination VPN Gateway, you can configure compression as well.

If the last stage of the link built (here encryption) is successfully passed, the colour of the tunnel indicates this by changing to green.

Now a connection is established.

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

Client Logon

If the VPN 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 profile for the destination system to connect to and then click on the OK button.

Local logoff:

With a click on this button the link build is stopped.

Activate Domain Logon:

With this option a safe WAN domain logon is possible, even if prior logoffs were not executed correctly. The logon takes several seconds. This function is not necessary if the PC was shutdown correctly and mapped drivers were disconnected properly.

Icons, illustrating the link being built in the same way as described above under "Connect", again depict the following phases until the connection is established.

Passwords and Usernames

The password (see → Dial-Up Network, Password) is used for identifying yourself to the remote Network Access System (NAS) when establishing a connection to your destination, or alternatively to your Internet Service Provider (ISP) if you are communicating across the Internet. The password may consist up to 256 characters. Normally the password will be assigned to you by your destination (e.g. your company Headquarters, User Help Desk, Internet Service Provider, etc.), because it must be supported and accepted by the NAS or ISP, for authentication purposes.

Upon entering your password all characters will be displayed as an asterisk (*) in order to keep them from being seen by others. Therefore it is necessary to be very careful that you enter your password exactly the way in which it was assigned to you (particularly pay attention to the use of upper- and lowercase characters).

If you do not wish to enter in the password needed to establish a connection to the NAS or ISP with every connection attempt; you may select "Save password". This then allows the VPN Client to store the password needed to establish a connection to the NAS/ISP; not the password needed to establish a VPN connection.

However, this does mean that when leaving the computer unattended, someone else can establish a connection; so one should exercise caution when selecting this possibility.

Username for NAS Dial-Up

The "Username"of the Dial-Up Network must always be entered in the configuration of the profile. Without this Username a dial-up to the NAS is impossible (see → Dial-Up Network)

VPN User ID and VPN Password

User ID and Password for a dial-up to the VPN Gateway (see → VPN Tunneling) can be entered completely in the configuration of the profile. They are saved for VPN dial-up even when (re)booting your PC. If they are not entered in the configuration, you are prompted to enter them in a dialog for VPN dial-up.

Disconnect

With the function “Disconnect” a connection can be terminated.

If the connection is terminated, the color of connection line changes until it disappears and the connection to the SecuriWall or VPN Gateway has been terminated.

Disconnect (the Monitor)

Using the “Disconnect” button in the Monitor can also terminate the connection. Depending on which option is selected, the behavior of the Monitor can be controlled as well. It is possible for the Monitor to be minimized when disconnected.

Please note that closing the Monitor does not automatically terminate the connection! This means that costs can still be incurred because the link is still up and active; despite the monitor having been closed; you will however, be warned for this event.

Upon selecting “No” you are indicating that the link is to stay active, but do not wish to monitor the status of the connection. In order to terminate the connection correctly you would have to restart the Monitor!

LIMITED WARRANTY

D-Link provides this limited warranty for its product only to the person or entity who originally purchased the product from D-Link or its authorized reseller or distributor.

Limited Software Warranty:

D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original delivery of the Software for a period of ninety (90) days ("Warranty Period"), if the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. DLink's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. The Warranty Period shall extend for an additional ninety (90) days after any replacement Software is delivered. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the nonconforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

What You Must Do For Warranty Service:

Registration Card. The Registration Card provided at the back of this manual must be completed and returned to an Authorized D-Link Service Office for each D-Link product within ninety (90) days after the product is purchased and/or licensed. The addresses/telephone/fax list of the nearest Authorized D-Link Service Office is provided in the back of this manual. FAILURE TO PROPERLY COMPLETE AND TIMELY RETURN THE REGISTRATION CARD MAY AFFECT THE WARRANTY FOR THIS PRODUCT.

Submitting A Claim. Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office. The claim must include a written description of the Software nonconformance in sufficient detail to allow D-Link to confirm the same. The original product owner must provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.

What Is Not Covered:

This limited warranty provided by D-Link does not cover:

Products that have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or License Key has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; and Any hardware, software, firmware or other products or services provided by anyone other than D-Link.

Disclaimer of Other Warranties:
EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability
TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT.

GOVERNING LAW
This Limited Warranty shall be governed by the laws of the Federal Republic of Germany. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may. not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

Trademarks

Copyright Statement

International Offices

D-Link U.S.A
17595 Mt. Herrmann Street
Fountain Valley, CA. 92708
TEL: 714-885-6000
Fax 866-743-4905
URL: www.dlink.com

Canada
2180 Winston Park Drive
Oakville, Ontario, L6H 5W1
Canada
TEL: 1-905-8295033
FAX: 1-905-8295223
URL: www.dlink.ca

Europe (U. K.)
4th Floor, Merit House
Edgware Road, Colindale
London NW9 5AB
U.K.
TEL: 44-20-8731-5555
FAX: 44-20-8731-5511
URL: www.dlink.co.uk

Germany
Schwalbacher Strasse 74
D-65760 Eschborn
Germany
TEL: 49-6196-77990
FAX: 49-6196-7799300
URL: www.dlink.de

France
Le Florilege #.2, Allee de la Fresnerie
78330 Fontenay le Fleury
France
TEL: 33-1-30238688
FAX: 33-1-30238689
URL: www.dlink-france.fr

Netherlands
Weena 290
3012 NJ Rotterdam
Netherlands
Tel: +31-10-282-1445
Fax: +31-10-282-1331
URL:
www.dlink-benelux.com

Belgium
Rue des Colonies 11
B-1000 Brussels
Belgium
Tel: +32(0)2 517 7111
Fax: +32(0)2 517 6500
URL:
www.dlink-benelux.com

Italy
Via Nino Bonnet n. 6/b
20154 – Milano,
Italy
TEL: 39-02-2900-0676
FAX: 39-02-2900-1723
URL: www.dlink.it

Sweden
P.O. Box 15036, S-167 15
Bromma
Sweden
TEL: 46-(0)8564-61900
FAX: 46-(0)8564-61901
URL: www.dlink.se

Denmark
Naverland 2, DK-2600
Glostrup, Copenhagen,
Denmark
TEL: 45-43-969040
FAX: 45-43-424347
URL:www.dlink.dk

Norway
Karihaugveien 89
1086 Oslo
Norway
TEL: 47-22-309075
FAX: 47-22-309085
URL: www.dlink.no

Finland
Pakkalankuja 7A
01510 Vantaa,
Finland
TEL : +358-9-2707 5080
FAX: + 358-9-2707 5081
URL: www.dlink-fi.com

Iberia
C/Sabino De Arana,
56 Bajos
08028 Barcelona
TEL: 34 93 4090770
FAX: 34 93 4910795
URL: www.dlinkiberia.es

Singapore
1 International Business Park
#03-12 The Synergy
Singapore 609917
TEL: 65-6774-6233
FAX: 65-6774-6322
URL: www.dlink-intl.com

Australia
1 Giffnock Avenue,
North Ryde, NSW 2113
Australia
TEL: 61-2-8899-1800
FAX: 61-2-8899-1868
URL: www.dlink.com.au

Japan
10F, 8-8-15 Nishi-Gotanda
Shinagawa-ku, Tokyo 141,
Japan
TEL: 81-3-5434-9678
FAX: 81-3-5434-9868
URL: www.d-link.co.jp

India
D-Link House, Kurla Bandra Complex Road,
Off CST Road, Santacruz (East), Mumbai - 400098.
India
TEL:
91-022-26526696/56902210
FAX: 91-022-26528914
URL: www.dlink.co.in

Middle East (Dubai)
P.O.Box: 500376
Office No.:103, Building:3
Dubai Internet City
Dubai, United Arab Emirates
Tel:+971-4-3916480
Fax:+971-4-3908881
URL: www.dlink-me.com

Turkey
Regus Offices
Beybi Giz Plaza, Ayazaga
Mah. Meydan Sok. No:28
Maslak 34396,
Istanbul-Turkiye
TEL: +90 212 335 2553
FAX: +90 212 335 2500
URL: www.dlink.com.tr

Egypt
19 El-Shahed Helmy, El Masri
Al-Maza, Heliopolis
Cairo,Egypt.
TEL:+202 414 4295
FAX:+202 415 6704
URL: www.dlink-me.com

Israel
11 Hamanofim Street
Ackerstein Towers, Regus Business Center
P.O.B 2148,
Hertzelia-Pituach 46120.
Israel
TEL: +972-9-9715700
FAX: +972-9-9715601
URL: www.dlink.co.il

LatinAmerica
Isidora Goyeechea 2934 of 702,
Las Condes
Santiago – Chile S.A.
TEL: 56-2-232-3185
FAX: 56-2-232-0923
URL: www.dlink.cl

Brasil
Av das Na--es Unidas, 11857,
cj 132 - Brooklin Novo
S-o Paulo - SP - Brazil
04578-000
TEL: (55 11) 550 39320
Fax: (55 11) 550 39321

South Africa
Einstein Park II
Block B
102-106 Witch-Hazel Avenue
Highveld Technopark
Centurion
Gauteng
Republic of South Africa
TEL: 27-12-665-2165
FAX: 27-12-665-2186
URL: www..d-link.co.za

Russia
Grafsky per., 14, floor 6
Moscow
129626 Russia
TEL: 7-095-744-0099
FAX: 7-095-744-0099 #350
URL: www.dlink.ru

China
Room 507/508, Tower W1,
The towers Oriental Plaza
NO.1,
East Chang An Ave.,
Dong Cheng District Beijing ,
100738, China.
TEL +86-010-85182533
FAX: +86-010-85182250
URL: www.dlink.com.cn

Taiwan
2F, No. 119, Pao-Chung Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2910-2626
FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw

Headquarters
2F, No. 233-2, Pao-Chiao Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2916-1600
FAX: 886-2-2914-6299
URL: www.dlink.com.tw

Registration Card

Print, type or use block letters.

Your name: Mr./Ms_____

Organization: _____ Dept. _____

Your title at organization: _____

Telephone: _____ Fax: _____

Organization's full address: _____

_____

Country: _____

Date of purchase (Month/Day/Year): _____

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:

Reseller's name: _____

Telephone: _____ Fax: _____

Reseller's full address: _____

_____

_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?

☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?

☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use ?

☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others_____

4. What network operating system(s) does your organization use ?

☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open
☐Banyan Vines ☐DECnet Pathwork ☐Windows NT ☐Windows NTAS ☐Windows '95
☐Others_____

5. What network management program does your organization use ?

☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS
☐NetView 6000 ☐Others_____

6. What network medium/media does your organization use ?

☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP
☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

7. What applications are used on your network?

☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM
☐Database management ☐Accounting ☐Others_____

8. What category best describes your company?

☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing
☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR
☐System house/company ☐Other_____

9. Would you recommend your D-Link product to a friend?

☐Yes ☐No ☐Don't know yet

10. Your comments on this product?

_____

_____

TO:

D-Link®