NCP
SECURE COMMUNICATIONS

Funktionsbeschreibung und Konfiguration

Mobile Computing mit Enterprise Clients

Mobile Computing

mit dem Secure Enterprise Client

NCP Hotline auf Abruf

Sie erreichen unsere NCP Experten unter folgenden Hotlines:

Kunden mit Hotline Service Vertrag
Sie erhalten sofortigen Support unter der vertraglich angegebenen Rufnummer.
Ihnen steht das komplette Serviceportfolio zur Verfügung.

Kunden ohne Hotline Service Vertrag
Sie können wählen zwischen:
Kostenpflichtige Service-Rufnummer 09001996800 (-,80 Euro / Minute)
E-Mail an support@ncp-e.com

Dienstleistungsauftrag (Berechnung nach Aufwand)
mit festen Reaktionszeiten und Zusatzservices.
Bitte nutzen Sie zur Anfrage das NCP Service-Formular von der Website
http://www.ncp-e.com/de/service-support/support.html

Sie möchten mehr über den NCP Hotline Service Vertrag wissen?
Bitte senden Sie eine E-Mail an:
vertrieb@ncp-e.com

Network
Communications
Products engineering GmbH

Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet http:// www.ncp-e.com
E-mail: info@ncp-e.com

Copyright

Mobile Computing mit Enterprise Clients

Im ersten Teil dieses Dokuments ist die Konfiguration des Secure Clients für den Fall beschrieben, dass eine Multifunktionskarte für das Verbindungsmedium GPRS / UMTS eingesetzt wird.

Im zweiten Teil werden WLAN-Konfiguration und Einstellungsmöglichkeiten für die Hotspot-Anmeldung via Funknetz insbesondere mittels WISPr-Protokoll beschrieben.

Inhaltsübersicht

Wie die Profil-Einstellungen über den Menüpunkt “Profile” im Konfigurationmenü des Monitors vorgenommen werden können, ist in der Dokumentation **Enterprise Client Parameter** beschrieben.

Eine Übersicht bietet der **Enterprise Client-Navigator**. In dieser PDF-Datei sind alle aktuell verfügbaren Dokumente zu Ihrem Produkt verzeichnet.

Vom Navigator aus können Sie alle relevanten Dokumente direkt anspringen und – falls sie noch nicht in Ihrem Navigatorverzeichnis gespeichert sind – von der NCP Homepage herunterladen.

Multifunktionskarte

Wird eine Mobilfunkdatenkarte (GRPS / UMTS / HSDPA / HSUPA) eingesetzt, so können mit der Client Software spezielle Features des Mobile Computings unter Einbeziehung der Karteneigenschaften genutzt werden. Aufgrund der direkten Unterstützung einer Multifunktionskarte durch den Secure Client kann die Installation einer Management-Software von der eingesetzten Karte entfallen.

Der NCP Secure 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 Verbindungsstatus der Feldstärke, des selektierten Netzes und Providers, beschrieben in der PDF-Datei **Enterprise Client Monitor**.

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.

Die mit Ihrer Client-Version unterstützten Multifunktionskarten können Sie der Kompatibilitätsliste entnehmen:

Ab der Version 9.02 Build 5 unterstützt der Secure Client nach Einspielen der Datei g3detect.dll neue PCMCIA-Funkkarten, die Sie bitte der neuesten Kompatibilitätsliste entnehmen unter:

```
http://www.ncp-e.com/de/
service-support/kompatibilitaeten/
mobile-connect-cards.html
```

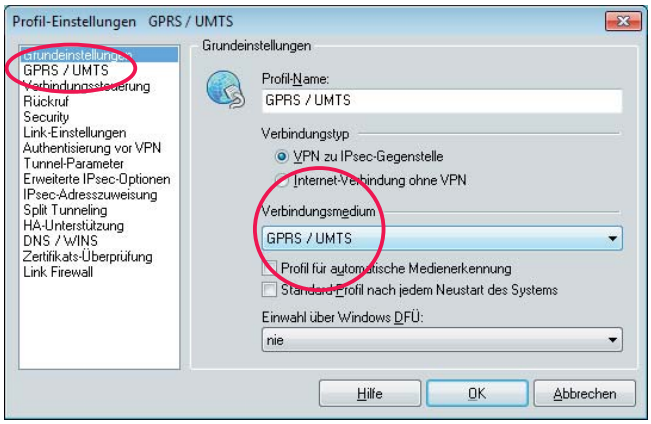
Bitte beachten Sie, dass Sie die Zugangsdaten Ihres Netzbetreibers benötigen:

– ggf. Benutzername, Passwort
– Zeichenfolge für Rufnummer (Ziel)
– Access-Point-Name (APN)
– SIM PIN
– PUK

Profil für Mobilfunkverbindung über UMTS / GPRS erstellen

Nach Installation der Multifunktionskarte und Aktualisierung der Client Software mit der Datei g3detect.dll, kann ein Profil erstellt werden, worin die Multifunktionskarte direkt als Modem angesprochen wird. So erstellen Sie das neue Link-Profil:

Grundeinstellungen



Profil-Name

Geben Sie dazu einen frei wählbaren Profil-Namen ein.

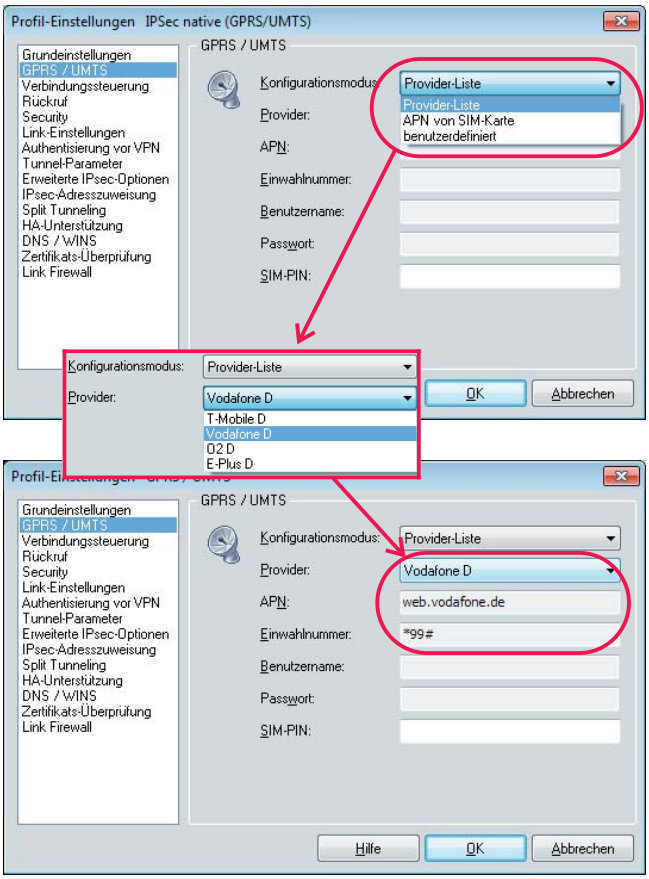
Verbindungsmedium

Selektieren Sie das Verbindungsmedium GPRS / UMTS (Abb. oben). Damit wird automatisch das Parameterfeld “GPRS / UMTS” in der Liste eingeblendet (Abb. oben).

GPRS / UMTS

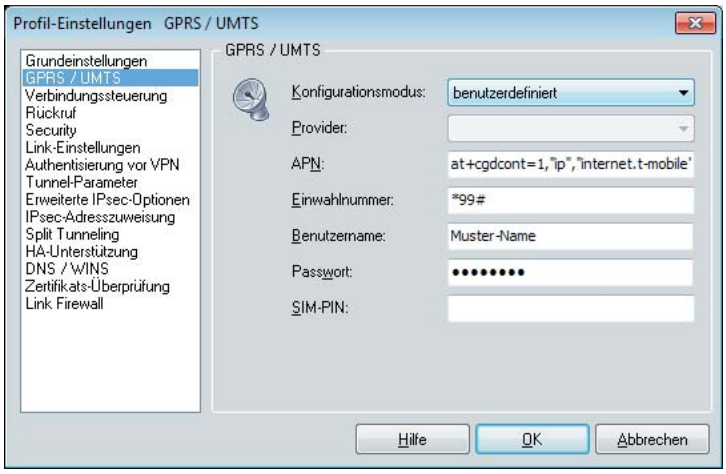
Öffnen Sie anschließend das Parameterfeld “GPRS / UMTS”. Hier stehen drei Konfigurationsmodi zur Auswahl:

In der Standardeinstellung (Abbildungen unten) kann aus einer **Provider-Liste** der gewünschte Anbieter ausgewählt werden. (Sollte Ihr Provider noch nicht aufgeführt sein, so können Sie die Liste mit den Daten zu Ihrem Provider erweitern; sie befindet sich als APN.INI-Datei im Installationsverzeichnis).



Im zweiten Modus wird der **APN aus der SIM-Karte** gelesen (derzeit nur für T-Mobile) (Abb. unten).

Schließlich kann der **benutzerdefinierte** Konfigurationsmodus eingestellt werden (Abb. unten), wobei alle Daten manuell eingegeben werden müssen;



APN

Den APN (Access-Point-Namen) erhalten Sie von Ihrem Provider. Er kann auch manuell eingetragen oder aus der Provider-Liste gelesen werden. Für Vodafone lautet er “web.vodafone.de”, für T-Mobile “internet.t-d1.de”;

[Der String für den AT-Befehl
`at+cgdcont=1,"ip",`
ist Standard für die Übergabe des APN an die SIM-Karte. Die Fortsetzung des Strings variiert jedoch je nach Provider. Beispiele:

`at+cgdcont=1,"IP", web.vodafone.de`
APN für Vodafone

`at+cgdcont=1,"IP","internet.t-d1.de"`
APN für T-Mobile (SIM-D1-Karte)]

Benutzername / Passwort

Als Zugangsdaten für den Internetdienstanbieter (Mobilfunk-Provider) muss im Modus “APN von SIM-Karte” und im benutzerdefinierten Konfigurationsmodus ein beliebiger Benutzername und ein beliebiges Passwort (hier “Muster-Name”) (Fig. 4) eingegeben werden, es sei denn, Sie haben vom Provider spezielle Kennwörter erhalten. Bei Vodafone und T-Online genügen Dummy-Werte;

Einwahlnummer

Als “Einwahlnummer” muss je nach Funkkarte und Provider eine bestimmte Zeichenfolge eingegeben werden, die der Multifunktions-Karte (UMTS-Karte) mitteilt, welche Art Datenverbindung aufgebaut werden soll. Im Regelfall lautet diese *99# (sollte der Verbindungsaufbau nicht möglich sein, kontaktieren Sie die Hotline Ihres Mobilfunkanbieters); anschließend geben Sie die SIM-PIN ein;

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.

Die Abrechnung (und die Identifikation) erfolgt über die SIM-Karte.

Sollte die Möglichkeit der Eingabe vom Administrator gesperrt sein, so können Sie im SIM PIN-Dialog die **SIM PIN eingeben** und in der Konfiguration speichern lassen. Dieser Dialog erscheint immer wenn Sie ein Link-Profil mit dem Verbindungsmedium GPRS / UMTS selektieren bzw. über GPRS / UMTS eine Verbindung aufbauen.

Die Multifunktionskarte im Client Monitor

Beachten Sie auch folgende Leistungsmerkmale und Einstellungsmöglichkeiten des Secure Client Monitors.

Nachdem eine Multifunktionskarte installiert wurde, wird der Menüpunkt “Multifunktionskarte” im Verbindungsmenü des Monitors dargestellt. (Abb. oben)

Außerdem wird die GPRS / UMTS-Anzeige im Monitor eingeblendet sobald ein Profil mit Verbindungsmedium GPRS / UMTS für den Verbindungsaufbau selektiert wurde wie in Abbildung oben rechts. (Siehe auch **Symbole des Monitors**).

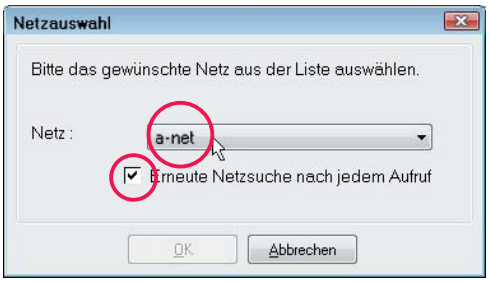
Netzsuche

Die installierte Multifunktionskarte sucht nach dem Öffnen der GPRS / UMTS-Anzeige automatisch nach einem Funknetz und zeigt es mit der entsprechenden Feldstärke an, sobald es gefunden wurde (“T-Mobile D” im Bild unten).

GPRS / UMTS-Anzeige

Bei zu geringer Feldstärke schaltet die Karte automatisch von der Datenübertragungstechnik UMTS auf GPRS, wobei die Verbindung bestehen bleibt. Erhöht sich die Feldstärke wieder, schaltet die Karte automatisch wieder zurück.

Durch Selektieren des Menüpunkts “Netzsuche” (Abb. oben links) oder mit einem Klick auf den [...]-Button (oben rechts) kann manuell eine Suche nach alternativen Netzen ausgelöst werden.



Wurde die Suche nach einem alternativen Netz durchgeführt, so wird ein Fenster zur Netzauswahl eingeblendet (oben). Das gewünschte Netz kann hier aus einer Liste ausgewählt werden.

Wird der Haken aus dem Fenster entfernt, so wird nach einem Klick auf den [...]-Button in der GPRS / UMTS-Anzeige die erneute Netzsuche nicht gestartet, sondern dieses Fenster erneut geöffnet. ausgeschaltet werden.

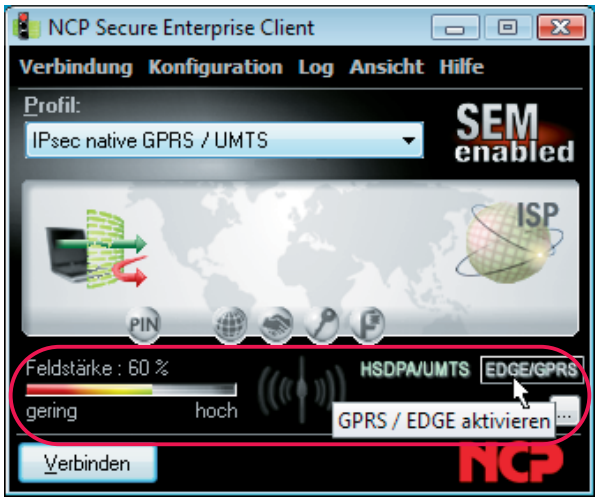
Der Verbindungsaufbau kann genauso erfolgen wie bei einem Festnetz, alternativ mit den Modi “automatisch, manuell oder wechselnd”.

Das aktuelle Verbindungsmedium wird in der GPRS / UMTS-Anzeige grün eingefärbt (unten 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.

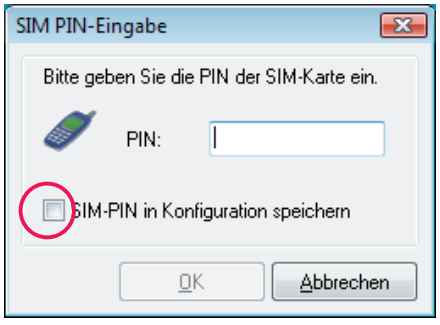
GPRS / UMTS aktivieren

Die Datenübertragungstechnik kann auch manuell gewechselt werden (Abb. unten). Dazu wird mit der Maus der Text mit der gewünschten Übertragungstechnik angeklickt oder dieser Menüpunkt gewählt. Bei einem manuellen Wechsel des Mediums wird die Verbindung zunächst abgebaut.



Die Verbindung wird dann wieder automatisch aufgebaut, wenn dies im Konfigurationsfenster **Verbindungssteuerung** konfiguriert wurde.

SIM PIN eingeben



Dieser Dialog zur Eingabe der SIM PIN erscheint automatisch bei einem Verbindungsaufbau, wenn die **SIM PIN** *noch nicht* gespeichert wurde.

Die nicht gespeicherte SIM PIN behält ihre Gültigkeit bis zum nächsten Boot-Vorgang.

SIM PIN in Konfiguration speichern
Über die Aktivierung dieser Funktion kann die SIM PIN auch dann in der Konfiguration gespeichert werden, wenn das Konfigurationsfenster GPRS / UMTS vom Administrator für Eingaben gesperrt wurde.

Beachten Sie dazu die **Konfigurations-Sperren des Enterprise Clients** in der Beschreibung **Secure Client Monitor**.

Über das Untermenü der Multifunktionskarte (vorige Seite) kann die **SIM PIN** bereits **vor dem Verbindungsaufbau** eingegeben werden ohne gespeichert zu werden.

SIM PIN ändern

Die Änderung der SIM PIN kann nur vorgenommen werden, wenn die bislang gültige SIM PIN korrekt eingegeben wird.

PUK Eingabe

Nach dreimaliger Falscheingabe der SIM PIN erscheint das Fenster zur Eingabe des PUK (Personal Unblocking Key), welcher der SIM-Karte beiliegt.

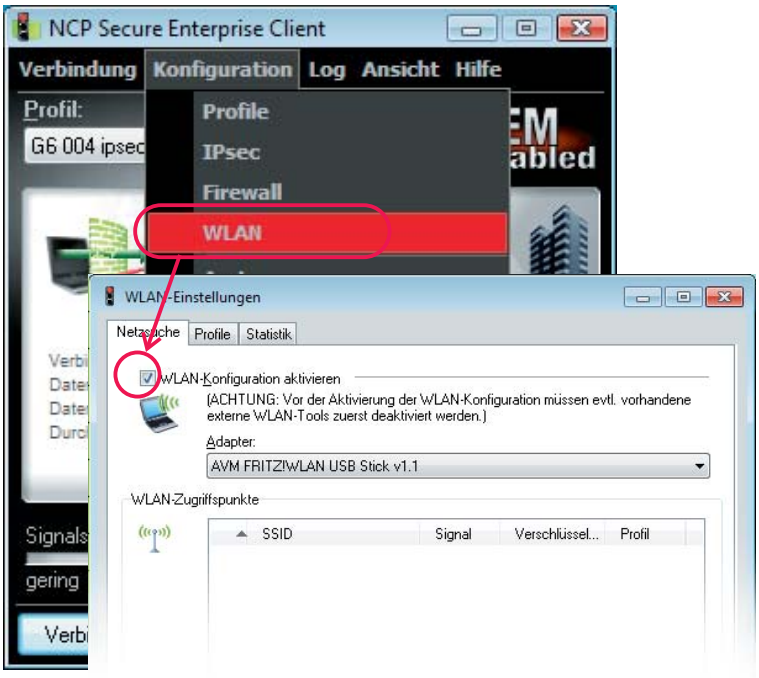
Nach korrekter Eingabe des PUK kann eine neue SIM PIN eingegeben werden.

Wireless LAN

Soll eine VPN-Verbindung des Clients zum Firmennetz über ein wireless LAN hergestellt werden, so wird in den Profil-Einstellungen des Clients das Verbindungsmedium **WLAN** eingestellt.

Für die Funknetzverbindung bis zum Access Point muss ein WLAN-Adapter installiert sein und am Client ein **WLAN-Profil** angelegt sein.

Nachdem der WLAN-Adapter betriebsbereit ist, starten Sie den Client Monitor. Im Konfigurationsmenü befindet sich der Menüpunkt WLAN (Abb. unten). Selektieren Sie diesen Menüpunkt, so können Sie das WLAN-Tool von NCP einschalten, indem Sie die "WLAN-Konfiguration aktivieren" (Abb. unten).



Dieses Management Tool wird als Tray Icon angezeigt (Abb. unten rechts). Es kann genauso eingesetzt werden wie übliche, dem WLAN-Adapter beigegebene Tools, hat darüber hinaus aber zusätzliche Leistungsmerkmale, insbesondere bezüglich der VPN-Verbindungen des Enterprise Clients.

Setzen Sie das NCP **WLAN Tool** ein, sollte ein konkurrierendes WLAN Tool über die Dienste-Verwaltung deaktiviert oder komplett entfernt werden.

WLAN-Status-Feld

Alternativ kann statt des Tray Icons auch der **WLAN-Status** über das Ansichtsmenü im Client Monitor angezeigt werden (Abb. oben). Mit einem Klick auf den WLAN-Button werden die WLAN-Einstellungen (siehe links mitte) geöffnet.

WLAN-Verbindung und WLAN-Profil

Eine Funknetzverbindung zu einem Access Point kann unabhängig von der VPN-Verbindung eines Link-Profils durch den Client aufgebaut werden, wenn ein WLAN-Profil für ein bestimmtes Funknetz erstellt wurde. Dieses WLAN-Profil wird für den Aufbau der Funknetz-Verbindung automatisch im Hintergrund verwendet, wenn Sie eine VPN-Verbindung zum Firmennetz herstellen und in dem eingesetzten VPN-Profil das Verbindungsmedium WLAN konfiguriert wurde. (Auch können mehrere WLAN-Profile in den WLAN-Einstellungen so konfiguriert sein, dass das jeweils passende über eine **WLAN-Automatik** für das aktuell verfügbare Funknetz ausgewählt wird. Siehe weiter unten.)

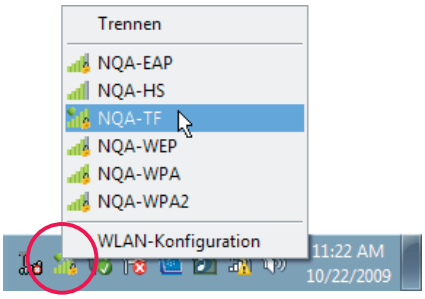
Bitte beachten Sie, dass Sie die Zugangsdaten für den WLAN Access Point und den Hotspot Ihres Netzbetreibers benötigen:

– SSID (Service Set Identifier)
– Verschlüsselung und Schlüssel
(Hotspot normalerweise unverschlüsselt)
– Benutzername, Passwort (für Hotspot-Anmeldung)

Verbindung zum WLAN-Zugriffspunkt und WLAN-Profil

Im folgenden ist beschrieben wie eine Verbindung zum WLAN Zugriffspunkt hergestellt wird – und sofern dies noch nicht möglich ist – wie ein WLAN-Profil, worin die Zugangsdaten zum Funknetz hinterlegt sind, mit dem internen WLAN Tool erstellt wird.

Sofern ein WLAN-Adapter installiert und die WLAN-Konfiguration aktiviert wurde, werden innerhalb weniger Sekunden die aktuell verfügbaren Funknetze gescannt.



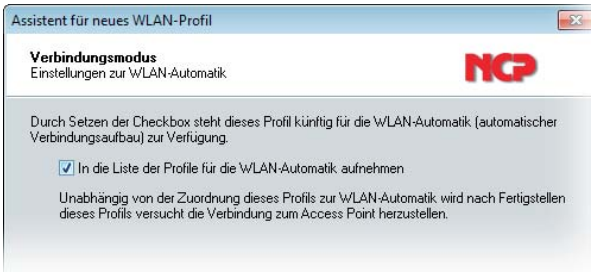
Mit einem Mausklick auf das Tray Icon werden die SSIDs der verfügbaren Netze angezeigt (Abb. links). Davor finden sich Symbole für die Signalstärke in einem Farbspektrum von grau bis grün. Funknetze mit zu schwacher Signalstärke werden grau dargestellt, Funknetze, über die eine WLAN-Verbindung zu einem Access Point sehr gut aufgebaut werden kann, werden grün dargestellt. Soll eine WLAN-Verbindung hergestellt werden, genügt ein Klick auf die SSID im Tray Icon.

Die Verbindung zum Access Point wird sofort aufgebaut und in der Statusansicht des Tray Icons angezeigt (Abb. links) wenn zu dieser SSID bereits ein WLAN-Profil hinterlegt ist.

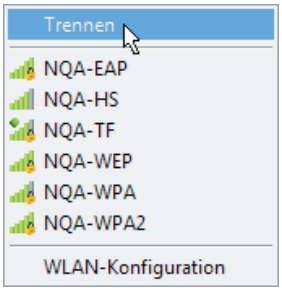
Assistent für WLAN-Profile

Existiert zur angeklickten SSID noch kein WLAN-Profil, wie nach einer Erstinstallation des Clients, so wird automatisch ein Assistent gestartet, mit dessen Hilfe das Profil in zwei Schritten hergestellt wird.

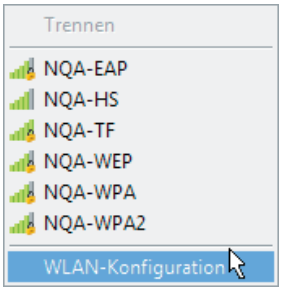
Im ersten Schritt muss dem WLAN-Assistenten nur der Schlüssel (den Sie von der Access Point-Verwaltung erhalten haben) übergeben werden. Die zweite Frage des Assistenten gibt Ihnen die Möglichkeit dieses WLAN-Profil zu einer später zu konfigurierenden **WLAN-Automatik** (Abb. rechts oben) hinzuzufügen. Unabhängig von der Zuordnung zur WLAN-Automatik wird nach einem



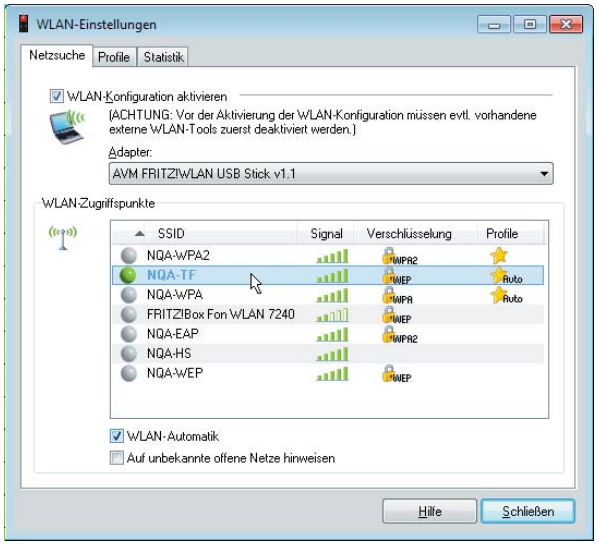
Mausklick auf “Fertigstellen” sofort versucht die Verbindung zum Access Point herzustellen.



Nachdem die Verbindung zum Access Point aufgebaut wurde, kann ein Klick auf den Menüpunkt “Trennen” (über der Liste der SSIDs) die WLAN-Verbindung wieder abbauen (Abb. links).



Ein Mausklick auf “WLAN-Konfiguration” (Abb. links) öffnet die WLAN-Einstellungen die vom Client für eine VPN-Verbindung übernommen werden können. Hier werden die SSIDs der gefundenen Funknetze mit Signalstärke und Verschlüsselungsart angezeigt. Außerdem sehen Sie, ob bereits ein WLAN-Profil zu diesem Netz existiert (mit einem Stern dargestellt) und ob dies für die WLAN-Automatik gespeichert wurde (Stern mit “Auto”) (Abb. unten).



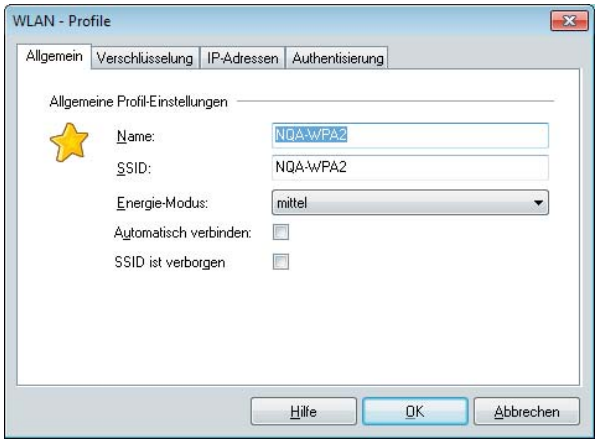
Per Mausklick auf ein selektiertes Profil kann die Verbindung zum Access Point aufgebaut oder getrennt werden (Abb. oben).

WLAN-Profile

Im WLAN-Profil sind die Zugangsdaten gespeichert und es legt fest wie eine Funkverbindung vom Client zu einem Access Point oder Hotspot hergestellt wird. Für jedes Funknetz können mehrere dieser Profile angelegt werden. Die WLAN-Konfiguration kann über das Tray Icon oder über das Konfigurationsmenü des Monitors mit Klick auf “WLAN” geöffnet werden.

Vier Konfigurationsfenster für die Einstellungen der WLAN-Profile stehen zur Verfügung:
– Allgemeine Profil-Einstellungen
– Verschlüsselung
– IP-Adressen
– Authentisieruung

Allgemeine Profil-Einstellungen



SSID

Die **SSID** wird nach einem Doppelklick auf das zu wählende Netz (*Beispiel: N1-HS*) bei einer neuen Profilerzeugung automatisch in das WLAN-Profil als **Name** und **SSID** übernommen, wenn zu diesem Netz noch kein Profil vorhanden war.

Name

Der Name kann nach belieben verändert werden, die SSID muss mit der des gescannten Netzes übereinstimmen.

Energie-Modus

Sofern der WLAN-Adapter dies gestattet, kann der Energie-Modus für ihn ausgewählt werden.

Automatisch verbinden

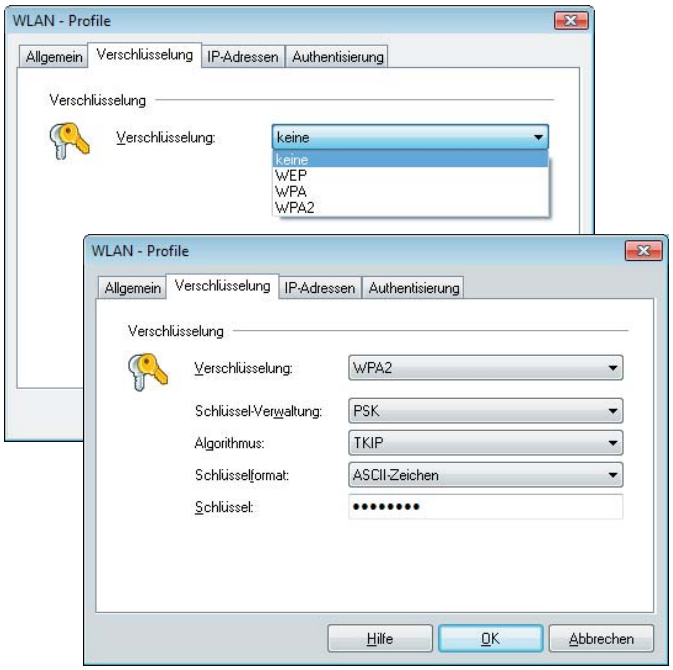
Wird für dieses Profil die Funktion “Automatisch verbinden” aktiviert, so wird es in der Profil-Liste für die WLAN-Automatik geführt und bei Bedarf automatisch ausgewählt. Siehe unten **WLAN-Automatik**.

SSID ist verborgen

Verborgene Netze werden ohne SSID angezeigt, d. h. sie können für eine Verbindung zum Access Point nicht nach der SSID selektiert werden.

Wenn Ihr WLAN als verborgenes konfiguriert ist, aktivieren Sie diese Funktion und geben dem manuell konfigurierten Profil einen Namen, den Sie später unter “Netzsuche” als Auswahlkriterium verwenden können.

Verschlüsselung



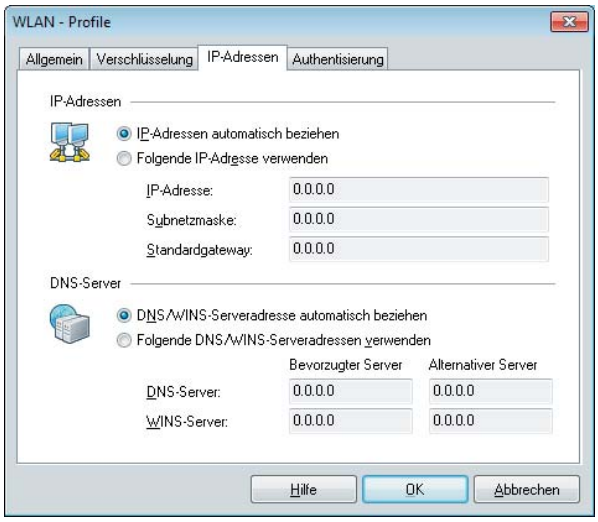
Der Verschlüsselungsmechanismus muss zu dem des Access Points passen und wird Ihnen vom Systemadministrator mitgeteilt. Standardeinstellung ist “keine”. Zur Verfügung stehen **WEP**, **WPA** und **WPA2** mit ihren jeweiligen Algorithmen und Schlüsselformaten.

Beachten Sie, dass unter Win XP ein Patch von Microsoft eingespielt werden muss, um WPA2 nutzen zu können.

Wird WPA mit EAP (TLS) genutzt, so müssen die **EAP-Optionen** im Konfigurations-Menü des Monitors aktiviert werden und ein Zertifikat konfiguriert sein. Beachten Sie dazu die PDF-Datei **Zertifikats-Konfiguration**.

IP-Adressen

Die hier gemachten Einstellungen zur IP-Adress-Konfiguration des WLAN-Adapters werden dann wirksam, wenn die WLAN-Konfiguration wie oben beschrieben aktiviert wurde. Standardeinstellung ist der automatische Modus unter Einsatz eines DHCP Servers.



Die hier eingetragene Konfiguration wird in die Microsoft-Konfiguration der Netzwerkverbindungen übernommen. (Siehe dort Netzwerkverbindungen / Eigenschaften von Internetprotokoll (TCP/IP)).

DNS Server

Die Adressen für DNS / WINS Server werden standardmäßig automatisch von einem DHCP Server bezogen. Einen DNS / WINS Server kann der WLAN-Adapter ggf. für die Namensauflösung des VPN Gateway-Namens nutzen.

Authentisierung

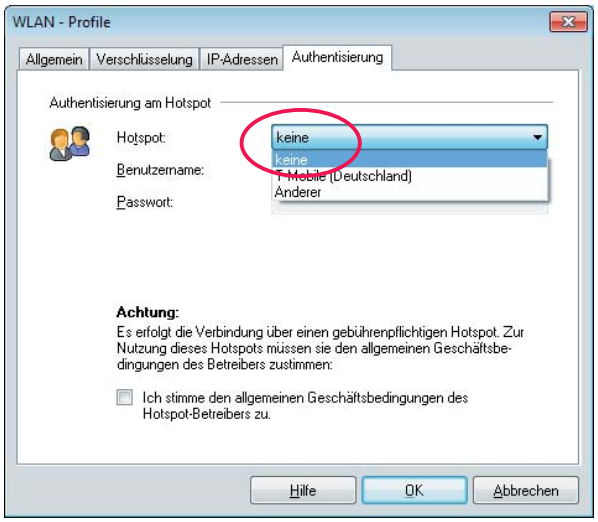
In diesem Fenster können die Zugangsdaten für die Anmeldung an einem Hotspot eingetragen werden. Diese Benutzerdaten werden nur für dieses WLAN-Profil verwendet.

keine Authentisierung am Hotspot

Wenn die Verbindung zum firmeneigenen Access Point des Nahbereich-Funknetzes ohne Hotspot hergestellt wird, wählen Sie *keine* Hotspot-Authentisierung. (Abb. unten)

Sie wählen *keine* Hotspot-Authentisierung wenn der Hotspot-Betreiber keine script-gesteuerte Authentisierung unterstützt.

In diesem Fall wird die Anmeldemaske des Providers zur Eingabe von Benutzernme und Passwort bei Verbindungsaufbau im Browser eingeblendet. Über diese Kennung erhalten Sie zugang am Hotspot und erfolgt die Rechnungstellung des Horspot-Betreibers. (Siehe weiter unten **Anmeldung am Hotspot**.)



Authentisierung am Hotspot

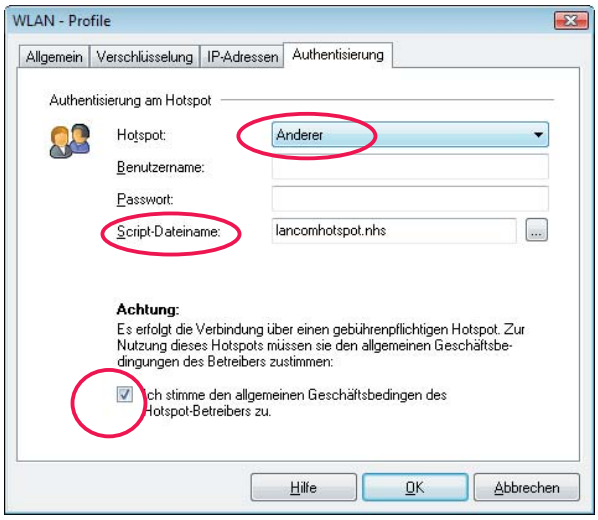
Bitte beachten Sie, dass sie für eine Authentisierung am Hotspot den Geschäftsbedingungen des Hotspot-Betreibers zustimmen müssen bevor das Profil gespeichert und eine Verbindung aufgebaut werden kann. (Abb. nächste Seite)

Authentisierung mit Script

Das Script automatisiert die Anmeldung beim Hotspot-Betreiber, da die Anmeldung script-gesteuert im Hintergrund erfolgt, ohne Einsatz eines Browsers.

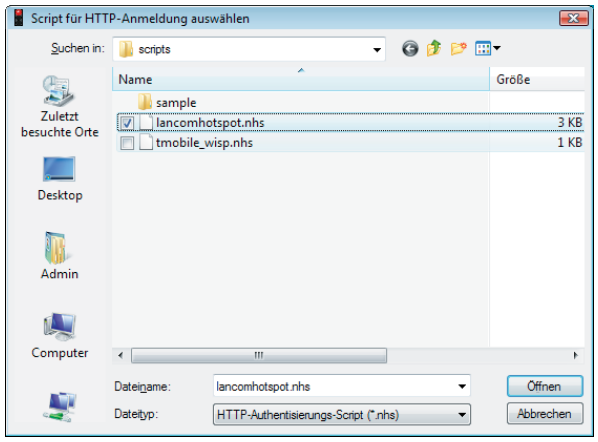
Anderer

Sie selektieren “Anderer” wenn sie einen *nicht namentlich in der Liste erwähnten anderen Hotspot* für die script-gesteuerte Anmeldung nutzen. (*namentlich erwähnt ist z. B. T-Mobile.*) (Abb. unten)



Script-Dateiname

Script-Dateinamen können bei *anderen* Hotspot-Betreibern zur Auswahl eingeblendet werden. Das passende Script für Ihren Hotspot wählen Sie aus dieser Liste*. (Abb. unten)



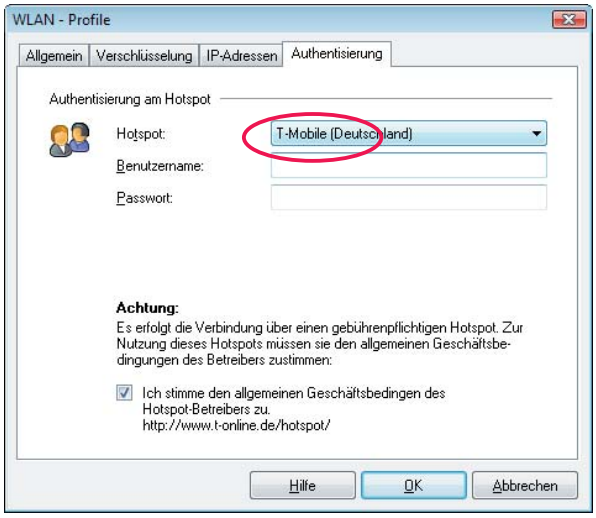
Benutzername / Passwort

Benutzername und Passwort werden entsprechend der Provider-Vorgaben eingegeben.

** (Scripte werden nach Bedarf von NCP erstellt. Ein Script wird im Installationsverzeichnis unter <scripts> eingespielt.)*

T-Mobile

Der T-Mobile Hotspot kann für die Anmeldung mittels WISPr-Technik gewählt werden. Ein Scriptname muss nicht eigens gewählt werden. Das entsprechende Script wird im Hintergrund automatisch geladen. (Abb. unten)



Benutzername / Passwort

Sie müssen nur noch Benutzername und Passswort entsprechend der Provider-Vorgaben eingeben.

WISPr-Anmeldung

Der NCP Secure Client unterstützt die neue Hotspot-Anmeldetechnik über das WISPr-Protokoll (Wireless Internet Service Provider roaming). Damit ist die Kompatibilität zu T-Mobile Hotspots in Deutschland, Österreich, Niederlande, Tschechien und Großbritannien, sowie in Lufthansa-Lounges einiger internationaler Flughäfen gewährleistet.

Die WISPr-Anmeldung erfolgt script-gesteuert ohne Browser mit VPN-Tunneling. Das Script wird für den *namentlich genannten* Hotspot-Betreiber (z. B. T-Mobile) automatisch im Hintergrund geladen.

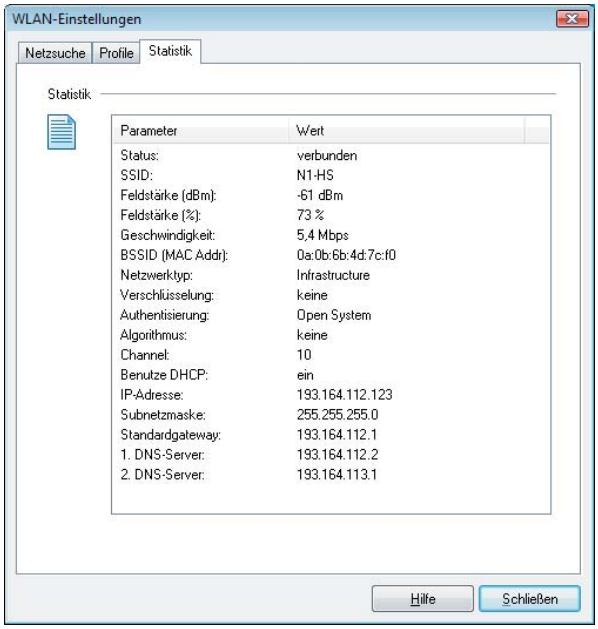
Sie legen ein WLAN-Profil mit Standard-Einstellungen an. D. h. die Verschlüsselung bleibt ausgeschaltet und die IP-Adressen werden automatisch zugewiesen.

Im Konfigurationsfeld für Authentisierung wählen Sie einen *namentlich genannten* Hotspot-Betreiber aus der Liste. Sie finden dort T-Mobile (siehe oben) und Andere. Diese Liste der WISPr-fähigen Hotspot-Betreiber wird von NCP ständig erweitert.

Bei **Anderen** als den hier bezeichneten, erfolgt die script-gesteuerte, browser-lose Anmeldung auf andere Weise. (Siehe oben Script-Dateiname).

Statisik

Das Statistik-Fenster der WLAN-Einstellungen zeigt im Klartext den Status der Verbindung zum Access Point. (Abb. unten)



Die Statistik ergänzt die grafische Anzeige im Monitor um zusätzliche Daten, wie die IP-Adresse des WLAN-Adapters und die DHCP-Einstellung.

VPN-Verbindung und WLAN-Status

Nach der Konfiguration eines WLAN-Profils sowie eines Link-Profils mit Verbindungsmedium WLAN kann eine VPN-Verbindung über den Access Point hergestellt werden.

Wählen Sie im Monitor das entsprechende Profil aus, so wird im Hintergrund automatisch das WLAN-Profil für die Funknetzstrecke eingesetzt, das in den WLAN-Einstellungen zuletzt von Ihnen selektiert wurde. (Siehe unten **WLAN-Automatik**)

Ob der Access Point erreicht werden kann, kann im Tray Icon oder im **WLAN-Status-Feld** abgelesen werden.

Dieses Feld wird über das Fenstermenü des Monitors eingeschaltet (Abb. oben) bzw. dann automatisch eingeblendet, wenn ein Profil mit Verbindungsmedium WLAN für eine VPN-Verbindung ausgewählt wurde (Abb. unten). (Siehe auch **Secure Client Monitor**)

Ist die Feldstärke zu gering oder wird keine SSID angezeigt, so öffnen Sie die WLAN-Einstellungen um ein anderes WLAN-Profil auszuwählen oder ein neues Profil anzulegen.

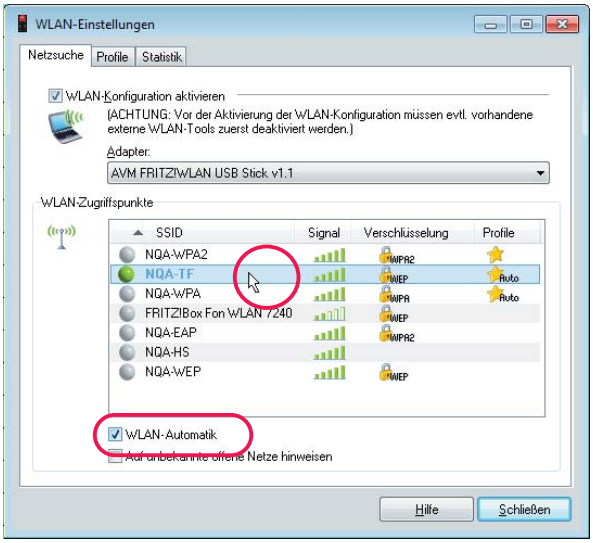
(Der WLAN-Status und die WLAN-Konfiguration können auch unabhängig vom selektierten VPN-Profil geöffnet werden.)

Kann über ein ausgewähltes WLAN-Profil die Verbindung zu einem Access Point hergestellt werden, so muss das WLAN-Status-Feld die **SSID** und die **Feldstärke** des Netzes anzeigen (Abb. unten). Die WLAN-Schrift erscheint grün.

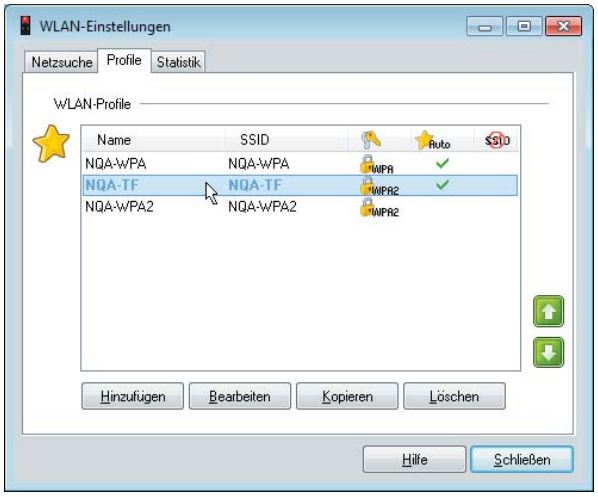
Kann *keine Verbindung* zum Access Point hergestellt werden, bleibt das Feld einschließlich WLAN-Schrift grau, ohne Anzeige von Feldstärke und SSID.

WLAN-Automatik

Ist die WLAN-Automatik aktiviert (Abb. unten), so wird die Verbindung zum entsprechenden Access Point aufgebaut, sobald Sie mit Ihrem Notebook in der Reichweite eines Funknetzes sind, zu dessen SSID ein Profil für die Automatik vorliegt.



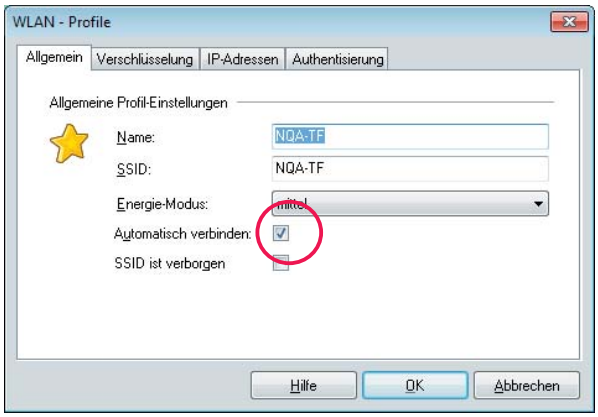
Ein Doppelklick auf die Zeile des entsprechenden Funknetzes kann die Verbindung zum Access Point beenden bzw. wieder herstellen.



Unter der Rubrik “Profile” (Abb. oben) sind die bereits vorhandenen Profile in einer Prioritätenliste gesammelt; die für die WLAN-Automatik vorbereiteten sind mit einem Haken markiert. Mit den grünen Pfeiltasten können selektierte Profile verschoben werden. Die WLAN-Automatik arbeitet immer die Liste von oben nach unten ab, bis mit einem Profil eine Verbindung zum Access Point hergestellt werden kann.

Soll ein Profil, das noch nicht für die Automatik angelegt wurde in die Liste für die WLAN-Automatik aufgenommen werden, so muss dessen Konfiguration mit Doppelklick oder über den Bearbei-

ten-Button geöffnet werden (Abb. unten) und “automatisch verbinden” eingestellt werden.



Aufbau der VPN-Verbindung

Die VPN-Verbindung kann mit einem funktionierenden WLAN-Profil über den Access Point hergestellt werden.

Wählen Sie im Monitor das entsprechende Profil für die VPN-Verbindung mit Verbindungsmedium WLAN aus und klicken auf den Verbindungsschalter, so wird im Hintergrund automatisch das WLAN-Profil für die Funknetzstrecke eingesetzt, das in den WLAN-Einstellungen zuletzt von Ihnen selektiert wurde oder über die WLAN-Automatik gefunden wird. (Abb. unten)

Roaming mit IPsec-Verbindungen

Wird dem Client während einer Session über eine wireless LAN- oder LAN-Verbindung per DHCP eine neue IP-Adresse zugewiesen, so übernimmt der Client die neue IP-Adresse und sendet eine NCP-spezifische Meldung an das Gateway um den Adresswechsel mitzuteilen. Die IPsec-Verbindung wird währenddessen nicht unterbrochen und muss nicht neu aufgebaut werden. Voraussetzung: NCP Secure Server >= 7.02 Build 25.

Sicheres Mobile Computing in WLANs und an Hotspots

Die Beschreibung in diesem Abschnitt gilt sowohl für die Hotspot-Anmeldung mit Script als auch über eine Anmeldeseite.

Auf öffentliche Hotspots kann jeder Anwender mit entsprechend ausgestattetem PC zugreifen. Für die Datensicherheit und den Schutz seines PCs muss er dabei selbst Sorge tragen, da der Hotspot-Betreiber dafür keine Leistungen übernimmt.

Zum Schutz der Vertraulichkeit (Datensicherheit) dient VPN Tunneling und Datenverschlüsselung. Für die Sicherheit des PCs wird eine Personal Firewall mit "Stateful Packet Inspection" benötigt. Beachten Sie die rechte Bildspalte!

Die Hotspot-Automatik der Personal Firewall des Clients sorgt dafür, dass lediglich die IP-Adresszuweisung per DHCP erfolgen darf, weitere Zugriffe ins WLAN bzw. vom WLAN werden unterbunden. Damit der PC bei der Anmeldung im WLAN zu keiner Zeit angreifbar ist, gibt die Firewall dynamisch die Ports für http bzw. https für die Anmeldung bzw. Abmeldung am Hospot frei, sobald der Menüpunkt **Hotspot-Anmeldung** angeklickt wird.

Dabei ist nur Datenverkehr mit dem Hotspot-Server des Betreibers möglich. Ein öffentliches WLAN wird auf diese Weise ausschließlich für die VPN-Verbindung zum zentralen Datennetz genutzt. Direkter Internet-Zugriff ist ausgeschlossen.

Derzeit unterstützt die Hotspot-Anmeldung des Clients ausschließlich Zugangspunkte, die mit der Umleitung (Redirect) einer Anfrage mittels Browser auf die Anmeldeseite des öffentlichen WLAN-Betreibers arbeiten (z. B. T-Mobile oder Eurospot).

Sind obige Voraussetzungen erfüllt, so öffnet ein Klick auf den Menüpunkt **Hotspot-Anmeldung** die Website zur Anmeldung im Standard-Browser. Nach Eingabe der Zugangsdaten kann die VPN-Verbindung z. B. zur Firmenzentrale aufgebaut und sicher kommuniziert werden.

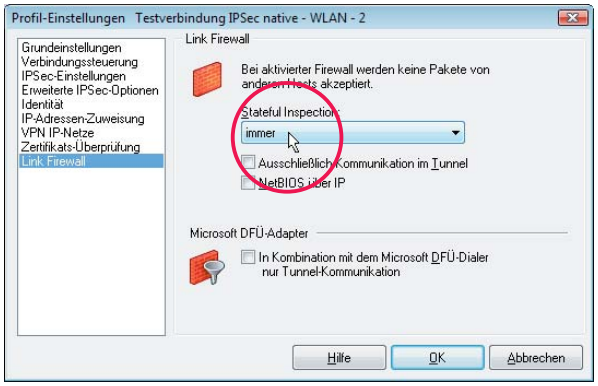
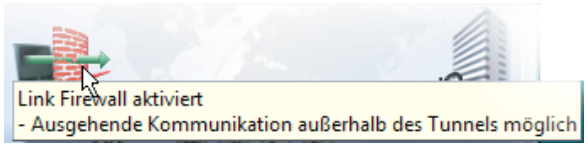
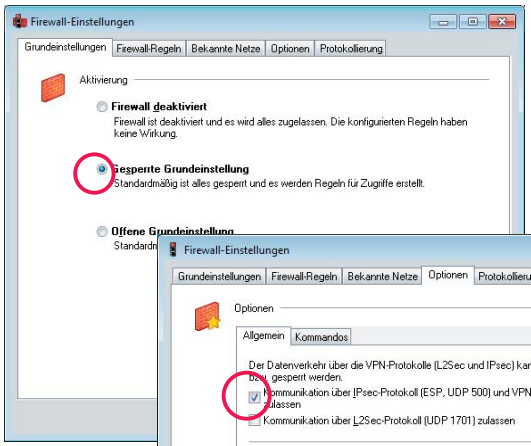


Abb. oben: Die **Link Firewall** *des Clients sollte* **immer** *auf Stateful Inspection geschaltet sein. Die Sicherheitsmechanismen von Stateful Inspection greifen auch, wenn der Client Monitor nicht gestartet ist. (Die Funktion der Link Firewall wird durch die* **Pfeil-Symbole** *im grafischen Feld des Monitors dargestellt. Abb. unten)*

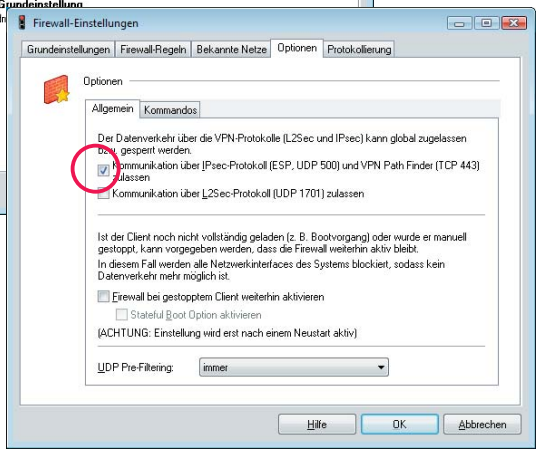


Beachten Sie jedoch: Wird in der **Link Firewall** *zusätzlich die Option* **Ausschließlich Kommunikation im Tunnel zulassen** *aktiviert, so kann auch die Hotspot-Anmeldeseite nicht mehr erreicht werden!*

Eine Anmeldung am Hotspot und die Unterbindung einer Internet-Verbindung unter Umgehung des VPN-Tunnels gestattet nur die integrierte Personal Firewall.



In der Firewall wird die gesperrte **Grundeinstellung** *aktiviert ...*



... und unter **Optionen** *die Kommunikation über IPsec und VPN Path Finder zugelassen.*

Zur Konfiguration weiterer Firewall-Regeln beachten Sie bitte die Beschreibung:

Personal Firewall

Automatische Hotspot-Anmeldung

Im folgenden Abschnitt sind nur einige Varianten zur Hotspot-Anmeldung beschrieben. Für weitere technische Details, insbesondere der Konfiguration der integrierten Personal Firewall, beachten Sie die Beschreibung **Personal Firewall**.

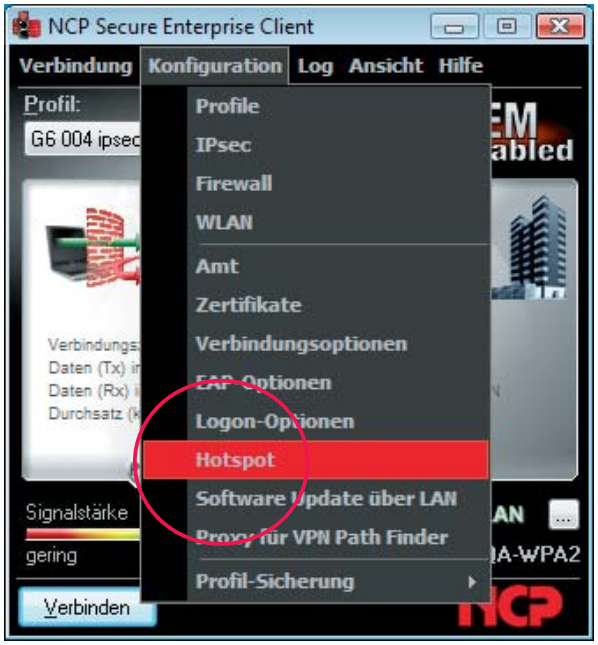
Voraussetzungen

Der Rechner muss sich mit aktivierter WLAN-Karte im Empfangsbereich eines Hotspots befinden. Die Verbindung zum Hotspot muss hergestellt und eine IP-Adresse für den WLAN-Adapater muss zugewiesen sein.

Wie oben beschrieben unter **WLAN-Profil konfigurieren**, scannen Sie zunächst die wireless LANs. Ihren Hotspot-Betreiber erkennen Sie an der SSID. Zu dieser SSID legen Sie ein WLAN-Profil an, wobei im Konfigurationsfenster Authentisierung keine Hotspot-Authentisierung eingestellt sein muss. Im **Statistik**-Fenster der WLAN-Einstellungen können Sie erkennen, ob der WLAN-Adapter eine IP-Adresse erhalten hat.

Hotspot-Konfiguration

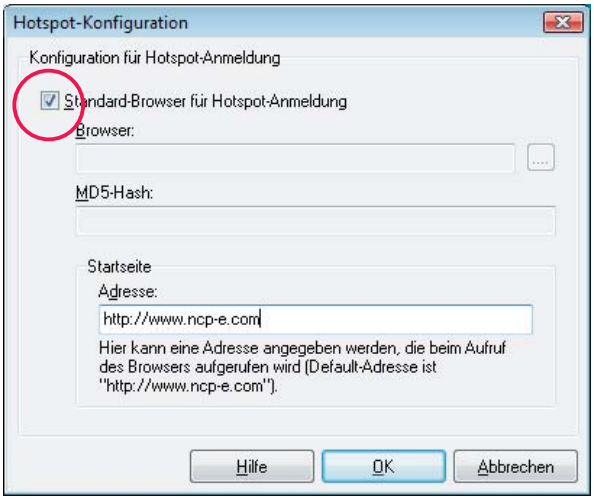
Im Konfigurationsmenü des Monitors unter Hotspot (Abb. unten) erfolgt die Konfiguration zur Hotspot-Anmeldung ohne VPN Tunneling.



Folgende Einstellungen sind möglich:

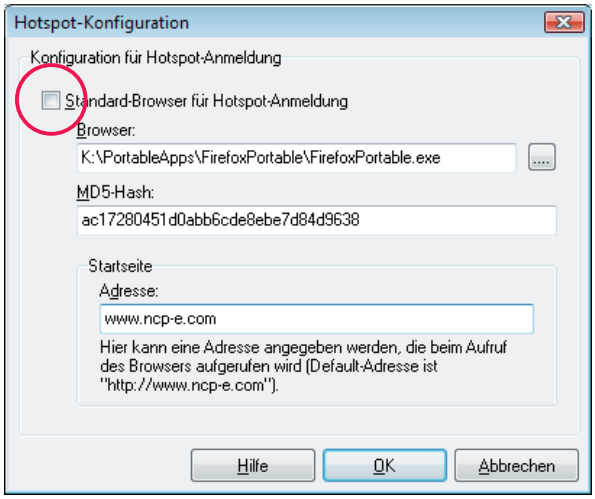
Standard-Browser

Die Grundeinstellung ist: **Standard-Browser für die Hotspot-Anmeldung** (Abb. unten). Sollte der Standard-Browser einen konfigurierten Proxy Server besitzen, so muss dieser unter Umständen deaktiviert werden. Wird der Haken in der Checkbox entfernt, kann ein anderer Browser angegeben werden.



Alternativer Browser

Für einen alternativen Browser wird der Haken im Check-Button entfenrt. Ein alternativer Browser (Abb. unten) wird in folgender Form angegeben:
`%PROGDIR%\Mozilla\Firefox\firefox.exe.`



Der alternative Browser ist nicht Bestandteil der Client Software und muss vom Administrator oder dem Benutzer installiert und eingerichtet werden.

Der alternative Browser kann speziell für die Anforderungen am Hotspot konfiguriert werden. D. h. es wird kein Proxy Server konfiguriert, alle aktiven Elemente (Java, Javascript, ActiveX) werden deaktiviert und die Adressleiste wird ausgeblendet. So kann dieser Browser nur für die Anmeldung am Hotspot genutzt werden.

Zusätzlich kann der MD5-Hash-Wert der Browser-Exe-Datei in das Feld “MD5-Hash” eingetragen werden (Abb. oben), nachdem er ermittelt wurde. Auf diese Weise wird sichergestellt, dass der eingesetzte Browser nicht ausgetauscht oder verändert worden ist.

Startseite

Als Startseite wird die Anmeldeseite des Hotspot-Betreibers eingegeben, entweder als IP-Adresse oder in der Form:
`http://www.meineFirma.de`

Hotspot-Anmeldung

Die Hotspot-Anmeldung erfolgt über den gleichnamigen Menüpunkt des Verbindungsmenüs am Monitor.

Nachdem dieser Menüpunkt (Abb. oben) angeklickt wurde, können verschiedene Verbindungsmeldungen am Bildschirm erscheinen:

– **Wenn sich der Benutzer bereits im Internet befindet**, wird er mit seiner Startseite verbunden. Bei NCP ist dies
`http://www.ncp-e.com`

Es erscheint ein Fenster mit folgender Meldung:

Dieser Text kann vom Administrator ausgetauscht werden, indem die Adresse einer anderen HTML-Startseite in der Form angibt
`http://www.meineFirma.de/hotspot_de.html`
... und eine andere Seite als hotspot_de.html am Web-Server ablegt.

– **Wenn der Benutzer keine Website erreicht**, weil der Hotspot nicht erreicht werden kann, die WLAN-Verbindung abgefallen ist oder andere Verbindungsprobleme aufgetreten sind, erscheint die Microsoft-Fehlermeldung

“... not found”.

– **Ist der Benutzer noch nicht angemeldet**, erscheint die Anmeldeseite des Hotspot-Betreibers mit der Aufforderung die Zugangsdaten einzugeben (Abb. unten).

Nach erfolgreicher Anmeldung mit dem Secure Client kann die VPN-Verbindung zur Firmenzentrale aufgebaut werden.