NCP
SECURE COMMUNICATIONS

Funktionsbeschreibung und Konfiguration

Enterprise Client Monitor

Secure Client Monitor

des Enterprise Clients

NCP Hotline auf Abruf

Sie erreichen unsere NCP Experten unter folgenden Hotlines:

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

Kunden ohne Hotline Service Vertrag
Sie können wählen zwischen:
Kostenpflichtige Service-Rufnummer 09001996800 (-,80 Euro / Minute)
E-Mail an support@ncp-e.com oder Telefax an 0911 99 68 458
(ohne feste Reaktionszeiten)

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

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

Network
Communications
Products engineering GmbH

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

Copyright

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 Parameter-Sperren des Enterprise Clients behandelt.

Inhaltsübersicht

Wie die Profil-Einstellungen vorgenommen werden können, ist im PDF **Enterprise Client Parameter** beschrieben.

Am komfortabelsten erhalten Sie die gewünschten Informationen über die **Enterprise Suite Navigation**. In dieser PDF-Datei sind alle aktuell verfügbaren Dokumente zu Ihrem Produkt verzeichnet.

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

Start des Secure Clients

Wenn die Software nach den Standardvorgaben installiert wurde und ein erstes Profil eingerichtet wurde (siehe **Enterprise Client Installation**), kann der Monitor über das Start-Menü “Programme / NCP Secure 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

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

Das Aussehen der Client-Oberfläche kann durch zwei unterschiedliche Eingriffe verändert werden. So wird die Oberfläche des Clients Monitors über das Ansichts-Menü des Monitors variiert, die Konfigurationsoberfläche in den Profil-Einstellungen und das Konfigurationsmenü selbst kann durch gezielte Parametersperren verändert werden.

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

– Titelzeile mit Anzeige der Software-Variante

– Hauptmenüleiste

– Profilauswahl

– grafisches Statusfeld zur Anzeige des Verbindungsstatus, der aktivierten Firewall und ggf. Fehlermeldungen, sowie der Weltkarte mit Zeitzonen. (Jeweils nach der am Rechner eingestellten Zeitzone wird ein entsprechender Ausschnitt der Weltkarte angezeigt: Europa, Amerika, oder Asien / Australien).

– Statistikfeld mit Anzeige der wichtigsten aktuellen Einstellungen und Werte zum ausgewählten Profil (siehe **Informationsfenster des Clients**)

– 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**)

– Verbindungsschalter mit Firmenlogo

Das Ansichts-Menü des Monitors

Das Ansichts-Menü (Abb. links) dient dazu, verschiedene Informations- und Statistikfelder ein- oder auszublenden und so die Größe des Monitors auf dem Bildschirm je nach Bedarf mit Informationsfeldern zu vergrößern oder durch Ausschalten aller Felder auf die kleinste Form zusammenzuschieben. Auch kann der Monitor immer in den Bildschirm-Vordergrund gerückt oder als Tray Icon minimiert werden.

So können sie die Bedienoberfläche des Monitors variieren und die Sprache für die Oberfläche festlegen. Sind alle Anzeige- und Statistikfelder aktiviert, nimmt der Monitor seine größte Fläche ein, wie nach dem ersten Start.

Nach Ausblenden der einzelnen Bestandteile erscheint der Monitor 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 Abb. links).

Wenn der Monitor mit dem Button [–] zum Icon verkleinert wird, erscheint er als Ampellicht im System Tray (Abb. links), wo an der Ampelfarbe der Verbindungsstatus abgelesen werden kann. Das Mauersymbol zeigt an, dass die Personal Firewall aktiviert ist. Im Kontextmenü der rechten Maustaste kann ein Profil selektiert und die Verbindung auf- oder abgebaut werden, außerdem kann der Monitor wieder hergestellt oder beendet werden.

Nach einer Mausberührung des Tray Icons wird in einem Popup der aktuelle Status der Verbindung und die Firewall-Konfiguration angezeigt (Abb. links). Beachten Sie dazu auch die Beschreibung zur **Personal Firewall**.

WLAN-Status anzeigen

Unabhängig vom Verbindungsmedium des aktuell selektierten Linkprofils kann das Feld zur grafischen Anzeige des WLAN-Status (Abb. links unten) geöffnet bzw. geschlossen werden, wenn im Monitormenü “Konfiguration” unter “WLAN-Einstellungen” die **WLAN-Konfiguration** aktiviert wurde. Wurde eine **Multifunktionskarte** konfiguriert, ist dieser Menüpunkt nicht aktiv.

Unabhängig vom Start des Monitors oder einer VPN-Verbindung zeigt das NCP WLAN Tool

den WLAN-Status an, sobald der Mauszeiger das Tray Icon berührt.

Beachten Sie zur WLAN-Konfiguration das PDF **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

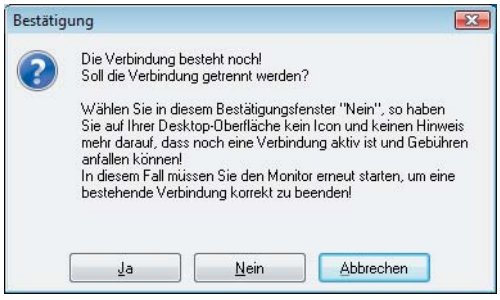
– Icon im System Tray: nach dem Booten den Monitor starten und minimiert in der Task-Leiste darstellen

– 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

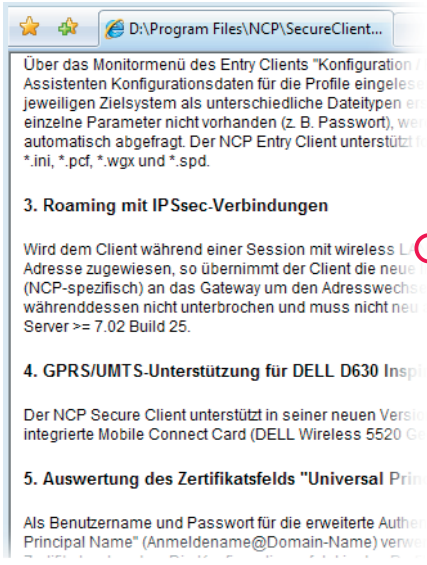
Die Standardsprache bei Auslieferung ist Deutsch. Um eine andere Sprache zu wählen, klicken Sie “Sprache” im Ansichts-Menü und wählen die gewünschte Sprache.

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. Entsprechend der Editierung der Datei Projektlogo.ini wird bei einer Mausberührung des Logos eine Quick-Info angezeigt und mit einem Mausklick auf das Logo eine lokale HTML-Seite vom Browser angezeigt.

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
```

Parameter-Sperren am Enterprise Client

Die Parametersperren des Clients 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.

Während die Software des Secure Enterprise Clients kann für größere VPN-Umgebungen mit vielen Benutzern über das Secure Enterprise Management administriert, konfiguriert und ausgerollt werden.

Begriffsklärung “Profil”

In älteren Versionen des Enterprise Clients < 9.1 wurde die Sammlung der einzelnen Konfigurationen “Telefonbuch” genannt. Ab Version 9.1 heißt sie **Profile**. Um ein Profil zu ändern wird dieser Konfigurationsmenüpunkt 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.

Die Parameter-Sperren des Enterprise Clients können nur mit dem Secure Enterprise Management (SEM) erstellt werden. Beachten Sie daher zur genauen Vorgehensweise bei Erstellung von Parameter-Sperren die Beschreibungen zum Management System, die Sie über den **SEM-Navigator** erreichen. Im folgenden werden nur die Schritte von der Vergabe der allgemeinen Benutzerberechtigungen bis zur Personalisierung der Software gezeigt.

Der Administrator erstellt am Management System mit dem Client Configuration Plug-in über Vorlagen (Templates) eine Software-Konfiguration, die zunächst gruppenspezifisch von allen Benutzern einer vorher festgelegten Gruppe eingesetzt werden kann.

(Diese Vorlage kann mittels SEM immer weiter ausdifferenziert werden, sodass schließlich pro Benutzer nicht nur verschiedene Profile mit ihren Sperren zugeordnet werden können, sondern auch die Profile hinsichtlich der Parameter-Sperren unterschieden werden können.)

Darüber hinaus können bei einem (Konfigurations-) Update ältere Profile, die ein Benutzer früher selbst angelegt hat, automatisch gelöscht werden.

Die Profile einschließlich ihrer jeweiligen Parameter-Sperren werden mit der benutzerspezisch bearbeiteten Oberfläche des Monitor-Menüs als CNF-Datei vom Management System als (Konfigurations-) Update an die entsprechenden Benutzer automatisiert verteilt. Beachten Sie dazu die Beschreibung zum automatischen Update, auch Konfigurations-Update, mit dem Secure Enterprise Management.

Für die Parameter-Sperren des Enterprise Clients gilt:

– Sie sind zentral abgefasst und werden automatisch an die entfernten Anwender-PCs verteilt;

– Berechtigungen für die Konfiguration im Client Monitor-Menü sind getrennt von

– Berechtigungen für die Konfiguration der Profile;

– beide können benutzerspezifisch mittels unterschiedlicher Links kombiniert werden;

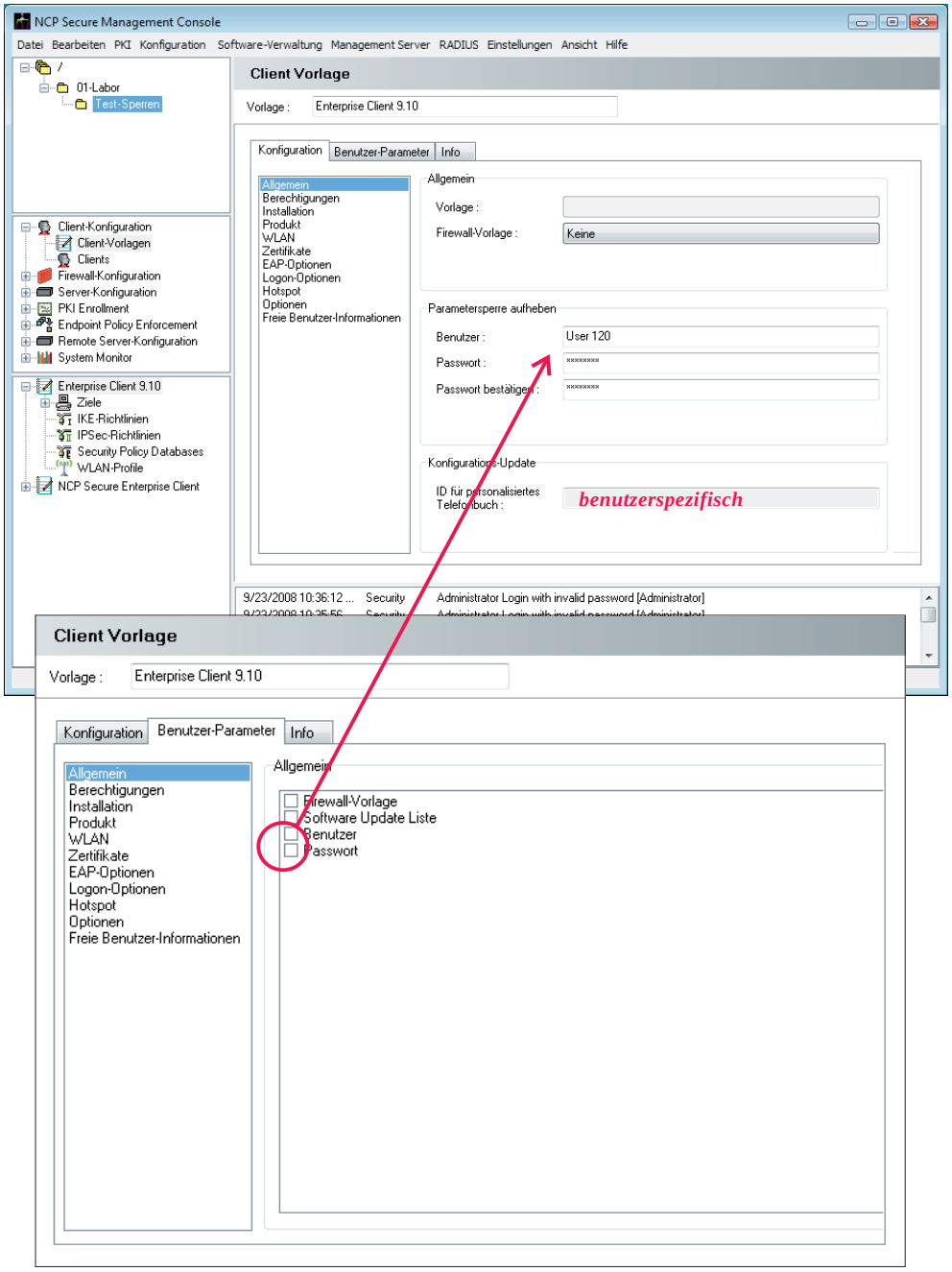
– innerhalb der Konfigurationsfelder für ein Profil können Parameter einzeln ausgeblendet werden, d. h. die Sperren können auch link-spezifisch differenziert werden;

– die Parameter-Sperren können durch “Benutzer” und “Passwort” bis zum nächsten Konfigurations-Update oder bis zum nächsten Start des Monitors durch ein Einmal-Passwort aufgehoben werden.

Konfiguration einer Vorlage mit Parameter-Sperren

Gruppenspezifische und benutzerspezifische Parameter

Die Einträge und Werte einer Vorlagen-Konfiguration sind für alle Mitglieder einer Organisationsgruppe (Abb. unten “Test-Sperren”) auf die diese Vorlage angewendet wird, identisch bzw. gruppenspezifisch – abgesehen von den individuellen Codes.



Die Vorlagen-Parameter, deren Eingabefelder im Konfigurationsbereich (Abb. links) deaktiviert sind, müssen am Ende in der individuellen Client-Konfiguration eingegeben werden.

Welche Vorlagen-Parameter individuell gesetzt werden, kann im Vorlagen-Feld der Benutzer-Parameter (Abb. links unten) definiert werden.

Beispiel: Standardmäßig sind beim ersten Öffnen der Vorlage im Konfigurationsbereich die Parameter “Benutzer” und “Passwort” für die “Parametersperre” konfigurierbar gehalten, wohingegen die “ID für das personalisierte Telefonbuch”, die benutzerspezifischen Profile, nicht eingetragen werden kann.

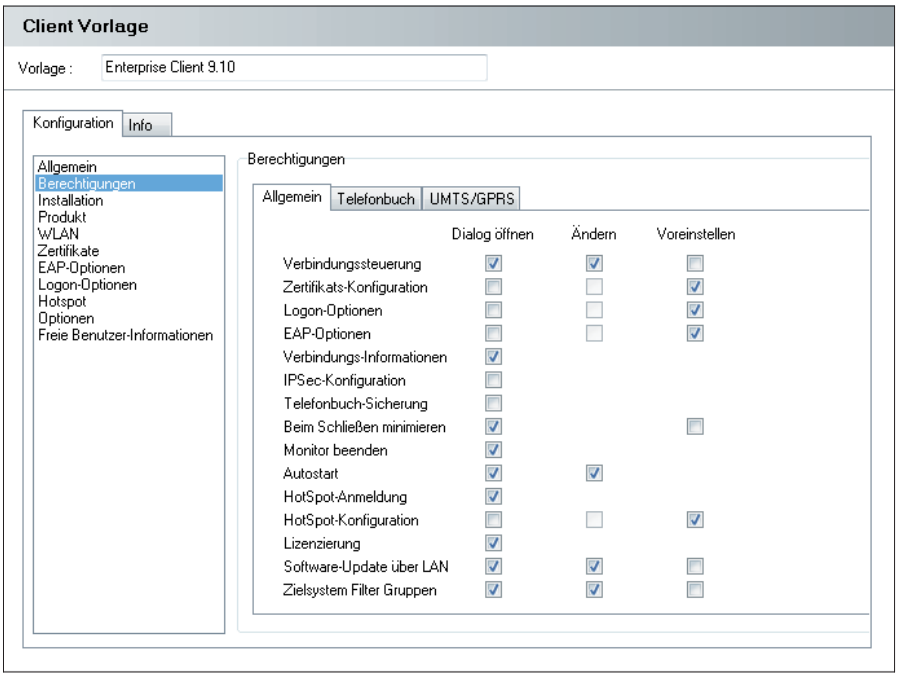
Dies bedeutet, dass alle Benutzer-Konfigurationen, für die diese Vorlage verwendet wird, gleiche Codes für Benutzer und Passwort zum Aufheben der Parametersperre besitzen, jedoch eine eindeutige ID für ihre persönlichen Profile. Diese muss am Ende in der Client-Konfiguration eingetragen werden.

Bitte beachten Sie, dass mit dieser Konfiguration nur definiert wird, welche Parameter für Mitglieder der Organisationsgruppe gleich sind und welche erst am Ende in der Benutzer-Konfiguration individuell eingetragen werden. Diese sogenannten “Benutzer-Parameter” werden mit einem Haken markiert.

Bezüglich der Parameter-Sperre wird hier nur definiert, ob alle Benutzer zum Aufheben der Parameter-Sperre gleiche oder unterschiedliche Codes erhalten. (In der Abb. oben sind es gleiche Codes.)
Zur ID für personalisiertes Telefonbuch beachten Sie bitte die Beschreibung zum Secure Enterprise Management.

Berechtigungen

Mit den Berechtigungen (siehe Abb. unten) kann der Administrator gruppenspezifische Sperren vorgeben. Er definiert hier wie die Oberfläche des Monitors beschaffen sein soll, welche Konfigurationen voreingestellt werden sollen und ob der Benutzer selbständig Änderungen in den Profilen (im Telefonbuch) vornehmen darf.

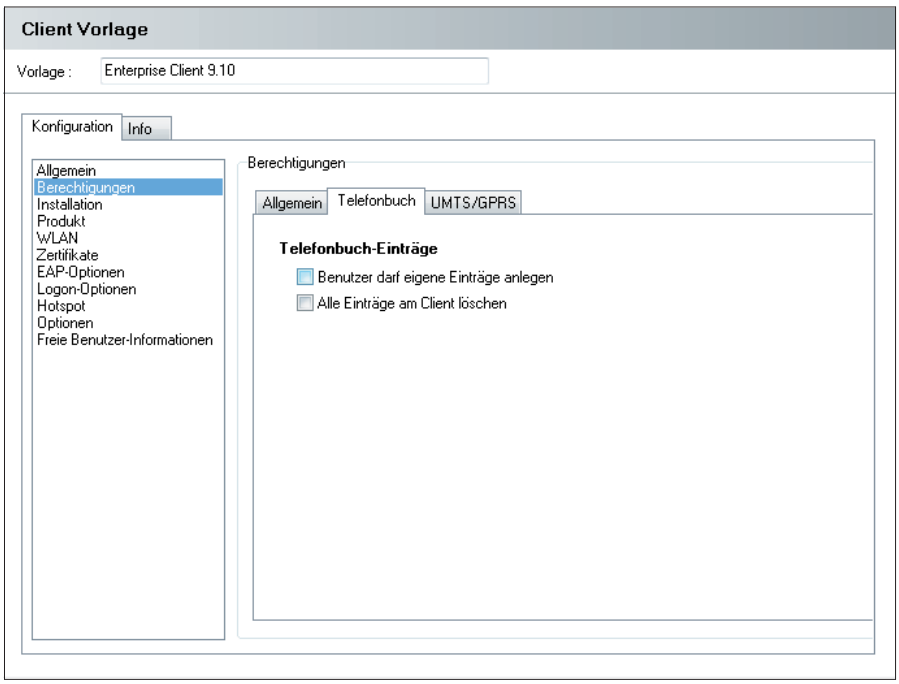


Client Monitor-Menü (Allgemein)

Die Berechtigungen in diesem Feld (Abb. links) beziehen sich auf Dialoge im Client Monitor, die sich unter dem Menüpunkt “Konfiguration” und “Fenster” befinden. Der Administrator kann Berechtigungen dafür vergeben, welche gestatten “nur” die Dialog-Boxen zu öffnen und die Voreinstellungen zu betrachten, oder auch die dort gezeigten Parameter zu ändern. Darf ein Dialog nicht geöffnet werden, ist er im Monitor-Hauptmenü “ausgegraut” dargestellt. Ist das Ändern verboten, so können keine Eingaben gemacht werden. Darüber hinaus kann sich der Administrator hier abhaken, welche Parameter er in der Vorlage voreinstellen möchte und ggf. auch nicht durch den Benutzer geändert haben möchte.

Wird die restriktivste Einstellung vorgenommen, indem der Administrator alle Konfigurationsmöglichkeiten voreinstellt und dem Benutzer alle Änderungsmöglichkeiten nimmt, so muss in einem Fehlerfall entweder eine neue CNF-Datei für den Client bereitgestellt werden – sofern der Client noch eine Verbindung aufbauen kann – oder der Administrator muss mit dem Benutzer kommunizieren und ihm das (Einmal-) Passwort zum Aufheben der Parameter-Sperre mitteilen, sodass der Benutzer anschließend die nötigen Änderungen vornehmen kann.

Profile (Telefonbuch)



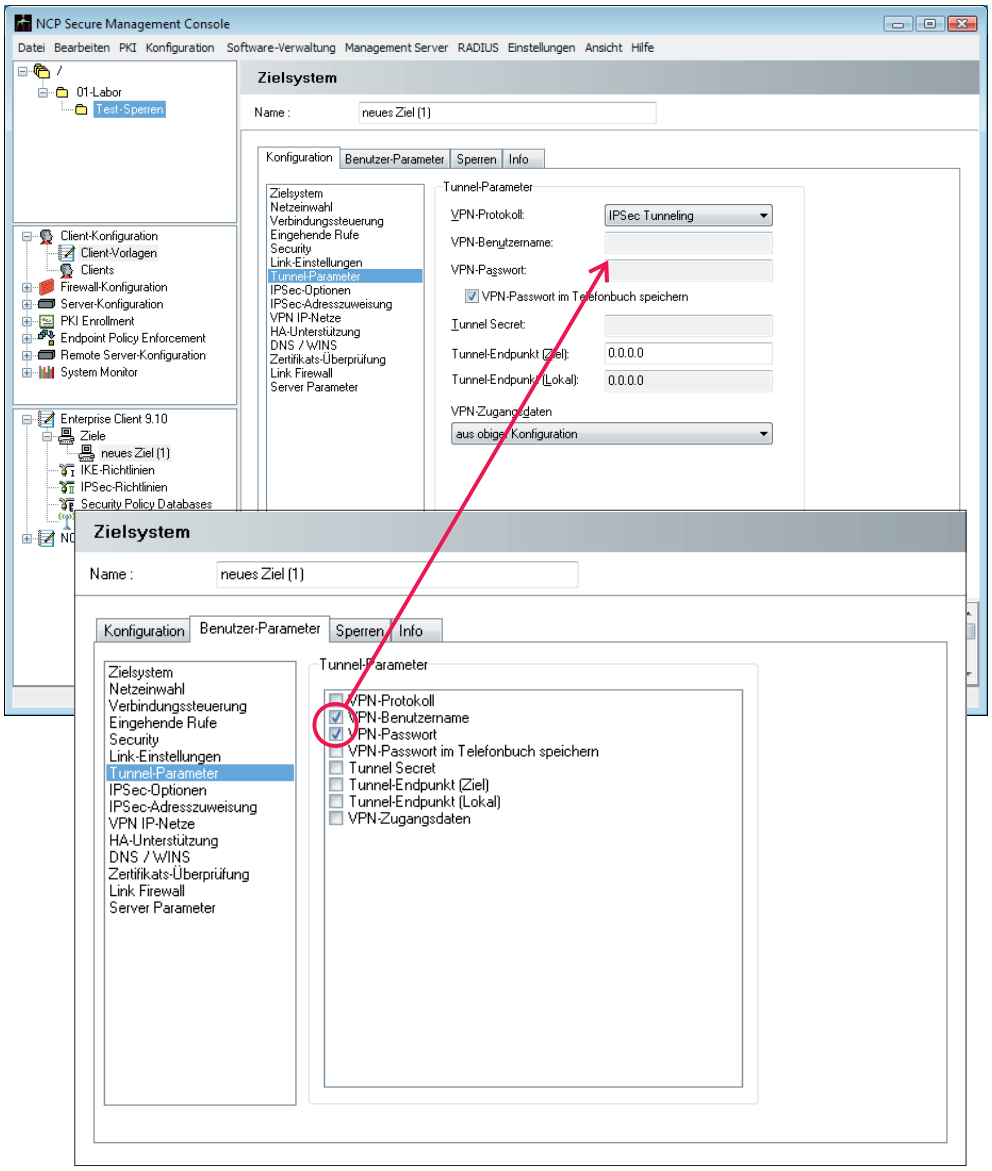
“Benutzer darf eigene Einträge anlegen” bedeutet, dass der Anwender neue Profile anlegen kann. Ist diese Funktion vom Administrator nicht abgehakt, so kann der Benutzer nur mit den administrativ vorgegebenen Profilen Verbindungen aufbauen.

Mit der Funktion “Alle Einträge am Client löschen” werden bei einem Konfigurations-Update, d. h. sobald der Client eine neue CNF-Datei erhalten hat, alle Profile gelöscht, inkl. denen die der Benutzer selbst anlegen konnte, bevor die neuen eingelesen wurden.

Unter **UMTS / GPRS** kann der Administrator die Speicherung der SIM-PIN sperren. (Siehe **Mobile Computing**.)

Konfiguration der Profile (Zielsysteme)

Die Profile (Zielsysteme) sind Bestandteil der Vorlagen. Über die Vorlage wird später dem Benutzer ein Profil (oder mehrere) zugeordnet. (Sollen z. B. innerhalb einer Gruppe einigen Benutzern drei Profile zugewiesen werden und anderen fünf, so müssen zwei Vorlagen definiert werden, eine Vorlage für zwei und eine für fünf Profile. Ebenso verhält es sich bei unterschiedlicher Zertifikatsnutzung.)



Ein Profil wird am Enterprise Client genauso konfiguriert wie an der Console des Management Systems, wobei hier unterschieden wird, welche Parameter für alle Clients gleich sind und welche benutzerspezifisch sind.

Die Vorlagen-Parameter, deren Eingabefelder im Konfigurationsbereich (Abb. links) deaktiviert sind, müssen am Ende in der individuellen Client-Konfiguration eingegeben werden. Welche Vorlagen-Parameter dies sind, kann im Vorlagen-Feld der Benutzer-Parameter (Abb. links unten) mit einem Haken definiert werden.

Beispiel: Standardmäßig sind beim ersten Öffnen der Vorlage im Konfigurationsbereich unter “Tunnel-Parameter” die für das VPN Gateway nötigen Zugriffsdaten nicht konfigurierbar.

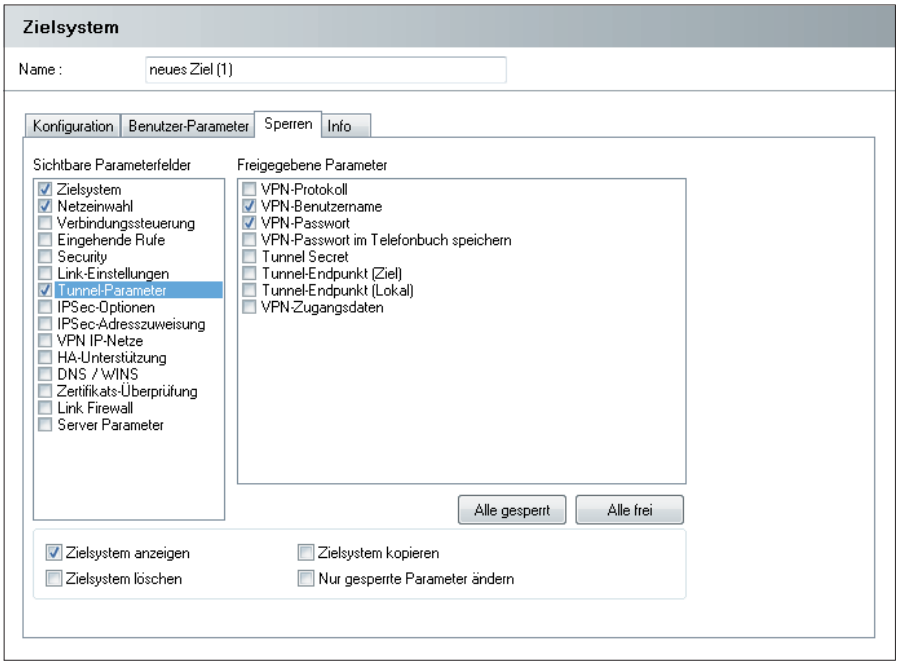
Dies bedeutet, dass alle Benutzer, die mit diesem Profil arbeiten, unterschiedliche Zugriffsdaten haben, welche am Ende der Client-Konfiguration eingetragen werden oder beim Verbindungsaufbau durch den Anwender.

Benutzer-Parameter

Parameter wie **VPN-Benutzername** und **VPN-Passwort** sind die persönlichen Zugriffsdaten eines jeden Benutzers und dürfen somit erst in der Client-Konfiguration eingesetzt werden (sofern sie nicht über ein Zertifikat ausgelesen werden). Siehe dazu **Secure Client Parameter**.

Dies bedeutet allgemein, dass alle Parameter, die in der Vorlage für das Profil nicht editierbar sind, persönliche und eindeutige Werte sind, die erst in der Client-Konfiguration am SEM oder am Client durch den Benutzer eingegeben werden können.

Sperren



Mit den Sperren bestimmen Sie das Erscheinungsbild der Profil-Einstellungen in der Oberfläche der Client Software in der Weise, dass der Benutzer bestimmte Parameter in den Profil-Einstellungen nicht verändern oder nicht sehen kann.

Eine Sperre ist immer einem Profil oder einem Parameterfeld in den Profil-Einstellungen des Secure Clients zugeordnet.

Sichtbare Parameterfelder

Unter den sichtbaren Parameterfeldern sind die Titel aller Parameterfelder aus den Profil-Einstellungen des Clients aufgeführt. Sind die Titel der Parameterfelder mit einem Haken versehenen, so werden die entsprechenden Parameterfelder der Profil-Einstellungen des Benutzers gezeigt. Parameterfelder ohne Haken werden aus den Profil-Einstellungen des Benutzers komplett ausgeblendet.

Freigegebene Parameter

In der Liste der freigegebenen Parameter werden alle Parameter eines markierten Parameterfeldes gezeigt. Ist ein Parameterfeld für den Benutzer sichtbar, so kann im einzelnen noch festgelegt werden, welche Parameter dieses Feldes für Benutzereingaben gesperrt und welche für Änderungen durch den Benutzer freigegeben werden.

Ein Parameter ist für Benutzereingaben freigegeben, wenn er mit einem Haken versehen ist. Er ist gesperrt, wenn er nicht abgehakt ist.

Modifikationen der Profile

Beachten Sie hierzu auch weiter unten “Profile am Client anlegen”.

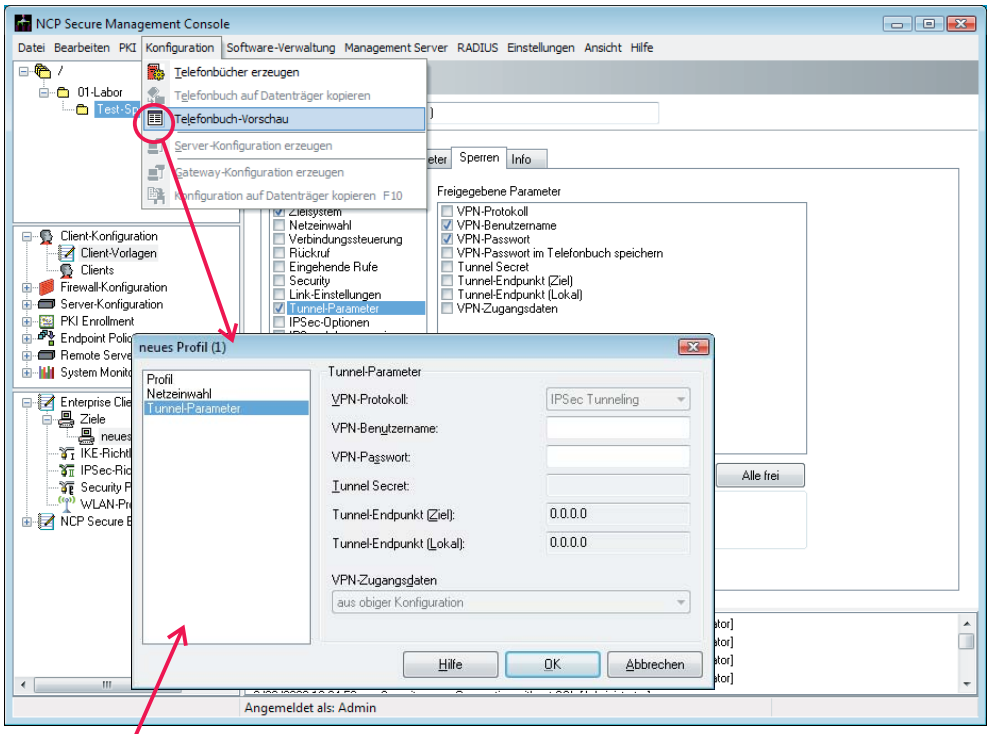
Mit den Funktionen “Profil anzeigen”, “...löschen” und “...kopieren” werden alle Buttons außer “Neuer Eintrag” im Verzeichnis der Profile im Client-Monitor aktiv oder grau geschaltet und dem Benutzer entsprechende Modifikationen gestattet. Der Button “Neuer Eintrag” wird mit der Berechtigung “Benutzer darf eigene Einträge anlegen” aktiv geschaltet. Diese Berechtigung betrifft alle Profile und nicht nur einzelne Profile, daher befindet sich diese Konfigurationsmöglichkeit in der Oberfläche der Vorlagen-Konfiguration (siehe oben “Berechtigungen”).

Für den Benutzer kann der Administrator dieses “Profil anzeigen” lassen, wenn ein Haken gesetzt ist. Ohne Haken wird der Eintrag des Profils dem Benutzer nicht angezeigt, sodass auch der Konfigurieren-Button grau bleibt. Entsprechend beeinflussen die Konfigurationsmöglichkeiten “Profil löschen” und “Profil kopieren” die Funktion der Buttons “Löschen” und “Kopieren”.

“Nur gesperrte Parameter ändern” bedeutet, dass bei einem Konfigurations-Update nur die Einstellungen der hier gesperrten Parameter überschrieben werden. Damit kann verhindert werden, dass Parameter, die durch den Benutzer am Client geändert wurden (z. B. Modemeinstellungen) durch ein Konfigurations-Update überschrieben werden.

Vorschau auf das Profil

Wenn die Konfiguration eines Profils abgeschlossen ist und Sperren definiert wurden, können im Hauptmenü unter “Konfiguration / Profil-Vorschau” oder in der Werkzeugleiste mit Klick auf den Vorschau-Button die Profile so betrachtet werden, wie sie dem Benutzer am Client erscheinen (Abb. links).



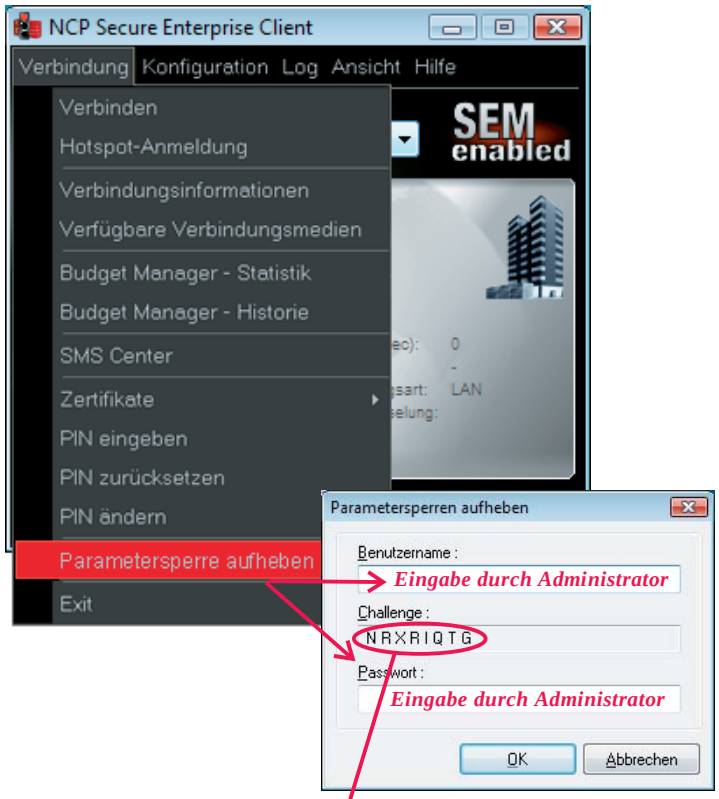
Darstellung der Parameter-Sperren in der Oberfläche des Enterprise Clients

Nach einem Rollout oder Konfigurations-Update, womit ein Anwender die Client Software mit Sperren erhält, stellt sich das Konfigurationsmenü des Enterprise Clients wie in nebenstehender Abbildung dar.

Die Konfigurationsfelder eines Link-Profils werden wie in der Vorschau am SEM dargestellt, sofern sie sich öffnen lassen (siehe Abb. oben).

Aufheben der Sperren

Eine Aufhebung oder Änderung der Sperren sollte nur in einer der genannten Weisen erfolgen, um eine Konfigurationssicherheit wahren zu können:



Zentral

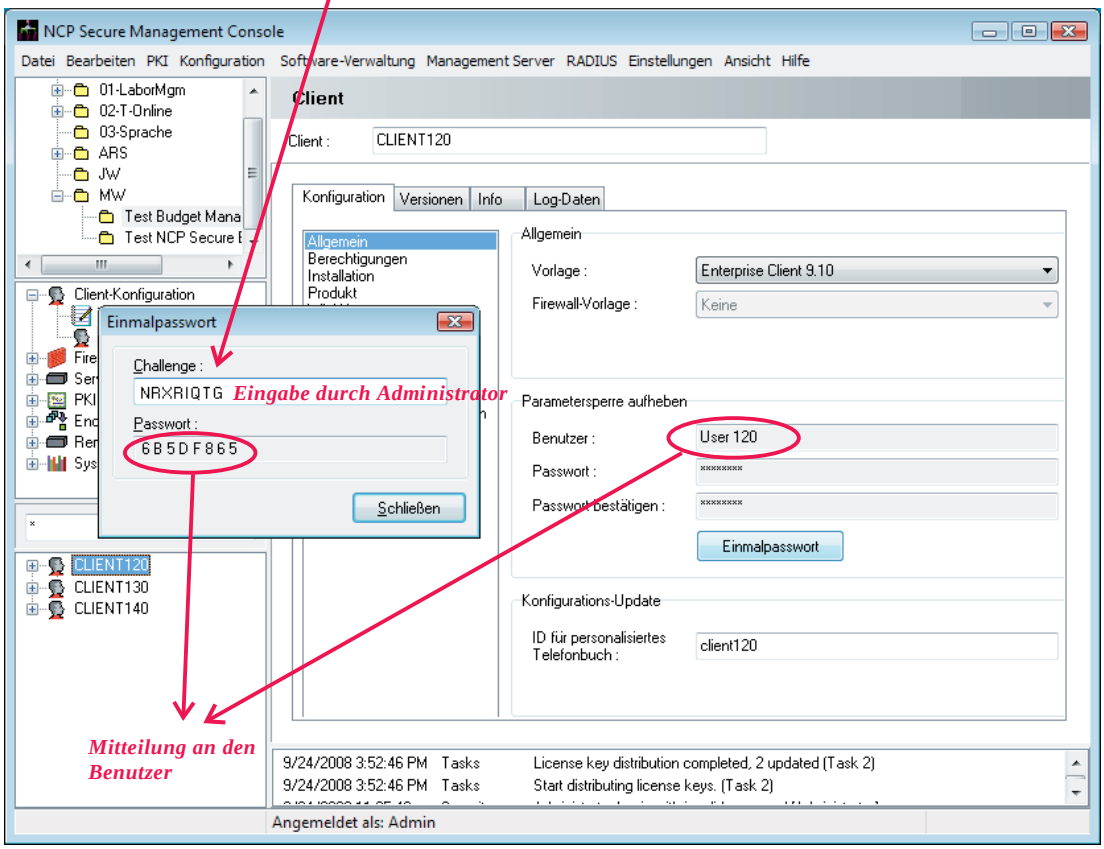
Der Administrator kann zentral am SEM eine neue Benutzer-Konfiguration erstellen und ein Konfigurations-Update am Management Server bereit stellen. Nach einem Update, das automatisch erfolgt, sind am entfernten Client die Änderungen wirksam. (Beachten Sie dazu die Beschreibung zum Konfigurations-Update mittels SEM).

Vor Ort

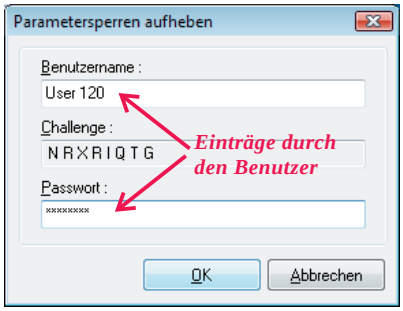
Sollte der entfernte Client keine Verbindung mehr zum Management-System aufbauen können, so kann der Administrator die Parameter-Sperre am Enterprise Client vor Ort aufheben. Dazu wird im Monitor-Konfigurationsmenü der Punkt “Parametersperre aufheben” selektiert (Abb. links) und anschließend Benutzername und Passwort eingegeben, wie sie in der Vorlage am SEM konfiguriert wurden (siehe oben: Gruppenspezifische und benutzerspezifische Parameter). Nach den Änderungen sollte nicht vergessen werden, die Sperren wieder herzustellen (siehe unten).

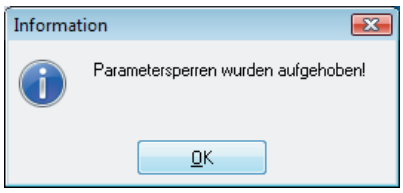
Remote

Im Ermessen des Administrators liegt es, Parameter-Sperren vom entfernten Anwender aufheben zu lassen. In diesem Fall muss ein telefonischer Kontakt zwischen Anwender und Administrator bestehen.



Der Anwender teilt dem Administrator den Challenge-Code mit, den er erhält, nachdem er den Menüpunkt “Parameter-Sperre aufheben” selektiert hat (siehe Abb. oben). Diesen Code teilt er dem Administrator mit, der ihn an der Management Console eingibt. Dazu selektiert dieser in der allgemeinen Konfiguration des Anrufers den Button Einmal-Passwort. Nach der Eingabe des Codes erhält er das Einmal-Passwort (Abb. links).





Dieses Passwort plus den Benutzer zum Aufheben der Parameter-Sperre (siehe Abb. vorige Seite) teilt der Administrator dem Anwender mit. Nach der Eingabe dieses Einmal-Passworts durch den Anwender (Abb. links) sind die Sperren aufgehoben.

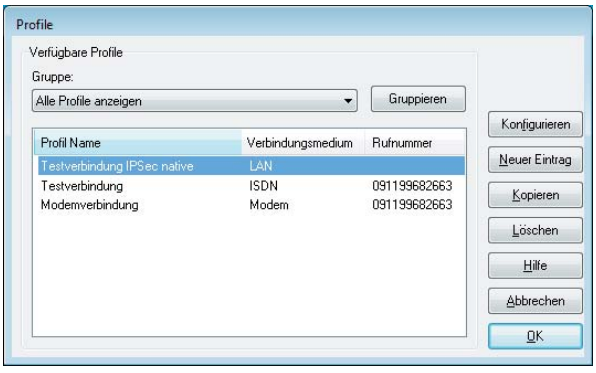
Die Entriegelung der Sperren hält an bis der Anwender den Menüpunkt “Parametersperre wieder herstellen” betätigt (Abb. links), spätestens bis zum Beenden des Monitors. Nach einem erneuten Start des Monitors sind die Sperren wieder hergestellt.

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 Secure Client Software sind noch keine Profile vorhanden. In diesem Fall wird automatisch ein Assistent (siehe Installationsbeschreibung Enterprise Client) eingeblendet, der dabei hilft Profile mit Test-Konfigurationen 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)

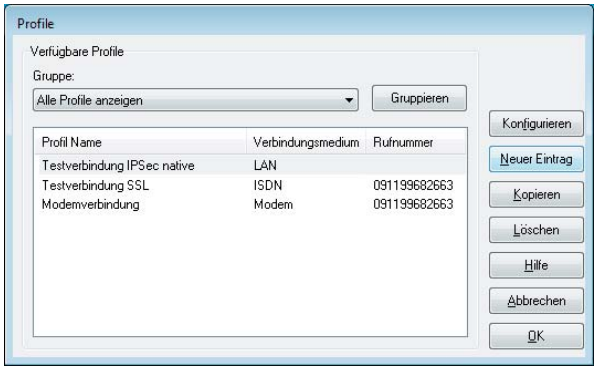


Die Buttons auf der rechten Seite der Profil-Einstellungen können nicht betätigt werden, wenn die entsprechenden Sperren eingestellt sind. Beachten Sie dazu oben für den Enterprise Client “Modifikationen der Profil-Einstellungen”.

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.

Vom Assistenten für ein neues Profil werden unterschiedliche Typen von Verbindungen angeboten. Nach Auswahl dieses Verbindungstyps wird nach wenigen Abfragen das neue Profil angelegt. Im folgenden die jeweils nötigen Daten zur Konfiguration:

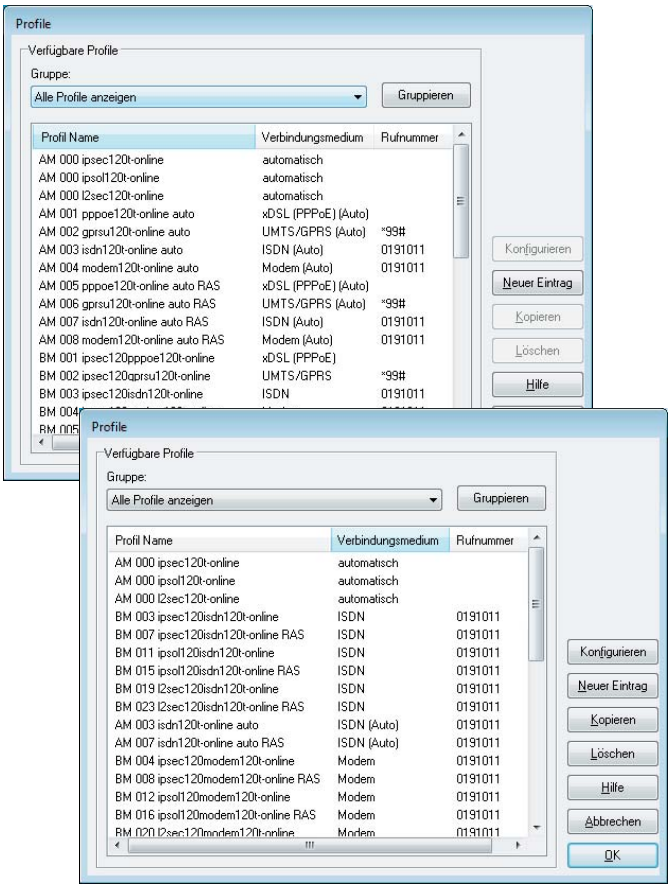
	Konfigurationsfelder
Verbindung zum Firmennetz über L2Sec	
– Profil-Name	**Grundeinstellungen**
– Verbindungsmedium	
– Zugangsdaten für Internet-Dienstanbeiter (Benutzername, Kennwort, Rufnr.)	**Netzeinwahl**
– VPN Gateway-Parameter (IP-Adresse, Tunnelsecret)	**Tunnel-Parameter**
– Nutzung von Zertifikaten	**Security**
– Zugangsdaten für VPN-Gateway (VPN-Benutzer, VPN-Passwort)	**Tunnel-Parameter**
– Statischer Schlüssel (Preshared Key) sofern kein Zertifikat eingesetzt wird	**Security**
– Firewall-Einstellungen	**Link Firewall**
Verbindung zum Firmennetz über IPSec over L2Sec	
– Profil-Name	**Grundeinstellungen**
– Verbindungsmedium	
– Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)	**Netzeinwahl**
– VPN Gateway-Parameter (IP-Adresse, Tunnelsecret)	**Tunnel-Parameter**
– Nutzung von Zertifikaten	**Security**
– Zugangsdaten für VPN-Gateway (VPN-Benutzer, VPN-Passwort)	**Tunnel-Parameter**
– Statischer Schlüssel (Preshared Key) sofern kein Zertifikat eingesetzt wird	**Security**
– Firewall-Einstellungen	**Link Firewall**
Verbindung zum Firmennetz über IPSec*	
– Profil-Name	**Grundeinstellungen**
– Verbindungsmedium	
– Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)	**Netzeinwahl**
– VPN Gateway-Parameter (IP-Adresse, Tunnelsecret)	**Tunnel-Parameter**
– Nutzung von Zertifikaten	**Security**
– Zugangsdaten für VPN-Gateway (VPN-Benutzer, VPN-Passwort)	**Tunnel-Parameter**
– Extended Authentication	**Erweiterte IPSec-Optionen**
– IPSec-Konfiguration (Exch. Mode, PFS-Gruppe, Kompression)	**IPSec-Konfiguration***
– Statischer Schlüssel (Preshared Key), ohne Zertifikat (IKE ID-Typ, IKE ID)	
– IP-Adressen-Konfiguration (IP-Adresse des Clients, DNS / WINS-Server)	
– Firewall-Einstellungen	**Link Firewall**
Verbindung mit dem Internet herstellen	
– Profil-Name	**Grundeinstellungen**
– Verbindungsmedium	
– Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)	
– Firewall-Einstellungen	**Link Firewall**

Zu weiteren Parametereinstellungen beachten Sie bitte die Enterprise Client Parameter. Mit einem Mausklick hier gelangen Sie direkt 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.

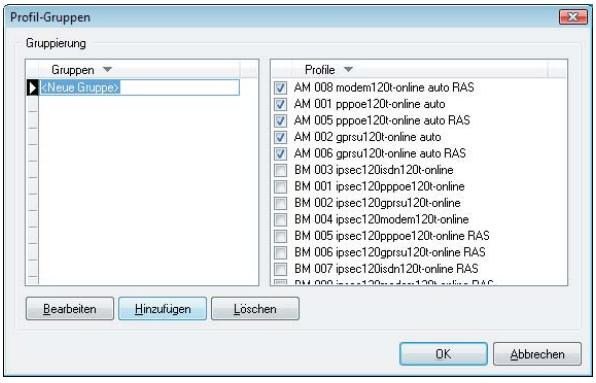
*** Zur IPSec-Konfiguration des Secure Clients, die über mehrere Konfigurationsfelder verteilt ist, gelangen Sie hier mit einem Mausklick.**

Profil-Gruppen

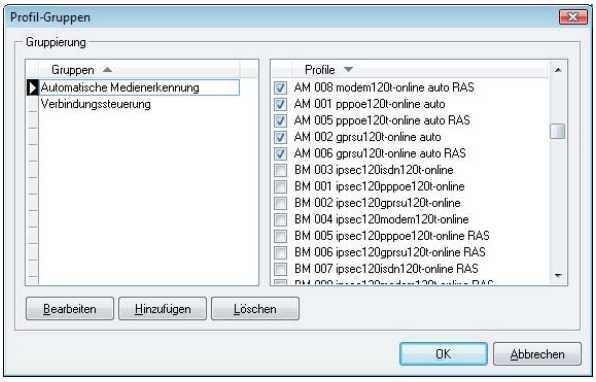


In der Anzeige aller Profile können diese nach ihrem Namen, nach der Verbindungsmedium und, sofern es sich um eine Wählverbindung handelt, nach der Rufnummer sortiert werden. (Abb. links)

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).



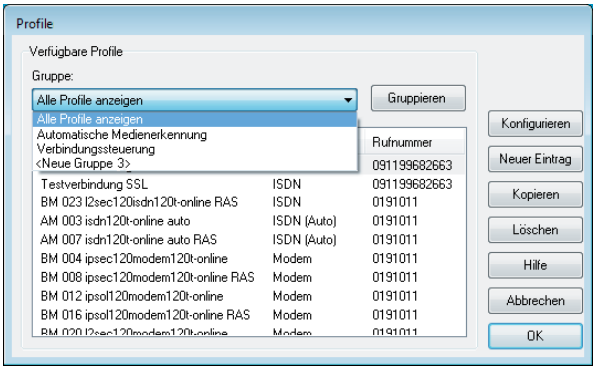
Mit “Hinzufügen” wird eine neue Gruppe in die linke Spalte eingefügt, der Sie einen eigenen Namen geben können, z. B. Gruppe “Automatische Medienerkennung” wenn Sie diese Profile in einer Gruppe zusammenstellen möchten. (Abb. links)



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)

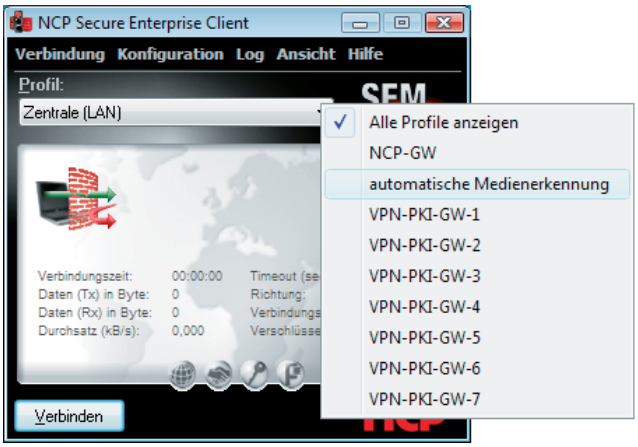
Der Bearbeiten-Button dient der Namensänderung der Gruppe. Mit dem Löschen-Button wird die jeweils aktuell angezeigte Gruppe gelöscht und die entsprechende Gruppenzugehörigkeit eines Profils, nicht aber das Profil selbst.

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

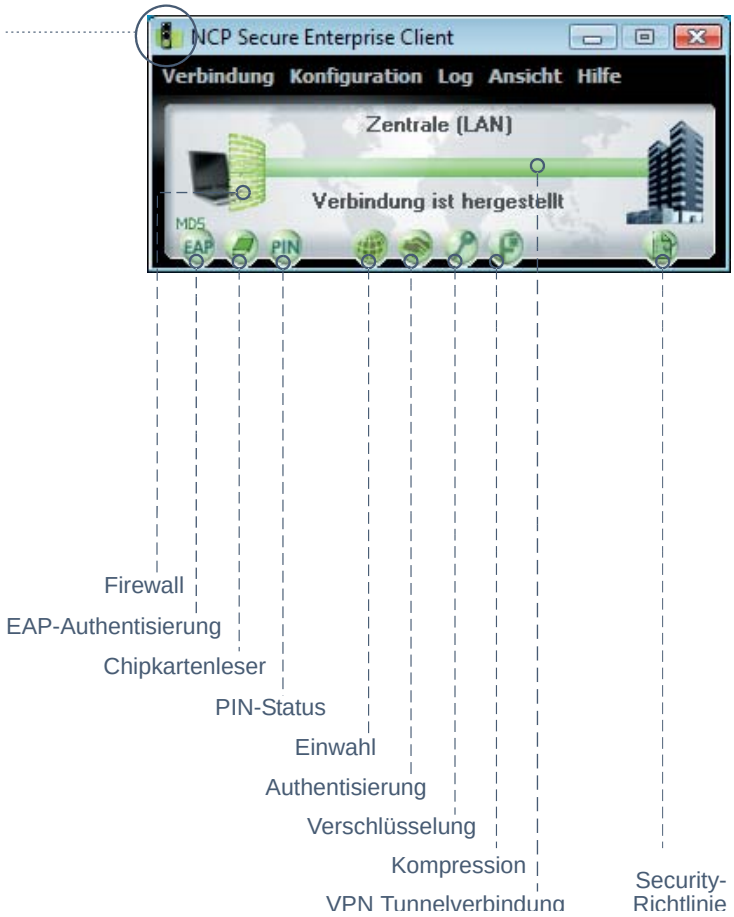
Die Symbole des Monitors

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.

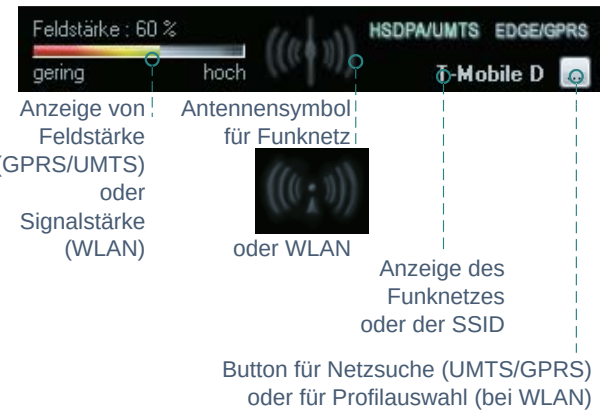
Eine rote Ampelbedeutet “keine Verbindung”, eine gelbe zeigt den Verbindungsaufbau an und eine grüne Ampel – auch in der Task-Leiste – symbolisiert immer eine bestehende Verbindung, für die ggf. Gebühren anfallen.

Die weiteren Symbole sind auf den folgenden Seiten ausführlich erklärt.



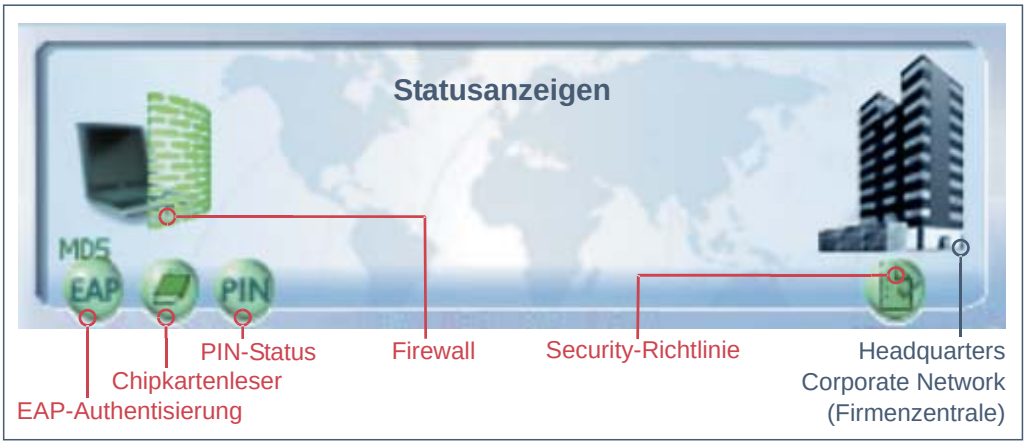
Je nach Konfiguration und Installation einer Multifunktionskarte erscheint zusätzlich alternativ ein **WLAN**- oder **UMTS / GPRS**-Panel im Monitor.

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.

Security-Richtlinie

Wollen Sie die Endpoint Security mit dem Enterprise Client einsetzen, dann beachten Sie die Beschreibungen zum Secure Enterprise Management (SEM-EPS-Plug-in und den **SEM-Navigator**)

Das Richtlinien-Symbol ist immer dann sichtbar, wenn vom zentralen Management Endpoint Policy Enforcement für diesen Client festgelegt wurde, d. h. wenn der PC des Clients oder der Client selbst zuerst Sicherheits-Richtlinien erfüllen muss, um Zugriff auf das Firmennetz zu erhalten.

Das Richtlinien-Symbol erschein in der Farbe **Gelb**, sobald die Verbindung zum Gateway aufgebaut wurde und die Prüfung der Policy durchgeführt wird.

Es erscheint in der Farbe **Grün**, wenn die Richtlinien erfüllt werden.

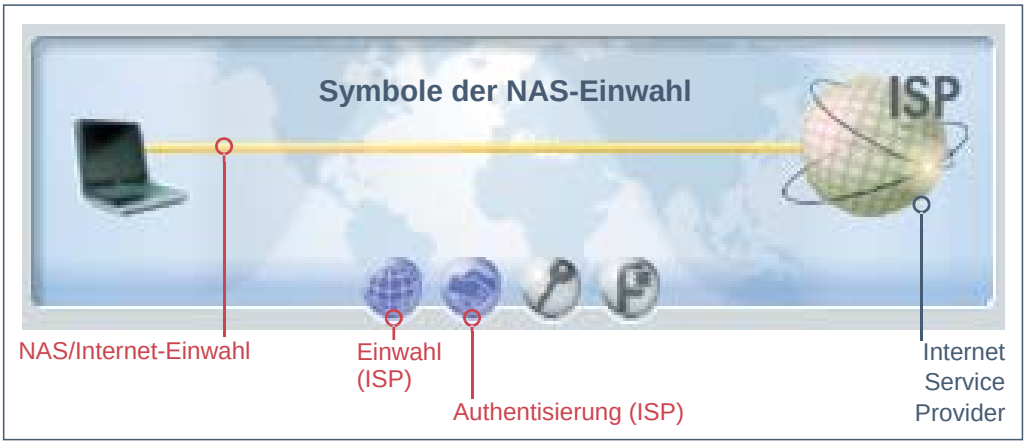
Wenn die Richtlinien nicht erfüllt werden in der Farbe **Rot**, wonach konfigurationsabhängig die Verbindung zum Gateway entweder abgebaut wird oder nur ein eingeschränkter Netzbereich für den Zugriff freigegeben wird, z. B. für ein Update.

Abweichungen am PC des Secure Clients von den Sollvorgaben werden protokolliert und können unterschiedliche Meldungen bzw. Aktionen auslösen. Diese sind:

– Anzeige einer Meldung
  in einem Informationsfenster am Client
– Ausgabe einer Meldung
  im Logbuch des Monitors
– Senden einer Meldung zum Management Server
– Senden einer Meldung zu einem Syslog Server
– Trennung der VPN-Verbindung
– Einschränkung auf einen Netzbereich

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 Ausstel-ler-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 / Tunnel-Parameter, bzw. Identität beim Entry Client) 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.

Dialog für Benutzername und Passwort

Die Dialoge für Benutzernamen- und Passwörter (Bn = Benutzername; Pw = Passwort) können vom Administrator über das Enterprise Management zusammengefasst werden. Welche Informationen in den beiden Feldern abgefragt werden, ergibt sich aus der Konfiguration der Sperren im NCP Secure Enterprise Management folgendermaßen:

– kein Bn hinterlegt => Bn-Feld leer und editierbar
– kein Pw hinterlegt => Pw-Feld leer und editierbar
– Tunnelparameter gesperrt => Bn-Feld grau,
  Bn nicht angezeigt, Pw-Feld leer und editierbar
– VPN-Bn gesperrt => Bn-Feld grau, Bn nicht angezeigt
– VPN-Bn offen => Bn-Feld editierbar,
  Bn angezeigt (falls vorhanden)

Ist in den Voreinstellungen der Management Console kein Passwort hinterlegt, so wird am Client nach erneutem Öffnen des Dialogs der zuletzt getätigte Eintrag angezeigt.

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 **Secure Enterprise 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

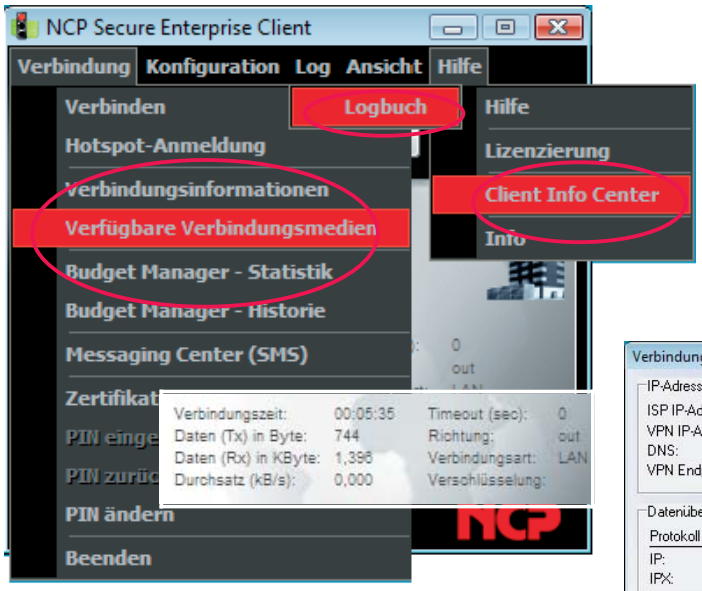
Ein automatischer Verbindungsabbau erfolgt wenn Sie den Timeout aktiviert haben. Mit diesem Parameter wird der Zeitraum festgelegt, der nach der letzten Datenbewegung (Empfang oder Versenden) verstreichen muss, bevor automatisch ein Verbindungsabbau erfolgt. Der Wert wird in Sekunden zwischen 0 und 65535 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.

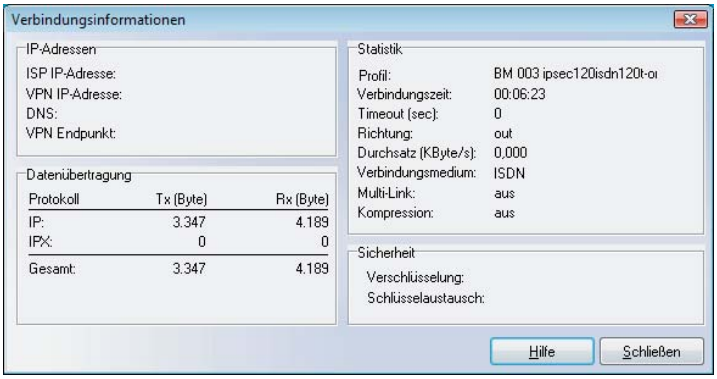
Informationsfenster des Clients

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.

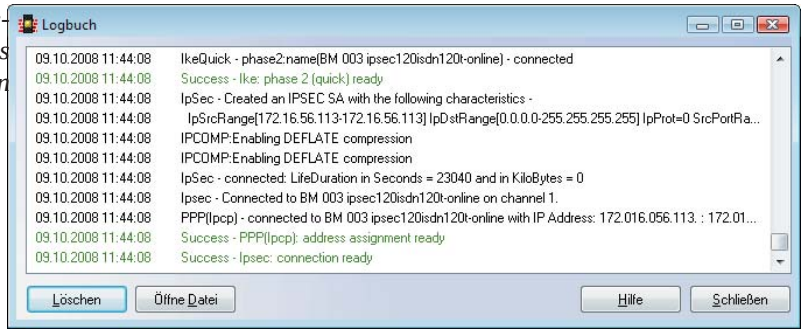


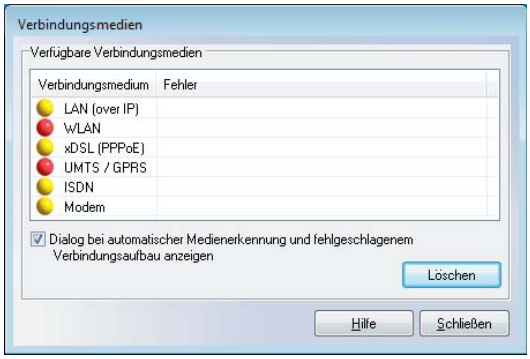
Diese Informationsfenster befinden sich im Monitormenü unter “Verbindung”, “Log” und “Hilfe”.

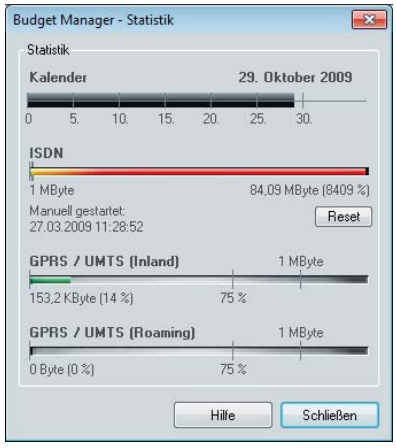
Die Informationsfenster unter “Verbindung” und “Log” können je nach Bedarf gleichzeitig offen gehalten werden (Abb. unten), währenddessen im Monitormenü oder in den Profil-Einstellungen Änderungen vorgenommen werden können.



Die Verbindungs-Informationen (rechts oben) 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 (oben) abgelesen werden.







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.

*Zur **Budget Manager-Historie** siehe weiter unten.*

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.

SSL

Der zu übertragende Session Key wird mit einem neu generierten Private Key verschlüsselt. Diese Schlüsselverhandlung wird von der Gegenstelle für den Security-Modus L2Sec vorgegeben.

SSL with Certificate

Der Private Key des verwendeten Zertifikats verschlüsselt den Session Key. Diese Schlüsselverhandlung wird von der Gegenstelle vorgegeben und in den Profil-Einstellungen unter “Security / Verschlüsselung (L2Sec)” eingegeben.

IKE (IPSec)

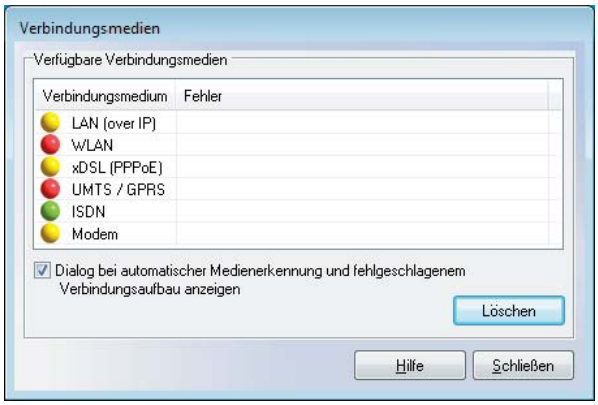
Zur Übertragung des Session Keys wird der verschlüsselte Kontrollkanal der Phase-1-Verhandlung verwendet (siehe IKE-Richtlinie).

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). Die Datenübertragung mit den SNA- und NetBIOS-Protokollen ist nur in der Client Software der Enterprise-Version aktiv.

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**.

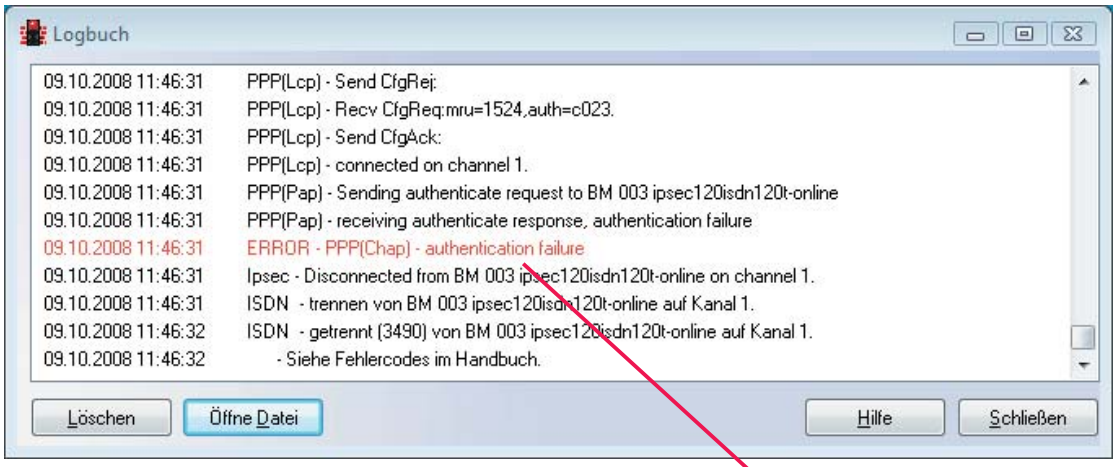
Logbuch

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.

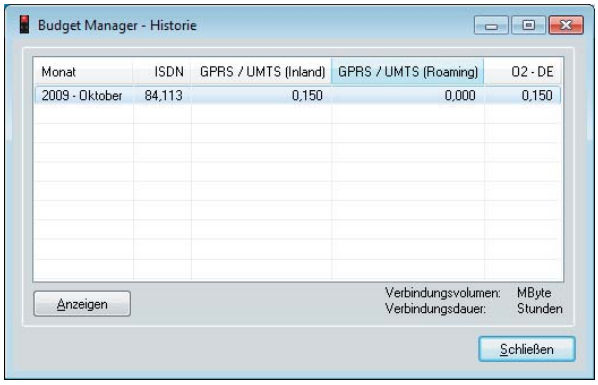
Eine zusätzliche Log-Datei speichert die Aktionen des Clients selbständig für die letzten sieben Tage. Log-Ausgaben, die älter als sieben Betriebstage sind, werden automatisch gelöscht. Die Datei steht im Installationsverzeichnis unter LOG und heißt NCPyymmdd.LOG. Sie wird mit Datumsangabe (yymmdd) immer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

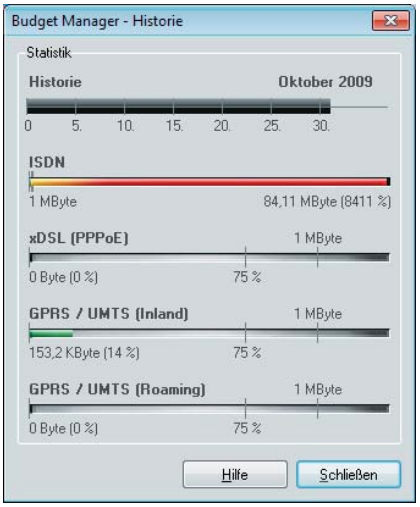
Budget-Manager Historie

Die Historie des Budget-Managers kann in zwei Fenstern angezeigt werden. Die tabellarische Übersicht (Abb. unten) zeigt pro Zeile das Verbindungsaufkommen eines Monats (max. 12 zurückliegende Monate) in Verbindungsmedien getrennt (je nach Verbindungsmedium in Stunden oder MByte).



Die grafische Ansicht (Abb. unten) erhalten Sie mit Klick auf Anzeigen. Sie zeigt die Daten korrespondierend zu den Limits, die Sie in den Verbindungsoptionen des Konfigurations-Menüs für das jeweilige Verbindungsmedium gesetzt haben.

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



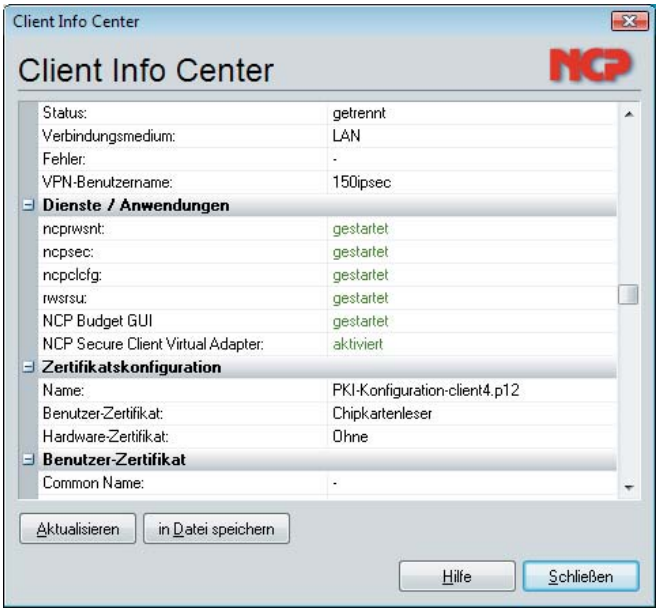
Info

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

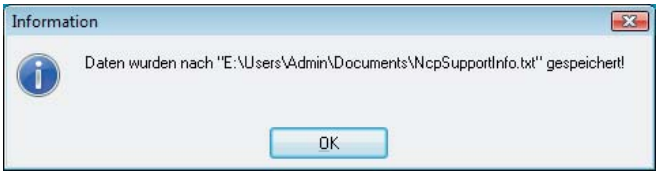
Client Info Center

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.



EAP-Optionen [Konfiguration]

In den “EAP-Optionen” des Monitor-Menüs kann angegeben werden, ob die EAP-Authentisierung nur über WLAN-, LAN- oder alle Netzwerkkarten erfolgen soll. Die hier gemachte Einstellung gilt global für alle Einträge des Telefonbuchs. In einer Aktivierungsbox kann die EAP-Authentisierung wie folgt eingestellt werden:
– deaktiviert
– für alle Netzwerkkarten
– nur für WLAN-Karten
– nur für LAN-Karten

EAP MP5

Der Einsatz des Extensible Authentication Protocols Message Digest5 (EAP MP5) kann dann zum Einsatz kommen, wenn für den Zugang zum LAN ein Switch oder für das wireless LAN ein Access Point verwendet werden, die 802.1x-fähig sind und eine entsprechende Authentisierung unterstützen. Mit dem Extensible Authentication Protocol (EAP MP5) kann verhindert werden, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.

Zur Authentisierung kann wahlweise “VPN-Benutzername” mit “VPN-Passwort” (**Tunnel-Parameter**) verwendet werden oder ein eigener “EAP-Benutzername” mit einem “EAP-Passwort”.

Zertifikatsinhalte können dergestalt automatisch übernommen werden, indem im Telefonbuch unter “Tunnel-Parameter” VPN-Benutzername und VPN-Passwort vom Zertifikat übernommen werden und in den EAP-Optionen “Verwende VPN-Benutzername und VPN-Passwort” aktiviert wird.

Bei **EAP-TLS** (mit Zertifikat) kann der EAP-Benutzername direkt aus der Zertifikats-Konfiguration bezogen werden. Folgende Inhalte des konfigurierten Zertifikats können genutzt werden, indem in die EAP-Konfiguration die entsprechenden Platzhalter eingegeben werden:

```
Commonname  : %CERT_CN%
E-Mail      : %CERT_EMAIL%
```

Dieser Parameter kann über die Management Console ab Version 1.04 Build 11 vorkonfiguriert werden.

Nach Konfiguration des EAP erscheint eine Statusanzeige im grafischen Feld des Monitors. Durch einen Doppelklick auf das **EAP-Symbol** kann das EAP zurückgesetzt werden. Anschließend erfolgt automatisch eine erneute EAP-Verhandlung.

Logon-Optionen

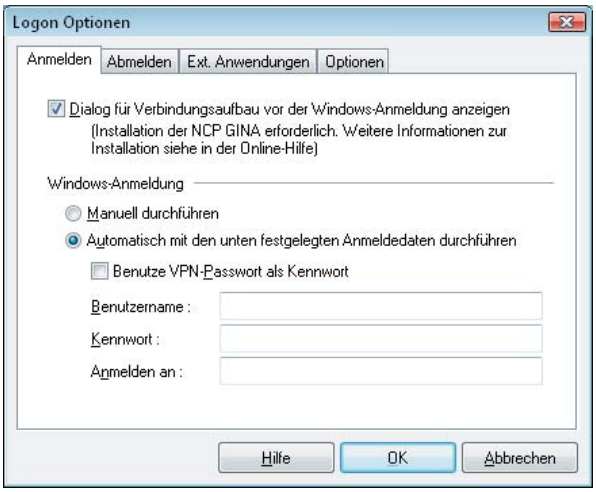
Bitte beachten Sie, dass es zur Anwendung dieses Menüpunkts unumgänglich ist, dass die Windows-Anmeldeoption (Gina / Credential) installiert wurde. Dies erfolgt normalerweise bei der Installation der Client Software, kann nachträglich aber auch mit dem Programm rwscmd.exe durchgeführt werden. Die Logon-Optionen werden erst dann wirksam, wenn der Rechner gebootet wird.

Anmelden [Logon Optionen]

Da der Verbindungsaufbau zum Gateway vor dem Windows Logon stattfindet, erfolgt die Anmeldung an der remote Domain bereits verschlüsselt und mit aktivierter Firewall.

Dialog für Verbindungsaufbau vor Windows-Anmeldung anzeigen

Die Dialoge der Logon-Option (GINA / Credential) können hier ausgeblendet werden, ohne dass dabei die Logon-Option deinstalliert wird. Für die jeweilige Arbeitsumgebung eventuell nötige Verkettungen der Logon-Option bleiben auf diese Weise bestehen.



Soll der Logon-Dialog eingeblendet werden, so ist darauf zu achten, dass die Logon-Option auf jeden Fall installiert sein muss. Dies kann auf dreierlei Weise stattfinden:

– Bei der **Software-Installation**; hierbei wird der Benutzer gefragt, ob er die Windows-Anmeldung über die Logon-Option (GINA / Credential) nutzen will. Wenn ja, wird sie installiert.
– Eine nachträgliche Installation ist über die Kommandozeilen-Schnittstelle rwscmd.exe möglich, ebenso die nachträgliche Deinstallation.
– Die Logon-Option wird auch installiert, wenn über das Secure Enterprise Management ein entsprechendes Telefonbuch bereitgestellt wird.

Wenn der Logon-Dialog nicht erscheint, kann die Verbindung zum Domain Server über die Logon-Option nicht hergestellt werden. D.h. Sie müssen den “Dialog für Verbindungsaufbau vor Windows-Anmeldung anzeigen” lassen, damit bereits in der Boot-Phase die Verbindung zum VPN Gateway hergestellt werden kann. Für diesen Verbindungsaufbau müssen ggf. die Zugangsdaten für die Netzeinwahl bzw. PIN und SIM-PIN vor der Windows-Anmeldung eingegeben werden.

Windows-Anmeldung

Die nachfolgende Windows-Anmeldung kann je nach Konfiguration manuell durchgeführt werden oder automatisch. “Manuell durchführen” bedeutet, dass der Benutzer seine Anmeldedaten per Hand in die Windows-Anmeldemaske eingibt. Automatisch bedeutet, dass die Client Software die hier eingetragenen Daten ohne Zutun des Benutzers an die Microsoft Logon-Schnittstelle (GINA / Credential) übergibt.

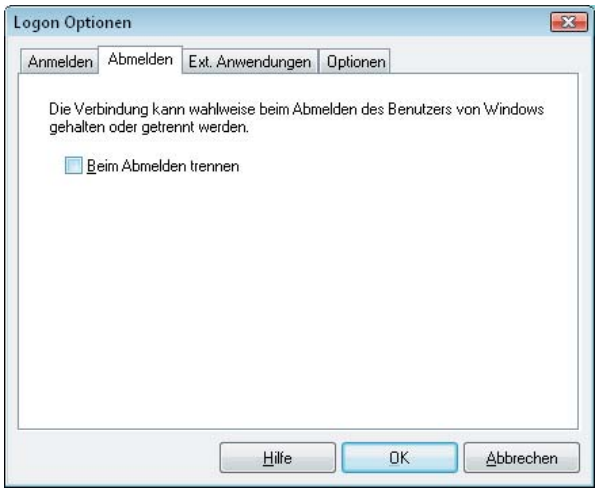
Für das Windows Logon kann auch das VPN-Passwort aus dem Telefonbuch unter “VPN-Parameter” benutzt werden, welches wiederum aus dem Zertifikat gelesen werden kann.

Wenn Sie die Logon-Option mit Rückruf nutzen, muss “Verhandle PPP Callback” aktiviert werden (siehe: Parameterfeld “Rückruf” im Telefonbuch).

Zur Anwahl an das Zielsystem mit der Logon-Option beachten Sie bitte den Abschnitt “Eine Verbindung herstellen - Client Logon” und den Anhang zum Mobile Computing.

Abmelden [Logon Optionen]

Die Verbindung des Clients zum VPN Gateway oder ISP kann beibehalten werden, wenn eine Windows-Abmeldung erfolgt.

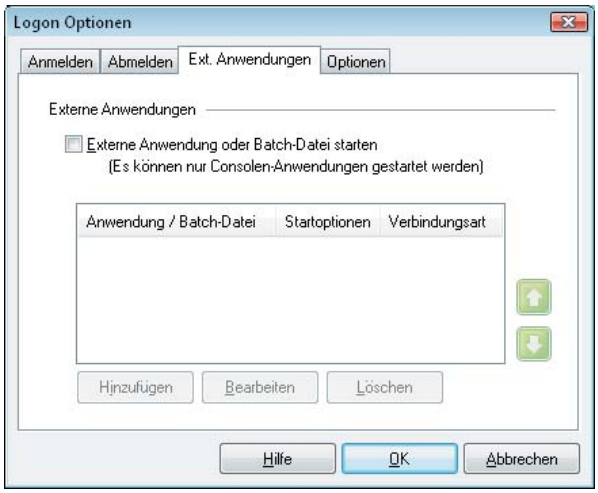


Dies gestattet einen Windows-Benutzerwechsel am Rechner vornehmen zu können, ohne die VPN-Verbindung abbauen zu müssen.

Externe Anwendungen [Logon Optionen]

Über dieses Konfigurationsfeld können in Abhängigkeit vom Client Monitor Consolen-Anwendungen oder Batch-Dateien gestartet werden (keine Windows-Programme!).

Die externen Anwendungen werden, wie weiter unten beschrieben, eingefügt. Die Reihenfolge ihres Aufrufs von oben nach unten, kann mit den grünen Pfeiltasten verändert werden. Nachdem Sie die Funktion “Externe Anwendungen oder Batch-Dateien starten” selektiert haben, können Sie über den Button mit “Hinzufügen” (siehe oben) eine Anwendung oder Batch-Datei vom Rechner selektieren, die je nach Startoption geladen wird:
– vor Verbindungsaufbau starten (precon)
– nach Verbindungsaufbau starten (postcon)
– nach Client Logon starten (immer)



Letztere Startoption gestattet das Starten von Anwendungen nach der EAP-Verhandlung über die Logon-Option (GINA / Credential) und anschließender “lokaler Anmeldung” ohne VPN-Verbindung.

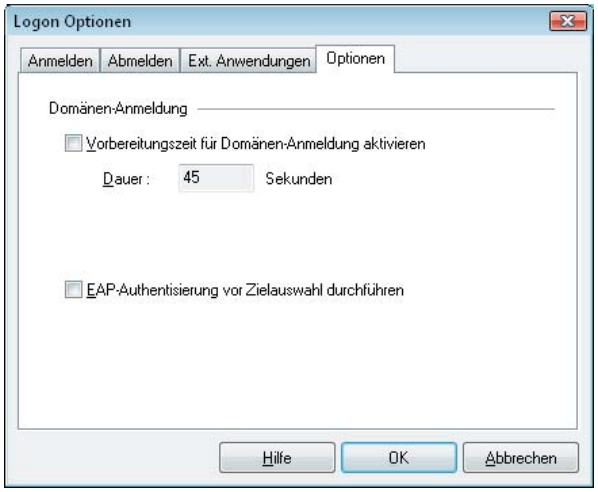
Die Anwendung kann außerdem in Abhängigkeit von der Verbindungsart des im Logon-Dialog selektierten Zielsystems gestartet werden. Die Applikation wird immer gestartet, wenn als Verbindungsart “Alle” gewählt wurde.

“Domänenvorbereitung abwarten (postdom)” bedeutet, dass die Anwendung erst nach der Domänenanmeldung gestartet wird.

Die Wait-Funktion “Warten bis Anwendung ausgeführt und beendet ist” kann dann von Bedeutung sein, wenn eine Reihe von Batch-Dateien nacheinander ausgeführt werden soll.

Optionen [Logon Optionen]

Zwischen Netzanmeldung und Domänen-Anmeldung benötigt Windows eine gewisse Initialisierungszeit. Diese Vorbereitungszeit für die Domänenanmeldung kann hier aktiviert und eingestellt werden. Die Windows-Anmeldung findet erst nach der hier eingestellten Initialisierungs-Zeit nach dem Verbindungsaufbau statt.



Der Standardwert beträgt 45 Sekunden und kann nach Bedarf verändert werden.

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

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

EAP-Authentisierung vor Zielauswahl

Standardmäßig erfolgt die EAP-Authentisierung vor dem Verbindungsaufbau zum VPN Gateway. Soll EAP genutzt werden, ohne dass anschließend eine Verbindung über den Client (reiner EAP Client) aufgebaut werden soll, so muss diese Funktion aktiviert werden. Wird EAP mit Zertifikat eingesetzt, so erscheint der PIN-Dialog zur Authentisierung an den Netzwerkkomponenten. Danach kann die Zielauswahl erfolgen.

Wird die Funktion nicht aktiviert, findet die EAP-Authentisierung erst nach der Zielauswahl statt.

Immer auf Start der NCP-Dienste vor der Übergabe an Windows-Anmeldung warten

Diese Option ist nur dann erforderlich, wenn der Dialog für den Verbindungsaufbau vor der Windows-Anmeldung unsichtbar geschaltet wurde. (Siehe oben “Anmelden / Dialog für Verbindungsaufbau vor Windows-Anmeldung anzeigen”.)

Mit Aktivierung dieser Funktion wartet die NCP Gina ab, bis alle NCP Dienste gestartet sind. Damit wird sichergestellt, dass diese Dienste für die nachfolgende Windows-Anmeldung zur Verfügung stehen. (Dies ist zum Beispiel beim Einsatz von von SafeGuard Easy mit Auto-Logon-Funktion erforderlich.)

Wird die Funktion “ohne Abbruch-Option” eingesetzt, so kann über das Meldungsfenster eines Dienstestarts (z. B. “Netzwerkdienste werden gestartet”) keiner der Dienste mit dem Abbruch-Button vorzeitig beendet werden.