funkwerk
enterprise communications

# Monitor

## des FEC Secure IPSec Clients

Wie Sie Funkwerk Enterprise Communications erreichen:

Funkwerk Enterprise Communications GmbH

Südwestpark 94
D-90449 Nürnberg
Germany
Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

# Der Monitor des Secure Clients

**Diese Dokumentation beschreibt das Design der Monitor-Oberfläche, sowie Auswertung und Benutzung der Anzeigemöglichkeiten. Dazu werden die Menüpunkte unter “Verbindung”, “Log” und “Fenster” beschrieben. Ausgenommen ist die Hotspot-Anmeldung, die unter Mobile Computing beschrieben ist.**

**Außerdem werden in dieser Dokumentation die Konfigurations-Sperren des IPSec Clients behandelt.**

## Inhaltsübersicht



Wie die Parameter-Einstellungen in den einzelnen Konfigurationsfenstern vorgenommen werden können, ist in der Dokumentation **Secure Client Parameter** beschrieben.

Am komfortabelsten erhalten Sie die gewünschten Informationen über **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.

## Start des Secure Clients

Wenn die Software nach den Standardvorgaben installiert wurde und ein erstes Profil eingerichtet wurde (siehe **Client Installation**), kann der Monitor über das Start-Menü “Programme / FEC Secure IPSec Client / Secure Client Monitor” aktiviert werden. Wird bei der Installation ein Icon auf dem Desktop angelegt, kann der Client auch mit Doppelklick auf das Icon gestartet werden. Damit öffnet sich das Fenster des Monitors auf dem Bildschirm (Bild unten).


*Programm-Icon*


*Client-Monitor nach erstem Start*

# Die Oberfläche des Client Monitors


Der Client Monitor besteht aus folgenden Bedien- und Anzeigefeldern von oben nach unten (Bild links):

Titelzeile mit Anzeige der Software-Variante, Hauptmenüleiste,

Profilauswahl mit einem Feld für die Amtsholung,

grafisches Statusfeld zur Anzeige des Verbindungsstatus und ggf. Fehlermeldungen,

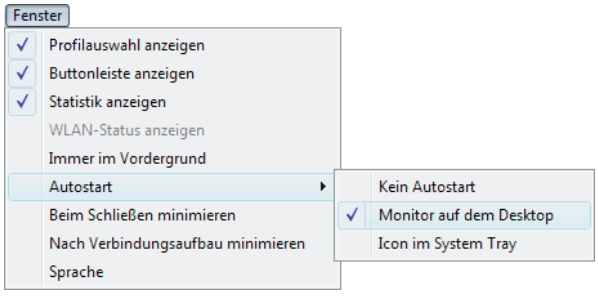
ggf. ein Feld mit der Anzeige der Signalstärke (wird nur für die Verbindungsarten **UMTS / GPRS** oder **WLAN** geöffnet, siehe Mobile Computing),

ggf. ein Feld zur Soft-Zertifikatsauswahl (beachten Sie dazu die Beschreibung in der Dokumentation **Zertifikate am Secure Client**),

der Buttonleiste mit “Verbinden” und “Trennen” und einem Statistikfeld.

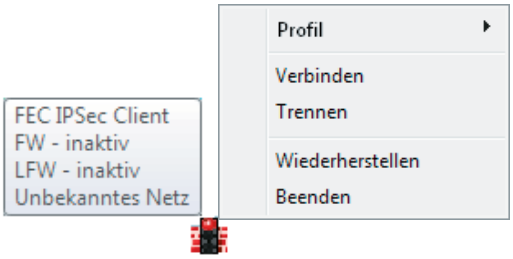
Die Benutzeroberfläche ist Windows-konform gestaltet. Die Bedienung erfolgt über die Pulldown-Menüs der Menüleiste, über die Buttons der Buttonleiste oder über das Kontextmenü (rechte Maustaste).

## Die Fensterdarstellungen des Monitors




Unter dem Menüpunkt “Fenster” (Abb. links) können Sie die Bedienoberfläche des Monitors variieren und die Sprache für die Oberfläche festlegen. Sind alle Anzeige- und Statistikfelder wie in nebenstehender Abbildung aktiviert, nimmt der Monitor seine größte Fläche ein, wie nach dem ersten Start.


Nach Ausblenden der einzelnen Bestandteile erscheint er am Ende in seiner kleinsten Form (Abb. links). Dabei lässt sich die Verbindungsart im Statistikfeld nicht mehr ablesen. Sie kann aber bei der Namensvergabe an das Zielsystem mit eingegeben werden, sodass sie auch im grafischen Statusfeld erscheint.




Wenn der Monitor mit dem Button [-] zum Icon verkleinert wird, erscheint er als Ampellicht im System Tray (Abb. links unten), wo in einer Quick-Info Firewall-Einstellungen und an der Ampelfarbe der Verbindungsstatus abgelesen werden können. (FW: **Personal Firewall**, LFW: **Link-Firewall**, Rot: keine Verbindung)

Mit einem rechten Mausklick auf das Symbol kann das mögliche Profil abgelesen und die Verbindung aufgebaut oder getrennt werden, bzw. bei abgebauter Verbindung der Monitor auch beendet werden.

## WLAN-Status anzeigen

Unabhängig vom Verbindungsmedium des aktuell selektierten Linkprofils kann das Feld zur grafischen Anzeige des WLAN-Status geöffnet bzw. geschlossen werden, wenn im Monitormenü “Konfiguration” unter “WLAN-Einstellungen” eine **WLAN-Konfiguration** aktiviert wurde.

Wurde eine **Multifunktionskarte** konfiguriert, ist dieser Menüpunkt nicht aktiv.

(Siehe PDF-Datei **Mobile Computing**)

## Immer im Vordergrund

Wenn Sie “Immer im Vordergrund” geklickt haben, wird der Monitor immer im Bildschirmvordergrund angezeigt, unabhängig von der jeweils aktiven Anwendung.

## Autostart

Mit diesem Menüpunkt wird der Monitor so eingestellt, dass er nach dem Booten selbständig startet. Folgende Optionen können eingestellt werden:

– kein Autostart: nach dem Booten nicht automatisch starten

– Icon im System Tray: nach dem Booten den Monitor starten und minimiert in der Task-Leiste darstellen

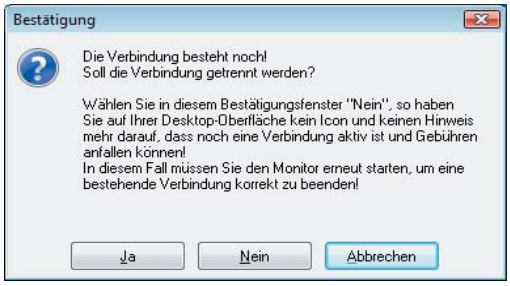
– Monitor auf dem Desktop: nach dem Booten den Monitor starten und in der eingestellten Fenstergröße darstellen

Wenn Sie oft mit der Secure Client Software arbeiten und die Informationen des Monitors benötigen, sollten Sie den Monitor auf dem Desktop starten lassen. Prinzipiell ist es für die Kommunikation mit der Gegenstelle nicht nötig, den Monitor zu starten.

## Beim Schließen minimieren

Der Monitor wird normalerweise über den Schließen-Button [x] rechts in der Kopfzeile oder über das Systemmenü links in der Kopfzeile geschlossen [Alt + F4] und als Anwendung beendet, sodass sowohl in der Task-Leiste als auch im Info-Bereich des Systems das Ampelsymbol des Monitors verschwindet.

Wird der Monitor auch bei einer bestehenden Verbindung auf diese Weise geschlossen, so informiert ein Bestätigungsfenster darüber, dass kein Ampelsymbol (Tray Icon) mehr erscheint, worüber der Status dieser Verbindung kontrolliert werden könnte. Dieses Bestätigungsfenster bietet drei Buttons an:




Ja = Damit wird die Verbindung vor dem Schließen des Monitors getrennt.

Nein = Der Monitor wird beendet aber die Verbindung wird nicht getrennt. In diesem Fall kann der Benutzer auf der Oberfläche seines Desktops nicht mehr erkennen, ob und wie lange noch Verbindungsgebühren anfallen, oder ob die Verbindung bereits beendet wurde. Um in diesem Fall den Status der Verbindung zu erfahren und sie gegebenenfalls korrekt zu beenden, muss der Monitor erneut gestartet werden.

Abbrechen = Das Bestätigungsfenster wird geschlossen, sodass die Verbindung ggf. korrekt getrennt werden kann, bevor der Monitor geschlossen wird. Auch kann nun die Fenster-Option **Beim Schließen minimieren** aktiviert werden.

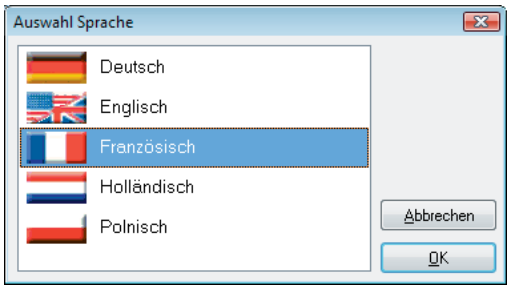
Wird **Beim Schließen minimieren** aktiviert, so wird ein versehentliches Beenden des Monitors durch den [x]-Button verhindert. Statt dessen wird er nur minimiert und erscheint als Ampelsymbol im Bereich des System-Info. Das Beenden des Monitors ist dann nur über das Hauptmenü “Verbindung / Beenden” möglich, woraufhin bei bestehender Verbindung wieder obiges Fenster erscheint.

## Nach Verbindungsaufbau minimieren

Wird diese Funktion aktiviert, so wird nach einem Verbindungsaufbau der Monitor in den Sys Tray (System-Info) als Ampelsymbol minimiert.

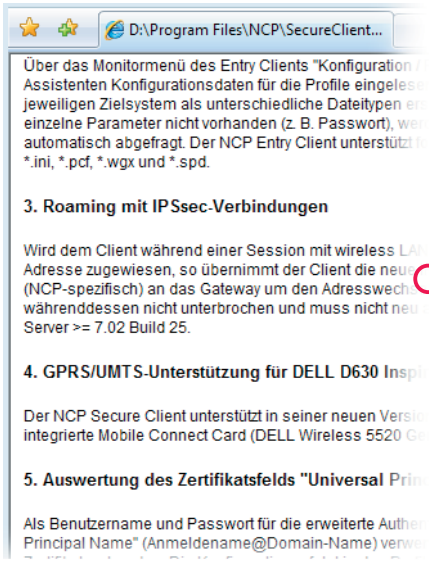
## Sprache

Die Standardsprache bei Auslieferung ist Deutsch. Um eine andere Sprache zu wählen, klicken Sie “Sprache” im Pulldown-Menü Fenster und wählen die gewünschte Sprache. Aktuell stehen folgende Sprachversionen zur Verfügung:



# Firmen- und Projektlogo in der Oberfläche des Clients

Bei der Installation der Client Software wird die Datei **Projectlogo.ini** im Installationsverzeichnis angelegt. In dieser Datei ist beschrieben wie ein Firmen- oder Projektlogo in der Oberfläche des Clients eingebaut werden kann, was bewirkt, dass bei einer Mausberührung des Logos eine Quick-Info angezeigt wird und mit einem Mausklick auf dieses Feld eine lokale HTML-Seite vom installierten Browser angezeigt wird.


In der Datei **Projectlogo.ini** können folgende Einträge gemacht werden:

```
[GENERAL]
Picture_96   = Logo
Picture_120  = Logo
ToolTip1     = Textzeile
HtmlLocal    = lokale HTML-Datei
```

## Logo

Das Logo erscheint in einem Panel des Clients ganz unten über die ganze Breite des Monitors (Abb. links). Für das Logo muss ein Bitmap (mit 96 oder 120 dpi) angelegt worden sein, mit 96 dpi für eine Bildschirmdarstellung mit kleinen Schriftarten, mit 120 dpi für eine Bildschirmdarstellung mit großen Schriftarten. Die Größe des Bitmaps ist vorgegeben mit “minimal 24 Pixel Höhe” und “genau 328 Pixel Breite” bei kleinen Schriftarten und “minimal 29 Pixel” und “genau 404 Pixel” bei großen Schriftarten. Das Bitmap kann in einem beliebigen lokalen Verzeichnis abgelegt werden. Wird es im Installationsverzeichnis abgelegt, muss zum Namen kein Pfad in der INI-Datei angegeben werden, ansonsten wird der Name des Bitmaps mit dem Pfad eingetragen.

## Textzeile

Textzeilen für eine Quick-Info werden mit fortlaufender Nummer pro Zeile angegeben, von ToolTip[1] bis ToolTip[n]. Zum Beispiel:

```
ToolTip[1] = Mit einem Mausklick erhalten Sie
ToolTip[2] = die Neuigkeiten zu diesem Client
```

## Lokale HTML-Seite

Die HTML-Datei, die angezeigt werden soll wenn ein Mausklick auf das Projekt-Logo erfolgt, muss in einem lokalen Verzeichnis auf dem Rechner verfügbar sein. Wird kein Pfad angegeben, wird die Datei aus dem Installationsverzeichnis des Clients gezogen. Zum Beispiel (Abb. links):

```
HtmlLocal = Neues.html
```

# Konfigurations- und Parameter-Sperren am Client

Die Konfigurations- und Parametersperren haben zwei wesentliche Funktionen. Zum einen kann damit die Komplexität der Konfigurationsmöglichkeiten reduziert werden, was dem Design der Software-Oberfläche ein schlankeres Aussehen verleiht. Dabei werden Parameterfelder für nicht benötigte Funktionen ausgeblendet, sodass der Benutzer nur die in seiner Umgebung relevanten Einstellungsmöglichkeiten vorfindet. Zum anderen können Voreinstellungen vorgenommen werden, die für den Benutzer unveränderbar sind, womit eine fehlerhafte Konfiguration und unerwünschte Verbindungsaufbauten ausgeschlossen werden können. Der Benutzer muss in diesem Fall nach der Installation nur seine persönlichen Kennwörter für den Verbindungsaufbau eingeben.

Die Konfigurationssperren am Client müssen vom Administrator am jeweiligen Anwender-PC benutzerspezifisch eingestellt werden.

### Begriffsklärung "Profil"

Um ein Profil zu ändern wird der Konfigurationsmenüpunkt **Profile** selektiert, ein Profil ausgewählt und dazu die **Profil-Einstellungen** geöffnet.

Die kompletten Profil-Konfigurationen werden als **Profile** mit spezifischem Namen im Konfigurationsmenü des Clients gespeichert.

In den Beschreibungen kann zur besseren Verständlichkeit ein **Profil** auch **Link-Profil** genannt werden, im Gegensatz zu WLAN-Profil, Zertifikatsprofil oder dergleichen.

Der Begriff Profil findet sich auch in verschiedenen Server-Komponenten wieder und bezeichnet innerhalb von Remote Access-Lösungen die komplette Konfiguration, die nötig und für bestimmte Eigenschaften (wie Sicherheit) erforderlich ist, um eine Client-Server-Verbindung herstellen zu können.

# Konfigurations-Sperren des IPSec Clients

Über die Konfigurations-Sperren im Hauptmenü (siehe Abb. unten) des Monitors kann das Konfigurations-Menü sowie die Einstellungsmöglichkeiten für die Profile so modifiziert werden, dass der Benutzer evtl. voreingestellte Konfigurationen nicht mehr abändern kann, bzw. ausgewählte Parameterfelder in den Profil-Einstellungen für den Benutzer nicht sichtbar sind.


Diese Sperren gelten in der definierten Form für alle am IPSec Client vorhandenen Link-Profile.

### Allgemein

Der Administrator legt die Konfigurations-Sperren benutzerspezifisch (personalisiert) für jeden Anwender-PC einzeln fest. Dabei wird als erstes jeweils eine ID für die Konfigurations-Sperre eingetragen, die sich aus "Benutzer" und "Passwort" zusammensetzt. (Diese ID kann für jeden Client eine andere sein).

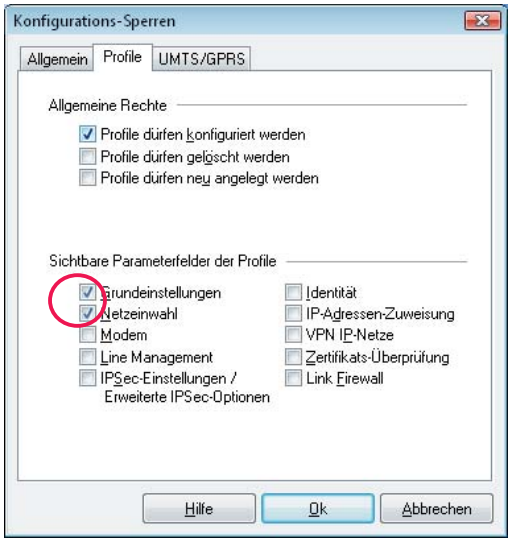
Bitte beachten Sie, dass die ID für das Festlegen und das Aufheben der Konfigurations-Sperre unbedingt nötig ist. Wird die ID vergessen, besteht keine Möglichkeit mehr, die Sperren wieder aufzuheben oder zu ändern!

Die Konfigurations-Sperren werden in der definierten Form für die drei Konfigurations-Felder wirksam, wenn die Einstellungen mit “OK” abgeschlossen werden. Wird der Abbrechen-Button gedrückt, wird auf die Standard-Einstellung zurückgesetzt.

Anschließend kann die Berechtigung, die Menüpunkte unter dem Hauptmenüpunkt “Konfiguration” zu öffnen, für den Benutzer eingeschränkt werden. Standardmäßig kann der Benutzer alle Menüpunkte öffnen und die Konfigurationen bearbeiten. Wird zu einem Menüpunkt der zugehörige Haken mit einem Mausklick entfernt, so wird dieser Menüpunkt grau dargestellt und lässt sich nicht mehr selektieren.

## Profile

Die Bearbeitungsrechte für die Konfigurations-Felder in den Profil-Einstellungen sind in drei Sparten unterteilt:
– Allgemeine Rechte
– Sichtbare Parameterfelder der Profile
– UMTS / GPRS




## Allgemeine Rechte

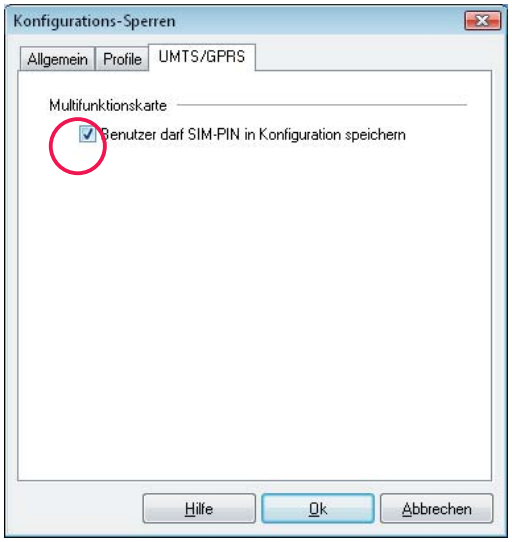
Die allgemeinen Rechte beziehen sich nur auf die Profil-Konfiguration (Abb. oben). Beispiel: Wird festgelegt “Profile dürfen neu angelegt werden” und “Profile dürfen konfiguriert werden” bleibt ausgeschlossen, so können zwar neue Profile definiert werden, eine nachfolgende Änderung einzelner Parameter ist jedoch nicht mehr möglich. Ist nur die Konfiguration von Profilen erlaubt, so können nur die vom Administrator vorgegebenen Profile modifiziert werden. Werden alle allgemeinen Rechte ausgeschlossen, so können nur bereits vorhandene Profile selektiert aber nicht betrachtet werden.

## Sichtbare Parameterfelder der Profile

Die genannten Konfigurations-Felder der Profil-Einstellungen können für den Benutzer ausgeblendet werden. Dabei ist zu beachten, dass Parameter eines nicht sichtbaren Feldes auch nicht konfiguriert werden können und umgekehrt, dass die Konfigurations-Felder auch nicht einsehbar sind, wenn die Profile nicht konfigurierbar sind. Im abgebildeten Beispiel links unten sind für alle vorhandenen Profile die Konfigurations-Felder “Grundeinstellungen” und “Netzeinwahl” konfigurierbar.

## GPRS / UMTS

Im Dialog zur Eingabe der SIM PIN für GPRS / UMTS-Karten (Multifunktionskarten) befindet die Option “SIM PIN in Konfiguration speichern”. Wird diese Funktion genutzt, so wird die einmal eingetragene SIM PIN für jedes Profil mit dem Verbindungsmedium GPRS / UMTS verwendet und muss nicht mehr eigens eingegeben werden.



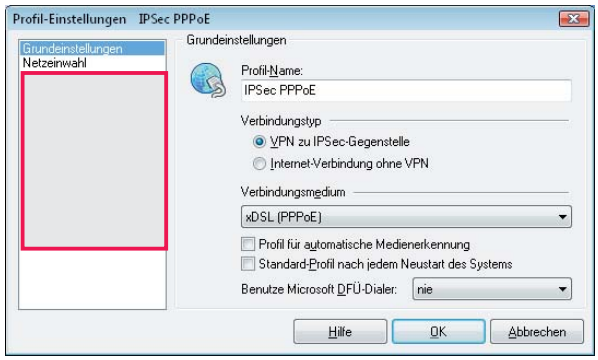

In der Standard-Einstellung des Clients ist diese Funktion nicht sichtbar. Sie wird dann für den Benutzer sichtbar und konfigurierbar, wenn ihm in den Konfigurations-Sperren unter “GPRS / UMTS” explizit die Berechtigung dazu erteilt wurde, d. h. “Benutzer darf SIM PIN in Konfiguration speichern” aktiviert wurde (siehe Abb. oben). Dies ist dann sinnvoll, wenn das Parameterfeld Modem unsichtbar geschaltet wurde wie in Abb. links, da der Benutzer die SIM PIN sonst bei jedem Verbindungsaufbau eingeben müsste.

Beachten Sie dazu die Beschreibungen:
**Secure Client Mobile Computing** und
**Secure Client Parameter**

## Die Darstellung der Sperren in der Oberfläche des Clients

Nachdem die Konfigurations-Sperren eingeschaltet sind, stellt sich das Konfigurationsmenü des Clients wie in untenstehender Abbildung dar.


Die Konfigurations-Felder eines Profils sehen z. B. wie unten dargestellt aus.




Die Konfigurationsfelder, die für den Benutzer nicht konfigurierbar bleiben sollen, werden nicht mehr dargestellt.

## Aufheben der Sperren

Eine Aufhebung oder Änderung der Sperren sollte nur über den Administrator erfolgen, da nach Bekanntgabe der ID für die Konfigurations-Sperre keine Konfigurationssicherheit mehr gewährt werden kann.

Nach Bekanntgabe der ID für die Konfigurations-Sperre sollte der Administrator baldmöglichst ein neues Telefonbuch mit neuen Profil-Einstellungen bzw. einer neuen ID für die Konfigurations-Sperre am Client des Anwenders einspielen.

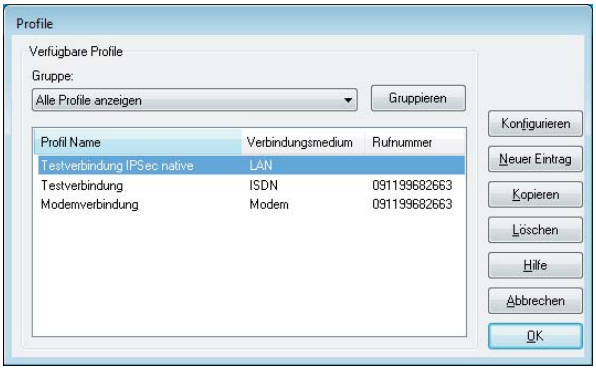

Sowohl das Aufheben der Konfigurations-Sperre über das Verbindungsmenü (womit alle Sperren gelöscht werden, siehe Abb. oben) als auch das Ändern der Sperren über das Konfigurationsmenü erfordern die gleiche ID (siehe Abb. unten).


# Profile am Client anlegen

Sofern dem Anwender nach einem Rollout gestattet ist eigene Profile anzulegen oder der Anwender nach einer Standard-Installation neue Profile anlegen möchte, geht er wie folgt vor.

Nach einer Standard-Installation der Client Software sind noch keine Profile vorhanden. In diesem Fall wird automatisch ein Assistent (siehe **Client-Installation**) eingeblendet, der dabei hilft Profile anzulegen. Damit werden zugleich die ersten Profile angelegt, deren Einträge nach belieben modifiziert werden können. Dies erfolgt über das Konfigurationsmenü des Monitors unter “Profile”. (Abb. unten)


Nachdem dieser Menüpunkt selektiert wurde, werden die bereits vorhandenen Profile in einer dreispaltigen Liste mit Name, Verbindungsart und Rufnummer gezeigt. (Abb. unten)

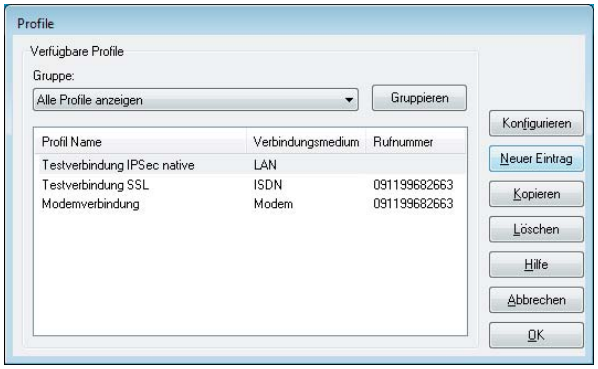



Die Buttons auf der rechten Seite der Profil-Einstellungen können nicht betätigt werden, wenn die entsprechenden Sperren eingestellt sind. Beachten Sie dazu oben “Die Darstellung der Sperren ...” für den IPSec Client.

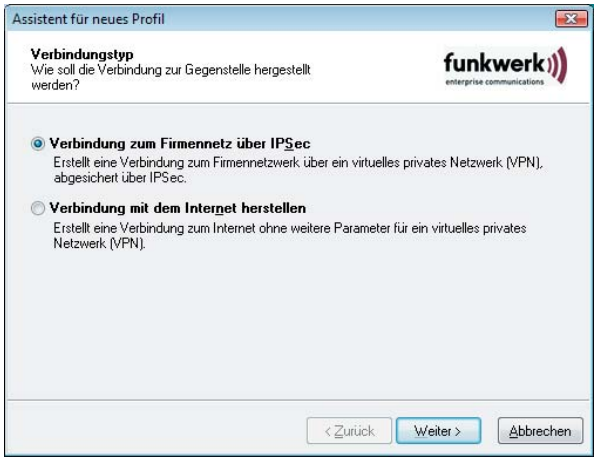
Wurden keine Einschränkungen für die Profil-Einstellungen vorgegeben, können alle Buttons betätigt und die darauf vermerkten Funktionen ausgeführt werden.

## Neues Profil mit Konfigurations-Assistent

Um ein neues Profil zu definieren, klicken Sie auf “Neuer Eintrag”.




Jetzt legt der Konfigurations-Assistent mit Ihrer Hilfe ein neues Profil an.




Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Profil angelegt. Für alle weiteren Parameterfelder des Profils werden Standardwerte eingetragen, die Sie nach dem Fertigstellen des Profils nach einem Klick auf den Konfigurieren-Button jederzeit abändern können.

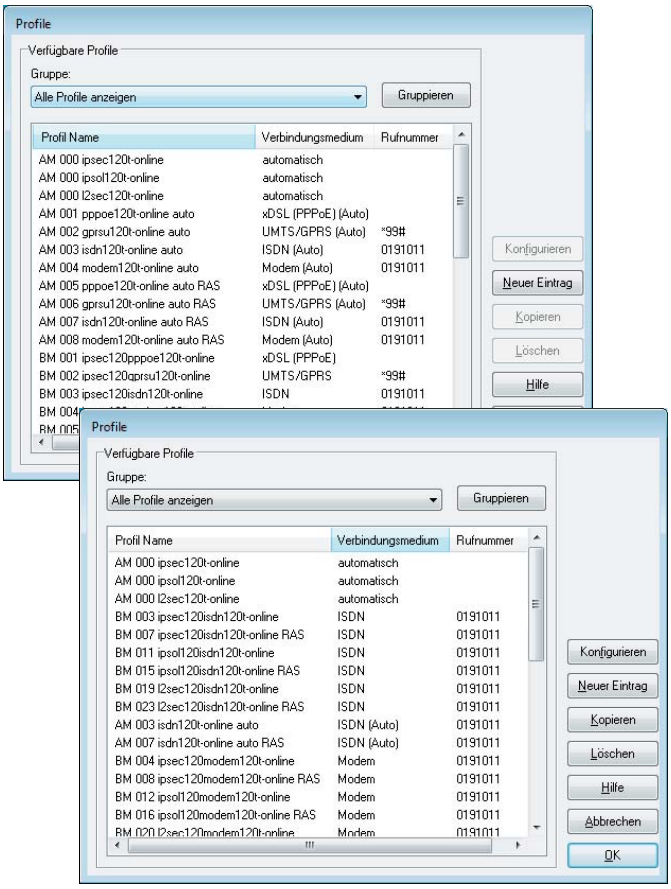
Der Assistent für ein neues Profil bietet unterschiedliche Typen von Verbindungen an. Nach Auswahl dieses Verbindungstyps wird nach wenigen Abfragen das neue Profil angelegt. Im folgenden die jeweils nötigen Daten zur Konfiguration:

| | Konfigurationsfelder: |
|---|---|
| **Verbindung zum Firmennetz über IPSec** | |
| – Profil-Name | **Grundeinstellungen** |
| – Verbindungsmedium | |
| – Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer) | **Netzeinwahl** |
| – VPN Gateway-Parameter (IP-Adresse) | **IPSec-Einstellungen** |
| – Nutzung von Zertifikaten | **Identität** |
| – Zugangsdaten für XAUTH (Benutzername, Passwort) | |
| – IPSec-Konfiguration (Exch. Mode, PFS-Gruppe, Kompression) | **IPSec-Einstellungen** |
| – Statischer Schlüssel (Preshared Key), ohne Zertifikat (IKE ID-Typ, IKE ID) | |
| – IP-Adressen-Konfiguration (IP-Adresse des Clients, DNS / WINS-Server) | **IPSec-Adresszuweisung** |
| – Firewall-Einstellungen | **Link Firewall** |
| **Verbindung mit dem Internet herstellen** | |
| – Profil-Name | **Grundeinstellungen** |
| – Verbindungsmedium | |
| – Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer) | **Netzeinwahl** |
| – Firewall-Einstellungen | **Link Firewall** |

**Zu weiteren Parametereinstellungen beachten Sie bitte die Secure Client Parameter. Dort sind für die Konfigurationsfelder und deren Parameter für den IPSec Client beschrieben. Mit einem Mausklick gelangen Sie dorthin.**

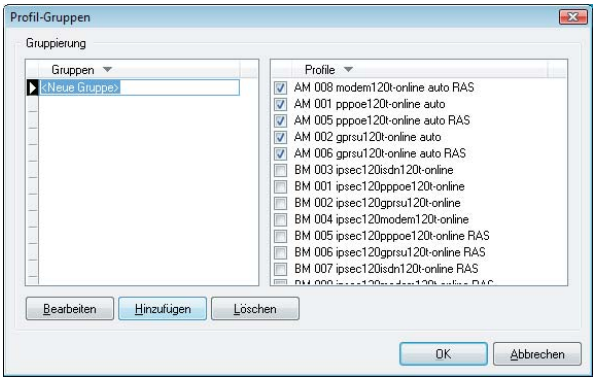
**Oben in der rechten Spalte sind die Konfigurationsfelder der Profil-Einstellungen aufgeführt, worin die abgefragten Daten einzugeben sind. Mit einem Mausklick auf den jeweiligen Begriff gelangen Sie sofort zu deren Beschreibung.**

## Profil-Gruppen

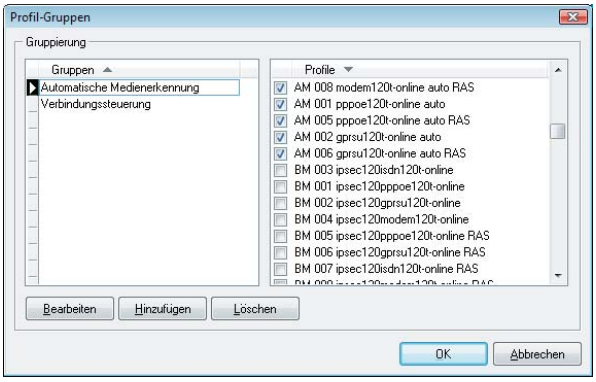



In der Anzeige aller Profile können diese nach ihrem Namen, nach der Verbindungsmedium und, sofern es sich um eine Wählverbindung handelt, nach der Rufnummer sortiert werden. (Abb. links)

Sollte die Liste der Profile zu lang sein, so können die Profile auch gruppiert werden. Dazu wird auf den Gruppieren-Button über der Rufnummernanzeige geklickt und die Gruppen-Konfiguration geöffnet (Abb. links unten).



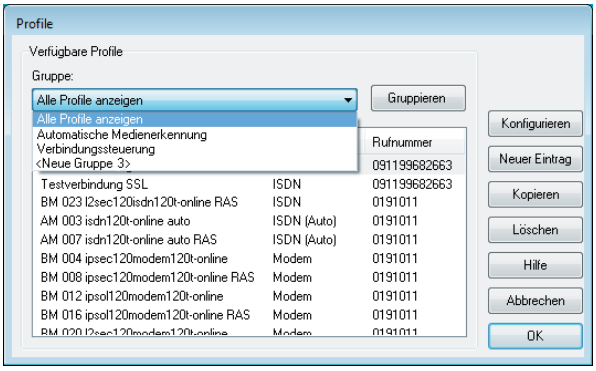

Mit “Hinzufügen” wird eine neue Gruppe in die linke Spalte eingefügt, der Sie einen eigenen Namen geben können, z. B. Gruppe “Automatische Medienerkennung” wenn Sie diese Profile in einer Gruppe zusammenstellen möchten. (Abb. links)




In der rechten Spalte können Sie mit einem Haken selektieren, welche Profile zu der Gruppe gehören sollen, die in der linken Spalte angezeitg wird. Mehrfache Zuordnungen von Profile zu verschiedenen Gruppen sind möglich. (Abb. links)

Der Bearbeiten-Button dient der Namensänderung der Gruppe. Mit dem Löschen-Button wird die jeweils aktuell angezeigte Gruppe gelöscht und die entsprechende Gruppenzugehörigkeit eines Profils, nicht aber das Profil selbst.

## Gruppen-Anzeige




Unter den verfügbaren Profilen können nun alle Profile angezeigt werden oder alternativ dazu auch nur die Profile einer ausgewählten Profil-Gruppe. (Abb. links)


In der Oberfläche des Monitors wird im Bereich der Profilauswahl ein Infotext eingeblendet, ...


... wonach auch hier die Anzeige aller Profile oder nur die Profile einer bestimmten Gruppe ausgewählt werden kann.

# Symbole und Meldungen im grafischen Anzeigefeld

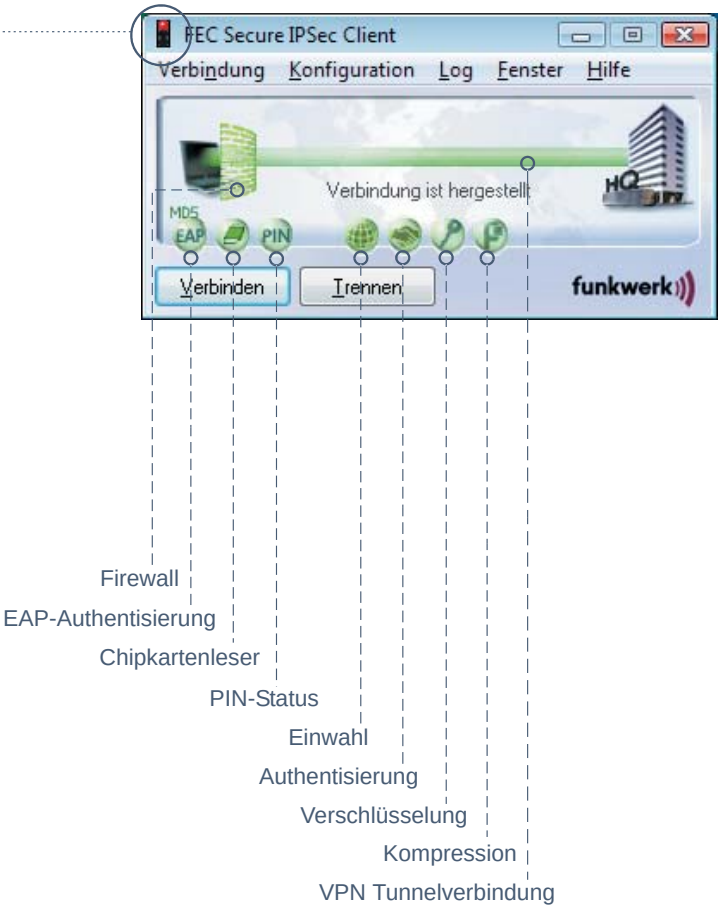
## Die Symbole des Monitors

Die Monitoroberfläche des Clients ist informativ mit Symbolen gestaltet. Je nach Anzeige und Farbe geben sie Auskunft über den aktuellen Status der Verbindung oder einzelne konfigurierte Features.

Das Ampelsymbol ist immer sichtbar wenn der Client gestartet ist. Ist der Monitor minimiert, d. h. geschlossen, erscheint es in der Task-Leiste. Mit einem Doppelklick auf dieses Icon kann der Monitor wieder geöffnet werden. Erst wenn der Monitor beendet wird, verschwindet auch das Ampelsymbol.

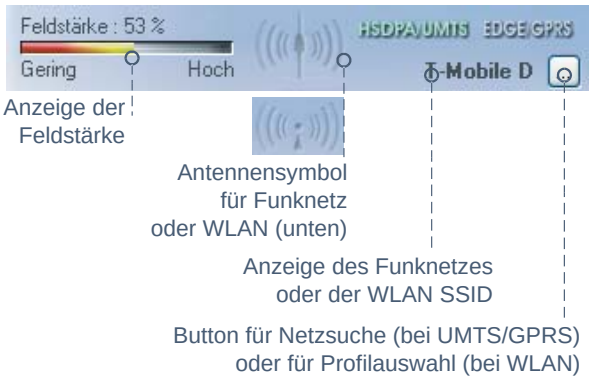
Eine rote Ampelbedeutet “keine Verbindung”, eine gelbe zeigt den Verbindungsaufbau an und eine grüne Ampel – auch in der Task-Leiste – symbolisiert immer eine bestehende Verbindung, für die ggf. Gebühren anfallen.

Die weiteren Symbole sind auf den folgenden Seiten ausführlich erklärt.



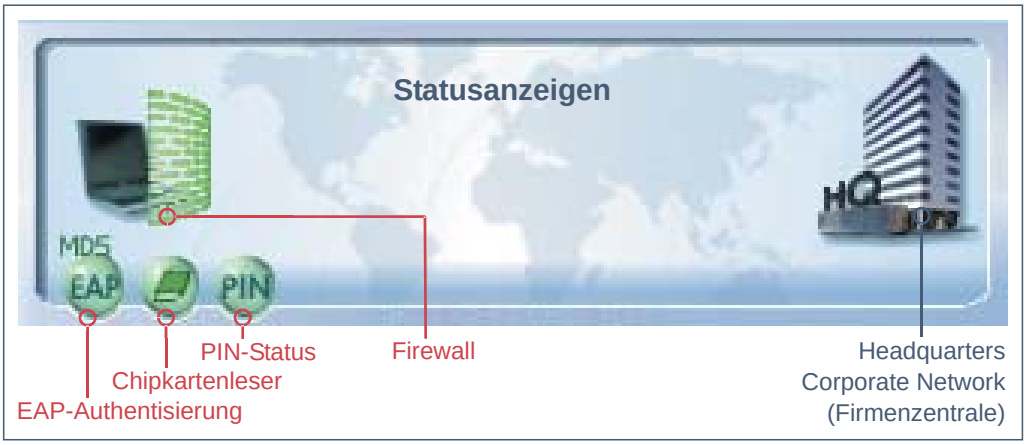

Je nach Konfiguration und Installation einer Multifunktionskarte erscheint zusätzlich alternativ ein **WLAN**- oder **UMTS / GPRS**-Panel im Monitor.

Im UMTS / GPRS-Panel kann das gewünschte Datenübertragungsverfahren durch Klick auf den jeweiligen Schriftzug gewählt werden. Es wird dann grün dargestellt.



# Statusanzeigen

Das grafische Feld des Client-Monitors zeigt je nach Konfiguration verschiedene Icons, sie während der Phasen des Verbindungsaufbaus einen jeweils verschiedenen Status annehmen können. Hinweise zu ihrer Bedeutung geben Kurzinfos, sobald der Mauszeiger über eines der Icons streift. Im folgenden sind die Statusanzeigen, wie in untenstehender Abbildung, von links nach rechts beschrieben.




## EAP-Authentisierung

Wenn eine erweiterte Authentisierung mittels Extensible Authentication Protocol (EAP) in den "EAP-Optionen" aktiviert wurde, wird dies mit dem EAP-Icon angezeigt. Die Farbe **Gelb** symbolisiert die EAP-Verhandlungsphase, **Rot** eine fehlgeschlagene Authentisierung, die Farbe **Grün** die erfolgreiche Authentisierung mit EAP. Durch einen Doppelklick auf das EAP-Symbol kann das EAP zurückgesetzt werden. Anschließend erfolgt automatisch eine erneute EAP-Verhandlung.

Bei erfolgreicher Authentisierung gegenüber einer Netzwerkkomponente, gibt die Gegenstelle zurück, welches Protokoll verwendet wurde, was immer mit einem Symbol in **Grün** und der Bezeichnung MD5 oder TLS dargestellt wird.

Erscheint EAP-Symbol in der Farbe **Rot** und die Verbindung wurde trotzdem aufgebaut, so bedeutet dies, dass im Client EAP konfiguriert wurde, die Netzwerkkomponente jedoch kein EAP benötigt.

## Chipkartenleser

Wurde ein Chipkartenleser installiert und konfiguriert (siehe die Beschreibung **Secure Client Zertifikate**), so wird sein Symbol in **Blau** dargestellt.

Wird die Chipkarte in den Leser gesteckt, wechselt die wird das Symbol in **Grün** dargestellt.

## PIN-Status

Ein PIN-Symbol in der Farbe **Grau** symbolisiert immer, dass die PIN für das jeweils konfigurierte Zertifikat noch eingegben werden muss. Ein Doppelklick auf dieses Symbol öffnet den Dialog zur Eingabe der PIN. Ein falsche PIN wird mit einer Fehlermeldung quittiert, wobeigleichzeitig die noch möglichen PIN-Eingaben heruntergezählt werden.

Nach korrekter PIN-Eingabe wird das Symbol in **Grün** dargestellt. Diese Farbe zeigt an, dass die eingegebene PIN gültig ist, auch wenn keine Verbindung aufgebaut ist! Wollen Sie sicherstellen, dass kein Unbefugter bei Ihrer Abwesenheit eine Verbindung herstellen kann, so muss die PIN zurückgesetzt werden (im Verbindungsmenü des Monitors PIN zurücksetzen) oder unter "Konfiguration / Zertifikat" die Funktion "PIN-Abfrage bei jedem Verbindungsaufbau" aktiviert sein. In letzterem Fall erscheint der Dialog zur PIN-Eingabe nicht nach Doppelklick auf das graue Symbol, sondern erst vor dem Verbindungsaufbau.

(Siehe auch die Beschreibung **Secure Client Zertifikate**)

## Firewall

Das Firewall-Symbol ist immer dann sichtbar, wenn eine Firewall aktiviert ist. Ist die globale Firewall (Personal Firewall) mit definierten Regeln aktiv und die link-spezifische Firewall nicht aktiv, so wird das Symbol ohne Pfeile in der Farbe **Rot** dargestellt.

Wurde vom Administrator ein Friendly Net (Friendly Net Detection) festgelegt, und befindet sich der Client darin, so wird das Firewall-Symbol in der Farbe **Grün** dargestellt. Die Friendly Net Detection wird im Monitor-Konfigurationsmenü unter “Firewall-Einstellungen / Bekannte Netze” vorgenommen, entweder indem ein statisches Netzwerk angegeben wird, oder indem die automatische Erkennung der bekannten Netze aktiviert wird. Siehe dazu die Beschreibung unter “Firewall-Einstellungen / Konfigurationsfeld - Bekannte Netze”.

Bei aktivierter Link Firewall wird das Symbol mit Pfeilen dargestellt, gleich ob die globale Firewall aktiv oder inaktiv ist.

Wird die Link Firewall im Telefonbuch aktiv geschaltet mit “Stateful Inspection aktivieren / immer” und wird konfiguriert, dass eine Kommunikation ausschließlich im Tunnel zugelassen wird, so wird das Firewall-Symbol mit **zwei rote**n **Pfeile**n dargestellt.

Wird die Option “Ausschließlich Kommunikation im Tunnel zulassen” ausgeschaltet, während Stateful Inspection eingeschaltet ist, so wird das Symbol mit einem **grünen und einem roten Pfeil** dargestellt.

Wird Stateful Inspection nur bei einer bestehenden Verbindung aktiviert, so erscheinen die Pfeil-Symbole nur nach einem Verbindungsaufbau.

Die **Pfeil-Symbole** erscheinen **vor einer grünen Firewall**, wenn zusätzlich zu Optionen der Link Firewall ein Friendly Net in der globalen Firewall definiert wurde, worin sich der Client aktuell befindet.

# Symbole des Verbindungsaufbaus

Neben den Statusanzeigen enthält das grafische Feld des Client-Monitors auch Symbole des Verbindungsaufbaus.


## Symbole der NAS-Einwahl

Findet eine Einwahl zu einem Network Access Server bzw. Internet-Dienste-Anbieter (ISP) ins Internet statt, so wird die Einwahlverbindung mit einer dünnen gelben Linie symbolisiert. Die Einwahl ist abgeschlossen und die Verbindung zum ISP erfolgreich hergestellt, wenn die dünne Verbindungslinie die Farbe Grün annimmt.

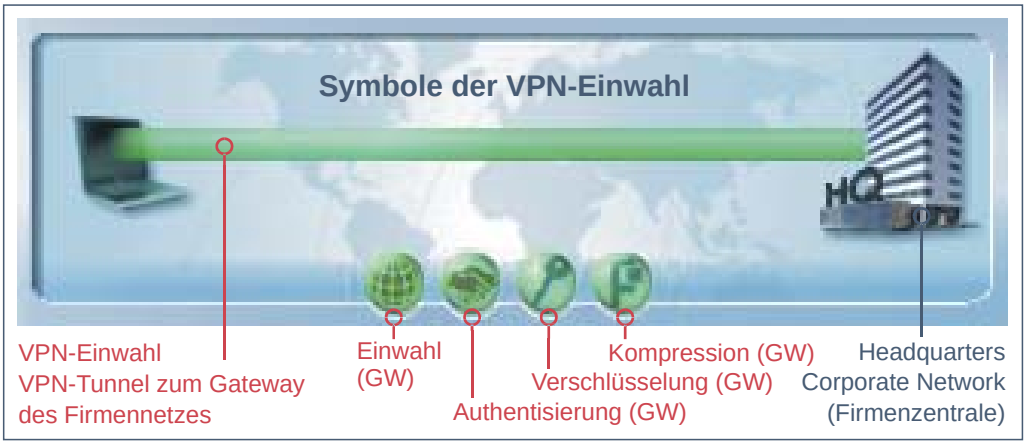
Gleichzeitig mit dem Start des Verbindungsaufbaus ändern sich auch die Farben der Symbole für die NAS-Einwahl.

Die Einwahl am ISP ist mit einem Globus dargestellt, die Authentisierung am ISP mit einem Händeschütteln. Die Farben wechseln während des Verbindungsaufbaus von grau  zu blau  , blinken dann grün, um schließlich bei erfolgreichem Verbindungsaufbau grün stehen zu bleiben.

Die Parameter für die NAS-Einwahl befinden sich in den Profil-Einstellungen unter “Netzeinwahl”. Soll das Profil für die “automatische Medienerkennung” verwendet werden, so muss unter “Netzeinwahl” unbedingt ein Benutzername und ein Passwort eingegeben sein.

## Symbole der VPN-Einwahl

Nach abgeschlossener NAS-Einwahl kann die VPN-Einwahl zum Firmen-Gateway stattfinden. Dabei wird die Einwahlverbindung mit einer dicken gelben Linie symbolisiert. Die Einwahl ist abgeschlossen und die Verbindung zum VPN Gateway erfolgreich hergestellt, wenn die dicke Verbindungslinie die Farbe Grün annimmt (Abb. unten).




Gleichzeitig mit dem Start des Verbindungsaufbaus zum Gateway ändern sich auch die Farben der Symbole für die VPN-Einwahl. Die Einwahl und die Authentisierung am VPN Gateway ist genauso wie bei der NAS-Einwahl dargestellt. Hinzu kommen noch die Symbole für die Schlüsselverhandlung (Schlüssel) und die Kompression (Zange), sofern deren Konfiguration von Seiten des Gateways vorgeschrieben ist.

Die Farben der Symbole der VPN-Einwahl wechseln von grau zu blau, blinken dann grün, um schließlich bei erfolgreichem Verbindungsaufbau grün stehen zu bleiben. Dabei muss der Vorgang der Einwahl und Authentisierung am VPN Gateway immer durchlaufen werden, Verschlüsselung und Kompression sind optional. Die Symbole der VPN-Einwahl sind von links nach rechts:

### Einwahl am VPN Gateway

Die Zieladresse des VPN-Gateways wird in den Profil-Einstellungen unter “IPSec-Einstellungen / Gateway” angegeben.

### Authentisierung am VPN Gateway

Die nötigen Parameter befinden sich in den Profil-Einstellungen unter “Identität”. Verwendet wird immer “Extended Authentication (XAUTH)”. Benutzername und Passwort werden entweder aus der Konfiguration unter diesem Parameter oder aus einem Zertifikat ausgelesen. Ein zu verwendendes Zertifikat wird im Monitor-Menü unter “Konfiguration / Zertifikate” konfiguriert, wobei das Aussteller-Zertifikat des anzuwählenden Gateways mit dem Benutzer-Zertifikat zusammenpassen muss.

### Verschlüsselung

Zur Verschlüsselung dient entweder ein Pre-shared Key oder der Private Key aus einem Zertifikat. Beide Alternativen werden in den Profil-Einstellungen unter “Identität” eingestellt. Wird der “Pre-shared Key” verwendet, muss das “Shared Secret” hier eingetragen werden. Wird der “Pre-shared Key” nicht verwendet, wird automatisch das Zertifikat benutzt. Welche Verschlüsselung benutzt werden muss gibt das Gateway vor.

### Kompression

Kompression wird nur genutzt, wenn sie auch vom Gateway unterstützt wird. Eingestellt wird sie in den Profil-Einstellungen unter “Erweiterte IPSec-Optionen / IP-Kompression verwenden”.

# Profilauswahl und Verbindungsaufbau

Sobald die Software installiert und ein Profil korrekt konfiguriert wurde, kann der Verbindungsaufbau zur Gegenstelle stattfinden.

Das gewünschte Profil wird über die Auswahl-Box unter dem Hauptmenü oder nach Klick auf die rechte Maustaste aus der angezeigten Profilliste gewählt.

Um eine Verbindung zum selektierten Profil bzw. zur Gegenstelle herzustellen, ist es *nicht* nötig, den Client Monitor eigens zu starten oder die Anwahl manuell durchzuführen. Lediglich die gewünschte Applikations-Software muss gestartet werden. Die Verbindung kann dann, entsprechend der jeweiligen Profil-Einstellungen, automatisch aufgebaut werden. Natürlich ist es auch möglich, eine Verbindung manuell über das Monitormenü oder den Verbinden-Button herzustellen.


Eine bestehende VPN-Verbindung (Abb. oben) wird mit einem dicken grünen, durchgehenden Balken zwischen Client und Server dargestellt, unter dem der Text “Verbindung ist hergestellt” eingeblendet wird.

Gleichzeitig wird die (Icon-)Ampel grün. Eine grüne Ampel – auch in der Task-Leiste – symbolisiert immer eine bestehende Verbindung, für die ggf. Gebühren anfallen. Wollen Sie das Verbindungsaufkommen kontrollieren, dann beachten Sie die Beschreibung zum Budget-Manager.

## Verbindungsaufbau zur Gegenstelle

Die Art des Verbindungsaufbaus ist in den Profil-Einstellungen konfigurierbar. Sie können aus drei Anwahl-Modi für den Verbindungsaufbeu wählen: automatisch, manuell und wechselnd.

Beachten Sie dazu auch in der Parameterbeschreibung den Abschnitt zu Verbindungssteuerung und dem automatischen Verbindungsaufbau.

### Automatischer Verbindungsaufbau

Im Unterschied zur Microsoft RAS-Technik, unter deren Verwendung die Verbindung zur Gegenstelle manuell hergestellt werdenmuss, arbeitet die Client Software nach dem Prinzip der LAN-Emulation. Dabei ist es lediglich erforderlich, die entsprechende Applikations-Software zu starten (Email, Internet Browser, Terminal Emulation, etc.). Die Verbindung wird dann, entsprechend den Parametern der Profil-Einstellungen, automatisch aufgebaut und gehalten.

### Manueller Verbindungsaufbau

Manuell wird die Verbindung über das Monitormenü “Verbindung / Verbinden” oder mittels Verbinden-Button hergestellt.

### Wechselnder Verbindungsaufbau

Wird “wechselnder Verbindungsaufbau” gewählt, muss zunächst die Verbindung “manuell” aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau wie folgt:
– Wird die Verbindung mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung “automatisch” hergestellt,
– wird die Verbindung “manuell” abgebaut, muss sie auch wieder “manuell” aufgebaut werden.

### Verbinden

Gleich wie die Verbindung aufgebaut wird, der Monitor, sofern er im Vordergrund sichtbar ist, zeigt immer den Status des Verbindungsaufbaus wie im Abschnitt “Symbole des Verbinungsaufbaus” beschrieben.

# Passwörter und Benutzernamen

Das Passwort (siehe Profil-Einstellungen / Netzeinwahl) wird benötigt, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können. Es darf bis zu 128 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort von der Gegenstelle zugewiesen, da Sie von ihr auch erkannt werden müssen. Sie erhalten es vom Internet Service Provider oder dem Systemadministrator.

Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.

Auch wenn Sie für den Verbindungsaufbau “automatisch“ gewählt haben, müssen Sie die Verbindung beim ersten Mal manuell aufbauen und das Passwort eingeben. Für jeden weiteren automatischen Verbindungsaufbau wird das Passwort selbständig übernommen, bis der PC erneut gebootet oder das Zielsystem gewechselt wird. D. h. für eine Reihe von “automatischen” Verbindungsaufbaus wird das Passwort nach der ersten Eingabe und dem ersten Verbindungsaufbau selbständig übernommen, auch wenn die Funktion “Passwort speichern” (siehe Profil-Einstellungen / **Netzeinwahl**) nicht aktiviert wurde. Erst ein Boot-Vorgang löscht das einmal eingegebene Passwort.

Soll das Passwort mit dem Booten nicht gelöscht werden, so muss die Funktion “Passwort speichern” aktiviert werden (siehe Profil-Einstellungen / Netzeinwahl). Bitte beachten Sie dabei, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Client Software arbeiten kann – auch wenn er die Passwörter nicht kennt.

## Benutzername für NAS-Verbindung

Der **Benutzername** für die Verbindung zum Internet muss immer in den Profil-Einstellungen eingegeben werden. Ohne diesen Benutzernamen kann keine Verbindung zum NAS erfolgen.

## Benutzername und Passwort für VPN-Verbindung

**VPN-Benutzername** und -Passwort für die VPN-Verbindung zum Gateway (siehe Profil-Einstellungen / **Identität**) können in den Profil-Einstellungen vollständig eingegeben werden. Wenn sie nicht eingegeben werden, werden sie beim Aufbau der VPN-Verbindung in einem Dialog abgefragt.

## Passwort für OTP-Token

Ein Einmal-Passwort, sofern ein OTP-Token verwendet wird, sowie die zugehörige PIN werden immer abgefragt (siehe Secure Client Parameter, **Verbindungssteuerung**). Je nachdem ob das OTP-Token für die NAS- oder die VPN-Verbindung verwendet wird, erscheint der entsprechende Dialog.

## Client Logon

Soll bei der Windows-Anmeldung eine Anmeldung an einem Domain Server erfolgen und es besteht noch keine Netzwerkverbindung, so muss die NCP GINA eingesetzt werden. Die Einstellungen dafür können in den **Logon-Optionen** des Konfigurationsmenüs vorgenommen werden, sofern sie bei der Installation aktiviert wurden (siehe **Client Installation**).

Der Verbindungsaufbau erfolgt bei einer Domänen-Anmeldung über VPN prinzipiell genauso, wie unter **Symbole des Verbindungsaufbaus** beschrieben. Nach der Auswahl des Profils wird mit Klick auf den OK-Button der Verbindugsaufbau eingeleitet. Nach Eingabe von Benutzername und Passwort, muss die PIN eingegeben werden, sofern die Verwendung eines (Soft-)Zertifikats konfiguriert wurde. Die weiteren Stationen des Verbindungsaufbaus erfolgen genauso wie oben beschrieben.

# Verbindungsabbau

Eine aktive Verbindung kann durch Fehler, durch einen Timeout-Automatismus, wie auch durch den Benutzer manuell abgebaut werden.

Wenn die Verbindung abgebaut wird, verschwindet die im Monitor dargestellte farbliche Verbindungslinie und die Farbe des Ampellichts wechselt für die gesamte Offline-Dauer auf rot.

## Verbindungsabruch und Fehler

Ereignet sich beim Verbindungsaufbau ein Fehler, so wird die Verbindung nicht hergstellt und die Fehlerursache im Monitor angezeigt. Ebenso wird bei einer physikalischen Unterbrechung der Verbindung eine Fehlermeldung generiert. Beachten Sie dazu weiter unten die Hinweise zu den Fehlermeldungen im Monitor und im Client Info Center.

## Verbindung manuell trennen

Wichtig: Eine bestehende Verbindung wird nicht getrennt bzw. abgebaut indem Sie den Monitor des Clients (mittels [x]-Button) beenden bzw. schließen. Beachten Sie dazu auch oben die Beschreibung zu den Fensterdarstellungen des Monitors und den Abschnitt “Beim Schließen minimieren”.

Eine Verbindung wird sachgerecht abgebaut indem entweder über das Monitormenü “Verbindung / Trennen” selektiert wird oder im Kontextmenü der rechten Maustaste die Funktion zum Trennen der Verbindung gewählt wird.

Wenn Sie die Möglichkeit behalten wollen, jederzeit die Verbindung manuell abbauen zu können, setzen Sie den Verbindungsaufbau auf “manuell” und deaktivieren den automatischen Timeout, indem Sie ihn auf Null (0) setzen. Die Konfiguration des Timeouts erfolgt in den Profil-Einstellungen unter Verbindungssteuerung.

## Automatischer Verbindungsabbau

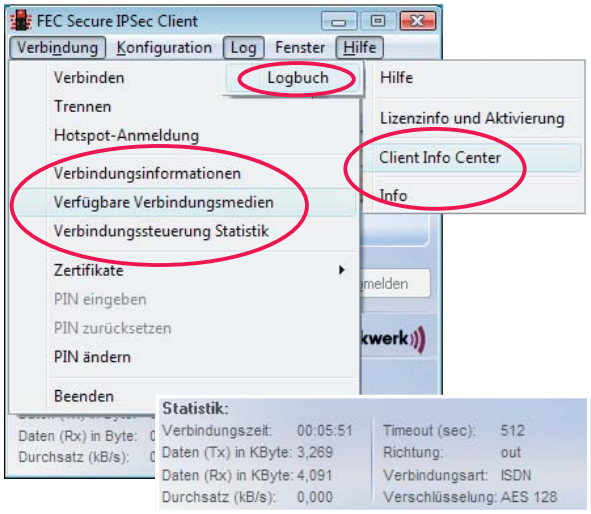
Ein automatischer Verbindungsabbau erfolgt wenn Sie den Timeout aktiviert haben. Mit diesem Parameter wird der Zeitraum festgelegt, der nach der letzten Datenbewegung (Empfang oder Versenden) verstreichen muss, bevor automatisch ein Verbindungsabbau erfolgt. Der Wert wird in Sekunden zwischen 0 und 65535 angegeben. Der Standardwert ist “100". Mit dem Wert ”0" wird der automatische Verbindungsabbau nicht ausgeführt.

Wenn Ihr Anschluss einen Gebührenimpuls erhält, verwendet die Secure Client Software das Impulsintervall, um den optimalen Zeitpunkt des Verbindungsabbaus bezüglich dem von Ihnen gesetzten Wert zu ermitteln. Der nach Gebührentakt optimierte Timeout läuft im Hintergrund und hilft die Verbindungskosten zu reduzieren.

Der Timer für das gewählte Zeitintervall läuft erst dann an, wenn keine Datenbewegung oder Handshaking mehr auf der Leitung stattfindet.

# Informationsfenster des Clients

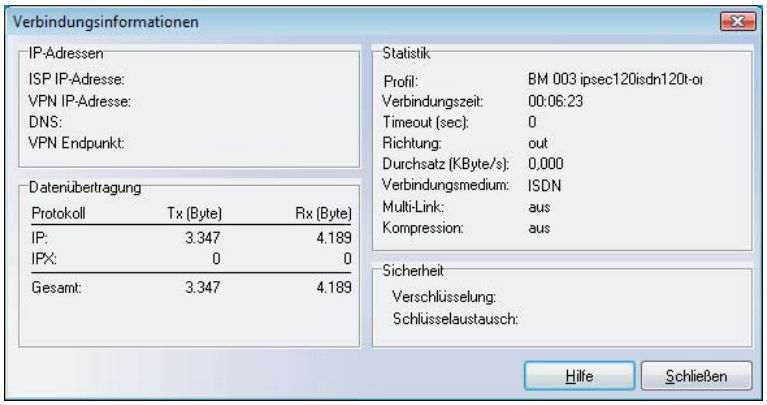
Der Secure Client verfügt über verschiedene Informationsfenster, die statistische Daten zu Verbindungsparametern, zu Phasen des Verbindungsaufbaus, zu eingesetzten Verschlüsselungstechniken und zum Online-Verhalten wie Übertragungsrate und -dauer liefern. Diese Informationsfenster können nach Bedarf alle gleichzeitig geöffnet werden.

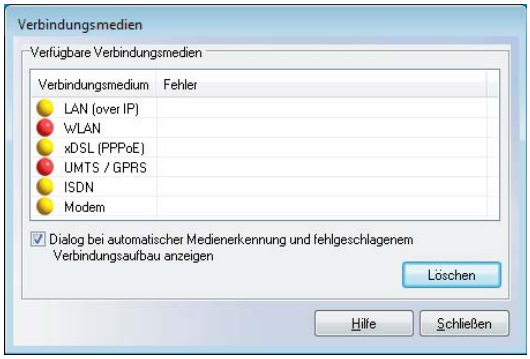


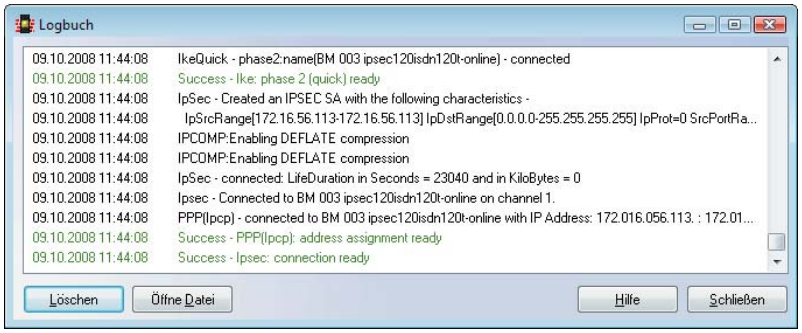

Diese Informationsfenster befinden sich im Monitormenü unter “Verbindung”, “Log” und “Hilfe”.

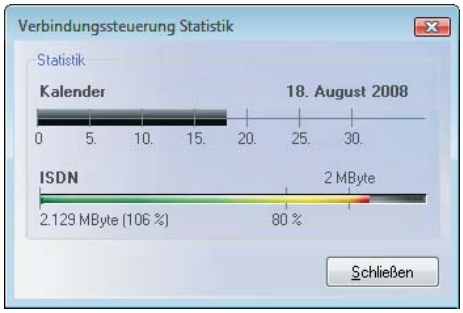
Die Informationsfenster unter “Verbindung” und “Log” können je nach Bedarf gleichzeitig offen gehalten werden (Abb. unten), währenddessen im Monitormenü oder in den Profil-Einstellungen Änderungen vorgenommen werden können.

*Die Verbindungs-Informationen (rechts) können vom Administrator ausgeblendet werden, sodass der Menüpunkt nicht aktiviert und die IP-Adressen nicht eingesehen werden können. Informationen zu Datenübertragung, Verbindungsmedium und Sicherheit können ersatzweise auch aus dem Statistik-Feld des Clients*



## Verbindungsinformationen

Die Verbindungs-Informationen zeigen statistische Werte, aber auch welche Security-Schlüssel verwendet werden und welche IP-Adressen über PPP-Verhandlung zwischen Client und Server ausgetauscht werden.

### Verbindungszeit

Als Verbindungszeit wird die gesamte Zeit angezeigt, während der Sie mit einer bestimmten Gegenstelle verbunden sind, unabhängig jedweder Timeouts. Der Wert für die Verbindungszeit wird nur dann auf (0) gesetzt, wenn Sie eine Verbindung zu einer neuen Gegenstelle herstellen oder den PC erneut booten.

### Timeout

Der Monitor zeigt die Zeit an, die bis zum nächsten Timeout noch verbleibt. Unmittelbar nachdem der letzte Datenaustausch erfolgt ist (einschließlich Handshake) beginnt die Uhr für den Timeout zu laufen. Der Timeout-Wert kann in den Profil-Einstellungen unter Verbindungssteuerung eingestellt werden.

### Richtung

Unter dieser Rubrik wird die Richtung der Kommunikation wie folgt angezeigt:
Out = eine abgehende Verbindung wird auf diesem Kanal registriert;
In = eine eingehende Verbindung wird auf diesem Kanal registriert.

### Durchsatz

Die angezeigte Zahl schwankt entsprechend des aktuellen Datendurchsatzes.

### Verbindungsmedium

Das in den Profil-Einstellungen unter Grundeinstellung konfigurierte Verbindungsmedium wird angezeigt.

### Multilink

Besteht die Verbindung über mehrere ISDN-B-Kanäle, so wird hier “on” angezeigt.

### Kompression

Soll Kompression für L2Sec eingesetzt werden, so muss sie in den Profil-Einstellungen unter Verbindungssteuerung aktiviert werden. Die Kompression kann nur dann erfolgreich eingesetzt werden, wenn auch die Gegenstelle die Kompression unterstützt. STAC-Kompression mit History ist CISCO-kompatibel. (IPSec-Kompression wird mit “on” angezeigt.)

### Verschlüsselung

Der verwendete Verschlüsselungsalgorithmus wird angezeigt. Folgende Typen werden unterstützt: AES, Blowfish, Triple DES. Die Verschlüsselungsart wird vom Zentralsystem vorgegeben, so dass in den Profil-Einstellungen des Clients unter Security nur “von Gegenstelle bestimmt” eingegeben werden muss.

### Schlüsselaustausch

Hier wird angezeigt, auf welche Art der Austausch des Session Keys erfolgt:

### Static Key

Der Schlüssel muss am Client und am Zentralsystem übereinstimmen. Er wird in den Profil-Einstellungen unter “Security / Statischer Schlüssel” eingetragen.

### IKE (IPSec)

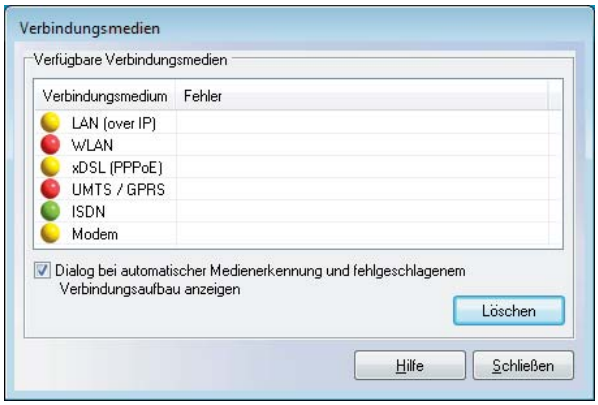
Zur Übertragung des Session Keys wird der verschlüsselte Kontrollkanal der Phase-1-Verhandlung verwendet (siehe IKE-Richtlinie).

### Rx und Tx Bytes

Rx und Tx Bytes zeigt die Datenmenge an, die gesendet (out) und empfangen (in) wird. Die Gesamtmenge (Total) und die nach Protokoll unterschiedenen Datenmengen werden in Bytes angezeigt (1 Byte = 1 Zeichen).

## Verfügbare Verbindungsmedien

Dieses Fenster dient der Benutzerinformation über die zur Verfügung stehenden Verbindungsmedien und das aktuell genutzte Medium. Werden wechselweise unterschiedliche Verbindungsmedien genutzt, so erkennt der Client welche Medien aktuell zur Verfügung stehen und stellt sie mit gelber Signallampe dar. Das von einem Profil genutzte Verbindungsmedium wird mit einer grünen Signallampe dargestellt.




Mit der Checkbox kann eingestellt werden, dass dieses Fenster bei automatischer Medienerkennung selbständig aufgeblendet wird, wenn der Verbindungsaufbau fehlgeschlagen ist. Dies gilt auch für den Fall, dass der Client-Monitor minimiert ist. Hinter der genutzten Medienart wird der Fehler in roter Schrift bezeichnet. Durch Löschen wird diese Schrift entfernt.

Bei **automatischer Medienerkennung** wird das schnellste Verbindungsmedium automatisch ausgewählt. Zur Konfiguration beachten Sie in der Beschreibung Secure Client Parameter die **Grundeinstellungen**.

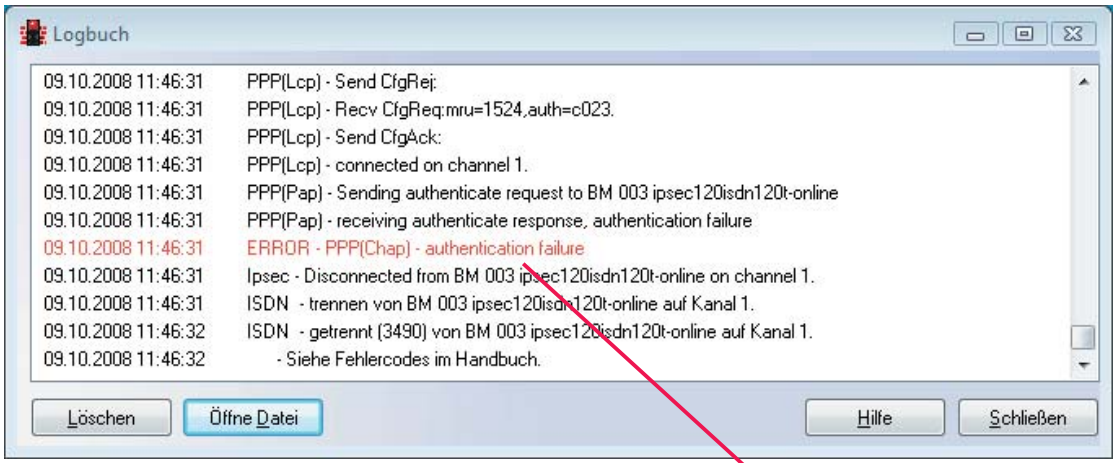
## Logbuch

Mit der Log-Funktion werden die Kommunikationsereignisse der Secure Client Software protokolliert. Selektieren Sie die Log-Funktion, öffnet sich das Fenster der “Protokollierung”. Die hier abgebildeten Daten werden bis zum nächsten Reboot im Speicher gehalten. Wenn Sie auf den Löschen-Button drücken, wird der Inhalt des Log-Fensters gelöscht.

Wenn Sie eine Datei öffnen, erhalten Sie in einem weiteren Fenster die Möglichkeit Name und Pfad einer Datei einzugeben, in die der Inhalt des Log-Fensters geschrieben wird (Standard: ncptrace.log). Alle Transaktionen wie Anwahl und Empfang, einschließlich der Adressen, werden automatisch protokolliert und in diese Datei geschrieben, bis Sie die Datei wieder schließen. Wenn Sie eine Datei anlegen, können Sie die Transaktionen über einen längeren Zeitraum verfolgen. Die geschlossene Log-Datei kann zur Analyse der Transaktionen mit dem Secure Client oder zur Fehlersuche verwendet werden.

Wenn Sie das Log-Fenster schließen, schließen Sie das Fenster der “Protokollierung” und kehren zum Monitor zurück.

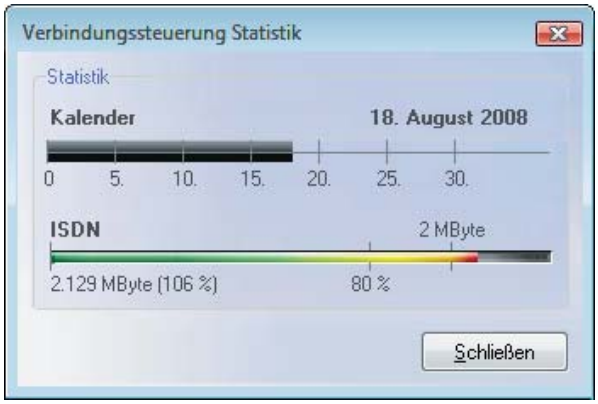
Eine zusätzliche Log-Datei speichert die Aktionen des Clients selbständig für die letzten sieben Tage. Log-Ausgaben, die älter als sieben Betriebstage sind, werden automatisch gelöscht. Die Datei steht im Installationsverzeichnis unter LOG und heißt NCPyymmdd.LOG. Sie wird mit Datumsangabe (yymmdd) immer bei Beenden des Monitors geschrieben. Die Datei kann mit einem Texteditor geöffnet und analysiert werden.




*Fehler werden im Logbuch in roter Schrift dargestellt. Diese Fehler erscheinen auch im grafischen Feld des Monitors (rechts).*

## Budget Manager Statistik

Einen Überblick über das (monatliche) Budget erhält der Anwender in der Statistik des Budget Managers. Die Statistik zeigt mit dem aktuellen Datum, wie viel des maximal auszuschöpfenden Budgets in Stunden oder Bytes bereits seit dem Ersten des aktuellen Monats bzw. seit dem Start der Überwachung verbraucht wurden. Ebenfalls ersichtlich sind hier Limits, die gesetzt werden können, um bestimmte Aktionen auszulösen.




*Die Statistik in der obigen Abbildung zeigt, dass der Benutzer sein monatliches Budget bereits überschritten hat. Der Warn-Level wurde auf 80% des Budgets eingestellt, sodass bereits eine Warnung nach Überschreiten dieses Limits ausgegeben werden musste.*

Beachten Sie zum **Budget Manager** die ausführliche Funktionsbeschreibung.

## Info

Das Info-Fenster zeigt die Produktbezeichnung und die Versionsnummer Ihrer eingesetzten Software.


## Client Info Center

Mit dem Client Info Center kann die Unterstützung durch den User Helpdesk optimiert werden. Die eingeblendete Übersicht stellt u. a. folgende Informationen zur Verfügung:

– Client Version (inkl. Build-Nummer)
– Aktueller Verbindungsstatus (verbunden, getrennt, getrennt mit Fehler)
– Status der Client-Dienste
– Aktuelle Zertifikatskonfiguration (inkl. Gültigkeit)
– VPN Benutzer-ID
– Benutzer für Management Server-Verbindung


Die dargestellten Daten können auch als Datei gespeichert werden, um sie per E-Mail an die Support-Abteilung zu senden. Der Speicherort wird in einem Informationsfenster (Abb. unten) angezeigt.