

Mobile Computing

mit dem FEC Secure IPSec Client

Benutzerhandbuch

FEC Secure IPSec Client



Copyright

Alle Rechte sind vorbehalten. Kein Teil dieses Handbuches darf ohne schriftliche Genehmigung der Firma Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwendet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

Marken

Funkwerk Enterprise Communications, FEC und das FEC Logo sind eingetragene Warenzeichen. Erwähnte Firmenund Produktnamen sind in der Regel eingetragene Warenzeichen der entsprechenden Hersteller.

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 Verkaufsund 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.

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

Mobile Computing mit Enterprise- und Entry Clients	5
Inhaltsübersicht nach Stichworten	5
Multifunktionskarte	6
Profil für Mobilfunkverbindung über UMTS / GPRS erstellen	7
Grundeinstellungen	7
Netzeinwahl	7
Modem	8
Die Multifunktionskarte im Client Monitor	9
Wireless LAN	11
WLAN-Profil konfigurieren	12
Netzsuche	12
WLAN-Profile	13
Allgemeine Profil-Einstellungen	13
Direktverbindung PC-PC	13
Verschlüsselung	13
IP-Adressen	14
Authentisierung	14
Authentisierung mit Script	14
WISPr-Anmeldung	15
Statisik	16
VPN-Verbindung und WLAN-Status	17
Verbindungstest	17
WLAN-Automatik	18
Aufbau der VPN-Verbindung	18
Sicheres Mobile Computing in WLANs und an Hotspots	19
Automatische Hotspot-Anmeldung	20
Voraussetzungen	20
Hotspot-Konfiguration	20
Hotspot-Anmeldung	21
VPN-Verbindungsaufbau	22

Mobile Computing mit dem FEC Secure IPSec Client

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

- Multifunktionskarte
- Profil f
 ür Mobilfunkverbindung über UMTS / GPRS erstellen
- Die Multifunktionskarte im Client Monitor
- Netzsuche
- GPRS / UMTS aktivieren
- Wireless LAN
- WLAN-Profil konfigurieren
- WISPr-Konfiguration
- VPN-Verbindung und WLAN-Status
- WLAN-Automatik
- Sicheres Mobile Computing
- Automatische Hotspot-Anmeldung
- Hotspot-Konfiguration
- Hotspot-Anmeldung



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



Eine Übersicht bietet der **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 Funkwerk-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 Secure 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 Verbindungsstatus der Feldstärke, des selektierten Netzes und Providers, beschrieben in der PDF-Datei Secure 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 sind in einer Kompatibilitätsliste gesammelt.

Ab der Version 2.02 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/ 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:

undeinstellunge

Verbindungsmedium:

Microsoft DFÜ-Dialer

GPRS / UMTS

Freel fiir

nie

IPSec native (GPRS/UMTS)

Standard-Profil nach jedem Neustart

Hilfe

aomatische Medienerkennung

OK

Profil-Name:



X

Abbrechen

Es sei denn, Sie haben vom Provider spezielle Kennwörter erhalten.

Als Zugangsdaten für den Mobilfunk-Provider

(ISP) muss lediglich ein (beliebiger) Benutzername

(Bei Vodafone und T-Online genügen Dummy-Werte).

The state of the s	
Netzeinwani	<u>B</u> enutzername:
Modem Verbindungssteuerung	Muster-Name
Bijekruf	Passwort:
Eingehende Rufe	*****
Security	
Link-Einstellungen	Passwort speichern
Tunnel-Parameter	
Erweiterte IPSec-Uptionen	<u>R</u> utnunmer (∠iel):
VPN IP-Netze	(*99 #)
HA-Unterstützung	
DNS / WINS	
Zertifikats-Überprüfung	Script- <u>D</u> atei:
Link Firewall	

Profil-Name

Grundeinstellu Netzeinwahl

Verbindungssteuerung Rückruf Eingehende Rufe

Security Link-Einstellungen

Tunnel-Parameter Erweiterte IPSec-Optionen

IPSec-Adresszuweisung

VPN IP-Netze HA-Unterstützung DNS / WINS Zertifikats-Überprüfung

Link Firewall

Modem

Geben Sie dazu einen frei wählbaren Profil-Namen ein.

Verbindungsmedium

Selektieren Sie das Verbindungsmedium GPRS / UMTS. (Abb. oben)

Passwort speichern

Netzeinwahl

Benutzername / Passwort

(+ Passwort) eingegeben werden.

Wählen Sie die Option "Passwort speichern" wenn Sie das Passwort eingegeben haben, damit Sie der Secure Client beim Verbindungsaufbau nicht erneut danach fragt.

Rufnummer (Ziel)

Als "Rufnummer (Ziel)" muss je nach Datenkarte und Provider eine bestimmte Zeichenfolge eingegeben werden, die dem Modem mitteilt, welche Art Datenverbindung aufgebaut werden soll. Entnehmen Sie diese Information dem Benutzerhandbuch, welches Sie mit Ihrer Multifunktionskarte erhalten haben, oder fragen Sie im Zweifelsfall die Hotline Ihres Mobilfunkanbieters.



(Rufnummer für T-Mobile: *99#)

Grundeinstellungen

Profil-Einstellungen IPSec native (GPRS/UMTS)

Modem



(Verwenden Sie zur Erzeugung des neuen Profils den Konfigurationsassistenten, dann selektieren Sie *nicht Impulswahl* im Konfigurationsfenster für Modem!)

Modemtyp

Entsprechend des oben gewählten Verbindungsmediums wird in der Modem-Auswahl Ihre Multifunktionskarte angezeigt. Selektieren Sie die installierte Karte.

Netzemwahl Modern Verbindungssteuerung Rickruf Eingehende Rufe Security Link-Einstellungen Link-Einstellungen Modernyp: Link-Einstellungen	COM1 57600 ein	4 4 4
Verbindungssteuerung Guckruf Singehende Rufe Security Imk-Einstellungen Umnel-Parameter Modemtyp: Imk-Einstellungen	57600 ein	4 4
ingehende Rufe Security ink-Einstellungen unnel-Parameter	ein	*
ink-Einstellungen <u>M</u> odemtyp: unnel-Parameter		
unnel-Parameter	Fusion UMTS GPRS WLAN - 3	
Trweiterte IPSec-Optionen Modem Init. String:	AT&F <cr>ATE0V1&D2&C1S0=</cr>	:0<
PSec-Adresszuweisung Dial Prefix:	ATDT	
HA-Unterstützung APN:	at+cgdcont=1,"ip","internet.t-d*	.de
Zertifikats-Überprüfung SIM-PIN A <u>I</u> -Befehl:	AT+CPIN=	
Link Firewall SIM- <u>P</u> IN:	** **	

Modem Init. String

Belassen Sie den zugehörigen Modem-Initialisierungsstring unverändert.

APN

Geben Sie den Access-Point-Namen in Form eines AT-Befehls an. Der APN wird für die GPRS- und UMTS-Einwahl benötigt. Sie erhalten ihn von Ihrem Provider. Der APN wird insbesondere zu administrativen Zwecken genutzt.

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:

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

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

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.

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



Sollte dieses **Modem-Konfigurationsfenster** vom Administrator gesperrt sein, sodass die SIM PIN an dieser Stelle nicht eingetragen und nicht in der Konfiguration gespeichert werden kann, so können Sie im SIM PIN-Dialog die **SIM PIN eingeben** und in der Konfiguration speichern lassen. Dieser Dialog erscheint 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).



1

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.

Bitte das ge	ewünschte Netz a	aus der Liste a	uswählen.
Netz :	a-net		•
(Frneute Net	zsuche nach je	dem Aufruf

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

SIM PIN-E	ingabe				×
Bitte ge	ben Sie o	lie P	IN der SI	M-Karte ein	
ø	PIN:	[
	-PIN in K	onfig	juration sp	peichern	
		<u>0</u> K		Abbreche	n

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 Modem vom Administrator für Eingaben gesperrt wurde.

Am Client muss dem Benutzer dafür ausdrücklich die Berechtigung erteilt werden.

Beachten Sie dazu die Konfigurations-Sperren des 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.

PUK-Eingabe	EX
Bitte geben Sie die PUK der SIM Sie eine neue PIN. Die neu verg künftigen Anmeldungen verwen	I-Karte ein und vergeben Jebene PIN muss für Ihre det werden.
PUK:	
Neue PIN :	
Bestätigung der PIN :	
	Abbrechen



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, sofern er unter dem Betriebssystem Windows 2000, XP oder Vista installiert wurde, das Verbindungsmedium "WLAN" eingestellt. (Siehe Secure Client Parameter).

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 ein WLAN-Profil konfigurieren.



Im WLAN-Profil sind die Zugangsdaten des Benutzers für den Access Point und zum Hotspot gespeichert und es legt fest wie eine Funkverbindung vom Client zu einem Access Point oder Hotspot hergestellt wird. Für jedes vom Client gescannte Funknetz können mehrere dieser Profile angelegt werden.

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)

SSID (Service Set Identifier) und Feldstärke des aktuellen Funknetzes, können nach der Konfigura-

I I C Secure IF Se	ic chefic		
Verbi <u>n</u> dung <u>K</u> on	figuration	Log <u>F</u> enster	<u>H</u> ilfe
Profil:		A	mt
Testverbindung IPS	iec native - \	WLAN 🔻	
2			HQ
Feldstärke : 0 % gering)	20 ;)))	WLADI
Feldstärke : 0 % gering Verbinden	hoch	20 ; //)	WLAN
Peldstärke : 0 % gering ⊻erbinden	hoch (((20 ; >>))	WLAN
Feldstärke : 0 % gering Verbinden Statistik: Verbindungszeit:	((() hoch Irennen 00:00:00	2 2 ; ()))	WLAN
Feldstärke : 0 % gering Verbinden Statistik: Verbindungszeit: Daten (Tx) in Byte:	((() hoch <u>Irennen</u> 00:00:00 0	(D) (Sec): Richtung:	WLAN (funkwerk))
Feldstärke : 0 % gering <u>Verbinden</u> Statistik: Verbindungszeit: Daten (Tx) in Byte: Daten (Rx) in Byte:	((() hoch <u>Irennen</u> 00:00:00 0	Timeout (sec): Richtung: Verbindungsart:	WLAN

tion mit dem **WLAN-Status** (Abb. oben) angezeigt werden. Der WLAN-Status wird über das Fenstermenü des Monitors geöffnet. Siehe weiter unten.

• • • • • 11

WLAN-Profil konfigurieren

Im folgenden ist beschrieben wie ein WLAN-Profil, erstellt mit der internen WLAN-Konfiguration des Clients, in wenigen Schritten eingesetzt werden kann.

Im WLAN-Profil werden die Zugangsdaten zum Funknetz hinterlegt. Es kann auch unabhängig vom aktuell selektierten Link-Profil über den WLAN-Status geöffnet werden.

Netzsuche

Nachdem Sie über das Konfigurationsmenü des Monitors die WLAN-Einstellungen geöffnet haben (Abb. unten), müssen zunächst mit der Netzsuche die vorhandenen Funknetze erkannt werden und dasjenige ausgewählt werden, dessen SSID (Service Set Identifier) von Ihrem Netzbetreiber oder Administrator vorgegeben wurde.

VLAN-Einste	llungen				
Netzsuche	Profile Statistik				
(WIA	N.Konfiguration aktiviere				
	(ACH LUNG: VOLDER)	AKTIVIErung der WLAN-	Konfiguration	müssen evtl.	
-	vorhandene externe \	WLAN-Tools zuerst dea	aktiviert werde	n.)	
	Adapter:				
	AVM FRITZ!WLANT	JSB Stick v1.1			•
WLAN-Ne	etze				
(((()))	SSID	Feldstärke	Versc	Netzwerktyp	
*					
WLAN-Pro	S <u>c</u> annen Difi				
-11	WLAN-Profil:				_
				2	•
	📃 Für Verbindungsa	ufbau Profile mit automa	atischer Verbir	ndungsart verwend	en
	⊻erbinden	Irennen			
			- 21	11.00	
			Hilfe	<u>S</u> chlie	ßen
				n de la companya de l	

WLAN-Konfiguration aktivieren

Aktivieren Sie die interne WLAN-Konfiguration des Clients (Abb. oben). Unter Windows 2000/XP und Vista übernimmt der Secure Client die Handhabung der WLAN-Verbindung. Andere WLAN Tools oder die WLAN Tools der Kartenhersteller müssen daher deaktiviert werden. (Soll das Management-Tool der WLAN-Karte genutzt werden, dann muss die WLAN-Konfiguration im Monitormenü deaktiviert werden.)

Adapter

Stellen Sie fest, ob der WLAN-Adapter betriebsbereit ist, erkennbar am Eintrag seines Namens und der Aktivierung des [Scannen]-Buttons (Abb. oben).

Scannen

Nach einem automatischen Scan-Vorgang von wenigen Sekunden, der manuell auch mit dem [Scannen]-Button ausgelöst werden kann, werden die aktuell verfügbaren Funknetze mit SSID, Feldstärke, Verschlüsselung und Netzwerktyp angezeigt. Die Netze können mit Klick auf SSID, Feldstärke etc. entsprechend sortiert werden. (Abb. unten)

Vetzsuche	Profile	Statistik				
V WLA	AN- <u>K</u> onfi <u>c</u> (ACH vorha	guration akt TUNG: Vor andene exte	ivieren der Aktivierung erne WLAN-Tool	der WLAN-Konfiguratio s zuerst deaktiviert were	n müssen evtl. den.)	
0	Adap	ter:	ANTICD CRAFT	4.1		_
AND AND M	AVM	11112.991	DAIN USB STICK 1	1.1		
WLAN-N	elze		12	102 02 0	1.08 1%	
(((3)))	SSI	D	Feldstärke	Verschlüsselung	Netzwerktyp	Â
	N1-	HS	68 %	Ja	Infrastructure	
	N1-	WPA	/0%	Ja	Infrastructure	
	NI-	WPAZ	69 % 70 %	Ja	Infrastructure	+
-WLAN-Pr	ofil <u>W</u> LAI	o <u>c</u> annen N-Profil:				
	Fi	ir Verbindu	ngsaufbau Profile	e mit automatischer Verl	pindungsart verwe	▼ nden
		(erbinden	Irenner	n		

Selektieren Sie ein Netz mit der Ihnen vom Netzbetreiber mitgeteilten SSID und führen sie einen Doppelklick aus oder wählen Sie über das Kontextmenü der rechten Maustaste **Profil erstellen**. In dem folgenden Bestätigungsfenster werden Sie gefragt, ob Sie ein WLAN-Profil zu diesem Netz anlegen wollen. (Abb. unten)

oreodonio	Profile Statistik				
VL/	AN-Konfiguration a	ktivieren			
-Ma	(ACHTUNG: V	or der Aktivierung d	ler WLAN-Konfiguration	n müssen evtl. Ion)	
-	Adapter:	Ateme w DANA TOOIS	Zuerst deaktiviert weit	ien.)	
		VI AN LISB Stick v	11		•
5.71 A.K. M					
WLAN-N	etze				_
(((**)))	SSID	Feldstärke	Verschlüsselung	Netzwerktyp	-
*	N1-HS	68 %	Ja	Infrastructure	
2	N1-WPA	70%	Ja	Infrastructure	
	Bestätigung			tructure	+
	Es ex	istiert noch kein WL	AN-Profil für dieses Ne	tzl	
	Soll e	in WLAN-Profil ange	elegt werden?		
WLAN-P					
-1		Ja 🖒	<u>N</u> ein		
<u>11</u>			5 - C I - O I	• •	-
<u></u>	🔲 Für Verbind	dungsaufbau Profile	mit automatischer Verb	indungsart verwe	nden
.11	Für Verbind	dungsaufbau Profile	mit automatischer Verb	indungsart verwe	_▼ nden
	Für Verbinder	dungsaufbau Profile	mit automatischer Verb	indungsart verwe	_▼_ nden

Bestätigen Sie die Anfrage mit "Ja" und öffnen Sie die Einstellungen für die WLAN-Profile.

WLAN-Profile

In der WLAN-Konfiguration stehen vier Konfigurationsfenster für die Einstellungen der WLAN-Profile 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.

Allgemein	Verschlüsselung	IP-Adressen	Authentisierung	
Allgem	eine Profil-Einstellu	ngen		
~	Name:	I	I1-HS	
	<u>S</u> SID:	N	I1-HS	
	Netzwerktyp:	Ir	ifrastructure	-
	<u>E</u> nergie-Modu	is: n	ittel	-
	<u>V</u> erbindungsa	rt: n	anuell	-
				34

Name

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

Netzwerktyp

Ebenso verhält es sich mit dem Netzwerktyp, der identisch sein muss mit dem des gewünschten Funknetzes.

Direktverbindung PC-PC



Der **Netzwerktyp** muss dann manuell auf **Ad-Hoc** umgestellt werden, wenn ein Profil für eine Direktverbindung von PC zu PC hergestellt werden soll.

Energie-Modus

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

Verbindungsart

Die Standardeinstellung ist "manuell". D. h.: Dieses Profil muss für eine Verbindung des Clients mit dem Medium WLAN in den WLAN-Einstellungen manuell selektiert werden. Siehe unten VPN-Verbindung und WLAN-Status.

Wird die Verbindungsart auf automatisch gestellt, so wird dieses Profil für die WLAN-Automatik (siehe unten) verwendet.

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.

seiding.	
keine WEP WPA WPA2	
erschlüsselung IP-Adres	sen Authentisierung
selung	
Verschlüsselung:	WPA
Schlüssel-Ver <u>w</u> altung:	PSK
Algorithmus:	ТКІР
Schlüsselformat:	ASCII-Zeichen
<u>S</u> chlüssel:	******
	keine WEPA WPA2 erschlüsselung Verschlüsselung: Schlüssel-Verwaltung: Algorithmus: Schlüsselformat: Schlüsselformat: Schlüsself

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.

llgemein Vei	rschlüsselung	IP-Adressen	Authentisierung	
IP-Adressei	n	n automatisch	beziehen	
ALK.	Folgende I	P-Adr <u>e</u> sse verv	wenden	
	IP-Adres:	se:	0.0.0.0	
	S <u>u</u> bnetzr	maske:	0.0.0.0	
	<u>S</u> tandard	lgateway:	0.0.0.0	- I)
DNS-Serve				
	ONSAWIN ○ Folgende [S-Serveradres: DNS/WINS-Se	se automatisch bezieh rveradressen <u>v</u> erwenc	en len
			Bevorzugter Server	Alternativer Server
	<u>D</u> NS-Ser	ver:	0.0.0.0	0.0.0.0
	<u>W</u> INS-Se	erver:	0.0.0.0	0.0.0.0
		0.0	5.9 m	

0

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.)

Allgemein	Verschlüsselung	IP-Adressen	Authentisierung	0	
Authe	ntisierung am Hotsp	ot	~		
	Ho <u>t</u> spot:		eine		-
	<u>B</u> enutzername	:	eine Mebile (Deutschla	and)	
	Passwort:	A	nderer		
	Achtung:	/erbindung üb	er einen gebühren	pflichtigen Ho	tspot. Zur
	E's enoigt die v		· · · · · · · · · · · · · · · · · · ·	mainan Gasel	
	Nutzung diese dingungen des	s Hotspots mu : Betreibers zu	issen sie den alige istimmen:	meinen Gesci	häftsbe-
	Nutzung diese dingungen des Ich stimme Hotspot-B	s Hotspots mu s Betreibers zu e den allgemeii etreibers zu.	issen sie den alige Istimmen: nen Geschäftsbed	ingen des	näftsbe-

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)

Aligemein	Verschlüsselung IP-Ad	ressen Authentisierun	g	
Authe	ntisierung am Hotspot —			
	Ho <u>t</u> spot:	Anderer		•
	<u>B</u> enutzername:			
	Passwort:			
	Script-Dateiname:	lancomhotspot.nh	ns	
	Achtung: Es erfolat die Verbind	ung über einen gebühr	enpflichtigen H	lotspot. Zur
(Autzung dieses Hots dingungen des Betrei Ch stimme den a Hotspot-Betreibe	oots müssen sie den all bers zustimmen: Illgemeinen Geschäftsb rs zu.	gemeinen Ges edingen des	chäftsbe-

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.

- nan

T-Mobile

mittels WISPr-Technik gewählt werden. Ein Scriptname muss nicht eigens gewählt werden. Das entsprechende Script wird im Hintergrund automatisch geladen. (Abb. unten)

Der T-Mobile Hotspot kann für die Anmeldung

Aligentein	Verschlüsselung IP-Adressen Authentisierung	
Auther	entisierung am Hotspot	
	Ho <u>t</u> spot: T-Mobile	•
	Benutzername:	
	Passwort:	
	Achtung: Es erfolgt die Verbindung über einen gebührenpflichtigen Hotsp Nutzung dieses Hotspots müssen sie den allgemeinen Geschäl dingungen des Betreibers zustimmen:	oot. Zur itsbe-
	Ich stimme den allgemeinen Geschäftsbedingen des Hotspot-Betreibers zu. http://www.tonline.de/hotspot/	

Benutzername / Passwort

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

WISPr-Anmeldung

Der Client unterstützt die neue Hot-spot-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 Hersteller ständig erweitert.

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

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



Statisik

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

tatistik			
		1.035.020	
	Parameter	Wert	
1	Status:	verbunden	
	SSID:	N1-HS	
	Feldstärke (dBm):	-61 dBm	
	Feldstärke (%):	73 %	
	Geschwindigkeit:	5,4 Mbps	
	BSSID (MAC Addr):	0a:0b:6b:4d:7c:f0	
	Netzwerktyp:	Infrastructure	
	Verschlüsselung:	keine	
	Authentisierung:	Open System	
	Algorithmus:	keine	
	Channel:	10	
	Benutze DHCP:	ein	
	IP-Adresse:	193.164.112.123	
	Subnetzmaske:	255.255.255.0	
	Standardgateway:	193.164.112.1	
	1. DNS-Server:	193.164.112.2	
	2. DNS-Server:	193.164.113.1	

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 über das Feld zum WLAN-Status getestet 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)

	FEC Secure IPSec Client
	Verbindung Konfiguration Log Fenster Hilfe
	Profit Amt.
	Testverbindung IPSec native - WLAN 👻
WLAN- Status- Feld	Feldstärke : 0 % ((((,)))) gering hoch
	Verbinden Irennen funkwerkı)

Ist die Feldstärke zu gering oder wird keine SSID angezeigt, so klicken Sie auf den [...]-Button und öffnen die WLAN-Einstellungen um Änderungen vorzunehmen (Abb. unten). (Siehe nächste Seite)



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

Verbindungstest

In den WLAN-Einstellungen können die bereits erstellten WLAN-Profile ausgewählt und getestet werden durch Klick auf den [Verbinden]-Button. (Abb. unten)

Netzsuche	Profile	Statistik				
VLA VLA	AN- <u>K</u> onfig (ACH1 vorhar <u>A</u> dapt	uration aktivieren 'UNG: Vor der A ndene externe W er:	ktivierung der WLAN-I /LAN-Tools zuerst dea	Konfiguration ktiviert werde	müssen evtl. n.)	
	AVM	FRITZ!WLAN U	SB Stick v1.1			•
WLAN-N	etze					
(((()))	SSIE)	Feldstärke	Versc	Netzwerktyp	*
A	N14	VPA2	73 %	Ja	Infrastructure	
	N1-H	łS	75 %	Ja	Infrastructure	
	N1-\	VPA.	73 %	Ja	Infrastructure	
	TES	T2F	67 %	Ja	Infrastructure	
WLAN-P	ofil	<u>c</u> annen				
75 %	WLAN	I-Profil: S				•
	Fu	r Verbindungsaul erbinden	fbau Profile mit automa Trennen	itischer Verbir	ndungsart verwei	nden

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. Über den [Trennen]-Button kann diese Verbindung auch wieder getrennt werden.

Feldstärke : 74 %	((()))	WLAN
gering	hoch	N1-HS

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

WLAN-F	Profile			
57	Name	SSID	Verschlüss	Netzwerktyp
~	N1-HS	N1-HS	WPA2	Infrastructure
	N1-WPA N1-WPA2	N1-WPA N1-WPA2	WPA WPA2	Infrastructure Infrastructure
	<u>N</u> eu	<u>B</u> earbeiten	<u>K</u> opieren	<u>L</u> öschen

In den WLAN-Einstellungen können WLAN-Profile entsprechend der Buttons bearbeitet werden. (Abb. oben)

I I I I 17

WLAN-Automatik

Kann mit einem oder mehreren WLAN-Profilen (in unterschiedlichen Umgebungen) eine Verbindung zum Access Point hergestellt werden, so kann auch die WLAN-Automatik genutzt werden.

aigemein	Verschlüsselung	IP-Adressen	Authentisierung	
Allgem	eine Profil-Einstellu	ngen ———		
$\langle \rangle$	<u>N</u> ame:	N	1-HS	
	<u>S</u> SID:	N	1-HS	
	Netzwerk <u>t</u> yp:	lı	nfrastructure	•
	<u>E</u> nergie-Modu	s: n	ittel	•
	Verbindungsa	rt: a	utomatisch	•

Unter "WLAN-Profil" (Abb. links unten) wird das Profil selektiert, über das eine Verbindung zum Access Point hergestellt werden soll. Es erhält im Konfigurationsfeld für "Allgemeine Profil-Einstellungen" die Verbindungsart "automatisch" (Abb. oben).

م الد					
74%	Eir Verbindungs	aufhau Profile mit a	utomatischer V	'erbindungsa	rt verwender
	rur verbindungs	aurbau Fronie mit au	tomatischer v	erbindungsa	n verwender
	Verbinden	Trennen			
	Verbinden	TIGUNGU			

Wurden mehrere Profile mit der Verbindungsart "automatisch" angelegt und wird die Funktion "Für Verbindungsaufbau Profile mit automatischer Verbindungsart verwenden" (Abb. oben) genutzt, so wird zunächst das zuletzt selektierte Profil für einen möglichen Verbindungsaufbau herangezogen. Kann damit keine Verbindung zum Access Point hergestellt werden, so werden anschließend die als "automatisch" konfigurierten Profile für einen möglichen Verbindungsaufbau herangezogen und das zuerst passende verwendet.

Testen Sie die WLAN-Automatik, so kann der [Trennen]-Button nicht betätigt werden, da die Automatik ständig eine Verbindung herstellen will.

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 [Verbinden]-Button, 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)

FEC Secure IPS	ee enem		
Verbi <u>n</u> dung <u>K</u> or	nfiguration	Log <u>F</u> enster	<u>H</u> ilfe
<u>P</u> rofil:		A	mt
Testverbindung IP	Sec native - ^v	WLAN 🔻	
	12.74	10-10-	
-2			
	Verbinduna	ist heraestellt	HQ
		and the general second	Contraction of the local division of the loc
	and an	0.0	
PIN		O P	
وری Feldstärke : 71 %	*	20	WLARI
Feldstärke : 71 %	(((2 (; 1))	WLABI N1-HS
Feldstärke : 71 % gering	hoch Irennen	20 ; ⁽⁾⁾⁾	سلامکس N1-HS funkwerk())
Feldstärke : 71 % gering Verbinde	hoch Irennen	2 2 ; **))] f	WLAN N1-HS funkwerk))
Feldstärke : 71 % gering Verbinde	() hoch <u>I</u> rennen 00:01:50	(0) (0) (10)	WLAN N1-HS funkwerk))
Feldstärke : 71 % gering Verbinde Statistik: Verbindungszeit: Daten (Tx) in KByte	() hoch Irennen 00:01:50 e: 78,7	Timeout (sec): Richtung:	WLAN (N1-HS funkwerk))) 37 out
Feldstärke : 71 % gering Verbinde Statistik: Verbindungszeit: Daten (Tx) in KByte Daten (Rx) in KByte	(() hoch <u>Irennen</u> 00:01:50 e: 78,7 e: 5,061	Timeout (sec): Richtung: Verbindungsart:	WLAN N1-HS funkwerk)) 37 out WLAN

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.

Grundeinstellungen Verbindungssteuerung IPSe-Einstellungen Erweitete IPSe-Optionen Identität IP-Adressen-Zuweisung VFN IP-Netze Zertifikats-Überprüfung Link Firewell	Eink Frewall Bei aktivierter Firewall werden keine Pakete von andeemHeste akzeptiert. Etateful Inspection immer AusschließlichKommunikation im junnel NetBIDS über IP
	Microsoft DFÜ-Adapter In Kombination mit dem Microsoft <u>D</u> FÜ-Dialer nur Tunnel-Kommunikation
	In Kombination mit dem Microsoft <u>D</u> FÜ-Dialer nur Tunnel-Kommunikation



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.





Zur Konfiguration weiterer Firewall-Regeln beachten Sie bitte die Beschreibung in der Online-Hilfe.



... und unter **Optionen** nur die Kommunikation über IPSec-Protokoll zugelassen.

— — — — 19

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. Oben im Abschnitt Verbindungstest ist beschrieben wie Sie mit diesem Profil eine Verbindung zum Hotspot herstellen. 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.

FEC Secure	e IPSec Client	• - X -
Verbi <u>n</u> dung	Konfiguration Log Fenster Hilfe	
Profil: Zentrale	Profile Firewall	
	WLAN	ISP
	Amt	3
-	Zertifikate	
	Verbindungsoptionen	
Verbinden	EAP-Optionen	erkill
	Logon-Optionen	
Statistik:	Konfigurations-Sperren	
Daten (Tx) in I	Profile importieren	
Daten (Rx) in I	Hotspot	
Durchsatz (kB	Profil-Sicherung	

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.

Hotspot-Konfiguration	X
Konfiguration für Hotspot-Anmeldung	
Stindard-Browser für Hotspot-Anmeldu Browser:	ng
<u>M</u> D5-Hash:	
Startseite A <u>d</u> resse:	
http://www.ncp-e.com	
Hier kann eine Adresse angegeb des Browsers aufgerufen wird (De ''http://www.ncp-e.com'').	en werden, die beim Aufruf fault-Adresse ist
<u>H</u> ilfe	<u>O</u> K <u>Abbrechen</u>

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.

FEC Secure IPSec Client	- 0 🔀
Verbindung Konfiguration	Log <u>F</u> enster <u>H</u> ilfe
Verbinden	it .
Irephen	
Hotspot-Anmeldung	
Verbindungsinformation	nen
Verfügbare Verbindungs	medien
Zertifikate	•
PIN eingeben	WLAW
PIN zurücksetzen	NQA-HS
PIN ändern	nkwerkill
Beenden	
Verbindungszeit: 00:00:00	Timeout (sec): 0
Daten (Tx) in Byte: 0	Richtung: -
Daten (Rx) in Byte: 0	Verbindungsart: WLAN
Durchsatz (kB/s): 0,000	Verschlüsselung:

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.

Es erscheint ein Fenster mit folgender Meldung:

Keine Hotspot Anmeldung notwendig

Sie befinden sich bereits im Internet. Eine Anmeldung am Hotspot ist nicht notwendig oder wurde bereits durchgeführt.

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).

🖉 Login - Windows Internet Explorer	×
😭 🏘 🔄 Login 🍡 🖓 🔻 🖶 🔻	**
Login	^
Bitte geben Sie Ihre Benutzerkennung und Ihr Passwort ein:	
Benutzerkennung:	
Passwort:	=
Einloggen Zurücksetzen	
<	Ψ F
Internet Geschützter Modus: Aktiv 🔍 100%	▼ i

VPN-Verbindungsaufbau

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





Copyright

Alle Rechte sind vorbehalten. Kein Teil dieses Handbuches darf ohne schriftliche Genehmigung der Firma Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwendet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

Marken

Funkwerk Enterprise Communications, FEC und das FEC Logo sind eingetragene Warenzeichen. Erwähnte Firmen- und Produktnamen sind in der Regel eingetragene Warenzeichen der entsprechenden Hersteller.

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 Verkaufsund Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslastungen.

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

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