

SecurITy
made
in
Germany
Trust Seal
www.teletrust.de/itsmig

NCP

NCP Secure Entry Client

Administrationshandbuch

Version 13



www.ncp-e.com

Kontakt

Wenn Sie weitere Informationen wünschen oder Fragen zu NCP-Produkten und Service-Leistungen haben:

Deutschland

NCP engineering GmbH
Dombühlerstraße 2
D-90449 Nürnberg
Tel.: +49 (911) 9968 0
Homepage: <http://www.ncp-e.com>
Mail: info@ncp-e.com

Support per E-Mail:

support@ncp-e.com (deutsch)
helpdesk@ncp-e.com (englisch)

Support Hotline:

0900 / 1 99 68 00
(nur aus Deutschland erreichbar, 80 Cent / Minute)
Unsere Supportzeiten sind von Mo - Fr von 08:00 - 17:00 Uhr.

USA, North America

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
Phone: +1 (650) 316-6273

Bei einer Support-Anfrage benötigen wir folgende Informationen:

- Genauer Produktname
- Seriennummer
- Versionsnummer
- Genaue Problembeschreibung
- Fehlermeldung

NCP Secure Entry Client

Alle Programme und diese Beschreibung wurden mit größter Sorgfalt erstellt und nach dem Stand der Technik auf Korrektheit überprüft. Alle Haftungsansprüche infolge direkter oder indirekter Fehler, oder Zerstörungen, die im Zusammenhang mit den Programmen stehen, sind ausdrücklich ausgeschlossen. Die in diesem Handbuch enthaltene Information kann ohne Vorankündigung geändert werden und stellt keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten. Ohne ausdrückliche schriftliche Erlaubnis von NCP engineering GmbH darf kein Teil dieser Beschreibung für irgendwelche Zwecke oder in irgendeiner Form elektronisch oder mechanisch, reproduziert oder übertragen werden. Alle anderen genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Inhaltsverzeichnis

Produktbeschreibung	10
FIPS-Zertifizierung	11
Personal Firewall	11
PKI-Unterstützung	11
Installation der Software	14
Client-Monitor	26
Verbindung [Menü]	27
Verbinden / Trennen	28
Home Zone	29
Hotspot-Anmeldung	29
Mobilfunkkarte	31
Netzsuche	31
Mobilfunknetz aktivieren	31
SIM PIN eingeben	31
SIM PIN ändern	32
PUK-Eingabe	32
Verbindungsinformationen	32
Verfügbare Verbindungsmedien	32
Budget Manager Statistik	34
Budget Manager Historie	34
Zertifikate [Ansicht]	35
Aussteller-Zertifikat anzeigen	36
Benutzer-Zertifikat anzeigen	38
Eingehendes Zertifikat anzeigen	40
CA-Zertifikate anzeigen	43
Computer-Zertifikat (Ansicht)	45
PIN eingeben	47
PIN zurücksetzen	47
PIN ändern	48
Sperrung aufheben	49
Beenden	50
Konfiguration [Menü]	51
Profile [Konfiguration]	51
Profil-Einstellungen	53
Profil-Gruppen	54

Firewall [Konfiguration]	55
Grundeinstellungen mit Standard-Konfiguration	57
Regel-Tabelle	60
Bekannte Netze	65
Manuelle Konfiguration der bekannten Netze	65
Automatische Erkennung der bekannten Netze	66
Optionen	68
Aktionen	69
Optionen [Firewall]	72
Allgemein	74
Kommandos [Firewall]	77
Protokollierung	77
VPN-Bypass	79
Quality of Service	81
WLAN-Management	87
Verbindungen	89
Profile [WLAN]	91
Allgemeine Profil-Einstellungen	92
Verschlüsselung [WLAN-Profil]	93
IP-Adressen [WLAN-Profil]	94
Authentisierung [WLAN-Profil]	95
Optionen [WLAN-Profil]	97
Statistik	97
Zertifikate [Konfiguration]	98
Benutzer-Zertifikat [Konfiguration]	99
Soft-Zertifikatsauswahl	102
PIN-Richtlinie	103
Zertifikatsverlängerung	103
Computer-Zertifikat	103
Verbindungsoptionen [Konfiguration]	105
Budget-Manager [Konfiguration]	105
Einstellungen [Budget-Manager]	106
Aktionen [Budget-Manager]	106
Mobilfunknetz [Budget-Manager]	107
WLAN-Zugriffspunkte [Budget-Manager]	107
Externe Anwendungen	109
Optionen [Mobilfunk]	110
Logon-Optionen	111
Anmelden [Logon Optionen]	112

Abmelden [Logon Optionen]	113
Externe Anwendungen [Logon Optionen]	114
Optionen [Logon Optionen]	115
Konfigurationssperren	116
Allgemein [Konfigurationssperren]	116
Profile [Konfigurationssperren]	116
Mobilfunknetz [Konfigurationssperren]	117
Weitere Optionen	118
Proxy für VPN Path Finder	118
EAP-Optionen [Konfiguration]	119
FIPS	120
Profil-Sicherung	121
Erstellen [Profil-Sicherung]	121
Wiederherstellen [Profil-Sicherung]	121
Ansicht	122
Profilauswahl anzeigen	122
Statistik anzeigen	122
WLAN-Status anzeigen	122
Tipps anzeigen	122
Immer im Vordergrund	123
Autostart	123
Beim Schließen minimieren	123
Nach Verbindungsaufbau minimieren	123
GUI-Skalierung	124
Sprache	124
Hilfe	125
Logbuch	126
Erweiterte Log-Einstellungen	128
Client Info Center	129
Netzwerkdiagnose	130
Support-Assistent	130
Auf Updates prüfen	130
Aktivierung	130
Client deaktivieren	132
Info	132
Konfigurationsparameter	133
Profile [Parameter]	135
Grundeinstellungen [Profile]	136

Profil-Name	137
Verbindungstyp	137
Verbindungsmedium	138
Standard-Profil nach jedem Neustart des Systems	140
Profil für automatische Medienerkennung	141
Einwahl über Windows DFÜ	142
Seamless Roaming	143
Netzeinwahl	144
Benutzername [Netzverbindung]	144
Passwort [Netzverbindung]	145
Passwort speichern	146
Rufnummer (Ziel)	147
RAS Script-Datei	148
Mobilfunknetz-Konfiguration	149
HTTP-Anmeldung [Profile]	151
Benutzername [HTTP-Anmeldung]	152
Passwort [HTTP-Anmeldung]	152
HTTP-Authentisierungs-Script [HTTP-Anmeldung]	152
Verbindungssteuerung [Profile]	153
Verbindungsaufbau [Verbindungssteuerung]	154
Timeout [Verbindungssteuerung]	155
Timeout-Richtung	156
OTP-Token	157
Tausche OTP (Einmalpasswort) und PIN	157
Benutzername unterdrücken bei Eingabeaufforderung	158
Logischen VPN-Tunnel bei Verbindungsunterbrechung trennen	159
Voice over IP (VoIP) priorisieren	159
Aktiviere Tunnel Traffic Monitoring	160
Alternative IP-Adresse	161
IP Broadcast erlaubt [Link-Einstellungen]	161
Quality of Service (für Profil)	162
Erweiterte Authentisierung [Authentisierung vor VPN]	164
Fingerabdrucksensor / Biometrische Authentisierung	164
EAP-Authentisierung [vor VPN]	164
HTTP-Authentisierung [vor VPN]	165
IPsec-Einstellungen	167
Gateway (Tunnel-Endpunkt)	170
Austausch-Modus (IPsec) [Profile]	171
Tunnel IP-Version	172

Richtlinien	173
IKE DH-Gruppe [IKE-Richtlinie]	173
IKEv1-Richtlinie [IPsec-Konfiguration]	174
Name [IKE-Richtlinie]	175
Authentisierung [IKE-Richtlinie]	175
Verschlüsselung [IKE-Richtlinie]	175
Hash [IKE-Richtlinie]	175
IKEv2-Authentisierung [Profile]	176
IKEv2-Richtlinie [IPsec-Konfiguration]	179
Name [IKEv2-Richtlinie]	179
Verschlüsselung [IKEv2-Richtlinie]	179
Pseudorandom-Funktion [IKEv2-Richtlinie]	179
Integritäts-Algorithmus [IKEv2-Richtlinie]	180
IPsec-Richtlinie [Auswahl]	181
IPsec-Richtlinie [Profile]	181
Name [IPsec-Richtlinie]	182
Protokoll [IPsec-Richtlinie]	182
Transformation / Verschlüsselung	182
Authentisierung [IPsec-Richtlinie]	182
PFS / DH-Gruppe	183
IPsec-Einstellungen [Richtlinien]	184
Art der Gültigkeit [Richtlinie]	184
Gültigkeitsdauer [Richtlinie]	184
Volumen [Richtlinie]	184
Erweiterte IPsec-Optionen	185
IPsec-Kompression	185
Standard IPsec / UDP Encapsulation	185
Deaktiviere DPD (Dead Peer Detection)	185
Anti-replay Protection	186
Aktiviere Verhandlung nach RFC 7427	186
VPN Path Finder	186
RFC 7427 Padding-Verfahren	186
IKEv2 RSA Authentisierung mit PRF-Hash	187
Identität	188
IKE ID-Typ [Identität]	189
IKE ID [Identität]	189
Pre-shared Key	189
Zertifikatskonfiguration [Profile]	190
Extended Authentication (XAUTH)	190

Benutzername [Identität]	190
Passwort [Identität]	190
VPN-Zugangsdaten aus Konfiguration	191
IPsec Adresszuweisung	193
Zuweisung der privaten IP-Adresse	193
DNS / WINS Server	194
Domain Name	194
Split Tunneling	195
Entfernte Netzwerke (IPv4)	195
Auch lokale Netze im Tunnel weiterleiten	196
Entfernte Netzwerke (IPv6)	196
VPN-Bypass	196
Zertifikats-Überprüfung	197
Benutzer des eingehenden Zertifikats	198
Aussteller des eingehenden Zertifikats	199
Fingerprint des Aussteller-Zertifikats	200
Benutze SHA1 Fingerprint statt MD5	200
Weitere Zertifikats-Überprüfungen	201
Link Firewall	203
Stateful Inspection	203
Ausschließlich Kommunikation im Tunnel zulassen	203
In Kombination mit dem Microsoft DFÜ-Dialer	203
Funktionen	204
Home Zone	205
VPN-Bypass	209
Biometrische Authentisierung	211
Credential Provider	213
QoS (Beschreibung)	215
IPsec RFCs	217
Werkzeuge	219
Kommandozeilen-Schnittstelle NCPClientCMD.EXE	220
Funktionserweiterungen mit NCPRWSNT.EXE	234
Allgemeine Registry-Werte	236

Produktbeschreibung

Der universelle IPsec Client

Der IPsec Client kann in beliebigen VPN-Umgebungen eingesetzt werden und kommuniziert auf der Basis des IPsec-Standards mit den Gateways verschiedenster Hersteller. Die Client Software emuliert einen Ethernet LAN-Adapter und verfügt über zusätzliche Leistungsmerkmale, die dem Anwender den Einstieg in eine ganzheitliche Remote Access VPN-Lösung ermöglichen.

Die grafische Oberfläche des Clients schafft Transparenz während des Einwahlvorganges und Datentransfers. Sie informiert u. a. über den aktuellen Datendurchsatz.

Features des IPsec Clients

- Unterstützung aller gängigen Microsoft Betriebssysteme (Windows 10). Lieferbar auch als OS X oder Android Client.
- Unabhängigkeit vom Übertragungsmedium (Mediatyp-neutral)
- Unterstützung aller marktgängigen Betriebssysteme und unterschiedlichster Endgeräte
- Sicherheit und Managebarkeit durch Unabhängigkeit vom Microsoft DFÜ-Dialer
- Kommunikation mit IPsec-Gateways auch von Drittherstellern (Kompatibilität)
- Installation auf Einzelplatz-PCs und LAN-PCs (auch hinter IP-Routern mit IP-NAT)
- Integrierte [Personal Firewall](#) ^[11]
- Domänenanmeldung ([Credential Provider](#)) ^[213]
- [Extended Authentication](#) ^[190] (XAUTH)-Support zur Authentisierung mittels User ID und Passwort
- [Internet Key Exchange Config Mode \(IKE CFG\)](#) ^[193] für eine dynamische Zuweisung von IP-Adresse, DNS Server, Windows Name Server und Domain Name
- [Dead Peer Detection \(DPD\)](#) ^[185] Konfiguration bei Tunnel Failover - Benutzerkonfigurierbare Zeitintervalle bei DPD-Vorfällen zur flexibleren Kontrolle für die Wiederherstellung von VPN-Tunnel
- Unterstützung des [Extensible Authentication Protocols \(EAP\)](#) ^[119] mit den Funktionen Transport Layer Security (TLS) und MD5 (User ID/Passwort) zur sicheren Authentisierung des Anwenders gegenüber Access Points und Switches
- Network Address Translation-Traversal (NAT-T) für die Kommunikation zwischen Client und Gateway über Netzwerkkomponenten, die NAT durchführen
- Intelligentes Verbindungs-Management zur Minimierung der Übertragungskosten und Erhöhung der Transparenz (Gebühren-Manager)

FIPS-Zertifizierung

Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul 140-2, das diese Algorithmen beinhaltet, besitzt die Zertifizierung #1747.

Die FIPS-Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

- Diffie Hellman-Gruppe: Gruppe 2 bis 14 (DH Länge von 1024 Bit bis 2048 Bit)
- Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit
- Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES

Die entsprechenden Module können in den [IPsec-Einstellungen](#)  konfiguriert werden.

Personal Firewall

Der Client verfügt über alle erforderlichen Funktionalitäten einer Personal Firewall um den PC-Arbeitsplatz umfassend gegenüber Angriffen aus dem Internet und anderer LAN-Teilnehmer (WLAN oder LAN) zu schützen. Außerdem besteht keine Möglichkeit, dass der Dialer von automatischen 0190er- und 0900er-Dialern für ungewollte Verbindungen missbraucht wird. Die wesentlichen Security-Mechanismen sind IP-NAT und Protokollfilter. NAT (Network Address Translation) ist ein Security-Standard zum Verbergen der individuellen IP-Adressen gegenüber dem Internet. NAT bewirkt eine Übersetzung der von außen sichtbaren Adresse in entsprechende Client-Adressen und umgekehrt. Ankommende Datenpakete werden auf der Basis eines ausgeklügelten Filterings nach genau definierten Eigenschaften überprüft und bei Nichtübereinstimmung abgewiesen. Das heißt: Der Internet-Port des jeweiligen Rechners wird vollständig getarnt und der Aufbau von unerwünschten Verbindungen unmöglich.

PKI-Unterstützung

Die Zugangssicherheit zum PC und damit dem Firmennetz kann durch den Einsatz digitaler Zertifikate in Form von Software (PKCS#12) oder Smart Cards (PKCS#11, CT-API, PC/SC) erhöht werden. Der Client unterstützt hierfür die Einbindung in eine PKI (Public Key Infrastruktur). Im Folgenden sind einige Elemente einer PKI beschrieben.

Public Key Infrastruktur

Public-Key-Infrastrukturen (PKI) beschreiben ein weltweit genutztes Verfahren, um zwischen beliebigen Kommunikationspartnern auf elektronischem Wege Schlüssel sicher auszutauschen. Die PKI bedient sich dabei sogenannter Schlüsselpärchen aus jeweils einem öffentlichen und einem privaten Schlüssel. In der Welt des elektronischen, globalen Informationsaustausches wird so eine Vertrauensbasis aufgebaut, wie wir sie in der traditionellen Geschäftswelt auf Papierbasis kennen. Die digitale Signatur in Verbindung mit Datenverschlüsselung ist das elektronische Äquivalent zur händisch geleisteten Unterschrift und belegt Ursprung sowie die Authentizität von Daten und Teilnehmer.

Eine PKI basiert auf digitalen Zertifikaten, die - von einer öffentlichen Zertifizierungsstelle (Trust Center) ausgestellt - als persönliche "elektronische Ausweise" fungieren und idealerweise auf einer Smart Card

abgespeichert sind. Sicherheitsexperten und der IETF (Internet Engineering Task Force) sind sich darüber einig, dass ein nachhaltiger Schutz vor Man-In-The-Middle-Attacken nur durch den Einsatz von Smart Cards mit Zertifikaten erreicht werden kann.

Smartcard

Smart Cards sind die ideale Ergänzung für hochsichere Remote Access-Lösungen. Sie bieten doppelte Sicherheit beim Login-Vorgang, nämlich Wissen über PIN (Persönliche Identifikations Nummer) und Besitz der Smart Card. Der Anwender identifiziert sich mit der Eingabe der PIN eindeutig als rechtmäßiger Besitzer (Strong Authentication). Die PIN ersetzt das Passwort und die Eingabe der User-ID (Basistechnologie für Single Sign On). Der Anwender weist sich nur noch gegenüber der Smart Card aus. Der Check gegenüber dem Netz erfolgt zwischen Smart Card und Security-System. Alle sicherheitsrelevanten Operationen laufen vollständig im Inneren der Karte - also außerhalb des PCs - ab. Das System ist neben individuellen Anpassungen an Schutzmechanismen offen für multifunktionalen Einsatz (z. B. als Company Card). Auch biometrische Verfahren lassen sich integrieren.

Unterstützte Schnittstellen und Formate

Der Secure Client kann in Public Key Infrastrukturen nach X.509 V.3 Standard eingesetzt werden und unterstützt folgende Schnittstellen / Formate:

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

CA-Zertifikate

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

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

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

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

Verwendung einer Sperrliste (CRL)

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

Werden Sperrlisten eingesetzt, so werden normalerweise dann keine Meldungen ausgegeben, wenn am Client keine Sperrliste für eingehende Zertifikate hinterlegt ist. Soll in solchen Fällen dennoch eine Meldung ausgegeben werden, muss die Datei NCPPKI.CONF editiert werden. Sie befindet sich im Installations-Verzeichnis. Der Standardeintrag im Abschnitt [General] lautet:

Enablecrlinfo = 0

Dies bewirkt, dass keine Meldungen ausgegeben werden, wenn zu einem Zertifikat der Gegenstelle keine Sperrliste am Client gefunden wird. Soll eine Meldung ausgegeben werden, so muss diese Einstellung abgeändert werden auf:

Enablecrlinfo = 1

Installation der Software

Folgende Installationsmöglichkeiten stehen zur Verfügung:

- Standard-Installation mit EXE-Datei
- Installation mit der MSI-Datei (extrahiert aus EXE-Datei)

Beachten Sie, dass eine Installation immer Administratorrechte erfordert.

Standard-Installation mit EXE-Dateien

Die Standard-Installation der Software für Windows-Systeme erfolgt komfortabel über Setup. Der Installationsablauf ist für alle Versionen des Clients identisch. Bitte beachten Sie vor der Installation die folgenden Punkte.

Release Notes

Bevor Sie die Software installieren, lesen Sie bitte die beiliegenden Release Notes.

Gegenstelle

Die Gegenstelle muss eines der folgenden Verbindungsmedien unterstützen: Mobilfunknetz, LAN over IP oder WLAN.

Lizenzschlüssel

Software Update und Lizenzschlüssel

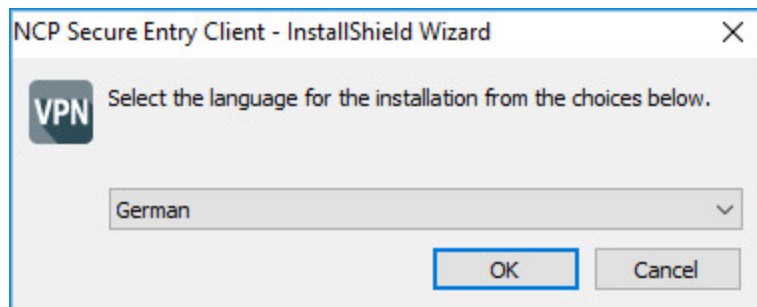
Ab der aktuellen Software-Version benötigt jedes zukünftige Major Release der Software einen neuen Lizenzschlüssel gleicher Version.

Erfolgt das Software Update ohne nachfolgendes Lizenz Update so kann der Client nur für die Restlaufzeit der 30-Tage-Testversion bis zum Erhalt der neuen Lizenz für die neue Version betrieben werden.

Neue Installation und Lizenzschlüssel

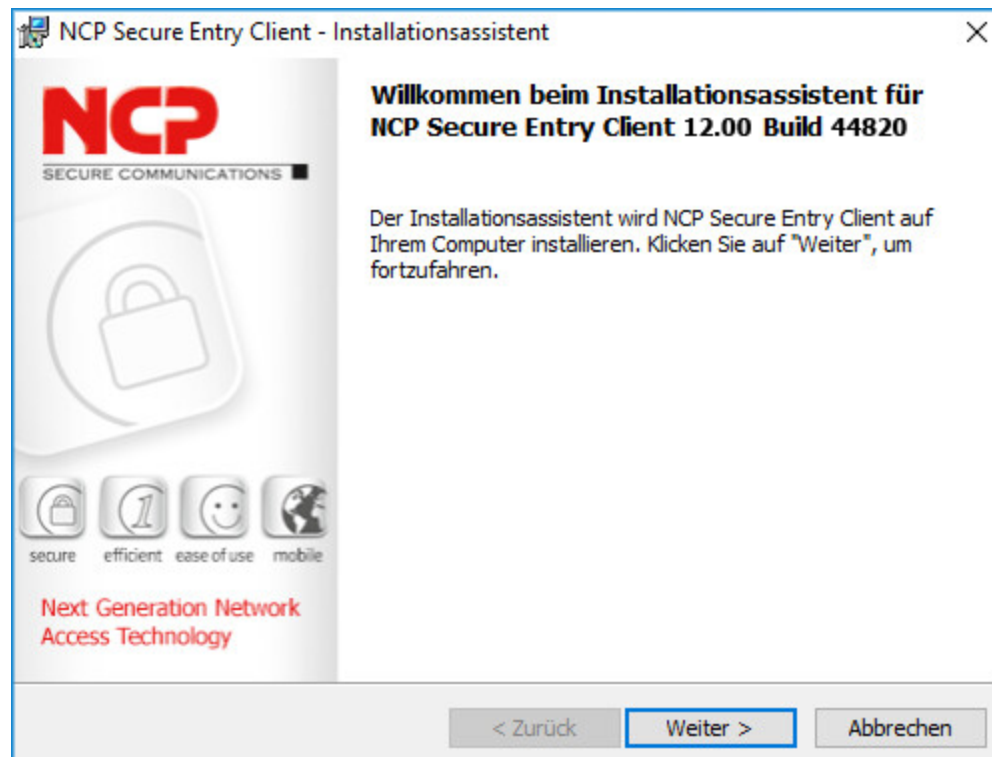
Bei Neu-Installationen wird die Client Software standardmäßig im Verzeichnis „Programme“ installiert und als [Testversion](#)¹⁶⁾ (max. 30 Tage) bis zur Eingabe der passenden Lizenz für die neue Version betrieben.

Um die Installation des *NCP Secure Entry Client* zu starten, starten Sie die Installationsdatei. Die Installation beginnt mit der Auswahl der Sprache des Installationsassistenten.

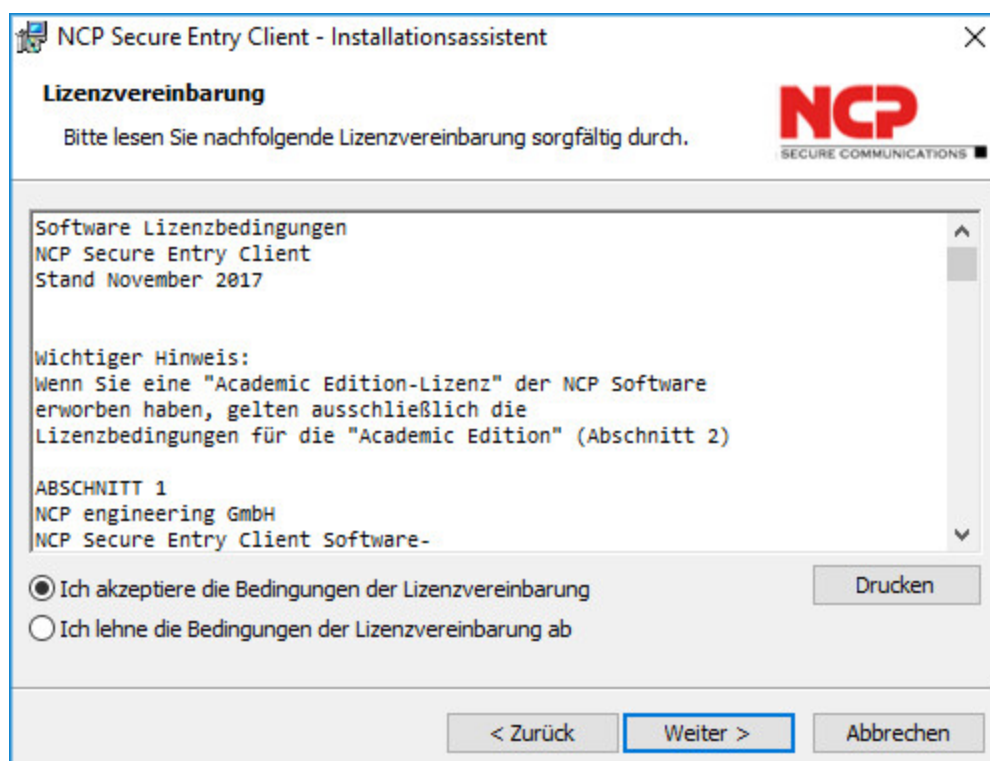


Der Installationsassistent (InstallShield Wizard) wird vorbereitet.

Es erscheint das Willkommen-Fenster. Mit „Weiter“ beginnen Sie die Installation.



Klicken Sie auf „Weiter“ und lesen Sie die Lizenzbedingungen ausführlich durch. Um die Installation fortzusetzen, akzeptieren Sie die Lizenzbedingungen. Lehen Sie die Lizenzbedingungen ab oder klicken auf „Abbrechen“ wird die Installation abgebrochen.



Folgen Sie den Anweisungen des Installationsassistenten.

Führen Sie nach erfolgreicher Installation einen Neustart Ihres Rechners aus.

Testversion

Starten Sie die Testversion, so ist diese vom Zeitpunkt der Installation für 30 Tage gültig und kann danach nicht mehr genutzt werden. Mit dem Start der Testversion können zugleich zwei VPN-Profile für Testverbindungen angelegt werden, eine für IPsec mit IKEv1, eine mit IKEv2.

ncpphone.cnf und ncpphone.cfg bei Installation importieren

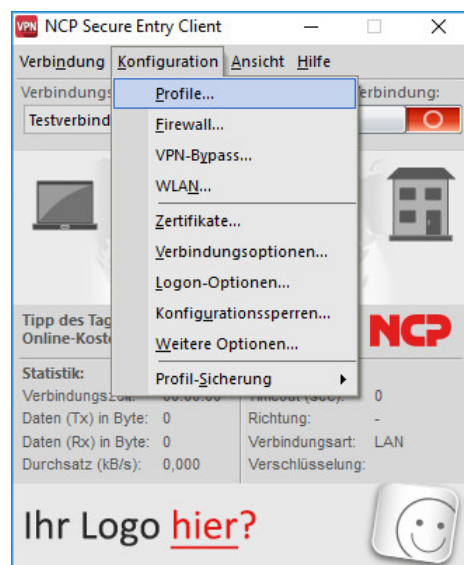
Befinden sich während der Installation die Dateien `ncpphone.cnf` oder `ncpphone.cfg` im Installationsordner, werden diese automatisch migriert. So werden deren Einstellungen übernommen und stehen nach der Installation zur Verfügung.

Hinweis: Wenn Sie eine Konfigurationsdatei während der Client-Installation einspielen, die *Stateful Boot*-Konfigurationen der Firewall enthält, werden diese als aktiv angezeigt, sind aber auf Treiberebene noch nicht wirksam. Hierfür ist ein weiterer Neustart des Systems notwendig.

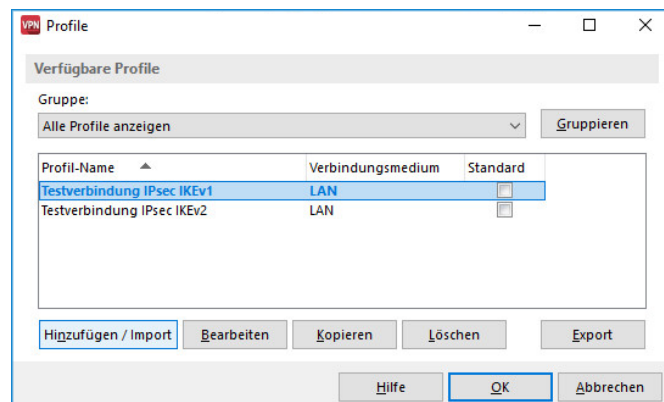
Hinzufügen eines Verbindungs-Profiles

Mit dem Konfigurations-Assistenten können Verbindungen mit dem Internet oder, je nach erforderlichlichem VPN-Übertragungsprotokoll, zum Firmennetz rasch hergestellt werden. Je nach Auswahl der gewünschten Grundeinstellung wird das VPN-Profil nach wenigen Konfigurationsabfragen in der Liste verfügbarer VPN-Profile abgelegt.

Starten Sie den Client und öffnen Sie in der Menüleiste den Menüpunkt „Konfiguration“ und wählen Sie „Profile...“. (siehe Bild unten).



In dem Fenster, das sich öffnet, haben Sie die Möglichkeit über „Hinzufügen“ ein neues Profil anzulegen (siehe Bild unten).



Im Folgenden die jeweils nötigen Daten zur Konfiguration:

Verbindung zum Firmennetz über IPSec:

- Profil-Name
- Verbindungsmedium
- Zugangsdaten für Internet-Dienstanbieter (Benutzer, Passwort, Rufnummer)
- VPN-Gateway-Parameter (VPN-Gateway, Tunnelsecret)
- Nutzung von Zertifikaten
- Zugangsdaten für VPN-Gateway (VPN-Benutzer, VPN-Passwort)
- Statischer Schlüssel (Preshared Key) sofern kein Zertifikat eingesetzt wird (IKE ID-Typ, IKE ID)

Verbindung mit dem Internet herstellen:

- Profil-Name
- Verbindungsmedium
- Zugangsdaten für Internet-Dienstanbieter (Benutzer, Passwort, Rufnummer)

Alternativ kann ein bereits bestehendes VPN-Profil folgender Formate importiert werden: *.ini; *.pcf; *.wgx; *.wgc

Installation mit der MSI-Datei (extrahiert aus EXE-Datei)

Die MSI-Datei ist in der bereitgestellten EXE-Datei enthalten. Mit folgendem NCP-spezifischen Kommando kann das MSI-Paket aus dem EXE-Installer extrahiert werden. Beim Extrahieren des MSI-Pakets muss bereits die gewünschte Sprache angegeben werden, damit auch die dazugehörige MST-Datei mit der Sprache extrahiert wird (ohne Sprachauswahl wird Englisch verwendet):

```
[filename].exe /s /l1031 /b"C:\[FolderInWhichMSIWillBeExtracted]" /v"/qn  
EXTRACT_MSI_ONLY=1 /log install.txt"
```

EXE-Kommandos:

/s = ohne Dialog für Sprachauswahl (optional)

/l = Sprach-ID (optional)

1031 = Deutsch

1033 = Englisch

1034 = Spanisch

1036 = Französisch

/b = Angabe des Verzeichnisses für das Extrahieren des MSI-Pakets

/v = Übergabe von Parameter an den MSI-Installer

(Die hier gezeigten MSI-Kommandos werden in der unten stehenden Tabelle erklärt.)

Durch das Extrahieren entstehen folgende Dateien:

setup.msi

<Sprach-ID>.mst

Aus diesem Grund stellt NCP ausschließlich die ausführbare EXE-Datei zur Verfügung, die im Dateinamen auch die aktuelle Version enthält. Die aktuelle Version ist im Namen der MSI-Datei nicht enthalten. Der Name der MSI-Datei kann beliebig verändert werden.

Installation mit der MSI-Datei

Mit Zuweisung von Parametern kann die Installation über Parameter beeinflusst und vordefiniert werden. Z.B. kann das Installationsverzeichnis vordefiniert und zusätzliche Dateien (z.B. Zertifikate) mitgegeben werden. Für eine Silent-Installation können darüber hinaus die Optionen gesetzt werden, welche ansonsten über den Installationsassistenten (Wizzard) per Hand vorgegeben werden müssen.

Gesetzt werden kann ein Parameter einfach über das Gleichheitszeichen „=“.

Zum Beispiel:

```
INSTALLDIR=C:\Programme\MyCompany\MyProduct
```

Übersicht von NCP-spezifischen und nützlichen MSI-Parametern

NCP_CREATE_DESKTOPICON	Secure Client	Erstellt ein Desktop-Icon zum Starten des Client Monitors.	0=off (default), 1=on	NCP
AUTORUN	Secure Client	Aktiviert den Autostart des Monitors.	0=off (default), 1=on	NCP
EXTRACT_MSI_ONLY	Secure Client	Beendet die Ausführung nach dem Entpacken des MSI-Pakets sofort wieder.	0=off (default), 1=on	NCP
ADDLOCAL=FipsMode REMOVE=FipsMode	Secure Client	Mit diesen standard MSI-Kommandos kann der FipsMode hinzugefügt werden oder als Feature gelöscht werden.*		NCP
INSTALLDIR	alle Produkte	Über diesen Parameter kann das Installationsverzeichnis der Software definiert werden. Beinhaltet der Name des Verzeichnisses Leerzeichen, muss es in Anführungszeichen gesetzt werden.	String	MSI
ProductLanguage	alle Produkte	Mit diesem Parameter kann die gewünschte Sprache vordefiniert werden. Abhängig davon wie das MSI-Paket erzeugt wurde, muss ggf. noch als Transform-Datei die dazugehörige Sprach-Datei mitgegeben werden.**	Deutsch=1031 Englisch=1033 Französisch=1036 Spanisch=1024	MSI
TRANSFORMS	alle Produkte	Hiermit kann die extrahierte Sprachdatei mitgegeben werden. Durch die Trennung mit ";" werden weitere Dateien mitgegeben.	Name der MST-Datei	MSI
REBOOT	alle Produkte	Hiermit kann der Neustart nach Abschluss der Installation gesteuert werden.	Force (default)= Neustart ReallySuppress= kein Neustart	MSI

* Bei Neu-Installation und im Wartungsmodus wird unter „Ändern/Change“ der Dialog „CustomSetup“ angezeigt, worüber diese MSI-Kommandos angegeben werden können.

****** Die in der Tabelle oben angezeigten Sprach-IDs sind von Microsoft definiert und werden von NCP unterstützt.

Spracheinstellung bei der Installation über das MSI-Paket

Soll die Installation über das MSI-Paket und einer vordefinierten Sprache erfolgen muss es mit folgenden Argumenten gestartet werden:

```
Msiexec /i "NCP_EpCl_Windows_x86-64.msi" ProductLanguage=1031  
TRANSFORMS=1031.mst /qn /Log C:\Windows\Temp\myinstall.log
```

In diesem Fall sorgen `/qn /Log` dafür, dass die Installation komplett ohne Benutzeroberfläche ausgeführt wird und Log-Dateien erzeugt werden.

Beim Installieren zusätzliche Dateien hinzufügen

Zusätzliche Dateien können zum Beispiel eigene Zertifikate oder Dateien für ein kundenspezifisches Projekt-Logo (CBO) sein, welche mit dem Setup installiert werden sollen.

Findet der Installer im Verzeichnis in dem sich auch das MSI-Paket oder der Installer als EXE-Datei befindet das Verzeichnis `IMPORTDIR`, werden aus diesem Verzeichnis alle Dateien rekursiv, inklusive aller Unterverzeichnisse, ins Installationsverzeichnis mit installiert. Der Rückgabewert beim Kopieren wird nicht berücksichtigt. Bei einem Fehler bricht die Installation nicht ab. Da der Installer diese Dateien nicht kennt, werden diese weder aktualisiert noch deinstalliert.

Eine weitere Möglichkeit Dateien, Icons, Registry-Einträge, usw. einer Installation hinzufügen ist der Weg über eine Transform-Datei. Hierfür kann über Admin-Tools diverser Hersteller (z.B. InstallShield, SuperOrca) das MSI-Paket geöffnet werden, beliebige Features, Komponenten, Dateien usw. hinzugefügt werden und eine Transform-Datei erstellt wird, welche bei der Installation übergeben wird. Folgender Befehl ist dafür notwendig:

```
msiexec /i myproduct.msi TRANSFORM=mytransform.mst[;mytransform2.mst]
```

Durch Trennung mit einem Strichpunkt, wie im angegebenen Befehl zu sehen, ist es möglich weitere Dateinamen anzugeben.

Dies ist der offizielle Weg, ein bestehendes MSI-Paket zu ergänzen. Vorteil ist, dass diese Ergänzungen dem Installer bekannt sind und er diese aktualisieren und deinstallieren kann.

ncpphone.cnf und ncpphone.cfg bei Installation importieren

Befinden sich während der Installation die Dateien `ncpphone.cnf` oder `ncpphone.cfg` im Installationsordner, werden diese automatisch migriert. So werden deren Einstellungen übernommen und stehen nach der Installation zur Verfügung.

Hinweis: Wenn Sie eine Konfigurationsdatei während der Client-Installation einspielen, die *Stateful Boot*-Konfigurationen der Firewall enthält, werden diese als aktiv angezeigt, sind aber auf Treiberebene noch nicht wirksam. Hierfür ist ein weiterer Neustart des Systems notwendig.

Beim Installieren eine Batch-Datei ausführen

Findet der Installer im Verzeichnis in dem sich auch das MSI-Paket oder der Installer als EXE-Datei befindet die Datei NcpInstall.bat, wird diese vom Installer am Ende der Installation ausgeführt. Der Rückgabewert wird nicht berücksichtigt. Tritt bei der Ausführung der Batch-Datei ein Fehler auf, so bricht die Installation nicht ab. Die Ausführungen sind dem Installer nicht bekannt und er kann diese auch nicht verwalten.

Testversion sofort starten

In manchen Projekten besteht der Wunsch, dass beim ersten Start des Monitors die Testversion ohne Abfrage „Testversion jetzt starten?“ sofort gestartet wird. Dies wird jetzt über den Kommandozeilenparameter „STARTTESTVERSION=1“ ermöglicht:

```
msiexec /i myproduct.msi STARTTESTVERSION=1
```

Nützliche Einstellungen für den Windows Installer

Silent Installation und Deinstallation

Der Windows Installer unterstützt eine eigene Silent Installation, welche z. B. über folgende Anzeigeoptionen angegeben werden kann.

```
msiexec /i myproduct.msi /qn
```

Protokollierung

Der Windows Installer gestattet eine sehr umfangreiche Protokollierung. Über die Art der Protokollierung kann konfiguriert werden. Zum Beispiel:

```
msiexec /i myproduct.msi /log "c:\temp\myinstall.log"
```

Beachten Sie, dass die Pfade und Namen der Log-Dateien beliebig sein können. Wird kein Pfad angegeben, wird die Log-Datei im Verzeichnis des Installers abgelegt.

Bei Deinstallation alle Dateien löschen

Wird der Client mit dem Assistenten deinstalliert, erfolgt die Abfrage, ob alle Dateien entfernt werden sollen, bevor dies erfolgt. Wird er statt dessen per Commandozeile deinstalliert, erfolgt keine Abfrage und die persönlichen Daten bleiben erhalten. In diesem Fall kann über die Commandozeile die Eigenschaft DELETEALL=1 gesetzt werden, damit alle Dateien entfernt werden. Zum Beispiel:

```
msiexec /x myproduct.msi DELETEALL=1
```

Update auf Version 13

Neue Verzeichnisstruktur bei neuem Client

Nach der Neuinstallation von Version 13 der Software des NCP Secure Entry Clients **sind nicht mehr alle Dateien** wie in früheren Versionen (bis Version 11) **im gleichen Verzeichnis** abgelegt, unter:

C:\Programme\NCP\SecureClient

In Version 13 werden die Dateien unter unterschiedlichen Pfaden gespeichert.

Unveränderliche Dateien werden ausschließlich abgelegt unter:

C:\Programme\NCP\SecureClient

Konfigurationsdateien bzw. **Dateien, die von der Software erzeugt werden**, werden gespeichert unter:

C:\ProgramData\NCP\SecureClient

Manuelles Update des Clients

Bei einem manuellen Update werden die mit der Vorgängerversion erzeugten Konfigurationsdateien automatisch in das Verzeichnis verschoben, welches der neuen Version entspricht.

Umbau der Datei-Struktur der Client-Software in Version 13.00

Beachten Sie dazu die weiter unten dargestellte [Verzeichnisstruktur](#)^[24].

Überprüfen der Verzeichnispfade

- Alle Konfigurationen, die Pfadangaben enthalten, müssen überprüft werden, ob sie von der Verzeichnisumstellung betroffen sind! Prüfen Sie alle Einträge, die ein Verzeichnis enthalten, und korrigieren Sie diese gegebenenfalls.
- Der bereits bei älteren Clients eingesetzte Platzhalter %INSTALLDIR% existiert weiterhin. Eine Ausnahme bildet dessen Einsatz bei der „Ermittlung der Pfade der Zertifikatskonfiguration“, siehe unten. (Vgl. dazu auch die [Ermittlungen der Verzeichnisse](#)^[24].)
- Zusätzlich können alle Windows-Umgebungsvariablen verwendet werden (z.B. %ProgramFiles%)
- Zusätzlich können alle Platzhalter der pathinfo.ini verwendet werden (siehe unten [Pathinfo.ini](#)^[24]).

Ermittlung der Pfade der Zertifikatskonfiguration

- Existiert die konfigurierte P12-Datei unter %CertDir%, wird nur noch der Dateiname angezeigt. Beim Speichern wird immer %CertDir% vorangestellt.
- Es wird daher empfohlen, alle Zertifikate in %CertDir% zu platzieren. Dadurch kann die Angabe des Verzeichnisnamens komplett entfallen. Es genügt den Dateinamen anzugeben.
- Wird eine Datei mit absolutem Pfad ausgewählt, der mit %CertDir% übereinstimmt, wird dieser durch %CertDir% ersetzt und nur der Dateiname angezeigt.

Verzeichnispfade der Client-Software in Version 13.00

Nach Standardisierungsmaßnahmen von Microsoft werden nur unveränderliche Dateien, wie Binaries oder Ressourcen, welche Ausführungsrechte benötigen, installiert werden unter

`C:\Programme`

Daher befinden sich in Client-Version 13.00 alle zur Ausführung nötigen Dateien der Secure Client-Software in dem Verzeichnis

`C:\Programme\NCP\SecureClient`

Dateien, die vom Benutzer modifiziert, ausgelesen oder eingespielt werden können (Konfigurations- und Log-Dateien, Logos und Statistiken) und solche, die während des Betriebs der Software dynamisch erzeugt werden, werden gespeichert unter

`C:\ProgrammData`

oder im Benutzerverzeichnis unter

`C:\Users`

Registry

Der frühere Registry-Eintrag `InstallDir` besteht immer noch und gibt nach wie vor das Verzeichnis unter `Program Files` zurück. Das ist auch der Registry-Eintrag über dem alle Module derzeit das Installationsverzeichnis ermitteln. Zusätzlich gibt es jetzt noch den Registry-Eintrag `InstallDirData`.

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\NCP engineering GmbH\NCP Secure Client]

`InstallDir` = `C:\\Program Files\\NCP\\SecureClient\\`

`InstallDirData` = `C:\\ProgramData\\NCP\\SecureClient\\`

Dateien mit Pfad „pathinfo.ini“





Bei der Installation der Client-Software wird die Datei `pathinfo.ini` durch das Setup automatisch geschrieben und unter `C:\Program Files\Company\Product` angelegt. Sie beinhaltet die verschiedenen Verzeichnisse der Client-Software. Die Verzeichnisse sind absolut und können direkt gelesen und verwendet werden.

[PATHS]		
<code>BaseInstallDir</code>	<code>C:\Program Files\NCP\SecureClient\</code>	Installationsverzeichnis für unveränderliche Programme
<code>BaseDataDir</code>	<code>C:\ProgramData\NCP\SecureClient\</code>	Ordner für Konfiguration
<code>CaCertDir</code>	<code>C:\ProgramData\NCP\SecureClient\cacerts</code>	CA-Zertifikate
<code>CertDir</code>	<code>C:\ProgramData\NCP\SecureClient\certs</code>	Benutzer-Zertifikate
<code>ArlDir</code>	<code>C:\ProgramData\NCP\SecureClient\arls</code>	Zertifikatssperlisten (ARL)
<code>CrlDir</code>	<code>C:\ProgramData\NCP\SecureClient\crls</code>	Zertifikatssperlisten (CRL)
<code>LogUserDir</code>	<code>C:\ProgramData\NCP\SecureClient\log_user</code>	Logdateien von Anwendungen und Diensten im System-Kontext
<code>LogDir</code>	<code>C:\ProgramData\NCP\SecureClient\log_system</code>	Logdateien von Anwendungen und Diensten im User-Kontext
<code>ConfigDir</code>	<code>C:\ProgramData\NCP\SecureClient\config</code>	Konfigurationsdateien

HotspotDir	C:\ProgramData\NCP\SecureClient\hotspot	Hotspot-Anmeldeskripte
HotspotCaCertDir	C:\ProgramData\NCP\SecureClient\hotspot\cacerts	Hotspot CA-Zertifikate

Client-Monitor

Der Client-Monitor enthält u. a. folgende Hauptmenüpunkte in der Menüleiste:

[Verbindung](#)  27
[Konfiguration](#)  51
[Ansicht](#)  122
[Hilfe](#)  125

Den Client-Monitor können Sie über das Icon auf Ihrem Desktop öffnen, sofern Sie bei der Installation den entsprechenden Haken für diese Option gesetzt haben. Alternativ können Sie den Client-Monitor über die Programmliste Ihres Windows-Startmenüs öffnen.

Verbindung [Menü]

Das Pulldown-Menü hat folgende Menüpunkte:

- [Verbinden / Trennen](#)  28
- [Home Zone](#)  29
- [Hotspot-Anmeldung](#)  29
- [Mobilfunkkarte](#)  31
- [Verbindungsinformationen](#)  32
- [Verfügbare Verbindungsmedien](#)  32
- [Budget Manager Statistik](#)  34
- [Budget Manager Historie](#)  34
- [Zertifikate \[Ansicht\]](#)  35
- [PIN eingeben](#)  47
- [PIN zurücksetzen](#)  47
- [PIN ändern](#)  48
- [Konfigurations-Sperren aufheben / wiederherstellen](#)  49
- [Beenden](#)  50

Verbinden / Trennen

Eine Verbindung kann nur aufgebaut werden, wenn ein Profil selektiert ist. Das selektierte Profil wird in der Monitoroberfläche unter der Menüleiste angezeigt.

Wenn Sie die Funktion "Verbinden" wählen, wird die Verbindung über das ausgewählte Profil manuell hergestellt.

Wenn Sie die Verbindung automatisch herstellen lassen wollen, so können Sie dies in den Profil-Einstellungen mit dem Parameter Verbindungsaufbau im Feld "Verbindungssteuerung" definieren.

Trennen

Mit der Funktion "Trennen" wird der Abbau der aktuell bestehenden Verbindung manuell durchgeführt.

Status-Darstellung des Produkt-Icons



Die Farben des Icons wechseln beim Verbindungsaufbau von rot nach grün.

Die Darstellung der Firewall als Linie unter „VPN“ zeigt, ob die Firewall aktiv ist und ob sich der Client in einem bekannten oder fremden Netz befindet. Befindet sich der Client in einem bekannten Netz (Friendly Net), wird die Linie gestrichelt dargestellt.

(Die Firewall wird auch in der grafischen [Monitor-](#)

[Oberfläche](#) dargestellt.)

Home Zone

Die Funktion der Home Zone ist unter der Rubrik [Funktionen](#)^[205] beschrieben.

Dieser Menüpunkt wird nur eingeblendet, wenn in den [Firewall-Einstellungen](#)^[57] eine Home Zone definiert wurde und die Firewall aktiv ist.

Eine gesetzte und nutzbare Home Zone wird in der grafischen Oberfläche des Clients als Symbol auf dem Desktop (Haus) hinter der aktiven Firewall angezeigt.

Der Netztyp *Home Zone* wurde dafür eingerichtet, einem Anwender im lokalen Netz seines Home Office die Möglichkeit zu geben, Geräte dieses privaten Netzes (z.B. Netzwerkdrucker) benutzen zu können.

Setzen der Home Zone: Mit dem Schalter *Setzen* wird die Firewall für den privaten Netzbereich geöffnet, um dort diverse Geräte nutzen zu können. Ändern sich die Netzwerkparameter der Home Zone zwischenzeitlich, etwa durch einen Standortwechsel des privaten Netzes, so wird durch erneutes Setzen der Home Zone die ältere Definition überschrieben und die aktuelle Einstellung in der Firewall verwendet. Eine Auswahl unter alternativen Home Zones ist nicht möglich.

Löschen der Home Zone: Mit dem Schalter *Löschen* wird die Funktion der Home Zone ausgeschaltet und der private Netzbereich wieder für den Zugriff gesperrt.

Hotspot-Anmeldung

Dieser Menüpunkt ist nur aktiv, wenn der WLAN-Manager des Clients nicht genutzt wird.

Befindet sich das Endgerät im Empfangsbereich eines öffentlichen WLANs, kann die Hotspot-Anmeldung vorgenommen werden. Der Client sucht dabei automatisch den Hotspot und öffnet die Website zur Anmeldung nur mit dem im Client integrierten Browser des jeweils aktuellen Windows Betriebssystems.






Mit der Integration des Browsers in den Client wurde sichergestellt, dass er nicht für andere Zwecke genutzt werden kann.

Nach erfolgter Hotspot-Anmeldung muss die VPN-Verbindung manuell durch Drücken des Verbinden-Buttons hergestellt werden.

Hinweis: Für die Nutzung des optionalen Features Hotspot-Erkennung muss die Microsoft Edge WebView2 Runtime auf der Plattform installiert sein (siehe <https://developer.microsoft.com/en-us/microsoft-edge/webview2/>). Ist das der Fall, muss der Plattform-Administrator dafür Sorge tragen, dass diese nach den Richtlinien der Plattform-Updates regelmäßig auf die neueste Version aktualisiert wird. Bei Nutzung der „Evergreen“-Variante der Runtime kann dies durch den Windows Update-Mechanismus erfolgen.

Mobilfunkkarte

Nachdem eine Mobilfunkkarte installiert wurde, wird eine Anzeige für das Mobilfunknetz im Monitor eingeblendet und das WLAN-Panel ausgeblendet. Siehe:

[Netzsuche](#)  31
[Mobilfunknetz aktivieren](#)  31
[SIM PIN eingeben](#)  31
[SIM PIN ändern](#)  32
[PUK-Eingabe](#)  32

Netzsuche

Die installierte Mobilfunkkarte sucht nach dem Start des Monitors automatisch nach einem Funknetz und zeigt es mit der entsprechenden Feldstärke an, sobald es gefunden wurde. Durch Anwahl des Menüpunkts oder des Buttons für "Netzsuche" kann eine erneute Netzsuche ausgelöst werden.

Bei zu geringer Feldstärke wechselt die Karte automatisch die Datenübertragungstechnik, wobei die Verbindung bestehen bleibt. Erhöht sich die Feldstärke wieder, schaltet die Karte automatisch wieder zurück.

Wurde eine Netzsuche durchgeführt, wird ein Fenster mit dem "Heimatnetz" eingeblendet.

Nur im Ausland und wenn Roaming aktiviert ist, werden entsprechend mehr alternative Netze zur Auswahl angezeigt.

Wird die erneute Netzsuche nach jedem Aufruf des Monitors nicht gewünscht, so muss die standardmäßig aktive Funktion über den Check-Button ausgeschaltet werden.

Mobilfunknetz aktivieren

Die Datenübertragungstechnik kann auch manuell gewechselt werden. Dazu wird mit der Maus der Text mit der gewünschten Übertragungstechnik angeklickt oder dieser Menüpunkt gewählt. Bei einem manuellen Wechsel des Mediums wird die Verbindung zunächst abgebaut. Die Verbindung wird dann wieder automatisch aufgebaut, wenn "automatischer Verbindungsaufbau" in den Profileinstellungen konfiguriert wurde.

SIM PIN eingeben

Der Dialog zur Eingabe der SIM PIN erscheint automatisch bei einem Verbindungsaufbau.

Über diesen Menüpunkt kann die SIM PIN auch vor einem Verbindungsaufbau eingegeben werden.

SIM PIN in Konfiguration speichern

Wird diese Funktion genutzt, so wird die SIM PIN für das aktuell aktive Mobilfunk-Profil übernommen und muss nicht mehr eigens eingegeben werden.

In der Standard-Einstellung des Entry Clients ist diese Funktion nicht sichtbar. Sie wird dann für den Benutzer sichtbar und konfigurierbar, wenn ihm in den Parameter-Sperren unter "Mobilfunknetz" die Berechtigung dazu erteilt wurde, d. h. "Benutzer darf SIM PIN in Konfiguration speichern" aktiviert wurde.

SIM PIN ändern

Die Änderung der SIM PIN bewirkt deren Änderung auf der SIM-Karte. Diese Änderung kann nur vorgenommen werden, wenn die bisherige SIM PIN korrekt eingegeben wurde.

Die entsprechende Änderung der SIM PIN in der Konfiguration des Mobilfunk-Profiles muss manuell erfolgen, entweder über das Menü "Konfiguration / Mobilfunk-Einstellungen" oder wenn die SIM PIN beim nächsten Verbindungsaufbau abgefragt wird.

PUK-Eingabe

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

Verbindungsinformationen

Die Verbindungsinformationen unter „Allgemein“ zeigen:

- den Namen des aktuell gewählten Profils
- statistische Werte (z.B. Zeit online, Timeout-Wert)
- IP-Adressen (VPN IP-Adresse, DNS-Server, VPN-Endpunkt)
- Security-Modus
- welche Security-Schlüssel verwendet werden

Die Verbindungsinformationen unter „Quality of Service“⁸¹ zeigen:

- die dem aktuell gewählten Profil zur Verfügung stehenden QoS-Gruppen, die nach Bedarf ein- oder ausgeschaltet werden können.
- eine grafische Darstellung der genutzten Bandbreite

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 automatisch, welche Medien aktuell zur Verfügung stehen und stellt sie mit gelber Signallampe dar. Das jeweils vom Client für eine Verbindung ausgewählte und aktivierte Medium wird mit einem grünen Haken 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-GUI minimiert ist. Hinter der genutzten Medienart wird der Fehler in roter Schrift bezeichnet. Durch Löschen wird diese Schrift entfernt.

Das selbständige Aufblenden des Fensters mit den Verbindungsmedien kann bei einem häufigen Medienwechsel und neuem Verbindungsaufbau lästig sein, z.B. wenn als Art des Verbindungsaufbaus der Modus "immer" gewählt wurde. Schalten Sie in diesem Fall den Automatismus ab, indem Sie den Haken aus der Checkbox entfernen.

Zur Konfiguration der automatischen Medienerkennung beachten Sie die Parameterbeschreibung zu den Profil-Einstellungen (Grundeinstellungen) des Clients.

Budget Manager Statistik

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.

Budget Manager Historie

Die Historie zeigt zum jeweiligen Jahresmonat - entsprechend Ihren Einstellungen, die Sie in den Verbindungsoptionen für das Budget Ihrer eingesetzten Verbindungsmedien vorgenommen haben - die tatsächliche Verbindungsdauer und das tatsächliche Verbindungsvolumen.

Mit Mausklick auf den Anzeigen-Button wird eine grafische Ansicht gezeigt.

Zertifikate [Ansicht]

Zertifikate (Certificates) werden von einer CA (Certification Authority) mittels PKI-Manager (Software) ausgestellt und auf eine Smart Card (Chipkarte) gebrannt oder als Soft-Zertifikat (auch digitales Zertifikat) als Datei eingespielt. Zertifikate mit digitalen Signaturen, können ähnlich wie ein digitaler Personalausweis genutzt werden.

Es können Zertifikate eingesetzt werden, die einen privaten Schlüssel bis zu einer Länge von 4096 Bits besitzen.

Wird ein Zertifikat genutzt, so wird (ggf. nach dem Tunnelaufbau) zwischen Client und VPN-Gateway nach der CHAP-Authentisierung (User ID und Passwort) die Erweiterte Authentisierung (Extended Authentication) mittels der bei Client und Gateway hinterlegten Zertifikate durchgeführt. Dabei erfolgt die "Erweiterte Authentisierung" und die Verhandlung des Session Keys für das vorher ausgewählte Verschlüsselungsverfahren nach dem SSL-Protokoll.

Beachten Sie für die [Erweiterte Authentisierung](#)^[190] die Konfigurationsmöglichkeiten unter [Identität](#)^[188].

Aussteller-Zertifikat anzeigen

Das Aussteller-Zertifikat kann angezeigt werden, sofern es im Benutzer-Zertifikat enthalten ist und die PIN für das Benutzer-Zertifikat eingegeben wurde.

Wenn Sie sich das Aussteller-Zertifikat anzeigen lassen, können Sie sehen welche Merkmale zur Erstellung des Zertifikats genutzt wurden, z. B. die eindeutige E-Mail-Adresse.

Allgemein

In der allgemeinen Anzeige finden Sie die Angaben zu Benutzer und Aussteller der Zertifikats (die bei einem Aussteller-Zertifikat identisch sind), sowie die Seriennummer, die Angaben zur Gültigkeitsdauer und den Fingerprint.

Aussteller (CA): Benutzer und Aussteller eines Aussteller-Zertifikates sind für gewöhnlich identisch (selfsigned certificate). Der Aussteller des Aussteller-Zertifikats muss mit dem Aussteller des Benutzer-Zertifikats identisch sein (siehe: Benutzer-Zertifikat anzeigen).

Seriennummer: Nach der Seriennummer werden die Zertifikate mit den in der Revocation List der Certification Authority gehaltenen verglichen.

Gültigkeitsdauer: Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit dem Erlöschen der Gültigkeit des Aussteller-Zertifikats erlischt automatisch die Gültigkeit eines vom gleichen Aussteller ausgestellten Benutzer-Zertifikates.

Fingerprint: = Hash-Wert. Der mit dem Private Key der CA verschlüsselte Hash-Wert ist die Signatur des Zertifikats.

Erweiterungen

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zertifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den Secure Client und den Secure Server sind folgende Erweiterungen von Bedeutung:

- KeyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- CDP (Certificate Distribution Point)

KeyUsage

Ist in einem eingehenden Zertifikat die Erweiterung KeyUsage enthalten, so wird diese überprüft. Folgende KeyUsage-Bits werden akzeptiert. Ist eines dieser Bits nicht gesetzt, wird die Verbindung abgebaut.

- Digital Signature
- Key Encipherment (Schlüsseltransport, Schlüsselverwaltung)
- Key Agreement (Schlüsselaustauschverfahren)

extendedKeyUsage

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der Client, ob der definierte erweiterte Verwendungszweck die "SSL-Server-Authentisierung" ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck "SSL-Server-Authentisierung" beinhalten muss.

subjectKeyIdentifier / authorityKeyIdentifier

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann kein CA-Zertifikat gefunden werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades. Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.

CDP (Certificate Distribution Point)

Im Certificate Distribution Point ist die URL für den Download einer CRL hinterlegt. Ist im Zertifikat die Erweiterung CDP enthalten, wird nach dem Verbindungsaufbau die CRL über die angegebene URL heruntergeladen und überprüft. Wird dabei festgestellt, dass das Zertifikat ungültig ist, wird die Verbindung abgebaut. Die CRL wird dabei unter dem Common-Name der CA im Installationsverzeichnis unter "\crls" gespeichert.

Benutzer-Zertifikat anzeigen

Nachdem die PIN eingegeben wurde, kann das Benutzer-Zertifikat eingesehen werden.

Wenn Sie sich Ihr Benutzer-Zertifikat anzeigen lassen, können Sie sehen welche Merkmale zur Erstellung des Zertifikats genutzt wurden, z.B. die eindeutige E-Mail-Adresse.

Allgemein

In der allgemeinen Anzeige finden Sie die Angaben zu Benutzer und Aussteller der Zertifikats (die bei einem Aussteller-Zertifikat identisch sind), sowie die Seriennummer, die Angaben zur Gültigkeitsdauer und den Fingerprint.

Aussteller (CA): Der Aussteller Ihres Benutzer-Zertifikates muss mit dem Aussteller des Aussteller-Zertifikates identisch sein. (siehe: Aussteller-Zertifikat anzeigen).

Seriennummer: Nach der Seriennummer werden die Zertifikate mit den in der Revocation List der Certification Authority gehaltenen verglichen.

Gültigkeitsdauer: Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit Erlöschen der Gültigkeit geht auch die Funktion des Zertifikats verloren.

Fingerprint: = Hash-Wert. Der mit dem Private Key der CA verschlüsselte Hash-Wert ist die Signatur des Zertifikats.

Erweiterungen

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zertifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den Secure Client und den Secure Server sind folgende Erweiterungen von Bedeutung:

- KeyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- CDP (Certificate Distribution Point)

KeyUsage

Ist in einen eingehenden Zertifikat die Erweiterung KeyUsage enthalten, so wird diese überprüft. Folgende KeyUsage-Bits werden akzeptiert:

- Digital Signature
- Key Encipherment (Schlüsseltransport, Schlüsselverwaltung)
- Key Agreement (Schlüsselaustaschverfahren)

Ist eines des Bits nicht gesetzt, wird die Verbindung abgebaut.

extendedKeyUsage

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der Client, ob der definierte erweiterte Verwendungszweck die "SSL-Server-Authentisierung" ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck "SSL-Server-Authentisierung" beinhalten muss.

subjectKeyIdentifier / authorityKeyIdentifier

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann kein CA-Zertifikat gefunden werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades. Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.

CDP (Certificate Distribution Point)

Im Certificate Distribution Point ist die URL für den Download einer CRL hinterlegt. Ist im Zertifikat die Erweiterung CDP enthalten, wird nach dem Verbindungsaufbau die CRL über die angegebene URL heruntergeladen und überprüft. Wird dabei festgestellt, dass das Zertifikat ungültig ist, wird die Verbindung abgebaut. Die CRL wird dabei unter dem Common-Name der CA im Installationsverzeichnis unter "\crls" gespeichert.

Eingehendes Zertifikat anzeigen

Anzeige des Zertifikats, das bei der SSL-Verhandlung von der Gegenstelle (Secure Server) übermittelt wird. Sie können z.B. sehen, ob Sie den hier gezeigten Aussteller in der Liste Ihrer CA-Zertifikate (siehe unten) aufgenommen haben.

Ist das eingehende Benutzer-Zertifikat einer der CAs aus der Liste "CA-Zertifikate anzeigen" nicht bekannt, oder passt es nicht zu dem Root-Zertifikat, das in der p12-Datei enthalten ist, kommt die Verbindung nicht zustande.

Allgemein

In der allgemeinen Anzeige finden Sie die Angaben zu Benutzer und Aussteller der Zertifikats (die bei einem Aussteller-Zertifikat identisch sind), sowie die Seriennummer, die Angaben zur Gültigkeitsdauer und den Fingerprint.

Erweiterungen

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zertifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den Secure Client und den Secure Server sind folgende Erweiterungen von Bedeutung:

- KeyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- CDP (Certificate Distribution Point)

KeyUsage

Ist in einem eingehenden Zertifikat die Erweiterung KeyUsage enthalten, so wird diese überprüft. Folgende KeyUsage-Bits werden akzeptiert:

- Digital Signature
- Key Encipherment (Schlüsseltransport, Schlüsselverwaltung)
- Key Agreement (Schlüsselaustaschverfahren)

Ist eines des Bits nicht gesetzt, wird die Verbindung abgebaut.

extendedKeyUsage

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der Client, ob der definierte erweiterte Verwendungszweck die "SSL-Server-Authentisierung" ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung

extendedKeyUsage vorhanden ist, den Verwendungszweck "SSL-Server-Authentisierung" beinhalten muss.

subjectKeyIdentifier / authorityKeyIdentifier

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann kein CA-Zertifikat gefunden werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades. Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.

CDP (Certificate Distribution Point)

Im Certificate Distribution Point ist die URL für den Download einer CRL hinterlegt. Ist im Zertifikat die Erweiterung CDP enthalten, wird nach dem Verbindungsaufbau die CRL über die angegebene URL heruntergeladen und überprüft. Wird dabei festgestellt, dass das Zertifikat ungültig ist, wird die Verbindung abgebaut. Die CRL wird dabei unter dem Common-Name der CA im Installationsverzeichnis unter "\crls" gespeichert.

HTTP Proxy für CRL Download

In der Datei NCPPKI.CONF im Installationsverzeichnis kann in der Gruppe "HttpProxy" ein Proxy für den CRL Download über HTTP konfiguriert werden:

```
[HttpProxy]
ProxyHost = xxx.xxx.xxx.xxx
#IP Adresse des Proxy Server für CRL Download über HTTP
ProxyPort = 80
#Port des Proxy Server für CRL Download über HTTP
ProxyUser = xyz
#Benutzername des Proxy Server für CRL Download über HTTP
ProxyPw = xxxx
#Passwort des Proxy Server für CRL Download über HTTP
```

Auswertung von CRLs und ARLs

Der Secure Client kann auch Revocation-Lists auswerten. Folgende Listen werden unterstützt:

- Certificate Revocation List (CRL)
- Authority Revocation List (ARL)

Die CRLs bzw. ARLs müssen in die entsprechenden Unterverzeichnisse des Installationsverzeichnisses nach "\CRL" bzw. "\ARL" kopiert werden.

CA-Zertifikate anzeigen

Mit der Client Software werden mehrere Aussteller-Zertifikate unterstützt (Multi CA-Unterstützung). Dazu müssen die Aussteller-Zertifikate im Installations-Verzeichnis unter "cacerts" gesammelt werden. Im Monitor des Clients wird die Liste der eingespielten CA-Zertifikate unter diesem Menüpunkt angezeigt.

Wird das Zertifikat einer Gegenstelle empfangen, so ermittelt der Client den Aussteller und sucht diesen anschließend auf den Aussteller-Zertifikaten.

Wird kein passendes Aussteller-Zertifikat gefunden, kommt die Verbindung nicht zustande (Kein Root-Zertifikat gefunden!).

Allgemein

In der allgemeinen Anzeige finden Sie die Angaben zu Benutzer und Aussteller des Zertifikats (die bei einem Aussteller-Zertifikat identisch sind), sowie die Seriennummer, die Angaben zur Gültigkeitsdauer und den Fingerprint.

Erweiterungen

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zertifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den Secure Client und den Secure Server sind folgende Erweiterungen von Bedeutung:

- KeyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- CDP (Certificate Distribution Point)

KeyUsage

Ist in einem eingehenden Zertifikat die Erweiterung KeyUsage enthalten, so wird diese überprüft. Folgende KeyUsage-Bits werden akzeptiert:

- Digital Signature
- Key Encipherment (Schlüsseltransport, Schlüsselverwaltung)
- Key Agreement (Schlüsselaustaschverfahren)

Ist eines der Bits nicht gesetzt, wird die Verbindung abgebaut.

extendedKeyUsage

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der Client, ob der definierte erweiterte Verwendungszweck die "SSL-Server-Authentisierung" ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung `extendedKeyUsage` vorhanden ist, den Verwendungszweck "SSL-Server-Authentisierung" beinhalten muss.

subjectKeyIdentifier / authorityKeyIdentifier

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann kein CA-Zertifikat gefunden werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfad. Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.

CDP (Certificate Distribution Point)

Im Certificate Distribution Point ist die URL für den Download einer CRL hinterlegt. Ist im Zertifikat die Erweiterung CDP enthalten, wird nach dem Verbindungsaufbau die CRL über die angegebene URL heruntergeladen und überprüft. Wird dabei festgestellt, dass das Zertifikat ungültig ist, wird die Verbindung abgebaut. Die CRL wird dabei unter dem Common-Name der CA im Installationsverzeichnis unter "`\crls`" gespeichert.

Computer-Zertifikat (Ansicht)

Wenn Sie sich das Computer-Zertifikat anzeigen lassen, können Sie sehen welche Merkmale zur Erstellung des Zertifikats genutzt wurden.

Allgemein

In der allgemeinen Anzeige finden Sie die Angaben zu Benutzer und Aussteller der Zertifikats (die bei einem Aussteller-Zertifikat identisch sind), sowie die Seriennummer, die Angaben zur Gültigkeitsdauer und den Fingerprint.

Austeller (CA): Der Aussteller des Computer-Zertifikates muss mit dem Aussteller des Aussteller-Zertifikates identisch sein. (Siehe: Aussteller-Zertifikat anzeigen).

Seriennummer: Nach der Seriennummer werden die Zertifikate mit den in der Revocation List der Certification Authority gehaltenen verglichen.

Gültigkeitsdauer: Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Computer-Zertifikats. Mit Erlöschen der Gültigkeit geht auch die Funktion des Zertifikats verloren.

Fingerprint: = Hash-Wert. Der mit dem Private Key der CA verschlüsselte Hash-Wert ist die Signatur des Zertifikats.

Erweiterungen

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zertifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den Secure Client und den Secure Server sind folgende Erweiterungen von Bedeutung:

- KeyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- CDP (Certificate Distribution Point)

KeyUsage

Ist in einen eingehenden Zertifikat die Erweiterung KeyUsage enthalten, so wird diese überprüft. Folgende KeyUsage-Bits werden akzeptiert:

- Digital Signature
- Key Encipherment (Schlüsseltransport, Schlüsselverwaltung)
- Key Agreement (Schlüsselaustaschverfahren)

Ist eines des Bits nicht gesetzt, wird die Verbindung abgebaut.

extendedKeyUsage

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der Secure Client, ob der definierte erweiterte Verwendungszweck die "SSL-Server-Authentisierung" ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck "SSL-Server-Authentisierung" beinhalten muss.

subjectKeyIdentifier / authorityKeyIdentifier

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann kein CA-Zertifikat gefunden werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades. Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.

CDP (Certificate Distribution Point)

Im Certificate Distribution Point ist die URL für den Download einer CRL hinterlegt. Ist im Zertifikat die Erweiterung CDP enthalten, wird nach dem Verbindungsaufbau die CRL über die angegebene URL heruntergeladen und überprüft. Wird dabei festgestellt, dass das Zertifikat ungültig ist, wird die Verbindung abgebaut. Die CRL wird dabei unter dem Common-Name der CA im Installationsverzeichnis unter "\crls" gespeichert.

PIN eingeben

Die PIN-Eingabe kann bereits vor einem Verbindungsaufbau erfolgen, nachdem der Monitor gestartet wurde. Wird zu einem späteren Zeitpunkt eine Verbindung aufgebaut, die ein Zertifikat erfordert, so kann dann die PIN-Eingabe unterbleiben - es sei denn, die Konfiguration zum Zertifikat verlangt dies.

Haben Sie den Menüpunkt "Verbindung / PIN eingeben" gewählt, kann in das geöffnete Eingabefeld die PIN (mindestens 4-stellig) eingegeben werden und mit "OK" bestätigt werden.

Sofern die PIN noch nicht vor einem Verbindungsaufbau eingegeben wurde, erscheint der Dialog zur PIN-Eingabe spätestens wenn die erste Verbindung zu einem Ziel hergestellt werden soll, das die Verwendung eines Zertifikats erfordert. Nachfolgend kann bei einem wiederholten manuellen Verbindungsaufbau die PIN-Eingabe unterbleiben, wenn dies so konfiguriert wurde.

Wurde die PIN korrekt eingegeben, so wird dies in der Monitoroberfläche mit einem grünen PIN-Symbol dargestellt.

Erst nach korrekter PIN-Eingabe kann der Verbindungsaufbau erfolgen.

Sicherung der PIN-Benutzung

Ist in der Zertifikatskonfiguration die Funktion "PIN-Abfrage bei jedem Verbindungsaufbau" aktiviert, kann über den Monitor-Menüpunkt "PIN eingeben" die PIN nicht mehr eingegeben werden. Der Menüpunkt "PIN eingeben" wird damit automatisch inaktiv geschaltet. Damit ist sichergestellt, dass erst unmittelbar vor dem Verbindungsaufbau die PIN abgefragt wird und eingegeben werden muss.

Bei Aktivierung dieser Funktion ist damit ausgeschlossen, dass ein unbefugter Benutzer bei bereits eingegebener PIN eine unerwünschte Verbindung aufbaut.

Ebenso wird für die Aktivschaltung der Funktion "PIN ändern" nicht mehr die bereits in anderem Funktionszusammenhang abgeforderte PIN verwendet - wie beim Verbindungsaufbau oder im Verbindungs-Menü "PIN eingeben". Sondern der Menüpunkt "PIN ändern" ist immer selektierbar, und die neue PIN wird unmittelbar nach der Änderung sogleich wieder zurückgesetzt.

Somit ist sichergestellt, dass bei Konfiguration der "PIN-Abfrage bei jedem Verbindungsaufbau" an einem unbeaufsichtigten Client-Monitor zu keinem Zeitpunkt eine bereits eingegebene PIN von einem unbefugten Benutzer für einen Verbindungsaufbau genutzt werden kann.

Die Richtlinien zur PIN-Eingabe können im Hauptmenü unter "Konfiguration / Zertifikate" festgelegt werden. Diese Richtlinien müssen auch befolgt werden, wenn die PIN geändert wird.

PIN zurücksetzen

Dieser Menüpunkt ist nur aktiv, wenn die PIN bereits richtig eingegeben wurde, d. h. das Zertifikat für die aufzubauende Verbindung genutzt werden soll.

Wird die PIN zurückgesetzt, kann dieses Zertifikat für einen Verbindungsaufbau nicht mehr genutzt werden, bis die dazugehörige PIN wieder richtig eingegeben wurde.

PIN ändern

Unter diesem Menüpunkt kann die PIN für eine Smart Card/ einen Token oder ein Soft-Zertifikat geändert werden, wenn vorher die richtige PIN eingegeben wurde.

Anschließend geben Sie Ihre neue PIN ein und bestätigen diese durch Wiederholung im letzten Eingabefeld. Mit Klick auf "OK" haben Sie Ihre PIN geändert.

Die einzuhaltenden PIN-Richtlinien werden unter den Eingabefeldern eingeblendet. Sie können im Hauptmenü unter PIN-Richtlinien eingestellt werden.

Sperre aufheben

Dieser Menüpunkt erscheint nur, wenn Konfigurations-Sperren durch den Administrator vorgegeben wurden.

Diverse Parameterfelder und Menüpunkte, die für Ihren Anschluss nicht von Bedeutung sind, können vom Systemadministrator ausgeblendet werden. Sie sind dann in den Profil-Einstellungen bzw. im Menü nicht mehr sichtbar.

Um die Parameter wieder einzublenden, wählen Sie diesen Menüpunkt. Nach Eingabe von User ID und Passwort des Administrators werden die Sperren aufgehoben.

Danach erscheint der Menüpunkt Konfigurations-Sperre wiederherstellen.

Beenden

Wurde die Verbindung bereits getrennt, beendet ein Klick auf diesen Menüpunkt oder der Schließen-Button den Monitor. Besteht noch eine Verbindung, kann nach Klick auf diesen Menüpunkt oder den Schließen-Button der Monitor ebenfalls beendet werden. Beachten Sie jedoch unbedingt, dass die Verbindung dabei nicht automatisch getrennt wird. Soll die möglicherweise kostenpflichtige Verbindung bestehen bleiben, obwohl der Monitor beendet wird, so wird dazu ausdrücklich eine Bestätigung verlangt.

Klicken Sie in diesem Bestätigungsfenster auf "Nein", so haben Sie auf Ihrer Desktop-Oberfläche kein Icon und keinen Hinweis mehr darauf, dass noch eine Verbindung aktiv ist und Gebühren anfallen können! In diesem Fall müssen Sie den Monitor erneut starten, um eine bestehende Verbindung korrekt zu beenden!

Konfiguration [Menü]

Das Pulldown-Menü hat folgende Menüpunkte:

Profile [Konfiguration]	51
Firewall [Konfiguration]	55
VPN-Bypass	79
Quality of Service (Konfiguration)	81
WLAN [Konfiguration]	87
Zertifikate [Konfiguration]	98
Verbindungsoptionen [Konfiguration]	105
EAP-Optionen [Konfiguration]	119
Logon-Optionen	111
Konfigurationssperren	99
Proxy für VPN Path Finder	118
Profil-Sicherung	121

Unter diesem Menüpunkt können sämtliche Einstellungen für die Arbeit mit dem Client vorgenommen werden. Dies betrifft das Anlegen der Profile, die IPsec-Konfiguration und die Wahl der Verbindungsart.

Darüber hinaus kann eigens konfiguriert werden, wie Zertifikate genutzt werden sollen und wie der Budget-Manager (unter "Link-Optionen") soll.

Profile [Konfiguration]

Profile am Client anlegen

Bei einer Erstinstallation der Client Software ist noch kein Profil vorhanden. In diesem Fall wird automatisch ein Konfigurations-Assistent eingeblendet, der Ihnen hilft, Konfigurationen anzulegen. Damit wird zugleich das erste Profil der IPsec Client Software angelegt.

Hinzufügen / Import

Nach Klick auf diesen Button wird ein Assistent gestartet, mit dessen Hilfe wahlweise ein neues Profil angelegt oder importiert werden kann.


Für den Import unterstützt der Client verschiedene Dateitypen (*.ini).

Die gewünschten Profil-Einstellungen können von der jeweiligen Gegenstelle erstellt oder manuell editiert werden. Im Installationsverzeichnis befinden sich dazu die Beispieldateien IMPORT_D.TXT und IMPORT_E.TXT. In den Beispieldateien sind auch Syntax und Parameterwerte beschrieben.

Export

Nach Klick auf diesen Button wird ein Assistent gestartet, mit dessen Hilfe das aktuelle selektierte Profil exportiert werden kann.

Siehe auch:


[Profil-Einstellungen](#)  53

[Profil-Gruppen](#)  54

Profil-Einstellungen

[Grundeinstellungen \[Profile\]](#)  136

[Netzeinwahl](#)  144

[Mobilfunknetz \[Profile\]](#)  149

[HTTP-Anmeldung \[Profile\]](#)  151

[Verbindungssteuerung \[Profile\]](#)  153

[IPsec-Einstellungen](#)  167

[Erweiterte IPsec-Optionen](#)  185

[Identität](#)  188

[IPsec-Adresszuweisung](#)  193

[Split Tunneling](#)  195

[Zertifikats-Überprüfung](#)  197

[Link Firewall](#)  203

Profil-Gruppen

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

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.

Mit "Hinzufügen" wird eine neue Gruppe in die linke Spalte eingefügt, der Sie einen eigenen Namen geben können.

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

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.

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.

Firewall [Konfiguration]

Alle Firewall-Mechanismen sind optimiert für Remote Access-Anwendungen und werden bereits beim Start des Rechners aktiviert.

Ist die Firewall des Clients aktiv, so wird deren Status an das Windows Security-Center bzw. das Wartungs-Center gemeldet und kann dort eingesehen werden.

D. h. im Gegensatz zu VPN-Lösungen mit eigenständiger Firewall ist der Telearbeitsplatz bereits vor der eigentlichen VPN-Nutzung gegen Angriffe geschützt.

Die Firewall bietet auch im Fall einer Deaktivierung der Client-Software vollen Schutz des Endgerätes.

Beachten Sie, dass die Firewall-Einstellungen für alle Profile gültig sind.

Eigenschaften der Firewall

Die Firewall arbeitet nach dem Prinzip der Paketfilterung in Verbindung mit Stateful Packet Inspection (SPI). Die Firewall prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis des konfigurierten Regelwerks, ob ein Datenpaket weitergeleitet oder verworfen wird.

Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen wird der unbefugte Zugriff auf Daten und Ressourcen im zentralen Datennetz verhindert. Zum anderen wird mittels Stateful Inspection der jeweilige Status bestehender Verbindungen überwacht. Die Firewall kann darüber hinaus erkennen, ob eine Verbindung "Tochterverbindungen" geöffnet hat - wie beispielsweise bei FTP oder Netmeeting - deren Pakete ebenfalls weitergeleitet werden müssen. Wird eine Regel für eine ausgehende Verbindung definiert, die einen Zugriff erlaubt, so gilt die Regel automatisch für entsprechende Rückpakete. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf.

Die Firewall-Regeln können dynamisch konfiguriert werden, d. h. ein Anhalten der Software oder ein Neustart des Systems ist nicht nötig.

Die Firewall-Einstellungen im Konfigurationsmenü des Client-Monitors gestatten eine genauere Spezifikation von Firewall-Filterregeln. Sie wirken global.

Die symbolische Darstellung der Firewall

Je nach Firewall-Konfiguration stellt sich das Firewall-Symbol in der GUI und in der Taskleiste anders dar:

Befindet sich der Rechner des Benutzers beim Verbindungsaufbau in einem bekannten Netz d.h. friendly Network, so wird das Schutzschild des Firewall-Symbols, mit einem zur Gegenstelle gerichteten grünen Rand dargestellt:



(Die Firewall wird auch mit dem [Produkt-Icon](#)²⁸⁾ dargestellt.)

D. h. unabhängig vom aktuell gewählten Profil werden immer zuerst die Regeln der Firewall-Einstellungen abgearbeitet, bevor die Regeln der Link-Firewall angewendet werden.

Eine Kombination der globalen und link-bezogenen Firewall kann in bestimmten Szenarien durchaus sinnvoll sein. Im Allgemeinen sollten jedoch nahezu alle Anforderungen über die globalen Einstellungsmöglichkeiten abzudecken sein.

Bitte beachten Sie, dass die link-bezogenen Firewall-Einstellungen bei Aktivierung Vorrang vor den globalen haben.

Ist z. B. die Link-Firewall auf "immer" und "Ausschließlich Kommunikation im Tunnel zulassen" eingestellt, kann trotz evtl. anders lautender Regeln der globalen Konfiguration nur ein Tunnel aufgebaut und darüber kommuniziert werden. Jeder andere Datenverkehr wird von der Link-Firewall verworfen.

Konfiguration der Firewall-Einstellungen

Die Filterregeln der Firewall können sowohl anwendungsbezogen als auch (zusätzlich) adressorientiert, bezüglich bekannter / unbekannter Netze, definiert werden.

Siehe auch:

[Grundeinstellungen mit Standard-Konfiguration](#)  57

[Regel-Tabelle](#)  60

[Bekannte Netze](#)  65

[Optionen](#)  72

[Protokollierung](#)  77

Grundeinstellungen mit Standard-Konfiguration

Standard-Konfiguration in den Grundeinstellungen

Bei einem Update der Client-Software bleiben die bisherigen Firewall-Einstellungen erhalten.

Bei einer Neuinstallation der Client-Software ist nach dem ersten Start des Client-Monitors die Firewall noch nicht aktiv.

Firewall aktivieren

Die Firewall wird aktiviert, indem über das Konfigurations-Menü im Monitor des Clients der entsprechende Menüpunkt "Firewall" selektiert wird und in der Regel-Übersicht der Grundeinstellungen die Funktion "Firewall aktivieren" angeklickt wird.

Sobald die Firewall aktiv ist, wird in der Oberfläche des Client-Monitors ein Symbol (Schutzschild) dafür angezeigt und jede IP-Kommunikation ins Netzwerk (LAN, Drucker, etc.) blockiert, gleich ob IPv4 oder IPv6, ob eingehend oder ausgehend. Dies erfolgt auch dann, wenn noch keine explizite Firewall-Regel erstellt oder aktiviert wurde.

Regeln für Testverbindung verwenden

Wurde bei der Installation der Software die Möglichkeit genutzt automatisch eine Testverbindung anzulegen (Testverbindung IPsec IKEv1 oder Testverbindung IPsec IKEv2), so kann bei aktivierter Firewall dann eine Verbindung aufgebaut werden, wenn in den Grundeinstellungen der Firewall unter den vordefinierten Firewall-Regel die "NCP-Regeln für Testverbindung" eingesetzt werden.

Auf diese Weise kann die Funktion der Firewall schnell ausprobiert werden.

Selektieren und Editieren einer Regel

Im Folgenden wird das Editieren am Beispiel vordefinierter Regeln beschrieben.

- Selektieren Sie die gewünschte Regel.
- Klicken Sie "Hinzufügen".
- Die Regeln werden in die Firewall übernommen, sobald die Firewall-Einstellungen mit OK geschlossen werden. Der "Übernehmen"-Button speichert die Regeln, ohne das Firewall-Fenster zu schließen.

Sind alle Regeln für die Testverbindung aktiv, und erscheint das Firewall-Symbol (Schutzschild) nach Schließen der Firewall-Einstellungen in der Monitor-Oberfläche, so kann mit dem Profil für die Testverbindung eine Verbindung zum VPN Gateway von NCP hergestellt werden.

Zusätzliche Regeln gestatten den definierten Tunnelaufbau

Mit den vordefinierten Regeln für die Testverbindung wurden folgende Einzelregeln in die Firewall eingetragen:

- NCP-DNS
- NCP Web-Browser
- NCP-FTP
- NCP Ping (IPv4)

Folgende Funktion ist in der Standard-Einstellung immer bereits aktiv:

- IPsec-Protokoll (ESP, UDP 500) und VPN Path Finder (TCP 443) zulassen

Damit kann der VPN-Tunnelaufbau global zugelassen werden.

Folgende für den Tunnelaufbau benötigten Protokolle und Ports werden per automatisch generierter Filter für IPsec freigegeben:

- IP-Protokoll 50 (ESP)
- UDP 4500 (NAT-T)
- UDP 67 (DHCPs)
- UDP 68 (DHCPc)
- TCP 443 (VPN Path Finder, falls konfiguriert)

Die Aktivierung dieser Funktion erspart die Einrichtung von Einzelregeln für die jeweilige VPN-Variante.

Bitte beachten Sie, dass dadurch lediglich der Tunnelaufbau ermöglicht wird. Existieren keine weiteren Regeln für VPN-Netze, die eine Kommunikation im Tunnel zulassen, kann über den VPN-Tunnel kein Datenaustausch erfolgen.

Weitere vordefinierte Firewall-Regeln können nach Bedarf ausgewählt und mit dem Button für "Hinzufügen" in die Liste der Firewall-Regeln aufgenommen und editiert werden.

Regel für DNS-Abfrage

In den Profil-Einstellungen für die Testverbindung, die bei der Installation automatisch generiert wurde, finden Sie als Tunnel-Endpunkt den DNS-Namen "vpntest.ncp-e.com". Ohne die Firewall-Regel NCP-DNS (oder eine andere zur DNS-Abfrage) kann kein Tunnelaufbau erfolgen, da der DNS-Name "vpntest.ncp-e.com" des Gateways nicht aufgelöst werden kann.

Um die Namensauflösung zu ermöglichen und einen DNS-Request zu gestatten, stehen außerdem folgende vordefinierte Firewall-Regeln zur Verfügung, die unverändert eingesetzt bzw. hinzugefügt werden können:

- DNS-Abfrage (IPv4)
- DNS-Abfrage (IPv6)
- DNS-Abfrage (unbekanntes Netz)

Regel für Web-Browser

Die NCP-Regel für Web-Browser, lässt den Zugriff auf den Web Server nur über einen VPN-Tunnel zum VPN Test-Gateway zu (Remote IP-Adresse 172.16.12.100). Zudem werden keine Websites mit Server-Verifizierung (Remote Port HTTPS, 443) unterstützt, sondern nur HTTP (Remote Port 80). Die Regel gilt nur für IPv4-Adressen.

Eine weitere Regel für Internet-Zugriff via Web-Browser gestattet den Zugriff über alle Netze, lässt auch HTTPS zu und gilt sowohl für IPv4 als auch für IPv6.

Regel für FTP

Die NCP-Regel für einen FTP-Zugriff lässt nur Verbindungen über einen VPN-Tunnel zum NCP Test-Gateway (Remote IP-Adresse 172.16.12.100) über die Remote Ports 20 und 21 zu.

Regel für Remote Desktop

Die Firewall-Regel, die den Zugriff auf einen entfernten Rechner gestattet (RDP-Zugriff), ist vorkonfiguriert mit dem Remote Port 3389.

Alle ausgehenden Verbindungen erlauben

Mit dieser Regel werden alle von diesem Rechner abgehenden Verbindungen gestattet, sowohl solche über ein VPN, wie auch solche in bekannte und auch unbekannte Netze.

Alle Verbindungen in bekannte Netze erlauben

Mit dieser Regel werden alle Verbindungen in bekannte Netze und aus bekannten Netzen zum Rechner gestattet. In diesem Fall können aus dem bekannten Netzwerk auch Zugriffe auf diesen Rechner erfolgen!

Alle Verbindungen im VPN erlauben

Mit dieser Regel werden alle Verbindungen über VPN gestattet. In diesem Fall können über VPN auch Zugriffe auf diesen Rechner erfolgen!

IPsec-Protokoll und VPN Path Finder zulassen

Der Aufbau von VPN-Verbindungen über das Register "Optionen" kann global zugelassen werden.

Folgende für den Tunnelaufbau benötigte Protokolle und Ports werden per automatisch generierter Filter für IPsec und die VPN Path Finder Technology freigegeben:

- IP-Protokoll 50 (ESP)
- UDP 4500 (NAT-T)
- UDP 67 (DHCP)
- UDP 68 (DHCP)
- TCP 443 (VPN Path Finder, falls konfiguriert)

Diese globale Definition erspart die Einrichtung dedizierter Einzelregeln für die jeweilige VPN-Variante.

Bitte beachten Sie, dass dadurch lediglich der Tunnelaufbau ermöglicht wird. Existieren keine weiteren Regeln für VPN-Netze, die eine Kommunikation im Tunnel zulassen, kann über die VPN-Verbindung kein Datenaustausch erfolgen.

Regel-Tabelle

Erstellen und Bearbeiten einer Firewall-Regel

Über die unten angezeigten Buttons werden die Regeln erzeugt oder bearbeitet. Um eine Firewall-Regel zu erstellen, klicken Sie auf "Neu" oder "Kopieren", um eine zu ändern auf "Bearbeiten" und zum Entfernen auf "Löschen".

Der Editiermodus kann wahlweise auch mit Doppelklick auf das zu editierende Parameterfeld oder die zu editierende Regel in der Tabelle eingeschaltet werden.

Mit der Tabulator-Taste kann in der zu editierenden Regel von Parameterfeld zu Parameterfeld gesprungen werden.

In der Regel-Tabelle werden alle Firewall-Regeln abgebildet, die aus der angebotenen Liste hinzugefügt werden oder neu erstellt werden.

Aus der Liste in die Tabelle hinzugefügte "fertige" Regeln sind automatisch aktiviert. Neu erstellte Regeln müssen erst aktiviert werden.

Mit Klick auf die Spaltenüberschriften bzw. Symbole werden die vorhandenen Regeln entsprechend sortiert.

Wurde nach dem Öffnen der Firewall-Konfiguration eine Regel geändert oder hinzugefügt, so wird der Übernehmen-Button aktiviert, um die neuen Einstellungen komplett in das Regelwerk der Firewall zu übernehmen, ohne die Firewall-Konfiguration mit OK verlassen zu müssen.

Die folgende Beschreibung orientiert sich an den Spaltenüberschriften bzw. den Symbolen der Regel-Tabelle von links nach rechts.

Aktivieren

Aus der Liste in die Tabelle hinzugefügte Regeln sind automatisch aktiviert. Neu erstellte Regeln müssen eigens aktiviert werden.

Nur wenn eine Regel aktiviert ist, wird sie auf Datenpakete angewendet.

Name

Der Name der Regel kann beliebig geändert werden.

Richtung

Mit der Richtung geben Sie an, ob diese Regel für eingehende oder ausgehende Datenpakete gelten soll. Wird die Richtung auf ausgehend gesetzt, wird nach dem Prinzip von Stateful Inspection gearbeitet. Stateful Inspection wird jedoch nur für die Protokolle UDP und TCP angewendet.

Auf "eingehend" kann z.B. dann geschaltet werden, wenn von Remote-Seite eine Verbindung aufgebaut werden soll (z. B. für Administrator-Eingriffe).

Die Einstellung "bidirektional" ist nur sinnvoll, wenn Stateful Inspection nicht zur Verfügung steht, z. B. für das ICMP-Protokoll (bei einem Ping).

Aktion

Die Aktion ist normalerweise immer auf "zulassen" gestellt!

Nur in Sonderfällen empfiehlt sich die Verwendung der Option "sperrern"; etwa wenn mit einer Regel die Zulässigkeit für einen IP-Adressbereich oder Port-Bereich definiert ist, und eine zweite Regel z. B. eine einzelne Adresse oder einen einzelnen Port, befindlich innerhalb des in der ersten Regel definierten Bereichs, ausschließen soll.

VPN / Bekanntes Netzwerk / Unbekanntes Netzwerk

Beim Neuanlegen einer Regel ist diese zunächst keinem Netz zugeordnet.

Unbekannte Netze

- sind alle Netze (IP-Netzwerkschnittstellen), die weder einem bekannten noch einem VPN-Netz zugeordnet werden können. Darunter fallen z.B. Verbindungen über das DFÜ-Netzwerk von Microsoft oder auch direkte und unverschlüsselte Verbindungen mit dem integrierten Dialer des Clients, wie auch Hotspot WLAN-Verbindungen.

Soll eine Regel für unbekannte Netze gelten, so muss diese Option aktiviert werden.

Bekannte Netze

- werden im gleichnamigen Register im Fenster "Firewall-Einstellungen" definiert. Soll eine Regel für bekannte Netze gelten, muss diese Option aktiviert werden.

VPN-Netze

- sind alle IPsec-Verbindungen in aufgebautem Zustand. Darüber hinaus fallen unter diese Gruppe auch alle verschlüsselten Direktwahlverbindungen über den integrierten Dialer des Clients. Soll eine Regel für VPN-Netze gelten, so muss diese Option aktiviert werden.

Protokoll

Je nach Anwendung oder Art der Verbindung ist das entsprechende Protokoll zu wählen: TCP, UDP, ICMP, GRE, ESP, AH, IGRP, RSVP, IPv6 over IPv4, ICMPv6, alle

Anwendung

Mit Klick auf das Verzeichnis-Symbol kann eine Anwendung selektiert werden, für die das Herstellen einer Verbindung möglich sein soll. Nur diese lokal installierte Anwendung, wie z. B. IExplore.exe, kann kommunizieren.

Kein automatischer Verbindungsaufbau

In der Standardeinstellung nicht aktiv!

(Nur relevant bei Wahlverbindungen wie einem Mobilfunknetz mit automatischem Verbindungsaufbau im aktuellen Profil!)

Diese Option ist nur sinnvoll, wenn im Profil im Parameterfeld "Verbindungssteuerung" der Verbindungsaufbau auf "automatisch" gestellt wurde. Für die über diese Regel definierten Datenpakete

findet bei Aktivierung dieser Funktion kein automatischer Verbindungsaufbau statt, für andere Datenpakete schon.

nur gültig bei inaktiver VPN-Verbindung

Sie wählen z. B. die Option, dass die hier konfigurierte Regel "nur gültig bei inaktiver VPN-Verbindung" ist, wenn Sie wünschen, dass z. B. eine Internet-Verbindung bei gleichzeitig bestehender VPN-Verbindung ausgeschlossen wird, ansonsten aber Internet-Verbindungen zu unbekannten Netzen zugelassen sein sollen. Dazu muss diese Regel für "unbekannte Netze" angewendet werden, d. h. diese Regel muss den Zugang zu unbekannten Netzen zulassen.

Lokale Ports und IP-Adressen

Diejenigen Datenpakete werden von der Firewall nach außen durchgelassen, deren Quelladresse (Source Address) mit der unter "Lokale IP-Adressen" übereinstimmt oder im Gültigkeitsbereich liegt.

Ebenso verhält es sich mit den IP-Ports. Diejenigen Datenpakete werden von der Firewall nach außen gelassen, deren Quell-Port (Source Port) unter die Definition der lokalen Ports fällt.

IP-Adressen

Mit den Einträgen der lokalen IP-Adressen lässt sich festlegen, für welche IP-Adressen abgehender Pakete die Firewall-Regel durchlässig ist. Folgende Einträge sind möglich:

anyv4: erlaubt die Kommunikation mit beliebigen IPv4-Adressen auf der lokalen Seite (Quell-Adressen), ohne Einschränkung.

anyv6: erlaubt die Kommunikation mit beliebigen IPv6-Adressen auf der lokalen Seite (Quell-Adressen), ohne Einschränkung.

bestimmte Adresse: einzelne IP-Adressen können untereinander nach Betätigen des [+] -Buttons (auch in unterschiedlichen IP-Protokollversionen abwechselnd) eingegeben werden.

Die Schreibkonventionen sind:

123.10.62.1 / 32 (für IPv4)

fd00:6e93:5063:37de:12:16:8005:7a / 128 (für IPv6)

Adressbereiche: für Adressbereiche können zwei Darstellungsformen gewählt werden.

Für IPv4 kann mit 32-, 24-, 16-, 8- oder anderen Bit-Darstellungen zwischen 1 und 32 ein Bereich ausmaskiert werden:

123.10.62.1 / 24 entspricht dem Bereich (von - bis) 123.10.62.0 - 123.10.62.255

Entsprechend kann für IPv6 mit Bit-Darstellungen zwischen 1 und 128 ein Bereich ausmaskiert werden:

fd00:6e93:5063:37de:12:2c35:987c:2450 / 64 entspricht dem Bereich (von - bis) fd00:6e93:5063:37de:: - ...

Ports

Mit den Einträgen unter Lokale Ports lässt sich festlegen, welche Ports am lokalen System genutzt werden. Folgende Einträge sind möglich:

any: erlaubt Kommunikation über alle Quell-Ports bei ausgehenden und Ziel-Ports bei eingehenden Paketen.

bestimmter Port: einen bestimmten Port anzugeben kann sinnvoll sein wenn diese Maschine einen Server-Dienst zur Verfügung stellt (z. B. Remote Desktop auf Port 3389).

Port-Bereiche: können verwendet werden, wenn mehrere Ports für eine Regel verwendet werden sollen (z. B. FTP Port 20/21).

Remote Ports und IP-Adressen

Diejenigen Datenpakete werden von der Firewall nach außen durchgelassen, deren Zieladresse (Destination Address) mit der unter "Remote IP-Adressen" übereinstimmt oder im Gültigkeitsbereich liegt.

Ebenso verhält es sich mit den IP-Ports. Diejenigen Datenpakete werden von der Firewall nach außen gelassen, deren Ziel-Port (Destination Port) unter die Definition der remote Ports fällt.

IP-Adressen

Mit den Einträgen unter Remote-IP-Adressen lässt sich festlegen, mit welchen entfernten IP-Adressen das System kommunizieren darf. Folgende Einträge sind möglich:

anyv4: erlaubt die Kommunikation mit beliebigen IPv4-Adressen der Gegenseite, ohne Einschränkung.

anyv6: erlaubt die Kommunikation mit beliebigen IPv6-Adressen der Gegenseite, ohne Einschränkung.

bestimmte Adresse: einzelne IP-Adressen können untereinander nach Betätigen des [+] -Buttons (auch in unterschiedlichen IP-Protokollversionen abwechselnd) eingegeben werden.

Die Schreibkonventionen sind:

123.10.62.1 / 32 (für IPv4)

fd00:6e93:5063:37de:12:16:8005:7a / 128 (für IPv6)

Adressbereiche: für Adressbereiche können zwei Darstellungsformen gewählt werden.

Für IPv4 kann mit 32-, 24-, 16-, 8- oder anderen Bit-Darstellungen zwischen 1 und 32 ein Bereich ausmaskiert werden:

123.10.62.1 / 24 entspricht dem Bereich (von - bis) 123.10.62.0 - 123.10.62.255

Entsprechend kann für IPv6 mit Bit-Darstellungen zwischen 1 und 128 ein Bereich ausmaskiert werden:

fd00:6e93:5063:37de:12:2c35:987c:2450 / 64 entspricht dem Bereich (von - bis)

fd00:6e93:5063:37de:: - ...

Ports

Mit den Einträgen unter Remote Ports lässt sich festlegen, über welche Ports mit entfernten Systemen kommuniziert werden darf. Folgende Einträge sind möglich:

any: setzt keinerlei Beschränkungen hinsichtlich Ziel-Port bei abgehenden bzw. Quell-Port bei eingehenden Paketen.

bestimmter Port: lässt nur eine Kommunikation über den angegebenen Port zu, wenn dieser als Ziel-Port im abgehenden bzw. als Quell-Port im eingehenden Paket vorkommt. Soll z. B. eine Regel nur Telnet zu einem anderen System zulassen, ist hier Port 23 einzutragen.

Port-Bereiche: können verwendet werden, wenn mehrere Ports für eine Regel verwendet werden sollen (z. B. FTP Port 20/21).

Bekannte Netze

Wurde in der Regel-Tabelle definiert, dass eine Regel auf Verbindungen mit bekannten Netzen (Friendly Nets) anzuwenden ist, so wird diese Regel immer dann angewendet, wenn ein Netz nach den hier anzugebenden Kriterien als Friendly Net identifiziert werden kann, also z. B. der LAN-Adapter sich in einem Friendly Net befindet.

Was ein Friendly Net ist, wird vom Administrator zentral verbindlich festgelegt. Dies kann erfolgen durch eine manuelle Konfiguration oder mittels des Automatismus über Friendly Net Detection.

Die manuelle Definition eines bekannten Netzes durch den Administrator und die automatische Erkennung eines bekannten Netzes mittels Friendly Net Detection schließen sich nicht aus, sondern können gleichzeitig eingesetzt und über die Registerkarten "Manuell" und "Automatisch" konfiguriert werden.

Die Signalisierung eines Friendly Net erfolgt im Monitor durch das Firewall-Symbol, dessen Rand sich halbseitig grün färbt, sobald sich der Client mit einem Friendly Net verbunden hat:



Außerdem können ausgewählte Aktionen gestartet werden, sobald ein Friendly Net erkannt wurde oder wenn die Friendly Net Detection fehlschlägt.

Siehe folgende Menüpunkte:

- [Manuelle Konfiguration der bekannten Netze](#) 65
- [Automatische Erkennung der bekannten Netze](#) 66
- [Optionen](#) 68
- [Aktionen](#) 69

Manuelle Konfiguration der bekannten Netze

Der LAN-Adapter des Clients befindet sich dann in einem Friendly Net wenn:

IP-Netze und Netz-Maske

- die IP-Adresse des LAN-Adapters aus dem angegebenen Netzbereich stammt. Ist z.B. das IP-Netz 192.168.254.0 mit der Maske 255.255.255.0 angegeben, so würde die Adresse 192.168.254.10 auf dem LAN-Adapter eine Zuordnung zum bekannten Netz bewirken.

DHCP Server

- die IP-Adresse von dem DHCP Server zugewiesen wurde, der die hier angegebene IP-Adresse besitzt;

Je mehr dieser Bedingungen erfüllt werden, desto präziser ist der Nachweis, dass es sich um ein vertrautes Netz handelt.

Die Zuordnung eines Adapters zu unbekannten oder bekannten Netzen wird automatisch protokolliert im Log-Fenster des Client-Monitors und in der Log-Datei der Firewall (siehe: Protokollierung).

Automatische Erkennung der bekannten Netze

Für die automatische Erkennung ist ein Friendly Net Detection Server (FNDS) erforderlich, d. h. eine Softwarekomponente, die in einem als "Friendly Net" definierten Netz installiert und über IP erreichbar sein muss.

IP-Adresse automatisch über DHCP beziehen

Mit dieser Option wird dem Client automatisch die IP-Adresse des FND-Servers durch den DHCP-Server mitgeteilt.

Voraussetzung ist, dass über den LAN-Adapter des Clients eine DHCP-Verhandlung angestoßen wird, um die IP-Adresse für den LAN-Adapter automatisch von einem DHCP Server zu beziehen. (Dies ist die Standard-Konfiguration in den Netzwerkeinstellungen des Betriebssystems.)

Am DHCP Server des Firmennetzes muss eine DHCP-Standardoption hinzugefügt werden, die den Code 159 und die IP-Adresse des FND Servers erhält, die dann automatisch mit der DHCP-Verhandlung verteilt wird.

IP-Adresse des Dienstes zur Erkennung der bekannten Netze

Soll die IP-Adresse des FND Servers fest vorgegeben werden, so kann sie hier eingetragen werden.

Um die Redundanz zu erhöhen, kann die IP-Adresse eines zweiten FND-Servers nach einem Komma, Strichpunkt oder Leerzeichen nach der ersten IP-Adresse eingetragen werden. Die IP-Adresse des ersten verfügbaren FND-Servers wird automatisch zur Erkennung der bekannten Netze selektiert.

Benutzername, Passwort (FNDS)

Die Authentisierung des Friendly Net Detection Servers erfolgt über MD5 oder TLS. Hier einzutragender Benutzername (erforderlich bei MD5 und TLS) und Passwort (nur erforderlich bei MD5) müssen mit jenen am FNDS hinterlegten übereinstimmen.

Friendly Net Detection mittels TLS

Soll die Friendly Net Detection mittels TLS erfolgen (einschließlich einer Authentisierung über den Fingerprint des Aussteller-Zertifikats), so muss sich im Programmverzeichnis "CaCerts" dieses Aussteller-Zertifikat befinden und dessen Fingerprint muss mit dem hier konfigurierten übereinstimmen.

Benutzer (Subject) des eingehenden Zertifikats

Das eingehende Zertifikat des FNDS wird auf diesen String hin geprüft. Nur bei Gleichheit handelt es sich um ein Friendly Net.

Fingerprint des Aussteller-Zertifikats

Um ein Höchstmaß an Fälschungssicherheit bieten zu können, kann der Fingerprint des Aussteller-Zertifikats überprüft werden. Er muss mit dem hier eingegebenen Hash-Wert übereinstimmen.

Auf bekannte Netze periodisch prüfen

Diese Art der periodischen Prüfung kann nicht eingesetzt werden, wenn die Erkennung des bekannten Netzes über DHCP erfolgt!

Die periodische Prüfung sollte dann aktiviert werden, wenn eine Zustandsänderung des Netzwerk-Adapters unverändert bleibt, zum Beispiel beim Ziehen des LAN-Kabels. Dies kann die Folge sein, wenn der Client in einer virtuellen Umgebung betrieben wird.

In diesem Fall bewirkt diese Funktion, dass im eingestellten Intervall geprüft wird, ob sich der Client noch in einem bekannten Netz befindet. Sobald das Friendly Net nicht mehr zur Verfügung steht, wird die Verbindung getrennt und mit den üblichen Mechanismen nach einem anderen bekannten Netz gesucht.

Für die periodische Prüfung kann ein Intervall in Sekundenlänge definiert werden. Voreingestellt ist der Maximalwert von 3600 Sekunden. Es wird unabhängig vom Zeitpunkt des Verbindungsaufbaus oder eines Medienwechsels geprüft.

Im Standardfall wird bei einem Verbindungsaufbau oder Medienwechsel immer geprüft, ob ein bekanntes Netz zur Verfügung steht. (Während dieses Prüfvorgangs wird im Monitor kurzzeitig das rote Balkensymbol angezeigt.)

Optionen

Optional können bestimmte Funktionen für Clients, die sich bereits im bekannten Netz befinden, ausgeblendet werden.

VPN-Verbindungsaufbau im bekannten Netz nicht zugelassen

Ist diese Option eingeschaltet, so ist kein zusätzlicher VPN-Tunnelaufbau mehr möglich, wenn sich der Client bereits im bekannten Netz befindet. Der Button für den Verbindungsaufbau (bzw. der Menüpunkt) im Client-Monitor wird deaktiviert. Eine bereits bestehende VPN-Verbindung, die möglicherweise durch eine andere Anwendung hergestellt wurde, kann jedoch getrennt werden.

Logon-Optionen im bekannten Netz ausblenden

Für den Fall, dass sich der Client bereits im bekannten Netz befindet, können die Logon-Optionen zur Domänen-Anmeldung hier ausgeblendet werden.

Wartezeit für Friendly Net-Erkennung vor Windows-Anmeldung

Die Zeitspanne für die automatische Friendly Net Detection kann unabhängig vom Timeout-Wert eingegeben werden. Der Wert für die Zeit der Netzsuche muss mindestens 30 Sekunden sein. (Standard sind 60 Sekunden).

Aktionen

Sobald der Client den Wechsel von einem bekannten zu einem unbekannten Netzwerk (oder umgekehrt) erkennt oder die [Home Zone](#) ^[205] aktiviert wird, kann in Abhängigkeit davon eine beliebige Aktion gestartet werden. So kann beispielsweise ein externes Programm oder eine Batch-Datei gestartet werden, was die Proxy-Einstellung des Windows-Systems umschaltet.

Anwendung / Batch-Datei

Nach Klick auf "Hinzufügen" kann eine Anwendung oder Batch-Datei selektiert werden (*.com, *.exe, *.bat).

Die Anwendung kann auch manuell mit Pfadangabe eingegeben werden, oder der Pfad wird mithilfe einer Umgebungsvariablen eingegeben.

Folgende Variablen werden unterstützt:

- NCP-Variablen: %SYSTEMROOT%, %INSTALLDIR%, %PROGDIR%
- Windows-Umgebungsvariablen: z.B.: NcpCIntInstallPath, ProgramData

Der aufzulösende Pfad der Anwendung kann Leerzeichen enthalten, muss in diesem Fall aber in Anführungszeichen gesetzt werden.

z.B.: "%INSTALLDIR%Ncp Client Cmd.exe" /connect

Wurden Umgebungsvariablen bei der Eingabe vom Anwender oder von der zentralen Administration (bei der Erstellung der Konfigurationsdateien ncpphone.cfg und ncpphone.cnf) verwendet, so werden die Umgebungsvariablen in die entsprechenden lokalen Pfade konvertiert, sobald sie einmal gespeichert wurden und am Client-Monitor eingelesen werden.

Startoption

Die Anwendung / Batch-Datei kann dann gestartet werden, wenn der Client ein bekanntes Netz erkannt hat bzw. der Netzadapter sich in einem Friendly Net befindet.

Die selektierte Anwendung / Batch-Datei kann auch dann gestartet werden, wenn der Client kein bekanntes Netz vorfindet bzw. der Netzadapter sich nicht in einem Friendly Net befindet.

Warten bis die Anwendung ausgeführt und beendet ist (wait)

Die Anwendungen und Batch-Dateien werden je nach Startoption in der Reihenfolge abgearbeitet, in der sie in der Übersichtstabelle der Aktionen aufgelistet sind. D. h. der Reihenfolge nach entweder alle bei bekanntem oder die bei unbekannten Netzen gestartet werden.

Das Abarbeiten von Anwendungen (nur *.com und *.exe) in der entsprechenden Reihenfolge kann mit der Wait-Funktion angehalten werden. D. h. die nächste Anwendung wird erst gestartet, wenn die mit der Wait-Funktion versehene vom Benutzer beendet wurde.

Bitte beachten Sie bei der Erstellung von Batch-Dateien:

Bei einer Batch-Datei (*.bat) kann die Wait-Funktion nur dann funktionieren, wenn die Batch-Datei fehlschlägt, d. h. stehen bleibt, weil sie nicht korrekt bis zu Ende ausgeführt werden kann. Ist in diesem Fall für die Batch-Datei die Wait-Funktion gesetzt, so muss die Batch-Datei zuerst manuell beendet werden, bevor die nachfolgende Anwendung gestartet wird.

Auf jedenfall sollte dem Benutzer über die Batch-Datei eine entsprechende Rückmeldung gegeben werden.

Übersichtstabelle der Anwendungen / Batch-Dateien

In der Übersichtstabelle sind die Aktionen zunächst in der Reihenfolge aufgelistet, in der sie erstellt wurden. Mit den grünen Pfeil-Tasten am rechten Rand der Tabelle können die Aktionen in der Reihenfolge verschoben werden.

Der Übersichtlichkeit wegen sollten jeweils die Aktionen übereinander stehen, die im bekannten bzw. unbekannten Netz gestartet werden.

Optionen [Firewall]

Im Register [Allgemein](#) ⁷⁴ kann die Firewall unter anderem auch bei nicht gestartetem Client aktiv geschaltet werden.

Im Register [Kommandos](#) ⁷⁷ können Passwort und Zeitspanne hinterlegt werden, um die Firewall temporär von der Kommandozeile aus zu öffnen, ebenso Konfigurationseinstellungen für die Hotspot-Anmeldung.

Allgemein

Firewall bei gestopptem Client weiterhin aktivieren

Die Firewall kann auch bei gestopptem Client aktiv sein, wenn diese Funktion selektiert wird. In diesem Zustand wird jedoch jede ein- und ausgehende Kommunikation unterbunden, so dass keinerlei Datenverkehr möglich ist, solange der Client deaktiviert ist.

Wird oben genannte Funktion nicht genutzt und der Client gestoppt, so wird auch die Firewall deaktiviert.

Stateful Boot-Option aktivieren

Ist die Firewall auch bei gestopptem Client aktiv geschaltet, so kann mit dieser Funktion Stateful Inspection eingeschaltet werden. Damit ist die Kommunikation von diesem PC in ein anderes Netz möglich. Antworten auf ausgehende Verbindungen werden so auch verarbeitet, alle anderen eingehenden Verbindungen aber konsequent geblockt.

Diese Einstellung wird erst nach einem Neustart des Dienstes (Reboot) aktiv.

Hinweis: Wenn Sie eine Konfigurationsdatei während der Client-Installation einspielen, müssen Sie das System neu starten. Dieser Neustart geschieht unabhängig von dem Neustart, der nach der Installation erforderlich ist. Erfolgt dieser Neustart nicht, wird Ihre Einstellung als aktiv angezeigt, ist aber auf Treiberebene noch nicht wirksam.

Hinweis: Beachten Sie zudem, dass

- wenn die Funktion Bekannte Netze (Friendly Net Detection, FND) aktiviert ist
und
- die Stateful Boot Option der Firewall ebenfalls aktiviert ist
und
- der Dienst (Firewall) gerade gestartet wurde,

die Stateful Boot Option der Firewall dann noch weitere 15 Sekunden auf allen LAN-Adaptern eingeschaltet bleibt und erst nach Ablauf dieser Zeitspanne die Regeln der normalen Firewall greifen. Damit wird gewährleistet, dass der Prozess der FND-Erkennung normal durchgeführt und abgeschlossen werden kann.

UDP Pre-Filtering

Die Funktionalität von UDP-Prefiltering kann nur bei aktivierter Firewall genutzt werden. Ist die Firewall nicht aktiv, wird unabhängig von der Schalterstellung die Funktionalität von UDP-Prefiltering auf aus gesetzt. Dies bedeutet, dass bei nicht aktiver Firewall alle UDP-Pakete auf den Client PC gelangen!

immer: Standardeinstellung. In dieser Schalterstellung gelangen bei gestartetem Client keine UDP-Pakete auf den Client PC.

nur bei unbekannten Netzen: In dieser Schalterstellung wirkt der UDP-Filter nur auf Pakete, die über Adapter unbekannter Netze eintreffen.

aus: Wird der Filter ausgeschaltet, gelangen alle UDP-Pakete auf den Client PC. Diese Einstellung sollte nur verwendet werden, wenn Probleme mit einer Anwendung auftreten.

VMware-Gastsysteme schützen

Ein VMware-Gastsystem kann bei aktivierter Firewall eines im Hauptsystem installierten Clients geschützt werden. D. h. die Firewall des Clients muss aktiv sein. Nur dann ist die Option "VMware-Gastsysteme schützen" auch gültig und wirksam. Eingehende Verbindungen auf das Gastsystem sind dann nicht möglich.

VMware bietet verschieden Modi für das Gastsystem an: Bridged, NAT und Host only.

Host Only Mode

Im Host only-Modus ist unabhängig von der Firewall grundsätzlich ausschließlich eine bidirektionale Kommunikation mit dem Hauptsystem möglich.

Bridged-Modus

Befindet sich das Gastsystem im Bridged-Modus und wird die Option "VMware-Gastsysteme schützen" gesetzt, so ist das Gastsystem komplett abgeschottet. Keine Verbindung vom Gastsystem ins Internet oder umgekehrt ist möglich. Auch DHCP-Anfragen werden blockiert.

Eine Kommunikation mit dem Hauptsystem ist weiterhin bidirektional möglich.

NAT-Modus

Befindet sich das Gastsystem im NAT-Modus und wird die Option "VMware-Gastsysteme schützen" gesetzt, so gelten die konfigurierten Firewall-Regeln für ausgehende Verbindungen. Verbindungen von außen sind nicht möglich.

Eine Kommunikation mit dem Hauptsystem ist weiterhin bidirektional möglich.

Ausgehenden Datenverkehr mit Reject quittieren

Der von einer Firewall blockierte ausgehende Datenverkehr wird wie folgt behandelt:

Wird die Option "Ausgehenden Datenverkehr mit Reject quittieren" aktiviert (Standardeinstellung), werden ausgehende Pakete, die von den aktuellen Firewall-Regeln blockiert werden, mit einem "Reject" an die sendende Anwendung quittiert (ICMP destination unreachable). Normalerweise sind die Applikationen bereits darauf ausgelegt, die Meldung "ICMP destination unreachable" als akzeptablen Netzwerkfehler zu verarbeiten.

Wird die Option "Ausgehenden Datenverkehr mit Reject quittieren" ausgeschaltet, werden ausgehende Pakete, die von den aktuellen Firewall-Regeln blockiert werden, ohne Rückmeldung an die sendende Anwendung verworfen. Da keinerlei Rückmeldung erfolgt, muss die Anwendung einen Netzwerk-Timeout abwarten, bevor sie eine spezielle Reaktion durchführt.

Aktiviere Home Zone

Um die [Funktionalität der Home Zone](#) ^[205] nutzen zu können, muss sie aktiviert werden und ein Adapter (LAN oder WLAN) verfügbar sein, über den die Verbindung in das als privat eingestufte Netz hergestellt werden soll.

Home Zone nur temporär setzen

Soll die Home Zone nur vorübergehend zur Verfügung stehen, kann dieser Schalter gesetzt werden. Dies bewirkt, dass die Einstellungen für die Home Zone in der Firewall zurück gesetzt werden, sobald die Home Zone nicht mehr aktiv genutzt wird.

Dies ist zum Beispiel dann der Fall

- wenn Dienste gestoppt und gestartet werden
- wenn ein Netzwerkwechsel von LAN zu WLAN oder umgekehrt stattfindet (unter der Einstellung WLAN aus wenn LAN aktiv)
- wenn der Netzwerk-Adapter deaktiviert / aktiviert wird
- wenn das LAN-Kabel gezogen oder gesteckt wird
- wenn das System neu gestartet wird

Kommandos [Firewall]

Die Firewall darf über das Kommando "RWSCMD /Firewalloff" temporär für einen bestimmten Zeitraum deaktiviert werden.

Soll das temporäre Öffnen der Firewall über die Kommandozeile möglich sein, muss diese Funktion hier aktiviert werden.

Die Eingabe eines Passworts ist optional. Wird hier ein Passwort eingegeben, muss dieses Passwort auch in der Kommandozeile wiederholt werden.

Das Kommando lautet:

```
rwscmd /firewalloff [Passwort] [Timeout]
```

Ein Timeout kann in der Kommandozeile ganzzahlig in Sekunden angegeben.

Die Firewall wird wieder aktiv wenn der Timeout abgelaufen ist oder nach dem Kommando:

```
rwscmd /firewallon
```

Die Eingabe eines Passworts ist optional. Wird hier ein Passwort eingegeben, muss dieses Passwort auch in der Kommandozeile wiederholt werden.

Die Eingabe des "Max. Timeouts" ist optional. Ein hier eingetragener Wert dient nur der Begrenzung des Timeouts, der in der Kommandozeile eingegeben werden muss.

Zusätzliche Ports zu den Standard-Ports 80 und 443, die automatisch zur Hotspot-Anmeldung geöffnet werden, werden dann geöffnet, wenn sie hier eingetragen werden. Mehrere Ports werden mit einem Komma getrennt. Ebenso können zusätzliche Port-Bereiche eingetragen werden (z. B. 50100-50200). Mehrere Port-Bereiche werden jeweils durch Komma getrennt.

Protokollierung

Die Aktivitäten der Firewall werden je nach Einstellung in eine Log-Datei geschrieben. Das "Ausgabeverzeichnis für Log-Dateien" befindet sich standardmäßig im Installationsverzeichnis unter [installdir]\log.

Die Log-Dateien für die Firewall sind im reinen Textformat geschrieben und benannt als fwyyymmdd.log (yyymmdd = Datum in Jahr, Monat, Tag). Sie beinhalten eine Beschreibung vom "abgelehnten Datenverkehr" und/oder "zugelassenen Datenverkehr". Wurde keine dieser Optionen selektiert, so werden nur Statusinformationen zur Firewall protokolliert.

Die Log-Dateien werden bei jedem Start der Firewall geschrieben. Maximal werden davon so viele im Log-Verzeichnis gehalten, wie die Anzahl der eingegebenen "Tage der Protokollierung".

Bitte beachten Sie, dass es bei aktivierter Protokollierung zu Performance-Einbußen kommen kann, da für jedes Paket, für welches diese Einstellung gilt, ein entsprechender Protokolltext ausgegeben werden muss.

VPN-Bypass

Die [VPN-Bypass-Funktion](#)^[209] gestattet Anwendungen oder Domänen festzulegen, die trotz deaktiviertem [Split Tunneling](#)^[195] an der VPN-Verbindung vorbei direkt ins Internet kommunizieren sollen. Ebenso ist es möglich, bestimmte Domänen zu bestimmen, deren Datenkommunikation am VPN-Tunnel vorbei stattfinden soll.

Diese Funktion kann unter anderem dazu genutzt werden, um regelmäßig notwendige, nicht sicherheitsrelevante Datenübertragung von der zentralen Infrastruktur fernzuhalten, um deren Performance nicht zu beeinträchtigen. Zum Beispiel könnten Updates des Betriebssystems oder des Virenschanners (mit bekannter Domäne) ohne Umweg über die VPN-Verbindung zugelassen werden, oder bei bestimmten Cloud-Services der direkte Zugriff der Anwendungen über das Internet ermöglicht werden.

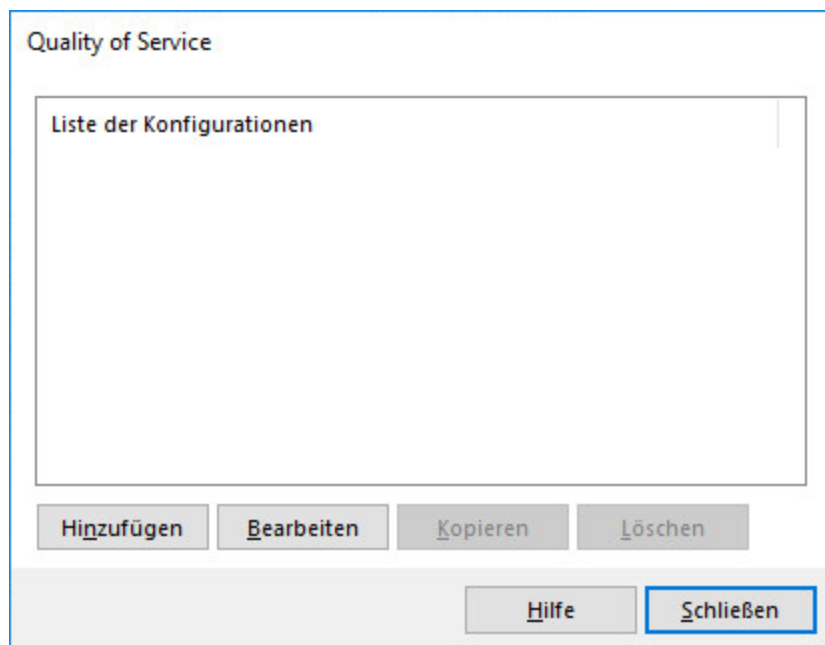
Konfiguration

- Als Vorbereitung für die Funktionalität werden an dieser Stelle zunächst die Applikationen oder Domänen festgelegt, deren Kommunikation am VPN-Tunnel vorbei stattfinden soll. Dabei kann gegebenenfalls noch festgelegt werden, ob dies nur für TCP oder UDP-Kommunikation erfolgen soll.
- Die entstandene Bypass-Liste von Anwendungen und Domänen für einen VPN-Bypass wird für die weitere Konfiguration in den [Profil-Einstellungen zum VPN-Bypass](#)^[196] benötigt. Dort wird definiert ob und für welches VPN-Profil ein bestimmter VPN-Bypass möglich sein soll.
- Neben dem Namen für die VPN-Bypass-Liste können Sie auch die IP-Adressen für einen primären und sekundären DNS-Server angeben.

Quality of Service

Beachten Sie zur Konfiguration von Quality of Service auch die ausführliche [Konfigurationsbeschreibung](#)²¹⁶ dieses Leistungsmerkmals.

Beim ersten Öffnen ist die Liste der Konfigurationen noch leer (Abb. unten).



Mit Klick auf „Hinzufügen“ wird der erste Konfigurationsdialog geöffnet (Abb. unten).

Quality of Service - Gruppen

Name:

Maximal verfügbare Netzwerkbandbreite MBit/s

Gruppe	Mindestbandbreite [MBit/s]
✓	80

Zunächst wird eine Konfiguration nach Eingabe des Namens mit Klick auf „OK“ erstellt (in obiger Abbildung „Meine-QoS-Konfiguration“). Dazu wird die maximal verfügbare Netzwerkbandbreite in MBit/s für alle Gruppen eingegeben. (Die gesamte zur Verfügung stehende Bandbreite kann dem Vertrag mit dem Netzdienstleister entnommen werden oder mit einem Speed-Test ermittelt werden. Siehe dazu im Hauptmenü „Verbindung / Verbindungsinformationen“). Maximal können 100 MBit/s eingetragen werden. Der Upstream-Standardwert beträgt bei VDSL 10Mbit/s.

Konfiguration von Gruppen

Im Folgenden können unter jeder Konfiguration mehrere Gruppen eingestellt werden (siehe Abb. unten), nachdem „Hinzufügen“ angeklickt wurde.

Der Name einer neuen Gruppe (Abb. unten „Video / Skype“) wird in das unten gezeigte Konfigurationsfenster eingefügt, nachdem „Hinzufügen“ angeklickt wurde. Damit öffnet sich untenstehendes Fenster, worin für diese Gruppe auch die gesamte Mindestbandbreite eingestellt werden kann (Abb. unten).

VPN Quality of Service - Gruppe

Gruppe:

Mindestbandbreite: MBit/s

Filter	Type
--------	------

Hinzufügen Bearbeiten Löschen

Hilfe OK Abbrechen

Mit Klick auf „OK“ wird die Gruppe in die Konfiguration übernommen (Abb. unten). Weitere Gruppen werden analog erstellt.

Quality of Service - Gruppen

Name:

Maximal verfügbare Netzwerkbandbreite: MBit/s

Gruppe	Mindestbandbreite [MBit/s]
▶ Video / Skype	50

✓ Verbleibende Bandbreite 30

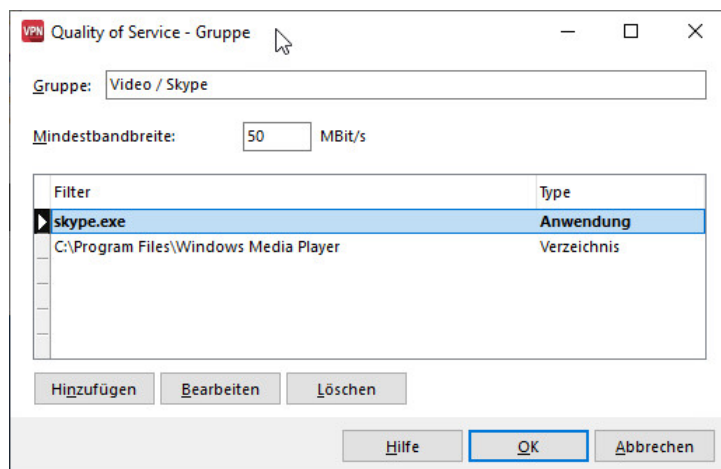
Hinzufügen Bearbeiten Löschen

Hilfe OK Abbrechen

Dabei darf bei Konfiguration mit mehreren Gruppen, die maximal verfügbare Netzwerkbandbreite nicht überschritten werden. Ansonsten kann die Konfiguration nicht gespeichert werden.

Konfiguration von Filtern

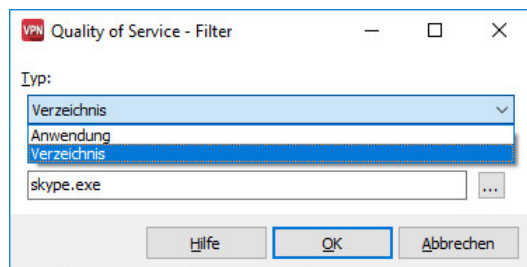
Im nächsten Schritt können unter der Funktionsbezeichnung einer der selektierten Gruppe mehrere Ausführungsbestimmungen, sogenannte Filter, zugeordnet werden. Dazu wird ein Doppelklick auf die markierte Gruppe (Abb. oben „Video / Skype“) ausgeführt oder „Bearbeiten“ angeklickt, woraufhin sich die bereits vorhandenen Namen der Filter und ihr Typ zeigen (Abb. unten).



Mit „Hinzufügen“ wird ein Dialogfenster gezeigt, worin zunächst der Typ des Filters (Anwendung, Verzeichnis) angegeben wird (Abb. unten).

Anwendung: Bei diesem Typ wählen Sie die Anwendung aus, für die die eingetragene Bandbreite sichergestellt wird. Wenn Sie den Namen der Anwendung kennen (z. B. skype.exe) kennen, können Sie diesen direkt in das Feld eintragen (siehe Bild unten).

Verzeichnis: Bei diesem Typ werden alle .exe Dateien ausgewählt, die in dem angegebenen Verzeichnis liegen.



Je nach Auswahl des Typs wird auch ein Feld für den korrespondierenden Eintrag angeboten (Abb. unten).

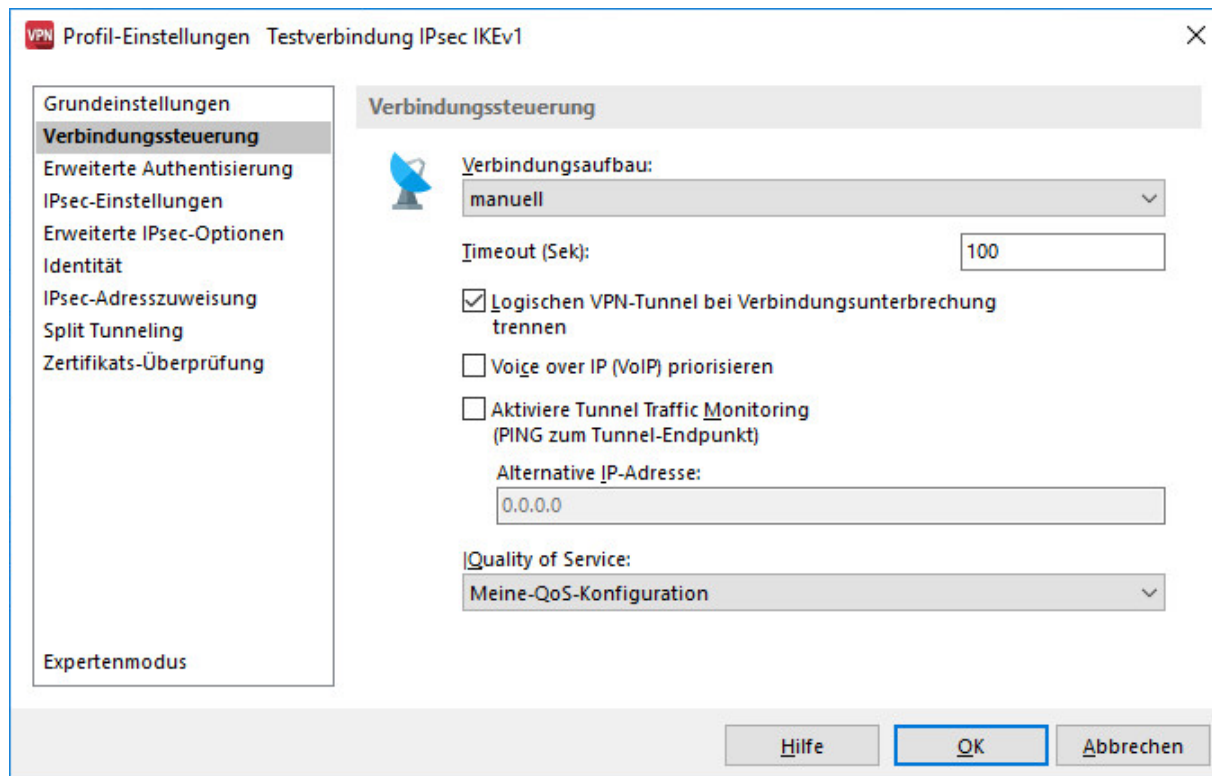
Werden diese Eingaben mit OK bestätigt, werden die Filter der Gruppe „Video / Skype“ dargestellt.

Zu beachten ist, dass nicht jeder einzelne Filter einer Gruppe die gesamte Mindestbandbreite bekommt. Statt dessen wird die Mindestbandbreite auf die Gruppe bezogen. Pro Gruppe teilt sich diese dann auf die einzelnen Filter auf, sofern mehrere davon aktiv sind. Deshalb muss entschieden werden, ob mehrere Filter sich eine bestehende Gruppe teilen oder stattdessen für einen Filter eine neue Gruppe erstellt wird.

Einsatz von Quality of Service im VPN-Profil

Eine Konfiguration für Quality of Service wird erst wirksam, nachdem sie einem bestimmten Profil zugeordnet wurde! Dies erfolgt über die GUI des Clients in den Profil-Einstellungen unter „Konfiguration / Profile“. Dort wird dasjenige Profil mit Doppelklick ausgewählt, wofür die Konfiguration für Quality of Service eingesetzt werden soll.

Unter „Erweiterte Konfiguration / [Verbindungssteuerung](#)¹⁶²“ kann zu „Quality of Service“ eine der vordefinierten Konfigurationen ausgewählt werden.







WLAN-Management

WLAN-Management aktivieren

Wenn das WLAN-Management des Clients aktiviert ist, kann die automatische WLAN-Erkennung und die vereinfachte Hotspot/WLAN-Anbindung genutzt werden.

Zur Erstellung von WLAN-Profilen mit dem Management-Tool können in folgenden Konfigurationsfenstern Einstellungen vorgenommen werden:

[Verbindungen](#)  89
[Profile](#)  91
[Optionen](#)  97
[Statistik](#)  97

WLAN-Management

Ist die Einstellung WLAN-Management aktivieren und unter Optionen Aktiviere Hotspot/WLAN-Erkennung gesetzt und steht keine Internet-Verbindung zur Verfügung, so wird bei vorhandenen WLAN-Netzen ein eigenes Panel in der Client-Oberfläche eingeblendet, welches einen Link anzeigt und einen Button enthält.

Ein Klick auf den Link oder den zugehörigen Button stellt die Hotspot-Verbindung (des aktuellen VPN-Profiles) immer dann automatisch her, wenn ein WLAN-Profil in der Liste des WLAN-Managements mit Verbindungsautomatik markiert ist.

Ist kein WLAN-Profil in der Liste des WLAN-Managements mit Verbindungsautomatik markiert, so wird diese Liste geöffnet. Sobald eines der angezeigten WLAN-Profile für den Verbindungsaufbau durch Drücken des Verbinden-Buttons selektiert wird, wird die Verbindung zum Hotspot aufgebaut. (Gleichzeitig wird das soeben selektierte WLAN-Profil mit Verbindungsautomatik markiert, die solange erhalten bleibt bis die VPN-Verbindung einmal manuell getrennt wird.)

Nach der Authentisierung am Hotspot wird die VPN-Verbindung aufgebaut, wobei ggf. noch Authentisierungsdaten für das VPN eingegeben werden müssen.

Ist die Anmeldung am Hotspot oder das Herstellen der verschlüsselten Verbindung zum Access Point erfolgreich und ein Zugriff auf das Internet möglich, wird automatisch der VPN Verbindungsaufbau (für das aktuelle VPN-Profil) initiiert, ohne dass der Benutzer aktiv werden muss.

Bitte beachten Sie, dass die automatisierte Hotspot-Anmeldung, wie oben beschrieben, nicht genutzt werden kann, wenn der Medientyp Mobilfunk für die automatische Medienerkennung zugelassen ist und die letzte VPN-Verbindung über ein Mobilfunknetz hergestellt wurde bzw. sich der Client im Seamless Roaming befindet.

Hotspot-Verbindung ohne WLAN-Automatik

Sofern der Benutzer nicht dem Link des Assistenten im Monitor des Clients folgt, sondern den WLAN Manager des Clients direkt verwendet, kann er bei Bedarf auch eine Verbindung zum WLAN einschließlich der Hotspot-Anmeldung herstellen, ohne dass im Anschluss die VPN-Verbindung gestartet wird.

Externes WLAN-Tool

Wenn in der WLAN-Konfiguration die Verwendung des WLAN-Managements (siehe oben) nicht aktiviert ist, muss das WLAN-Tool eines anderen Herstellers verwendet werden (z.B. Microsoft).

In diesem Fall wird im Verbindungsmenü des Clients der Menüpunkt Hotspot-Anmeldung eingeblendet. Wird dieser Menüpunkt selektiert, so erfolgt wenn nötig eine Schlüsselabfrage, bevor ein eigenes Browser-Fenster für die Eingabe der Zugriffsdaten geöffnet wird.

Verbindungen

Ist als Verbindungsmedium WLAN ausgewählt, so wird unter dem Menüpunkt "Konfiguration / WLAN" zunächst die Rubrik "Verbindungen" geöffnet.

Wird diese "WLAN-Konfiguration aktiviert", so muss das Management-Tool der WLAN-Karte bzw. das Microsoft-Tool deaktiviert werden. (Alternativ kann auch das Management-Tool der WLAN-Karte oder das Microsoft-Tool genutzt werden, dann müssen die jeweils nicht eingesetzten deaktiviert werden.)

Adapter

Sofern ein mehr als ein WLAN-Adapter installiert ist, wird dieser angezeigt. Bei mehreren Adaptern kann hier der gewünschte selektiert werden.

WLAN-Zugriffspunkte

Nach einem automatischen Scan-Vorgang von wenigen Sekunden werden die derzeit verfügbaren Netze mit den Daten zu SSID, Signalstärke, Verschlüsselung und Profil angezeigt.

Existiert zu einer SSID noch kein Profil, wie nach einer Erstinstallation des Clients, so kann dieses nach einem Doppelklick auf die SSID mit Hilfe eines Assistenten in zwei Schritten erstellt werden (siehe unten WLAN-Profil).

SSID / Signal / Verschlüsselung / Profile

Der Name für die SSID (Standard Security) wird vom Netzbetreiber vergeben und unter dem grafischen Feld des Monitors wie auch im Tray Icon angezeigt. Die SSID wird nach einem Doppelklick auf das zu wählende Netz automatisch in ein WLAN-Profil für diesen Adapter übernommen wenn zu diesem Netz noch kein Profil erstellt wurde.

Die Signalstärke des WLANs wird grafisch dargestellt.

Die jeweilige Verschlüsselung (WEP, WPA, WPA2, WPA3) wird hinter dem Verschlüsselungssymbol dargestellt.

Ist bereits ein Profil vorhanden wird es mit einem Stern symbolisiert. Ist dieses Profil für die WLAN-Automatik vorbestimmt, ist der Begriff "Auto" am Stern platziert.

WLAN-Profil

Zur automatisierten Erstellung eines WLAN-Profiles führen Sie einen Doppelklick auf die SSID aus. Dem daraufhin geöffneten WLAN-Assistenten teilen Sie im ersten Schritt nur der Schlüssel mit (den Sie von der Access Point-Verwaltung erhalten haben).

Die zweite Frage des Assistenten gibt Ihnen die Möglichkeit dieses WLAN-Profil zu einer später zu konfigurierenden WLAN-Automatik (siehe unten) hinzuzufügen. (Unabhängig von der Zuordnung zur WLAN-Automatik wird nach einem Mausklick auf "Fertigstellen" sofort versucht die Verbindung zum Access Point herzustellen.)

Nachdem die Verbindung zum Access Point aufgebaut wurde, kann ein Klick auf den Menüpunkt "Trennen" im Tray Icon (über der Liste der SSIDs) die WLAN-Verbindung wieder abbauen.

WLAN-Automatik

Wurden mehrere Profile mit der Verbindungsart "automatisch" angelegt und wird diese Funktion aktiviert, so wird zunächst das zuletzt selektierte Profil für einen möglichen Verbindungsaufbau herangezogen. Ist die SSID nicht passend, sodass mit diesem Profil keine Verbindung zum Access Point hergestellt werden kann, so werden anschließend die als "automatisch" konfigurierten Profile in der konfigurierten Reihenfolge für den Verbindungsaufbau herangezogen und das erste mit der passenden SSID verwendet. (Beachten Sie dazu auch die Beschreibung unter Profile.)

Auf unbekannte offene Netze hinweisen

Wenn diese Funktion aktiviert ist, werden auch Netze ohne Verschlüsselung angezeigt, die für eine Hotspot-Anmeldung verwendet werden können. Eine entsprechende Meldung wird neben dem Tray Icon angezeigt.

Profile [WLAN]

Bereits erstellte Profile werden in einer Liste dargestellt. Die für die WLAN-Automatik vorbereiteten Profile sind mit einem Haken markiert. Mit den grünen Pfeiltasten können selektierte Profile verschoben werden. Die WLAN-Automatik arbeitet immer die Liste von oben nach unten ab, bis mit einem Profil eine Verbindung zum Access Point hergestellt werden kann. Soll ein Profil, das noch nicht für die Automatik angelegt wurde in die Liste für die WLAN-Automatik aufgenommen werden, so muss dessen Konfiguration mit Doppelklick oder über den Bearbeiten-Button geöffnet werden und "automatisch verbinden" eingestellt werden.

Ein neues Profil wird erzeugt, indem der Button "Neu" gedrückt wird oder im vorigen Fenster auf das zugehörige Netz ein Doppelklick ausgeübt oder die rechte Maustaste geklickt wird.

Über die entsprechenden Buttons können Profile auch bearbeitet oder gelöscht werden.

Allgemeine Profil-Einstellungen

Name

Der Name kann frei vergeben werden und ist bei einer neuen Profilerzeugung nach Doppelklick auf das gescannte Netz zunächst identisch mit der SSID dieses Netzes.

SSID

Die SSID wird automatisch eingetragen, wenn sie gescannt werden kann. Die SSID muss bei verborgenen Netzes manuell eingetragen werden.

Energie-Modus

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

Automatisch verbinden

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

SSID ist verborgen

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

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

Trennen bei VPN-Verbindungsabbau

Durch Setzen dieser Option wird die Sicherheit im Hotspot-Umfeld erhöht.

Getaktete Verbindung

Wird bei einem Medienwechsel der VPN-Tunnel nicht mehr über LAN sondern über eine mobile Datenleitung aufgebaut, wodurch Verbindungskosten entstehen, so kann dies dem Server mitgeteilt werden. Dazu wird in der Profileinstellung für WLAN die Parametereinstellung „getaktete Verbindung“ aktiviert. (Standard: deaktiviert)

Zur besseren Verwaltung der kostenpflichtigen Verbindung, erhält der Client beim Tunnelaufbau vom Server eine IP-Adresse aus einem dafür angelegten Pool für Clients mit Mobilfunkanbindung.

Dies erfolgt auch dann, wenn das Client-System die Mobilfunkverbindung nicht direkt herstellt, sondern über WLAN mit einem LTE-Router verbunden ist, welcher die Mobilfunkverbindung aufbaut.

Wird die Einstellung für "Getaktete Verbindung" geändert, so muss eine eventuell bestehende WLAN-Verbindung zu einem Access Point getrennt und erneut aufgebaut werden, sonst wird die Konfigurationsänderung nicht aktiv.

Verschlüsselung [WLAN-Profil]

Der Verschlüsselungsmechanismus wird vom Access Point (WLAN Router) vorgegeben und über den Administrator mitgeteilt.

Für die WPA-Verschlüsselung kann die Option „EAP“ hinzugefügt werden, vorausgesetzt, es wurde ein Zertifikat konfiguriert. Unabhängig von der EAP-Konfiguration wird hier immer EAP mit Zertifikat genutzt.

Konfiguration eines WLAN-Profiles mit 802.1x-Authentifizierung

Hinweis

Die Absicherung einer WLAN-Verbindung ist mit Hilfe einer 802.1x-Authentifizierung möglich. Ziehen Sie für die Voraussetzungen und Einrichtung dieser die Microsoft-Dokumentation zu Rate.

Beachten Sie, dass die für die Authentifizierung notwendigen Zertifikate vor der Konfiguration des WLAN-Profiles in Windows im Zertifikatsspeicher abgelegt sein müssen. Das Ausstellerzertifikat der Gegenstelle (etwa des WLAN-Accesspoints) sollte bei den "Vertrauenswürdigen Stammzertifizierungsstellen" im Computer-Zertifikatsspeicher abgelegt werden. Das Zertifikat, mit dem sich der Rechner authentisiert, kann je nach Wunsch ein Benutzerzertifikat oder ein Computerzertifikat sein und wird unter "Eigene Zertifikate" im Benutzer- bzw. Computer-Zertifikatsspeicher abgelegt.

Die Zertifikatskonfiguration des Clients ist über den NCP WLAN-Manager möglich.

Um eine 802.1x-Authentifizierung in einem WLAN-Profil zu konfigurieren, gehen Sie wie folgt vor:

1. Klicken Sie im Client Interface auf *Konfiguration* und wählen Sie die Option *WLAN*.
2. Erstellen Sie im Reiter *Profile* über *Hinzufügen* ein neues WLAN-Profil oder öffnen Sie ein bestehendes Profil.
3. Wählen Sie den Reiter *Verschlüsselung*. Bestimmen Sie unter *Verschlüsselung* für dieses Profil eine WPA-Verschlüsselung (WPA3, WPA2 oder WPA) und unter *Schlüssel-Verwaltung* den Schlüssel EAP.
4. Über die *Zertifikatsauswahl* wählen Sie Ihr gewünschtes Zertifikat aus. Außerdem können Sie hier die Smartcard- oder Zertifikatseigenschaften selektieren.
5. Mit Klick auf *OK* übernehmen Sie die Konfigurationen.

IP-Adressen [WLAN-Profil]

In diesem Fenster wird die IP-Adress-Konfiguration der WLAN-Karte vorgenommen.

Die hier gemachten Einstellungen werden dann wirksam, wenn die WLAN-Konfiguration wie oben beschrieben aktiviert wurde. In diesem Fall wird die hier eingetragene Konfiguration in die Microsoft-Konfiguration der Netzwerkverbindungen übernommen. (Siehe dort: Netzwerkverbindungen / Eigenschaften von Internetprotokoll (TCP/IP)).

Authentisierung [WLAN-Profil]

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

Die Authentisierung kann durch Eintragen von Benutzername und Passwort an der Eingabemaske des Hotspot-Betreibers erfolgen oder über Script. Das Script automatisiert die Anmeldung beim Hotspot-Betreiber.

Beachten Sie dabei, dass die Verbindung über einen Hotspot-Betreiber gebührenpflichtig ist. Sie müssen den Geschäftsbedingungen des Hotspot-Betreibers zustimmen, wenn die Verbindung aufgebaut werden soll.

Keine Authentisierung am Hotspot

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

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

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

Authentisierung am Hotspot

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

Authentisierung mit Script

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

Anderer

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

Script-Dateiname

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

* (Scripte werden auf Anfrage vom Support erstellt. Ein Script wird im Installationsverzeichnis unter eingespielt.)

Benutzername / Passwort

Benutzername und Passwort werden entsprechend der Provider-Vorgaben eingegeben.

T-Mobile

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

Benutzername / Passwort

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

WISPr-Anmeldung

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

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

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

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

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

Optionen [WLAN-Profil]

WLAN bei gestecktem LAN-Kabel ausschalten

Mit Hilfe der Funktion wird mobilen Teleworkern ein manuelles Umschalten erspart. Sobald ein Teleworker, der über WLAN mit dem Firmennetz verbunden ist, inhouse das LAN-Kabel in sein Notebook steckt, wird der WLAN-Adapter deaktiviert und die LAN-Verbindung ins Firmennetz genutzt.

Dies erfolgt unabhängig davon, ob er den WLAN-Manager des Clients oder den eines fremden Herstellers benutzt. Wird das LAN-Kabel wieder gezogen, wird auch der WLAN-Adapter wieder aktiviert.

Aktiviere Hotspot/WLAN-Erkennung

Wird dieser Schalter aktiv gesetzt und besteht für den mobilen Client aktuell keine Internetverbindung, obwohl ein WLAN-Netzwerk verfügbar ist, so wird dies erkannt und im Monitor über dem WLAN Panel eine entsprechende Meldung eingeblendet:

„Es stehen WLAN-Netze zur Verfügung. Klicken Sie hier um sich zu verbinden.“

Mit einem Klick wird der Verbindungsaufbau eingeleitet, indem der WLAN-Manager gestartet wird (siehe WLAN Management).

Das WLAN-Profil, das für die Verbindung selektiert wird, wird unmittelbar für "automatisches Verbinden" in der Liste des WLAN-Managers gespeichert (auch ein bisher unbekanntes WLAN) und die Verbindung zum Access Point des WLAN wird hergestellt.

Ist eine weitere Anmeldung am WLAN erforderlich, wird automatisch ein Browser-Fenster für die Eingabe der Benutzerdaten eingeblendet.

(Bei einem verschlüsselten WLAN wird zudem der Schlüssel abgefragt, sofern es sich um ein bislang unbekanntes WLAN handelt, dessen Daten noch nicht im WLAN-Profil gespeichert sind.)

Sobald der Zugriff auf das Internet nach Anmeldung am Hotspot und/oder der Herstellung einer verschlüsselten Verbindung zum Access Point erfolgen kann, wird automatisch die VPN-Verbindung aufgebaut.

Statistik

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

Zertifikate [Konfiguration]

Hier wird festgelegt, ob Zertifikate zur Authentisierung des Clients eingesetzt werden und wo die Benutzer-Zertifikate hinterlegt werden.

In weiteren Konfigurationsfeldern werden die Richtlinien zur PIN-Eingabe festgelegt und das Zeitintervall eingestellt innerhalb dessen das Zertifikat abläuft bzw. eine Zertifikatsverlängerung beantragt werden muss.

Einstellungen zu folgenden Parametern können vorgenommen werden:

[Benutzer-Zertifikat](#)  99
[PIN-Richtlinie](#)  103
[Zertifikatsverlängerung](#)  103
[Computer-Zertifikat](#)  103

Name und "Standard Zertifikatskonfiguration"

Pro Secure Client kann eine Vielzahl von Zertifikatskonfigurationen unter einem jeweils eigenen Namen hinterlegt werden.

Die Zertifikatskonfiguration eines Clients älter als Version 9.1 wird bei einem Update auf diese Version automatisch in die "Standard Zertifikatskonfiguration" konvertiert. Ebenso wird die "Standard Zertifikatskonfiguration" nach einer Erstinstallation der Version 9.1 eingerichtet wenn eine Testverbindung mit Zertifikat angelegt wird.

Aus den verschiedenen Zertifikatskonfigurationen kann pro Profil jeweils eine selektiert werden. Dadurch besteht die Möglichkeit unterschiedlicher Authentisierung mit verschiedenen Zertifikaten gegen verschiedene VPN-Gegenstellen. Z. B. zu VPN Gateway 1 mit Softzertifikat und zu Gateway 2 mit einem auf Token gespeicherten Zertifikat.

Im Konfigurationsfeld Identität kann das Zertifikat für die erweiterte Authentisierung (Extended Authentication) selektiert werden.

Benutzer-Zertifikat [Konfiguration]

Zertifikat

Hier bestimmen Sie ob Sie Zertifikate und damit die erweiterte Authentisierung nutzen wollen, und wo Sie die Zertifikate hinterlegen wollen.

ohne:

Wählen Sie in der Listbox "Zertifikat" die Einstellung "ohne", so wird kein Zertifikat ausgewertet und die erweiterte Authentisierung findet nicht statt.

aus PKCS#12 Datei:

Wählen Sie "aus PKCS#12 Datei" aus der Listbox, so werden bei der erweiterten Authentisierung die relevanten Zertifikate aus einer Datei auf der Festplatte Ihres Rechners gelesen.

aus Chipkartenleser:

Wählen Sie "aus Chipkartenleser" in der Listbox, so werden bei der erweiterten Authentisierung die relevanten Zertifikate von der Smart Card in ihrem Chipkartenleser ausgelesen.

PKCS#11-Modul:

Wählen Sie "PKCS#11-Modul" in der Listbox, so werden bei der erweiterten Authentisierung die relevanten Zertifikate von der Smart Card in einem Chipkartenleser oder von einem Token gelesen.

CSP Benutzer-Zertifikatsspeicher:

Wählen Sie den "CSP Benutzer-Zertifikatsspeicher" in der Listbox, so wird zur erweiterten Authentisierung das Zertifikat aus dem CSP Benutzer-Zertifikatsspeicher verwendet, dessen "Benutzer CN" (Subject CN) und "Aussteller CN" (Issuer CN) Sie in die entsprechenden Felder eintragen.

Der Client unterstützt an dieser Stelle die Eingabe von Umgebungsvariablen des Systems, um eine genauere Zertifikatsauswahl zu treffen.

Beachten Sie folgendes zu den Variablen:

- Mehrere Variablen können so eingefügt werden: %Variable% / %Variable%
- Kann eine Variable nicht aufgelöst werden, wird sie durch keinen Wert ersetzt.
- Das Auflösen der Variablen erfolgt unmittelbar nach dem Schließen des Konfigurationsfensters.
- Wird ein alleinstehendes Prozentzeichen vorangesetzt, werden alle darauffolgenden Variablen ignoriert.
- Doppelte Prozentzeichen werden nicht wie ein einzelnes Prozentzeichen unterstützt, bzw. erzeugen sie keins.
- Wird eine neue Konfiguration in den Client importiert, werden diese Einträge beim Einlesen einer neuen Konfiguration ersetzt und hier eingetragen.

Der Subject- bzw. Issuer-Name ist der komplette X.500 Name, einzelne Elemente werden mit Komma getrennt. Hier einige Beispiele für X.500 Namen in Zertifikaten:

```
CN=NCP engineering GmbH, OU=Digital ID Class 3 - Microsoft Software Validation v2,  
O=NCP engineering GmbH, L= Nuernberg, S=Bavaria, C=DE  
  
CN=VeriSign Class 3 Code Signing 2009-2 CA, OU=Terms of use https:\  
\verisign.com\rpa (c)09, OU=VeriSign Trust Network, O="VeriSign,Inc.",  
C=US CN=NCP Demo CA 1, O=NCP, S=Bayern, C=DE, S=Bayern, L=Nuernberg, O=NCP,  
OU=ou3, OU=ou2, OU=ou1, E=123456.de, SN=F, G=T, CN=TF
```

Hinweis

Die einzelnen Elemente werden nicht sortiert, sondern in der Reihenfolge wie sie im Zertifikat stehen ausgegeben.

Chipkartenleser:

Wenn Sie die Zertifikate von der Smart Card mit Ihrem Lesegerät nutzen wollen, wählen Sie Ihren Chipkartenleser aus der Listbox. (Siehe auch PIN eingeben)

Die Client Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind. Die Client Software erkennt dann den Chipkartenleser nach einem Boot-Vorgang automatisch. Erst dann kann der installierte Leser ausgewählt und genutzt werden.

Port:

Der Port wird bei korrekter Installation des Lesegeräts automatisch bestimmt. Bei Unstimmigkeiten können die COM Ports 1-4 gezielt angesteuert werden.

Auswahl Zertifikat:

1. Zertifikat ... 4.:

(Standard = 1) Aus der Listbox kann aus verschiedenen Zertifikaten gewählt werden, die sich auf der Chipkarte befinden. Die Anzahl der Zertifikate auf der Chipkarte ist abhängig von der Registration Authority, die diese Karte brennt. Unterstützt werden folgende Typen:

Telesec TCOS 3.0 Signature Card 2.0

Atos 5.0 und 5.3 Chipkarten

Andere als die hier genannten können nur über die CSP- oder PKCS11-Schnittstelle verwendet werden.

Wenden Sie sich zu weiteren Fragen bitte an Ihren Systemadministrator.

PKCS#12-Dateiname:

Nutzen Sie das PKCS#12-Format, so erhalten Sie von Ihrem Systemadministrator eine Datei, die auf der Festplatte Ihres Rechners eingespielt werden muss. In diesem Fall muss Pfad und Dateiname der PKCS#12 Datei eingegeben, bzw. nach einem Klick auf den [...] -Button (Auswahl-Button) die Datei ausgewählt werden.

Wichtig: Der Pfad für den Dateinamen kann mit der Variablen %CertDir% (für das Verzeichnis der Benutzer-Zertifikate) abgekürzt werden. Z. B.:

%CertDir%/Test.p12

PKCS#11-Modul:

Nutzen Sie das PKCS#11-Format, so erhalten Sie eine DLL vom Hersteller des Chipkartenlesers oder des Tokens, die Sie lokal auf Ihrem PC speichern müssen.

Geben Sie zur Verwendung des PKCS#11-Moduls hier den entsprechenden Pfad und Dateinamen der Programmbibliothek ein.

Hinweis

Beachten Sie, dass PKCS#11-Module aus Sicherheitsgründen nur geladen werden, wenn sie sich unterhalb des Windows-Hauptordners WINDIR oder eines der Standardprogrammverzeichnisse PROGRAMFILES / PROGRAMFILES (x86) befinden.

Ist es dennoch erforderlich, einen alternativen Speicherort zu verwenden, kann dies durch den folgenden Registry-Eintrag unter Angabe des entsprechenden Verzeichnisses in dem Platzhalter P11DllPath auf dem lokalen PC aktiviert werden:

HKLM\\Software\\NCP engineering GmbH\\NCP Secure Client\\P11DllPath.

Es wird empfohlen, dass das verwendete Verzeichnis nur mit Administratorberechtigung beschrieben werden kann.

Sie können auch mit Hilfe eines Assistenten nach installierten PKCS#11-Modulen suchen und das gewünschte Modul mit dem dazugehörigen Slot selektieren. Dazu klicken Sie auf den Button in der Zeile mit PKCS#11-Modul.

CSP Benutzer-Zertifikatsspeicher:

Wählen Sie den "CSP Benutzer-Zertifikatsspeicher" in der Listbox, so wird zur erweiterten Authentisierung das Zertifikat aus dem CSP Benutzer-Zertifikatsspeicher verwendet, dessen "Benutzer CN" und "Aussteller CN" Sie in die entsprechenden Felder eintragen.

Da diese Funktionalität erst nach einer Anmeldung des Benutzers am Windows-System zur Verfügung steht, kann sie nicht zur Domänenanmeldung über VPN eingesetzt werden (siehe Computer-Zertifikat).

Erweiterte Schlüsselverwendung:

Anhand der Erweiterten Schlüsselverwendung (Extended Key Usage) kann die Auswahl eines bestimmten Benutzer- oder Computer-Zertifikats für Authentisierung oder Verschlüsselung voreingestellt werden.

Kein Verbindungsabbau bei ziehen der Chipkarte:

Diese Option besteht immer dann, wenn ein Chipkartenleser oder ein PKCS#11-Modul verwendet wird.

PIN-Abfrage bei jedem Verbindungsaufbau:

Standardeinstellung: Wird diese Funktion nicht genutzt, so wird die PIN nur einmalig beim ersten Verbindungsaufbau des Clients abgefragt.

Wird diese Funktion aktiviert, so wird bei jedem Verbindungsaufbau die PIN erneut abgefragt.

Soft-Zertifikatsauswahl

PC-Sharing (Nutzung mehrerer Soft-Zertifikate an einem Client-PC)

Soll ein PC-Sharing für mehrere Benutzer, die jeweils ein eigenes Zertifikat einsetzen, eingerichtet werden, so kann dazu eine Konfiguration vorgenommen werden.

Unter "Benutzer-Zertifikat" muss der Menüpunkt "Softzertifikatsauswahl aktivieren" eingeschaltet werden und ein "Zertifikatspfad" angegeben werden. Dieser Pfad kann über den Auswahl-Button gewählt werden, wenn er vorher angelegt wurde. (Z. B. %CertDir%). Unter diesem Pfad müssen anschließend die verschiedenen Benutzer-Zertifikate abgelegt werden.

Werden diese Einstellungen mit "OK" gespeichert, so erscheint unter dem grafischen Feld des Monitors die Zertifikatsleiste mit der Liste aller unter dem Zertifikatspfad gespeicherten Benutzer-Zertifikaten (z. B. user1 bis user4).

Hat der Benutzer sein Soft-Zertifikat ausgewählt (z. B. user2) und stellt eine Verbindung zum zentralen VPN Gateway her, so muss er zunächst seine PIN eingeben. Danach wird die Verbindung zum Zielsystem aufgebaut.

Verlässt der Benutzer den Arbeitsplatz, so sollte er den Button mit "Abmelden" betätigen. Dadurch wird die Verbindung vollständig abgebaut und die PIN zurück gesetzt (dies geschieht auch, wenn bei einer bestehenden Verbindung ein anderes Zertifikat ausgewählt wird). Findet keine Abmeldung statt, können nicht berechtigte Benutzer über die bestehende Verbindung Zugang zum VPN Gateway erhalten!

Ein nachfolgender Benutzer geht genauso vor. Zunächst wählt er sein Zertifikat aus, klickt anschließend die Funktion "Verbinden" und gibt seine PIN ein. Erst dann kann die Verbindung korrekt aufgebaut werden. Wird der Arbeitsplatz verlassen, klickt der Benutzer den Button mit "Abmelden".

Softzertifikatsauswahl aktivieren

Diese Funktion wird nur für PC-Sharing benötigt, wenn mehrere Benutzer des PCs mit verschiedenen Soft-Zertifikaten arbeiten.

Zertifikatspfad

Verschiedene Soft-Zertifikate für mehrere Benutzer dieses PCs können unter diesem Pfad gespeichert werden.

PIN-Richtlinie

Minimale Anzahl der Zeichen

Standard ist eine 6-stellige PIN. Aus Sicherheitsgründen werden 8 Stellen empfohlen.

Weitere Richtlinien

Es wird empfohlen alle PIN-Richtlinien einzusetzen, außer der, dass nur Zahlen enthalten sein dürfen. Zudem sollte die PIN nicht mit einer Zahl beginnen.

Die vorgegebenen Richtlinien werden eingeblendet, wenn die PIN geändert wird und die Richtlinien, die bei der Eingabe erfüllt werden, werden grün markiert (siehe: PIN ändern).

Zertifikatsverlängerung

In diesem Konfigurationsfeld kann eingestellt werden, ob und wie viele Tage vor Ablauf der Gültigkeit des Zertifikats eine Meldung ausgegeben werden soll, die vor dem Ablauf der Gültigkeit warnt. Sobald die eingestellte Zeitspanne vor Ablauf in Kraft tritt, wird bei jeder Zertifikatsverwendung eine Meldung aufgeblendet, die auf das Ablaufdatum des Zertifikats hinweist.

Computer-Zertifikat

Damit die zusätzliche Authentisierung mit einem Computer-Zertifikat genutzt werden kann, muss am Gateway die Option "Computer-Zertifikat CN" unter Link-Profile eingeschaltet werden.

Mit einem Computer-Zertifikat authentisiert sich der Rechner gegenüber dem Gateway. Wird es zusätzlich zu einem Benutzer-Zertifikat eingesetzt, so kann sichergestellt werden, dass sich der Benutzer immer vom gleichen Rechner aus einwählt.

Verbindungsoptionen [Konfiguration]

Unter den "Verbindungsoptionen" kann der Budget-Manager konfiguriert werden und in Abhängigkeit vom Client Monitor Anwendungen oder Batch-Dateien gestartet werden.

Siehe auch:

[Budget-Manager \[Konfiguration\]](#)  105

[Externe Anwendungen](#)  109

[Optionen \[Mobilfunk\]](#)  110

Budget-Manager [Konfiguration]

Funktionen des Budget Managers

Der Budget Manager ist Bestandteil der Verbindungssteuerung des Clients und dient in erster Linie der persönlichen Selbstkontrolle. Er misst und überwacht das Datenvolumenaufkommen während einer bestimmten Zeitspanne, oder der aufgelaufenen Online-Dauer innerhalb dieser Zeitspanne (z. B. innerhalb eines Monats), sofern die Verbindungen über eine Medienart aufgebaut wurde, die vom eigenen Dialer unterstützt wird. Sofern vom Administrator keine Parametersperren in der Client Software gesetzt sind, kann der Anwender die Budget-Limits selbst setzen.

Sollte ein Limit überschritten werden und danach kein Verbindungsaufbau mehr möglich sein, muss sich der Anwender mit seinem Administrator verständigen, sofern Parametersperren gesetzt sind. Die Parametersperren müssen aufgehoben werden; erst danach kann der Anwender eine neue Konfiguration durchführen.

Siehe auch:

[Einstellungen \[Budget-Manager\]](#)  106

[Aktionen \[Budget-Manager\]](#)  106

[Mobilfunknetz \[Budget-Manager\]](#)  107

[WLAN-Zugriffspunkte \[Budget-Manager\]](#)  107

Einstellungen [Budget-Manager]

Budget-Limitierung nach Volumen oder Online-Dauer

Die entsprechenden Einstellungen, ob Datenvolumen oder Online-Dauer während eines Monats oder eines anderen festzulegenden Zeitraums gemessen werden sollen, können über das Monitormenü "Konfiguration / Verbindungssteuerung" vorgenommen werden.

Für alle vom eigenen Dialer unterstützten Verbindungsmedien, kann je nach Abrechnungsart separat bestimmt werden, ob das (monatliche) Verbindungsvolumen oder die Verbindungsdauer gemessen werden sollen. So kann für WLAN oder für das Mobilfunknetz eine maximale Verbindungsdauer bzw. ein maximales Verbindungsvolumen pro Monat vorgegeben werden.

Kleinere Budgets für mobile Computing

Steht ein begrenztes Budget für einen begrenzten Zeitraum zur Verfügung, zum Beispiel für die Zeit eines Hotelaufenthalts, so kann der Startzeitpunkt manuell gesetzt werden. Dazu wird die Statistik über das Monitormenü "Verbindung" geöffnet und für die ausgewählte Verbindungsart der Reset-Button gedrückt. Damit wird der Startzeitpunkt festgesetzt, ab dem vom vorgegebenen Budget abgebucht wird. (Ein nochmaliges Drücken des Reset-Buttons startet die Verbindungskontrolle erneut mit gleichen Vorgaben und löscht die bisherigen Aufzeichnungen.)

Aktionen [Budget-Manager]

Budget-Statistik und automatisierte Warnungen

Einen Überblick über sein (monatliches) Budget erhält der Anwender in der Statistik der Verbindungssteuerung. Die Statistik zeigt mit dem aktuellen Datum, wie viel des maximal auserschöpfenden 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 Aktionen werden wie die Verbindungskontrolle für jedes Medium einzeln festgelegt. So kann ab einem prozentualen Verbrauch des festgesetzten Verbindungsvolumens oder der maximalen Verbindungszeit eine Warnung ausgegeben werden, die darauf aufmerksam macht, dass das Budget bald ausgeschöpft ist. Oder es werden nach Ausschöpfen des Budgets keine Verbindungen mehr für diesen Monat zugelassen.

Wächst die Budget-Anzeige in der Statistik deutlich schneller als der Balkenanzeige für den Kalender, so ist das zugewiesene Budget nicht ausreichend. Die Budget-Anzeige färbt sich nach dem Erreichen des Warnbereichs gelb, nach dem Erreichen des maximalen Werts rot. Wird der Verbindungsaufbau nach Überschreiten des Maximalwerts nicht mehr zugelassen, erscheint im Client-Monitor eine Meldung.

Mobilfunknetz [Budget-Manager]

Kostspieliges Roaming vermeiden

Für den Medientyp Mobilfunknetz wird die Verbindungskontrolle getrennt für Inlands- und Roaming-Verbindungen aktiviert. Unnötiges Roaming bei Mobilfunknetz-Verbindungen z. B. in Grenzgebieten kann weitgehend ausgeschlossen werden durch gezielte Sicherheitsabfragen. So können Listen von zulässigen Inlands-Netzbetreibern und zulässigen Roaming-Netzbetreibern erstellt werden, die auf komfortable Weise erlauben, den jeweils günstigsten auszuwählen oder unerwünschte Provider von vorne herein auszuschließen.

Inlands-Netzbetreiber und Roaming-Netzbetreiber

Ebenso wie die Verbindungskontrolle getrennt für Inlandsverbindungen und Roaming-Verbindungen aktiviert wird, werden auch getrennte Listen für zulässige Inlands-Netzbetreiber und Roaming-Netzbetreiber geführt. Über diese Listen, die in den Einstellungen "Allgemein" geführt werden, wird die Provider-Auswahl automatisiert. Jeder Provider, den der Anwender über die automatische Netzbetreiber-Verwaltung oder manuell in eine der Listen unter Inland oder Roaming eingetragen hat, wird für einen Verbindungsaufbau genutzt, sobald ihn das System erkennt. Bislang unbekannte Provider werden entsprechend der Einstellung für unzulässige Netzbetreiber behandelt.

Automatische Netzbetreiber-Verwaltung

Wird die automatische Netzbetreiber-Verwaltung aktiviert, so wird der Anwender bei jedem neuen Provider, der dem System noch nicht über seine Listen bekannt ist, gefragt, in welche Liste der neue Provider aufgenommen werden soll: in die Liste der Inlands-Netzbetreiber, in die der Roaming-Netzbetreiber oder in die der abzuweisenden unzulässigen Netzbetreiber. Die Liste der abzuweisenden Netzbetreiber kann unter "Erweiterung" jederzeit bearbeitet werden, um einen Provider z. B. daraus zu löschen und in eine andere Liste aufzunehmen.

Wird die automatische Netzbetreiber-Verwaltung nicht benutzt, so wird ein Provider, den das System noch nicht kennt wie ein unzulässiger Netzbetreiber behandelt und der Verbindungsaufbau über diesen Provider gemäß der Optionen für unzulässige Netzbetreiber unter den Einstellungen "Allgemein" vorgenommen.

WLAN-Zugriffspunkte [Budget-Manager]

Verbindungskontrollen für einzelne WLAN-Profile

Für jedes WLAN-Profil, das im Monitormenü „Konfiguration“ konfiguriert wurde kann eine eigene Verbindungskontrolle eingerichtet werden. Dazu wird die SSID aus dem jeweiligen WLAN-Profil in die Verbindungssteuerung für die WLAN-Netze übertragen. Die Verbindungskontrolle kann für jedes WLAN-Profil einzeln über die Einstellungen oder für mehrere in der Übersicht unter WLAN aktiviert werden.

Externe Anwendungen

Funktionen

Nachdem Sie die Funktion "Externe Anwendungen oder Batch-Dateien starten" selektiert haben, können Sie über den Button mit "Hinzufügen" eine Anwendung oder Batch-Datei vom Rechner selektieren, die je nach Startoption geladen wird:

- vor Verbindungsaufbau starten (precon)
- nach Verbindungsaufbau starten (postcon)
- nach Verbindungsabbau starten (discon)

Wollen Sie nach dem Verbindungsaufbau den Standard-Browser starten, so aktivieren Sie diese Funktion und tragen die Website des Browsers ein.

Zusätzlich können diese auszuführenden Anwendungen auch an ein bestimmtes Profil gebunden werden. Dieses Profil kann aus der Liste der bereits verfügbaren Profil-Einstellungen selektiert werden, nachdem Sie den Button mit "Hinzufügen" oder "Bearbeiten" angeklickt haben.

Achten Sie darauf, dass in dem Namen des selektierten Profils kein Komma vorkommt! Die Funktion schlägt fehl und die externe Anwendung wird nicht gestartet, wenn im Profilnamen Kommas vorkommen!

Ausführung von "(dis)connect.bat" nicht zulassen

Diese Funktion sollte immer aktiviert sein

- wenn nicht unbedingt für eine gewünschte Anwendung die Ausführung der genannten Batch-Dateien mit Administrator-(System-)Rechten erforderlich ist.

Die Anwendungen (Batch-Dateien) für deren Ausführung Benutzerrechte genügen, können im Monitormenü "Externe Anwendungen ..." gestartet werden (siehe oben).

Optionen [Mobilfunk]

Mobilfunk bei gestecktem LAN-Kabel ausschalten

Mit Hilfe dieser Funktion wird mobilen Teleworkern ein manuelles Umschalten erspart. Sobald ein Teleworker, der über Mobilfunk mit dem Firmennetz verbunden ist, inhouse das LAN-Kabel in sein Notebook steckt, wird der LTE/UMTS-Adapter deaktiviert und die LAN-Verbindung ins Firmennetz genutzt.

Wird das LAN-Kabel wieder gezogen, wird auch der LTE/UMTS-Adapter wieder aktiviert.

Mobilfunk bei bestehender WLAN-Verbindung ausschalten

Sobald ein Teleworker, der über Mobilfunk mit dem Firmennetz verbunden ist, eine Verbindung zum Firmennetz über WLAN nutzen kann, wird der LTE/UMTS-Adapter deaktiviert.

Geht die WLAN-Verbindung verloren, wird statt dessen die Verbindung über den LTE/UMTS-Adapter wieder aktiviert.

Logon-Optionen

Das Menü der Logon-Optionen dient dazu, Einstellungen für den Tunnelaufbau zu einer Windows-Domäne vor einer Benutzeranmeldung vornehmen zu können. Dazu muss die Anmeldeoption [Dialog für Verbindungsaufbau vor der Windows-Anmeldung anzeigen](#)^[112] im Konfigurationsfeld [Anmelden](#)^[112] zunächst initialisiert werden.

Weitere Konfigurationsoptionen stehen nach der Aktivierung dieser Funktion unter [Ext. Anwendungen](#)^[114] und [Optionen](#)^[115] zur Verfügung.

Beachten Sie hierzu auch die Funktionsbeschreibung zum [Credential Provider](#)^[213].

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 (Credential Provider) 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.

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 (Credential Provider) übergibt.

Für das Windows Logon kann auch der "VPN-Benutzername als Benutzername" verwendet werden, welcher in der Profil-Einstellung unter "Identität" eingetragen wurde. Gleiches gilt für das "VPN-Passwort als Passwort" für die Windows-Anmeldung.

Ist in der Profil-Einstellung unter "Identität" definiert, dass die VPN-Zugangsdaten (VPN-Benutzername und VPN-Passwort) aus einem Feld des eingesetzten Zertifikats gelesen werden, so wird diese Einstellung automatisch auch für die Windows-Anmeldung verwendet. Alternativ können für die Windows-Anmeldung auch eigene Zugangsdaten eingesetzt werden.

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.

Beim Abmelden trennen

Mit Aktivierung dieser Funktion wird die Verbindung bei Eintreten des Standby-Modus (oder Hibernation) getrennt. Nach der Rückkehr aus dem Standby-Modus muss die Verbindung neu aufgebaut werden. Wenn diese Funktion nicht aktiviert wird, wird die Verbindung über den Standby-Modus hinaus gehalten.

Nach Ruhezustand / Energiesparen die Zugangsdaten aus Cache löschen

Die Eingabe von Benutzername und Passwort muss zwingend immer dann erfolgen, wenn diese Funktion aktiviert ist, da hiermit Benutzername und Passwort aus dem Cache gelöscht werden.

Diese Option ist nur möglich wenn die Zugangsdaten nicht in der Konfiguration hinterlegt sind.

Externe Anwendungen [Logon Optionen]

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

Sicherheitshinweise

Beachten Sie, dass die Anwendungen im *Systemkontext* ausgeführt werden und somit über erhöhte Rechte verfügen. Die Ausführung einer Anwendung, ohne vorherige Anmeldung im *Benutzerkontext*, ist als sicherheitskritisch anzusehen.

Außerdem wird empfohlen, nur Konsolenanwendungen und nichtinteraktive Programme einzusetzen, da sonst weitere Sicherheitsprobleme verursacht werden können (z.B. über das Öffnen des File-Explorers mit erhöhten Rechten).

Die externen Anwendungen werden, wie weiter unten beschrieben, eingefügt. Die Reihenfolge ihres Aufrufs von oben nach unten, kann mit den Pfeiltasten verändert werden.

Anwendung / Batch-Datei

Nach Klick auf *Hinzufügen* kann eine Anwendung oder Batch-Datei selektiert werden (*.com, *.exe, *.bat).

Es stehen nur Dateien zur Auswahl die vorab unter %BaseDataDir%\scripts (Default: C:\ProgramData\NCP\SecureClient\scripts\) abgelegt wurden.

Start-Option

Die Anwendung oder Batch-Datei kann je nach Startoption geladen werden:

- **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 (Credential Provider) und anschließender "lokaler Anmeldung" ohne VPN-Verbindung.

Verbindungsmedium

Die Anwendung kann außerdem in Abhängigkeit von der Verbindungsart des im Logon-Dialog selektierten Zielsystems gestartet werden. Die Applikation wird immer gestartet, wenn als Verbindungsmedium "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]

Vorbereitungszeit

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.

EAP-Authentisierung vor Zielauswahl

Standardmäßig erfolgt die EAP-Authentisierung vor dem Verbindungsaufbau zum 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 die Funktion nicht aktiviert, findet die EAP-Authentisierung erst nach der Zielauswahl statt.

Wird EAP mit Zertifikat eingesetzt, so erscheint der PIN-Dialog zur Authentisierung an den Netzwerkkomponenten. Danach kann die Zielauswahl erfolgen.

Dialog für Verbindungsaufbau automatisch öffnen

Anschließend können Sie wählen, ob Sie den "Dialog für Verbindungsaufbau automatisch öffnen" lassen, um den Verbindungsaufbau zum Gateway anstoßen zu können.

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 eingegeben werden.

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

Beim Anmelden das vorselektierte Icon maximiert darstellen

Hiermit wird ausschließlich das Credential dargestellt.

Konfigurationssperren

Mit Konfigurationssperren lässt sich die Oberfläche des Clients übersichtlicher gestalten.

Zudem kann damit vermieden werden, dass unberechtigte oder zufällige Veränderungen in den Profileinstellungen vorgenommen werden.

Um Konfigurations-Sperren wirksam festlegen zu können, muss "Benutzer" und "Passwort" eingegeben werden. Das Passwort muss anschließend bestätigt werden.

Beachten Sie dazu die Beschreibungen zu folgenden Parameterfeldern:

[Allgemein](#) ¹¹⁶

[Profile](#) ¹¹⁶

[Mobilfunknetz](#) ¹¹⁷

Allgemein [Konfigurationssperren]

ID für Konfigurationssperre

Die Konfigurations-Sperren werden in der definierten Form erst wirksam, wenn die Einstellungen mit "OK" übernommen werden. Wird der "Abbrechen"-Button gedrückt, wird auf die Standard-Einstellung zurückgesetzt.

Um die Konfigurations-Sperren wirksam festlegen zu können, muss eine ID eingegeben werden, die sich aus "Benutzer" und "Passwort" zusammensetzt. Das Passwort muss anschließend bestätigt werden.

Bitte beachten Sie, dass die ID für die Konfigurations-Sperre unbedingt nötig ist, die Sperren wirksam werden zu lassen oder die Konfigurations-Sperren auch wieder aufzuheben. Wird die ID vergessen, besteht keine Möglichkeit mehr, die Sperren wieder aufzuheben!

Berechtigungen für Konfiguration

Anschließend kann festgelegt werden, ob der Anwender die Berechtigung hat, die Menüpunkte unter dem Hauptmenüpunkt "Konfiguration" zu öffnen und zu verändern. Standardmäßig kann der Benutzer alle Menüpunkte öffnen und die Konfigurationen bearbeiten. Wird zu einem Menüpunkt der zugehörige Haken mit einem Mausklick entfernt, so kann der Benutzer diesen Menüpunkt nicht mehr öffnen.

Die Bearbeitungsrechte für die Parameter der [Profile](#) ¹¹⁶ sind in zwei Sparten unterteilt.

Zusätzlich kann noch eine Berechtigung zur Speicherung einer SIM für die [Mobilfunkkarte](#) ¹¹⁷ vergeben werden.

Profile [Konfigurationssperren]

Allgemeine Rechte

Die allgemeinen Rechte beziehen sich nur auf die (Konfiguration der) Profile. Wird festgelegt "Profile dürfen neu angelegt werden", bleibt jedoch "Profile dürfen konfiguriert werden" ausgeschlossen, so

können zwar mit dem Assistenten neue Profile definiert werden, eine nachfolgende Änderung einzelner Parameter ist dann jedoch nicht mehr möglich.

Sichtbare Parameterfelder der Profile

Die Parameterfelder der Profil-Einstellungen können für den Benutzer ausgeblendet werden.

Beachten Sie, dass Parameter eines nicht sichtbaren Feldes auch nicht konfiguriert werden können.

Mobilfunknetz [Konfigurationssperren]

Bei Einsatz einer Mobilfunkkarte kann dem Benutzer gestattet werden, die SIM PIN zu speichern.

In der Standard-Einstellung des Entry Clients ist diese Funktion nicht sichtbar. Sie wird dann für den Benutzer sichtbar und konfigurierbar, wenn ihm hier die Berechtigung dazu erteilt ist, d. h. "Benutzer darf SIM PIN in Konfiguration speichern" aktiviert ist.

Weitere Optionen

Folgende Konfigurations-Optionen stehen zur Verfügung:

[Proxy für VPN Path Finder](#) ¹¹⁸

[EAP-Optionen](#) ¹¹⁹

[FIPS-Unterstützung](#) ¹²⁰

Proxy für VPN Path Finder

Wurde die Funktionalität VPN Path Finder unter [Erweiterte IPsec-Optionen](#) ¹⁸⁵ innerhalb der Konfiguration der Profile aktiviert, und muss der Internet-Verbindung ein Proxy Server vorgeschaltet sein, so können Sie hier den Proxy Server des Systems selektieren oder die Daten für den firmeneigenen Proxy Servers eingeben.

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 Profile. In einer Aktivierungsbox kann die EAP-Authentisierung wie folgt eingestellt werden:

- deaktiviert
- für alle Netzwerkkarten
- nur für WLAN-Karten
- nur für LAN-Karten

Der Einsatz des Extensible Authentication Protocols Message Digest5 (EAP MD5) kann über das Einstellungsmenü des Monitors definiert werden. Dieses Protokoll kann dann zum Einsatz kommen, wenn für den Zugang zum LAN ein Switch oder für das wireless LAN ein Access Point verwendet werden, der 802.1x-fähig ist und eine entsprechende Authentisierung unterstützt. Mit dem Extensible Authentication Protocol (EAP MD5) kann verhindert werden, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.

Zur Authentisierung kann wahlweise der [Benutzername](#)^[190] und das [Passwort](#)^[190] ([Identität](#)^[190]) verwendet werden oder ein eigener "EAP-Benutzername" mit einem "EAP-Passwort".

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%

FIPS

In der Standardeinstellung ist der FIPS-Modus deaktiviert.

Um die für den FIPS-Standard erforderlichen Kryptografie-Module automatisch zu laden, kann der FIPS-Modus aktiviert werden.

Beachten Sie, dass nach jeder Statusänderung des FIPS-Modus die VPN-Dienste neu gestartet werden.

Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul 140-2, das diese Algorithmen beinhaltet, besitzt die Zertifizierung #1747.

Die FIPS-Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

- Diffie Hellman-Gruppe: Gruppe 2 bis 14 (DH Länge von 1024 Bit bis 2048 Bit)
- Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit
- Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES

Die entsprechenden Module können in den [IPsec-Einstellungen](#) ¹⁶⁷ konfiguriert werden.

Profil-Sicherung

Existiert noch kein gesichertes Profil, zum Beispiel bei einer Erstinstallation, so wird automatisch ein erstes angelegt (NCPPHONE.SAV).

Erstellen [Profil-Sicherung]

Nach jedem Klick auf den Menüpunkt "Erstellen" wird nach einer Sicherheitsabfrage eine Profil-Sicherung angelegt, die die Konfiguration zu diesem Zeitpunkt enthält.

Wiederherstellen [Profil-Sicherung]

Nach jedem Klick auf "Wiederherstellen" wird die letzte Profil-Sicherung eingelesen. Änderungen in der Konfiguration, die seit der letzten Profil-Sicherung vorgenommen wurden gehen damit verloren.

Ansicht

Unter dem Menüpunkt „Ansicht“ können Sie die Bedienoberfläche des Monitors variieren und die Sprache für die Monitoroberfläche festlegen. Folgende Einstellungen stehen zur Auswahl:

- [Profilauswahl anzeigen](#) ¹²²
- [Statistik anzeigen](#) ¹²²
- [WLAN-Status anzeigen](#) ¹²²
- [Tipps anzeigen](#) ¹²²
- [Immer im Vordergrund](#) ¹²³
- [Autostart](#) ¹²³
- [Beim Schließen minimieren](#) ¹²³
- [Nach Verbindungsaufbau minimieren](#) ¹²³
- [GUI-Skalierung](#) ¹²⁴
- [Sprache](#) ¹²⁴

Profilauswahl anzeigen

Stehen mehrere konfigurierte Profile zur Verfügung, kann aus deren Liste das gewünschte ausgewählt werden.

Statistik anzeigen

Wenn Sie auf "Statistik anzeigen" klicken, werden Informationen zu Datenmenge, Verbindungszeit, Timeout etc. angezeigt. Die Monitor-Oberfläche ist dann entsprechend größer.

WLAN-Status anzeigen

An dieser Stelle kann unabhängig vom Verbindungsmedium des aktuell selektierten Linkprofils ein eigenes Feld zur grafischen Anzeige der WLAN-Feldstärke geöffnet bzw. geschlossen werden, wenn im Monitormenü "Konfiguration" unter "WLAN" eine WLAN-Konfiguration aktiviert wurde.

Ein Button [...] in diesem Panel führt direkt in das Konfigurationsfeld der "WLAN-Einstellungen".

Wurde eine Mobilfunkkarte konfiguriert, ist der Menüpunkt "WLAN-Panel" nicht aktiv.

Tipps anzeigen

Die Tipps geben Ihnen wichtige und schnelle Hinweise zu Konfiguration und individueller Gestaltung der Monitor-Oberfläche.

Schalten Sie die Tipps ein, wird unter dem grafischen Anzeigefeld neben dem Firmenlogo, das sie übrigens austauschen können (Tipp 9), in Form einer Frage auf einige (15) wesentliche Leistungsmerkmale des Clients hingewiesen.

Mit der Tastenkombination [Strg] + [t] können Sie den Fragenkatalog durch blättern.

Mit einem Mausklick auf die Frage erhalten Sie die Antwort.

Immer im Vordergrund

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

Autostart

Über diesen Menüpunkt können folgende Optionen eingestellt werden:

- kein Autostart: nach dem Booten muss der Monitor manuell gestartet werden, entweder aus dem Programm-Menü oder mit dem Icon vom Desktop;
- Monitor auf dem Desktop: nach dem Booten wird der Monitor automatisch gestartet und in normaler Größe dargestellt;
- Icon im System Tray: nach dem Booten wird der Monitor gestartet und als Icon in Form einer Ampel minimiert im System-Tray dargestellt;

Wenn Sie oft mit der Client Software arbeiten und die Informationen des Monitors benötigen, so sollten Sie die Einstellung "maximiert starten" wählen. Prinzipiell ist es für die Kommunikation mit dem Zielsystem nicht nötig, den Monitor zu starten.

Beim Schließen minimieren

Funktion nicht aktiviert

Wird der Monitor des Clients über den Button [x] rechts in der Kopfzeile oder über das Systemmenü "Verbindung" mit Klick auf "Beenden" (Tastenkombination [Alt + F4]) geschlossen, so verschwindet die grafische Darstellung des Monitors.

Der Status einer eventuell noch bestehenden Verbindung wird nicht mehr angezeigt.

Funktion aktiviert

Ist dieser Menüpunkt aktiviert, so wird der Monitor beim Schließen nur minimiert und erscheint in der Task-Leiste als VPN-Icon, worüber der Status der Verbindung abgelesen werden kann.

Nach Verbindungsaufbau minimieren

Ist dieser Menüpunkt aktiviert, so wird der Monitor nach erfolgreichem Verbindungsaufbau automatisch minimiert.

GUI-Skalierung

Unter Tablets mit hoher Auflösung kann der Client auch über einen Touch Screen bedient werden, nachdem er auf eine handhabbare Größe skaliert wurde.

Ein Skalierungsgrad von 150 % ist voreingestellt und kann durch einen Doppelklick auf das Logo aktiviert oder wieder deaktiviert werden.

Die Darstellungsgröße kann in Stufen von 100, 125, 150, 175 und 200 % variiert werden eingestellt werden. Eine dynamische Änderung der Skalierung ist mit der Tastenkombination [Strg] [+] bzw. [Strg] [-] möglich.

Hinweis: Die für Verbindungsaufbau und Statistikanzeige erforderlichen Dialoge wurden für skalierbare Darstellung optimiert, nicht aber alle Konfigurationsdialoge.

Die Einstellungen werden in der Datei NCPMON.INI unter folgendem Abschnitt gespeichert:

[GENERAL]

Scaled=0

ScaleFactor=150









Sprache

Die Client Software ist mehrsprachig angelegt. Die Standardsprache bei Auslieferung ist Deutsch. Um eine andere Sprache zu wählen, klicken Sie "Language / Sprache" im Pull-Down-Menü Fenster und wählen die gewünschte Sprache.

Hilfe

Unter diesem Menüpunkt können alle verfügbaren Informationen zum Client eingesehen werden. Dies betrifft den kompletten Hilfetext, einschließlich der Produktbeschreibung

Weitere Informationen zum Stand der Software und aktuellen Funktionalitäten erhalten Sie unter folgenden Menüpunkten:

- [Logbuch](#)  126
- [Erweiterte Log-Einstellungen](#)  128
- [Client Info Center](#)  129
- [Netzwerkdiagnose](#)  130
- [Auf Updates prüfen](#)  130
- [Aktivierung](#)  130
- [Client deaktivieren](#)  132
- [Info](#)  132

Logbuch

Automatisierte Protokollierung

Die Log-Funktion ist ständig im Hintergrund aktiv, auch bei einem nicht geöffneten Log-Fenster. Sie zeichnet selbständig alle relevanten Kommunikationsereignisse der Client-Software auf und speichert sie für den Zeitraum einer Woche pro Betriebstag in einer Log-Datei. Log-Ausgaben, die älter als sieben Betriebstage sind, werden automatisch gelöscht.

Diese Log-Datei wird im Installationsverzeichnis unter "Log" automatisch bei Beenden des Monitors unter dem Namen NCPymmdd.LOG generiert, wobei "ymmdd" dem Datum entspricht.

In den erweiterten Log-Einstellungen kann dieser Aufzeichnungsrhythmus variiert werden.

Mittels einfacher Texteditoren können die Log-Dateien geöffnet und gelesen werden.

Ausgewählte Protokolle

Bei geöffnetem Log-Fenster werden die aktuellen Log-Ausgaben gelistet und können verfolgt werden. Dabei werden die Zeilen des Log-Protokolls automatisch gescrollt. Das hier vom Zeitpunkt des Öffnens des Log-Fensters bis zu dessen Schließung erzeugte Protokoll wird bis zum nächsten Reboot im Speicher gehalten. Der Inhalt des Log-Fensters kann aber auch manuell gelöscht, gespeichert oder nach bestimmten Ereignissen durchsucht werden.

Folgende Kommandos im Fußbereich des Log-Fensters stehen für diese Funktionen bereit:

Fensterinhalt löschen

Wenn Sie auf diesen Button drücken wird das Fenster von den letzten Protokolleinträgen geleert.

Log-Fenster schließen

Hiermit wird das Log-Fenster geschlossen, ohne dessen Inhalt in eine Datei zu schreiben.

Suchfunktion einblenden

Zwei Suchfunktionen erleichtern das Auffinden von Strings und Begriffen im Text des Log-Protokolls.

Suche

In das Eingabefeld kann ein Such-String eingetragen werden. Nach dem Start der Suche werden alle dementsprechenden Fundstellen im Log-Protokoll markiert.

Mit [F3] wird von der zeitlich ältesten Fundstelle mit diesem String zur nächst jüngeren gesprungen, mit Shift + [F3] von der aktuellsten Fundstelle zur nächst älteren.

Scrollen beenden

Um das ständige Einlesen neuerer Log-Meldungen zu stoppen kann „Protokollierung anhalten“ gesetzt werden.

Eine Suche nach mehreren Strings gleichzeitig ist nicht möglich.

Filter

Nach dem String, der in dieses Feld eingegeben wird, wird im Log-Text gesucht. Mehrere Strings können durch Leerzeichen getrennt gleichzeitig gesucht werden. In der Standardeinstellung werden die Zeilen mit den entsprechenden Fundstellen aus dem Log-Protokoll ausgeblendet.

Umgekehrt können hiermit nur die Zeilen angezeigt werden, worin sich die gefilterten Strings befinden.

Speicherung der Such- und Filtereingaben

Die letzten zehn Such- und Filtereingaben werden in der Auswahlliste gepuffert und angezeigt.

Die maximale Anzahl der Log-Ausgaben, welche intern gepuffert werden, ist normalerweise auf 1000 gesetzt. Dieser Wert kann über die NCPMON.INI geändert werden.

Folgende Werte werden in der NCPMON.INI für diese Funktion gespeichert:

MaxTraceLines=1000

WholeWords=0

CaseSensitive=0

MaxSearchEntries=10

SearchEntry_X=X. Such-Eintragstring

MaxFilterEntries=10

FilterEntry_X=X. Filter-Eintragstring

Erweiterte Log-Einstellungen

Mit dieser Funktion können zusätzliche Log-Ausgaben abgefragt werden:

Client PKI Support

- PKI
- PKI Interface GaCC

Log-Ausgaben für PKI-Module werden nur geschrieben, wenn sie an dieser Stelle aktiviert werden.

Anwendungen

- Client Monitor
- RWSCMD / NcpClientCmd
- Credential Provider

Für die hier genannten modularen Anwendungen können bei Bedarf eigenen Log-Ausgaben aktiviert werden.

Sind erweiterte Log-Ausgaben aktiviert, blinkt ein entsprechender Text am Monitor. Mit einem Doppelklick auf diesen blinkenden Text kann der Dialog für die erweiterten Log-Ausgaben geöffnet werden.

Bei der Aktivierung und Deaktivierung von Log-Ausgaben für Dienste kann der dazu gehörige Dienst über den Button "Neustart" ohne Administrator-Rechte gestartet werden.

Der Button "Neustart" startet nur die Dienste neu, nicht das System!

Client Info Center

Mit dem Client Info-Center kann die Unterstützung durch den User Helpdesk optimiert werden.

Die eingeblendete Übersicht stellt folgende allgemeine 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

Darüber hinaus werden Informationen zu folgenden Bereichen eingeblendet:

- Verbindungen
- Dienste
- Zertifikatskonfiguration
- Netzwerkadapter

Mittels Button in der GUI sind diese Werte in eine Textdatei exportierbar. Alternativ dazu kann dies auch unabhängig von einem Start des Monitors erfolgen, wenn folgendes RWSCMD-Kommando eingegeben wird: `rwscmd /writeClientInfoCenterData [OutFileName]`.

Netzwerkd Diagnose

Mit den hier angebotenen Netzwerk-Tests kann die Internet-Verfügbarkeit getestet werden. Sie gestatten sowohl einen PING auf eine IP-Adresse im Internet auszuführen als auch die Auflösung eines Internet-Domain-Name (DNS-Request) in die entsprechende IP-Adresse zu prüfen, wobei der Domain-Name in Form von "name.com" angegeben wird.

Nach Eingabe der Adresse wird der entsprechende Test-Button gedrückt, woraufhin die Aktion ausgeführt wird.

Die Testergebnisse werden über ein Symbol angezeigt (erfolgreich: grüner Haken, erfolglos: rotes Kreuz). Mehr Informationen zeigt ein kleines Log in Klartext.

Die Tests sind insbesondere von Bedeutung wenn Firewall-Regeln für DNS-Request und ausgehende Verbindungen über das Internet geprüft werden sollen.

Support-Assistent

Mit Hilfe des Support-Assistenten können erweiterte Log-Ausgaben und Systeminformationen an den Support gesendet werden. Bei Bedarf können auch zusätzliche Dateien wie Screenshots angehängt werden.

Nach der automatisierten Erzeugung einer Archiv-Datei (*Support.zip) wird diese über das E-Mail-Programm an die Adresse des Supports (support@ncp-e.com) geschickt. Alternativ kann der Browser mit einem Formular zur Support-Anfrage gestartet werden.

Auf Updates prüfen

Unter diesem Menüpunkt kann geprüft werden, ob eine neuere Software vorliegt, als die von Ihnen installierte. Dies ist auch dann möglich, wenn eine Testversion installiert wurde. Liegt eine neuere Version vor, so ist immer ein Software-Update möglich. Informationen zum Leistungsumfang der neuesten Software erhalten Sie über die angegebene Website.

Der Abfragezyklus (nie, täglich, wöchentlich, monatlich) kann konfiguriert werden oder der Button Jetzt prüfen wird gedrückt.

Aktivierung

Hier wird die eingesetzte installierte Software-Version und gegebenenfalls die lizenzierte Software-Version mit Seriennummer angezeigt.

Die verbliebene Zeitdauer bis zur Software-Aktivierung, d. h. die Gültigkeitsdauer der Testversion, wird in der Hinweisleiste des Monitors neben dem Aktivierungs-Button angezeigt.

Um eine zeitlich unbegrenzt gültige Vollversion nutzen zu können, muss die Software mit dem erhaltenen Lizenzschlüssel und der Seriennummer im Aktivierungs-Dialog freigeschaltet werden.

Mit der Aktivierung akzeptieren Sie die Lizenzbedingungen, die Sie nach einem Klick auf den entsprechenden Button im Aktivierungs-Dialog einsehen können.

Gültigkeitsdauer der Testversion

Die Gültigkeitsdauer der Testversion beträgt 30 Tage. Ohne Software-Aktivierung bzw. Lizenzierung ist nach dieser Zeitspanne kein Verbindungsaufbau mehr möglich. Während der Testphase kann die Lizenzierung über den Aktivierungsrahmen am Fuß des Monitors angestoßen werden.

Ab dem Zeitpunkt der Installation wird bei jedem Start der Software die Gültigkeitsdauer im Popup-Fenster angezeigt. Darüber hinaus wird im Aktivierungsrahmen am Fuß des Monitors eingeblendet wie lange die Testversion noch verwendet werden kann und in einer Message-Box, ab der verbliebenen Zeitspanne der Gültigkeit von 10 Tagen, nachdrücklich darauf aufmerksam gemacht, dass die Software noch nicht lizenziert ist. Diese Message-Box erscheint einmalig pro Tag.

Ist die Testphase abgelaufen, können mit der Client Software nur noch Verbindungen zu Zielsystemen aufgebaut werden, die der Software-Aktivierung/-Lizenzierung dienen. So kann eines der Profile des Clients dazu verwendet werden, eine Internet-Verbindung zum Zweck der Lizenzierung aufzubauen.

Software-Aktivierung

Spätestens wenn die Testphase abgelaufen ist, muss die Software aktiviert oder deinstalliert werden.

Zur Aktivierung selektieren Sie im Monitormenü "Hilfe" den Menüpunkt "Lizenzinfo und Aktivierung".

Sie können hier ablesen um welche Software-Version es sich handelt und wie die Software lizenziert ist, d. h. dass die Testversion abgelaufen und die Software noch nicht aktiviert/lizenziert ist.

Mit Klick auf die Lizenzbedingungen wird der entsprechende Vertragstext eingeblendet. Mit der Aktivierung/Lizenzierung der Software akzeptieren Sie die Lizenzbedingungen.

Der Aktivierungs-Dialog kann sowohl über den Aktivierungs-Button in der Hinweisleiste des Monitors als auch über das Monitormenü "Hilfe / Lizenzinfo und Aktivierung" geöffnet werden. Im folgenden Fenster kann gewählt werden, auf welche Art der Client über einen Assistenten lizenziert werden soll.

Offline

In der Offline-Variante muss eine Datei, die nach Eingabe von Lizenzschlüssel und Seriennummer erzeugt wird, an den Web Server geschickt werden und der daraufhin auf der Website angezeigte Aktivierungsschlüssel notiert werden.

Online

In der Online-Variante werden die Lizenzierungsdaten über einen Assistenten unmittelbar nach Eingabe an den Web Server weitergegeben und die Software damit unverzüglich freigeschaltet.

Client deaktivieren

Um eine lizenzierte Client Software bei einem Rechnerwechsel ohne Einschränkungen weiterhin benutzen zu können, müssen die Lizenzdaten (Seriennummer und Lizenzschlüssel), die an Hardware und Betriebssystem gebunden sind, vorher vom Aktivierungs-Server für eine erneute Lizenzierung freigegeben werden.

Der Anwender gibt dem Aktivierungs-Server bekannt, dass er vorübergehend seine Lizenz nicht einsetzt, indem er im Hilfe-Menü des Monitors den Menüpunkt Client deaktivieren selektiert. In einer Eingabemaske gibt der Anwender daraufhin seinen Namen, optional auch den seiner Firma, sowie eine gültige E-Mail-Adresse an. Klickt der Benutzer auf abschicken, werden diese Daten plus Seriennummer, Lizenzschlüssel und die Sprach-ID an den Aktivierungs-Server geschickt.

Der Client deaktiviert sich daraufhin, erkennbar am Text "Software nicht aktiviert", der in einem Banner der Client-Oberfläche dargestellt wird.

Der Anwender erhält an die angegebene E-Mail-Adresse eine Nachricht mit einem Link. Erst nachdem der Link angeklickt wurde, wird die Lizenz am Aktivierungs-Server zurückgesetzt, d.h. die Lizenzdaten können für eine Aktivierung der Client Software an einem anderen Rechner erneut eingegeben werden.

Info

Das Info-Fenster zeigt Produktbezeichnung und Versionsnummer.

Konfigurationsparameter

Verfügbare Profile

In der Übersicht „Verfügbare Profile“ werden die zur Verfügung stehenden Verbindungsprofile in mehreren Spalten aufgelistet (Profil-Name / Verbindungsmedium / Standard). Die Überschriften der Spalten können als Sortierkriterium der angezeigten Profile verwendet werden, die Checkbox in der dritten Spalte dient einer schnellen Konfigurationsänderung bei Verwendung eines Standardprofils. Um die zuletzt genannte Funktion konfigurieren zu können, muss die Profil-Einstellung nicht eigens geöffnet werden.

Konfigurieren einer Profil-Einstellung

Die Buttons unter der Liste der Profile können nicht betätigt werden, wenn die entsprechenden Sperren eingestellt sind. Wurden keine Einschränkungen für die Profil-Einstellungen vorgegeben, können alle Buttons betätigt und die darauf vermerkten Funktionen ausgeführt werden.

Um die (Standard-)Werte einer Profil-Einstellung zu editieren, wählen Sie mit der Maus das Profil aus und klicken Sie anschließend auf den [Bearbeiten]-Button.

Die Konfigurationsparameter erreichen Sie über das Untermenü:

[Profile \[Parameter\]](#) ¹³⁵

Die IPsec-Konfiguration erfolgt in den Profil-Einstellungen indem der [Editor]-Button gedrückt wird unter:

[IPsec](#) ¹⁶⁷

Profile [Parameter]

Nachdem Sie "Profile" im Menü des Monitors angeklickt haben, wird eine Übersicht über die bereits definierten Profile gezeigt. Darunter finden Sie Buttons, über die Sie die Profil-Einstellungen modifizieren können.

Um ein neues Profil zu definieren, klicken Sie in der Menüleiste des Monitors auf "Profile". Das Menü öffnet sich nun und zeigt die bereits definierten Profile. Klicken Sie jetzt auf "Hinzufügen". Jetzt legt der "Assistent für neues Profil" mit Ihnen ein neues 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 werden Standardwerte eingetragen.

Die Parameter, die das jeweilige Profil spezifizieren, sind in verschiedenen Konfigurationsfeldern gesammelt. In der Kopfzeile der Profil-Einstellungen steht der Name des Profils. Seitlich sind die Titel der Konfigurationsfelder angeordnet:


Grundeinstellungen [Profile]	136
Netzeinwahl	144
Mobilfunknetz [Profile]	149
HTTP-Anmeldung [Profile]	151
Verbindungssteuerung [Profile]	153
Erweiterte Authentisierung / Authentisierung vor VPN	164
IPsec-Einstellungen	167
Erweiterte IPsec-Optionen	185
Identität	188
IPsec-Adresszuweisung	193
Split Tunneling	195
Zertifikats-Überprüfung	197
Link Firewall	203

Grundeinstellungen [Profile]

Die Client Software gestattet die Einrichtung individueller Profile, die den Benutzeranforderungen entsprechend konfiguriert werden können. Um Profil-Einstellungen voneinander unterscheiden zu können, muss in diesem Parameterfeld zunächst ein Name für das Profil vergeben werden.


Beachten Sie auch folgende Parameter:

[Profil-Name](#)  137

[Verbindungstyp](#)  137

[Verbindungsmedium](#)  138

[Standard-Profil nach jedem Neustart des Systems](#)  140

[Profil für automatische Medienerkennung](#)  141

[Einwahl über Windows DFÜ](#)  142

[Seamless Roaming](#)  143

Profil-Name

Wenn Sie ein neues Profil definieren, sollten Sie zunächst einen unverwechselbaren Namen für dieses System eintragen (z. B. IBM London). Der Name des Ziels darf jeden gewünschten Buchstaben wie auch Ziffern beinhalten und darf, Leerzeichen mitgezählt, bis zu 39 Zeichen lang sein.

Verbindungstyp

Alternativ stehen zwei Verbindungstypen zur Wahl:

VPN zu IPsec-Gegenstelle:

In diesem Fall wählen Sie sich mit dem IPsec Client in das Firmennetz ein (bzw. an das Gateway an). Dazu wird ein VPN-Tunnel aufgebaut.

Internet-Verbindung ohne VPN:

In diesem Fall nutzen Sie den IPsec Client nur zur Einwahl in das Internet. Dabei wird Network Address Translation (IPNAT) weiterhin im Hintergrund genutzt, sodass nur Datenpakete akzeptiert werden, die angefordert wurden.

Verbindungsmedium

Das Verbindungsmedium kann für jedes Profil eigens eingestellt werden, vorausgesetzt die entsprechende Hardware ist angeschlossen und im System installiert. Folgende Verbindungsmedien können eingestellt werden:

LAN (over IP)

Angeschlossene Hardware: LAN-Adapter;

Netze: Local Area Network mit Ethernet;

Gegenstellen: Die Gegenstellen des lokalen Multiprotokoll-Routers im LAN;

Mobilfunknetz

Diese Verbindungsart wählen Sie, wenn die Einwahl über das Mobilfunknetz erfolgen soll.

WLAN

Hardware: WLAN-Adapter;

Netze: Funknetz;

Gegenstellen: Access Point;

Im Monitormenü erscheint unter "Konfiguration" der Menüpunkt "WLAN", worin die Zugangsdaten zum Funknetz in einem Profil hinterlegt werden können, wenn das "WLAN-Management aktiviert" wird. In diesem Fall wird das Management-Tool des Betriebssystems deaktiviert. (Alternativ kann auch das Management-Tool der WLAN-Karte genutzt werden, dann muss die WLAN-Konfiguration im Monitormenü deaktiviert werden.)

Mit Hilfe des WLAN-Managements können individuelle WLAN-Profile mit Zugriffsdaten zu drahtlosen Netzen vorkonfiguriert werden.

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

automatische Medienerkennung

Werden wechselweise unterschiedliche Verbindungsmedien genutzt, wie zum Beispiel LAN oder WLAN (im Firmennetz) oder Mobilfunknetz, so kann die manuelle Auswahl des Profils mit dem jeweils zutreffenden Verbindungsmedium entfallen, wenn das Profil mit dem Verbindungsmedium LAN auf "automatische Medienerkennung" umkonfiguriert wurde und je ein Profil mit einem alternativ verfügbaren Verbindungsmedium vorhanden ist.

Das Profil mit automatischer Medienerkennung muss mit allen für die Verbindung zum VPN Gateway nötigen Parametern (insbesondere der IP-Adresse des VPN Gateways [Gateway \(Tunnel-Endpunkt\)](#)¹⁷⁰) konfiguriert sein.

Die alternativen Profile müssen die Parameter für das jeweilige Verbindungsmedium enthalten - und sie benötigen im Parameterfeld "Netzeinwahl" die Zugangsdaten für den Internet Diensteanbieter sowie im Parameterfeld "Grundeinstellungen" die Einstellung ihres Verwendungszwecks als "Profil für automatische Medienerkennung". (Die Verwendung als Profil für "Autom. Medienerkennung" kann auch in der Profil-Auswahl vorgenommen werden.)

Vor einem Verbindungsaufbau muss das Profil mit dem Verbindungsmedium "automatische Medienerkennung" selektiert sein. Der Client erkennt dann automatisch, welche Verbindungsmedien genutzt werden können und wählt von den alternativ zur Verfügung stehenden Profilen das schnellste aus.

Konfigurationsanweisung:

1. Konfigurieren Sie ein Profil für die Verbindung über LAN oder WLAN zum VPN Gateway innerhalb Ihres Firmennetzes. Dazu benötigen Sie die IP-Adresse des VPN Gateways und Ihre Authentisierungsdaten (u. a. VPN-Benutzername, VPN-Passwort), ggf. auch die Zertifikatskonfiguration.
2. Schalten Sie das Verbindungsmedium von LAN oder WLAN auf "automatische Medienerkennung". (Die Verbindung zum VPN Gateway im Firmennetz muss damit genauso möglich sein!)
3. Konfigurieren Sie ein alternatives Profil, worin Sie die Zugangsdaten für den Internet-Diensteanbieter und die Parameter für ein alternatives Verbindungsmedium eintragen und bestimmen Sie den Verwendungszweck dieses Profils als "Profil für automatische Medienerkennung". (Die Verwendung als Profil für "Autom. Medienerkennung" kann auch in der Profil-Auswahl vorgenommen werden.)
4. Das alternative Profil kann für weitere alternative Verbindungsmedien kopiert werden, wonach nur die medienspezifischen Parameter entsprechend eingestellt werden müssen.
5. Achten Sie darauf, dass vor dem Verbindungsaufbau das Profil mit dem Verbindungsmedium "automatische Medienerkennung" in der Profilauswahl selektiert ist.

Standard-Profil nach jedem Neustart des Systems

Normalerweise wird der Client-Monitor nach einem Neustart mit der zuletzt genutzten Profil-Einstellung geöffnet. Wird diese Funktion aktiviert, wird nach einem Neustart des Systems immer das hierzu gehörige Profil geladen, unabhängig davon, welches zuletzt genutzt wurde.

Profil für automatische Medienerkennung

Mit Aktivierung dieser Funktion wird dieses Profil an den Eintrag für automatische Medienerkennung gebunden und bei Verfügbarkeit des entsprechenden Mediums automatisch für einen potentiellen Verbindungsaufbau herangezogen.

Beachten Sie dazu die Beschreibung zu [Verbindungsmedium](#)¹³⁸.

Das Profil kann auch manuell selektiert werden, um eine Verbindung herzustellen, sofern die Tunnel-Parameter für den Zugang zum VPN Gateway korrekt eingetragen sind.

Soll ein Zielsystem oder Profil mit der Verbindungsart Mobilfunknetz für die automatische Medienerkennung bereitgestellt werden, so muss die SIM-PIN für die Karte in der Konfiguration unter "Verbindung / Mobilfunkkarte" eingegeben werden.

Einwahl über Windows DFÜ

Zur Einwahl am ISP (Internet Service Provider) kann der Microsoft DFÜ-Dialer genutzt werden. Dies ist immer dann nötig, wenn der Einwahlpunkt ein Einwahl-Script benötigt. Der DFÜ-Dialer unterstützt dieses Script. Im Parameterfenster "Netzeinwahl" wird anschließend die Script-Datei unter Eingabe von Pfad und Namen zur eingespielten Script-Datei eingetragen (siehe unten Script-Datei).

nie

Mit der Einstellung "nie" wird ausschließlich der Dialer des Clients zur Einwahl verwendet.

nur bei Script-Einwahl

Soll der DFÜ-Dialer "nur bei Script-Einwahl" verwendet werden, so wählen Sie diese Option. Bei einem Einwahlpunkt, der kein Script verlangt, wird automatisch auf den Dialer des Clients umgeschaltet.

immer

Soll der DFÜ-Dialer immer verwendet werden, muss die entsprechende Einstellung vorgenommen werden.

Im Parameterfenster "Netzeinwahl" wird anschließend die RAS Script-Datei unter Eingabe von Pfad und Namen zur eingespielten Script-Datei eingetragen. Die Script-Datei erhalten Sie von Ihrem Provider.

(Bei Verwendung eines internationalen Telefonbuchs wird die Script-Datei automatisch in die Konfiguration eingetragen und kann nicht mehr verändert werden.)

Seamless Roaming

Seamless Roaming wird mittels zweier Profile konfiguriert. Im ersten Profil mit der automatischen Medienerkennung (LAN/WLAN) zum Gateway, wird der Schalter Seamless Roaming gesetzt; in einem zweiten Profil wird die Verbindung zum Gateway über Mobilfunknetz definiert, und dieses Profil für automatische Medienerkennung aktiviert.

Sofern ein WLAN-Profil und/oder eine Hotspot-Konfiguration vorhanden sind, und eine WLAN-Karte aktiv ist, versucht der Client automatisch in der Reihenfolge LAN, WLAN, Mobilfunknetz die Verbindung aufzubauen, indem er das schnellste der zur Verfügung stehenden Medien nutzt.

Dabei ist zu beachten, dass je nach genutztem Verbindungsmedium verschieden hohe Gebühren anfallen können.

(Seamless Roaming wird nur für IKEv1-Verbindungen unterstützt.)

Seamless Roaming wird im Hintergrund über die Verbindungsmedien LAN/WLAN und Mobilfunknetz automatisch immer dann ausgeführt, wenn die Internet-Verbindung über eines dieser Medien gestört oder für eine gewisse Zeit unterbrochen wird. Der Secure Client schaltet in diesem Fall automatisch auf das jeweils zur Verfügung stehende Medium um, wobei das schnellere Verbindungsmedium Vorrang hat.

Durch den nahtlosen Wechsel des Verbindungsmediums wird eine Always-on-Funktionalität bereitgestellt. Anwendungen, die den VPN-Tunnel nutzen, bleiben vom automatischen Medienwechsel oder einem Abbruch der physikalischen Verbindung unberührt. Die logische Verbindung bleibt auch während möglicher Verbindungspausen bis zum nächsten Wiederaufbau der physikalischen Verbindung erhalten.

Netzeinwahl

Dieses Parameterfeld beinhaltet den Benutzernamen und das Passwort, die beim Verbindungsaufbau zum Zielsystem zur Identifizierung benötigt werden. Diese beiden Größen werden auch für die PPP-Verhandlung zum ISP (Internet Service Provider) benötigt.

Siehe auch die Parameter:

[Benutzername \[Netzeinwahl\]](#)  144

[Passwort \[Netzeinwahl\]](#)  145

[Passwort speichern](#)  146

[Rufnummer \(Ziel\)](#)  147

[RAS Script-Datei](#)  148

Benutzername [Netzverbindung]

Mit dem Benutzernamen weisen Sie sich gegenüber dem Network Access Server (NAS) aus, wenn Sie eine Verbindung zum Zielsystem aufbauen wollen. Der Name für den Benutzer kann bis zu 254 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Benutzername vom Zielsystem zugewiesen, da Sie von dort auch erkannt werden müssen. Sie erhalten ihn von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

(Er muss die Authentisierungsanforderungen durch den NAS, RAUDIUS oder LDAP Server erfüllen.)

Passwort [Netzverbindung]

Das Passwort benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 128 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie vom Zielsystem auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Hinweis: Wenn Profile für die "automatische Medienerkennung" konfiguriert werden, ist es zwingend erforderlich, dass für alle diese Profile ein (NAS-)Passwort eingegeben wird, andernfalls kommt der Verbindungsaufbau nicht zustande.

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.

Hinweis: Für den Fall, dass Sie den Parameter "Passwort speichern" nicht aktiviert haben, gilt: Auch wenn Sie für den Verbindungsmodus "automatisch" gewählt haben, müssen Sie die Verbindung beim ersten Mal manuell aufbauen. Dabei werden Sie nach dem Passwort gefragt. Für jeden weiteren automatischen Verbindungsaufbau wird dieses Passwort selbständig übernommen, bis Sie den PC erneut booten oder Sie das Zielsystem wechseln.

Passwort speichern

Dieser Parameter muss aktiviert (angeklickt) werden, wenn gewünscht wird, dass das Passwort (sofern es eingegeben ist) gespeichert wird. Andernfalls wird das Passwort gelöscht, sobald der PC gebootet wird oder zu einem anderen Ziel für die Anwahl gewechselt wird. Standard ist die aktivierte Funktion.

Wichtig: Bitte beachten Sie, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Secure Client Software arbeiten kann - auch wenn er die Passwörter nicht kennt.

Rufnummer (Ziel)

Für jedes Ziel muss eine Rufnummer definiert sein, da der Secure Client ansonsten keine Verbindung herstellen kann. Diese Rufnummer muss genauso eingetragen werden, als würden Sie diese Telefonnummer per Hand wählen.

D.h. Sie müssen alle notwendigen Vorwahlziffern berücksichtigen: Amtsholung, Landesvorwahl, Ortsvorwahl, Durchwahlziffern, etc.

Beispiel: Sie wollen eine Verbindung von Deutschland nach England herstellen:

00 (für die internationale Verbindung, wenn Sie von Deutschland aus wählen)

44 (dies ist die landesspezifische Vorwahl für England)

171 (Vorwahl für London)

1234567 (die Nummer, die Sie zu erreichen wünschen)

Insgesamt wird nach diesem Beispiel folgende Nummer im Telefonbuch gespeichert und für die Anwahl verwendet: 00441711234567

Die Rufnummer des Ziels kann bis zu 30 Ziffern beinhalten.

Alternative Rufnummern

Möglicherweise ist das Zielsystem ein Network Access Server (NAS), der mit mehreren S0-Anschlüssen für verschiedene Rufnummern ausgestattet ist. In diesen Fall empfiehlt es sich, alternative Rufnummern einzugeben - falls zum Beispiel die erste Nummer besetzt ist. Die alternativen Rufnummern werden der ersten Nummer angehängt, nur mit einem Doppelpunkt (:) oder einem Semikolon (;) getrennt.

Maximal werden 8 alternative Rufnummern unterstützt.

Beispiel : 000441711234567:000441711234568

Die erste Nummer ist die Standard-Rufnummer und wird immer zuerst gewählt. Kann keine Verbindung hergestellt werden, weil besetzt ist, wird die zweite Nummer gewählt, usw.

Wichtig: Bitte beachten Sie, dass der Verbindungsaufbau nur funktionieren kann, wenn die Protokoll-Eigenschaften für die Anschlüsse der alternativen Rufnummern die gleichen sind.

RAS Script-Datei

Wenn Sie den Microsoft RAS-Dialer benutzen, tragen Sie hier die Script-Datei unter Eingabe von Pfad und Namen ein.

Mobilfunknetz-Konfiguration

Hier werden die Einwahlparameter für den Mobilfunk-Diensteanbieter eingeblendet.

Drei Konfigurationsmodi stehen zur Verfügung:

Konfigurationsmodus

automatisch

In der Standardeinstellung wird die APN aus der SIM-Karte gelesen. Wird der Typ APN von SIM ausgewählt, werden alle Felder der Providerkonfiguration gelöscht. Nach diesem Kriterium wird der Treiber veranlasst, sich den APN über die NetID der SIM-Karte aus der APN.INI zu suchen. Somit muss kein APN mehr konfiguriert werden.

Provider-Liste

Alternativ kann der gewünschte Anbieter aus einer Provider-Liste ausgewählt werden. (Sollte Ihr Provider noch nicht aufgeführt sein, so können Sie die Liste mit den Daten Ihres Providers erweitern; sie befindet sich als APN.INI-Datei im Installationsverzeichnis).

benutzerdefiniert

Als dritter Konfigurationsmodus kann der benutzerdefinierte Konfigurationsmodus eingestellt werden, wobei alle Daten manuell eingegeben werden müssen.

Land

Im Konfigurationsmodus mit Provider-Liste wählen Sie das Land, worin sich Ihr Anbieter befindet. Dazu werden die wichtigsten Provider angezeigt. (Die Provider-Liste ist editierbar im Installationsverzeichnis als APN.ini abgelegt.)

Provider

Im Konfigurationsmodus mit Provider-Liste werden je nach Landes-Auswahl die wichtigsten Provider zur Wahl gestellt. (Sollte Ihr Provider noch nicht aufgeführt sein, so können Sie die Liste mit den Daten zu Ihrem Provider erweitern; sie befindet sich als APN.INI-Datei im Installationsverzeichnis). Wählen Sie einen Provider aus, werden die weiteren Parameter, soweit in der Liste vorhanden, automatisch eingetragen.

APN

Den APN (Access Point Name) erhalten Sie von Ihrem Provider. Er kann auch manuell eingetragen oder aus der Provider-Liste gelesen werden. Für Vodafone lautet er "web.vodafone.de", für T-Mobile "internet.t-d1.de", etc.. Der APN wird insbesondere zu administrativen Zwecken genutzt.

Einwahlnummer

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

Authentisierung

Je nach Mobilfunk-Provider werden verschiedene Authentisierungs-Protokolle für die Verbindung der Mobilfunk-Geräte zum Netzwerk verwendet. PAP und CHAP sind die am häufigsten eingesetzten Protokolle. Diese Protokolle können auch automatisch und dynamisch selektiert werden wenn die Verbindung im Internet aufgebaut wird.

Im manuellen Modus wählen Sie das vom Provider vorgegebene Protokol (PAP oder CHAP). Wenn vom Provider nichts vorgegeben wird, belassen Sie den automatischen Modus.

Benutzername, Passwort

Als Zugangsdaten für den Internetdienstanbieter (Mobilfunk-Provider) muss im Modus "APN von SIM-Karte" und im benutzerdefinierten Konfigurationsmodus ein beliebiger Benutzername und ein beliebiges Passwort eingegeben werden, es sei denn, Sie haben vom Provider spezielle Kennwörter erhalten. Bei Vodafone und Deutscher Telekom genügen Dummy-Werte.

Zur Passwortabfrage bei Mobilfunk-Verbindungsaufbau

Zur Interneteinwahl via Mobilfunknetz bedarf es im Normalfall keines individuellen Benutzernamens oder Passwortes. Erfordert die Verbindung ins Internet dennoch die Eingabe von Benutzername oder Passwort, weil z. B. der Internet-Firmenzugang einen eigenen APN beim Provider besitzt, so kann die Abfrage der Benutzerkennung in einem eigenen Fenster automatisiert eingeblendet werden.

Dazu muss im Konfigurationsfeld unter "Passwort" folgender Eintrag in spitzen Klammern vorgenommen werden: <pwreq&g>

SIM PIN

Benutzen Sie eine SIM-Einsteckkarte für das Mobilfunknetz, so geben Sie hier die PIN für diese Karte ein. Wird die SIM PIN nicht eingetragen, so wird sie beim Verbindungsaufbau mit diesem Profil in einer Checkbox abgefragt. Dabei können Sie entscheiden ob sie für dieses Profil gespeichert werden soll.

Benutzen Sie ein Mobiltelefon, so wird diese PIN bei Einschalten des Handys bereits eingegeben.

HTTP-Anmeldung [Profile]

Mit den Einstellungen in diesem Parameterfeld kann die automatische HTTP-Anmeldung vorgenommen werden. Zentral erstellte Anmelde-Scripts und die hinterlegten Anmeldedaten können vom Access Point (Hotspot) übernommen werden, ohne dass ein Browserfenster geöffnet wird.

Die Automatisierung der Hotspot-Anmeldung geschieht in der Weise, dass bei einem Verbindungsaufbau zum Access Point von dort ein HTTP Redirect an den Client mit einer Website zur Anmeldung erfolgt. Anstatt eines Browser-Starts zur HTTP-Authentisierung, erfolgt mit den hier gemachten Eingaben die Authentisierung automatisch im Hintergrund.

Bitte beachten Sie, dass die Verbindung über einen Hotspot-Betreiber gebührenpflichtig ist. Sie müssen den Geschäftsbedingungen des Hotspot-Betreibers zustimmen, wenn die Verbindung aufgebaut werden soll.


Für die script-gesteuerte Anmeldung kann ein Script aus dem Installationsverzeichnis

<install>\scripts\samples

für weitere Hotspots entsprechend angepasst werden.

Siehe auch die Parameter:

[Benutzername \[HTTP-Anmeldung\]](#)  152

[Passwort \[HTTP-Anmeldung\]](#)  152

[HTTP-Authentisierungs-Script \[HTTP-Anmeldung\]](#)  152

Benutzername [HTTP-Anmeldung]

Dies ist der Benutzername, den Sie von Ihrem Hotspot-Betreiber erhalten haben.

Passwort [HTTP-Anmeldung]

Dies ist das Passwort, das Sie von Ihrem HotSpot-Betreiber erhalten haben. Das Passwort wird mit verdeckter Schreibweise (mit *) eingegeben.

HTTP-Authentisierungs-Script [HTTP-Anmeldung]

Hier kann nach Klick auf den [Suchen]-Button das hinterlegte Anmelde-Script selektiert werden.

Um eingehende Zertifikate bei der HTTP-Authentisierung überprüfen zu können, muss im Script die Variable CACERTDIR gesetzt worden sein. Desweiteren können auch Inhalte des WEB Server-Zertifikats überprüft werden. Hierzu stehen weitere Variablen zur Verfügung:

CACERTVERIFY_SUBJECT: Überprüft den Inhalt des Subjects (z.B. cn=WEB Server 1)

CACERTVERIFY_ISSUER: Überprüft den Inhalt der Issuers

CACERTVERIFY_FINGERPRINT: Überprüft den MD5 Fingerprint des Aussteller-Zertifikats

Stimmt der Inhalt der Variable mit dem eingegebenen Zertifikat nicht überein, wird die SSL-Verbindung nicht hergestellt und eine Log-Meldung im Monitor ausgegeben.

Script für Vodafone WebSessions

Wollen Sie den mobilen Internet-Zugang über Vodafone WebSessions nutzen, muss nur die Vodafone WebSession SIM-Karte für die Mobilfunkkarte (3G-Karte) installiert sein und ein Profil mit der Verbindungsart Mobilfunknetz angelegt werden.

Selektieren Sie das HTTP-Authentisierungs-Script, das Ihrer geplanten Verweildauer im Internet entspricht

(30 Minuten = vodafonewebsession30m.nhs,

1 Stunde = vodafonewebsession01h.nhs,

24 Stunden = vodafonewebsession24h.nhs).

In den Profil-Einstellungen muss unter [Mobilfunknetz](#)^[149] benutzerdefiniert der APN mit "event.vodafone.de" und die Einwahlnummer "*99#" angegeben werden.

Nach dem Verbindungsaufbau und der Eingabe Ihrer Zugangsdaten gelangen Sie direkt ins Internet.


Verbindungssteuerung [Profile]

In diesem Parameterfeld bestimmen Sie, wie der "Verbindungsaufbau" erfolgen soll und stellen die Timeout-Werte ein.

Siehe auch die Parameter:

[Verbindungsaufbau \[Verbindungssteuerung\]](#)  154

[Timeout \[Verbindungssteuerung\]](#)  155

[Logischen VPN-Tunnel bei Verbindungsunterbrechung trennen](#)  159

[Voice over IP \(VoIP\) priorisieren](#)  159

[Aktiviere Tunnel Traffic Monitoring](#)  160

[Alternative IP-Adresse](#)  161

[Quality of Service \(Profil\)](#)  162

Verbindungsaufbau [Verbindungssteuerung]

Hier definieren Sie die Art des Verbindungsaufbaus:

manuell

(Standardeinstellung des Verbindungsmodus)

In diesem Fall müssen Sie die Verbindung zum Zielsystem manuell herstellen. Ein Trennen der Verbindung erfolgt je nach eingestelltem Wert für den Timeout. Ist der Timeout auf Null (0) gesetzt, d. h. kein Timeout eingestellt, müssen Sie in jedem Fall die Verbindung manuell trennen.

Wichtig: Wenn eine Verbindung so konfiguriert wurde, dass sie "automatisch" aufgebaut wird, so muss unbedingt ein (NAS-)Passwort eingegeben werden, andernfalls kommt der Verbindungsaufbau nicht zustande.

immer

Mit dieser Einstellung wird unmittelbar nach dem Start des Clients ständig der VPN-Verbindungsaufbau angeregt. Dies erfolgt unabhängig vom Betätigen des Verbinden-Buttons, unabhängig von anstehendem Datenverkehr und unabhängig von der Darstellung des Monitors, die unter Autostart eingestellt werden kann.

wechselnd (Immer-Modus manuell starten)

Ist dieser Modus eingestellt, wird mit dem einmaligen Betätigen des Verbinden-Buttons der beständige Verbindungsaufbau "immer" angeregt. Dies erfolgt für die gesamte Betriebszeit des Monitors bis zu dessen Beenden.

Timeout [Verbindungssteuerung]

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.

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.

Hinweis: Um den Timeout zu aktivieren, ist es nötig, einen Wert zwischen 1 und 65356 einzutragen. Mit dem Wert "0" wird der automatische Timeout (Verbindungsabbau) nicht ausgeführt. Der Wert "0" bedeutet, dass das Trennen der Verbindung manuell durchgeführt werden muss.

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

Timeout-Richtung

Mit diesem Parameter bestimmen Sie, für welche Übertragungsrichtung der Timeout gelten soll. Drei verschiedene Einstellungen sind möglich:

TxRx (Standard):

Der Client achtet sowohl auf das Ende der gesendeten (out) als auch der empfangenen (in) Daten, bevor der Timer angestoßen wird.

Tx:

Nur die Senderichtung (out) wird beobachtet.

Rx:

Nur die Empfangsrichtung (in) wird beobachtet.

OTP-Token

Wird ein OTP-Token verwendet, so kann statt "Benutzername" und "Passwort" für die Einwahl die PIN und das Onetime-Passwort des Tokens eingegeben werden.

Wofür der OTP-Token genutzt wird, wird mit folgenden Einstellungen bestimmt:

aus

(standard) OTP wird nicht genutzt

NAS-Einwahl

Wird ein OTP für die Einwahl an einem NAS genutzt, wird das Feld für "Passwort" unter "Netzeinwahl" inaktiv geschaltet.

VPN-Einwahl

Wird ein OTP für die Einwahl zum VPN Gateway genutzt, wird entsprechend das Feld für "VPN-Passwort" unter "Tunnel-Parameter" inaktiv geschaltet.

Bei der Einwahl erscheint ein Dialogfenster für die Eingabe des "Einmalpassworts", in welches PIN und Einmalpasswort des Tokens eingetragen werden müssen.

Werden vom ACE-Server auf Grund des RSA-Tokens Nachrichten versendet, werden diese am Monitor in einem Informationsfenster mit Eingabefeld angezeigt (z. B. "Ablauf der gültigen PIN" oder "Ablauf des OTP-Passworts"). Geben Sie die neue PIN oder das neue Passwort von Ihrem Token in das Eingabefeld ein.

Tausche OTP (Einmalpasswort) und PIN

Dieser Expertenparameter sollte nur von einem erfahrenen Systemadministrator gesetzt werden, der über die Systemarchitektur der eingesetzten Zwei-Faktor-Authentisierung informiert ist.

Beim VPN-Verbindungsaufbau wird ein Popup-Fenster eingeblendet, welches drei Authentisierungsparameter immer in der gleichen Reihenfolge abfragt:

- Benutzername (VPN-Benutzername)
- PIN (PIN zum Einsatz eines RSA-Tokens)
- Einmalpasswort (OTP)

PIN und Einmalpasswort werden beim Versenden an den OTP-Server zu einem VPN-Passwort in String-Form verkettet. Dabei muss die Reihenfolge der Zusammensetzung von PIN und Einmalpasswort den Anforderungen des jeweiligen OTP-Servers genügen. Der RSA Authentication Manager (SecurID Server) erwartet in der Regel ein VPN-Passwort nach dem Standardmuster „PIN + Einmalpasswort“.

Sollte der RSA Authentication Manager bzw. OTP-Server ein Ergebnis erwarten, das dem Muster „Einmalpasswort + PIN“ entspricht, so kann dieses Ergebnis durch Aktivieren der Konfigurationsoption „Tausche Einmalpasswort und PIN“ erzeugt werden.

Beachten Sie, dass dieser Parameter keine Auswirkung auf die Darstellung in der Oberfläche des Popup-Fensters hat.

Benutzername unterdrücken bei Eingabeaufforderung

Bei einem wiederholten Verbindungsaufbau mit manueller Eingabe der Zugangsdaten (nachdem eine VPN-Verbindung getrennt wurde) kann für eine erneute Aktivierung der Verbindung die neuerliche Eingabe des Benutzernamens erzwungen werden. Dazu muss diese Funktion aktiviert werden. Diese Funktion ist sowohl im Eingabe-Dialog für den Verbindungsaufbau als auch beim Windows Pre-Logon wirksam.

In der Standardeinstellung (deaktiviert) muss bei einem wiederholten Verbindungsaufbau nur das Passwort eingegeben werden, da der Benutzername im Cache gehalten wird. In der Standard-Einstellung, die aufgrund der Abwärtskompatibilität beibehalten wird, entsteht eine Sicherheitslücke, da auch von nichtberechtigten Personen der wieder eingeblendete Benutzername im Eingabe-Dialog gelesen werden kann.

Bei aktivierter Funktion ist sichergestellt, dass bei jedem Aufbau einer VPN-Verbindung die kompletten Zugangsdaten des entsprechenden Benutzers zur Authentisierung verwendet werden.

Logischen VPN-Tunnel bei Verbindungsunterbrechung trennen

Dieser Schalter verändert das Standard-Verhalten des Clients

(logische Verbindung halten)

Ist das Standardverhalten des Clients umgeschaltet, geht bei einer Störung oder Unterbrechung der physikalischen Verbindung auch die logische Verbindung verloren und der VPN-Tunnel wird abgebaut.

Wichtig

Das Verhalten bei Seamless Roaming ist unabhängig vom eingestellten Standardverhalten des Clients. Das heißt, sobald für den Verbindungsaufbau ein Profil mit Seamless Roaming verwendet wird, wird die logische Verbindung über die Zeitdauer der physikalischen Verbindung hinaus gehalten.

Nur ohne den Einsatz von Seamless Roaming wirkt sich die Einstellung des Standardverhaltens bei einem Abbruch der physikalischen Verbindung auf das Erhalten der logischen Verbindung aus.

Optische Rückmeldung beim logischen Halten des Tunnels

Wenn die Verbindung über das jeweilige Verbindungsmedium eines VPN-Profiles unterbrochen wird, bleibt der VPN-Tunnel weiterhin bestehen. D. h. der VPN-Tunnel wird über einen beliebig langen Zeitraum bis zum Wiederaufbau der physikalischen Verbindung über das jeweilige Medium logisch gehalten.

Während der Haltedauer der logischen Verbindung wird der grüne Balken der VPN-Verbindung im Client-Monitor in gestrichelter Form dargestellt. Während dieser Zeitspanne leuchtet das Ampellicht im Systemtray gleichzeitig grün und gelb bis die physikalische Verbindung wieder hergestellt ist (grünes Licht).

Dieses Verhalten des Monitors geht verloren, wenn das voreingestellte Standardverhalten umgeschaltet wurde und für den Verbindungsaufbau ein Profil ohne Seamless Roaming verwendet wird.

Voice over IP (VoIP) priorisieren

Wird dieser Client für Kommunikation mit Voice over IP genutzt, so sollte diese Funktion aktiviert werden, um die Sprachdaten verzögerungs- und verzerrungsfrei senden und empfangen zu können.

Aktiviere Tunnel Traffic Monitoring

Wird Tunnel Traffic Monitoring aktiviert, so wird alle 10 Sekunden überprüft, ob der Tunnel-Endpunkt des aktuellen Profils (oder eine andere Adresse hinter dem VPN Gateway) erreicht werden kann. Je nach Verbindungsqualität wird die grafische Darstellung im Monitor alle 10 Sekunden aktualisiert.

Tunnel Traffic Monitoring sollte besonders dann aktiviert werden, wenn sich der Client in einer Umgebung mit schwachen drahtlosen Netzen befindet, wo ein VPN-Tunnel aufgebaut und dies im Client-Monitor mit einem grünen Balken dargestellt werden kann, obwohl keine Daten über das zu schwache Trägermedium übertragen werden können.

PING zum Tunnel-Endpunkt

Bei aktiviertem Tunnel Traffic Monitoring wird in der Standardeinstellung alle 10 Sekunden die Adresse von [Gateway \(Tunnel-Endpunkt\)](#)^[170] des aktuellen Profils angepingt. Soll eine andere Adresse angepingt werden, kann diese unter [Alternative IP-Adresse](#)^[161] eingegeben werden.

Erfolgt keine korrekte Antwort auf den Ping, wird der grüne durchgezogenen Balken im grafischen Feld des Monitors gestrichelt dargestellt. Zusätzlich wird die Meldung "VPN internet connection is temporarily broken" ausgegeben.

Fehlerhafte VPN-Tunnel werden automatisch abgebaut. Anschließend wird versucht, erneut einen VPN-Tunnel aufzubauen.

Alternative IP-Adresse

Bei aktiviertem Tunnel Traffic Monitoring wird in der Standardeinstellung alle 10 Sekunden die Adresse von [Gateway \(Tunnel-Endpunkt\)](#)¹⁷⁰ des aktuellen Profils angepingt. Soll eine andere Adresse angepingt werden, kann diese hier eingegeben werden.

Diese Adresse kann zum Beispiel eine hinter dem VPN Gateway sein, die nur erreicht werden kann, wenn der VPN Tunnel korrekt aufgebaut ist.

IP Broadcast erlaubt [Link-Einstellungen]

Mit diesem Parameter entscheiden Sie, ob die Client Software die Übertragung von IP-Broadcasts zulassen soll. IP-Broadcasts werden z. B. dann eingesetzt, wenn ein LAN-Client (wie etwa die Client Software) im Netz nach einem File Server sucht. Im Fall des Clients wäre das Netz ein Remote-LAN, an welches der Client angeschlossen ist.

IP-Broadcasts werden unterdrückt, wenn das Feld nicht angeklickt ist (standard).

IP-Broadcasts müssen Sie zulassen, wenn Sie DHCP nutzen um eine IP-Adresse vom Zielsystem anfordern zu können.

Quality of Service (für Profil)

Wählen Sie hier ein VPN-Profil aus, für welches eine Konfiguration von [Quality of Service](#)⁸¹ eingesetzt werden soll.

Die Konfiguration von Quality of Service wird unmittelbar nach dem VPN-Verbindungsaufbau mit diesem Profil zum Gateway wirksam.

(In den „[Verbindungsinformationen](#)“³² können während der aktiven Verbindung zu Testzwecken QoS-Gruppen ein- oder ausgeschaltet werden.)

Erweiterte Authentisierung [Authentisierung vor VPN]

Vor dem VPN-Tunnelaufbau können verschiedene Verfahren der Authentisierung gefordert werden.

Biometrische Authentisierung

Dabei gestattet die Konfiguration von „Windows Hello“ unterschiedliche Arten der biometrischen Authentisierung.

Beachten Sie dazu [Fingerabdrucksensor / Biometrische Authentisierung](#) ¹⁶⁴.

Fingerabdrucksensor / Biometrische Authentisierung

Diese Profilkonfiguration bewirkt die Abfrage der Authentisierungsdaten unmittelbar nach Betätigen des Verbinden-Buttons auf der Monitor-Oberfläche des Clients. Erst nach einer erfolgreichen Authentisierung durch ein von „Windows Hello“ vorkonfiguriertes Verfahren (Fingerabdruck-, Gesichtserkennung, PIN-Eingabe etc.) wird der VPN-Tunnelaufbau eingeleitet.

Wird die Option „Fingerabdrucksensor / Biometrische Authentisierung“ aktiviert, muss „Windows Hello“ entsprechend vorkonfiguriert sein.

Beachten Sie dazu die ausführliche Beschreibung unter [Biometrische Authentisierung](#) ²¹¹.

EAP-Authentisierung [vor VPN]

Muss sich der Client mit EAP (Extensible Authentication Protocol) authentisieren, so muss diese Funktion aktiviert werden. Sie bewirkt, dass für dieses Profil die EAP-Konfiguration im Monitor-Menü unter EAP-Optionen eingesetzt wird.

Bitte beachten Sie, dass die EAP-Konfiguration im Monitor-Menü für alle Profile gültig ist und aktiv geschaltet sein muss, wenn diese linkspezifische Einstellung wirksam sein soll.

EAP wird dann eingesetzt, wenn für das wireless LAN ein Access Point verwendet wird, der 802.1x-fähig ist und eine entsprechende Authentisierung verlangt.

EAP kann aber auch dann eingesetzt werden, wenn der Client über einen Router auf ein anderes Netzsegment des Firmennetzes zugreifen möchte.

Generell wird mit EAP verhindert, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.

Nach Konfiguration des EAP muss eine Statusanzeige im grafischen Feld des Monitors erscheinen. Ist dies nicht der Fall, so muss die EAP-Konfiguration im Monitor-Menü aktiv geschaltet werden. Durch einen Doppelklick auf das EAP-Symbol kann das EAP zurückgesetzt werden. Anschließend erfolgt die EAP-Verhandlung erneut.

HTTP-Authentisierung [vor VPN]

Für die automatische HTTP-Authentisierung am Access Point (Hotspot) muss diese Funktion aktiviert werden.

Damit wird ein weiteres Konfigurationsfeld in den Profil-Einstellungen zugeschaltet, in welches die Authentisierungsdaten eingegeben werden können (siehe [HTTP-Anmeldung](#)¹⁵¹).

Bei einem Link mit der Verbindungsart WLAN wird die HTTP-Anmeldung nicht zugeschaltet!

Statt dessen wird mit der Aktivierung dieser Funktion bewirkt, dass für dieses Profil die Authentisierungsdaten aus den WLAN-Einstellungen im Monitor-Menü zum Einsatz kommen.

Bitte beachten Sie, dass die Verbindung über einen HotSpot-Betreiber gebührenpflichtig ist. Sie müssen den Geschäftsbedingungen des HotSpot-Betreibers zustimmen, wenn die Verbindung aufgebaut werden soll.

IPsec-Einstellungen

In diesem Konfigurationsfeld geben Sie die Adresse des IPsec Gateways an. Darüber hinaus legen Sie in Abstimmung mit den Vorgaben der Gegenstelle die Richtlinien fest, die für die Verhandlungen zur IPsec-Verbindung verwendet werden sollen.

Sofern der automatische Modus genutzt wird, schlägt der Client eine Liste von Richtlinien vor, woraus ein Vorschlag zu einer Richtlinie am Gateway der Gegenstelle passen muss. Ist dies nicht der Fall, müssen die Richtlinien in Abstimmung mit der Gegenstelle konfiguriert werden. Dazu selektieren Sie eine der vorgeschlagenen Richtlinien aus der Listbox.

Folgende Richtlinien werden mit der Software ausgeliefert:

IKE-Richtlinie

Unter der Listbox zur IKEv1-Richtlinie liegen die Richtlinien "Pre-shared Key" und "RSA-Signatur" die Sie statt der Standardeinstellung "automatischer Modus" auswählen können.

IKEv2-Richtlinie

Alternativ werden auch IKEv2-Richtlinien zur Verfügung gestellt.

IPsec-Richtlinie

Unter der Listbox zur IPsec-Richtlinie finden sie die Richtlinie "ESP-AES128-MD5". Auch diese können Sie statt der Standardeinstellung "automatischer Modus" selektieren. (Beachten Sie dazu auch die Hinweise zu der Vorschlagsliste für IPsec-Richtlinien).

Unter der Listbox zur IPsec-Richtlinie finden sie die Richtlinie "ESP-3DES-SHA". Auch diese können Sie statt der Standardeinstellung "automatischer Modus" selektieren. (Beachten Sie dazu auch die Hinweise zu der Vorschlagsliste für IPsec-Richtlinien).

Siehe auch:

[Gateway](#) [170] [Tunnel Endpunkt](#) [170]
[Austausch-Modus](#) [Profile] [171] [IKEv2-Richtlinie](#) [Auswahl] [179]
 IKE DH-Gruppe [Auswahl]
[IPsec Policy](#) [Auswahl] [181]
[PFS-Gruppe](#) [Profile] [183]
[Gültigkeitsdauer](#) [184]

Die IPsec-Konfiguration der Richtlinien wird in der Regel nur dann benötigt wenn eine Richtlinien-Anpassung vorgenommen werden muss, weil aus der Vorschlagsliste des Clients keine Richtlinie zu der IPsec-Konfiguration am Gateway passt.

IPsec-Konfiguration

Sie öffnen die IPsec-Konfiguration indem Sie den [Editor]-Button drücken.

Sie finden im Fenster der Richtlinien-Konfiguration zwei Konfigurationsknoten: entsprechend der Konfiguration in den IPsec-Einstellungen unter Austausch-Modus einen zur IKEv1-Richtlinie oder IKEv2-Richtlinie sowie einen zur IPsec-Richtlinie. Richtlinien können hinzugefügt oder modifiziert werden.

Unter der IPsec-Richtlinie finden sie die Richtlinie "ESP-AES128-MD5".

Editieren der Richtlinien

Um die (Standard-)Werte innerhalb der Richtlinien zu editieren, d. h. Parameter so einzustellen oder abzuändern, wie es den Verbindungsanforderungen zur Gegenstelle entspricht, wählen Sie mit der Maus die Richtlinie, deren Werte Sie ändern möchten - die Buttons zur Bedienung werden dann aktiv.

Bearbeiten:

Um eine Richtlinie abzuändern, wählen Sie mit der Maus den Namen der Richtlinie deren Werte Sie ändern möchten und klicken auf "Konfigurieren". Dann öffnet sich das entsprechende Konfigurationsfeld.

Hinzufügen:

Wenn Sie eine neue Richtlinie anlegen möchten, selektieren Sie eine der Richtlinien und klicken auf "Neuer Eintrag". Die neue Richtlinie wird erzeugt. Alle Parameter sind auf Standardwerte gesetzt, bis auf den Namen.

Kopieren:

Um die Parameter-Einstellungen eines bereits definierten Richtlinie zu kopieren, markieren sie die zu kopierende Richtlinie und klicken auf "Kopieren". Daraufhin wird das Parameterfeld geöffnet. Ändern Sie nun den Namen und klicken Sie anschließend Ok. Die neue Richtlinie ist nun angelegt. Die Parameterwerte sind zu denen der kopierten identisch, bis auf den Namen.

Löschen:

Wenn Sie eine Richtlinie aus dem Konfigurationsbaum löschen wollen, selektieren Sie sie und klicken auf "Löschen". Die Richtlinie damit auf Dauer aus der IPsec-Konfiguration gelöscht.

Schließen:


Wenn Sie das IPsec-Feld schließen, kehren Sie zum Monitor zurück. Die Daten werden so wie sie konfiguriert wurden behalten.

Speichern:

Jede Änderung in der IPsec-Konfiguration wird mit "OK" gespeichert.

Richtlinien-Gültigkeit

Die Gültigkeitsdauer wird global für alle Richtlinien eines Profils, sowohl IKE- und IKEv2- als auch IPsec-Richtlinie, über den [Gültigkeit]-Button festgesetzt.

Weitere Informationen zu FIPS siehe: [FIPS-Zertifizierung](#) 

Gateway (Tunnel-Endpunkt)

An dieser Stelle muss die Adresse bzw. der Tunnel-Endpunkt des Gateways eingetragen werden. Sie erhalten sie von Ihrem Administrator entweder als IP-Adresse oder als Namens-String.

IP-Adresse

Wenn das Gateway über eine feste offizielle IP-Adresse verfügt, kann die IP-Adresse eingetragen werden.

Für die Kommunikation zwischen dem Client und dem VPN Gateway kann sowohl IPv4 als auch IPv6 verwendet werden. Dabei muss die eingetragene Adresse den Regeln für die Formatierung von IPv4 bzw. IPv6 entsprechen. Dabei gelten folgende Regeln:

IPv4 (32 Bit-Adressen):

die Adresse muss in der Dezimalschreibweise mit Punkten wie folgt angegeben werden: 15.168.1.253

IPv6 (128 Bit-Adressen):

die Adresse muss in hexadezimaler Schreibweise angegeben werden (8 Gruppen von 4 hexadezimalen Zeichen, getrennt mit Doppelpunkt) z.B. 2001:0db8:ac10:002b:0000:0000:0000:0002

Eine verkürzte Schreibweise ist gestattet:

Führende Nullen können unterdrückt werden wie z.B. 2001:db8:ac10:2b:0:0:0:2

Mehrere Null-Gruppen können zu einem Doppelpunkt zusammengezogen werden, z.B.

2001:db8:ac10:fe01:2b::2

Namens-String

Wenn das Gateway wechselnde IP-Adressen von einem Internet Service Provider erhält, so wird hier der Namens-String eingetragen. Es handelt sich dabei um den DNS-Namen des Gateways, der beim DynDNS Service Provider hinterlegt wurde.

Hinweise

Weitere alternative Tunnel-Endpunkte können sowohl in Form einer IP-Adresse als auch mit DNS-Namen nach dem ersten Tunnel-Endpunkt eingetragen werden. Dabei müssen die Adressen entweder alle durch ein Komma (,) oder alle durch ein Semikolon (;) getrennt werden, wobei keine Leerzeichen vorkommen dürfen.

Insgesamt können maximal vier verschiedene Tunnel-Endpunkte von der Client-Software für einen Verbindungsaufbau nach folgenden Varianten genutzt werden:

1. Werden die alternativen Tunnel-Endpunkte, nur IP Adressen, durch ein Semikolon (;) voneinander getrennt, so erfolgen die Versuche des Verbindungsaufbaus in der angegebenen Reihenfolge der Tunnel-Endpunkte, beginnend beim ersten. Insgesamt unternimmt der Client maximal sieben Versuche eine Verbindung herzustellen.
2. Werden die alternativen Tunnel-Endpunkte, nur IP Adressen, durch ein Komma (,) voneinander getrennt, so erfolgen die Versuche des Verbindungsaufbaus in der angegebenen Reihenfolge der Tunnel-Endpunkte, wobei die Adresse für den ersten Versuch zufällig aus der Reihe der alternativen Adressen selektiert wird. Insgesamt unternimmt der Client maximal sieben Versuche eine Verbindung herzustellen, wobei nach der Beginn-Adresse die angegebene Reihenfolge beibehalten wird.

Austausch-Modus (IPsec) [Profile]

Main Mode (IKEv1):

Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden - daher auch "Identity Protection Mode".

Aggressive Mode (IKEv1):

Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.

IKEv2:

Das Key Exchange Protocol Version 2 (IKEv2) enthält im Client-Unterbau die Mobility Extensions (MOB IKE)

Tunnel IP-Version

Mit diesem Parameter kann konfiguriert werden für welche IP-Version die IPsec-Verhandlung durchgeführt werden soll. Die Konfigurationsmöglichkeit besteht nur für IPsec-Verbindungen mit Schlüsselaustausch über IKEv2!

Nur wenn der [Austausch-Modus IKEv2](#)¹⁷¹ gesetzt ist, wird die Möglichkeit eingeblendet, die Tunnel IP-Version zu wählen:

IPv4

ist die Standardeinstellung (damit ist gewährleistet, dass sich der VPN Client nach einem Software Update genauso wie vorher verhält).

IPv6

Unterstützt das Gateway eines fremden Herstellers IPv6, so kann diese Einstellung gewählt werden. VPN-Gateways anderer Hersteller, welche kein IPv6 unterstützen aber IPv6-Pakete erhalten, verhalten sich unterschiedlich und bauen evtl. keinen Tunnel auf. Deshalb wird empfohlen, in diesem Fall keine IPsec-Verhandlung für IPv6 zu konfigurieren.

IPv4 + IPv6

Mit dieser Einstellung kann zum Beispiel eine Netzwerkarchitektur unterstützt werden, deren Gateway (Zieladresse) nur IPv4 unterstützt, die Geräte des Firmennetzes aber IPv6.

Richtlinien

IKEv1- und IKEv2-Richtlinie [Profile]

IKEv1-Richtlinie

Die IKEv1-Richtlinie wird aus der Listbox selektiert. (Vorkonfiguriert befinden sich dort: "Pre-shared Key" und "RSA-Signatur"). In der Listbox werden namentlich alle IKEv1-Richtlinien aufgeführt, die bei der Installation oder während der IPsec-Konfiguration angelegt wurden.

automatischer Modus: In diesem Fall kann die Konfiguration der IKEv1-Richtlinie über die IPsec-Konfiguration entfallen.

Pre-shared Key: Diese vorkonfigurierte Richtlinie kann ohne PKI-Unterstützung genutzt werden. Beidseitig wird der gleiche "Statische Schlüssel" verwendet.

(Siehe Pre-shared key / Shared secret im Konfigurationsfeld [Identität](#) ).

RSA-Signatur: Diese vorkonfigurierte Richtlinie kann nur mit PKI-Unterstützung eingesetzt werden (Secure Server). Als zusätzliche, verstärkte Authentisierung ist der Einsatz der RSA-Signatur nur sinnvoll unter Verwendung einer Smartcard oder eines Soft-Zertifikats.

Soll der IPsec Client spezielle IKEv1-Richtlinien verwenden, so müssen diese über den [Editor]-Button in den "IPsec-Einstellungen" erstellt oder modifiziert werden.

IKEv2-Richtlinie [Profiles]

Soll der IPsec Client spezielle IKEv2-Richtlinien verwenden, so müssen diese über den [Editor]-Button in den IPsec-Einstellungen erstellt oder modifiziert werden.

Mit dem automatischen Modus muss keine spezielle IKEv2-Richtlinie über das IPsec-Konfigurationsmenü erstellt werden.

Wichtig: Wurde bei Einstellung des Austausch-Modus IKEv2 gewählt, so muss dazu eine der möglichen Authentisierungsmethoden für IKEv2 zugeordnet werden.

IKE DH-Gruppe [IKE-Richtlinie]

Mit der Wahl einer der angebotenen Diffie-Hellman-Gruppen wird festgelegt, wie sicher der Key Exchange erfolgen soll, nach welchem der spätere symmetrische Schlüssel erzeugt wird. Je höher die DH-Gruppe, umso sicherer ist der Key Exchange.

Bei einer Maus-Berührung erscheint ein Tool-Tip für die jeweils gewählte Gruppe mit dem entsprechenden RFC-Standard.

IKEv1-Richtlinie [IPsec-Konfiguration]

Die Parameter in diesem Feld beziehen sich auf den Internet Key Exchange (IKE) mit dem der Kontrollkanal für die SA-Verhandlung aufgebaut wird.


Die IKEv1-Richtlinien, die Sie hier konfigurieren, werden zur Auswahl gelistet.

Funktional unterscheiden sich zwei IKEv1-Richtlinien, die standardmäßig mit der Software ausgeliefert werden: "Pre-shared Key" und "RSA-Signatur". Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf (IKEv1-Richtlinie, Authentisierung, Verschlüsselung), d. h. eine Richtlinie kann aus verschiedenen Vorschlägen bestehen. Eine IKEv1-Richtlinie ist standardmäßig mit der Software ausgeliefert werden: "Pre-shared Key". Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf (IKEv1-Richtlinie, Authentisierung, Verschlüsselung), d. h. eine Richtlinie kann aus verschiedenen Vorschlägen bestehen.


Für alle Benutzer sollten die gleichen Richtlinien einschließlich zugehöriger Vorschläge (Proposals) gelten. D. h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Algorithmen und Parameter

Die folgenden Richtlinien-Parameter gelten für alle Verbindungsprofile gleichermaßen.

[Name \[IKEv1-Richtlinie\]](#) 

[Authentisierung \[IKEv1-Richtlinie\]](#) 

[Verschlüsselung \[IKEv1-Richtlinie\]](#) 

[Hash \[IKEv1-Richtlinie\]](#) 

Name [IKE-Richtlinie]

Geben Sie dieser Richtlinie einen Namen, über den sie später zugeordnet werden kann.

Authentisierung [IKE-Richtlinie]

Bevor der Kontrollkanal für die Phase 1-Verhandlung (IKE Security Association) aufgebaut werden kann, muss beidseitig eine Authentisierung stattgefunden haben.

Pre-shared Key

Zur gegenseitigen Authentisierung wird der gemeinsame Pre-shared Key verwendet. Diesen Schlüssel legen Sie im Konfigurationsfeld [Identität](#) ¹⁸⁸ fest.

RSA Signatur

Zur gegenseitigen Authentisierung wird das Zertifikat verwendet, das Sie für die "Erweiterte Authentisierung" (XAUTH) konfiguriert haben.

(Im Main Mode wird das Zertifikat zusätzlich verschlüsselt. Wenn PKI-Unterstützung für das System vorhanden ist, wählen Sie "RSA-Signatur".)

Verschlüsselung [IKE-Richtlinie]

Nach einem der optionalen Verschlüsselungsalgorithmen erfolgt die symmetrische Verschlüsselung der Messages 5 und 6 im Kontrollkanal, sofern der Main Mode (Identity Protection Mode) gefahren wird. Im automatischen Modus wird die Verschlüsselung vom Kommunikationspartner bestimmt.

Für jeden Vorschlag zur IKE-Richtlinie kann ein eigener Verschlüsselungs-Algorithmus aus dem Pulldown-Menü gewählt werden.

Hash [IKE-Richtlinie]

Modus, wie der Hash-Wert über die ID bzw. das Zertifikat der Messages im Kontrollkanal gebildet wird.

Aus der angezeigten Liste kann ein Wert ausgewählt werden.

IKEv2-Authentisierung [Profile]

Die Teilnehmer an IKEv2-Verhandlungen (Initiator: Secure Client, Gegenstelle: VPN Gateway) müssen sich gegenseitig authentisieren, d.h. Client → VPN Gateway und VPN Gateway → Client.

Am Client kann aus vier möglichen IKEv2-Authentisierungsmethoden ausgewählt werden:

Zertifikat

Dazu konfigurieren Sie zunächst das entsprechende Zertifikat unter [Identität / Zertifikatskonfiguration](#) ¹⁹⁰.

Wird die Authentisierung mit Zertifikat gewählt, authentisieren sich Client und VPN Gateway gegenseitig, indem sie die jeweils lokal gespeicherten Zertifikate nutzen:

Client → VPN Gateway durch Verwendung des Benutzerzertifikats des Clients;

VPN Gateway → Client durch Verwendung des Server-Zertifikats des Gateways.

Pre-shared Key

Dazu tragen Sie zunächst den Pre-shared Key im Konfigurationsfeld [Identität / Pre-shared Key](#) ¹⁸⁹ ein.

Wird die Authentisierung mit Pre-shared Key selektiert, authentisieren sich Client und VPN Gateway gegenseitig, indem sie den jeweils lokal gespeicherten Pre-shared Key nutzen.

EAP

Mit dem Extended Authentication Protocol wird Benutzername und Passwort (VPN-Benutzername und VPN-Passwort) dieses aktuellen Profils eingesetzt.

Benutzername und Passwort werden im Konfigurationsfeld [Identität](#) ¹⁸⁸ festgelegt.

Wird die Authentisierung mit EAP selektiert, wird EAP nur vom Client genutzt um sich gegenüber dem Gateway zu authentisieren. Das Gateway nutzt in diesem Fall sein Aussteller-Zertifikat um sich gegenüber dem Client zu authentisieren. Dies bedeutet, dass das Benutzer-Zertifikat am Client vom gleichen Aussteller wie das Aussteller-Zertifikat am Gateway sein muss.

Das Benutzer-Zertifikat am Client wird im Konfigurationsfeld [Identität / Zertifikatskonfiguration](#) ¹⁹⁰ konfiguriert.

SAML

Security Assertion Markup Language (SAML) ist ein offener Standard, der verknüpfte Authentifizierungs- und Autorisierungsprozesse für Benutzer, Identitätsprovider (IdP) und Dienstanbieter wie den NCP Authentication Provider (AuthProv) vereinfacht und verwaltet.

1. Geben Sie die *URL des Authentication Providers* ein.
2. Geben Sie den zugehörigen *Realm* ein.

Die entsprechenden Angaben erhalten Sie von ihrem Systemadministrator beziehungsweise Identitätsprovider.

Der SAML Authentisierungsvorgang des NCP Secure Enterprise Client erfolgt über den Webbrowser, der sich beim Verbinden automatisch öffnet. Der Nutzer gibt dort seine erforderlichen Zugangsdaten ein, der NCP Authentication Provider prüft deren Gültigkeit beim IdP und der VPN-Tunnel wird hergestellt.

IKEv2-Richtlinie [IPsec-Konfiguration]

Diese Parameter definieren das IKEv2-Protokoll (Internet Key Exchange version 2) womit der Kontrollkanal für die Sicherheitsverhandlung (SA) aufgebaut wird.

Die hier konfigurierten IKEv2-Richtlinien werden zur Auswahl im entsprechenden Pulldown-Menü der IPsec-Konfiguration aufgelistet.

Mit der Software werden keine vorkonfigurierten IKEv2-Richtlinien ausgeliefert.

Algorithmen und Parameter

[Name \[IKEv2-Richtlinie\]](#) ¹⁷⁹
[Verschlüsselung \[IKEv2-Richtlinie\]](#) ¹⁷⁹
[Pseudorandom-Funktion \[IKEv2-Richtlinie\]](#) ¹⁷⁹
[Integritäts-Algorithmus \[IKEv2-Richtlinie\]](#) ¹⁸⁰

Alle hier aufgeführten Parameter können für die jeweils selektierte Richtlinie editiert oder hinzugefügt werden.

Name [IKEv2-Richtlinie]

Geben Sie der neuen Richtlinie beim Hinzufügen zunächst einen Namen, der später in der Auswahlliste angezeigt werden kann.

Verschlüsselung [IKEv2-Richtlinie]

Die symmetrische Verschlüsselung der IKEv2-Meldungen 3 und 4 (zweiter Austausch) im Kontrollkanal erfolgen entsprechend des Verschlüsselungs-Algorithmus, der zwischen Initiator und Gegenstelle während des Meldungen 1 und 2 des IKEv2-Austauschs (erster Austausch) ausgehandelt wurde.

Die verwendeten Schlüssel werden mit der Pseudorandom-Funktion während des ersten Austauschs ausgehandelt. Im automatischen Modus wird die Verschlüsselung vom Kommunikationspartner bestimmt.

Für jeden Vorschlag zur IKEv2-Richtlinie kann ein eigener Verschlüsselungs-Algorithmus aus dem Pulldown-Menü gewählt werden.

Pseudorandom-Funktion [IKEv2-Richtlinie]

Die Zufallswerte, die für Integritätsschutz und Verschlüsselung während des zweiten Austauschs verwendet werden, werden mit Hilfe einer Pseudorandom-Funktion erzeugt, die zwischen Initiator und Gegenstelle während des ersten Austauschs ausgehandelt wird.

Für jeden Vorschlag zur IKEv2-Richtlinie kann eine eigene Pseudorandom-Funktion gewählt werden.

Integritäts-Algorithmus [IKEv2-Richtlinie]

IKEv2 beinhaltet einen Integritätsschutz, um den Prozess der SA-Erzeugung vor der Einflussnahme durch Dritte zu schützen.

Der für den Integritätsschutz benötigte Algorithmus kann für jeden Vorschlag zur IKEv2-Richtlinie eigens gewählt werden.

Wählen Sie für jeden einzelnen Vorschlag einen Integritätsalgorithmus aus der Pulldown-Liste aus.

IPsec-Richtlinie [Auswahl]

Vorkonfiguriert: ESP-AES128-MD5.

In der Listbox werden namentlich alle IPsec-Richtlinien aufgeführt, die bei der IPsec-Konfiguration angelegt wurden.

automatischer Modus:

In diesem Fall kann die Konfiguration der IPsec-Richtlinie über die IPsec-Konfiguration entfallen.

ESP-AES128-MD5:

Wird diese vorkonfigurierte IPsec-Richtlinie gewählt, muss die gleiche Richtlinie mit ihren Vorschlägen für alle Benutzer gültig sein. Dies bedeutet, dass sowohl auf Client- als auch auf Server-Seite die gleichen Vorschläge für die Richtlinien zur Verfügung stehen müssen.

Soll der IPsec Client spezielle Richtlinien verwenden, so müssen diese über den [Editor]-Button in den „[IPsec](#) ¹⁶⁷“-Einstellungen“ erstellt oder modifiziert werden.

IPsec-Richtlinie [Profile]

Die Parameter in diesem Feld beziehen sich auf die Phase 2 der SA-Verhandlung. Die IPsec-Richtlinien die Sie hier konfigurieren, werden zur Auswahl für die intern erzeugte SPD gelistet.

Nur eine IPsec-Richtlinie mit ESP (Encapsulating Security Payload) wird standardmäßig mit der Software ausgeliefert. Da der IPsec-Modus mit AH-Sicherung für flexiblen Remote Access ungeeignet ist, wird nur eine IPsec-Richtlinie mit ESP-Protokoll ausgeliefert. Jede IPsec-Richtlinie listet mindestens einen Vorschlag (Proposal) zu IPsec-Protokoll und Authentisierung auf, d. h. eine Richtlinie kann aus verschiedenen Vorschlägen bestehen.

Für alle Benutzer sollten die gleichen Richtlinien einschließlich zugehöriger Vorschläge (Proposals) gelten. D. h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Algorithmen und Parameter

[Name \[IPsec-Richtlinie\]](#) ¹⁸²
[Protokoll \[IPsec-Richtlinie\]](#) ¹⁸²
[Verschlüsselung \[IPsec-Richtlinie\]](#) ¹⁸²
[Authentisierung \[IPsec-Richtlinie\]](#) ¹⁸²

Name [IPsec-Richtlinie]

Geben Sie dieser Richtlinie einen Namen, über den sie später zugeordnet werden kann.

Protokoll [IPsec-Richtlinie]

Der fest eingestellte Standardwert ist ESP.

Transformation / Verschlüsselung

Für das Sicherheitsprotokoll ESP kann definiert werden mit welchem Algorithmus die Nutzdaten verschlüsselt werden sollen. Wählen Sie einen Algorithmus aus der Liste.

Authentisierung [IPsec-Richtlinie]

Für das Sicherheitsprotokoll ESP kann der Modus der Authentisierung aus der dargestellten Liste ausgewählt werden.

PFS / DH-Gruppe

Mit der Wahl einer der angebotenen Diffie-Hellman-Gruppen wird festgelegt, wie sicher der Key Exchange (PFS) erfolgen soll, nach welchem der spätere symmetrische Schlüssel erzeugt wird. Je höher die DH-Gruppe, umso sicherer ist der Key Exchange.

IPsec-Einstellungen [Richtlinien]

Die IPsec-Richtlinien, die hier konfiguriert werden, stehen global allen Profilen zur Verfügung. In den "IPsec-Einstellungen" des Profils können sie nach Bedarf selektiert werden.

Gültigkeit [IPsec-Einstellungen]

Die Gültigkeit wird global für alle Richtlinien eines Profils, sowohl IKE- als auch IPsec-Richtlinie, über den [Gültigkeit]-Button festgesetzt, der im Konfigurationsfenster IPsec-Einstellungen gedrückt werden kann.

Siehe auch:

[Art der Gültigkeit \[Richtlinie\]](#)
[Dauer der Gültigkeit \[Richtlinie\]](#)
[kBytes \[Richtlinie\]](#)

FIPS-Zertifizierung

Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1747).

Die FIPS Kompatibilität ist immer gegeben, wenn die folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

- Diffie Hellman-Gruppe: Gruppe 2 bis 14 (DH Länge von 1024 Bit bis 2048 Bit)
- Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit
- Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES

Siehe auch:

[IKE-Richtlinie \[Auswahl\]](#)
[IPsec-Richtlinie \[Auswahl\]](#)

Art der Gültigkeit [Richtlinie]

Die Art bestimmt nach welchen Kriterien die Schlüsselgültigkeit festgelegt wird, nach Dauer, nach übertragenen kBytes oder nach beiden. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt.

Gültigkeitsdauer [Richtlinie]

Die Größe der Zeitspanne kann eigens eingestellt werden. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt. (Standard für Phase 1: 8 Std., für Phase 2: 1 Std.)

Volumen [Richtlinie]

Die Menge der hier angegebenen kBytes, die zwischen Client und Server übertragenen werden, bestimmt die Gültigkeitsdauer einer Security Association (siehe [IPsec-Richtlinie](#)). Nach Übertragung der angegebenen kBytes findet eine neuerliche SA-Verhandlung statt. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt.

Erweiterte IPsec-Optionen

Siehe auch die Parameter:

[IPsec-Kompression](#)  185

[Deaktiviere DPD \(Dead Peer Detection\)](#)  185

[Anti-replay Protection](#)  186

[Aktiviere Verhandlung nach RFC 7427](#)  186

[Standard IPsec / UDP Encapsulation](#)  185

[VPN Path Finder](#)  186

IPsec-Kompression

Die Datenübertragung mit IPsec kann ebenso komprimiert werden wie ein Transfer ohne IPsec. Dies ermöglicht eine Steigerung des Durchsatzes um maximal das 3-fache.

Standard IPsec / UDP Encapsulation

Standard IPsec (Port 500) und UDP Encapsulation können alternativ verwendet werden.

Mit UDP-Encapsulation muss an der externen Firewall nur der Port 4500 freigeschaltet werden (anders bei NAT Traversal oder UDP 500 mit ESP). Wird die UDP-Encapsulation verwendet, so kann der Port frei gewählt werden.

Standard für IPsec mit UDP ist der Port 4500, für IPsec ohne UDP der Port 500.

Das NCP Gateway erkennt die UDP-Encapsulation automatisch.

Deaktiviere DPD (Dead Peer Detection)

DPD (Dead Peer Detection) wird automatisch im Hintergrund ausgeführt, sofern dies das Ziel-Gateway unterstützt. Der Client nutzt DPD, um in regelmäßigen Intervallen, die in Sekunden eingestellt werden können, zu prüfen, ob die Gegenstelle noch aktiv ist.

Wenn über den VPN-Tunnel keine Daten empfangen werden, löst der VPN-Client DPD aus. Erhält der Client eine Antwort vom VPN-Gateway, wird weiterhin im konfigurierten Intervall geprüft, ob die Verbindung besteht.

Falls der Client keine Antwort erhält, sendet er standardmäßig innerhalb von 5 Sekunden einen erneuten Versuch, um schnell eine inaktive Sitzung zu erkennen.

Erhält der Client nach wiederholter Prüfung keine Antwort, unterbricht er die Sitzung.

Mit dieser Funktion kann DPD ausgeschaltet werden.

Anti-replay Protection

Zeitversetzt eintreffende IP-Pakete könnten beschädigt sein. Mit dieser Funktion (nach RFC 2406) werden diese Pakete verworfen.

Folgende Meldung zeigt das Erkennen und Verwerfen der Pakete an:

Esp: Warning - AntiReplay error on sequence number=xxxx

Aktiviere Verhandlung nach RFC 7427

Die Client Software unterstützt für den IKEv2 die zertifikatsbasierte Authentisierung nach RFC 7427, womit auch modernes Padding-Verfahren (RSASSA-PSS) möglich ist.

Standard: aktiviert

VPN Path Finder

Der VPN Path Finder setzt als Gegenstelle ein VPN Gateway mit NCP VPN Path Finder Technology voraus (z. B. den NCP Secure Server 8.00 oder höher). Dort muss in den Einstellungen zu VPN / IPsec für das lokale System ein alternativer Port konfiguriert sein.

Die Funktionalität VPN Path Finder schaltet automatisch auf das alternative Verbindungsprotokoll TCP Encapsulation mit SSL Header (Port 443) um, sobald Standard IPsec über Port 500 bzw. UDP Encapsulation über einen frei konfigurierbaren Port nicht möglich ist.

Dies ist dann von Bedeutung, wenn für den Client nur der HTTPS Port 443 zur Verfügung steht und eine reine IPsec-Verbindung nicht möglich ist, wie dies z. B. in Hotels oder an Hotspots der Fall sein kann.

Wenn für die Verbindung ein Proxy Server vorgeschaltet sein muss, kann dieser im Konfigurationsmenü unter Proxy für VPN Path Finder eingestellt oder konfiguriert werden.

Wurde die Verbindung mit dieser Technologie über den Port 443 aufgebaut, wird dies über ein Icon in der Statusanzeige des Monitors (rechts unter dem HQ/Gateway) angezeigt.

Das Icon erscheint in der Monitor-Oberfläche bei der VPN-Einwahl.

RFC 7427 Padding-Verfahren

Ist für IKEv2 die zertifikatsbasierte Authentisierung nach RFC7427 aktiviert, kann über diesen Parameter das gewünschte Padding-Verfahren ausgewählt werden.

Folgende Padding-Verfahren sind möglich:

- PKCS#1 v.1.5 Padding
- RSASSA-PSS

Die Standardeinstellung ist: RSASSA-PSS

Hinweis: Die hier am Client konfigurierte Authentisierung für IKEv2, einschließlich des Padding-Verfahrens, muss von der Gegenstelle unterstützt und akzeptiert werden.

IKEv2 RSA Authentisierung mit PRF-Hash

Der Parameter IKEv2 RSA Authentisierung mit PRF-Hash bewirkt, dass als Hash-Algorithmus für die IKEv2-RSA Authentisierung nicht der nach RFC empfohlene Standard (SHA-1) verwendet wird.

Stattdessen wird mit Einschalten dieser Funktion der aktuell über die [Pseudorandom Funktion](#)^[179] (PRF) konfigurierte Algorithmus aus den IKEv2-Richtlinien verwendet.

In der Standardeinstellung ist diese Funktion deaktiviert.

Identität

Entsprechend des Sicherheitsmodus IPsec können noch detailliertere Sicherheitseinstellungen vorgenommen werden.

Siehe auch folgende Parameter:

[IKE ID-Typ \[Identität\]](#)

[IKE ID \[Identität\]](#)

[Zertifikatskonfiguration](#)

[Pre-shared Key](#)

IKE ID-Typ [Identität]

Bei native IPsec wird zwischen abgehenden und eingehenden Verbindungen unterschieden. Der Wert, den der Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein.

Folgende ID-Typen stehen zur Auswahl:

- IP-Adresse
- Fully Qualified Domain Name
- Fully Qualified Username
- ASN1 Distinguished Name
- IP Subnet-Adresse
- ASN1 Gruppen-Name
- String für Gruppenidentifikation

IKE ID [Identität]

Bei IPsec wird zwischen abgehenden und eingehenden Verbindungen unterschieden. Der Wert, den der Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein.

Automatisches Setzen des VPN-Benutzernamens

Der Administrator kann zentralseitig für den VPN-Benutzernamen eine Umgebungsvariable, %USERNAME% oder %NCPUSERNAME%, vorkonfigurieren. Diese Variable wird dann aus den Settings des Client-PCs ausgelesen und automatisch als VPN-Benutzername verwendet.

Wird %USERNAME% vorgegeben, so wird beim ersten Start des Clients diese Windows-Umgebungsvariable einmalig ausgelesen und bleibt auch über nachfolgende Neustarts erhalten.

Wird %NCPUSERNAME% vorgegeben, so wird bei jedem Start des Clients diese Windows-Umgebungsvariable erneut ausgelesen, sodass je nach Windows-Logon für verschiedene Benutzer, der jeweilige USERNAME aus den Windows-Settings übernommen wird.

Diese Variablen können nicht eingesetzt werden, wenn das Windows-Logon über den Credential Provider erfolgt.

Entsprechend dem [IKE ID-Typ](#) ¹⁸⁹ muss die zugehörige "IKE ID" als String eingetragen werden.

Pre-shared Key

"IPsec Pre-shared Key" ist ein Passwort, das für den Tunnelaufbau benötigt wird. Nur wenn dieses Passwort beim VPN-Gateway und dem Secure Client übereinstimmt, wird der Tunnel aufgebaut. Das Passwort kann bis zu 16 Zeichen lang sein.

Zertifikatskonfiguration [Profile]

Ein über die Zertifikatskonfiguration des Client-Monitors eingesetztes Zertifikat, kann hier für die erweiterte Authentisierung (XAUTH) selektiert werden.

keine:

Für Datenverschlüsselung und Authentisierung wird kein Zertifikat eingesetzt.

Standard PKI-Konfiguration:

Die Zertifikatskonfiguration eines Clients älter als Version 9.1 wird bei einem Update auf diese Version automatisch in die Standard PKI-Konfiguration konvertiert. Ebenso wird die Standard PKI-Konfiguration nach einer Erstinstallation der Version 9.1 eingerichtet wenn eine Testverbindung mit Zertifikat angelegt wird.

Extended Authentication (XAUTH)

Am Entry Client ist Extended Authentication (XAUTH Protokoll, Draft 6) standardmäßig nicht aktiv. Sie kann an dieser Stelle eingeschaltet werden wenn sie vom IPsec Gateway unterstützt wird. Zusätzlich zum Pre-shared Key können dann noch folgende Parameter zur Authentisierung genutzt werden:

Benutzername [Identität]

Den Benutzernamen für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

Passwort [Identität]

Das Passwort für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

Alternativ kann auch ein Zertifikat aus der Zertifikatskonfiguration genutzt werden.

Wird das Internet Key Exchange Protocol Version 2 (IKEv2) eingesetzt, so wird als Authentisierungsprotokoll Microsoft CHAP Version 2 (MSCHAPv2) verwendet.

Benutzername [Identität]

Den Benutzernamen für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

Hinweis: Dieser Parameter wird nur benötigt, um Zugriff auf das Gateway der remote Seite zu bekommen.

Passwort [Identität]

Das Passwort für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

Hinweis: Dieser Parameter wird nur benötigt, um Zugriff auf das Gateway der remote Seite zu bekommen.

VPN-Zugangsdaten aus Konfiguration

Als Zugangsdaten für ein VPN können folgende Einträge ausgelesen und verwendet werden:

Zugangsdaten aus obiger Konfiguration

Dies bedeutet, dass die in diesem Parameterfeld unter "Benutzername" und "Passwort" gemachten Angaben zur erweiterten Authentisierung verwendet werden.

Zugangsdaten aus dem Zertifikatsfeld (E-Mail)

Dies bedeutet, dass statt "Benutzername" und "Passwort" der E-Mail-Eintrag des Zertifikats verwendet wird.

Zugangsdaten aus dem Zertifikatsfeld (Common Name)

Dies bedeutet, dass statt "Benutzername" und "Passwort" der Benutzer-Eintrag des Zertifikats verwendet wird.

Zugangsdaten aus dem Zertifikatsfeld (Seriennummer)

Dies bedeutet, dass statt "Benutzername" und "Passwort" die Seriennummer des Zertifikats verwendet wird.

Zugangsdaten aus dem Zertifikatsfeld (User Principal Name, UPN)

Dies bedeutet, dass statt "Benutzername" und "Passwort" der User Principal Name (Anmeldename@Domain-Name) verwendet wird, vorausgesetzt das Attribut ist im Zertifikat vorhanden.

Zugangsdaten aus dem Zertifikatsfeld (Subject Alternative Name: E-Mail)

Dies bedeutet, dass statt "Benutzername" und "Passwort" der Anzeige-Name der E-Mail-Adresse verwendet wird.

IPsec Adresszuweisung

Unter Einsatz von native IPsec können die IP-Adressen des Clients auf unterschiedliche Weisen, die hier konfiguriert werden können, zugewiesen werden.

Siehe:

[Zuweisung der privaten IP-Adresse](#) ¹⁹³

[DNS-Server](#) ¹⁹⁴

[DNS Domains im Tunnel auflösen](#) ¹⁹⁴

Zuweisung der privaten IP-Adresse

In diesem Parameterfeld kann angegeben werden, wie die IP-Adresse zugewiesen werden soll.

IKE Config Mode

Mit IKE Config Mode (Draft 2) werden dynamisch die IP-Adressen des Clients, des DNS-Servers sowie der Domain Name zugewiesen.

Für die NAS-Einwahl können alle bisherigen WAN-Schnittstellen verwendet werden.

Bei "IPsec-Tunneling" wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau.

Der Einsatz von NAT Traversal erfolgt beim Client automatisch und ist immer nötig, wenn seitens des Zielsystems ein Gerät mit Network Address Translation zum Einsatz kommt.

Lokale IP-Adresse verwenden

In diesem Fall wird die aktuell in den Netzwerkeinstellungen des PCs konfigurierte IP-Adresse (auch DHCP) für den IPsec Client genutzt.

Dies ist die Standard-Einstellung für den Entry Client.

IP-Adresse manuell vergeben

IP-Adresse und die Subnet-Maske können hier eingegeben werden. In diesem Fall wird die hier eingetragene Adresse genutzt, unabhängig von der Konfiguration in den Netzwerkeinstellungen.

DHCP über IPsec

Alternativ zur Verwendung des IKE Config Modes kann auch ein DHCP Server des Gateways genutzt werden. Dabei wird über den VPN-Tunnel dem Client in einer DHCP-Verhandlung die IP-Adresse zugewiesen.

DNS / WINS Server

In diesem Parameterfenster kann ein durch die PPP-Verhandlung automatisch zugewiesener Server durch alternative Server ersetzt werden. Dazu muss in den Netzwerk-Einstellungen des Betriebssystems der DNS-Modus eingestellt sein.

Je nach Anwendung können ein oder zwei DNS-Server eingetragen werden. Genutzt wird immer der jeweils erste. Wird am Client kein DNS-Server eingetragen, wird der über die PPP-Verhandlung zugewiesene Server genutzt.

erster / zweiter DNS-Server: Der zuerst eingetragene DNS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt. Der zweite DNS-Server dient als Backup-DNS-Server.

Domain Name

Dies ist der Domain Name der sonst per DHCP dem System in den Netzwerkeinstellungen übergeben wird.

Zum Beispiel: Host-Name.Domain-Name (Rechner1.Firma.3erStock.at)

DNS Domains im Tunnel auflösen

Tragen Sie hier die Domänennamen ein, die clientseitig auf dem virtuellen NCP-Adapter aufgelöst werden sollen.

Split Tunneling

Hier können genau die IP-Netze definiert werden, über die der Client via VPN-Tunnel kommunizieren kann. Wenn Tunneling genutzt wird und hier keine Einträge erfolgen, so wird die Verbindung immer zum Tunnel-Endpunkt des Gateways aufgebaut. Soll alternierend einerseits ein Tunneling zur Zentrale erfolgen, andererseits über das Internet kommuniziert werden, so müssen hier die IP-Netze eingetragen werden, die vom Client erreicht werden sollen. Sie können dann zwischen dem Internet und dem Gateway der Firmenzentrale hin und her springen. Dies wird auch als „Netzwerk Gegenstelle“ bezeichnet.

Klicken Sie auf den Button „Hinzufügen“, so können Sie in das daraufhin erscheinende Fenster IP-Adresse und Netzmaske einzelner Netze eintragen.

Siehe auch:

[Entfernte Netzwerke \(IPv4\)](#) 

[Auch lokale Netze im Tunnel weiterleiten](#) 

[Entfernte Netzwerke \(IPv6\)](#) 

Entfernte Netzwerke (IPv4)

Hier tragen Sie die Adresse des IP-Netzes ein, das vom Client über das VPN-Gateway erreicht werden soll. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Machen Sie in dieser Liste keinen Eintrag, so werden alle IP-Pakete über den VPN-Tunnel gesendet.

Bitte achten Sie ferner darauf, dass die IP-Adresse des VPN-Gateways nicht im Bereich der Netz-Adresse liegt.

Maximal können zwanzig Netze konfiguriert werden.

Entfernte IP-Netzmasken (IPv4)

Hier tragen Sie die zugehörige Netzmaske des IP-Netzes ein. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Achten Sie darauf, dass die IP-Adresse des VPN-Gateways nicht im Bereich der Netz-Adresse liegt.

Nutzen Sie die Möglichkeit des Split Tunneling, so beachten Sie auch die Hinweise zu DNS-Anfragen.

Alternative Adresseingabe

Wird bei der Eingabe der IP-Adresse zusätzlich die Präfixlänge eingegeben (z.B. 175.16.15.0/24), so wird beim Verlassen des Eingabefelds aus der Präfixlänge die Subnetz-Maske erstellt und in die entsprechende Spalte eingetragen.

Auch lokale Netze im Tunnel weiterleiten

Wenn der Datenverkehr des lokalen Netzes über VPN-Tunneling weitergeleitet werden soll, so muss diese Funktion (*Full Local Network Enclosure Mode*) aktiviert werden.

Entfernte Netzwerke (IPv6)

Die Dateneingabe für ein IPv6-Netz erfolgt über die Eingabe der IP-Adresse und der angehängten Präfixlänge (z.B. 2001:0db8:85a3:08d3::/64)

Maximal können zwanzig Netze konfiguriert werden.

VPN-Bypass

Hier kann aus der Bypass-Liste der Applikationen und Domänen, die am VPN-Tunnel vorbei kommunizieren und über das Internet erreicht werden sollen, die gewünschte ausgewählt werden.

Bitte beachten Sie, dass für diese Anwendungen und Domänen keine Firewall-Regel des Client greift. Weder kann die Kommunikation weiter eingeschränkt werden, noch lassen sich in der Protokollierung der Client Firewall die Verbindungen darstellen.

(Siehe auch [VPN-Bypass-Funktion](#) ²⁰⁹)

Zertifikats-Überprüfung

Überprüfung der Zertifikatsinhalte

Im Parameterfeld "Zertifikats-Überprüfung" kann pro Zielsystem des Secure Clients vorgegeben werden, welche Einträge in einem Zertifikat der Gegenstelle (Secure Server) vorhanden sein müssen (siehe: Eingehendes Zertifikat anzeigen, Allgemein).

Siehe auch die Parameter:

[Benutzer des eingehenden Zertifikats](#)  198

[Aussteller des eingehenden Zertifikats](#)  199

[Fingerprint des Aussteller-Zertifikats](#)  200

[Benutze SHA1 Fingerprint statt MD5](#)  200

[Weitere Zertifikats-Überprüfungen](#)  201

Benutzer des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Benutzers, soweit bekannt - auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu, welche Einträge bei "eingehendes Zertifikat anzeigen" unter Benutzer aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

cn	Common Name / Name
s	Surname / Nachname
g	Givenname / Vorname
t	Title / Titel
o	Organization / Firma
ou	Organization Unit / Abteilung
c	Country / Land
st	State / Bundesland, Provinz
l	Location / Stadt, Ort
email	e-mail / E-Mail
sn	Serialnumber / Seriennummer

Beispiel:

cn=VPNGW*, o=MyCompany, c=de

Der Common Name des Security Servers wird hier nur bis zur Wildcard "*" überprüft. Alle nachfolgenden Stellen können beliebig sein, etwa 1 - 5 als Numerierung. Die Organization muss in diesem Fall immer "MyCompany" sein und das Land Deutschland.

Aussteller des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Ausstellers, soweit bekannt - auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu welche Einträge bei "eingehendes Zertifikat anzeigen" unter Aussteller aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

cn	Common Name / Name
s	Surname / Nachname
g	Givenname / Vorname
t	Title / Titel
o	Organization / Firma
ou	Organization Unit / Abteilung
c	Country / Land
st	State / Bundesland, Provinz
l	Location / Stadt, Ort
email	e-mail / E-Mail
sn	Serialnumber / Seriennummer

Beispiel:

cn=My Common Name

In diesem Beispiel wird nur der Common Name des Ausstellers überprüft.

Fingerprint des Aussteller-Zertifikats

Um zu verhindern, dass ein Unberechtigter, der die vertrauenswürdige CA imitiert, ein gefälschtes Aussteller-Zertifikat verwenden kann, kann zusätzlich der Fingerprint des Ausstellers, soweit bekannt, eingegeben werden.

Geprüft wird die Übereinstimmung der eingegebenen Zeichen. Diese müssen vom ersten Zeichen des Fingerprints an eingegeben werden. Die Genauigkeit der Prüfung steigt mit der Anzahl der Zeichen.

Benutze SHA1 Fingerprint statt MD5

Der Algorithmus zur Erzeugung des Fingerprints kann MD5 (Message Digest 5) oder SHA1 (Secure Hash Algorithm 1) sein.

Weitere Zertifikats-Überprüfungen

Neben der Zertifikats-Überprüfung nach Inhalten erfolgt am Client eine weitere Zertifikatsprüfung in mehrfacher Hinsicht.

1. Auswahl der CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies erfolgt, indem er die CA-Zertifikate seiner Wahl in das Verzeichnis %INSTALLDIR%\CACERTS\ spielt.

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

Wird am Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Verzeichnis %INSTALLDIR%\CACERTS\. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande.

Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

2. Überprüfung der Zertifikats-Erweiterung

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zertifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den Client und den Secure Server sind drei Erweiterungen von Bedeutung:

- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier

extendedKeyUsage:

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der Client, ob der definierte erweiterte Verwendungszweck "SSL-Server-Authentisierung" enthalten ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D. h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck "SSL-Server-Authentisierung" beinhalten muss.

subjectKeyIdentifier / authorityKeyIdentifier:

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann keine Übereinstimmung erkannt werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades.

(Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.)

3. Überprüfung von Sperrlisten

Zu jedem Aussteller-Zertifikat kann dem Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Installations-Verzeichnis unter "\crls" gespielt. Ist eine CRL vorhanden, so überprüft der Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Gleiches gilt für eine ARL (Authority Revocation List), die in das Installations-Verzeichnis unter "\arls" gespielt werden muss.

Sind eingehende Zertifikate in den Listen von CRL oder ARL enthalten, wird die Verbindung nicht zugelassen.

Sind CRLs oder ARLs nicht vorhanden findet keine diesbezügliche Überprüfung statt.

Link Firewall

Die Firewall-Einstellungen können für alle Netzwerkadapter wie auch für RAS-Verbindungen genutzt werden. Die aktivierte Link Firewall wird in der grafischen Oberfläche des Clients als Schutzschild mit Pfeilen dargestellt.

Grundsätzliche Aufgabe einer Firewall ist es, zu verhindern, dass sich Gefahren aus anderen externen Netzen (Internet) im eigenen Netzwerk ausbreiten. Deshalb wird eine Firewall auch am Übergang zwischen Firmennetz und Internet installiert. Sie prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis vorher festgelegter Konfiguration, ob dieses Paket passieren darf oder nicht.

Die hier zu aktivierende Firewall arbeitet nach dem Prinzip der Stateful Inspection. Zum einen verhindert diese Funktionalität den unbefugten Zugriff auf Daten und Ressourcen im zentralen Datennetz. Zum anderen überwacht sie als Kontrollinstanz den jeweiligen Status aller bestehenden Internet-Verbindungen. Die Stateful Inspection Firewall erkennt darüber hinaus, ob eine Verbindung "Tochterverbindungen" geöffnet hat - wie beispielsweise bei FTP oder Netmeeting - deren Pakete ebenfalls weitergeleitet werden müssen. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen Datenaustausch nach vereinbarten Regeln genutzt werden darf. Siehe auch die Parameter:

[Stateful Inspection](#) ²⁰³

[Ausschließlich](#) ²⁰³ [Kommunikation im Tunnel zulassen](#) ²⁰³

[In Kombination mit dem Microsoft DFÜ-Dialer nur Tunnel-Kommunikation](#) ²⁰³

Stateful Inspection

aus: Die Sicherheitsmechanismen der Firewall werden nicht in Anspruch genommen.

immer: Die Sicherheitsmechanismen der Firewall werden immer in Anspruch genommen, d. h. auch wenn keine Verbindung aufgebaut ist, ist der PC vor unberechtigten Zugriffen geschützt.

bei bestehender Verbindung: Das Endgerät ist dann nicht angreifbar, wenn eine Verbindung besteht.

Ausschließlich Kommunikation im Tunnel zulassen

Bei aktivierter Firewall kann diese Funktion zusätzlich eingeschaltet werden, um in ein- und ausgehender Richtung ausschließlich VPN-Verbindungen zuzulassen. Jeder weitere Datenverkehr wird abgelehnt.

In Kombination mit dem Microsoft DFÜ-Dialer

Bei Verwendung des Client-Monitors wird bei Aktivierung dieser Funktion verhindert, dass eine Kommunikation über den DFÜ-Dialer zum Internet stattfinden kann.

Auch komprimierte Verbindungen des RAS-Dialers können vom Client als normaler IP-Verkehr überwacht werden, da sowohl die Kompression (CCP) als auch die VanJacobson-IP-Header-Kompression (im IPCP) nicht mehr ausgehandelt werden.

Funktionen


In den folgenden Abschnitten sind Einsatzmöglichkeiten spezieller Funktionen, deren Konfiguration und die Bedienung über das Menü der Client-Oberfläche beschrieben:+

[Die Funktionalität der Home Zone](#)  205

[Die VPN-Bypass-Funktion](#)  209

[Biometrische Authentisierung](#)  211

[Credential Provider](#)  213

[Quality of Service \(Beschreibung\)](#)  215

Home Zone

Die Funktionalität der Home Zone

Arbeitet ein Anwender im Firmennetz, so kann er darin all die Ressourcen nutzen, die ihm administrativ durch Zugangsberechtigungen und Firewall-Einstellungen zur Verfügung gestellt werden.

Auf diese Ressourcen hat er auch von zu Hause aus als Teleworker über das VPN (oder SSL-VPN) Zugriff, wo er an seinem Rechner wie im LAN der Firma arbeiten kann. Bestimmte Geräte aber, wie zum Beispiel ein Drucker oder spezielle Anwendungen (eine eigene Datenbank, FTP- oder Web-Server), die in seinem Heimnetzwerk lokalisiert sind, stehen nicht zur Verfügung.

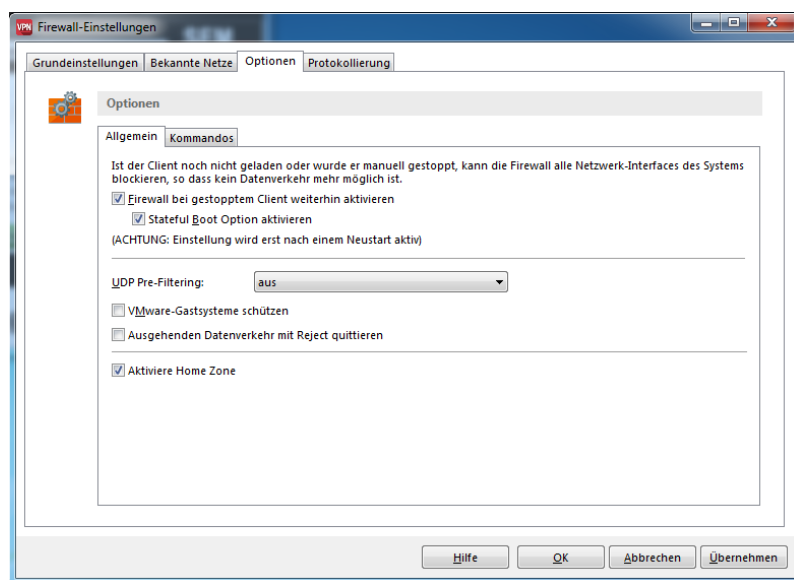
Die Funktionalität der Home Zone wurde als Option in der Firewall implementiert, um auch die Ressourcen eines Heimnetzwerks zur Verfügung stellen zu können, ohne dass die Administration jedes einzelne IP-Netz im Home-Office seiner Mitarbeiter kennen muss.

Ebenso kann die Funktionalität der Home Zone auch für verschiedene andere Aufgaben-Stellungen genutzt werden, zum Beispiel um Service-Technikern das Arbeiten an Maschinensteuerungen zu ermöglichen, wobei die Maschinen über TCP/IP angebunden sind, das Netzwerk, mit dem sich der Techniker verbindet, dabei aber kein „bekanntes Netz“ mit vollkommen transparenter Kommunikation sein soll, aber auch kein „unbekanntes Netz“ mit vollkommen restriktiver Kommunikation und die IP-Adress-Bereiche auch nicht als Ausnahmen in der Firewall vorgesehen werden können, weil sie unter Umständen im Vorfeld nicht bekannt sind.

Sobald sich der Rechner des Anwenders in einer Home Zone befindet und über den Client auf diesem Rechner eine VPN-Verbindung in die Firma aufgebaut wird, greifen die jeweiligen Firmenrichtlinien.

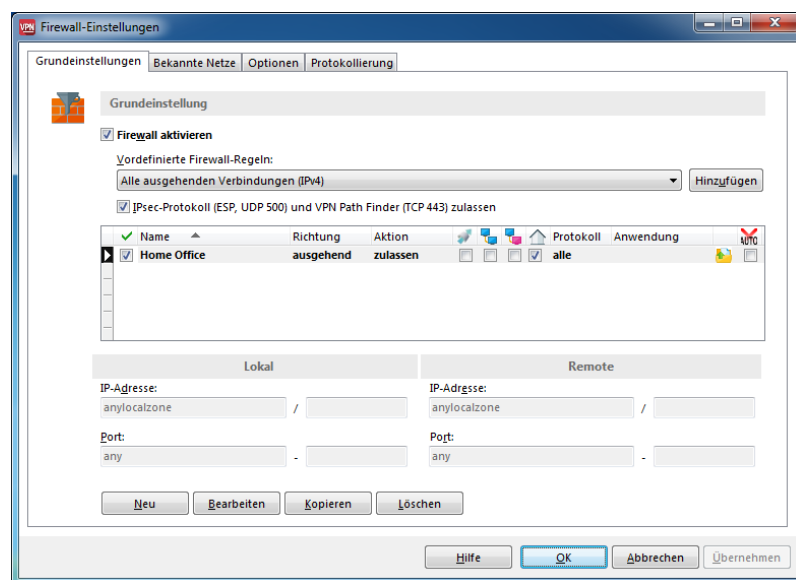
Konfiguration am Client

- Dazu muss in den [Firewall-Optionen unter „Allgemein“](#)⁷⁴ die Home Zone aktiviert werden. Intern wird LAN oder WLAN genutzt, worüber die Verbindung ins private Netz (Heimnetzwerk) hergestellt werden kann (siehe Abb. unten).



Andere Schnittstellen, z.B. Mobile Broadband oder DFÜ, können nicht für eine Home-Zone genutzt werden. Über die Mac-Adresse des Default Gateways dieses aktiven Netzadapters wird die zugehörige Home Zone gesetzt. Dies bedeutet, dass der Administrator keine Kenntnisse über das Heimnetzwerk benötigt.

- Zusätzlich muss die [vordefinierte Firewall-Regel „Home Zone“ der „Firewall / Grundeinstellungen“](#)⁵⁷ für die aktivierte Firewall hinzugefügt werden und wirksam sein. Falls der Administrator eine Regel so einschränken möchte, dass eine Firewall-Regel ausschließlich für lokal am Endgerät angeschlossene IP-Netzwerke gilt, lässt sich in der Konfiguration einer Firewall-Regel eine neue Variable neben „anyv4“ und „anyv6“ verwenden: „anylocalzone“.



Da dem Administrator die IP-Adresse des privaten Netzwerks in der Regel nicht bekannt ist, wird für den IP-Adressbereich automatisch „anyLocalZone“ gesetzt. Ebenfalls automatisch gesetzt wird für lokale und remote Ports „any“, womit der Anwender kompletten Zugriff auf die Home Zone hat, d.h. sein Netzwerk. Gegebenenfalls können die IP-Adressbereiche und die zulässigen Ports modifiziert werden.

- Außerdem lassen sich automatisiert Aktionen ausführen, sobald am Client das Regelwerk für Home Zone aktiviert wird, genau wie dies bereits für „bekanntes Netz“ oder „unbekanntes Netz“ möglich ist. Die Voreinstellung dazu erfolgt über das Konfigurationsmenü des Clients unter [„Firewall / Bekannte Netze / Aktionen“](#)^[69].

Wurden diese Einstellungen vorgenommen, wird im Verbinden-Menü des Monitors der Menüpunkt [„Home Zone“](#)^[29] angezeigt.

Bedienung über die Client GUI

Der Anwender kann jetzt mit einem Klick die [Home Zone setzen oder löschen](#)^[29]. Eine gesetzte und nutzbare Home Zone wird in der grafischen Oberfläche des Monitors und im Statusdialog des Clients als Haus-Symbol auf dem Desktop hinter dem Schutzschild der aktiven Firewall angezeigt. (Bild unten)



Mit dem Setzen der Home Zone

wird das Regelwerk für „Home-Zone angewandt und die Hardware-Adresse des Default Gateways des aktiven Netzwerk-Adapters in der Konfiguration des Clients gespeichert. Sind mehrere Netzwerk-Schnittstellen mit jeweils einem Default-Gateway aktiv, so wird die Default-Route zum Speichern der Hardware-Adresse berücksichtigt, die die kleinste Metric aufweist.

Soll zu einem späteren Zeitpunkt ein anderes privates Netz als Home Zone genutzt werden, so reicht ein erneuter Klick des Anwenders auf „Setzen“ aus, wenn er sich in diesem neuen privaten Netzwerk befindet. Die jeweils für die Home Zone gesetzte MAC-Adresse wird im [Client Info Center](#)^[129] angezeigt. Bei jedem neuen Setzen der Home Zone wird die vorherige MAC-Adresse überschrieben.

Mit diesen Einstellungen ist es dem Anwender möglich, alle Ressourcen in seinem Heimnetzwerk zu nutzen.

Mit dem Löschen der Home Zone

kann diese wieder gelöscht bzw. ausgeschaltet werden, z.B. auch wenn diese Funktion versehentlich aktiviert ist und durch das Haus-Symbol angezeigt wird. Sicheres Löschen der Home Zone ist jedoch nur gewährleistet, wenn sich der Netzwerkadapter in der Home Zone befindet (ein ggf. externer Adapter auch gesteckt ist) und wenn nach dem Löschen ein Reboot erfolgt.

Der Anwender, der sich nach der Arbeit in der Home Zone seines Home Office vor Ort in der Firma wieder über LAN/WLAN am Firmennetzwerk anmeldet, ist automatisch nicht mehr mit der Home Zone seines privaten Netzes verbunden. Der Zugriff auf die Ressourcen im Firmennetz wird wieder administrativ durch Zugangsberechtigungen und Firewall-Einstellungen (ggf. durch Friendly Net Detection) zur Verfügung gestellt.

Besucht der Benutzer das Netzwerk, in dem er Home-Zone gesetzt hat, erneut nach einiger Zeit und hat zwischenzeitlich den Schalter „Home-Zone – Setzen“ oder „Home-Zone – Löschen“ nicht betätigt, so erkennt der Client das Netzwerk anhand der Hardware-Adresse des Routers wieder und wendet auf die Schnittstelle, auf der der Router mit der gespeicherten Hardware-Adresse aktiv ist, das Regelwerk für Home-Zone erneut an. Ist gleichzeitig eine weitere, grundsätzlich zugelassene Schnittstelle aktiv, in der das Default-Gateway eine andere Hardware-Adresse besitzt, wird auf dieser das Regelwerk für Home-Zone nicht aktiv.

Im Monitor-Log des Clients
werden Home Zone-Aktivitäten wie folgt protokolliert:

... enter home-zone

... exit home-zone

(Siehe [Hilfe / Logbuch](#) ¹²⁶)

VPN-Bypass

Die VPN-Bypass-Funktion

Die VPN-Bypass-Funktion ermöglicht es einem Administrator trotz deaktiviertem [Split Tunneling](#)¹⁹⁵ zu bestimmen, welche Anwendungen oder Domänen direkt mit dem Internet kommunizieren und welche ihre Daten durch den VPN-Tunnel schicken. Die auf diese Weise erstellten VPN-Bypassregeln sorgen dafür, dass bestimmte Apps/Websites/Domänen ihre Daten über eine gewöhnliche Verbindung übertragen. Gleichzeitig stellt eine Bypassregel aber auch sicher, dass keinerlei Daten entsprechender Apps/Websites/Domänen in den VPN-Tunnel gelangen.

Diese Funktion kann unter anderem dazu genutzt werden, um regelmäßig notwendige, nicht sicherheitsrelevante Datenübertragung von der zentralen Infrastruktur fernzuhalten, um deren Performance nicht zu beeinträchtigen. Zum Beispiel könnten Updates des Betriebssystems oder des Virenschanners (mit bekannter Domäne) ohne Umweg über die VPN-Verbindung zugelassen werden, oder bei bestimmten Cloud-Services der direkte Zugriff der Anwendungen über das Internet ermöglicht werden.

Konfiguration am Client

Die Konfiguration der Applikationen und Domänen für den VPN-Bypass kann durch den Administrator der VPN-Umgebung oder durch den Benutzer direkt am Client erfolgen.

- Als Vorbereitung für die Funktionalität werden im Konfigurationsmenü der Client GUI unter „[VPN-Bypass](#)“⁷⁹ zunächst die Applikationen oder Domänen festgelegt, deren Kommunikation am VPN-Tunnel vorbei stattfinden soll. Dabei kann gegebenenfalls noch festgelegt werden, ob dies nur für TCP oder UDP-Kommunikation erfolgen soll.

Hinweis: Bei den Pfadangaben für Applikationen können einzelne Verzeichnisebenen durch eine Wildcard (*) ersetzt werden. Die Wildcard deckt dabei immer nur eine Verzeichnisebene ab. Sollen weitere Unterebenen berücksichtigt werden, werden zusätzliche Wildcards benötigt.

Achtung: Bei falscher Verwendung der Wildcard kann die VPN-Bypass-Konfiguration Verzeichnisse abdecken, die nicht dafür vorgesehen sind.

Beispiel:

- Pfadangabe für eine Applikation

```
C:\Program Files\NCP\SecureClient\ncpmon.exe
```

```
C:\Program Files\NCP\*\ncpmon.exe
```

```
C:\Program Files\*\*\ncpmon.exe
```

- Domainangabe

```
support.ncp-e.com
```

```
ncp-e.com
```

Die entstandene Liste der Anwendungen und Domänen für einen VPN-Bypass am VPN-Tunnel vorbei, wird für die weitere Konfiguration benötigt.

- In den VPN-Profilen des Clients, die über das Konfigurationsmenü der GUI unter „Profile“ geöffnet werden, kann im Konfigurationsfeld „VPN-Bypass“ die Applikation oder Domäne aus der [VPN-Bypass-Liste](#) gewählt werden, die während der VPN-Verbindung des aktuell selektierten VPN-Profiles am Tunnel vorbei kommunizieren soll.
- Mit der DNS-Eingabe für VPN-Bypass wird sichergestellt, dass für externe VPN-Bypass-Ziele die Namensauflösung durch den VPN-Tunnel nur durch die beiden konfigurierten DNS-Server erfolgt. Hierfür können in der VPN-Bypass-Konfiguration ein primärer und ein sekundärer DNS, wahlweise als IPv4 oder IPv6-Adresse, eingetragen werden.

Hinweis: Die konfigurierten DNS-Server sind ausschließlich für konfigurierte Webdomains wirksam. Konfigurierte Applikationen innerhalb der VPN-Bypass-Funktionalität werden nicht berücksichtigt.

Beachten Sie, dass für diese Anwendungen und Domänen keine Firewall-Regel des Client greift. Weder kann die Kommunikation weiter eingeschränkt werden, noch lassen sich in der Protokollierung der Client Firewall die Verbindungen darstellen.

Biometrische Authentisierung

Die Funktionalität der biometrischen Authentisierung via „Windows Hello“ vor VPN-Tunnelaufbau steht ab der Client-Version 11.1 zur Verfügung.

Ab der Client-Version 11.1 kann vom Anwender vor jedem manuellen VPN-Verbindungsaufbau eine Benutzerauthentisierung abverlangt werden. Diese Funktionalität bietet erweiterten Schutz vor Zugriffen unbefugter Dritter auf einen nicht-gesperrten Arbeitsplatzrechner. Der nicht berechtigte VPN-Tunnelaufbau in das zentrale Firmennetz wird damit ausgeschlossen. Voraussetzung zur Nutzung dieser Funktionalität ist die Verwendung ab Windows 8.1 und der darin enthaltenen Anmeldeoption „Windows Hello“.

Als Bestandteil des Windows-Betriebssystems muss „Windows Hello“ entsprechend konfiguriert werden, damit sich ein Benutzer an seinem lokalen Rechner anmelden kann. Diese lokale Authentisierung sollte nach der Konfiguration der zur Verfügung stehenden Schnittstellen durch die Erfassung biometrischer Daten erfolgen, wie beispielsweise durch Fingerabdruck- oder Gesichtserkennung. Je nach Priorisierung der zur Verfügung stehenden Daten kann sie auch durch Eingabe von Benutzer-ID und Passwort vorgenommen werden.

Konfiguration

Für den VPN-Tunnelaufbau kann auch die Client-Software das Verfahren der lokalen Authentisierung erzwingen und vom Benutzer des Clients die gleichen Authentisierungsdaten anfordern wie bei der Benutzeranmeldung am Windows-System. Dazu muss in den Einstellungen des jeweiligen VPN-Profiles am Client folgende Konfiguration vorgenommen werden: Unter „Erweiterte Authentisierung“ muss die Option „Fingerabdrucksensor / biometrische Authentisierung“ aktiviert werden.

Diese Profilkonfiguration bewirkt die Abfrage der Authentisierungsdaten unmittelbar nach Betätigen des Verbinden-Buttons auf der Monitor-Oberfläche des Clients. Erst nach einer erfolgreichen Authentisierung durch ein von „Windows Hello“ vorkonfiguriertes Verfahren (Fingerabdruck-, Gesichtserkennung, PIN-Eingabe etc.) wird der VPN-Tunnelaufbau eingeleitet.

Voraussetzung für die Sicherheit der erweiterten Authentisierung, die mittels „Windows Hello“ für den sicheren Tunnelaufbau eingesetzt wird, ist immer die persönliche Interaktion des Benutzers. Aus diesem Grund kann die erweiterte Authentisierung für einen automatisierten Tunnelaufbau ohne Benutzeraktion (durch die Verbindungsmodi „automatisch“ oder „immer“) nicht eingesetzt werden. Der konfigurierte „Verbindungsmodus“ im VPN-Profil des Clients muss auf „manuell“ oder „wechselnd“ gesetzt sein, um dieses Leistungsmerkmal nutzen zu können. Diese Einstellung kann im jeweiligen VPN-Profil unter „Verbindungssteuerung / Verbindungsaufbau“ überprüft und geändert werden.

Verfahren

Der vom Betriebssystem gestartete Dialog zur lokalen Authentisierung hat das Erscheinungsbild der Windows-Version und variiert entsprechend der Hardware-Ausstattung des Rechners. Besitzt der Rechner keine Hardware zur biometrischen Authentisierung, oder ist diese nicht aktiviert, erscheint der Dialog zur Eingabe von Benutzername und Passwort, wobei der Benutzername nicht mehr eingegeben werden kann, da dies bereits beim Start des Rechners zur lokalen Authentisierung erfolgte.

Der Dialog enthält Texte vom Betriebssystem und des Clients, weshalb bei unterschiedlicher Spracheinstellung von Betriebssystem und Client unterschiedliche Sprachen im Dialog erscheinen können.

Credential Provider

Der Credential Provider stellt zum Zeitpunkt der Benutzeranmeldung am Windows-System einen VPN-Tunnel in die Firmenzentrale zur Verfügung. Die Benutzerauthentisierung geschieht dadurch nicht am lokalen Windows-System, sondern an der zentralen Windows-Domäne. Die Verwendung des Credential Providers schließt die Nutzung der biometrischen Authentisierung vor dem VPN-Tunnelaufbau im Client jedoch aus.

Parametersperren und Konfigurationssperren

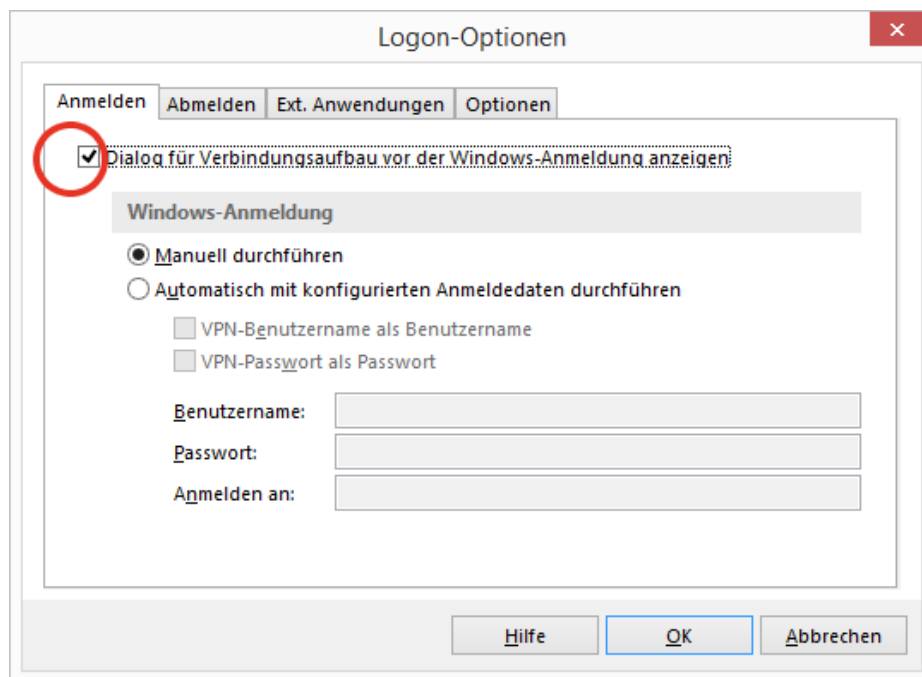
Für die Benutzer eines Entry Clients kann administrativ eine Konfigurationssperre gesetzt werden, sodass dieses Feature in den Profileinstellungen des Clients für den Anwender nicht mehr sichtbar und damit auch nicht mehr konfigurierbar ist.

Credential Provider




Der Credential Provider wird automatisch immer mit der Client-Software eingerichtet. Auf dem Desktop zeigt er das Aussehen der Client GUI.

Initialisierung

Die Initialisierung des Credential Provider erfolgt über die Client-Oberfläche: Dazu wird im Hauptmenü „Konfiguration“ unter „Logon-Optionen“ im Register für [Anmelden](#)¹¹² die Option „Dialog für Verbindungsaufbau vor der Windows-Anmeldung anzeigen“ aktiviert. (Abb. unten)



(Weitere Konfigurationsoptionen stehen nach der Aktivierung dieser Funktion unter [Ext. Anwendungen](#)¹¹⁴ und [Optionen](#)¹¹⁵ zur Verfügung.)

Nach dem Abmelden vom System oder einem Neustart wird im Windows-Startbildschirm unter dem Symbol für die Benutzeranmeldung  das VPN-Symbol für den Pre-Logon  (und dem Produktnamen des Clients) angezeigt. Das VPN-Symbol erscheint dann auf dem Windows-Startbildschirm in grüner Farbe  wenn der Pre-Logon bereits erfolgt ist.

Oberfläche des Credential Providers

Wird der Pre-Logon selektiert, erscheint die Oberfläche des Credential Providers und die Aufforderung die Verbindung herzustellen. Die VPN-Verbindung zur Anmeldung an die Windows-Domäne kann nun mit einem Klick auf „Verbinden“ aufgebaut werden. (Je nach Profil- bzw. Zertifikatskonfiguration kann eine PIN-Eingabe nötig sein.)

Oberfläche des Client-Monitors

Nach der Benutzeranmeldung an der Domäne wechselt die Oberfläche von der des Credential Providers zu der des Clients. Mit dieser Client GUI werden dem Benutzer alle Konfigurationsmöglichkeiten des Clients zur Verfügung gestellt.

Nur in dieser Oberfläche können auch die Einstellungen zur Domänen-Anmeldung modifiziert werden, wie oben zur Initialisierung beschrieben wurde.

Pre-Logon-Funktionen

In der Konfigurationsoberfläche des Credential Providers können jene Funktionen ausgeführt und Konfigurationsmöglichkeiten vorgenommen werden, die im Pre-Logon möglich sind.

Im Menü „Verbindung“ ist dies neben manuellem Verbinden/Beenden und dem Abruf statistischer Informationen insbesondere die Funktion der [Hotspot-Anmeldung](#)²⁹.

Im Menü „Konfiguration“ können [WLAN-Einstellungen](#)⁸⁷ vorgenommen werden.

Benutzerauthentifizierung mit dem Credential Provider

Der Credential Provider stellt zum Zeitpunkt der Benutzeranmeldung am Windows-System einen VPN-Tunnel in die Firmenzentrale zur Verfügung. Die Benutzerauthentifizierung erfolgt dadurch nicht am lokalen Windows-System, sondern an der zentralen Windows-Domäne. Die Nutzung der biometrischen Authentifizierung durch „Windows Hello“ vor dem VPN-Tunnelaufbau ist ausgeschlossen.

QoS (Beschreibung)

Quality of Service (QoS) oder Dienstgüte ist die Qualität eines Kommunikationsdienstes aus der Sicht des Anwenders. Die Dienstgüte wird daran gemessen, wie der Dienst den entsprechenden Anforderungen entspricht.

In Netzwerken werden für gewöhnlich alle Datenpakete, gleich aus welchen Anwendungen, gleichbehandelt. Solange im Netzwerk nur Datenpakete von Anwendungen übertragen werden, die wenig Bandbreite erfordern, macht sich eine voll ausgelastete Bandbreite allenfalls durch kurze Verzögerungen während der Datenübertragung bemerkbar.

Bei Echtzeit-Anwendungen, die eine höhere Bandbreite benötigen, wie Voice Over IP Telefonie oder auch Videostreaming, skype youtube etc., wirken sich Verzögerungen und Paketverluste negativ aus. Bei VoIP Telefonie äußert sich dies durch abbrechende, verzögerte Gespräche oder durch eine niedrige Sprachqualität, bei Videostreaming durch unsynchronisierte Übertragung von Bild und Ton.

Verantwortlich hierfür ist das Standardnetzwerkprotokoll TCP/IP, welches nicht unterscheidet von welcher Anwendung welche Daten gesendet wurden und die Daten gleichbehandelt überträgt. Dies bedeutet auch, dass bei Auslastung der Bandbreite auf alle in der Übertragung befindlichen Datenpakete gleichmäßig aufgeteilt wird und dabei die Wiedergabequalität der Echtzeit-Anwendungen leidet.

Mithilfe des „Quality of Service“ (QoS, Dienstgüte) können nun bestimmte Datenpakete priorisiert werden. Mit der Priorisierung des Datenstroms können Echtzeit-Anwendungen bei der Zuteilung von Bandbreite bevorzugt werden, sodass immer die benötigte Bandbreite für eine qualitativ hochwertige Anwendung ohne Abbrüche oder Verzerrungen bereitgestellt wird. Andere bandbreitenintensive Anwendungen müssen dann warten, bis ausreichend Bandbreite wieder freigegeben ist. Dies äußert sich dann durch langsamere Geschwindigkeiten, die aber bei Nicht-Echtzeit-Programmen wenig kritisch sind.

QoS dient dabei als „Bandbreiten-Management“, das keine zusätzliche Bandbreite zur Verfügung stellt, sondern lediglich bestimmte Datenübertragungen bevorzugt.

Clients im VPN

Im Client wurde diese Management-Funktion hinzugefügt. Über diese Funktion kann eine Mindestbandbreite des Datenverkehrs für eine bestimmte Anwendung oder einen Dienst definiert werden. Somit kann z. B. erreicht werden, dass bei hoher Netzwerklast anstehende VoIP-Pakete bevorzugt versendet werden, um immer eine gute Sprachqualität zu gewährleisten. Ein Herunterladen eines Updates, welches im Hintergrund erfolgt, geschieht entsprechend langsamer.

Bei der Konfiguration von Quality of Service ist Folgendes zu beachten

Eine korrekte Verteilung der Datenraten laut QoS-Konfiguration kann nur erreicht werden, wenn die „Maximal verfügbare Netzwerkbandbreite“ der tatsächlichen Bandbreite entspricht oder darunter liegt. Dabei sollte die Netzwerkbandbreite möglichst konstant bleiben. Bei einem zu gering konfigurierten Maximum wird eventuell ein Teil der Bandbreite nicht produktiv genutzt. (Für QoS werden keine Log-Dateien protokolliert.)

VPN und Verbindungsrichtung

Die Priorisierung der Pakete erfolgt nur für den Datenverkehr der VPN-Verbindung, nicht über andere LAN-Adapter.

QoS kann nur für das Senden von Daten vom Client zum Gateway eingesetzt werden. Der Empfang von Daten vom Gateway wird nicht durch QoS reguliert.

Verfügbare Netzwerkbandbreite

Bei der Konfiguration von QoS muss ein Wert für die „Maximal verfügbare Netzwerkbandbreite“ konfiguriert sein. Dieser Wert kann zwischen 1 und 100 Megabit pro Sekunde liegen und muss in ganzen Zahlen angegeben werden.

Ein VPN-Profil mit einer QoS-Konfiguration kann maximal mit einer Bandbreite von diesem konfigurierten Wert Daten senden, auch wenn mehr verfügbar wäre. D.h. die Datenrate wird dabei immer auf den zur Verfügung gestellten Maximalwert eingegrenzt. Wird ein zu hoher Wert konfiguriert, so entsprechen die tatsächlichen Datenraten der konfigurierten QoS-Gruppen nicht den erwarteten Ergebnissen.

Schwankende Bandbreiten

Bei stark schwankenden Bandbreiten, wie bei WLAN oder Mobilfunk, kann die konfigurierte Mindestbandbreite einer QoS-Gruppe nicht garantiert werden. Die konfigurierte Bandbreite wird im Mittel zwar erreicht, kann temporär jedoch darunter liegen.

Prinzipiell wird QoS auch bei Seamless Roaming, dem automatischen Wechsel des Verbindungsmediums, unterstützt. Tatsächlich sind die maximalen Bandbreiten bei den verschiedenen Verbindungsmedien (LAN, WLAN, Mobilfunk) in der Regel stark unterschiedlich, sodass der entsprechende QoS-Wert nicht korrekt konfiguriert werden kann.

Filtertypen

Bei einem konfigurierten Filter des Typs „Verzeichnis“ werden Anwendungen in Unterverzeichnissen nicht berücksichtigt. Die Konfiguration des Verzeichnisnamens ist „case sensitive“.

Bei einem konfigurierten Filter des Typs „Anwendung“ ist die Konfiguration des Anwendungsnamens „case sensitive“.

Es ist nicht möglich, den Dateitransfer des Windows Explorers in eine QoS Gruppe aufzunehmen. Als „work around“ kann man eine Anwendung „unknown“ konfigurieren. Dadurch werden jedoch evtl. auch andere Anwendungen, die dem VPN Dienst als „unknown“ genannt werden, mit berücksichtigt.

IPsec RFCs

RFCs implemented / used in Client Products

IPsec general

rfc4301- Security Architecture for the Internet Protocol

rfc4945 - The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

IANA defined parameters and transform IDs

- IKEv1 - Internet Key Exchange (IKE) Attributes
- IKEv2 - Internet Key Exchange Version 2 (IKEv2) Parameters
- ISAKMP (ESP, ...) - "Magic Numbers" for ISAKMP Protocol

ESP

- rfc4303- IP Encapsulating Security Payload (ESP)
- rfc3948- UDP Encapsulation of IPsec ESP Packets

IKEv1

- rfc3526- More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- rfc3947- Negotiation of NAT-Traversal in the IKE

IKEv2

- rfc7296- Internet Key Exchange Protocol Version 2 (IKEv2)
- rfc4555- IKEv2 Mobility and Multihoming Protocol (MOBIKE)
- rfc5685- Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)
- rfc5739- IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)
- rfc7383- Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation
- rfc7427- Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)
 - rfc3279, Section 2.2.3 - ECDSA Signature Algorithm (ECDSA)
 - rfc3447, Section 8 - RSASSA-PSS und RSASSA-PKCS1-v1_5 signature schemes

ECC

- rfc5639- Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation

ECC in DH

- rfc5903- Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2
- rfc6954- Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2)
- rfc6989- Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)

Ecc in AUTH Payload

- rfc4754- IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)

Algorithms

CBC

- rfc2451- The ESP CBC-Mode Cipher Algorithms

AES-CTR

- rfc3686- Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)
- rfc5930- Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol

AES-GCM

- rfc4106- The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- rfc5282- Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
- rfc6379- Suite B Cryptographic Suites for IPsec

Padding

- rfc3447, Section 8- RSASSA-PSS und RSASSA-PKCS1-v1_5 signature schemes

EAP

- IANE EAP Registry
- rfc3748- Extensible Authentication Protocol (EAP)

Werkzeuge

Im Installationsverzeichnis des Clients befinden sich Applikationen, womit der Client über Batch oder Script gesteuert werden kann.

Die Kommandozeilen-Tools müssen mit den entsprechenden Kommandos und Parametern in einer DOS-Box im Installationsverzeichnis gestartet werden:

[Beschreibung der Kommandos, Parameter und Rückgabewerte von NCPClientCMD.EXE](#)  ²²⁰

Folgende Funktionserweiterungen können mit NCPRWSNT.EXE genutzt werden:

[Funktionserweiterungen mit NCPRWSNT.EXE](#)  ²³⁴

Informationen zu den *Allgemeinen Registry-Werten* finden Sie [hier](#)  ²³⁶.

Kommandozeilen-Schnittstelle NCPClientCMD.EXE

NcpClientCmd /connect

Der Befehl stößt den Verbindungsaufbau an, ohne zu warten bis die Verbindung erfolgreich aufgebaut ist.

Befehl:

NcpClientCmd /connect [ProfileName] [user] [pwd]

Parameter:

ProfileName = Bezeichnung des Profils mit dem die Verbindung aufgebaut werden soll. Wird kein Profilname angegeben, wird die Verbindung mit dem aktuellen Profil aufgebaut (optional)

UserID = Benutzername für die VPN-Einwahl (optional)

Password = Passwort für die VPN-Einwahl (optional)

Rückgabewerte:

0 = OK - Der Verbindungsaufbau wurde gestartet

11 = Fehler - System ist bereits im bekannten Netz

12 = Fehler - Der übergebene Profilname existiert nicht

13 = Fehler - PIN für Zertifikat nicht eingegeben

14 = Fehler - Keine Authentisierungsdaten für Internet-Einwahl vorhanden

15 = Fehler - Keine Authentisierungsdaten für VPN-Einwahl vorhanden

Beispiel:

NcpClientCmd /connect MyProfil user MyUserID pwd MyPassort

NcpClientCmd /connectWait

Der Befehl startet den Verbindungsaufbau und bleibt solange aktiv bis die Verbindung erfolgreich aufgebaut wurde oder der übergebene Timeout (Standardwert 60 Sekunden) erreicht ist.

Befehl:

NcpClientCmd /connectWait [Timeout]

Parameter:

Timeout = Maximale Wartezeit für den Verbindungsaufbau in Sekunden

Rückgabewert:

0 = OK - Verbindung wurde erfolgreich aufgebaut

10 = Fehler - Timeout ist abgelaufen

11 = Fehler - System ist bereits im bekannten Netz

13 = Fehler - PIN für Zertifikat nicht eingegeben

14 = Fehler - Authentisierungsdaten für Internet-Einwahl fehlen

15 = Fehler - Authentisierungsdaten für VPN-Einwahl fehlen

XX = Fehler - Spezifischer Fehlercode

NcpClientCmd /disconnect

Der Befehl leitet die Trennung der Verbindung ein, ohne zu warten bis die Verbindung vollständig getrennt ist.

Befehl:

NcpClientCmd /disconnect

Parameter:

keine

Rückgabewert:

0 = Verbindung wird getrennt

NcpClientCmd /disconnectWait

Der Befehl trennt die Verbindung und bleibt solange aktiv bis die Verbindung vollständig getrennt ist.

Befehl:

NcpClientCmd /disconnectWait

Parameter:

keine

Rückgabewert:

0 = Verbindung wird getrennt

16 = Neue Konfiguration konnte nicht gelesen werden

146 = Der NCP RWSNT-Dienst ist nicht gestartet

NcpClientCmd /getConnectionState

Der Befehl gibt den aktuellen Verbindungsstatus zurück.

Befehl:

NcpClientCmd /getConnectionState

Parameter:

keine

Rückgabewert:

0 = Verbindung ist getrennt

1 = Verbindung wird aufgebaut

2 = Verbindung ist erfolgreich aufgebaut

XX = Spezifischer Fehlercode

20 = NCP RWSNT-Dienst ist nicht gestartet

NcpClientCmd /getServiceState

Der Befehl gibt den aktuellen Status des zentralen NCPRWSNT-Dienstes zurück.

Befehl:

NcpClientCmd /getServiceState [Time]

Parameter:

Time = Zeit in Sekunden wie lange auf den Dienst gewartet werden soll

Rückgabewert:

0 = Ok

20 = Fehler - NCPRWSNT-Dienst ist nicht gestartet

21 = Fehler - NCPRWSNT-Dienst antwortet nicht

NcpClientCmd /select

Der Befehl wechselt das aktive Profil.

Befehl:

NcpClientCmd /select

Parameter:

ProfileName = Profil auf das gewechselt werden soll

Rückgabewert:

0 = Ok - Das aktive Profil wurde gewechselt

1 = Fehler - Falsche Parameterübergabe

12 = Fehler - Der übergebene Profilname existiert nicht

Beispiel:

NcpClientCmd /select "Testverbindung IPsec IKEv1"

NcpClientCmd /sleep

Über diese Funktion kann eine beliebige Wartezeit zwischen den Befehlen in einer Batch-Datei gesetzt werden.

Befehl:

NcpClientCmd /sleep

Parameter:

Time = Wartezeit in Millisekunden

Rückgabewert:

0 = Ok

NcpClientCmd /stop

Der Befehl stoppt alle zum NCP Secure Entry Client NCP Secure Entry Client gehörigen Anwendungen und Dienste.

Befehl:

NcpClientCmd /stop

Parameter:

keine

Rückgabewert:

0 = Ok

NcpClientCmd /start

Der Befehl startet alle zum NCP Secure Entry Client gehörigen Anwendungen und Dienste.

Befehl:

NcpClientCmd /start

Parameter:

keine

Rückgabewert:

0 = Ok

NcpClientCmd /setInitUser

Soll die Personalisierung des Clients ohne Interaktion mit dem Benutzer erfolgen, können über diesen Befehl die Authentisierungsdaten hinterlegt werden.

Befehl:

NcpClientCmd /setinituser [Password]

Parameter:

InitUserId = Benutzername für die Personalisierung

Password = Password für die Personalisierung (optional)

Rückgabewert:

0 = OK

1 = fehlgeschlagen

NcpClientCmd /rsuAutoAnswer

Mit diesem Befehl kann vorgegeben werden, wie die Benutzer-Interaktion bei einem Konfigurations-Update erfolgen soll.

Befehl:

NcpClientCmd /rsuAutoAnswer

Optionen:

- Off = Interaktion mit dem Benutzer
- Yes = Konfiguration soll ohne Benutzer-Interaktion übernommen werden
- No = Konfiguration soll ohne Benutzer-Interaktion abgelehnt werden

Rückgabewert:

0 = OK - Option wurde gesetzt

1 = Fehler - Option konnte nicht gesetzt werden

Beispiel:

NcpClientCmd /rsuAutoAnswer off

NcpClientCmd /ginaInstall

Dieser Befehl installiert den Credential Provider und gibt den Installationsstatus zurück.

Befehl:

NcpClientCmd /ginaInstall

Parameter:

keine

Rückgabewert:

0 = OK - Installation war erfolgreich

1 = Fehler - Installation ist fehlgeschlagen

NcpClientCmd /ginaUninst

Dieser Befehl deinstalliert den Credential Provider und gibt den Installationsstatus zurück.

Befehl:

NcpClientCmd /ginaUninst

Parameter:

keine

Rückgabewert:

0 = OK - Deinstallation war erfolgreich

1 = Fehler - Deinstallation ist fehlgeschlagen

NcpClientCmd /ginaOn

Dieser Befehl aktiviert den Credential Provider damit er bei der Windows-Anmeldung angezeigt wird.

Beachten Sie, dass der Credential Provider bereits installiert sein muss. Falls es bei der Installation nicht installiert wurde, kann er mit dem Befehl "ncpClientCmd [/ginaInstall]" nachträglich installiert werden.

Befehl:

NcpClientCmd /ginaOn

Parameter:

keine

Rückgabewert:

0 = OK - Aktivierung war erfolgreich

1 = Fehler - Aktivierung ist fehlgeschlagen

NcpClientCmd /ginaOff

Dieser Befehl deaktiviert den Credential Provider damit er bei der Windows-Anmeldung nicht angezeigt wird.

Beachten Sie, dass der Credential Provider mit diesem Befehl nicht deinstalliert wird, sondern nur ausgeblendet. Zur Deinstallation muss der Befehl "ncpClientCmd [/ginaUninst]" ausgeführt werden.

Befehl:

NcpClientCmd /ginaOff

Parameter:

keine

Rückgabewert:

0 = OK - Deaktivierung war erfolgreich

1 = Fehler - Deaktivierung ist fehlgeschlagen

NcpClientCmd /ginalInfo

Dieser Befehl gibt zurück ob der Credential Provider installiert ist.

Befehl:

NcpClientCmd /ginalInfo

Parameter:

keine

Rückgabewert:

0 = nicht installiert

1 = installiert

NcpClientCmd /writeReaderIni

Dieser Befehl schreibt die "reader.ini" in das übergebene Verzeichnis. Die "reader.ini" wird am SEM benötigt, um dort die Chipkartenleser der lokalen Systeme bekannt zu geben.

Befehl:

NcpClientCmd /writeReaderIni

Parameter:

OutputPath = Ausgabeverzeichnis für die "reader.ini" (ohne Angabe eines Dateinamen)

Rückgabewert:

0 = OK - Die "reader.ini" wurde erfolgreich geschrieben

1 = Fehler - Falsche Parameterübergabe

10 = Fehler - Die "reader.ini" konnte nicht geschrieben werden

NcpClientCmd /writeClientInfoCenterData

Dieser Befehl gibt die Informationen des "Client Info Center" aus und erstellt die Datei "ClientInfoCenter.txt". Wird kein Ausgabepfad angegeben, wird die Datei ins Dokumente-Verzeichnis des Benutzers geschrieben.

Befehl:

NcpClientCmd /writeClientInfoCenterData [OutputPath]

Parameter:

OutputPath = Ausgabeverzeichnis für die "ClientInfoCenter.txt" (ohne Angabe eines Dateinamens)

Rückgabewert:

0 = OK

1 = fehlgeschlagen

NcpClientCmd /ShowLogs

Diese Funktion zeigt die aktuell gehaltenen Log-Ausgaben in der Konsole an und schreibt sie in das Log-Verzeichnis des Secure Client. Wird der Wert -1 übergeben, werden sie solange protokolliert, bis der Aufruf mit STRG-C abgebrochen oder die Konsole geschlossen wird. Es werden maximal die Log-Ausgaben der letzten 7 Tage gespeichert.

Befehl:

NcpClientCmd /showLogs [Timer]

Parameter:

Timer = Wieviele Sekunden die Log-Ausgaben protokolliert werden sollen. Wird kein Wert übergeben, werden nur die aktuell gehaltenen Log-Ausgaben angezeigt und gespeichert.

Rückgabewert:

0 = OK

NcpClientCmd /firewallOff

Über diesen Befehl kann die Firewall temporär geöffnet werden. Die Funktion muss in den Firewall-Einstellungen aktiviert sein.

Befehl:

NcpClientCmd /firewallOff [Password]

Parameter:

Password = Passwort über das die Funktion geschützt ist

Timeout = Dauer der temporären Freischaltung

Rückgabewert:

0 = OK - Firewall wurde geöffnet

1 = Fehler - Falsche Parameterübergabe

11 = Fehler - Firewall ist nicht aktiviert

12 = Fehler - Die Authentisierung ist fehlgeschlagen

13 = Fehler - Die Funktion ist nicht erlaubt

14 = Fehler - Kein Timeout übergeben

NcpClientCmd /firewallOn

Über diesen Befehl kann die temporär geöffnete Firewall wieder vorzeitig aktiviert werden.

Befehl:

NcpClientCmd /firewallOn

Parameter:

keine

Rückgabewert:

0 = OK - Firewall wurde wieder aktiviert

11 = Fehler - Firewall ist nicht aktiviert

13 = Fehler - Die Funktion ist nicht erlaubt

NcpClientCmd /actionUpdateOverLan

Dieser Befehl wird intern vom Update-Client aufgerufen wenn ein Konfigurations-Update über LAN erfolgte. Er startet die in der GUI konfigurierte externe Anwendung für die Option "Anwendungen bei einem Konfigurations-Update über LAN starten".

Im Kommandozeilen-Tool wird geprüft ob die GUI gestartet ist. Ist sie gestartet, werden die externen Anwendung gestartet, ansonsten liest das Tool die Konfiguration und startet die Anwendungen.

Befehl:

NcpClientCmd /actionUpdateOverLan

Parameter:

keine

Rückgabewert:

0 = OK

NcpClientCmd /actionUpdateOverVpn

Dieser Befehl wird intern vom Update-Client aufgerufen wenn ein Konfigurations-Update über VPN erfolgte. Er startet die in der GUI konfigurierte externe Anwendung für die Option "Anwendungen bei einem Konfigurations-Update über VPN starten".

Im Kommandozeilen-Tool wird geprüft ob die GUI gestartet ist. Wenn ja, werden die externen Anwendung gestartet, ansonsten liest das Tool die Konfiguration und startet die Anwendungen.

Befehl:

NcpClientCmd /actionUpdateOverVpn

Parameter:

keine

Rückgabewert:

0 = OK

NcpClientCmd /CheckNewCert

Dieser Befehl wird intern vom Update-Client aufgerufen wenn ein Konfigurationsupdate erfolgte. Der Aufruf prüft ob über den SEM ein neues Zertifikat übertragen wurde.

Befehl:

NcpClientCmd /CheckNewCert

Parameter:

keine

Rückgabewert:

0 = OK

NcpClientCmd /CheckNcpdb

Dieser Befehl wird intern vom Update-Client aufgerufen wenn durch den Update Client die Lizenz-Datenbank (ncp.db) geändert wurde.

Befehl:

NcpClientCmd /CheckNcpdb

Parameter:

keine

Rückgabewert:

0 = OK

NcpClientCmd /ReadCnf

Dieser Befehl liest die Konfigurationsdatei (ncpphone.cfg) und eine evtl. vorhandene Konfiguration vom SEM (ncpphone.cnf) ein und erzeugt daraus die neue Konfigurationsdatei.

Das Kommando wird vom Update-Client nach einem Konfigurations-Update über LAN aufgerufen, damit die erhaltene Konfiguration eingelesen und aktiv wird.

Ist die GUI getartet, wird die neue Konfiguration darüber eingelesen, ansonsten durch das Kommandozeilen-Tool.

Befehl:

NcpClientCmd /ReadCnf

Parameter:

keine

Rückgabewert:

0 = OK

1 = Fehlgeschlagen

NcpClientCmd /getConnectionMedium

Dieser Befehl liest den Medientyp aus und gibt das aktuell gesetzte Verbindungsmedium des Clients zurück.

Befehl:

NcpClientCmd /getConnectionMedium

Parameter:

keine

Rückgabewert:

1 = Verbindung ist getrennt

8 = LAN

18 = Mobilfunknetz

20 = WLAN

21 = Automatische Medienerkennung

100 = NCPRWSNT-Dienst ist nicht gestartet

Funktionserweiterungen mit NCPRWSNT.EXE

Folgende Funktionserweiterungen des NCP Clients (mit NCPRWSNT.EXE) können genutzt werden, sofern die entsprechenden Konfigurationsparameter und deren Werte in die Registry eingetragen werden.

Parameter der Registry, die von ncprwsnt.exe geschrieben werden

64-bit: [HKEY_LOCAL_MACHINE\Software\Wow6432Node\NCP engineering GmbH\NCP RWS/GA\6.0]

32-bit: [HKEY_LOCAL_MACHINE\Software\Ncp Engineering GmbH\NCP RWS/GA\6.0]

Key	Type	Meaning	Value
SecClCSI.	REG_DWORD	current connection state	1 = connected / 0 = disconnected
SecClFNDState	REG_DWORD	current fnd state	1 = fnd on an adapter / 0 = no fnd

Parameter der Registry, die von ncprwsnt.exe ausgewertet werden

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ncprwsnt]

Key	Type	Meaning	Value
WlanUsed	String	Name of last used wifi adapter. Is used for re-enabling the adapter.	<some name>
SecCliDef	DWORD	enable firewall	0/1, default: 0
SecCliFw	DWORD	enable firewall	0/2, default: 0
FipsFallbackToNcpCrypto	DWORD	fallback to old crypto if FIPS failes to initialize	0/1, default: 0
DisableDPD	DWORD	no function in trunk r31002	0/1, default: 0
EnableDefGw	DWORD	set default gateway instead of half routes (see below)	0/1, default: 0
UseHighPrio	DWORD	set own process priority	0=NORMAL, 1=HIGH, default: 0
NoHideAdapter	DWORD		0=release ports, 1=don't release ports, default: 0
PreventIkePortRelease	DWORD	release ike sockets if not used	0/1, default: 0

Ikev2AuthFollowPrf	DWORD	special handling for IKEv2 "Digitale Signatur Algorithmus" (see below)	0/1, default: 0
FullTrace	DWORD	enable full trace. Don't forgot to turn it off when done!	0/1, 2=also enable driver trace, default: 0
FullTracePath	String	full filename of fulltrace log	default: "C:\ncptrace.log"
NoMbnConnection	DWORD	disable the use of MobileBroadband API	0/1, default: 0
PrgType	DWORD	disables some NAT	0/1, default: 0

Half Routes / Default Gateway

Durch die Verwendung von Half Routes statt eines Default Gateways für den virtuellen Netzwerkadapter des NCP Clients gibt es Probleme mit der NLA (Network Location Awareness) von Windows.

Im Client-Code ist die Verwendung von Half Routes bereits über eine "TRUE-Bedingung" per Default aktiviert. Dies erfolgt durch die Abfrage eines entsprechenden Registry Keys.

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ncprwsnt]
```

Key	Type	Value
EnableDefGw	REG_DWORD	0 - Half-Routes (Standardverhalten wie bisher) / 1 - Default Gateway

Ist dieser Registry Wert nicht vorhanden, arbeitet der Client wie EnableDefGw = 0

IKEv2AuthFollowPRF

Gültig ab Version 10.10.3

```
[System\CurrentControlSet\Services\ncprwsnt]
```

Key	Type	Value
Ikev2AuthFollowPrf	WORD	1

Dies ist erforderlich, wenn die "Digitalen Signaturalgorithmen" dem ausgehandelten "PRF" folgen sollten, anstatt den Standard-SHA1 zu verwenden. Im Fall von Cisco-ASA wird dies automatisch durchgeführt, ohne dass dieser Eintrag erforderlich ist. Dieser Eintrag ist hinfällig, sobald alle Gateways dem neuen RFC folgen.

Routing Functionality of the Client

```
[HKLM\System\CurrentControlSet\Services\ncprwsnt]
```

Key	Type	Value	Description
-----	------	-------	-------------

SecIRtr.	REG_DWORD	0=disallow, 1=allow, default=0	Allow client to route
SecIRtrNet	REG_SZ	(example) 192.168.254.0/24,192.168.253.0/24	When routing allowed, specifies the source nets negotiated

Routing selbst muss unabhängig vom Betriebssystem aktiviert werden, da dies nicht automatisch erfolgt.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters]

Key	Type	Value
IPEnableRouter	REG_DWORD	1

DNS Handling on non NCP Adapters

Zusätzliche Unterstützung für einen Registrierungsschlüssel für die Steuerung der DNS-Behandlung auf Nicht-NCP-Adapttern im verbundenen Zustand.

[HKLM\System\CurrentControlSet\Services\ncprwsnt]

Key	Type	Value
DNSHandling	DWORD (32-bit)	0=throw away /default), 1 = respond "no such name", 2 = icmp unreachable response, 3 = pass through

Allgemeine Registry-Werte

ConnectState

Der Registry-Wert gibt den aktuellen Verbindungsstatus zurück.

Registry-Schlüssel:

HKEY_LOCAL_MACHINE\SOFTWARE\NCP engineering GmbH\NCP Secure Client
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\NCP engineering GmbH\NCP Secure Client

Name:

ConnectState

Werte:

- 0 = Verbindung ist getrennt
- 1 = Verbindung wird aufgebaut
- 2 = Verbindung ist erfolgreich aufgebaut
- 3 = Internetverbindung ist unterbrochen, VPN-Verbindung wird gehalten