FEC Secure IPSec Client

Anhang

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

Haftung

Alle Programme und das Handbuch wurden mit größter Sorgfalt erstellt und nach dem Stand der Technik auf Korrektheit überprüft. Alle Haftungsansprüche infolge direkter oder indirekter Fehler, oder Zerstörungen, die im Zusammenhang mit dem Programm stehen, sind ausdrücklich ausgeschlossen. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslastungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Änderungen zu diesem Produkt finden Sie unter www.funkwerk-ec.com.

Anhang zu
FEC Secure IPSec Client:

Mobile Computing via GPRS/UMTS und Domänenanmeldung mit 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

Inhalt

1. Mobile Computing via “GPRS/UMTS”

Wird eine Multifunktionskarte* für UMTS/GPRS/WLAN eingesetzt, so können mit der Client Software spezielle Features des Mobile Computings unter Einbeziehung der Karteneigenschaften genutzt werden.

Aufgrund der direkten Unterstützung der Multifunktionskarte für UMTS/GPRS/WLAN durch den Client kann die Installation einer Management-Software von der eingesetzten Karte entfallen.

Der IPSec Client vereint alle kommunikations- und sicherheitstechnischen Mechanismen für eine wirtschaftliche Datenkommunikation auf Basis des Ende-zu-Ende Sicherheitsprinzips. Der Client-Monitor verfügt über optische Anzeigen aller Verbindungsstati, der Feldstärke, des selektierten Netzes und Providers. Auch die integrierte dynamische Personal Firewall ist optimiert für Remote Access und schützt den mobilen Telearbeitsplatz bereits bei Systemstart gegen jegliche Angriffe und garantiert ein Maximum an Sicherheit auch während der automatischen Hotspot-Anmeldung. Die VPN-Verbindung wird unabhängig vom Microsoft DFÜ-Netzwerk über den integrierten Dialer aufgebaut.

* derzeit unterstützte Multifunktionskarten:

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

1.1 Installation

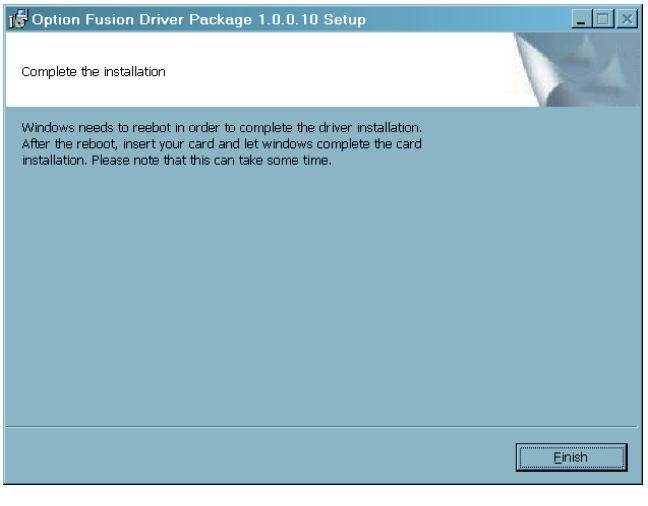
Installieren Sie zunächst die Software des FEC Secure IPScec Clients und spielen Sie anschließend den Treiber der PCMCIA-Karte an Ihrem Notebook ein.

1.2 Installation des Treibers

Der Treiber zur PCMCIA-Karte Qualcomm 3G CDMA befindet sich auf der zugehörigen CD im Verzeichnis

`Software\Modems\Language Independent\`

Starten Sie dort “OptionFusion.exe” mit Doppelklick und bestätigen Sie die daraufhin erscheinenden Fenster mit “OK”.



Nach der erfolgten Komplettierung der Installation, beenden Sie das Setup mit einem Klik auf “Finish”.

Daraufhin wird der Rechner gebootet.

Nachdem Reboot stecken Sie die Karte in einen PCMCIA-Slot.

Bitte beachten Sie bei Einsatz des Betriebssystems Windows XP

Wird Windows XP mit Service Pack 2 und Sicherheits-Packages eingesetzt, so kann eine Verbindung über die Karte nicht hergestellt werden.

Bei einem Verbindungsaufbau zeigt die Software eine Fehlermeldung an (siehe Abbildung links).

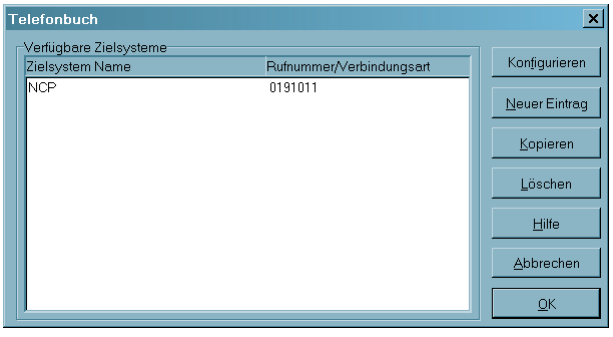
In diesem Fall muss ein neuer Treiber eingespielt werden. Dafür ist die Datei OptionCardInstaller.exe erhältlich.

Ein entsprechend neuerer Treiber befindet sich auch auf der Treiber-CD zur neueren Multimedia NetCard von T-Mobile, die nur UMTS/GPRS unterstützt.

2. Konfiguration eines Zielsystems (Profils)

Legen Sie ein neues Zielsystem (Profil) der Client Software an. Beachten Sie dazu die Beschreibung im Handbuch zur Client Software.

2.1 Konfiguration mit Assistenten



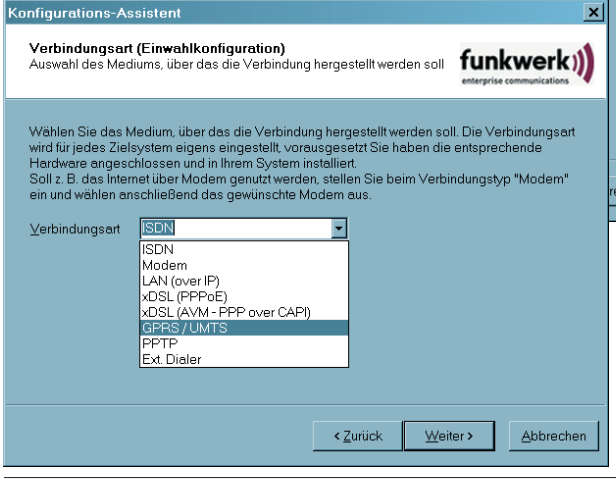
Klicken Sie auf “Neuer Eintrag” und erfüllen Sie die Eingabeaufforderungen des Assistenten. Anschließend kann die Konfiguration im Telefonbuch komplettiert werden.

Im folgenden wird als Beispiel eine Verbindung zum Firmennetz über L2Sec beschrieben.

Als Zielsystem dieser Testverbindung dient ein NCP Gateway.

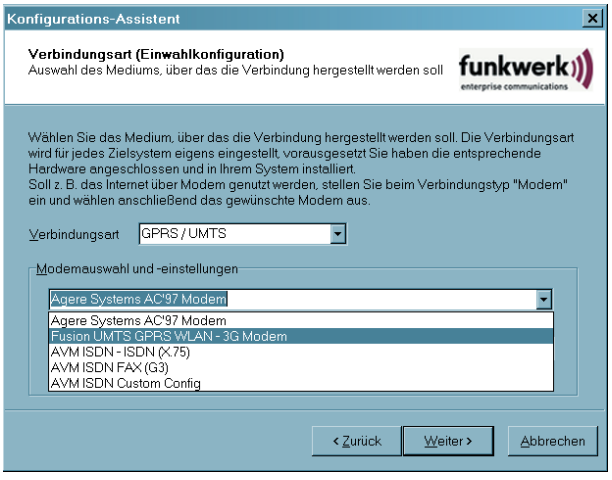
Anschließend auf “Weiter”

Geben Sie für dieses Zielsystem (Profil) einen Namen ein.

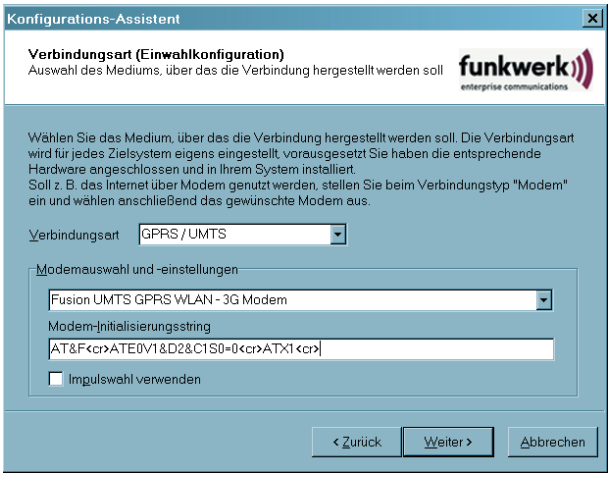


Anschließend auf “Weiter”

Als Verbindungsart wählen Sie GPRS/UMTS.

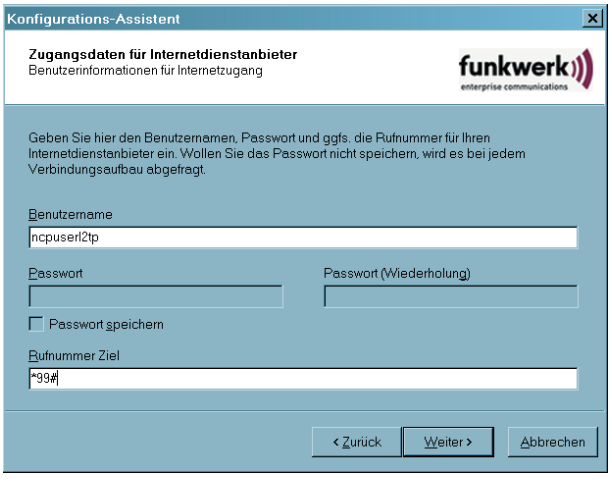


Entsprechend wird in der Modem-Auswahl die Karte “Fusion UMTS GPRS WLA - 3G Modem” angezeigt. Selectieren Sie diese Karte.



Belassen Sie den zugehörigen Modem-Initialisierungsstring unverändert. Schalten Sie die Impulswahl nicht ein.

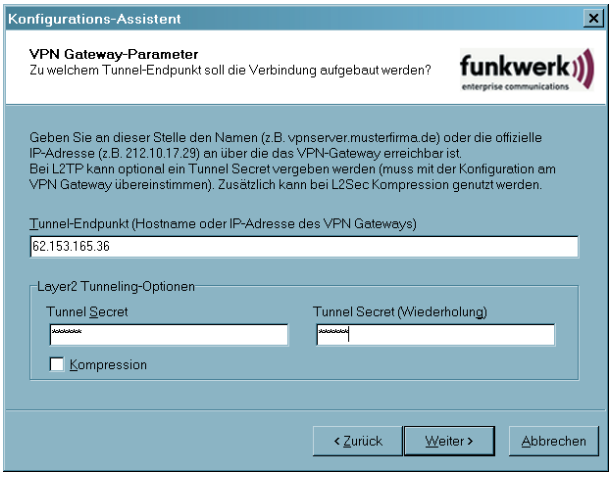
Anschließend auf “Weiter”



Als Zugangsdaten für den Internetdienstanbieter (ISP) muss lediglich ein (beliebiger) Benutzername eingegeben werden, es sei denn Sie haben vom Provider spezielle Kennwörter erhalten. Die Abrechnung (und die Identifikation) erfolgt über die SIM-Karte.

Für eine Testverbindung zu einem NCP Gateway tragen Sie als Rufnummer ein:
*99#

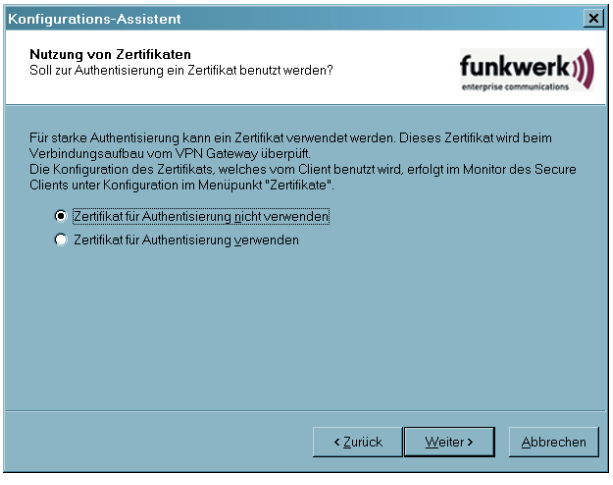
Anschließend auf “Weiter”



Beachten Sie die Beschreibung zu den VPN Gateway-Parametern.

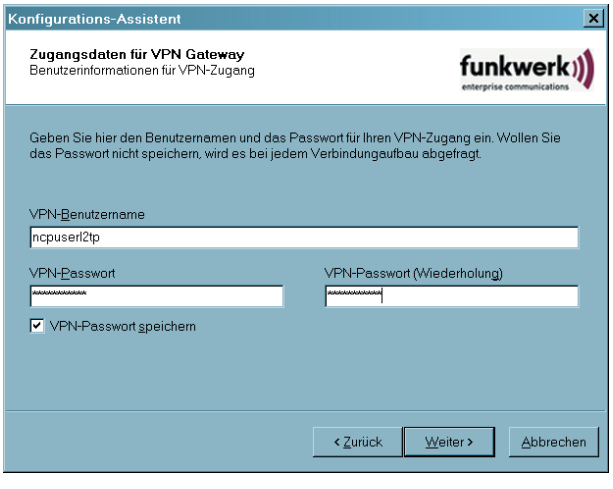
Soll eine Testverbindung zum NCP Gateway hergestellt werden, so geben Sie als Tunnel-Endpunkt ein:
`62.153.165.36`
als Tunnel Secret:
`secret`
Kompression wird nicht benötigt.

Anschließend auf "Weiter"



Für eine Testverbindung zum NCP Gateway ist die Nutzung eines Zertifikats nicht nötig.

Anschließend auf "Weiter"

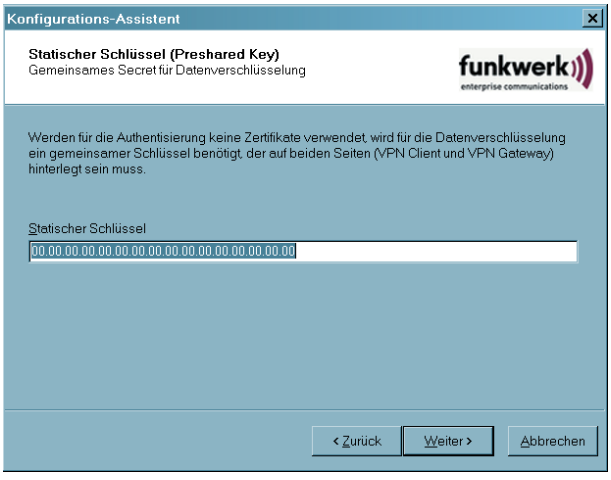


Als Zugangsdaten für das NCP VPN Gateway geben Sie folgendes ein:

VPN Benutzername:
`ncpuserl2tp`

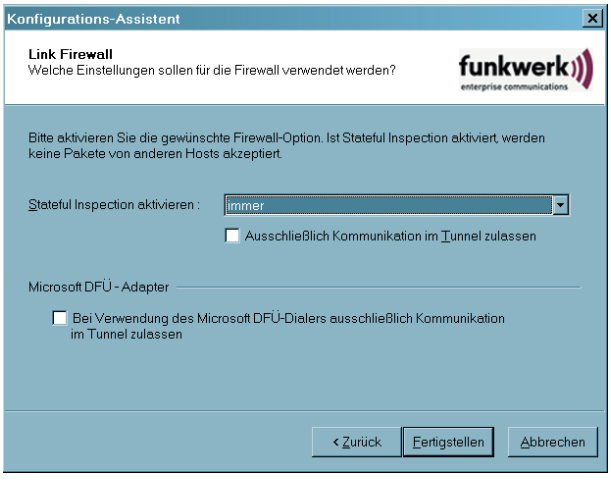
Klicken Sie auf "VPN-Passwort speichern" und geben Sie als VPN-Passwort ein:
`ncpuserl2tp`

Anschließend auf "Weiter"



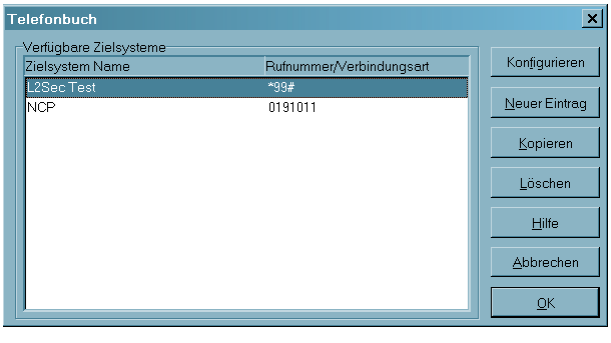
Für die Testverbindung belassen Sie die Einstellung für den Statischen Schlüssel.

Anschließend auf "Weiter"



Die Link Firewall muss für die Testverbindung nicht unbedingt gesetzt werden.

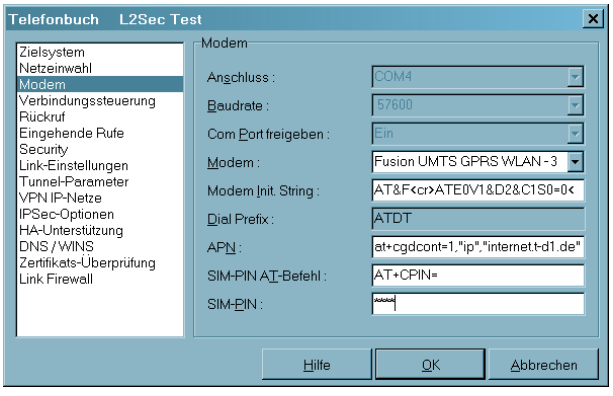
Anschließend auf "Weiter"



Damit ist die Konfiguration mit dem Assistenten abgeschlossen.

Klicken Sie jetzt auf "Konfigurieren" und vervollständigen Sie die Konfiguration im Telefonbuch.

2.2 Konfiguration im Telefonbuch



Selektieren Sie für die Testverbindung das Parameterfeld “Modem” und nehmen Sie folgende Einträge vor:

APN

Der APN (Access Point Name) wird für die GPRS und UMTS-Einwahl benötigt. Sie erhalten ihn von Ihrem Provider. Der APN wird insbesondere zu administrativen Zwecken genutzt.

Der AT-Befehl
`at+cgdcont=1,"ip",`
ist Standard für die Übergabe des APN an die SIM-Karte, kann aber je nach Provider variieren.

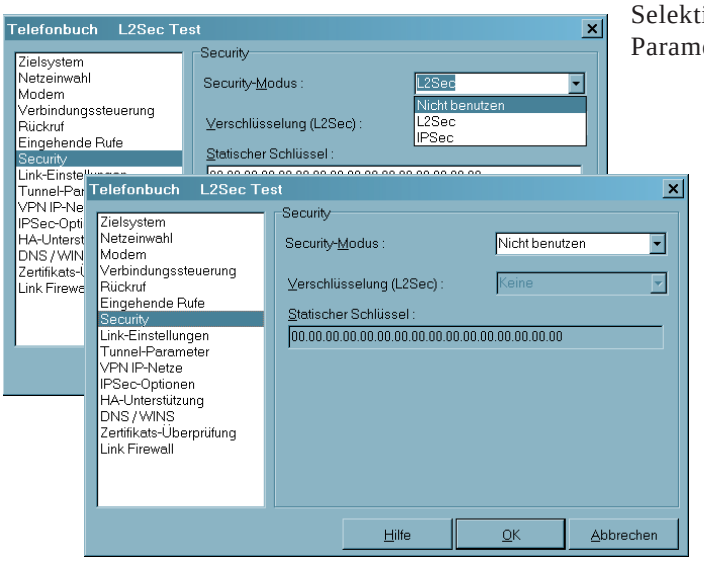
Der APN
`“internet.t-d1.de”`
variiert je nach SIM-Karte und gilt nur für die SIM-D1-Karte von T-Mobile.

SIM PIN AT-Befehl

Bei Verwendung einer GPRS/UMTS-Karte muss der jeweils spezifische AT-Befehl eingegeben werden. Dieses Kommando
`AT+CPIN=`
ist Standard und bewirkt, dass die SIM PIN richtig erkannt wird.

SIM PIN

Benutzen Sie eine SIM-Einsteckkarte für GPRS oder UMTS, so geben Sie hier die PIN für diese Karte ein. Benutzen Sie ein Handy, so muss diese PIN am Mobiltelefon eingegeben werden.



Selektieren Sie das Parameterfeld “Security”.

Security-Modus

Benutzen Sie für die Testverbindung keinen Security-Modus!

Wählen Sie “Nicht benutzen” und klicken Sie anschließend auf “OK”.

Speichern Sie die Telefonbucheinstellungen und öffnen Sie anschließend den Monitor.

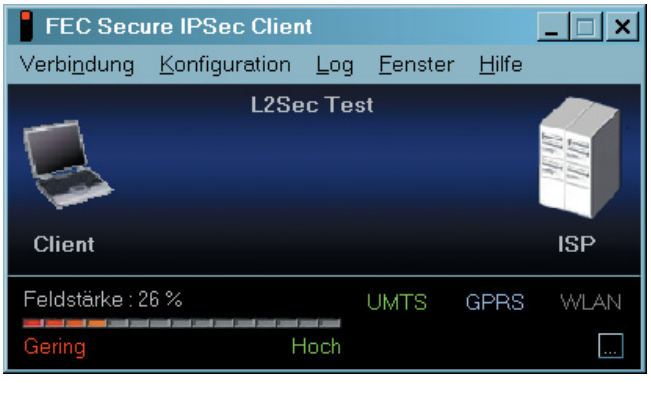
3. Der Monitor

Starten Sie den Monitor.

Der Monitor des VPN/PKI Clients (Enterprise Client) muss sich wie in nebenstehender Abbildung darstellen. Der Monitor des Entry Clients zeigt sich nur unwesentlich anders.

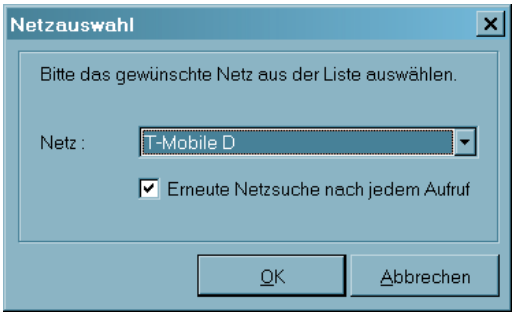
Zwischen dem grafischen Feld und der Button-Leiste muss die Feldstärke des Funknetzes angezeigt werden.

Wird die Feldstärke nicht angezeigt, erscheint eine Fehlermeldung, die auf einen Modemfehler hinweist. Fahren Sie in diesem Fall fort wie unter “1.1 Installation des Treibers” beschrieben wurde!



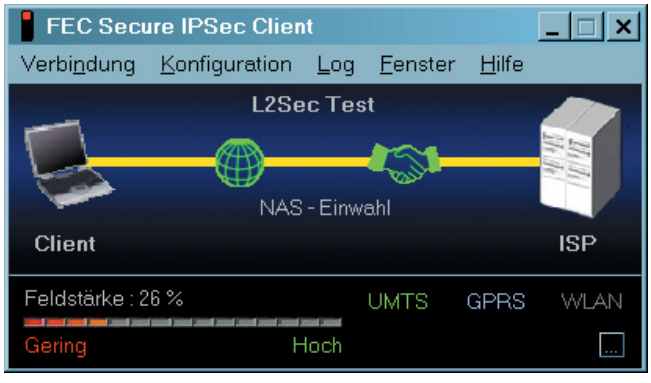
Die Karte sucht nach dem Start des Monitors automatisch nach einem Funknetz und zeigt es mit der entsprechenden Feldstärke an, sobald es gefunden wurde (in der Abbildung links “T-Mobile D”).

Wird das Netz angezeigt, kann durch Klick auf den [...]-Button eine erneute Netzsuche ausgelöst werden.



Nach Netzsuche nach einem alternativen Netz wird das Fenster zur Netzauswahleingeblendet (links). Das gewünschte Netz kann aus einer Liste ausgewählt werden.

Wird die erneute Netzsuche nach jedem Aufruf des Monitors nicht gewünscht, so muss die standardmäßig aktive Funktion über den Check-Button ausgeschaltet werden.



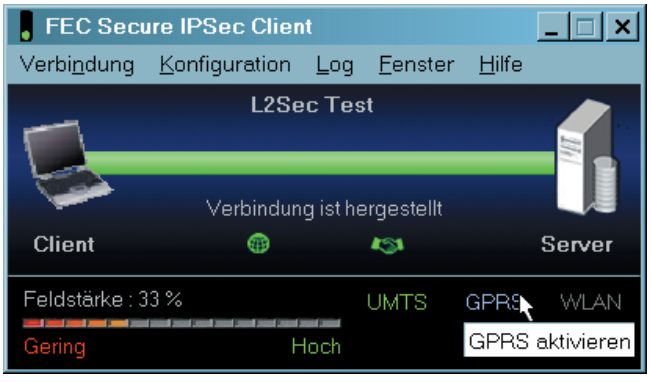
Der Verbindungsaufbau kann genauso erfolgen wie bei einem Festnetz (vgl. im Handbuch zur Client Software “Verbindungsaufbau”), alternativ mit den Modi “automatisch, manuell oder wechselnd”.

Die Verbindungsart wird grün eingefärbt (links “UMTS”).

Wenn die Verbindung steht, kann wie im lokalen Firmennetz gearbeitet werden.

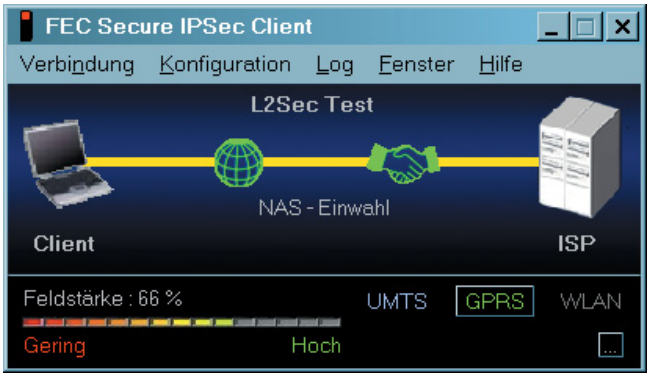
Dies gilt auch für den Fall, dass die Karte bei zu geringer Feldstärke automatisch vom Verbindungsmedium UMTS auf GPRS wechselt. Da in diesem Fall die Verbindung bestehen bleibt.

Erhöht sich die Feldstärke wieder, schaltet die Karte automatisch wieder zurück.



Das Verbindungsmedium kann auch manuell gewechselt werden. Dazu wird mit der Maus das gewünschte Medium angeklickt, im Bild links “GPRS aktivieren”.

Bei einem manuellen Wechsel des Mediums wird die Verbindung jedoch zunächst abgebaut.

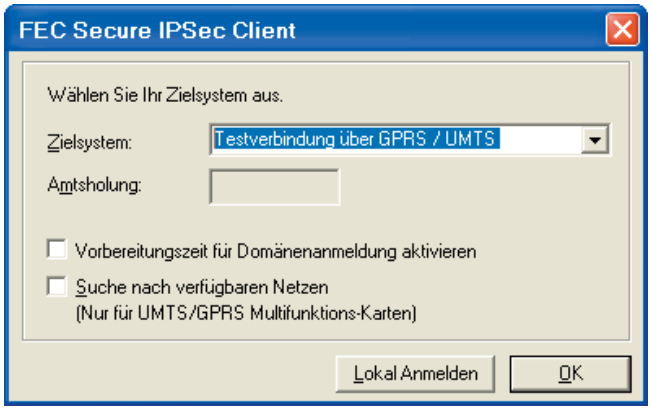


Die Verbindung wird dann wieder automatisch aufgebaut, wenn dies für den Verbindungsaufbau im Telefonbuch konfiguriert wurde.

4. Domänenanmeldung mit NCP Gina

Die Client Software wird bereits in der Boot-Phase im Hintergrund gestartet und fängt den Call “Crtl-Alt-Delete” ab.

Die integrierte Personal Firewall der NCP Software ist zu diesem Zeitpunkt bereits aktiv, sodass der PC bereits geschützt ist.

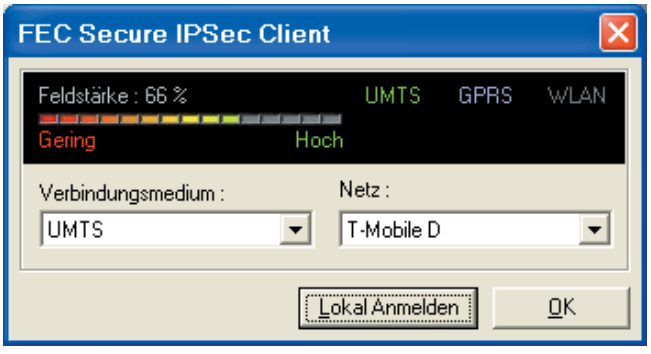


Bereits während der Boot-Phase kann das Zielsystem, das für das Verbindungsmedium GPRS/UMTS konfiguriert wurde, selektiert werden.

(Die Funktion “Vorbereitungszeit für Domänen-Anmeldung aktivieren” wird nur benötigt, wenn vorher keine ordnungsgemäße Abmeldung erfolgte! Die “Suche nach verfügbaren Netzen” nimmt einige Sekunden in Anspruch und ist in der Regel nur im Ausland von Bedeutung. Vorbereitungszeit für die Domänenanmeldung kann bei Bedarf verlängert werden.)

Bitte beachten Sie zu den möglichen Einstellungen die Beschreibung der Logon-Optionen im Handbuch des Clients!

Die SIM-PIN muss nur dann eingegeben werden, wenn sie in der Konfiguration des Zielsystems (Profils) im Parameterfeld “Modem” im Telefonbuch noch nicht eingegeben wurde oder die abgespeicherte PIN nicht zur aktuell eingesetzten SIM passt.



Anschließend werden die Signale der Karte angezeigt, nach der Netzsuche das gefundene Funknetz mit der jeweiligen Feldstärke.

Wurde die Suche nach alternativen Netzen aktiviert, so kann ein anderes Netz, wie auch ein anderes Verbindungs-medium manuell gewählt werden.

Danach klicken Sie auf “OK”, um in der Domänenanmeldung fortzufahren.

(Mit “Lokal Anmelden” brechen Sie den Dialog zur Domänenanmeldung ab.)

Wurde für diese Verbindung die Nutzung eines Zertifikats konfiguriert, muss an dieser Stelle dessen PIN eingegeben werden.

Anschließend klicken Sie auf “OK”.

Damit wird die Verbindung hergestellt und ein Tunnel in das Firmennetz der Zentrale hergestellt.

Je nach Konfiguration im Monitormenü unter “Konfiguration / Logon-Optionen” erfolgt das weitere Vorgehen.

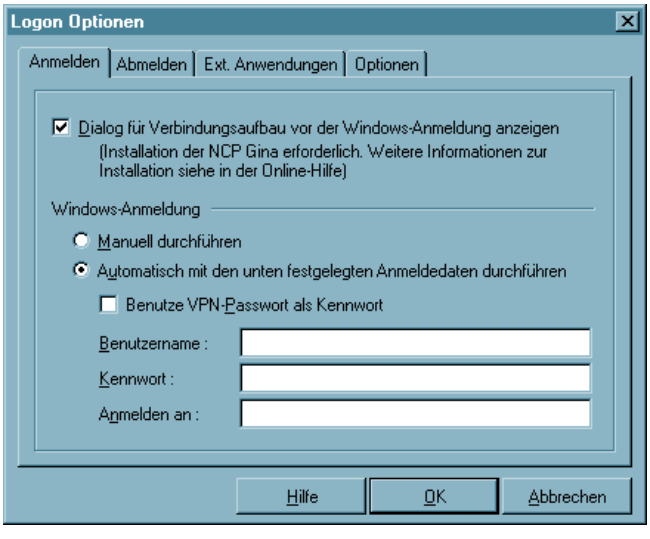
1. Der Benutzer gibt wie in der Standard Windows-Anmeldung die gefragten Anmeldedaten manuell ein (siehe in der Abbildung unten “Standard Windows-Anmeldung”)

2. Die Client Software übergibt die gefragten Anmeldedaten automatisch in diese Maske (der MS-GINA), sodass der Benutzer für das Windows Logon keine Eingaben mehr machen muss. Dazu muss in den Logon-Optionen “Gespeicherte Anmeldedaten verwenden” aktiviert sein und die Daten in den Feldern eingetragen sein.

4.1 Logon-Optionen

Die Logon-Optionen werden über das Monitormenü “Konfiguration” selektiert.

Bitte beachten Sie zu den möglichen Einstellungen die ausführliche Beschreibung der Logon-Optionen im Handbuch des Clients!



Anschließend können Sie wählen, ob über den “Dialog für Verbindungsaufbau vor der Windows-Anmeldung” an einer remote Domain die Verbindung von der Client-Software zum Gateway aufgebaut werden soll. Für die Verbindung zum Gateway müssen ggf. die PIN für das Zertifikat, wie auch für die SIM-Karte und das (nicht gespeicherte) Passwort für die Netzeinwahl bereits vor dem Passwort für das Windows Logon eingeben werden.

Beachten Sie desweiteren:

Aktivieren Sie diesen Dialog nicht, so findet die Passwort- und PIN-Abfrage für das Client Logon erst nach dem Windows Logon statt.

Findet der Verbindungsaufbau vor dem Windows Logon statt, erfolgt die Anmeldung an der remote Domäne bereits verschlüsselt.

Wenn Sie die Logon-Option mit Rückruf nutzen, muss “Verhandle PPP Callback” aktiviert werden (siehe →“Ruckruf”).

Nach jeder Änderung der Logon-Optionen im Monitor muss der Rechner gebootet werden.

Diese Funktion kann nur mit Administratorrechten aktiviert werden!

5. Log-Dateien

Ist eine Multifunktionskarte für UMTS/GPRS installiert, wird eine Log-Datei mit folgenden Spalten ins Log-Verzeichnis des Secure Clients geschrieben:

1. Spalte: Zeit

2. Spalte: Aktuelle Feldstärke

3. Spalte: Durchschnittliche Feldstärke der letzten Minute

4. Spalte: Durchschnittliche Feldstärke der letzten 5 Minuten

5. Spalte: Durchschnittliche Feldstärke der letzten 10 Minuten

6. Spalte: Aktueller Netztyp (UMTS oder GPRS)

7. Spalte: Aktuelles Netz

Alle 10 Sekunden wird ein Eintrag erstellt, jedoch nur alle 5 Minuten die Einträge in die Datei geschrieben.
Für jeden Tag wird eine Log-Datei mit dem Namen “mfc<DATUM>.log” erstellt.
Es werden die Log-Dateien der letzten 7 Tage gespeichert.

Anhang zu
FEC Secure IPSec Client:

Dienste und Applikationen des Clients

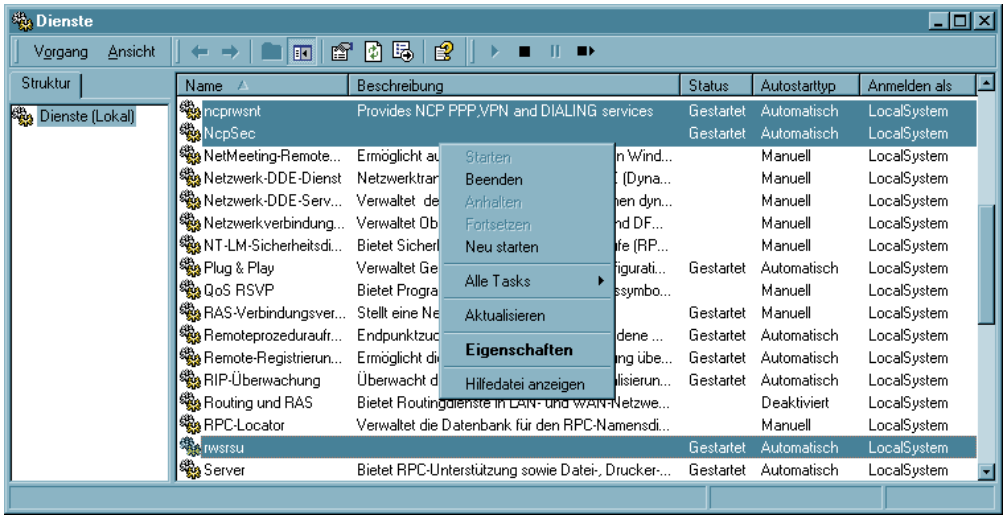
Wie Sie Funkwerk Enterprise Communications erreichen:
Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

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

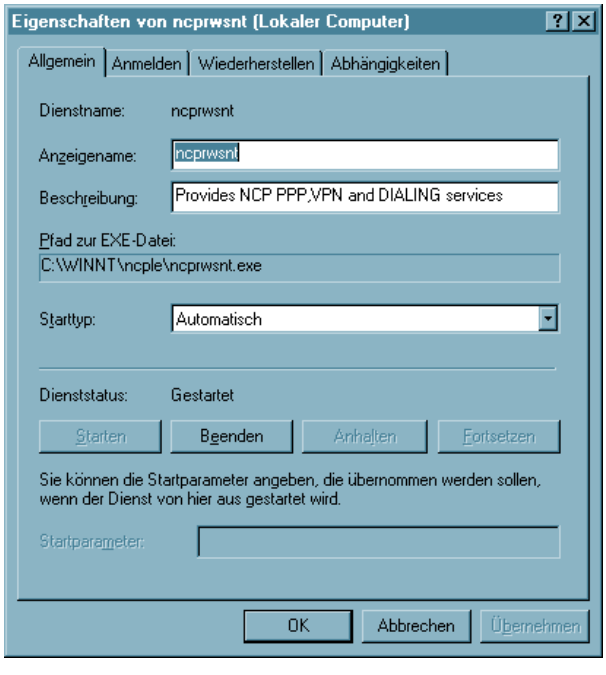
Inhalt

1. Dienste und Applikationen des Clients

In der Diensteübersicht des Windows-Systems (im Windows-Startmenü unter “Einstellungen – Systemsteuerung – Verwaltung – Dienste”) können die Dienste ncpsec.exe, ncprwsnt.exe und rwsrsu.exe aufgesucht werden (Bild unten, Die Dienste sind in der Abbildung eingefärbt).



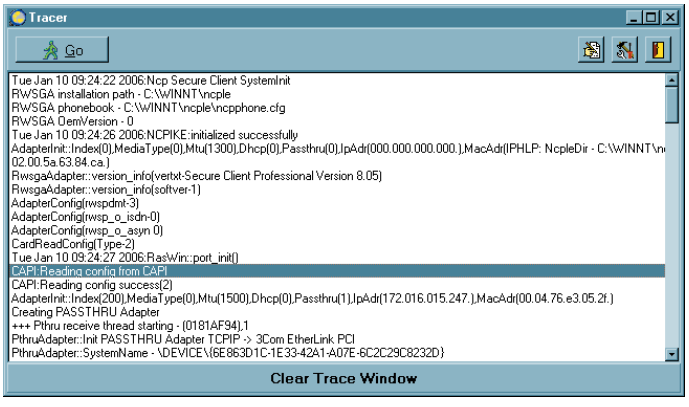
Von dieser Windows-Oberfläche können die Eigenschaften der Dienste abgelesen werden (Bild unten), bzw. die Dienste gestoppt oder gestartet werden..



Alle Dienste des Secure Clients werden nach der Installation der Software automatisch aus dem Installationsverzeichnis gestartet.

Zusätzlich zu den Diensten befinden sich außerdem auch Applikationen im Installationsverzeichnis:

ncptrcw.exe



Trace-Monitor; kann auch gestartet werden über “Windows – Programme – Secure Client Tracer”. Dies ist ein eigenes Anwendungsprogramm für qualifizierte Systemtechniker. Mit seiner Hilfe können z.B. Traces zur Fehlersuche erstellt werden. Der Tracer ist nicht für den normalen Benutzer gedacht!

ncpmon.exe

startet den Client-Monitor; kann gestartet werden durch Doppelklick auf das Ampelsymbol in der Task-Leiste oder über “Windows – Programme – Secure Client Monitor”. Die Handhabung und die Menüführung zum Monitor ist ausführlich im Handbuch zum jeweiligen Secure Client beschrieben.

ncpike9x.exe

IKE-Protokoll für Windows 95/98

ncpike.exe

IKE-Protokoll für Windows 2000/XP

lbtrace.exe

Tracer auf Treiberebene für virtuellen NCP-Adapter.

inst95.exe

Installationsprogramm für Windows 95/98

insrnt5.exe

Installationsprogramm für Windows 2000/XP

uninst.exe

Mit diesem Programm kann unter Umgehung der Windows Software-Verwaltung der Secure Client deinstalliert werden.

3monapl.exe

Feldstärkenanzeige für UMTS/GPRS bei Nutzung einer Multifiunktionskarte.

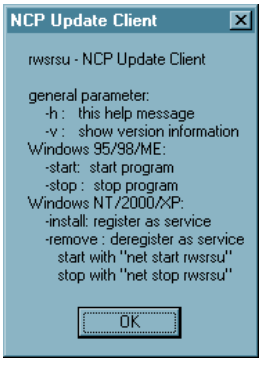
ncpauth.exe

dient der Http-Authentisierung

ncprwsnt.exe

Zuständig für das Frame Processing der Datenkommunikation über NCP PPP und VPN, sowie die Wähldienste.

rwsrsu.exe



Update Client; korrespondiert mit dem Programm ncprsu.exe am Management Server, siehe →unten

rwsrsuhlp.exe

Hilfeprogramm für rwsrsu.exe; wird gestartet mit:
`rwsrsu -h`

ncprndll.exe

Wird vom Update Client genutzt und ruft eine DLL auf, die die Dienste des Clients im Update-Fall stoppt bzw. wieder startet.

ncpbudgt.exe

Budget Manager, siehe →unten

ncpmsg.exe

Korrespondiert mit dem Budget Manager und öffnet, sofern im Client-Monitor konfiguriert, das Meldungsfenster mit der entsprechenden Warnung für den Benutzer.

rwscmd.exe

Kommandozeilen-Schnittstelle, siehe →unten

ncppopup.exe

Programm zur Eingabe von Lizenzdaten und Darstellung der Software-Version; kann gestartet werden über “Windows – Programme – Secure Client Popup”.

ncpsec.exe

PKI-Modul der Client Software; dieses Programm wird nur bei Einsatz von digitalen Zertifikaten benötigt. Die Konfiguration von Chipkartenlesern und Soft-Zertifikaten ist ausführlich im Handbuch des jeweiligen Secure Clients im Abschnitt “Monitor” beschrieben.

ncpepsec.exe

Modul für die Endpoint Security zwischen Secure Client und VPN Gateway; die Policies für die Endpoint Security werden am Secure Enterprise Management mit dem Plug-In “Endpoint Policy Enforcement” konfiguriert. Die Erzwingung der Endpoint Sicherheits-Richtlinien (Endpoint Policy Enforcement) ist deshalb nur möglich, wenn das NCP Secure Enterprise Management eingesetzt wird. Nur mit diesem zentralen Management Tool können die Sicherheits-Richtlinien allen Endpunkten der eingesetzten Komponenten gleichermaßen zugeteilt werden. Während die Endpoint Sicherheits-

Richtlinien vom Enterprise Management ausgegeben werden, muss der Download der Sicherheits-Richtlinien (die der Management Server vorschreibt) am VPN Gateway aktivieert werden. Dies erfolgt am Secure Server Manager im Konfigurationszweig “Client Policy Enforcement”. Ist die Endpoint Security aktiviert, so erfolgt der Abgleich und der Download der aktuellen Policies über das Programm ncpepsec.exe.

Folgende Dienste und Applikationen sind weiter unten ausführlicher beschrieben:

ncpbudgt.exe
rwscmd.exe
ncprwsnt.exe

1.1 Übersicht der Ports des Clients

bei Win2000/XP:

ncpmon.exe	10544
ncpsec.exe	10522, 10542
ncprwsnt.exe	1701, 500, 10523, 10530, 10550, 10600, 10610
rwsrsu.exe	Dynamischer Port nach 12501 (Management Server)

bei 98/ME:

ncpmon.exe	10544
ncpbudgt.exe	10522, 10542
ncpike9x.exe	1701, 500, 10523, 10530, 10550, 10600, 10610
rwsrsu.exe	Dynamischer Port nach 12501 (Management Server)

Weitere Ports:

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

2. ncpbudgt.exe – Budget-Manager (Verbindungssteuerung/Verbindungsstatistik)

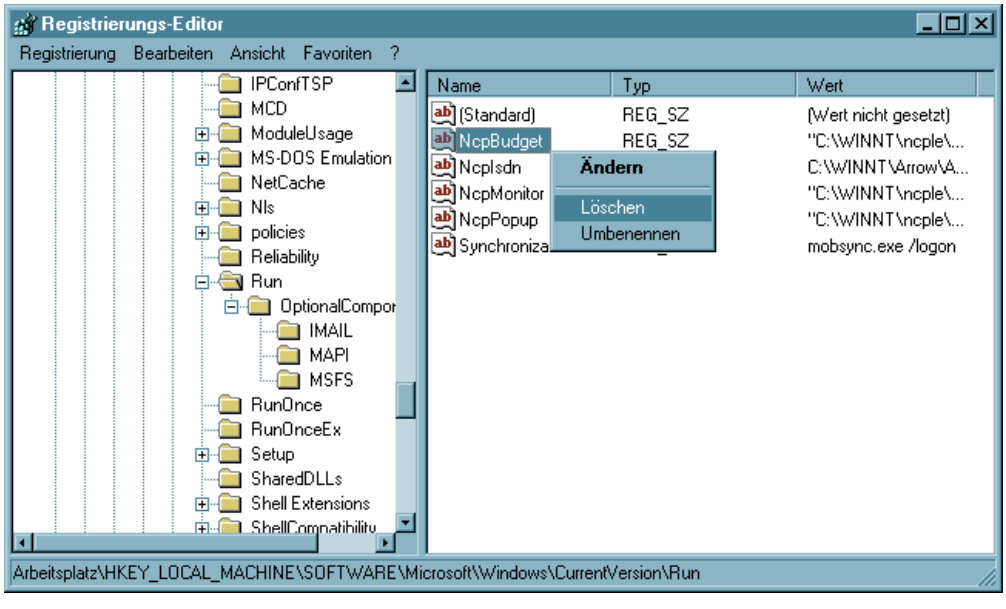
Nach der Installation der Client Software läuft der sogenannte Budget-Manager für Verbindungssteuerung und -statistik automatisch bei Start des Monitors mit.

Der Budget-Manager hat die Aufgabe, Verbindungen der Client Software nach genau definierten Kriterien zu überwachen.

Diese Kriterien werden im Monitormenü unter “Konfiguration / Verbindungssteuerung” festgelegt. (Siehe auch Handbuch zum Secure Client, Monitor, Verbindungssteuerung)

Die Verbindungssteuerung im Monitormenü zu aktivieren ist nur dann sinnvoll, wenn die Verbindungen nicht zu einem Gateway des Firmennetzes führen oder wenn für die Verbindungen Gebühren für Verbindungszeit oder -häufigkeit anfallen. Ansonsten kann das Gebühren-Management zentral administriert werden.

Wird der Budget-Manager nicht genutzt, so kann er aus der Registry entfernt werden (siehe Bild unten). Dabei ist darauf zu achten, dass er bei einem Update oder einer Neuinstallation automatisch wieder installiert wird. Danach muss er erneut mit regedit gelöscht werden.



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

3. rwscmd.exe – Kommandozeilen-Schnittstelle

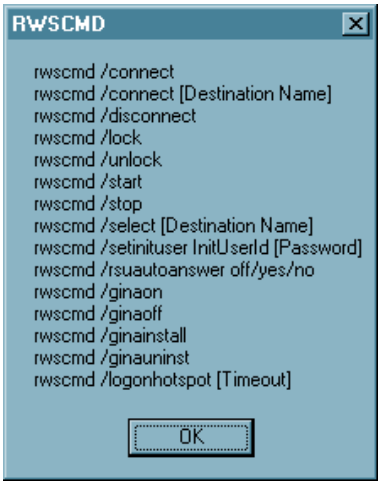
Achtung! Die folgende Beschreibung gilt nur für Windows-Systeme.

3.1 Übergabe von Kommandos an den Client

Der Client verfügt mit rwscmd.exe über eine Kommandozeilen-Schnittstelle, die für andere Anwendungen genutzt werden kann. Voraussetzung für die Nutzung des Programms rwscmd.exe ist eine Client Software, die mindestens den Stand 7.0 (Enterprise Client) bzw. 8.0 (Entry Client) hat.

Bei der Installation wird der Kommandozeileninterpreter in das ncple-Verzeichnis unter Windows kopiert. Der Aufruf erfolgt aus diesem Verzeichnis (z.B.):

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



Wird die Syntax beim Aufruf nicht eingehalten oder ein Kommando falsch oder unvollständig angegeben, so erscheint ein Fenster, in dem die möglichen Kommandos aufgelistet sind:

```
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 Voraussetzung für die Nutzung des Programms

- ☐ Die Dienste ncprwsnt, ncpsec und rwsrsu müssen gestartet sein. Diese Dienste werden nach der Installation der Client Software standardmäßig gestartet – sie befinden sich im Verzeichnis
  `C:\Windows\ncple>`

- ☐ Der Monitor muss nur gestartet werden, wenn Passwörter oder Pin-Eingaben erforderlich sind, da rwscmd.exe keinen PIN-Dialog startet.

- ☐ Weiterhin müssen Schreibrechte bestehen auf den Registrykey:
  `KEY_LOCAL_MACHINE\`
  `Software\NCP engineering GmbH\NCP Enterprise Monitor`

3.3 Beschreibung der Kommandos

`rwscmd /connect`
Erforderliche Windows Berechtigung: User Rechte
Beschreibung: Verbindungsaufbau mit dem zuletzt im Monitor gesetzten Zieleintrag.

`connect [Destination Name]`
`z.B.: rwscmd /connect "LAN via Router (IP)"`
Erforderliche Windows Berechtigung: User Rechte
Beschreibung: Verbindungsaufbau mit dem übergebenen Zieleintrag.

Die Hochkommas werden statt der eckigen Klammern gesetzt. Sie sind notwendig, da es sich um eine Übergabe mit Leerzeichen handelt.

`rwscmd /disconnect`
Erforderliche Windows Berechtigung: User Rechte
Beschreibung: Trennt die aktuelle Verbindung.

`rwscmd /lock`
Erforderliche Windows Berechtigung: User Rechte
Beschreibung: Sperrt den Client, kein Verbindungsaufbau mehr möglich

`rwscmd /unlock`
Erforderliche Windows Berechtigung: User Rechte
Beschreibung: Entsperrt den Client, setzt die durch Lock gesetzte Sperre zurück

`rwscmd /start`
Erforderliche Windows Berechtigung: Administrator Rechte
Beschreibung: Startet alle Dienste, Popup und Monitor des Clients

Bei erneutem Aufruf kommt der Hinweis “Secure Client ist bereits geöffnet”.

`rwscmd /stop`
Erforderliche Windows Berechtigung: Administrator Rechte
Beschreibung: Stoppt alle Dienste und den Monitor des Clients

Zu beachten ist außerdem, dass, wenn das Kommando rwscmd /stop ausgeführt wurde, danach das Kommando rwscmd /start ausgeführt werden muss, damit die Dienste und der Monitor wieder gestartet werden. Ein Reboot genügt in diesem Fall nicht, da das Popup und der Monitor nicht gestartet werden.

`rwscmd /select “Destination Name”`
Erforderliche Windows Berechtigung: User Rechte
Beschreibung: Im Secure Client wird auf das gewünschten Ziel gewechselt.

Die Hochkommas werden statt der eckigen Klammern gesetzt. Sie sind notwendig, da es sich um eine Übergabe mit Leerzeichen handelt.

`rwscmd /setinituser UserId “Passwort”`
Erforderliche Windows Berechtigung: Administrator Rechte
Beschreibung: Soll kein Fenster bei der Initialverbindung angezeigt werden, kann die User Id des Benurzers für die Erstanmeldung und optional das Passwort für den Initprozess übergeben werden.

Die Hochkommas werden statt der eckigen Klammern gesetzt. Sie sind notwendig, da es sich um eine Übergabe mit Leerzeichen handelt.

`rwscmd /rsuautoanswer off/yes/no`
Erforderliche Windows Berechtigung: Administrator Rechte
Beschreibung: Hier wird eingestellt, wie bei Anfragen nach einem Softwareupdate reagiert wird.

yes	Client Software erhält automatisch ohne Nachfrage ein Update.
no	automatisches Software Update wird abgelehnt und nicht ausgeführt.
off	Bei der Einstellung off wird in einem Meldungsfenster nachgefragt, ob die Software aktualisiert werden soll.

`rwscmd /ginainstall`
Erforderliche Windows Berechtigung: Administrator Rechte
Beschreibung: Installiert die NCP Gina, sofern dies noch nicht bei der Software-Installation geschehen ist (vergleiche im Client-Handbuch den Abschnitt “Installation”).

`rwscmd /ginaunins`
Erforderliche Windows Berechtigung: Administrator Rechte
Beschreibung: Deinstalliert die NCP Gina. Sollte die NCP Gina von einer fremden Gina aufgerufen werden, so ist die Deinstallation mit diesem Kommando nicht möglich. In diesem Fall muss die Entfernung aus der Registry manuell vorgenommen werden, oder die Ginas in umgekehrter Reihenfolge der Installation wieder deinstalliert werden (vergleiche im Client-Handbuch den Abschnitt “Logon Optionen”).

`rwscmd /ginaon`
Erforderliche Windows Berechtigung: Administrator Rechte
Beschreibung: Schaltet die NCP Gina-Dialoge zur Anmeldung an das VPN Gateway sichtbar, sofern die NCP Gina installiert wurde.

`rwscmd /ginaoff`
Erforderliche Windows Berechtigung: Administrator Rechte
Beschreibung: Schaltet die NCP Gina-Dialoge unsichtbar und überspringt damit die VPN Gateway-Anmeldung mit der NCP Gina.

`rwscmd /logonhotspot [Timeout]`
Soll über einen externen Dialer eine Hotspot-Anmeldung erfolgen, kann mit diesem Befehl die Firewall für die Ports 80 (HTTP) und 443 (HTTPS) freigeschaltet werden. Damit wird eine dynamische Regel erzeugt, die den Datenverkehr zulässt, bis der übergebene Timeout (in Sekunden) abgelaufen ist.

Weil damit über die Kommandozeile die Firewall freigeschaltet werden kann, wurde in den Firewall-Einstellungen unter “Optionen” der Parameter “Hotspot-Anmeldung für externe Dialer zulassen” hinzugefügt. Erst wenn dieser aktiviert ist, kann der Befehl über rwscmd ausgeführt werden. (Siehe dazu →Konfigurationsparameter / Telefonbuch, Firewall-Einstellungen).

4. ncprwsnt.exe

Zuständig für das Frame Processing der Datenkommunikation über NCP PPP und VPN, sowie die Wähldienste.

Mit diesem Dienst können automatisch Anwendungen nach einem Verbindungsauf- oder -abbau gestartet werden, die Systemrechte benötigen. Dazu müssen im Installationsverzeichnis zwei Batch-Dateien editiert werden:

connect.bat

In der Batch-Datei mit genau dieser Schreibweise werden die ausführbaren Programme oder Batch-Dateien eingetragen, die nach einem Verbindungsaufbau ausgeführt werden sollen.

disconnect.bat

In der Batch-Datei mit genau dieser Schreibweise werden die ausführbaren Programme oder Batch-Dateien eingetragen, die nach einem Verbindungsabbau ausgeführt werden sollen.

Beachten Sie dazu auch den Parameter “Ausführung von ”(dis)connect.bat" nicht zulassen". Er befindet sich im Monitormenü “Verbindungssteuerung / Ext. Anwendungen” unter dem Menüpunkt “Konfiguration”.

Diese Funktion sollte immer aktiviert sein, wenn nicht unbedingt für eine gewünschte Anwendung die Ausführung der genannten Batch-Dateien mit Administrator-Rechten erforderlich ist.

Die Anwendungen (Batch-Dateien) für deren Ausführung Benutzerrechte genügen, können aus eben diesem Monitormenü “Konfiguration / Verbindungssteuerung/ Ext. Anwendungen” gestartet werden, indem sie dort direkt eingetragen werden (siehe → Client-Monitor / Verbindungssteuerung).