FEC Secure IPSec Client

Appendix

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

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

Liability

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

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

Appendix to the
FEC Secure IPSec Client:

Mobile Computing via GPRS/UMTS and Domain Login via NCP Gina

Wie Sie Funkwerk Enterprise Communications erreichen:
Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

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

Contents

1. Mobile Computing via “GPRS/UMTS”

If you are using a multi-function card* for UMTS/GPRS/WLAN, then with the client software, special features of the mobile computing can be used depending on the card characteristics.

Due to the direct support of the multi-function card for UMTS/GPRS/WLAN through the client, installation of management software from the card implemented, is not necessary.

The IPSec Client combines all communication and technical security mechanisms for economic data communication on the basis of the end-to-end principle of security. The client Monitor has visual displays of all connection states, field strength, the selected network, and the provider. Also the integrated dynamic Personal Firewall is optimized for remote access and protects the mobile teleworkstation (even at system start) against any attacks and guarantees maximum security, also during the automatic hotspot login. The VPN connection is established via the integrated Dialer independent of the Microsoft data communications network.

* Currently supported multi-function cards:

T-Mobile Multimedia NetCard
Vodafone Mobile Connect Card
KPN Mobile Connect Card

1.1 Installation

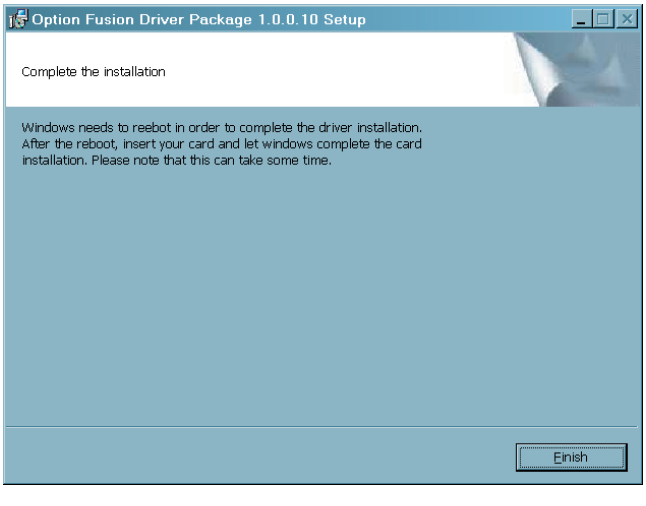
First install the appropriate software version and then install the PCMCIA card driver on your notebook.

1.2 Driver Installation

The driver for the Qualcomm 3G CDMA PCMCIA card is on the included CD in the directory

`Software\Modems\Language Independent\`

Start “OptionFusion.exe” with a double click and confirm the query that is displayed with “OK”.



After completing the installation end setup by clicking on “Finish”.

Then the computer will re-boot.

After the reboot insert the card in a PCMCIA slot.

Please note the following if using the Windows XP operating system

If Windows XP is used with Service Pack 2 and security packages, then a connection cannot be established via the card.

The software will display an error message when attempting to establish a connection (see Fig. to the left).

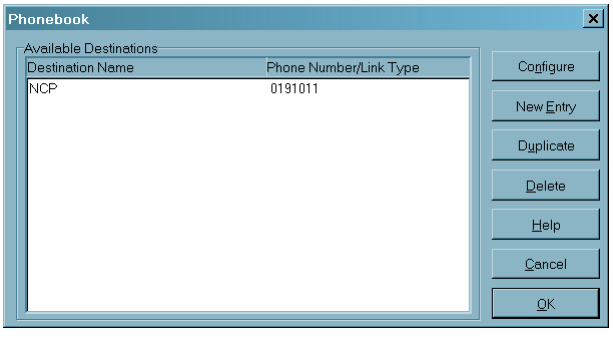
In this case a new driver must be installed. For this purpose the file OptionCard-Installer.exe is available.

A newer driver is on the driver CD for the newer Multimedia NetCard from T-Mobile, which only supports UMTS/GPRS.

2. Configuring a Destination System (Profile)

Create a new destination system (profile) in the client software. Follow the instructions provided in the Client Software Manual.

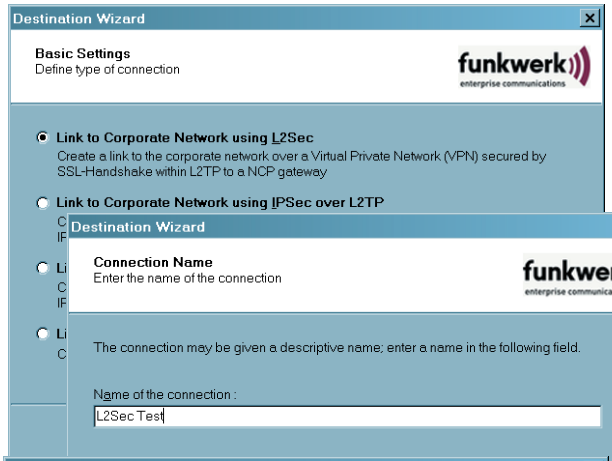
2.1 Configuring with a Wizard



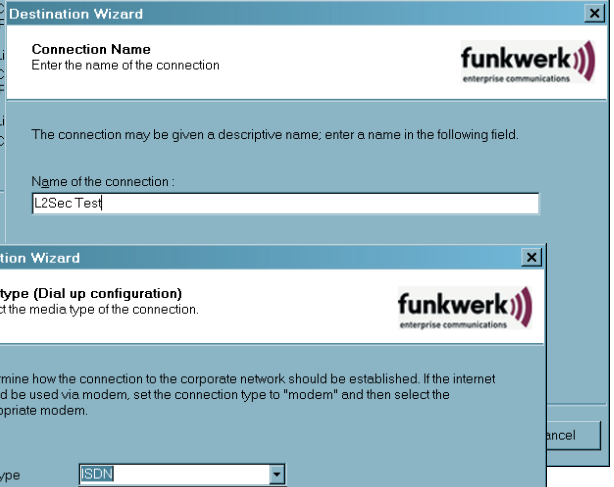
Click on “New entry” and follow the wizard’s instructions. Afterwards you can complete the configuration in the telephone book.

A connection to the corporate network is provided below as an example.

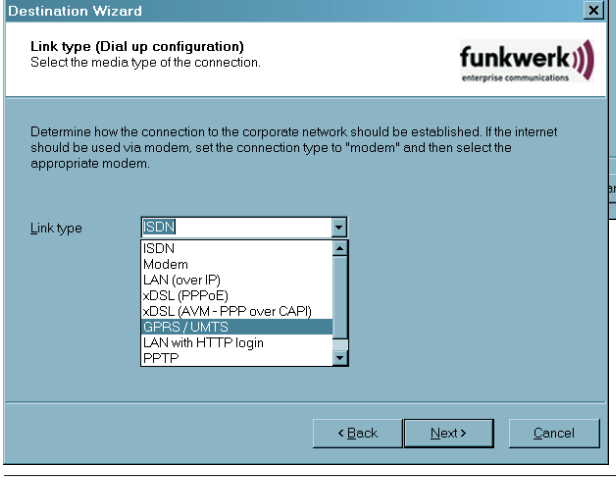
An NCP Gateway is used as the destination system for this test connection.



Click on “Next”

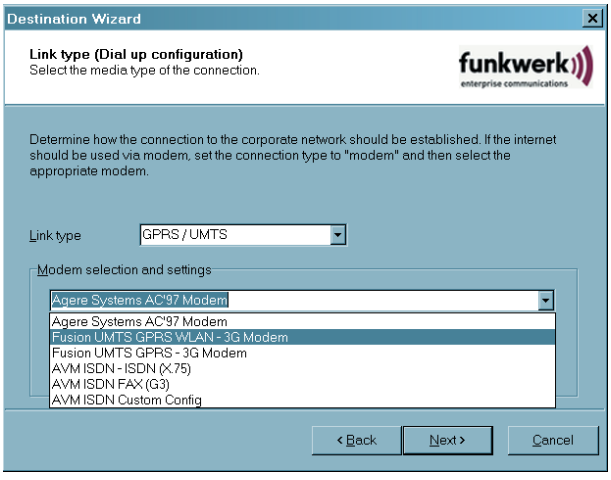


Enter a name for this destination system (profile).

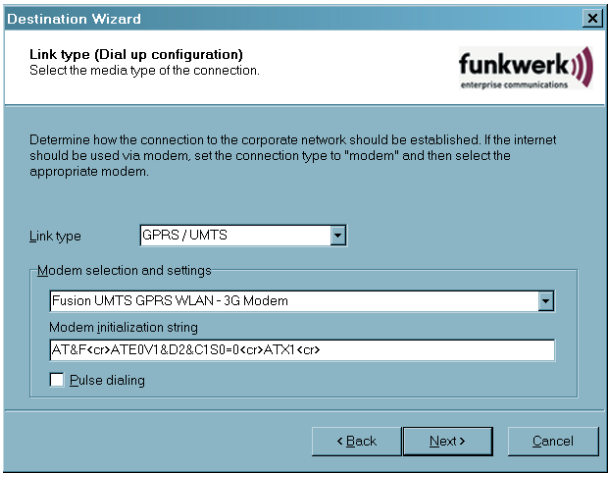


Click on “Next”

Select GPRS/UMTS as connection type.

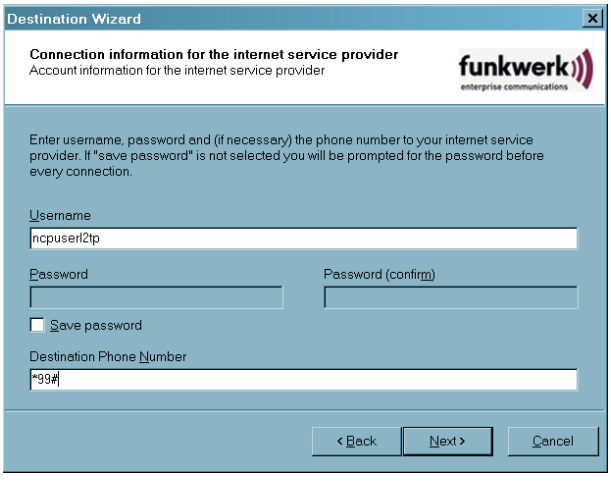


The card “Fusion UMTS GPRS WLAN - 3G modem” will be displayed accordingly. Select this card.



Do not make any changes to the modem initialization string. Do not switch pulse dialing on.

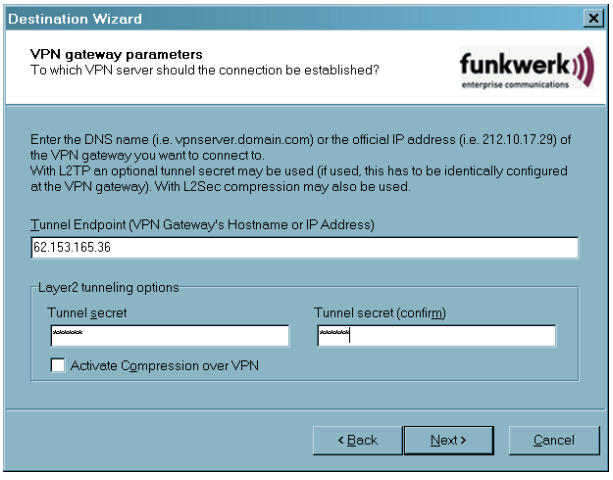
Click on “Next”



You only need to enter a (any) user name for the Internet Service Provider (ISP) unless you have received special passwords from the provider. Billing (and the identification) is executed via the SIM card.

For a test connection to an NCP Gateway enter as telephone number:
* 9 9 #

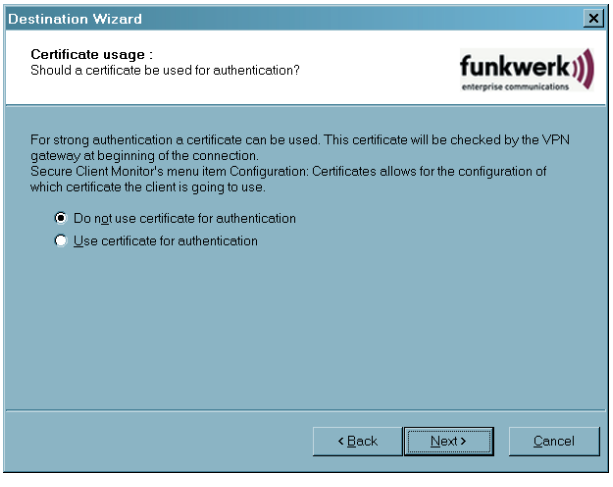
Click on “Next”



Read the description of the gateway parameters.

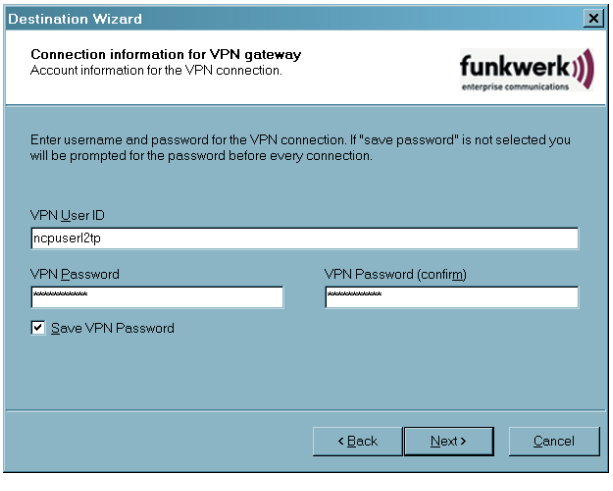
If you want to setup a test connection to the NCP Gateway then enter as tunnel endpoint:
`62.153.165.36`
as tunnel secret:
`secret`
Compression is not necessary.

Click on "Next"



You do not need a certificate for a test connection to the NCP Gateway.

Click on "Next"

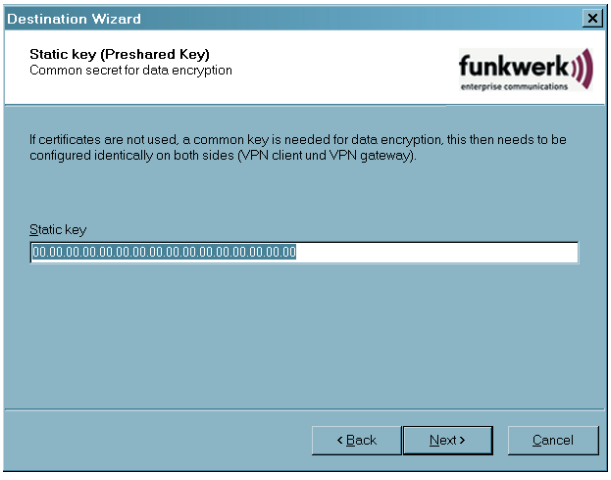


Enter the following as access data for the NCP VPN Gateway:

VPN User ID:
`ncpuserl2tp`

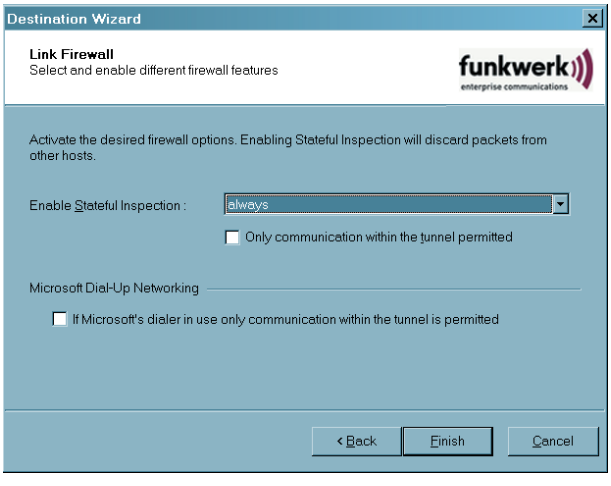
Click on "Save VPN Password" and enter the following as VPN password:
`ncpuserl2tp`

Click on "Next"



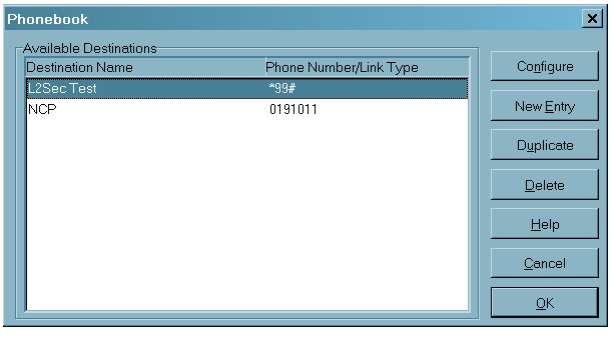
Do not change the static key setting for the test connection.

Click on "Next"



It is not necessary to set the Link Firewall for the test connection.

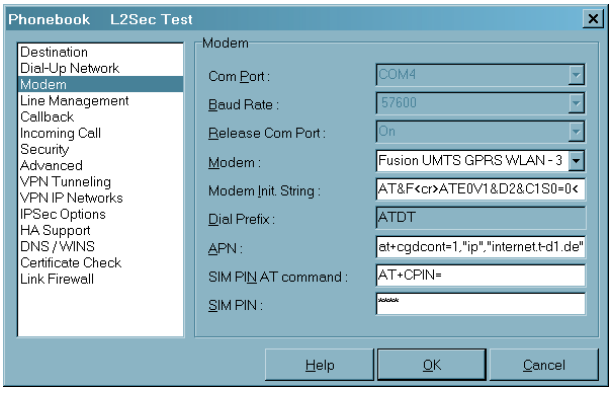
Click on "Next"



This concludes the configuration with the assistant.

Now click on "Configuration" and complete the configuration in the telephone book.

2.2 Configuration in the Phonebook



For the test connection select the parameter “Modem” and make the following entries:

APN

The APN (Access Point Name) is required for the GPRS and UMTS dial-in. You get the APN from your provider. The APN is used primarily for administrative purposes.

The AT command
`at+cgdconf=1,"ip",`
is standard for the transferring the APN to the SIM card, however it can vary depending on the provider.

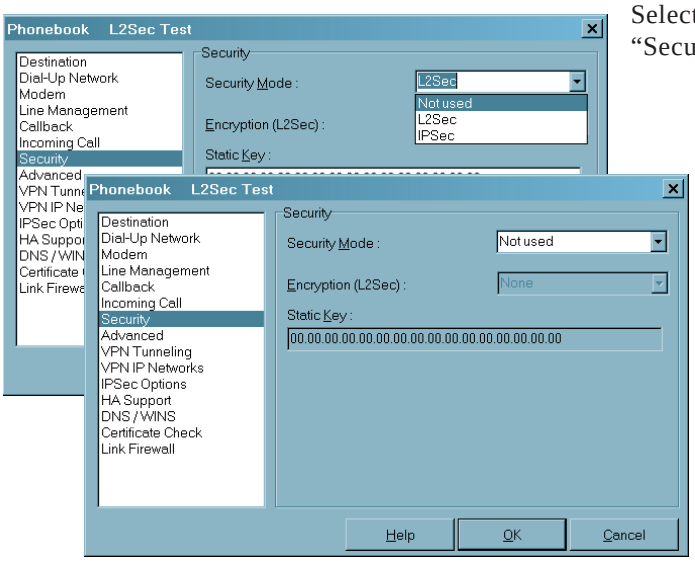
The APN
`“internet.t-d1.de”`
varies depending on the SIM card and only applies for the SIM D1 card from T-Mobile.

SIM PIN AT command

When using a GPRS/UMTS card the specific AT command must be entered. This command
`AT+CPIN=`
is standard and causes the SIM PIN to be correctly detected.

SIM PIN

If you are using a SIM card for GPRS or UMTS then enter the PIN for this card here. If you are using a mobile phone, then this PIN must be entered on the mobile phone.



Select the parameter field “Security”.

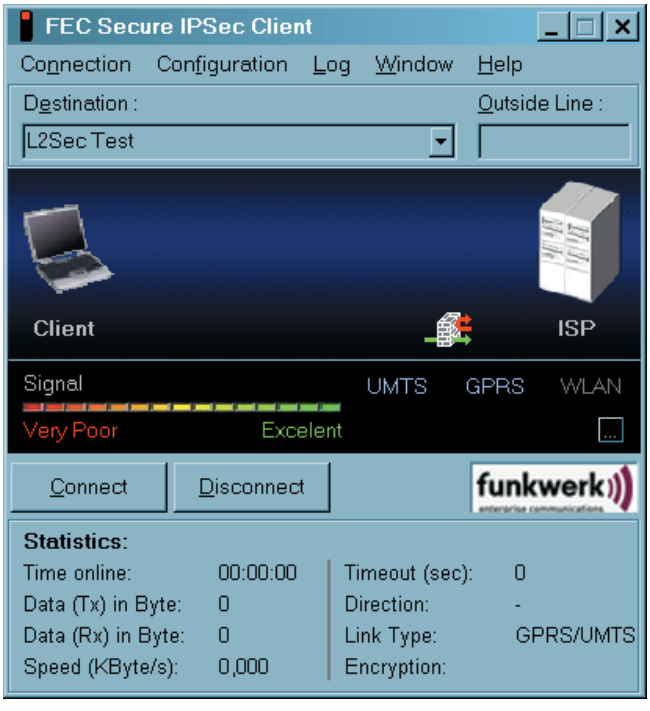
Security Mode

Do not use security mode for the test connection!

Select “Do not use” and then click on “OK”.

Save the telephone book setting and then open the Monitor.

3. The Monitor

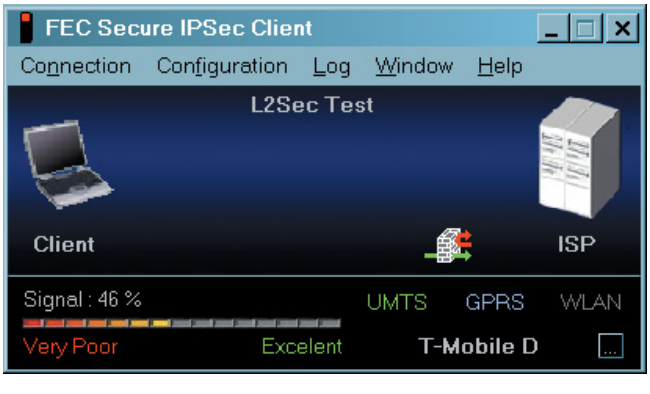


Start the Monitor.

The Monitor of the IPSec Client must look like the adjacent illustration. The Entry Client Monitor is essentially the same.

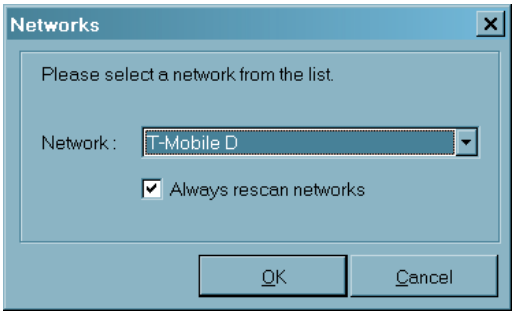
The field strength of the wireless network must be displayed between the graphic field and the toolbar.

If the field strength is not displayed, then an error message will appear which refers to a modem error. In this case proceed as described under “1.1 Driver installation”.



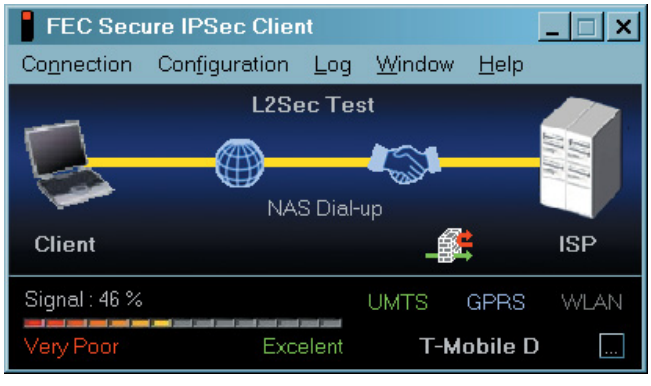
After the Monitor starts the card will automatically search for a wireless network and displays it with the corresponding field strength, once a wireless network has been found (T-Mobile D" in the fig. to the left).

If the network is displayed, then another network search can be triggered by clicking on the [...] button.



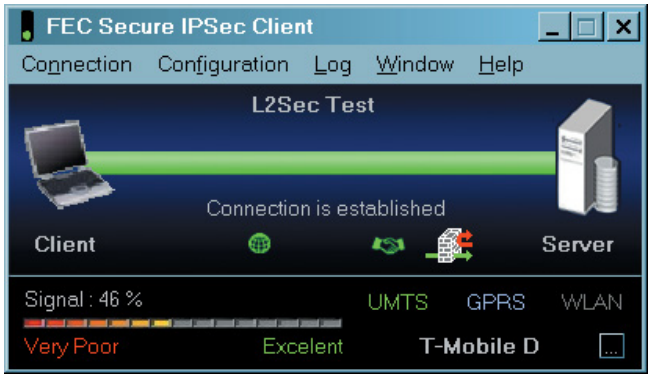
After searching for an alternative network the window for network selection will be displayed. The desired network can be selected from a list.

If a new network search is not desired every time the Monitor is called up, then this function (which is active by default) must be switched off via the Check button.



The connection set-up can be executed precisely in the same manner as for a stationary network (see “Connection setup” in the Client Software Manual), alternatively the connection can be setup with the modes “automatic”, “manual” or “alternating”.

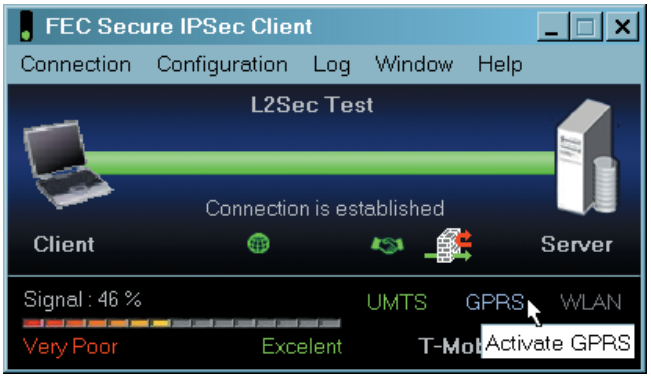
The connection type is displayed in green (“UMTS” to the left).



Once the connection is set-up, then you can work in the same manner you work in your local corporate network.

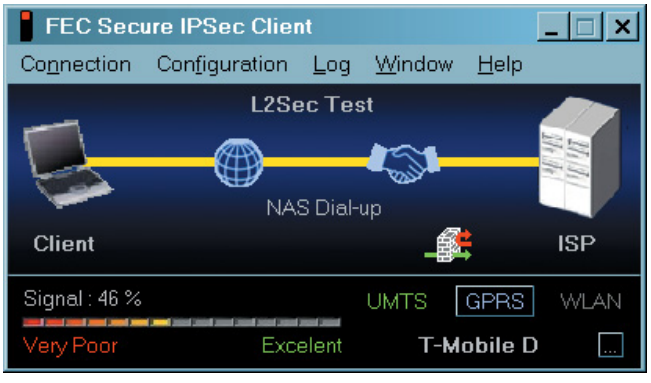
This also applies if the card automatically changes from the connection medium UMTS to GPRS due to low field strength. In this case the connection remains intact.

If the field strength increases again, then the card automatic switches back.



You can also change the connection medium manually. Click on the desired medium with the mouse, in the Fig. to the left, “Activate GPRS”.

However if you change the medium manually the connection will be disconnected.

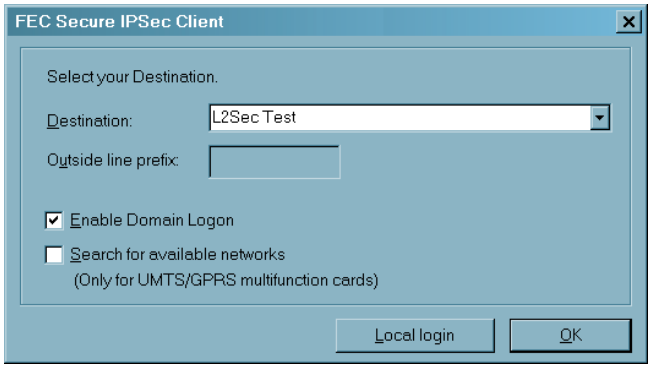


Then the connection will be reestablished automatically, if this is what has been configured for the connection setup in the phonebook.

4. Domain Login via NCP Gina

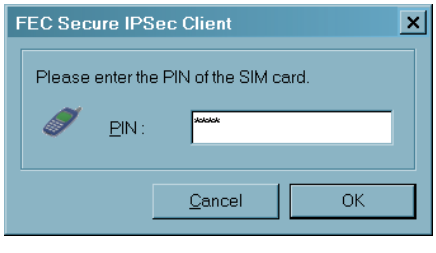
The client software starts in background in the boot phase and captures the call “Crtl-Alt-Delete”.

The integrated Personal Firewall provided by the software is already active at this time, so that the PC is already protected.

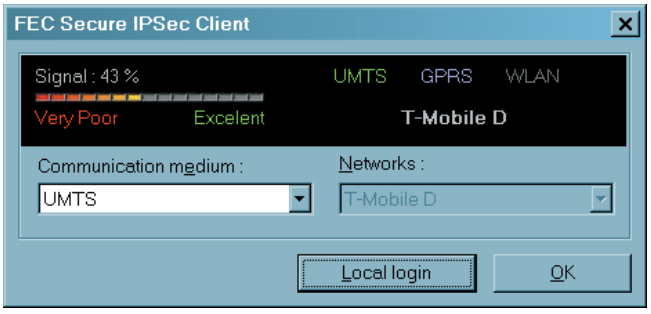


The destination system that has been configured for the connection medium GPRS/UMTS can be selected during the boot phase.

(The function “Activate domain login” is only required if there was previously an incorrect logoff! The search for available alternative networks takes a few seconds and is usually only significant abroad.)



The SIM PIN must then only be entered if it has not yet been entered in the configuration of the destination system (profile) in the “Modem” parameter field in the telephone book or if the saved PIN does not agree with SIM you are using.

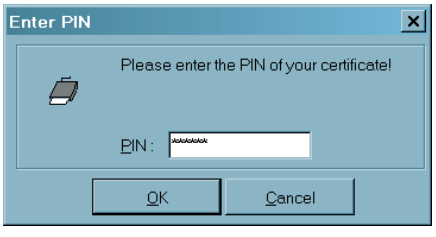


Then the signals of the card will be displayed, after the network search the wireless network found is shown with the respective field strength.

If search for alternative networks has been activated, then a different network as well as a different connection medium can be selected manually.

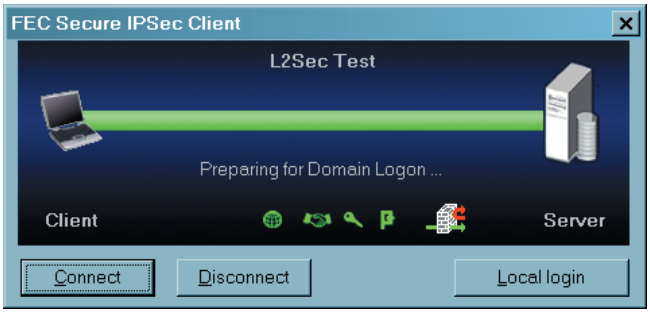
Then click on “OK” in order to continues with domain login.

(Use “Local login” to exit the domain login dialog.)



If use of the certificate has been configured for this connection, then at this point its PIN must be entered.

Then click on “OK”.



This establishes the connection and a tunnel into the central corporate network is setup.

Further procedure depends on the configuration in the Monitor menu under “Configuration / Logon options”.

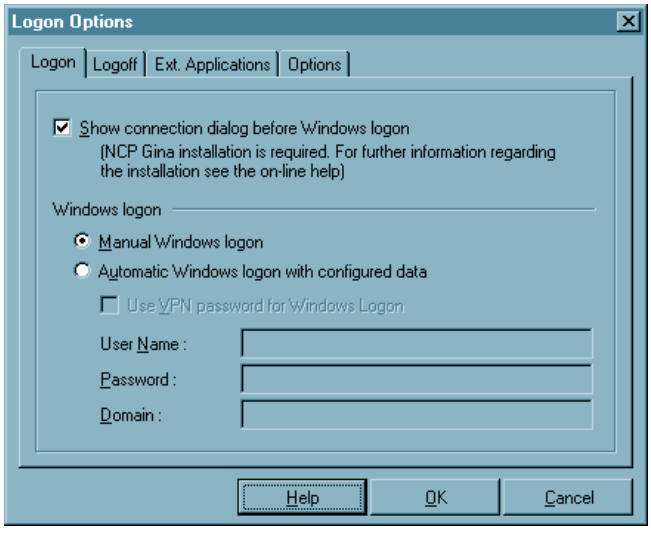
1. The user enters the request login data as in the standard Windows login (see “Standard Windows login” in the Fig. below)

2. The client software transfers the requested login data into this screen (the MS0GINA) automatically, so that the user does need to enter anything else for the Windows login. For this “Use saved login data” must be activated in the logon options, and the data must be entered in the fields.

4.1 Logon Options

The logon options are selected via the “Configuration” Monitor menu.

Please note the descriptions in your handbook of the client about possible settings in this windows.



In this window you can decide wether via “the connection dialog before Windows logon” on a remote domain the connection from the client to the gateway should be established. For connection setup to the gateway it may be necessary to enter the PIN for the certificate, as well as for the SIM card, and the (non-saved) password for network dial-in prior to entering the password for the Windows login.

If the connection setup takes place prior to the Windows logon, then the login to the remote domains will be encrypted.

If you use the logon option with callback, then “Negotiate PPP callback” must be executed (see →“Callback”).

The computer must be rebooted after every change of logon options made in the Monitor.

This function can only be activated with administrator rights!

5. Log Files

If a multi-function card for UMTS/GPRS is installed, then a log file is written in the log directory of the Secure IPSec Client, with the following columns:

1st Column: Time

2nd Column: Current field strength

3rd Column: Average field strength of the last minute

4th Column: Average field strength of the last 5 minutes

5th Column: Average field strength of the last 10 minutes

6th Column: Current network type (UMTS or GPRS)

7th Column: Current network

An entry is created every 10 seconds; however the entries are only written to the file every 5 minutes.
A log file is created with the name “mfc<DATE>.log” for each day.
The log files for the last 7 days are saved.

For your notes →

Appendix to the
FEC Secure IPSec Client:

Services and Applications of the Client

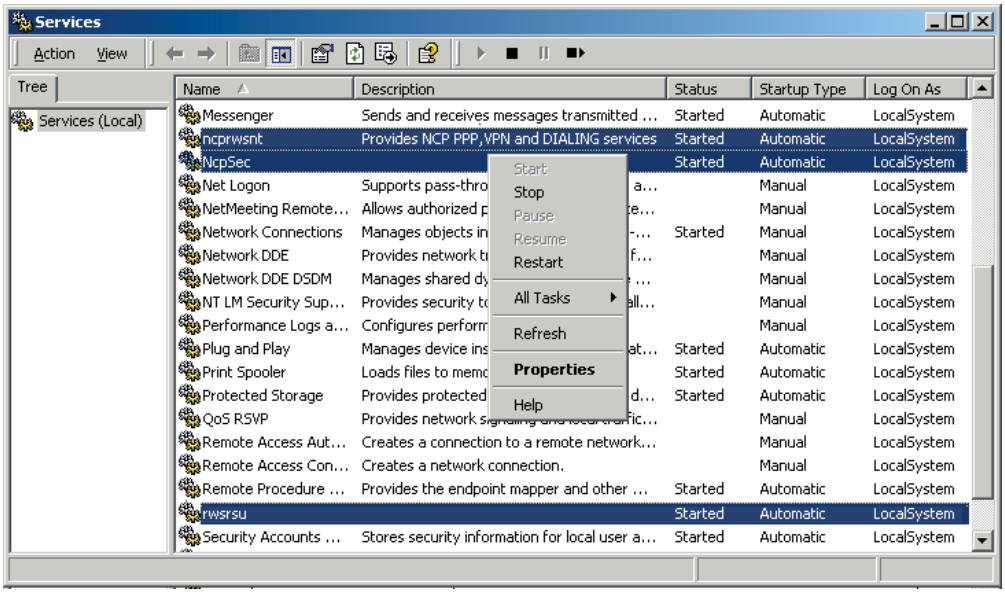
Wie Sie Funkwerk Enterprise Communications erreichen:
Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

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

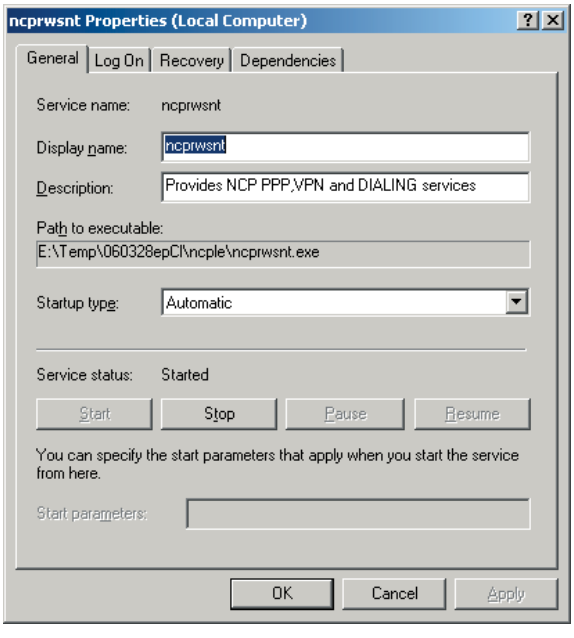
Contents

1. Services and Applications of the Secure Client

The services ncpsec.exe, ncprwsnt.exe, and rwrsu.exe can be called from the Windows system service overview (accessed via the Windows start menu under “Control Panel – Administrative Tools – Services”, the services are highlighted in the Fig. below).



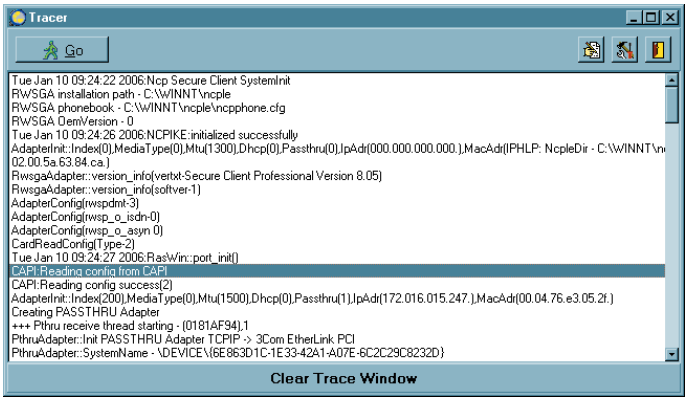
You can view the properties of these services from this Windows screen, or you can start or stop the services.



All services of the Secure Client are started automatically from the installation directory after the software is installed.

In addition to the services there are also applications in the installation directory:

ncptrcw.exe



Trace-Monitor; can also be started via “Windows – Programs – Secure Client Tracer”. This is an autonomous application program for qualified system technicians. For example it can used to create traces for troubleshooting purposes. The tracer is not intended for the normal user!

ncpmon.exe

starts the Client Monitor; can be started by double clicking on the traffic light icon in the toolbar or via “Windows – Programs – Secure Client Monitor”. Monitor operation and menu prompts are described in detail in the manual for the respective Secure Client.

ncpike9x.exe

IKE protocol for Windows 95/98

ncpike.exe

IKE protocol for Windows 2000/XP

lbtrace.exe

tracer on driver level for virtual NCP adapter

inst95.exe

installation program for Windows 95/98

insrnt5.exe

installation program for Windows 2000/XP

uninst.exe

The Secure Client can be deinstalled with this program by bypassing the Windows software administration.

3monapl.exe

Field strength display for UMTS/GPRS when using a multi-function card.

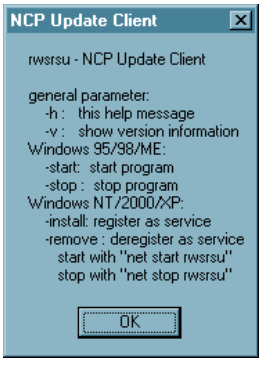
ncpauth.exe

is used for http authentication

ncprwsnt.exe

Responsible for data communication frame processing via NCP PPP and VPN, as well as the dial services.

rwsrsu.exe



Update Client; corresponds to the program ncprsu.exe on the Management Server, see →below

rwsrsuhlp.exe

Help program for rwsrsu.exe; start it with:
`rwsrsu -h`

ncprndll.exe

Is used by the Update Client and calls a DLL that stops or restarts the Client when there is an update.

ncpbudgt.exe

Budget Manager, see →below

ncpmsg.exe

Corresponds to the Budget Manager and if configured in the Client Monitor, it opens the message window with the appropriate warning for the user.

rwscmd.exe

Command line interface, see →below

ncppopup.exe

Program for entering license data and viewing the software version information; it can be started via “Windows – Programs – Secure Client Popup”.

ncpsec.exe

PKI module of the Client software; this program is only necessary when using digital certificates. The configuration of smart card readers and soft certificates is described in detail in the respective Secure Client manual, in the “Monitor” section.

ncpepsec.exe

Module for endpoint security between the Secure Client and VPN Gateway; the policies for endpoint security are configured on the Secure Enterprise Management system with the plug-in “Endpoint Policy Enforcement”. Consequently Endpoint Policy Enforcement is only possible if NCP Secure Enterprise Management is implemented. The security policies of all endpoints of the components implemented can only be uniformly allocated to all endpoints with this central management tool. While the Endpoint Security Policies are output from the Enterprise Management system, download of the security policies (which the Management Server prescribes) must be activated on the

VPN Gateway. This is done on the Secure Server Manager in the configuration branch “Client Policy Enforcement”. If endpoint security is activated then the current policies are compared and downloaded via the program ncpepsec.exe.

The following services and applications are described in more detail below:

ncpbudgt.exe
rwscmd.exe
ncprwsnt.exe

1.1 Overview of the ports of the Client

for Win2000/XP:

ncpmon.exe	10544
ncpsec.exe	10522, 10542
ncprwsnt.exe	1701, 500, 10523, 10530, 10550, 10600, 10610
rwsrsu.exe	dynamic port after 12501 (Management Server)

for 98/ME:

ncpmon.exe	10544
ncpbudgt.exe	10522, 10542
ncpike9x.exe	1701, 500, 10523, 10530, 10550, 10600, 10610
rwsrsu.exe	dynamic port after 12501 (Management Server)

additinal ports:

PKI	10523
PPPoE	10550
IPHlp	10560
WSUP (Driver)	10600
DNS Client	10610

2. ncpbudgt.exe – Budget-Manager (Connection Management/Statistics)

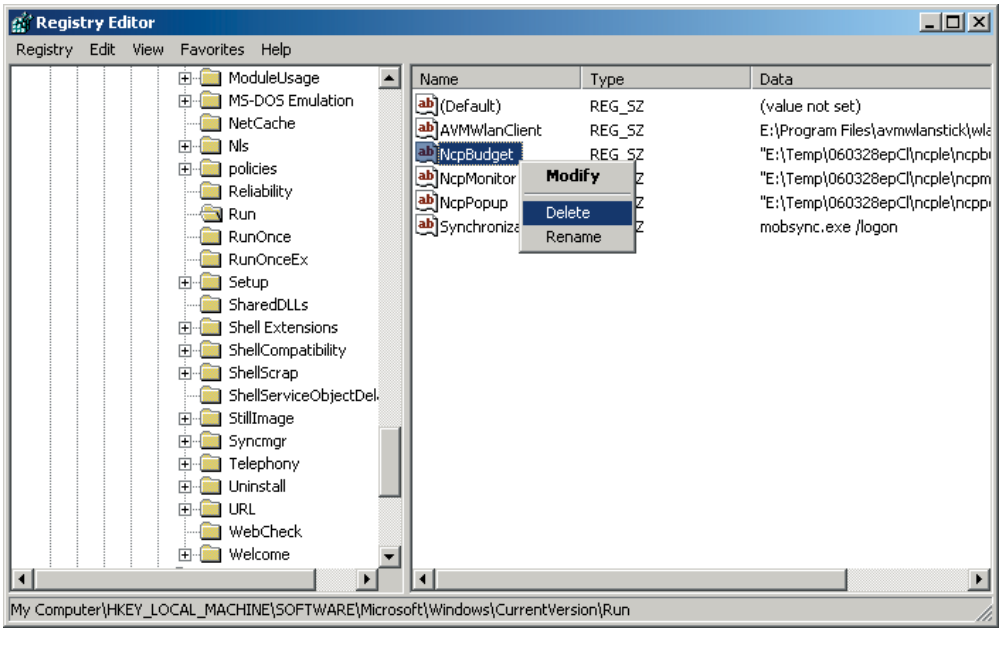
After installation of the Client Software the so-called Budget Manager runs automatically for connection management and statistics when the monitor starts.

The Budget Manager is responsible for monitoring Client software connections in accordance with precisely defined criteria.

These criteria are specified in the Monitor menu under “Configuration / Connection Management”. (See the manual for the Secure Client, Monitor, and Connection Management)

Activating Connection Management in the monitor menu is only practical if the connections are not routed to a corporate network gateway, or if charges are incurred for connection time or frequency of the connections. Otherwise charge management can be administered centrally.

If the Budget Manager is not used then it can be removed from the registry (see Fig. below). In this regard, note that it is automatically re-installed for an update or for a new installation. Thereafter it must be deleted again with regedit.



Key: Software\Microsoft\Windows\CurrentVersion\Run\NCPBudget

3. rwscmd.exe – Command Line Interface

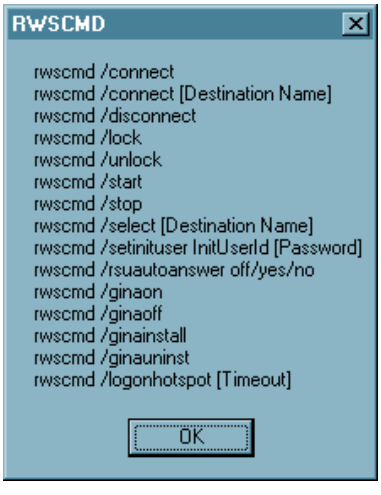
Attention! The following description only applies for Windows systems.

3.1 Transferring Commands to the Client

With rwscmd.exe the client has a command line interface that can be used for other applications. The prerequisite to use the rwscmd.exe program is Client software of at least version 7.0 (Enterprise Client) or 8.0 (Entry Client).

At installation the command line interpreter is copied into the ncple directory under Windows. It is called from this directory (e.g.):

```
C:\Windows\ncple>rwscmd /<Kommando>
```



If the syntax is not observed, or if a command is specified incorrectly, or incompletely, then a window will be displayed that lists the possible commands:

```
connect
connect [Destination Name]
disconnect
lock
unlock
start
stop
select [Destination Name]
setinituser InitUserId [Password]
rsuautoanswer off/yes/no
ginaon
ginaoff
ginainstall
ginaunins
logonhotspot [Timeout]
```

3.2 Prerequisite for Program Use

- ☐ The services ncprwsnt, ncpsec, and rwsrsu, must be started. These services start as a standard function after installation of the Client Software – they are located in the directory
  `C:\Windows\ncple>`

- ☐ It is only necessary to start the Monitor if passwords or PIN entries are required, since rwscmd.exe does not start a PIN dialog..

- ☐ In addition write authorizations must exist to the registry key:
  `KEY_LOCAL_MACHINE\`
  `Software\NCP engineering GmbH\NCP Enterprise Monitor`

3.3 Description of the Commands

`rwscmd /connect`
Required Windows authorization: User rights
Description: Connection setup with the last destination entry set in the Monitor.

`connect [Destination Name]`
`e.g.: rwscmd /connect "LAN via Router (IP)"`
Required Windows authorization: User rights
Description: Connection setup with the transferred destination entry.

Apostrophes are set instead of the square brackets. They are necessary because this is a transfer with spaces.

`rwscmd /disconnect`
Required Windows authorization: User rights
Description: Disconnects the current connection.

`rwscmd /lock`
Required Windows authorization: User rights
Description: Locks the Client, connection setup is no longer possible

`rwscmd /unlock`
Required Windows authorization: User rights
Description: Unlocks the Client, resets the lock that was set with Lock

`rwscmd /start`
Required Windows authorization: Administrator rights
Description: Starts all services, popup and monitor of the client

If called again the message “IPSec Client is already open” is displayed.

`rwscmd /stop`
Required Windows authorization: Administrator rights
Description: Stops all services, popup and Monitor of the client

Also note that if the command rwscmd /stop has been executed then the command rwscmd /start must be executed thereafter, so that the services and the monitor can be restarted. In this case a reboot is not sufficient, as the popup and the monitor are not started.

`rwscmd /select “Destination Name”`
Required Windows authorization: User rights
Description: In the Secure Client the system goes to the desired destination.

Apostrophes are set instead of the square brackets. They are necessary because this is a transfer with spaces.

`rwscmd /setinituser UserId “Passwort”`
Required Windows authorization: Administrator rights
Description: If you do not want a window to be displayed for the initial connection, then the user ID, and optionally the password, can be transferred for the initial logon for the initprocess.

Apostrophes are set instead of the square brackets. They are necessary because this is a transfer with spaces.

`rwscmd /rsuautoanswer off/yes/no`
Required Windows authorization: Administrator rights
Description: This is where you set how the system will respond to queries for a software update.

yes	Client software automatically gets an update without query.
no	Automatic software update is rejected and not executed.
off	With the off setting the system asks (in a message window) whether the software should be updated.

`rwscmd /ginainstall`
Required Windows authorization: Administrator rights description: Installs the NCP Gina, if this has not yet occurred in the software installation (see the section “Installation” in the Client manual).

`rwscmd /ginaunins`
Required Windows authorization: Administrator rights
Description: Deinstalls the NCP Gina. If an external Gina calls the NCP Gina, then deinstallation is not possible with this command. In this case it must be removed from the registry manually, or the Ginas must be deinstalled again in the reverse sequence (see the section “Logon options” in the Client manual.

`rwscmd /ginaon`
Required Windows authorization: Administrator rights
Description: Switches the NCP Gina dialogs for logon to the VPN Gateway so that they are visible if the NCP Gina has been installed.

`rwscmd /ginaoff`
Required Windows authorization: Administrator rights
Description: Switches the NCP Gina dialogs invisible and thus skips the VPN Gateway logon with the NCP Gina.

`rwscmd /logonhotspot [Timeout]`
If a hotspot logon will be executed via an external dialer, then the firewall can be released for ports 80 (HTTP) and 443 (HTTPS) with this command. This generates a dynamic rule that allows data traffic for this hotspot logon, until the transferred timeout (in seconds) has elapsed.

Because the firewall can thus be released via the command line, the parameter “Allow hotspot logon for external dialers” has been added under “Options” in the firewall settings. The command can only be executed via rwscmd if this parameter is active. (See → Configuration parameters / Phonebook, Firewall settings).

4. ncprwsnt.exe

Responsible for data communication frame processing via NCP PPP and VPN, as well as the dial services.

Applications which need system rights can be started with this service automatically after a connect or a disconnect. For that purpose two batch files in the installation directory have to be edited:

connect.bat

This batch file includes the executable programs or batch files which should be executed after a connect.

disconnect.bat

This batch file includes the executable programs or batch files which should be executed after a disconnect.

Note the parameter “Deny the start of the (dis)connect.bat”. It is located in the monitor menu “Call Control Manager / Ext. Applications” under the item “Configuration”.

This function should always be activated, exceptionally the execution with of one of the batch files administrator rights is absolutely necessary.

Applications (batch files) which require only user rights can be started via this monitor menu “Configuration / Call Control Manager / Ext. Applications” by entering their names (see →Client Monitor / Call Control Manager).