

NCP Secure Entry Client

Administrationshandbuch

© NCP engineering GmbH 2023

Version 4.70 macOS



Next Generation Network
Access Technology

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

Online-Hilfe	8
Produktbeschreibung	9
Konfigurations-Tipps	10
Profil-Erstellung	11
Verbindungs Aufbau	12
FIPS-Zertifizierung	13
Anpassung der GUI	13
Zertifikats-Konfiguration	14
Konfigurationsparameter	15
Einstellungen	19
Zertifikate [Konfiguration]	20
Benutzer-Zertifikat	21
PIN-Richtlinie	21
Zertifikatsverlängerung	22
Computer Zertifikat	22
IPsec Konfiguration	24
IKEv1-Richtlinie [IPsec-Konfiguration]	26
Name [IKE-Richtlinie]	27
Authentisierung [IKE-Richtlinie]	27
Verschlüsselung [IKE-Richtlinie]	27
Hash [IKE-Richtlinie]	27
IKEv2-Richtlinie [IPsec-Konfiguration]	28
Name [IKEv2-Richtlinie]	28
Verschlüsselung [IKEv2-Richtlinie]	28
Pseudorandom-Funktion [IKEv2-Richtlinie]	28
Integritäts-Algorithmus [IKEv2-Richtlinie]	29
IPsec-Richtlinie [Profile]	30
Name [IPsec-Richtlinie]	31
Protokoll [IPsec-Richtlinie]	31
Transformation / Verschlüsselung	31
Authentisierung [IPsec-Richtlinie]	31
Proxy für VPN Path Finder	32

Software Update über LAN [Konfiguration]	33
EAP-Optionen [Konfiguration]	34
Profile [Parameter]	35
Grundeinstellungen [Profile]	37
Profil-Name	38
Verbindungssteuerung [Profile]	39
Verbindungsaufbau [Verbindungssteuerung]	40
Timeout [Verbindungssteuerung]	41
Voice over IP (VoIP) priorisieren	41
Logischen VPN-Tunnel bei Verbindungsunterbrechung trennen	42
IPsec [Profile]	42
Gateway (Tunnel-Endpunkt)	43
IPsec-Richtlinie [Auswahl]	43
Austausch-Modus (IPsec) [Profile]	44
Tunnel IP-Version	46
Gültigkeitsdauer [Richtlinie]	46
Art der Gültigkeit (IPsec) [Richtlinie]	46
Dauer [Security]	47
Volumen [Richtlinie]	47
PFS / DH-Gruppe	47
Erweiterte IPsec-Optionen	48
IPsec-Kompression	48
Deaktiviere DPD (Dead Peer Detection)	48
VPN Path Finder	48
Identität	50
Typ [Identität]	51
IKE ID [Profile]	51
Zertifikatskonfiguration [Profile]	52
IPsec Pre-shared Key [Tunnel-Parameter]	52
Extended Authentication (XAUTH)	52
IPsec-Adresszuweisung	53
Zuweisung der privaten IP-Adresse	53
DNS Server	53
Domain Name	54
Split Tunneling / Netzwerk-Gegenstelle	56
Entfernte Netzwerke (IPv4)	56
Auch lokale Netze im Tunnel weiterleiten	57

Entfernte Netzwerke (IPv6)	57
Zertifikats-Überprüfung	58
Benutzer des eingehenden Zertifikats	58
Aussteller des eingehenden Zertifikats	60
Fingerprint des Aussteller-Zertifikats	61
Benutze SHA1 Fingerprint statt MD5	61
Erweiterte Authentisierung [Authentisierung vor VPN]	62
IKEv1 / IKEv2	62
IKEv1-Richtlinie	63
IKEv2-Richtlinie	63
Gültigkeitsdauer [Richtlinie]	64
IKE DH-Gruppe [IKE-Richtlinie]	65
IKE ID-Typ [Profile]	66
IKE ID [Profile]	66
Ansicht	67
Profilauswahl anzeigen	67
Statistik anzeigen	67
Verbinden / Trennen	68
Verbindungsinformationen	68
Zertifikate [Ansicht]	70
Aussteller-Zertifikat anzeigen	71
Benutzer-Zertifikat anzeigen	73
Eingehendes Zertifikat anzeigen	75
CA-Zertifikate anzeigen	78
Hardware-Zertifikat (Ansicht)	80
PIN eingeben	82
PIN zurücksetzen	82
PIN ändern	83
Konfigurationssperren	83
Sperre aufheben	84
Beenden	85

Logbuch	86
Lizenzierung	88

Online-Hilfe

Die Struktur der Online-Hilfe für den [NCP Secure Entry Client](#)^[10]

Einstellungen: Globale Einstellungen, die für alle VPN-Verbindungen gültig sind, können vorgenommen werden

- zur Verwendung der [Zertifikate](#)^[14]
- für die [IPsec-Konfiguration](#)^[24]
- zum Einsatz von [VPN Path Finder](#)^[48]
- für das [EAP](#)^[34]

Profile: In einem Profil sind die Konfigurationsdaten für die jeweilige VPN-Verbindung gespeichert, insbesondere die Zugangsdaten für ein bestimmtes VPN-Gateway. Nachdem eines der angelegten [Profile](#)^[11] aus dem Pull-Down-Menü im Client Monitor ausgewählt wurde, kann die VPN-Verbindung zum entsprechenden Ziel-Gateway aufgebaut werden. Neue Profile können über diesen Menüpunkt manuell oder mit Hilfe eines Assistenten erstellt werden.

Verbindung

Eine VPN-Verbindung kann über das Menü [Verbindung](#)^[12] manuell aufgebaut oder wieder getrennt werden. Unter diesem Menüpunkt können Sie sich auch die eingesetzten [Zertifikate anzeigen](#)^[70] lassen und die PIN eingeben, zurücksetzen oder ändern. Sollten [Parameter-Sperren](#)^[84] seitens des zentralen Managements konfiguriert sein, so können diese über das Verbindungs-Menü deaktiviert werden. Hierzu ist die Kenntnis eines im zentralen Management vorkonfigurierten Benutzernamens und Passworts notwendig.

Bearbeiten

Unter Bearbeiten können markierte Texte kopiert und an anderer Stelle wieder eingesetzt werden, sowie bestimmte Sonderzeichen abgerufen werden.

Ansicht

Im Menüpunkt [Ansicht](#)^[13] lässt sich das Aussehen der GUI verändern. So lässt sich beispielsweise eine Statistik ein- oder ausblenden, sowie das Pull-Down Menü mit der Profilauswahl.

Log

Mit der [Log](#)^[86]-Funktion werden die Kommunikationsereignisse der Client Software protokolliert. Über dieses Menü können Sie die aktuellen Log-Ausgaben einsehen oder eine Log-Datei anlegen.

Hilfe

Über das Menü [Hilfe / NCP Secure Entry Client](#)^[10] erhalten Sie [Konfigurations-Tipps](#)^[10].

Zu jedem der Untermenüpunkte des Clients wurde ein eigenes Hilfe-Kapitel mit Index und ggf. ein Konfigurationstipp angelegt. Von diesen beiden Hilfeseiten gelangen Sie zu den Funktionsbeschreibungen der einzelnen Parameter. Die entsprechenden Funktionsbeschreibungen werden auch dann geöffnet, wenn Sie im jeweiligen Konfigurationsfeld der Profil-Einstellungen am Monitor den Hilfe-Button betätigen.

Tipps für den schnellen Einsatz des Clients

[Das VPN-Profil für die Verbindung zum Firmennetz erstellen](#) ¹¹

[So wird die VPN-Verbindung aufgebaut](#) ¹²

[Wenn ein Zertifikat eingesetzt wird](#) ¹⁴

[FIPS-Zertifizierung](#) ¹³

[Wie die Oberfläche des Clients angepasst werden kann](#) ¹³

Übersicht:

[Alle Konfigurationsbereiche und ihre Parameter](#) ¹⁵

Produktbeschreibung

Der *NCP Secure Entry Client* kann in beliebigen VPN-Umgebungen eingesetzt werden. Er kommuniziert auf der Basis des IPsec-Standards mit den Gateways verschiedenster Hersteller und ist die Alternative zu der am Markt angebotenen, einheitlichen IPsec-Client-Technologie.

Die Client Software nutzt für den Verbindungsaufbau zum Gateway die zuvor eingerichtete Standard-Verbindung ins Internet.

Weitere Leistungsmerkmale erleichtern den Einstieg in eine ganzheitliche Remote Access VPN-Lösung:

- * Kompatibilität mit nahezu allen marktgängigen VPN-Gateways
- * Extending Authentication (XAUTH)-Support zur Authentisierung mittels USER ID/Passwort und/oder OTP
- * Internet Key Exchange Config Mode (IKE CFG) für eine dynamische Zuweisung von IP-Adresse, DNS Server und Domain Name
- * Dead Peer Detection (DPD)- Konfiguration bei Tunnel Failover – Benutzerkonfigurierbare Zeitintervalle bei DPD-Vorfällen zur flexibleren Kontrolle für die Wiederherstellung von VPN-Tunnel
- * Network Address Translation-Traversal (NAT-T) für die Kommunikation zwischen Client und Gateway über Netzwerkkomponenten, die NAT durchführen
- * Einsatz digitaler Zertifikate in einer Public Key-Infrastruktur (PKI)
- * Grafische Benutzeroberfläche

Client Monitor – Grafische Benutzeroberfläche

Die grafische Oberfläche des Clients schafft Transparenz für den Benutzer. Sie informiert den Benutzer darüber, ob der Computer online ist und wie lange, wie der aktuelle Datendurchsatz ist und zu welcher Zieladresse er verbunden ist.

PKI-Unterstützung

Die Zugangssicherheit zum Computer und damit dem Firmennetz kann durch den Einsatz digitaler Zertifikate in Form von Soft-Zertifikaten (PKCS#12) oder den Einsatz der PKCS#11-Schnittstelle erhöht werden. Der Client unterstützt hierfür die Einbindung in eine PKI (Public Key Infrastruktur).

Unterstützung der High Availability Services

Der Client kann Failsafe- und Loadbalancing-Server für max. Verfügbarkeit und gleichmäßige Auslastung aller zentralen Gateways nutzen.

Management-fähig

Der Client kann über das NCP Secure Enterprise Management (SEM) für die zentrale Verwaltung eines VPN administriert werden.

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 einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

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

Die entsprechenden Module können in den [IPsec-Einstellungen](#)²⁴ konfiguriert werden.

Konfigurations-Tipps

In den Tipps sind die wichtigsten und am häufigsten angewendeten Konfigurationsprozeduren beispielhaft beschrieben. Folgende Titel sind angeboten:

[Das VPN-Profil für die Verbindung zum Firmennetz erstellen](#)¹¹

[So wird die VPN-Verbindung aufgebaut](#)¹²

[Wenn ein Zertifikat eingesetzt wird](#)¹⁴

[FIPS-Zertifizierung](#)¹³

[Wie die Oberfläche des Clients angepasst werden kann](#)¹³

[Übersicht der Konfigurationsbereiche und ihrer Parameter](#)¹⁵

Profil-Erstellung

In den Tipps sind die wichtigsten und am häufigsten angewendeten Konfigurationsprozeduren beispielhaft beschrieben.

[So wird die VPN-Verbindung aufgebaut](#) ¹²

[Wenn ein Zertifikat eingesetzt wird](#) ¹⁴

[FIPS-Zertifizierung](#) ¹³

[Wie die Oberfläche des Clients angepasst werden kann](#) ¹³

Mit Hilfe eines Assistenten können am Client eine Vielzahl von Profilen angelegt werden, die nach Bedarf bequem per Mausklick aus der [Profil-Auswahl](#) ⁶⁷ für den Verbindungsaufbau selektiert werden können.

Profile mit Assistent erstellen

Selektieren Sie "Profile" im Menü der Client-GUI und öffnen Sie mit Klick auf den Button [+] den Assistenten für ein neues Profil.

Anschließend geben im folgenden Fenster einen frei wählbaren Namen für das zu erstellende Profil ein.

Die „VPN Gateway-Parameter“ und die weitergehende „IPsec-Konfiguration“ müssen mit dem Administrator des IPsec Gateways abgestimmt sein. Von ihm erhalten Sie die benötigten Daten.

Profile manuell erstellen und abändern

Diese Daten können auch zu einem späteren Zeitpunkt eingegeben oder geändert werden, nachdem das Profil zum ersten Mal gespeichert wurde.

Unten sind die wichtigsten Parameter aufgeführt. In eckigen Klammern dahinter ist angegeben, in welchen Parameterfeldern der Profil-Einstellungen sie sich befinden.

[Gateway \(Tunnel-Endpunkt\)](#) ⁴³

[Extended Authentication](#) ⁵²

[Erweiterte IPsec-Optionen](#) ⁴⁸ mit VPN Path Finder

[IPsec-Einstellungen](#) ²⁴ zu den jeweiligen Richtlinien

[IP-Adressen-Zuweisung](#) ⁵³ [[IPsec-Adresszuweisung](#) ⁵³]

[DNS Server](#) ⁵³

Speichern Sie das neue [VPN-Profil](#) ³⁵. Haben Sie eine Vielzahl verschiedener Profile angelegt, können Sie diese in [Gruppen](#) ³⁵ organisieren und nach verschiedenen Kriterien anzeigen lassen.

Hinzufügen / Importieren

Klicken Sie auf diese Schaltfläche, um einen Assistenten zu starten, mit dem Sie entweder ein neues Profil konfigurieren oder ein vorhandenes Profil importieren können.

Der Client unterstützt verschiedene Arten von Importdateien (* .ini).

Extended Authentication (XAUTH) mit Zertifikat

Soll statt Benutzername und Passwort ein Zertifikat für die Extended Authentication eingesetzt werden, so muss eine [Zertifikats-Konfiguration](#)^[14] ausgeführt werden. Dazu selektieren Sie im Menü *NCP Secure Entry Client* die Menüpunkte [Einstellungen](#)^[19] und [Zertifikate](#)^[20].

Verbindungsaufbau

Die VPN-Verbindung zwischen Rechner und Firmennetz kann mit dem MAC Client mit nur einem Klick hergestellt werden, wenn eine Internet-Verbindung über ein beliebiges Verbindungsmedium besteht und ein Profil eingerichtet wurde, worin Ihre persönlichen Daten und die Daten für das VPN Gateway hinterlegt sind. Der [Verbindungsaufbau](#)^[40] kann jedoch auch automatisch erfolgen oder wechselnd zwischen manuell und automatisch.

In den Einstellungen der Profile werden dafür drei Verbindungsmodi im Parameterfeld [Verbindungssteuerung](#)^[39] zur Verfügung gestellt.

Manueller Verbindungsaufbau

Die Standard-Einstellung für den Verbindungsaufbau ist "Manuell". In diesem Fall müssen Sie die Verbindung manuell herstellen, d. h. den Verbindungsschalter betätigen. Ein Trennen der Verbindung erfolgt je nach eingestelltem Wert für den Timeout. Ist der Timeout auf Null (0) gesetzt, d. h. kein Timeout eingestellt, muss die Verbindung manuell getrennt werden.

Sollten Sie diesen Modus für den Verbindungsaufbau nutzen, so sollten Sie den Timeout aktivieren und auf einen deutlich höheren Wert als null (0) setzen, um den Verbindungsabbau für den Fall zu automatisieren wenn keine Nutzdaten mehr fließen. Andernfalls könnten unnötige Verbindungskosten für Sie entstehen.

Automatischer Verbindungsaufbau

Bei Verwendung der Client Software muss lediglich die entsprechende Applikations-Software gestartet werden (E-Mail, Internet Browser, Terminal Emulation, etc.), um den automatischen Verbindungsaufbau für das jeweilige Profil anzustoßen.

Die Verbindung zur Gegenstelle wird automatisch nach den Einstellungen des aktuell selektierten Profils hergestellt. Dies bedeutet, dass Benutzername und Passwort für den Internet-Diensteanbieter im Parameterfeld Netzeinwahl eingetragen sein müssen, da ansonsten die Automatik bei der Passwortabfrage stehen bleibt und keine Verbindung zustande kommt.

Das automatische Trennen der Verbindung erfolgt durch den Timeout.

Wechselnder Verbindungsaufbau

Nachdem Sie den Modus des wechselnden Verbindungsaufbaus eingestellt haben, muss die Verbindung zunächst "manuell" aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau:

Wird die Verbindung nun mit Timeout, also automatisch, beendet, so wird die Verbindung bei der nächsten Anforderung, z. B. durch den Browser, "automatisch" aufgebaut. Wird die Verbindung manuell durch Betätigen des Verbindungsschalters abgebaut, muss sie auch wieder manuell aufgebaut werden.

Beachten sie auch beim wechselnden Verbindungsaufbau: Ist der Timeout auf Null (0) gesetzt, d. h. kein Timeout eingestellt, müssen Sie in jedem Fall die Verbindung manuell trennen.

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 einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

- Diffie Hellman-Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 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 über das [IPsec](#)^[42]-Menü eingesehen werden. Die entsprechenden Module können in den [IPsec-Einstellungen](#)^[24] konfiguriert werden.

Anpassung der GUI

Das Aussehen der Client-Oberfläche kann durch unterschiedliche Eingriffe verändert werden. So wird die Oberfläche des Clients Monitors über das Menü [Ansicht](#)^[67] variiert. Die Konfigurationsoberfläche in den Profil-Einstellungen und das Konfigurationsmenü selbst kann mit gezielten [Parametersperren](#)^[83] durch den Administrator verändert werden.

Monitor-Oberfläche

Das Ansichts-Menü dient dazu, verschiedene Informations- und Statistikfelder ein- oder auszublenden und so die Größe des Monitors auf dem Bildschirm je nach Bedarf mit Informationsfeldern zu vergrößern oder durch Ausschalten aller Felder auf die kleinste Form zusammenzuschieben. Auch kann der Monitor zum Icon verkleinert werden, das in der Menüleiste angezeigt wird (siehe Menü [Ansicht](#)^[67]).

Konfigurations-Oberfläche

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

Die Parametersperren können wieder aufgehoben werden. Dazu muss Benutzername und Passwort eingegeben werden. Siehe dazu [Parametersperre aufheben](#) ⁸⁴.

Zertifikats-Konfiguration

Mit dem vorliegenden Client können beliebig viele verschiedene Zertifikate eingesetzt werden. Welches der am Rechner zur Verfügung stehenden Zertifikate in welcher Weise zum Einsatz kommt, kann in einer Zertifikatskonfiguration definiert werden.

Wenn Sie im Einstellungsmenü des Clients den Menüpunkt "Zertifikate" zum ersten Mal selektieren, wird die [Standard Zertifikatskonfiguration](#) ²⁰ "ohne" ein Zertifikat angezeigt.

Wenn Sie diese Konfiguration bearbeiten und sich für eine der angebotenen Zertifikatsarten entschieden haben, können Sie je nach Art des Zertifikats - ob auf Festplatte gespeichertes Soft-Zertifikat (PKCS#12-Datei) oder von einem Token (PKCS#11-Modul) gelesen - typenspezifische Einstellungen vornehmen.

Die Standard-Zertifikats-Konfiguration bleibt immer erhalten. Eine zusätzliche Zertifikats-Konfiguration muss unter einem anderen Namen gespeichert werden.

Eine weitere Zertifikatskonfiguration kann zur gleichen Zertifikatsart aber unterschiedlichem Soft-Zertifikat oder zu einer anderen Zertifikatsart angelegt werden. Auf diese Weise können Sie beliebig viele Zertifikatskonfigurationen hinzufügen.

Aus den verschiedenen Zertifikatskonfigurationen kann pro Profil jeweils eine selektiert werden. Dadurch besteht die Möglichkeit der Authentisierung mit unterschiedlichen Zertifikaten gegen verschiedene VPN-Gegenstellen, z. B. zu VPN Gateway 1 mit Soft-Zertifikat (PKCS#12) und zu Gateway 2 mit einem auf einem Token gespeicherten Zertifikat (PKCS#12).

Für welche VPN-Verbindung welche Zertifikats-Konfiguration verwendet wird, können Sie in den Profil-Einstellungen festlegen. Im Konfigurationsmenü des Monitors selektieren Sie "Profile" und wählen zunächst das gewünschte Profil aus. Öffnen Sie dann das Parameterfeld "Security".

Hier selektieren Sie die gewünschte Zertifikatskonfiguration. Das Zertifikat, das auf diese Weise für dieses VPN-Profil verwendet wird, dient der Authentisierung im IPsec-Verbindungsaufbau (zum IKE-Schlüsselaustausch).

Das gleiche Zertifikat kann durch einen weiteren Konfigurationsschritt anstatt eines Pre-shared Keys auch zur Verschlüsselung verwendet werden ([XAUTH mit Zertifikat](#)⁵²). Anstatt Benutzername und Passwort unter [Identität](#)⁵² einzugeben, kann eines der im Auswahlfenster angebotenen Zertifikatsfelder gewählt werden, woraus dann die entsprechenden Inhalte für die Authentisierung am Gateway verwendet werden.

Ansicht der Zertifikate

[Zertifikate \[Ansicht\]](#)⁷⁰

[Aussteller-Zertifikat anzeigen](#)⁷¹

[Benutzer-Zertifikat anzeigen](#)⁷³

[Eingehendes Zertifikat anzeigen](#)⁷⁵

[CA-Zertifikate anzeigen](#)⁷⁸

PIN-Handling

[PIN eingeben](#)⁸⁰

[PIN zurücksetzen](#)⁸²

[PIN ändern](#)⁸³

Verwendung der Zertifikate

[Zertifikate \[Konfiguration\]](#)²⁰

[Benutzer-Zertifikat](#)²¹

[PIN-Richtlinie](#)²¹

[Zertifikatsverlängerung](#)²²

[Zertifikats-Überprüfung](#)⁵⁸

[Benutzer des eingehenden Zertifikats](#)⁵⁸

[Aussteller des eingehenden Zertifikats](#)⁶⁰

[Fingerprint des Aussteller-Zertifikats](#)⁶¹

[Benutze SHA1 Fingerprint statt MD5](#)⁶¹

Konfigurationsparameter

[Einstellungen von Zertifikaten](#)⁵²

[Zertifikate \[Konfiguration\]](#)²⁰

[Benutzer-Zertifikat](#)²¹

[PIN-Richtlinie](#)²¹

[Zertifikatsverlängerung](#)²²

[Einstellung der IPsec-Richtlinien](#)

[IKEv1-Richtlinie \[IPsec-Konfiguration\]](#) 

[Name \[IKE-Richtlinie\]](#) 

[Authentisierung \[IKE-Richtlinie\]](#) 

[Verschlüsselung \[IKE-Richtlinie\]](#) 


[Hash \[IKE-Richtlinie\]](#) 

[IKEv2-Richtlinie \[IPsec-Konfiguration\]](#) 

[Name \[IKEv2-Richtlinie\]](#) 

[Verschlüsselung \[IKE-Richtlinie\]](#) 

[Pseudorandom-Funktion \[IKEv2-Richtlinie\]](#) 

[Integritäts-Algorithmus \[IKEv2-Richtlinie\]](#) 

[IPsec-Richtlinie \[Profile\]](#) 

[Name \[IPsec-Richtlinie\]](#) 

[Protokoll \[IPsec-Richtlinie\]](#) 

[Verschlüsselung \[IPsec-Richtlinie\]](#) 

[Authentisierung \[IPsec-Richtlinie\]](#) 


[EAP-Optionen](#)

[Einstellungen der Profile](#)

[Grundeinstellungen \[Profile\]](#) 

[Verbindungssteuerung \[Profile\]](#) 

[Verbindungsaufbau \[Verbindungssteuerung\]](#) 

[Timeout \[Verbindungssteuerung\]](#) 

[Voice over IP \(VoIP\) priorisieren](#) 

[Logischen VPN-Tunnel bei Verbindungsunterbrechung trennen](#) 

[Erweiterte Authentisierung \[Authentisierung vor VPN\]](#) 

[IPsec](#) 

[Gateway \(Tunnel-Endpunkt\)](#) 

[IPsec-Richtlinie \[Auswahl\]](#) 

[Art der Gültigkeit \[Richtlinie\]](#) 

[Dauer \[Security\]](#) 

[Volumen \[Richtlinie\]](#) 

[PFS / DH-Gruppe \[Auswahl\]](#) 

[IPsec Kompression](#) 

[Erweiterte IPsec-Optionen](#) 

[Deaktiviere DPD \(Dead Peer Detection\)](#) 

[VPN Path Finder](#) 

[IPsec-Adresszuweisung](#) 

[Zuweisung der privaten IP-Adresse](#) 

[DNS Server](#) 

WINS Server

[Domain Name](#) 

[Split Tunneling \[Profile\]](#) 

[Remote Networks \[Split Tunneling\]](#)  56

Schließen der GUI

[Beenden](#)  85

Bedienung unter dem Menüpunkt "Verbindung"

Verbindung

[Verbinden / Trennen](#)  68

Ansicht der Zertifikate

[Zertifikate \[Ansicht\]](#)  70

[Aussteller-Zertifikat anzeigen](#)  71

[Benutzer-Zertifikat anzeigen](#)  73

[Eingehendes Zertifikat anzeigen](#)  75

PIN Handling

[PIN eingeben](#)  82

[PIN zurücksetzen](#)  82

[PIN ändern](#)  83

Parametersperren

[Parametersperren aufheben / wiederherstellen](#)  84

Informationen unter dem Menüpunkt "Ansicht"

[Ansicht \[Menü\]](#)  67

[Profilauswahl anzeigen](#)  67

[Statistik anzeigen](#)  67

Informationen unter dem Menüpunkt "Log"

[Log](#)  86

Lizenzierung unter dem Menüpunkt "Hilfe"




[Hilfe](#)  10

[Lizenzierung](#)  88

Einstellungen

Unter dem Menüpunkt **NCP Secure Entry Client** (mit Konfiguration) können manuell die wichtigsten Konfigurationseinstellungen vorgenommen werden.

Dies betrifft die Einstellungen:

- [für die IPsec-Richtlinien](#)  24
- [zur Verwendung der Zertifikate](#)  20
- [zum Einsatz von VPN Path Finder](#)  32

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](#) ²¹

[PIN-Richtlinie](#) ²¹

[Zertifikatsverlängerung](#) ²²

[Computer-Zertifikat](#) ²²

Name und "Standard Zertifikatskonfiguration"

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

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

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.

PKCS#11-Modul:

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

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.:

%INSTALLDIR%/Certs/Test.p12

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.

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.

Schlüsselbund

Das Zertifikat wird über die Schlüsselbundverwaltung in den Schlüsselbund "System" mit dem Private Key importiert. Wurde ein Zertifikat entsprechend importiert, so kann dies vom Client zur Authentisierung genutzt werden.

Subject CN / Issuer CN

Das jeweilige Zertifikat vom Schlüsselbund kann mit dem zugehörigen Common Name von Antragsteller und Aussteller (Subject CN und Issuer CN) selektiert werden, wenn mehrere Zertifikate vorhanden sind.

Tragen Sie den entsprechenden String entweder in das Feld für Subject CN oder in das für Issuer CN ein. Beachten Sie dabei:

- a) der String kann Sterne (*) für Wildcards enthalten.
- b) wenn der Such-String mit einem Zirkumflex ˆ beginnt, bezeichnet der String genau den Ausdruck, der für die Suche verwendet werden soll.

IPsec Konfiguration

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).

Siehe auch:

[Gateway \(](#) [Tunnel Endpunkt\)](#)
[Austausch-Modus \[Profile\]](#) [IKEv2-Richtlinie \[Auswahl\]](#)

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.

Unter der IPsec-Richtlinie finden sie die Richtlinie "ESP-AES128-MD5".

Nach der Maßgabe der IPsec-Richtlinie wird festgelegt, wie die Nutz-Daten gemäß des IPsec-Protokolls bearbeitet werden s

Nach der Maßgabe der IKE-Richtlinie wird die Authentisierungsverhandlung zwischen Client (IPsec-Initiator) und Gegenstel

Siehe auch:

[IKEv1-Richtlinie \[IPsec-Konfiguration\]](#)

[IKEv2-Richtlinie \[IPsec-Konfiguration\]](#)

[IPsec-Richtlinie \[Profile\] \(Phase 2-Parameter\)](#)

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.

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-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 \[IKEv2-Richtlinie\]](#)  
[Verschlüsselung \[IKEv2-Richtlinie\]](#) 
[Pseudorandom](#)  [Funktion \[IKEv2-Richtlinie\]](#) 
[Integritäts-Algorithmus \[IKEv2-Richtlinie\]](#) 

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 [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 \[IPsec-Richtlinie\]](#)  31
[Protokoll \[IPsec-Richtlinie\]](#)  31
[Verschlüsselung \[IPsec-Richtlinie\]](#)  31
[Authentisierung \[IPsec-Richtlinie\]](#)  31

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.

Proxy für VPN Path Finder

Wurde die Funktionalität VPN Path Finder unter [Erweiterte IPsec-Optionen](#)⁴⁸ 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.

Software Update über LAN [Konfiguration]

Befindet sich der Secure Client im Firmennetz, so kann er ohne VPN-Tunneling ein Software Update vom Management Server erhalten, wenn am Management-System für seine RSUID ein Eintrag vorliegt.

Erster / Zweiter Management Server

Dies ist die IP-Adresse des Management Servers im Firmennetz (LAN).

Benutzername

Den Benutzernamen (RSUID) erhalten Sie von Ihrem Systemadministrator.

EAP-Optionen [Konfiguration]

In den "EAP-Optionen" des Monitor-Menüs kann angegeben werden, ob die EAP-Authentisierung (802.1x) für 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

Der Einsatz des Extensible Authentication Protocol 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](#)^[52] und das [Passwort](#)^[52] ([Identität](#)^[52]) verwendet werden oder ein eigener "EAP-Benutzername" mit einem "EAP-Passwort".

Zertifikatsinhalte können dergestalt automatisch übernommen werden, indem aus dem Konfigurationsfeld [Identität](#)^[50] / [Extended Authentication](#)^[52] der [Benutzername](#)^[52] und das [Passwort](#)^[52] vom Zertifikat übernommen werden oder in den EAP-Optionen "Verwende VPN-Benutzername und VPN-Passwort" aktiviert wird.

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

Commonname: %CERT_CN%

E-Mail: %CERT_EMAIL%

Profile [Parameter]

In diesem Fenster werden die bereits eingerichteten Profile in einer Liste angezeigt.

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 eines Profils zu editieren, wählen Sie mit der Maus das Profil aus und klicken Sie anschließend auf den [Bearbeiten]-Button.

Die Profil-Einstellung zeigt nun im linken Fenster eine Liste von Begriffen, denen jeweils ein Parameterfeld zugeordnet ist:

Grundeinstellungen [Profile]	37
Verbindungssteuerung [Profile]	39
IPsec [Konfiguration]	42
Erweiterte IPsec-Optionen	48
Identität	50
IPsec-Adresszuweisung	53
Split Tunneling	56
Zertifikats-Überprüfung	58
Erweiterte Authentisierung	62

Profil-Gruppen

In der Anzeige aller Profile sind diese nach ihrem Namen sortiert.

Sollte die Liste der Profile zu lang sein, so können die Profile auch gruppiert werden. Dazu wird auf den Gruppieren-Button geklickt und die Gruppen-Konfiguration geöffnet.

Mit [+] 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 [-] 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 kann im Bereich der Profilauswahl nach einem rechten Mausklick die Anzeige aller Profile oder nur die Profile einer bestimmten Gruppe ausgewählt werden kann.

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, siehe [Profil-Name](#) ³⁸.

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.

Verbindungssteuerung [Profile]

In diesem Parameterfeld bestimmen Sie, wie der "Verbindungsaufbau" erfolgen soll und stellen die Timeout-Werte ein.

Siehe auch die Parameter:

[Verbindungsaufbau \[Verbindungssteuerung\]](#)  40

[Timeout \[Verbindungssteuerung\]](#)  41

[Voice over IP \(VoIP\) priorisieren](#)  41

[Logischen VPN-Tunnel bei Verbindungsunterbrechung trennen](#)  42

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.

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.

Hinweis: Um den Timeout zu aktivieren, ist es nötig, einen Wert zwischen 1 und 65536 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.

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.

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.

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 verwendet wird.

IPsec [Profile]

Hier können die vorkonfigurierten IPsec-Richtlinien selektiert werden, sowie die Verschlüsselung festgelegt und ggf. die IPsec-Kompression eingestellt werden:

[Gateway \(Tunnel-Endpunkt\)](#)  43

[Austausch-Modus](#)  44

[Tunnel IP-Version](#)  46

[IKE-Richtlinie](#)  62

[IKE DH Gruppe](#)  65

[IPsec-Richtlinie](#)  43

[PFS-Gruppe \(DH-Gruppe\)](#)  47

[Gültigkeit](#)  46

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.

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.

IPsec-Richtlinie [Auswahl]

automatischer Modus:

In diesem Fall kann die Konfiguration der IPsec-Richtlinie über die IPsec-Konfiguration entfallen.

ESP-AES256:

Als Alternative zum automatischen Modus kann diese vorkonfigurierte IPsec-Richtlinie eingesetzt werden.

Vorkonfiguriert befindet sich dort als Standard ESP AES_GCM256. Vorkonfiguriert: ESP-AES128-MD5.

Soll der IPsec Client spezielle Richtlinien verwenden, so müssen diese in den „[IPsec](#) ²⁴“-Einstellungen“ erstellt oder modifiziert werden.

Austausch-Modus (IPsec) [Profile]

Der Austausch-Modus bestimmt wie der Internet Key Exchange vonstatten gehen soll. Zwei Modi stehen zur Verfügung, der Main Mode (IKEv1), auch Identity Protection Mode und der Aggressive Mode (IKEv1). Die Modi unterscheiden sich durch die Anzahl der Messages und durch deren Verschlüsselung.

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](#) ⁴⁴ 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.

Beachten Sie, dass Split-Tunneling nur für IPv6 sichtbar ist, wenn der Austauschmodus IKEv2 ausgewählt ist und die Tunnel-IP-Version IPv6 eingestellt ist.

Gültigkeitsdauer [Richtlinie]

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 \[Richtlinie\]](#) ⁴⁶
[Dauer der Gültigkeit \[Richtlinie\]](#) ⁶⁴
[kBytes \[Richtlinie\]](#) ⁴⁷

Art der Gültigkeit (IPsec) [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.

Dauer [Security]

Bestimmt die Gültigkeitsdauer einer SA, die nach der IPsec-Richtlinie erstellt wurde. Nach Ablauf der Zeitspanne (in Sekunden), erfolgt eine neue SA-Verhandlung.

Volumen [Richtlinie]

Die Menge der hier angegebenen kBytes, die zwischen Client und Server übertragenen werden, bestimmt die Gültigkeitsdauer einer Security Association (siehe [IPsec-Richtlinie](#)^[24]). Nach Übertragung der angegebenen kBytes findet eine neuerliche SA-Verhandlung statt. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt.

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.

Erweiterte IPsec-Optionen

Siehe auch die Parameter:

[IPsec-Kompression](#)
[Deaktiviere DPD \(Dead Peer Detection\)](#)
[VPN Path Finder](#)

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.

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.

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.

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](#)

[Extended Authentication \(XAUTH\)](#)

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 [Profile]

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.

Entsprechend dem [IKE ID-Typ](#)⁵¹ muss die zugehörige "IKE ID" als String eingetragen werden.

Zertifikatskonfiguration [Profile]

Ein über die Zertifikatskonfiguration des Client-Monitors eingesetztes Zertifikat, kann hier für die erweiterte Authentisierung (XAUTH) selektiert werden.

Siehe auch:

[Benutzer-Zertifikat](#) ²¹
[PIN-Richtlinie](#) ²¹
[Zertifikatsverlängerung](#) ²²

keine:

Für Datenverschlüsselung und Authentisierung wird kein Zertifikat eingesetzt.

IPsec Pre-shared Key [Tunnel-Parameter]

"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.

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.

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](#)  53

[DNS-Server](#)  53

[DNS Domains im Tunnel auflösen](#)  54

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.

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 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

Domain Name im Tunnel auflösen

In der Standard-Einstellung für ein neues VPN-Profil ist dieses Feld leer, d. h. dieser Parameter ist nicht in Funktion und alle DNS-Anfragen werden am VPN-Tunnel vorbei an den DNS Server geschickt, der (vom Provider) aus dem Internet zugewiesen wird.

Wird ein Stern "*" eingetragen, werden alle DNS-Anfragen des Clients durch den VPN-Tunnel geleitet.

Wird ein Eintrag vorgenommen, so prüft der Client die vom Rechner abgehenden DNS-Pakete danach, welcher DNS-Name angefragt wird. Sind die letzten Zeichen des in den Paketen mitgegebenen DNS-Namens identisch mit den hier eingegebenen, so werden die DNS-Anfragen durch den VPN-Tunnel geleitet. Bei Nichtübereinstimmung werden die DNS-Anfragen ins Internet weiter geschickt. DNS-Anfragen mit Namen die keinen "." enthalten, werden immer in den Tunnel geleitet.

Der per IKE Config Mode erhaltene Domain-Suffix wird automatisch der Liste der im Tunnel aufzulösenden Domainnamen hinzugefügt.

Syntax

- Der Unterschied zwischen Groß- und Kleinschreibung wird nicht beachtet.
- Alle alphanumerischen Zeichen einschließlich Minuszeichen "-" sind gestattet (0 - 9, a - z), keine Umlaute oder Sonderzeichen!
- Als Trennzeichen zwischen mehreren Domainnamen können Komma, Strichpunkt oder Leerzeichen verwendet werden.
- Als Joker können Fragezeichen "?" oder Stern "*" verwendet werden, wobei "*" nur jeweils zu Beginn des Domainnamens stehen darf.

Beispiele:

*.ncp.de ->

www.ncp.de, oder

www.intranet.ncp.de, oder

www.webserver.ncp.de, ...

www??.uni.de ->

www01.uni.de, oder

www02.uni.de, oder

www03.uni.de, ...

www.ncp-e.com -> www.ncp-e.com

Split Tunneling / Netzwerk-Gegenstelle

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 \(IPv4\)](#)  56

[Auch lokale Netze im Tunnel weiterleiten](#)  57

[Entfernte Netzwerke \(IPv6\)](#)  57

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.

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](#)  58
[Aussteller des eingehenden Zertifikats](#)  60
[Fingerprint des Aussteller-Zertifikats](#)  61
[Benutze SHA1 Fingerprint statt MD5](#)  61

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 Digit 5) oder SHA1 (Secure Hash Algorithm 1) sein.

Erweiterte Authentisierung [Authentisierung vor VPN]

Lokale biometrische Authentisierung bevor der VPN-Tunnel aufgebaut ist, ermöglicht MacOS ab der Version 10.10.

Biometrische Authentisierung

Das Aktivieren dieser Funktion bewirkt die Abfrage der Authentisierungsdaten unmittelbar nach Betätigen des Verbinden-Buttons auf der Monitor-Oberfläche des Clients. Erst nach einer erfolgreichen Authentisierung durch das Verfahren das am Betriebssystem konfiguriert wurde (Fingerabdruck-, Gesichtserkennung, PIN-Eingabe etc.), wird der VPN-Tunnelaufbau eingeleitet.

IKEv1 / IKEv2

Je nach Einstellung des [Austausch-Modus](#)^[44] wird zur weiteren Konfiguration entweder eine IKEv1-Richtlinie oder eine IKEv2-Richtlinie vorgeschlagen.

[IKEv1-Richtlinie](#)^[63] bei Auswahl des Main Mode (IKEv1), auch Identity Protection Mode, oder des Aggressive Mode (IKEv1).

[IKEv2-Richtlinie](#)^[63] bei Auswahl des IKEv2 Austausch-Modus.

Weitere Parameter:

[Gültigkeitsdauer](#)^[64] der Richtlinie

[IKE DH-Gruppe](#)^[65]

[IKE ID-Typ](#)^[51]

[IKE ID](#)^[51]

IKEv1-Richtlinie

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.

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.

IKEv2-Richtlinie

Mit dem automatischen Modus muss keine spezielle IKEv2-Richtlinie über das [IPsec-Konfigurationsmenü](#) ²⁴ erstellt werden.

Alternativ wird die [IKEv2-Richtlinie](#) ²⁸ AES-GCM256-HMAC-SHA384 bereitgestellt, die gegebenenfalls in den IPsec-Einstellungen umkonfiguriert werden kann.

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.)

IKE DH-Gruppe [IKE-Richtline]

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.

IKE ID-Typ [Profile]

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 [Profile]

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.

Entsprechend dem [IKE ID-Typ](#)⁵¹ muss die zugehörige "IKE ID" als String eingetragen werden.

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](#)  67

[Statistik anzeigen](#)  67

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.

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.

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

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.

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 (Schlüsselaustauschverfahren)

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 `keyIdentifier`s 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 `NCPPI.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 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.

Hardware-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.

Aussteller (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.

Konfigurationssperren

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!

Anschließend kann die Berechtigung, die Menüpunkte unter dem Hauptmenüpunkt „Konfiguration“ zu öffnen, für den Benutzer eingeschränkt werden. Standardmäßig kann der Benutzer alle Menüpunkte öffnen und die Konfigurationen bearbeiten. Wird zu einem Menüpunkt der zugehörige Haken mit einem Mausklick entfernt, so kann der Benutzer diesen Menüpunkt nicht mehr öffnen.

Die Bearbeitungsrechte für die Parameter in den Profil-Einstellungen sind in zwei Sparten unterteilt:

- Allgemeine Rechte
- Sichtbare Parameterfelder der Profile

Die allgemeinen Rechte beziehen sich nur auf die (Konfiguration der) Profile. Wird festgelegt „Profile dürfen neu angelegt werden“, „Profile dürfen konfiguriert werden“ bleibt jedoch ausgeschlossen, so können zwar mit dem Assistenten neue Profile definiert werden, eine nachfolgende Änderung einzelner Parameter ist dann jedoch nicht mehr möglich.

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 den Client.

Besteht noch eine Verbindung, kann in einem Abfragefenster die Verbindung mit Klick auf "Ja" getrennt werden. Danach wird auch der Client beendet.

Mit Klick auf "Nein" bleibt die Verbindung bestehen und der Client-Monitor wird beendet.

In diesem Fall 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 Client erneut starten, um eine bestehende Verbindung korrekt zu beenden!

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 NCPyymmdd.LOG generiert, wobei "yymmdd" 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:

[Datei öffnen](#)

Wenn Sie auf diesen Button klicken, erhalten Sie in einem weiteren Fenster die Möglichkeit Name und Pfad einer Datei einzugeben, in die der Inhalt des Log-Fensters geschrieben wird (Standard: ncpmon.log). Alle Transaktionen mit der Client Software, wie Anwahl und Empfang, einschließlich der Rufnummern, werden automatisch mitprotokolliert und in diese Datei geschrieben, bis Sie die Datei schließen. Wenn Sie eine Log-Datei anlegen, können Sie die Transaktionen mit dem Client über einen längeren Zeitraum verfolgen.

[Datei schließen](#)

Wenn Sie auf diesen Button klicken, wird eine Datei mit dem Log-Protokoll des Fensterinhalts geschlossen und unter einem frei zu vergebenden Namen gespeichert. Diese Datei kann zur Analyse der Transaktionen mit dem Secure Client oder zur Fehlersuche verwendet werden.

[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 „Automatisches Scrollen beenden“ 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

Lizenzierung

Unter dem Menüpunkt Lizenzierung wird die eingesetzte Software-Version und gegebenenfalls die lizenzierte Version mit Seriennummer angezeigt.

Wird die Software als Testversion eingesetzt, so kann die verbliebene Dauer der Gültigkeit im Popup abgelesen werden.