# Installation

## des FEC Secure IPSec Clients

# Installation des Secure IPSec Clients

**In diesem Dokument finden Sie neben der Installationsbeschreibung eine kurze Produktbeschreibung. Zudem sind spezielle Installationsmöglichkeiten und die Lizenzierung beschrieben.**

## Inhaltsübersicht



Weiterführende Beschreibungen zur Erstellung von Profilen und zur IPSec-Konfiguration finden Sie in den Beschreibungen **Secure Client Monitor** und **Secure Client Parameter**.

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

# Produktbeschreibung

## FEC Secure IPSec Client – universelle Lösung für sichere VPN-Lösungen

Der IPSec Client kann in beliebigen VPN-Umgebungen eingesetzt werden. Er kommuniziert auf der Basis des IPSec-Standards mit den Gateways verschiedenster Hersteller* und ist die Alternative zu der am Markt angebotenen, einheitlichen IPSec-Client-Technologie. Die Client Software emuliert einen Ethernet LAN-Adapter. Der IPSec Client verfügt über zusätzliche Leistungsmerkmale, die dem Anwender den Einstieg in eine ganzheitliche Remote Access VPN-Lösung ermöglichen.

## Der IPSec Client bietet

– Unterstützung aller gängigen Betriebssysteme

– Einwahl über alle Übertragungsnetze

– Kompatibilität mit den VPN Gateways unterschiedlichster Hersteller

– Integrierte Personal Firewall für mehr Sicherheit

– Dialer-Schutz (keine Bedrohung durch 0190er- und 0900er-Dialer)

– Höhere Geschwindigkeit im ISDN (Kanalbündelung)

– Gebührenersparnis (Kosten- und Verbindungskontrolle)

– Bedienungskomfort (grafische Oberfläche)

## Leistungsumfang

Der IPSec Client unterstützt alle gängigen Betriebssysteme 32/64 Bit (Windows 2000, XP und Vista). Die Einwahl in das Firmennetz erfolgt unabhängig vom Mediatyp, d. h. neben ISDN, PSTN (analoges Fernsprechnetz), GSM, GPRS/UMTS und xDSL wird auch LAN-Technik wie im WLAN (am Firmengelände und Hotspot) oder lokalen Netzwerk (z. B. Filialnetz) unterstützt. Auf diese Weise kann mit ein und demselben Endgerät von unterschiedlichen Lokationen auf das Firmennetz zugegriffen werden:

Weitere Informationen erhalten Sie auf der Funkwerk-Website: http://www.funkwerk-ec.com

– in der Filiale über WLAN

– in der Zentrale über LAN

– unterwegs an Hotspots und beim Kunden über WLAN bzw. GPRS

– im Home Office über xDSL oder ISDN

# Installationsvoraussetzungen

**Bevor Sie die Software installieren müssen, zur vollen Funktionsfähigkeit die entsprechenden Installationsvoraussetzungen erfüllt sein.**

## Betriebssystem

Die Software kann auf Computern (min. 128 MB RAM) mit den Betriebssystemen Microsoft Windows 2000, Windows XP oder Windows Vista installiert werden. Halten Sie für die Dauer der Installation die Datenträger für das jeweils im Einsatz befindliche Betriebssystem bereit, um Daten für die Treiberdatenbank des Betriebssystems nachladen zu können!

## Gegenstelle

Die Gegemstelle muss eines der folgenden Verbindungsmedien unterstützen: ISDN, PSTN (analoges Modem), GSM, GPRS/UMTS, LAN over IP, WLAN oder PPP over Ethernet. (Im folgenden sind die Verbindungsmedien aufgeführt, wovon jeweils eines pro Profil der Gegenstelle am Secure Client eingestellt sein muss. Mit Mausklick auf einen der rot markierten Begriffe springen Sie in das Dokument **Client-Parameter** oder **Mobile-Computing** zur jeweiligen Konfigurationsbeschreibung.)

## Secure Client

Eine der folgenden Kommunikationsschnittstellen muss am Client PC verfügbar sein.

### ISDN-Adapter (ISDN)

Der ISDN-Adapter muss die **ISDN** CAPI 2.0 unterstützen. Wenn Sie **PPP Multilink** nutzen, kann die Software bis zu 8 ISDN B-Kanäle (je nach Kanalanzahl des Adapters) bündeln. Prinzipiell kann jeder ISDN-Adapter, der die ISDN-Schnittstelle CAPI 2.0 unterstützt, eingesetzt werden. (Für gewöhnlich wird die CAPI bei der Installation eines ISDN-Adapters automatisch eingerichtet.)

### Analoges Modem (Modem)

Für die Kommunikation über **Modem** muss das Modem korrekt installiert sein, sowie Modem Init. String und COM-Port Definition zugewiesen sein. Das Modem muss den Hayes-Befehlssatz unterstützen.

Ebenso können Mobiltelefone für die Datenkommunikation genutzt werden, nachdem die zugehörige Software installiert wurde, die sich für den Client genauso darstellt wie ein analoges Modem. Als Schnittstelle zwischen Handy und PC kann die serielle Schnittstelle, die IR-Schnittstelle (Infrarot) oder Bluetooth genutzt werden. Je nach Übertragungsrat (GSM, V.110, GPRS oder HSCSD) muss die Gegenstelle über die entsprechende Einwahlplattform verfügen. Der in die Modemkonfiguration des Secure Clients einzutragende Initialisierungs-String ist vom ISP oder dem Hersteller des Mobiltelefons zu beziehen.

### LAN-Adapter (LAN over IP)

Um die Client-Software mit der Verbindungsart **LAN (over IP)** in einem Local Area Network betreiben zu können, muss zusätzlich zum bereits installierten LAN-Adapter (Ethernet) kein weiterer Adapter installiert werden. Die Verbindung der LAN-Clients ins WAN stellt ein beliebiger Access Router her. Einzige Voraussetzung: IP-Verbindung zum Zielsystem muss möglich sein. Die VPN-Funktionalität liefert die Client Software.

Adapter für ein wireless LAN (WLAN-Adapter) werden genauso behandelt wie normale LAN-Adapter.

### xDSL (xDSL (PPPoE))

Das Verbindungsmedium **PPP over Ethernet** setzt voraus, dass eine Ethernet-Karte installiert und darüber ein xDSL-Modem mit Splitter korrekt angeschlossen ist.

### xDSL (AVM - PPP over CAPI)

Das Verbindungsmedium **AVM - PPP over CAPI** kann gewählt werden, wenn eine AVM Fritz! DSL-Karte eingesetzt wird. Im Feld “Rufnummer (Ziel)” in der Gruppe “Netzeinwahl” können für die Verbindung über CAPI noch AVM-spezifische Intitialisierungskommandos eingetragen werden. Unter Windows Betriebssystemen wird jedoch empfohlen den Standard “xDSL (PPPoE)” zu verwenden, da damit direkt über die Netzwerkschnittstelle mit der Karte kommuniziert wird.Bei Verwendung der AVM Fritz! DSL-Karte wird keine separate zusätzliche Netzwerkkarte benötigt.

### Multifunktionskarte

Wird eine Mobilfunkkarte (für: GRPS / UMTS / HSDPA / HSUPA) eingesetzt, so können mit der Client Software spezielle Features des Mobile Computings unter Einbeziehung der Karteneigen-

schaften 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 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.

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/service-support/kompatibilitaeten/mobile-connect-cards.html

### WLAN-Adapter (WLAN)

Der WLAN-Adapter wird mit dem Verbindungsmedium **WLAN** betrieben werden. Im Monitormenü erscheint eigens der Menüpunkt “WLAN-Einstellungen”, worin die Zugangsdaten zum Funknetz in einem Profil hinterlegt werden können. Wird diese “WLAN-Konfiguration aktiviert”, so muss das Management-Tool der WLAN-Karte deaktiviert werden. (Alternativ kann auch das Management-Tool der WLAN-Karte genutzt werden, dann muss die WLAN-Konfiguration im Monitormenü deaktiviert werden.)

Wird die Verbindungsart WLAN für ein Profil eingestellt, so wird unter dem grafischen Feld des Monitors eine weitere Fläche eingeblendet, auf der die Feldstärke und das WLAN-Netz dargestellt werden.

Bitte beachten Sie zur Konfiguration der WLAN-Einstellungen die Beschreibung zum **Mobile Computing**.

### Automatische Medienerkennung

Werden wechselweise unterschiedliche Verbindungsmedien genutzt, so erkennt der Client automatisch, welche Verbindungsarten aktuell zur Verfügung stehen und wählt davon die schnellste aus.

Auf Grundlage eines vorkonfigurierten Profils wird automatisch die Verbindungsart erkannt und eingesetzt, die für den Client-PC aktuell zur Verfügung steht, wobei bei mehreren alternativen Übertragungswegen automatisch der schnellste gewählt wird. In einer Suchroutine ist die Priorisierung der Verbindungsarten in folgender Reihenfolge festgelegt: 1. LAN, 2. WLAN, 3. DSL, 4. UMTS/GPRS, 5. ISDN, 6. MODEM.

Die Konfiguration erfolgt mit dem Verbindungsmedium **automatische Medienerkennung** in den “Grundeinstellungen” eines Profils. Alle für diesen Client-PC vorkonfigurierten Profile zum VPN Gateway des Firmennetzes können dieser automatischen Medienerkennung, sofern gewünscht, zugeordnet werden (über das Parameterfeld “Grundeinstellung”). Damit erübrigt sich die manuelle Auswahl eines Mediums (WLAN, UMTS, Netzwerk, DSL, ISDN, Modem) aus den Profilen.

Die Eingangsdaten für die Verbindung zum ISP werden für den Anwender transparent aus den vorhandenen Profileinträgen übernommen.

# Voraussetzungen für Zertifikatsverwendung

Sollen Zertifikate für die erweiterte Authentisierung eingesetzt werden, so beachten Sie bitte das Dokument **Secure-Client-Zertifikate**.

## Unterstützte Schnittstellen und Formate

Der Secure Client kann in Public Key Infrastrukturen nach X.509 V.3 Standard eingesetzt werden.

Der Secure Client unterstützt folgende Schnittstellen / Formate:
– Smartcards, USB-Token:
PKCS#11, TCOS 1.2 und 2.0, CSP
– Soft-Zertifikate: **PKCS#12-Datei**
– PC/SC-konforme **Chipkartenleser**:
Die Client Software unterstützt alle Chipkartenleser, die PC/SC-konform sind. Diese Chipkartenleser werden in einer Liste des Clients aufgenommen, wenn der Leser angeschlossen und die zugehörige Treiber-Software installiert wurde.
– **Automatische Erkennung des angeschlossenen PC/SC-Lesers**: Ist für das PKI-Umfeld die Verwendung eines PC/SC Chipkartenlesers am Client konfiguriert, so erkennt und verwendet der Client automatisch den jeweils angeschlossenen.
– **PKCS#11-Modul**: Mit der Software für die Smartcards oder den Tokens werden Treiber in Form einer PKCS#11-Bibliothek (DLL) mitgeliefert. Diese Treiber-Software muss zunächst installiert werden. Anschließend kann über einen Assistenten das entsprechende PKCS#11-Modul selektiert werden.

## CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies geschieht dadurch, dass er die CA-Zertifikate seiner Wahl in das Installationsverzeichnis unter <CACERTS> einspielt. Das Einspielen kann bei der Software-Distribution automatisiert stattfinden, wenn sich die Aussteller-Zertifikate bei der Installation der Software von einem Datenträger dort im Verzeichnis <DISK1> befinden.

Nachträglich können Aussteller-Zertifikate, sofern der Benutzer über die notwendigen Schreibrechte in genanntem Verzeichnis verfügt, von diesem selbst eingestellt werden.

Derzeit werden die Formate *.pem und *.crt für Aussteller-Zertifikate unterstützt. Sie können im Monitor unter dem Hauptmenüpunkt “Verbindung / Zertifikate / **CA-Zertifikate anzeigen**” eingesehen werden.

Wird am Secure Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der Client den Aussteller indem er das Aussteller-Zertifikat, zunächst auf Smartcard bzw. USB-Token oder in der PKCS#12-Datei, anschließend im Installationsverzeichnis unter <CACERTS> sucht. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande. Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

Werden Soft-Zertifikate mit dem PKI Plug-in des Management Servers erstellt, so wird das Aussteller-Zertifikat in der PKCS#12-Datei gespeichert.

## Verwendung von Sperrlisten (CRL)

Zu jedem Aussteller-Zertifikat kann dem Secure Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Installationsverzeichnis unter <CRLS> gespielt. Ist eine CRL vorhanden, so überprüft der Secure Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Der Client lädt die zugehörige CRL automatisch herunter wenn das eingehende Benutzer-Zertifikat des Servers die **Zertifikatserweiterung CDP** enthält.

# Installation der Software

Die vorliegende Version und künftige Versionen des Clients werden von der Qualitätssicherung nur noch für die Windows-Betriebssysteme Windows 2000, Windows XP und Windows Vista getestet. Für Windows NT sowie Windows 98 oder älter kann somit keine Gewähr mehr für die volle Funktionsfähigkeit der Client Software übernommen werden.

Sie können die Software in Form einer EXE-Datei als Download von der Funkwerk-Internetseite unter www.funkwerk-ec.com beziehen. Die Installation erfolgt für die Betriebssysteme Windows 2000/XP und Vista im Wesentlichen gleich.

Bitte achten Sie jedoch darauf, ob Sie von Festplatte, CD oder Diskette installieren.

## Installation und Lizenzierung

Der FEC Secure IPSec Client wird zunächst immer als Testversion installiert. Haben Sie eine Lizenz erworben, so können die Lizenzierungsdaten nach der Installation und einem Reboot im Monitor-Menü “Hilfe / Lizenzinfo und Aktivierung” eingegeben werden. Spätestens in den letzten 10 Tagen vor Ablauf der 30-tägigen Gültigkeitsdauer der Testversion werden Sie im Client-Monitor daran erinnert, dass eine Lizenzierung vorgenommen werden muss, wenn die Client Software weiter verwendet werden soll. Bitte beachten Sie zur Lizenzierung die Beschreibung **Secure-Client-SW-Aktivierung**.

## Installation von der CD

Nachdem Sie die CD in das Laufwerk Ihres Computers eingelegt haben, erscheint nach einigen Sekunden automatisch die Begrüßungsmaske auf Ihrem Monitor. Sie wählen aus, welches Produkt Sie installieren möchten und klicken anschließend auf “Installieren”. Das weitere Verfahren ist mit der Installation von Wechseldatenträger ab “Wählen der Setup-Sprache” identisch.

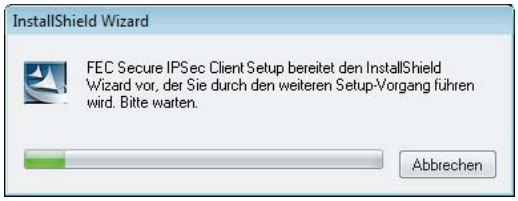
# Standard-Installation

Die EXE-Datei, die Sie mit einem Download oder mit der CD erhalten haben, kopieren Sie auf die Festplatte des PCs z. B. in das Verzeichnis <Disk1>. Der Dateiname der EXE-Datei beinhaltet Versions- und Build-Nummer der Software, z. B.:
`FEC_EntryCl_Win32_910_058.EXE`
Wählen Sie im Windows-Hauptmenu “Start / Einstellungen / Systemsteuerung”. In der Windows-Systemsteuerung wählen Sie “Software” oder “Neue Programme hinzufügen”. Klicken Sie dann auf den Button zum Installieren von CD oder Diskette. Im daraufhin erscheinenden Fenster klicken Sie auf “Durchsuchen”, um die EXE-Datei Ihrer Software im Verzeichnis <Disk1> zu suchen. Wenn sie angezeigt wird, klicken Sie auf “Fertigstellen”.

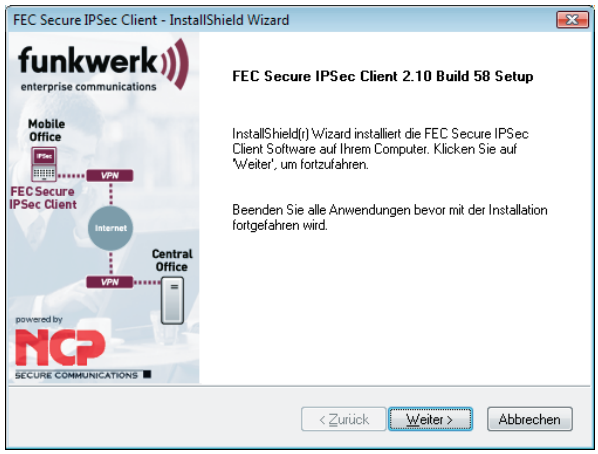
## Wählen der Setup-Sprache

Im folgenden Fenster können Sie die Setup-Sprache auswählen. Klicken Sie danach auf “OK”.

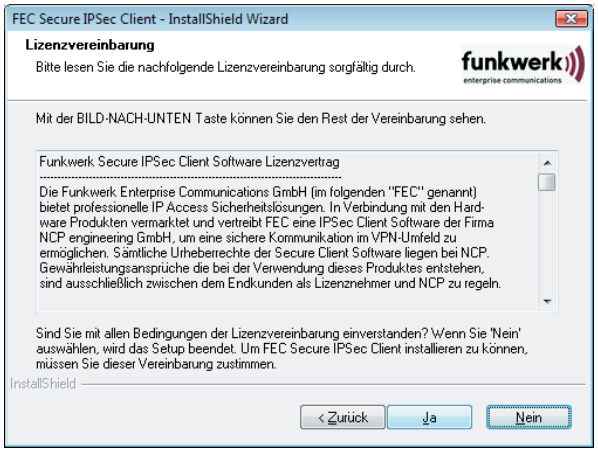

Anschließend bereitet das Setup-Programm den Install-Shield Assistenten vor, mit dessen Hilfe die Installation fortgesetzt wird.




Lesen Sie bitte die Hinweise im Willkommen-Fenster des Setup-Programms bevor Sie auf “Weiter” klicken.

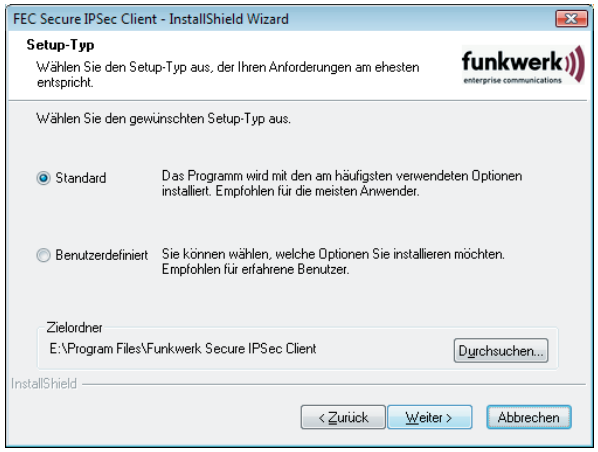



Anschließend werden die Lizenzbedingungen gezeigt. Stimmen Sie dem Vertag mit “Ja” zu, sonst wird die Installation abgebrochen.




Standard-Installationsverzeichnis ist:
`Programme\`
`Funkwerk Secure IPSec Client`
(Unter Windows Vista kann auch “Program Files\Funkwerk Secure IPSec Client” angezeigt werden.)

Unabhängig von Standard- oder benutzerdefinierter Installation können Sie einen beliebigen Zielordner für die Software wählen, wenn Sie “Durchsuchen” anklicken. Dies ist insbesondere dann wichtig, wenn der Benutzer keine Rechte auf das System-Root-Verzeichnis hat.

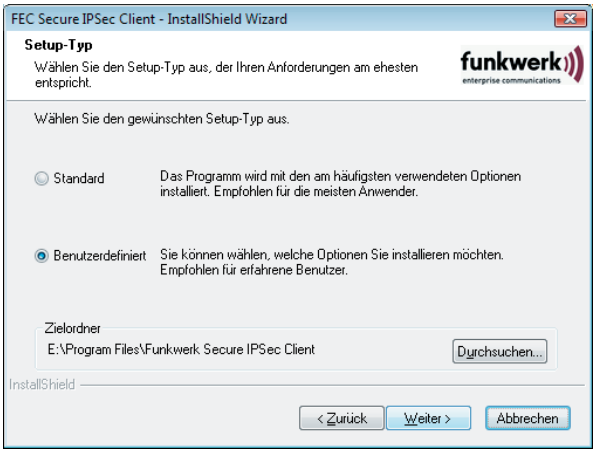



Wenn Sie eine “Standard” Installation vornehmen, ist das Setup mit diesem Fenster abgeschlossen. (Abb. oben)

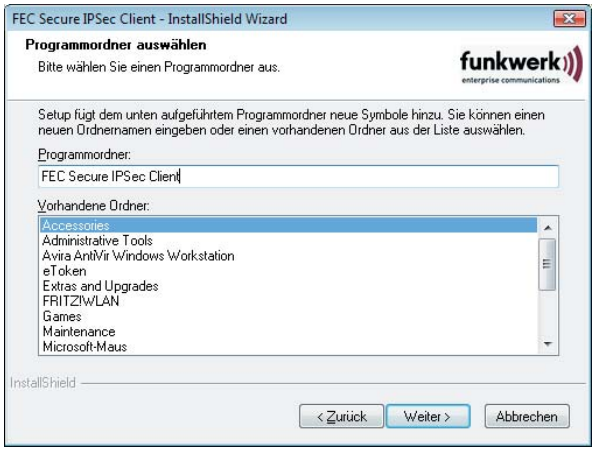
Nehmen Sie eine “Benutzerdefinierte Installation” vor, so können Sie weitere Einstellungen vornehmen. (Abb. nächste Seite)

## Benutzerdefinierte Installation

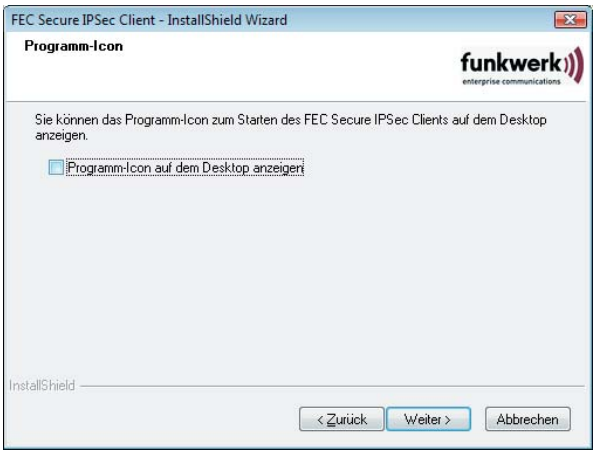
Nehmen Sie eine “Benutzerdefinierte Installation” vor, so können Sie weitere Einstellungen machen.




Im folgenden Fenster der “Benutzerdefinierten Installation” bestimmmen Sie den Programmordner für die Client Software (Abb. unten). Standard ist:
`%Programme%\`
`Funkwerk Secure IPSec Client`




Außerdem kann das Programm-Icon auf dem Desktop angezeigt werden. (Abb. unten)




Zu den weiteren Einstellungen bezüglich Ihres Kommunikations-Gateways sind nähere Informationen von Ihrem Administrator oder Internet Service Provider nötig.


Mit DHCP (Dynamic Host Control Protocol) zu kommunizieren, bedeutet, dass Sie für jede Session automatisch eine IP-Adresse zugewiesen bekommen. In diesem Fall klicken Sie auf “IP-Adresse wird von Server vergeben”. (Abb. oben)

Wenn Sie die “IP-Adresse selbst festlegen”, geben Sie in nachfolgendem Fenster die IP-Adressen ein.


Bitte beachten Sie: Ist bereits eine Netzwerkkarte mit Default Gateway installiert, so muss der Eintrag “Default Gateway” hier gelöscht werden. Es darf nur eine Netzwerkkarte mit Default Gateway installiert sein. Die DNS-Adresse bitte nur eintragen, wenn Sie sie von Ihrem Provider oder Systemadministrator zur Verfügung gestellt bekommen haben.

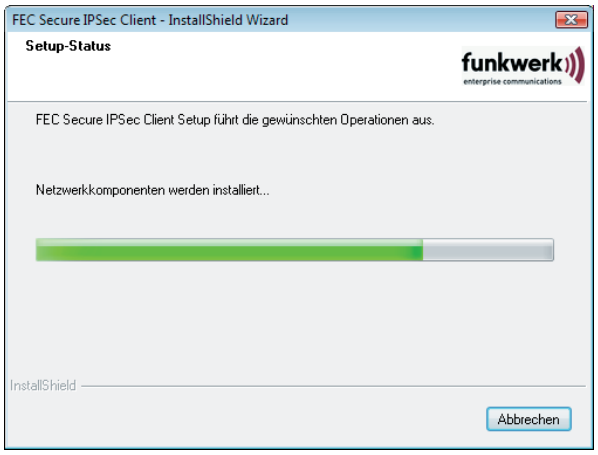
Wenn Sie die “IP-Adresse selbst festlegen”, ist es erforderlich, daß Sie IP-NAT (Network Address Translation) einschalten. IP-NAT ist standardmäßig immer eingeschaltet (siehe **IP Network Address Translation**).

Sie können anschließend entscheiden, ob vor dem Windows-Logon an einer remote Domain die Verbindung zum VPN Gateway aufgebaut werden soll. Für diesen Verbindungsaufbau müssen Sie gegebenenfalls die PIN für ihr Zertifikat und das (nicht gespeicherte) Passwort für die Client Software eingeben. Nachdem die Verbindung zum Gateway hergestellt wurde, können Sie sich an die remote Domain anmelden. Diese Anmeldung erfolgt dann bereits verschlüsselt über den VPN-Tunnel. (Abb. unten)

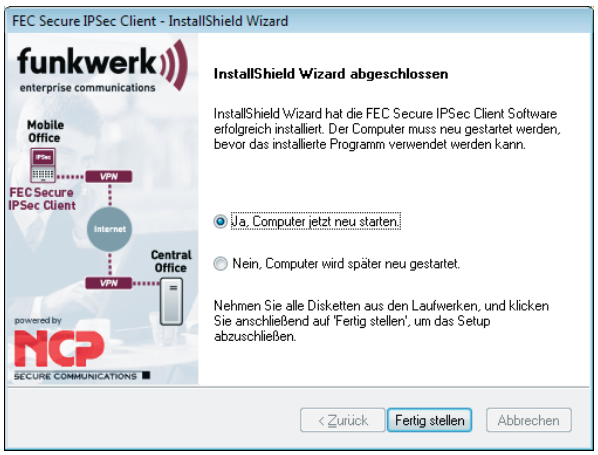

Bitte beachten Sie: Aktivieren Sie diese Option vor dem Windows Logon, so wird hiermit automatisch die NCP Gina installiert. Nur wenn die NCP Gina – wie in diesem Setup-Fenster möglich – nach der Windows Gina installiert ist, können die Logon-Optionen auch genutzt werden. Diese Logon-Optionen können über das Monitormenü des Clients unter “Konfiguration” gesetzt werden.

Wird die Logon-Option hier nicht aktiviert, und soll sie jedoch zu einem späteren Zeit-punkt genutzt werden, so kann die NCP Gina nach diesem Setup mit dem Kommando “rwscmd / ginainstall” dauerhaft installiert werden.

Danach werden die Dateien der Client Software eingespielt und die Netzwerkkomponenten installiert.



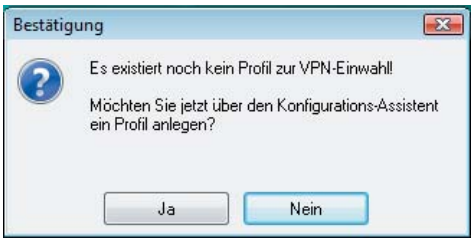

Damit ist die Installation der Client Software abgeschlossen. Die neuen Einstellungen werden erst wirksam, wenn Sie den Computer neu starten. Klikken Sie “Ja, Computer jetzt neu starten” und betätigen Sie den Beenden-Button, um Ihr System zu booten. (Abb. unten)



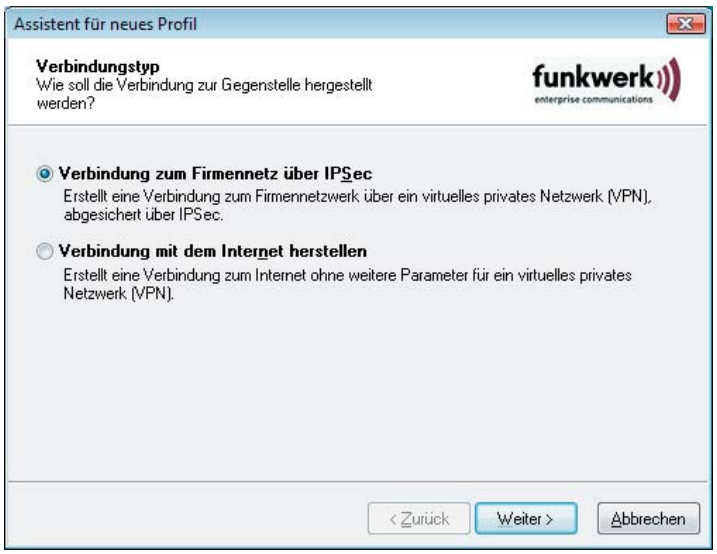
# Assistent für neues Profil

Nachdem Sie die Software installiert haben und zum Abschluss der Installation den Rechner gebootet haben, wird der Client Monitor automatisch nach dem Booten geladen (Abb. rechts).


Vorausgesetzt Sie haben den Secure Client zum ersten Mal installiert oder die Profil-Einstellungen gelöscht, wird automatisch der “Assistent für neues Profil” gestartet wenn Sie im Bestätigungsfenster (Abb. rechts mitte) auf “Ja” klicken. Sie befinden sich im Installationsverzeichnis (siehe **Deinstallation**).




Der Assistent (Abb. rechts unten) kann auch zu einem späteren Zeitpunkt gestartet werden. Dazu wird der Menüpunkt “Profil-Einstellungen” im Hauptmenü des Monitors unter “Konfiguration” aktiviert. Dort erstellen Sie die Profile wie im Handbuch zum **Client-Monitor** beschrieben.




Nutzen Sie den “Assistent für neues Profil”, so klicken Sie auf den Button “Weiter”. Dann legt der Assistent nach der Vorgabe Ihrer Daten ein Profil für eine IPSec-Testverbindung in den Profil-Einstellungen an.

## Testverbindung

Um die Einstellungen Ihres IPSec Clients auf Funktionstüchtigkeit hin zu uberprüfen, bietet Funkwerk Enterprise Communications einen entsprechenden öffentlichen Testzugang.

Eine detaillierte Konfigurationsanleitung zur Nutzung dieses VPN-Testzugangs in Verbindung mit dem FEC Secure IPSec Client finden Sie unter:
`www.funkwerk-ec.com.`

# Secure Client-Programme

Wenn der Secure Client installiert wurde, finden Sie in der Windows Programmgruppe, die Sie zur Installation angegeben haben, drei Programme:

**Secure Client Monitor**
**Secure Client Popup**
**Secure Client Tracer**
**Uninstall**

Haben Sie kein **Programm-Icon** zum Start des Secure Clients auf dem Desktop angelegt (siehe oben), so kann der Secure Client über den Menüpunkt **Secure IPSec Client Monitor** gestartet werden (siehe **Client-Monitor**).

Das **Secure IPSec Client Popup** zeigt an, ob es sich bei der Software um eine lizenzierte oder unlizenzierte Version handelt. Handelt es sich um eine unlizenzierte Testversion, so wird die Version der Software und die noch verbliebene Dauer der Gültigkeit in Tagen angezeigt. Die Software kann jederzeit nachträglich lizenziert werden. Der Aktivierungs-Dialog kann sowohl über den Aktivierungs-Button in der Hinweisleiste des Monitors als auch über das Monitormenü “Hilfe / **Lizenzinfo und Aktivierung**” geöffnet werden. (Abb. rechts)


Wurde die Software lizenziert, so wird die Seriennummer angezeigt, darunter die Software-Version einschließlich der Build-Nummer, sowie die Versionsnummer der lizenzierten Version. Zum Beispiel kann eine höhere Software-Version mit älteren Seriennummer und Aktivierungsschlüssel, sprich für eine niedrigere Version, lizenziert worden sein.

Der **Secure Client Tracer** ist ein eigenes kleines Anwendungsprogramm für qualifizierte Systemtechniker. Mit seiner Hilfe können Traces zur Fehlersuche erstellt werden.

## Unistall – Deinstallation

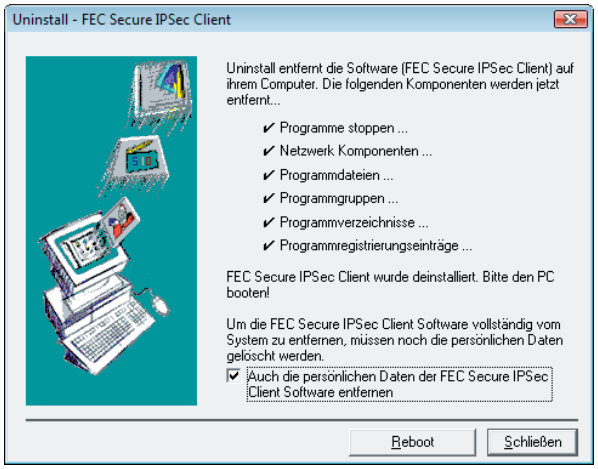
Zum Entfernen der Client Software kann zwischen zwei Optionen gewählt werden:

1. Sie wählen im Windows-Startmenü aus der Programmgruppe “FEC Secure IPSec Client” das Programm **Uninstall**.

Wenn Sie die Sicherheitsabfrage “FEC Secure IPSec Client deinstallieren” mit “Ja” beantworten, entfernt das Uninstall Shield Programm die Client Software von Ihrem PC.

2. Sie wählen im Windows-Startmenü nach den “Einstellungen” die Gruppe “Systemsteuerung”. Klicken Sie nun auf “Software” und wählen Sie den Client aus der Liste. Klicken Sie dann auf den Button mit “Hinzufügen / Entfernen”. Das Uninstall Shield Programm löscht nun die Client Software von Ihrem PC.

Wenn Sie den Client deinstalliert haben, erhalten Sie die Möglichkeit Ihre Konfigurationen und Profil-Einstellungen im Installationsverzeichnis des Clients zu behalten. Wird zu einem späteren Zeitpunkt eine neuere Version des Clients im gleichen Verzeichnis installiert, so können diese persönlichen Daten wieder genutzt werden. Sollen die persönlichen Daten des Clients auch gelöscht werden, so müssen Sie dies eigens bestätigen. In diesem Fall werden restlos alle Daten und Verzeichnisse des Clients entfernt. (Abb. unten)



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